Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg: Technikgeschichte und informatikhistorische Aspekte

Von der Philosophischen Fakultät der
Technischen Universität Chemnitz genehmigte

Dissertation

zur Erlangung des akademischen Grades
doctor philosophiae (Dr.phil.)

von Dipl.-Ing. Michael Pröse,
geb. 27.9.1938 in Leipzig.

Gutachter: Prof. Dr. habil Finger
Prof. Dr. Krieger
Prof. Dr. Dr. habil Naumann
(zugleich Betreuer)

Leipzig, im Dezember 2004

Inhaltsverzeichnis

1 Einführung

ENIGMA (gr. Rätsel) ist für das Publikum weltweit ein Synonym für Begriffe wie „Chiffriermaschine“ und „Codebrechung“, dafür sorgten u.a. U-Boot-Filme und ebensolche Romane, zuletzt der vor wenigen Jahren verfilmte Roman „ENIGMA“ von R. HARRIS. Doch dessen pseudo-authentischen Darstellungen der Kriegshandlungen und Arbeiten zum Knacken des U-Boot-Codes hatten mit den realen Vorgängen kaum etwas zu tun.

Daß es außer der ENIGMA noch andere ebenso wichtige Chiffriermaschinen gab, zu deren Brechung ganz neuartige Maschinen entwickelt wurden, und welche Folgen das für den Zweiten Weltkrieg und danach hatte, davon weiß das Publikum recht wenig. Kein Wunder – es findet darüber kaum Informationen, weder in populären Lexika und Nachschlagewerken, geschweige in „Tatsachenromanen“ usw. Denn diese enthalten, wenn überhaupt, darüber oft unvollständige und/oder falsche Einträge.[1] Das ist zu bedauern, denn die Brechung der Chiffriermaschinen, das „Knacken ihrer Codes“ im Zweiten Weltkrieg, hatte eine überragende historische Bedeutung: Die Alliierten verkürzten dank des damit erreichten Informationsvorsprungs den Krieg erheblich, weil sie in der ersten Kriegshälfte manche Schwächen kompensieren und später ihre Ressourcen optimal einsetzen konnten. Alliierte Fachhistoriker schätzen, daß sonst der Krieg um bis zu zwei Jahre länger gedauert hätte, mit der Folge vieler weiterer Opfer – und möglicherweise des Abwurfs von Atombomben auf Deutschland.

Doch diese von den alliierten Entzifferungen beeinflußten historischen Vorgänge sind ausdrücklich nicht Gegenstand dieser Abhandlung. Vielmehr sollen die wissenschaftlichen, technischen und organisatorischen Umstände und Hintergründe dargelegt werden, welche die „Brechung der Codes“ ermöglichten. Und – besonders wichtig – wie und warum es dabei gelang, maschinelle Verfahren zu entwickeln und täglich effizient einzusetzen. Freilich benötigt man dazu den jeweiligen historische Kontext, um die komplexen Zusammenhänge transparenter zu machen und ebenso die Wechselwirkungen zwischen Entzifferungstechnik und Kriegsgeschehen aufzuzeigen.

Hierzu gibt es viele unvollständige, manchmal fehlerhafte Berichte auch seriöser Autoren – vermutlich eine Folge der Geheimhaltungspolitik der Alliierten, welche die Forschung sehr erschwerte. Sie wurden ergänzt und/oder berichtigt,

[1] Bspw. Stichwort „Ultra“ in: Barth, R. und Bedürftig, F.: Taschenlexikon Zweiter Weltkrieg. München 2000. Danach wurde in der „Operation ULTRA mit Hilfe eines Simultanrechners in das ENIGMA-System eingebrochen....“ usw., eine völlig unrichtige Darstellung. Vgl. hierzu 5.2.2.
Ein anderes Beispiel: Die 10-bändige Propyläen Geschichte Deutschlands (Groh, D., Hrsg., Berlin 1995, S. 400) enthält darüber ganze 2 (!) Zeilen.

und auch die Dokumentefreigaben der letzten Jahre einbezogen, so daß diese Abhandlung den aktuellen Stand enthält, bezogen auf die frei zugänglichen Informationen.

Darüber hinaus sind kaum Untersuchungen bekannt, die aufzeigen, ob die mit den Entzifferungen verbundenen wissenschaftlich-technischen Leistungen die Entwicklung der Digitalelektronik beeinflußten und wie das informatikhistorisch zu bewerten ist. Dieser Mangel könnte bewirkt haben, daß sogar Informatiker sich für Chiffriermaschinen und die zugehörende Entzifferungstechnik wenig interessieren sollen. Beispielsweise beklagte der Technikhistoriker SCHNEIDER dieses Desinteresse und nannte als eine weitere Ursache: „Leider hat die Bearbeitung [informatik-] historischer Themen, z.B. in Diplomarbeiten und anderen wissenschaftlichen Arbeiten, wie auch in der Forschungsförderung, ein sehr schlechtes Image. Das ist angesichts der wirtschaftlichen und besonders der kulturellen Einflüsse der Informatik schwer nachvollziehbar.“[2]

Schließlich könnte auch die in den letzten drei Jahrzehnten zu beobachtende Überbewertung der Geistes- und Sozialwissenschaften dazu beigetragen haben, wodurch das „Image“ technischer Fächer sich verschlechterte, ein Phänomen, das freilich hier nicht zu diskutieren ist. Womöglich war das ein Grund für die Zuordnung der Informatik zu den Geisteswissenschaften, die immer noch gelegentlich zu finden ist. Doch die Erfahrungen gerade aus der Entzifferungstechnik, und der daraus entstandenen Digitalelektronik, sollten eine andere Betrachtung nahelegen, nämlich daß Informatik eine Ingenieurwissenschaft ist. Der letzte Abschnitt enthält dazu einige Beispiele aus der Sicht des Verfassers.

[2] Schneider, Henner: Simulation und Animation historischer Geräte. In: Jahrestagung 1999 Deutscher Museumsbund, HNF Paderborn, 26. bis 28. April 1999, Fachgruppe Technikhistorische Museen. Von: www.fbi.fh-darmstadt.de/, am 6.3.03.

1.1 Historischer Kontext

Die Brechung der ENIGMA und anderer Chiffriermaschinen verschaffte den Alliierten nicht nur militärisch-taktische Informationen: Sie entzifferten ebenso zahlreiche geheime Sendungen nichtmilitärischer Dienststellen, wie der Reichsbahn, der Polizei und SS, der Abwehr, und schließlich des Auswärtigen Amtes. Auch Sendungen der Achsenmächte gehörten dazu, besonders der japanischen Diplomatie (Tarnbezeichnung MAGIC) und des italienischen Militärs. Damit erhielten sie umfassende und stets aktuelle Informationen nicht nur über die militärische, sondern ebenso über die innere Lage Deutschlands und seiner Verbündeten. Diese Informationen, und deren Auswertung in einer „intelligenten" Zusammenschau, erhielten die Tarnbezeichnung ULTRA, und waren die wichtigste Entscheidungshilfe der Alliierten. Vor allem deren Authentizität schätzte man, denn Berichte aus anderen Quellen (Spionage, Luftaufklärung etc.) konnten freilich nicht immer zuverlässig sein. Nach der umfangreichen Literatur (s.u.), ermöglichte ULTRA den Alliierten gezielt sowohl taktisch zu reagieren, als auch längerfristig zu planen und ihre Ressourcen optimal einzusetzen. Sie konnten damit in der ersten Kriegshälfte Schwächen kompensieren, dann ihre erreichte Überlegenheit nutzen, und damit den Krieg erheblich verkürzen.

Glücklicherweise endete so der Zweite Weltkrieg rechtzeitig in Europa, bevor die Atombombe einsatzbereit war, denn diese wäre sonst wahrscheinlich auf Deutschland abgeworfen worden. Beispielsweise vertritt diese Meinung der mit der ULTRA-Historiographie offiziell beauftragte britische Historiker Sir Harry HINSLEY, ein ehemaliger Mitarbeiter in Bletchley Park, in seinem Hauptwerk „*British Intelligence in the Second World War: Its Influence on Strategy and Operations*".[3] Dazu begründete er in einem berühmt gewordenen Vortrag „*The Influence of ULTRA in the Second World War*"[4] seine Meinung, daß der Krieg ohne ULTRA ca. zwei Jahre länger gedauert hätte, vor allem wegen der dann erst 1946 möglich gewesenen Invasion. Andere Fachhistoriker kommen zu ähnlichen Folgerungen, nur zur Länge der Kriegsverkürzung gibt es unterschiedliche Meinungen.
Doch selbst wenn man einen Atomwaffeneinsatz ausschließt, hätte die deutsche Nachkriegsgeschichte ohne ULTRA, d.h. ohne informationelle und damit militärische Überlegenheit der Alliierten einen anderen Verlauf genommen: So wäre bspw. die Rote Armee den Westalliierten in Deutschland zuvorgekommen und hätte mindestens ganz Deutschland besetzt, eine Meinung, die nicht nur der

[3] Hinsley, F. Harry et. al.: British Intelligence in the Second World War: Its Influence on Strategy and Operations. 5 vols., London 1991.
[4] Hinsley, F. Harry: The Influence of ULTRA in the Second World War. Vortrag an der University of Cambridge am 19.Okt. 1993. Von: http://www.cix.co.uk/~klockstone/index.html, am 02.06.02.

ehemalige *Chief Air Dept* in Bletchley Park, Capt. F.W. WINTERBOTHAM, in seinem bekannten Buch vertritt.[5]

ULTRA war das „Produkt" einer viele Tausend Mitarbeiter umfassenden Abteilung des britischen Geheimdienstes. Diese entwickelte Verfahren zur Entzifferung geheimer Funksendungen, vor dem Krieg getarnt als *Government Code and Cypher School* (GC&CS) des Außenministeriums. Sie wurde mit Kriegsbeginn nach Bletchley Park (bei London) verlagert, Tarnbezeichnung „*Station X*", doch bald gab es Kapazitätsprobleme und bürokratische Hemmnisse der Finanzierung. Nach einer Beschwerde der Wissenschaftler sorgte Premierminister Winston CHURCHILL dann für die Freistellung geeigneter Wissenschaftler und Ingenieure vom Militärdienst, und für genügend Mittel, um diese dort einzustellen.[6]

CHURCHILL kannte nämlich die Bedeutung von Entzifferungen schon aus dem Ersten Weltkrieg: Als Marineminister ordnete er im November 1914 an, nicht nur alle abgehörten bzw. abgefangenen[7] Telegramme zu entziffern und für militärische Zwecke zu nutzen, sondern darüber hinaus „*...alle ... entschlüsselten Meldungen nicht nur der Gegenwart, sondern auch der Vergangenheit zu studieren* [... und] *dadurch das deutsche Denken und Handeln zu durchschauen...* ", womit er ULTRA weitsichtig vorwegnahm.[8] Und die Informationen aus dem dazu installierten „*room 40*"[9] bestätigten CHURCHILL: Der bekannteste Erfolg – die Entzifferung des „Zimmermann-Telegramms"[10] – forcierte den von ihm betriebenen Kriegseintritt der USA.
Ebenso weitsichtig ordnete CHURCHILL 1914 die Errichtung von Funk-Abhörstationen an – damals eine völlig neue Idee –, um insbesondere den Seefunkverkehr überwachen zu können, später „Y-Service" genannt, der bis zum Zweiten Weltkrieg weltweit ausgebaut wurde und die Abhörprotokolle zur Entzifferung lieferte.
Die britische Army unterhielt in ihrem Geheimdienst ebenfalls eine Entzifferungsabteilung MI1b, die nach Kriegsende mit dem *room 40* verbunden wurde zur Government Code & Cypher School (CC&CS). Diese wiederum wurde 1923 dem Außenministerium bzw. dessen Geheimdienst MI6 zugeordnet und sollte sich vorwiegend mit der Entzifferung von diplomatischen Nachrichten befassen.[11]

---

[5] Winterbotham, F.W.: The Ultra Secret, New York, Harper, 1974.
[6] Mit seiner berühmten Anweisung „Heute noch zu erledigen!"
[7] Die deutschen Übersee-Telegramme mußten via London gesendet werden, da die Royal Navy sofort nach der Kriegserklärung auf Befehl Churchills die deutschen Untersee-Kabel kappte. Die Telegramme wurden in London kopiert, dann im „Room 40" entziffert und ausgewertet.
[8] Vgl. Smith, Michael: *Enigma entschlüsselt,* S. 25. München 2000.
[9] Tarnbezeichnung der kryptanalytischen Abteilung der britischen Admiralität im Ersten Weltkrieg.
[10] Das „Zimmermann-Telegramm" enthielt Anweisungen an den dt. Botschafter in Mexiko, die mexikanische Regierung zum Krieg gegen die USA aufzufordern – um deren befürchtete Invasion in Europa zu verhindern. Das entzifferte Telegramm wurde über britische Agenten via Mexiko trickreich der US-Regierung zugespielt, so daß diese nicht den wahren „Lieferanten" erkannte.
[11] Vgl. Smith, Michael: Enigma entschlüsselt, S. 27-28.

Der geniale Stratege Winston CHURCHILL erkannte dann (wie nur wenige Andere) in der Zwischenkriegszeit, daß die Entzifferung von Funknachrichten in einem modernen Krieg, also einem Bewegungskrieg, zu einer Waffe würde: Denn dieser konnte nur per abhörbaren Funk geführt werden und die zu erwartenden zahlreichen Funksendungen mußten daher verschlüsselt werden. Wenn es nun gelang, davon einen wesentlichen Teil zu entziffern, und diesen Erfolg vor dem Gegner geheimzuhalten, dann verfügte man quasi über ein zusätzliches Waffensystem dank des Informationsvorsprungs, der den optimalen Einsatz der eigenen Kräfte sicherte. Und das nicht nur für taktische, also kurzfristige Maßnahmen, sondern ebenso waren auch längerfristige strategische Planungen denkbar – insbesonders wenn es gelang, auch die besser gesicherte Funk-Kommunikation der Führungsebene zu entziffern.

Ob dieses Potential von der militärischen Führung des Dritten Reiches (HITLER soll das als „idiotisch" abgetan haben) erkannt wurde, muß man bezweifeln: Denn die Militärs dachten stattdessen an „Funkaufklärung"[12] im traditionellen taktischen Sinne und unterhielten dazu im Oberkommando der Wehrmacht (OKW) die Abteilung Chi mit einigen wenigen Kryptologen, deren wichtigste Aufgabe[13] die Entwicklung von Methoden zur Entzifferung von „Feindsendungen" war. Die Entzifferungsarbeit oblag dann den Nachrichtentruppen der Teilstreitkräfte, über die das OKW keine Kommando-gewalt besaß. Und diese frontnahen Aufklärer unter der Leitung des Stabsoffiziers „Ic" waren traditionsgemäß Gehilfen der Kommandeure, die sich freilich nur für taktisch verwertbare Informationen ihres Frontabschnittes interessierten.

Diese traditionelle Aufgabenverteilung im deutschen Militär scheint mit einer Überbewertung des militärischen Sachverstandes einher gegangen zu sein: Denn man beurteilte die Chiffriertechnik nach militärischen Prüfungen, und dafür waren nicht Kryptologen zuständig, wie man meinen sollte, etwa im OKW/Chi, sondern die technikorientierten Waffenämter. Diese formulierten die Ausschreibungen, vergaben die Aufträge und nahmen die fertigen Maschinen ab. Zwar konsultierten die Ämter nach drei Kriegsjahren immer öfter die Experten im OKW/Chi, doch inzwischen dahin hatten die Alliierten genügend Erfahrungen bei der Brechung deutscher Chiffriermaschinen gesammelt und konnten den dann vorgenommenen Verbesserungen der Geräte folgen. Mithin verursachte die traditionelle Aufgabenverteilung schon lange vor dem Krieg das spätere Desaster der deutschen Chiffrierungen, weil man die Geräte eben nicht nach kryptologischen Kriterien beurteilte. Als aber dann im Krieg die Feinde

---

[12] Die üblich Übersetzung des Begriffs „signals intelligence" durch „Funkaufklärung" ist schon aus diesem Grunde mißverständlich und sollte im Zusammenhang mit dem 2. WK durch „ULTRA-Informationen" ersetzt werden.

[13] Das änderte sich – inoffiziell – vermutlich 1942/43, als Beratungsaufgaben für eigene Chiffriermaschinen hinzu kamen (s. dazu 5.4.3).

dank ULTRA immer offenkundiger bestens informiert waren, schob man das auf Verrat und Spionage, denn einen Fehler konnte man wohl nicht offen einräumen. Womöglich begriffen die Verantwortlichen überhaupt nicht, einen Fehler begangen zu haben.
Über diese Vorgänge sind Forschungsergebnisse nicht bekannt; gleichwohl wird im Abschnitt 5.4 versucht diesen Hintergrund aufzuhellen.

Ein weiteres Problem verursachte die sog. Polykratie im Dritten Reich, wonach Zuständigkeiten nicht klar geregelt und oft mehreren Instanzen zugeordnet wurden. Daraus resultierten Kompetenz- und Machtkämpfe, mit der Folge, daß die jeweiligen Machthaber auch eigene Chiffrierdienste installierten. Nach LEIBERICH gab es sieben „Chiffrierbehörden", die nicht nur nicht zusammen arbeiteten, sondern sogar ihre jeweiligen Erfahrungen untereinander geheim hielten[14] wie gegen den Feind, denn die „Konkurrenz" könnte ja davon profitieren. Dennoch erzielten die Dienste beachtliche Erfolge auf der taktischen Ebene, konnten jedoch nicht in die Chiffrierungen der alliierten Führungsebene einbrechen, weil die wenigen Kryptologen nahezu isoliert arbeiten mußten.
Dagegen zeigt das Beispiel Bletchley Park, wie intensive wissenschaftlich-technische Zusammenarbeit möglichst vieler geeigneter Kräfte fast alle Probleme lösen konnte.

Zusammenfassend bleibt festzuhalten: Dank weitsichtiger Führung konnte in Bletchley Park (dann auch in Arlington Hall/USA) eine einmalige Konzentration von Fachleuten die entzifferten Informationen und deren Auswertung zu einer Waffe machen, ULTRA genannt. Mit leistungsstarken Maschinen, deren Grundlagen erst zu entwickelten und die dann in kürzester Zeit zu bauen waren, entzifferten Tausende Mitarbeiter und bewältigten die große Menge von tägliche Tausenden Funknachrichten. Im Dritten Reich hingegen verhinderten traditionelle militärische Zuordnungen und die allgemeine Zersplitterung der Verantwortung ein deutsches Bletchley Park von vornherein.

In der Literatur hat sich der Begriff ULTRA inzwischen als Synonym eingebürgert für alles, was im Zweiten Weltkrieg unter SIGINT = *signals intelligence* verstanden und von britischen Diensten erarbeitet wurde. ULTRA löste in 1941 die bis dahin verwendete Tarnbezeichnung SPECIAL ab, die jedoch nur die reinen Ergebnisse der Entzifferungen umfaßte. Diese wurden immer intensiver in einer Zusammenschau ausgewertet, unter Einbeziehung auch nichtmilitärischer Entzifferungen und anderer Quellen, und ermöglichten so auch vorausschauende strategische Planungen. Daher umfaßt ULTRA weit mehr als der deutsche Begriff „Funkaufklärung", der sich nur auf traditionelle militärische Aufklärung bezieht, und demzufolge in der Literatur gelegentlich mißverständlich verwendet wird.

[14] Leiberich, Otto: Vom diplomatischen Code zur Falltürfunktion. Hundert Jahre Kryptographie in Deutschland. In: Spektrum der Wissenschaft 4/2001, S. 15.

Die Abkürzung BP = Bletchley Park hat sich ebenso in der Literatur etabliert, um die Geheimdienst-Organisation *Government Code and Cypher School* ohne Umschreibungen zu nennen, die ULTRA dort „produzierte“. Beide Begriffe werden nachfolgend gleichermaßen abgekürzt verwendet.

Der in diesem Zusammenhang gelegentlich genannte Begriff MAGIC bezeichnet hingegen die US-Entzifferungen der japanischen Diplomatie-Funksendungen. Besondere Bedeutung für den europäischen Kriegsschauplatz erlangten die Entzifferungen der Sendungen der japanischen Botschaft Berlin: Deren Diplomaten ließen häufig ausführliche Berichte senden, die, neben militärisch wichtigen Informationen, viele Interna des Dritten Reiches enthielten, die sie dank bester Beziehungen zu HITLER und anderen Nazigrößen erfuhren.

1.2 Forschungsgegenstand

Das Phänomen ULTRA untersuchten Forscher bisher überwiegend nach historischen Kriterien[15], oder aber – seltener – sie publizierten kryptologisch orientierte Studien über die dabei eingesetzten Maschinen. Hingegen fehlen Untersuchungen, die Wechselbeziehungen aufzeigen, denn: Die verwendeten Chiffriermaschinen, deren fehleranfälliger Einsatz im Kriege, und die dazu korrespondierenden kryptanalytischen Maschinen scheinen ein gemeinsames System zu bilden. Dazu gehören freilich auch die besonderen Leistungen der beteiligten Wissenschaftler und Ingenieure, und zwar nicht nur die der wenigen Prominenten. Darüber hinaus interessiert noch die Frage, ob die maschinelle Kryptologie einen Einfluß auf die Entwicklung der Digitalelektronik bis hin zu elektronischen Rechnern hatte, und falls ja, welche Erkenntnisse dazu beitrugen.
Die Relevanz des Forschungsgegenstandes kann man auch am Mangel an einschlägiger technikhistorischer Literatur erkennen: Für eine umfassende Untersuchung muß man die jeweilige Technikgeschichte der Geräte einbeziehen, ebenso wie die zugehörende historische Kryptographie, womit der Beginn des Untersuchungszeitraumes bestimmt wird. Die andere Begrenzung des Untersuchungszeitraumes ergibt sich aus der Definition des Forschungsgegenstandes: Dieser umfaßt die maschinellen kryptologischen Verfahren, und zwar die, die nicht der späteren computerbasierten Kryptologie zuzuordnen sind. Denn diese könnten – strenggenommen – ebenfalls als „maschinell“ bezeichnet werden, weil ebenfalls „Maschinen“, die Computer, Texte verarbeiten, jedoch ausschließlich mit Software, die alle erforderlichen Algorithmen enthält. Die Computer selbst, die Hardware, sind hierbei quasi nur Hilfsgeräte. Im Gegensatz dazu verfügten die kryptologischen Maschinen über einen implementierten festen Algorithmus, als den einen Teil des Chiffriersystems. Den anderen Teil, die „Software“, erbrachten die menschlichen

[15] Die umfangreiche Historiographie beschreibt zwar die Auswirkungen von ULTRA auf das Kriegsgeschehen, besonders ausführlich auf den Seekrieg, kaum jedoch den „deutschen Anteil“, der ja ULTRA erst ermöglichte.

Anwender bei der Vorbereitung und Durchführung der Chiffrierung/Dechiffrierung bzw. Entzifferung.

Der Übergang von maschinellen zu computerbasierten kryptologischen Verfahren erfolgte freilich nicht abrupt zu einem definierten Zeitpunkt. Er begann in der letzten Phase des Krieges, dauerte mehrere Jahre, und ist durch Geheimhaltung und nationalistisch gefärbte Desinformationen gekennzeichnet. Gleichwohl wurde dieser letzte Teil des Forschungsgegenstandes mit einbezogen, soweit das wegen fortbestehender Geheimhaltung möglich war. Zugleich ist damit das Ende des Untersuchungszeitraumes vorgegeben.

Dabei stehen besonders die Geräte im Blickpunkt, deren Bau zur Entwicklung elektronischer Digitalschaltungen beitrugen. Das läßt sich nicht immer eindeutig trennen, denn der Übergang von der Elektromechanik über die Digitalelektronik zu den ersten Computern verlief nicht in direkter Folge, manches wurde parallel verwendet, und es bleibt aufzuzeigen, welche Maschinen jeweils welche Maßnahmen erforderten. Zum besseren Verständnis der Zusammenhänge enthält die Untersuchung freilich dazu verwandte maschinelle bzw. elektronische Geräte, die zu den Entwicklungen eher indirekt beitrugen.

Bei der Untersuchung der Methoden zur maschinellen Entzifferung von Funksendungen fanden sich überraschende Wechselwirkungen: Denn diese Entzifferungsverfahren waren abhängig von bestimmten Gewohnheiten der Anwender der jeweiligen Chiffriermaschinen, zumeist setzten sie diese sogar voraus. Und diese Gewohnheiten waren vermutlich eine Folge der erwähnten traditionellen Aufgabenverteilung im deutschen Militär, so daß diese Zusammenhänge nicht erkannt wurden. Mithin kann der Forschungsgegenstand, die maschinelle Kryptologie, nur mit einer systemischen Betrachtung richtig beurteilt werden, die auch diese Wechselwirkungen mit enthält.

Schließlich war noch ein Neben-Forschungsgegenstand zu bearbeiten:
Bei der Untersuchung dieses Themenkomplexes findet man ungewöhnlich viele fehlerhafte Angaben oder Lücken, sogar in seriösen Publikationen – vermutlich eine Folge der Geheimhaltung und der Desinformationen zur Tarnung des ULTRA-Geheimnisses. Das war freilich im Krieg absolut erforderlich, doch nach dem Krieg diente es vor allem einer perfiden Strategie der Geheimdienste: Regierungsstellen übergaben „großzügig“ zahlreichen Staaten, darunter auch Alliierten, erbeutete ENIGMA- und andere Maschinen, die ja damals offiziell sicher waren, zur Verschlüsselung geheimer Sendungen. Und konnte so deren Geheimnachrichten mitlesen – das ULTRA-Geheimnis mußte also weiter gewahrt werden. Erst 1974, als überall die elektromechanischen Chiffriermaschinen außer Betrieb genommen und durch computerbasierte Systeme ersetzt waren, durfte der frühere BP-Mitarbeiter Captain F.W. WINTERBOTHAM ein Buch darüber publizieren, nachdem schon einige Informationen „durchgesickert“ waren.[16] Er

[16] Winterbotham, F.W.: The Ultra Secret, New York, Harper, 1974.

erhielt jedoch keinen Zugang zu Dokumenten und mußte aus dem Gedächtnis schreiben. So blieben Fehler nicht aus, die in die Historiographie übernommen und später nicht immer revidiert wurden. Aber auch mangelndes technisches Verständnis scheint bei manchen Autoren die Fehlerquote gesteigert zu haben.

Demzufolge mußten Fehler eliminiert bzw. unzureichende Angaben ergänzt werden, eine Aufgabe, die sorgfältiges vergleichendes Arbeiten erforderte. Damit bietet diese Arbeit eine berichtigte aktuelle Zusammenstellung der derzeit frei zugänglichen, relevanten Informationen.

1.3 Schwerpunkte und Gliederung

Die Erfindung und Verwendung von Chiffriermaschinen markierte einen Entwicklungssprung, nachdem man jahrhundertelang mit Papier und Federkiel oder Bleistift, dann auch mit Hilfsmitteln (Codebücher, Scheiben, Zylinder etc.), vertrauliche Texte chiffrierte. Solche Entwicklungen geschehen kaum zufällig, es müssen bestimmte Randbedingungen erfüllt sein, wie die Technikgeschichte an zahlreichen Beispielen zeigt. Daher wird im Kapitel 2 als erstes gesucht nach den Gründen für die Entwicklung von Chiffriermaschinen sowie danach, welche wissenschaftlichen Erkenntnisse und technischen Möglichkeiten vorhanden sein mußten, und welche wirtschaftlichen und politischen Einflüsse dabei eine Rolle spielten.

Unter dem Einfluß des Ersten Weltkrieges beschleunigte sich diese Entwicklung, wohl weil Erfinder nun einen wesentlich größeren „Markt“ für Chiffriermaschinen sahen, die sie den Militärs zu verkaufen gedachten. Überdies standen nun Novitäten wie die elektrische Schreibmaschine und der Fernschreiber als Basis zur Verfügung. Beide Geräte regten die Phantasie der Erfinder an, denn sie eröffneten neue technische Möglichkeiten und wurden so zu Vorläufern der späteren Chiffriermaschinen. Entsprechend der unterschiedlichen Technik dieser Basismaschinen, bildeten sich zwei grundverschiedene Methoden der maschinellen Chiffrierung heraus, die im Bau ebenso unterschiedlicher Maschinen mündeten, und dementsprechend eine Betrachtung in zwei getrennten Kapiteln nahelegen.

Im Kapitel 3 wird gezeigt, wie aus Chiffrier-Schreibmaschinen, über elektrische Schreibmaschinen dann schließlich Rotor-Chiffriermaschinen entstanden. Die bekannteste und erfolgreichste Geräteserie dieser Entwicklungslinie namens ENIGMA (grch. Rätsel) erlangte später große historische Bedeutung. Die Besonderheiten einiger ENIGMA-Versionen rechtfertigen eine ausführlichere Untersuchung, auch um die immer noch verbreiteten Legenden um diese Maschinen zu entzaubern. Dazu wurde eine Tabelle erarbeitet, die erstmals alle

ENIGMA-Versionen übersichtlich auflistet; die wichtigsten Modelle sind ausführlich beschrieben.
Schwerpunktmäßig wird dazu erläutert, wieso die theoretisch sehr hohe Zahl der ENIGMA-Schlüsseleinstellungen, die sog. Periode, allein wenig aussagekräftig ist.

Eine besondere Art der Verschlüsselung enthalten die mechanischen Chiffriermaschinen, die man zwar nicht direkt den Rotormaschinen zuordnen kann, doch wegen vieler Gemeinsamkeiten in die Untersuchung mit einbeziehen muß. Diese Geräteklasse wurde überdies zur erfolgreichsten im Zweiten Weltkrieg, wenn man die Stückzahlen als Erfolgskriterium wertet, und verdient schon aus diesem Grund nähere Betrachtung. Diese Maschinen entstanden nahezu parallel zu den verwandten mechanischen Rechen- und Buchungsmaschinen, mit deren Technik sie vieles verbindet.

Die Fortschritte der Telegraphie ermöglichten zwar immer schnellere Übertragungsgeschwindigkeiten, doch solange der zeitraubende Umweg über Telegraphenämter blieb, war die Systemleistung sehr begrenzt. Erst mit dem Fernschreiber konnte diese Begrenzung überwunden werden, und schon bald nach dessen Vorstellung erfand der US-Telegrapheningenieur Gilbert VERNAM ein dafür geeignetes Chiffrierverfahren. Im Kapitel 4 wird daher die binär codierte Telegraphie erläutert, als Grundlage des Fernschreibers und ebenso des Vernam-Chiffrierverfahrens. Die daraus entstandenen Geräte und deren historische Entwicklung wird dargelegt.

Im Zusammenhang mit der Erfindung des Vernam-Verfahrens entstand das sog. One-Time-Pad bzw. Einmalschlüsselverfahren. Es ist das einzig *beweisbar* unbrechbare Verfahren, und den Beweis dafür lieferte der Informations-theoretiker Claude SHANNON, dessen Arbeiten hierzu diskutiert werden.

Im Kapitel 5 wird gezeigt, wie die beginnende militärische Verwendung der Chiffriermaschinen – erstmals 1926 in Deutschland – die potentiellen Gegner veranlaßte, Entzifferungsverfahren zu entwickeln. Nicht zufällig begannen damit polnische Kryptologen bereits 1930, da Polen sich der latenten Kriegsgefahr stets bewußt war. Doch dazu mußten sie erst die wissenschaftlichen Grundlagen erarbeiten, weil die damals bekannten, sog. linguistischen Methoden der Kryptanalyse gegen maschinelle Chiffrierungen wenig geeignet waren.

Untersuchungsschwerpunkt des Kapitels 5 ist die praktische Umsetzung der wissenschaftlichen Erkenntnisse: Die mathematischen Analysen (die nicht zum Forschungsgegenstand zählen) deckten die jeweiligen Chiffrieralgorithmen der Chiffrierung auf, wenn ausreichende Informationen erarbeitet waren. Damit konnte man dann unbekannte Chiffriermaschinen oder Verfahren rekonstruieren, und anschließend Methoden erarbeiten, um die jeweils wechselnden Einstellungen und Schlüsselvereinbarungen („Spruchschlüssel“) möglichst maschinell zu ermitteln. Denn die herkömmlichen Methoden der Kryptanalyse –

die Entzifferung mit Papier und Bleistift – genügten nicht mehr im vom Funk dominierten zukünftigen Krieg, denn sehr viele Sendungen, täglich Tausende, müssen dann in kurzer Zeit entziffert werden. Das erkannten rechtzeitig vor dem Krieg die polnischen Kryptanalytiker als erste und konstruierten zur Lösung dieses Problems auch die ersten kryptanalytischen Maschinen.

Nach Kriegsbeginn und der folgenden Besetzung Polens und Frankreichs übernahm der britische Geheimdienst zunächst die polnischen Verfahren und setzte die Entzifferungsarbeit fort in BP. Dort sorgte eine einmalige Konzentration von Wissenschaftlern und Ingenieuren für erfolgreiche Analysen der inzwischen weiterentwickelten Chiffriermaschinen und für den ebenso erfolgreichen Bau korrespondierender kryptanalytischer Maschinen. Die dazu erforderlichen wissenschaftlichen Grundlagen erarbeitete der Mathematiker A. TURING, die ausführlich erläutert werden.

Ab 1942 erhielt die Brechung der Chiffrierfernschreiber immer größere Bedeutung, da die oberste deutsche Führungsebene zunehmend per Funkfernschreiben Nachrichten austauschte. Hierzu mußte man völlig neue Methoden der Kryptanalyse entwickeln und dann möglichst maschinell umsetzen. Besonders eingehend wird die Rekonstruktion des „Schlüsselzusatz“ SZ40/42 zum Lorenz-Fernschreiber untersucht, weil zur Entzifferung der Bau teilelektronischer Maschinen und später von Elektronenrechnern erforderlich wurde. Überdies demonstriert die rein mechanische Schlüsselgenerierung des SZ40/42 eindrücklich den Zusammenhang von Pseudo-Irregularitäten der Chiffrierung, die eine erhöhte Schlüsselsicherheit zu bieten schien, aber durch mathematische Kryptanalyse überwindbar war.

Die erfolgreiche Gewinnung der ULTRA-Informationen scheint, folgt man Literaturangaben, nur zwei Gründe gehabt zu haben: Der enorme Personal- und Materialaufwand der Alliierten, und die wissenschaftlich-technischen Leistungen der beteiligten Kryptologen (die der Ingenieure werden gern „vergessen“). Doch die Erläuterungen der verschiedenen Entzifferungsverfahren zeigen, daß man für maschinelle Entzifferungen stets aktuelle Klartextfragmente benötigte, sog. *cribs*, und das für jeden täglich wechselnden Schlüsselkreis. Fernschreiben konnten nur mit Hilfe von *dephts* entziffert werden, Sendungen also, die man durch andere Sendungen kompromittieren konnte. Wieso aber die Entzifferer scheinbar mühelos und täglich diese Klartextfragmente bzw. kompromittierte Sendungen erarbeiten konnten, dieses Phänomen ist ein Schwerpunkt des Kapitels 5, dem daher ein eigener Abschnitt 5.4 zugeordnet wurde.

Im Kapitel 6 stehen elektronische Logikschaltungen im Mittelpunkt, denn die bereits vor dem Krieg in ersten Rechnern (ZUSE, später AIKEN) verwendeten Relais besaßen wegen ihrer begrenzten Schaltgeschwindigkeit kein weiteres Entwicklungspotential. Daher wurden elektronische Logikschaltungen schon länger erforscht, wegen vermuteter Unzuverlässigkeit jedoch noch nicht praktisch verwendet.

Forschungsschwerpunkt dieses Kapitels ist ein Vergleich der bis 1942 bekannten elektronischen Digitalschaltungen. Dabei soll geklärt werden, welche Schaltungen potentiell verwendbar waren und ob sie besonders einem Dauerbetrieb standhalten würden. Denn damals herrschte weitverbreitete Skepsis gegen deren Verwendung; man glaubte, die Ausfallquote von Elektronenröhren sei gemäß den Erfahrungen mit der Analogtechnik zu hoch und das würde in digitalen Rechenschaltungen inakzeptable Fehler bewirken, die man womöglich zu spät entdecken könnte. Die Lösung dieses Problems, nämlich der sichere Dauerbetrieb von Elektronenröhren, war entscheident für den Bau der ersten elektronischen Rechner, die wiederum Voraussetzung für die Implementierung elektronischer Speicher war – und damit der Computerentwicklung.

Der Schluß des Kapitels 6 behandelt eine wenig bekannte Gerätekategorie, deren Algorithmen die Übertragung menschlicher Sprache so erschweren sollten, daß unbefugte Lauscher nichts mehr verstehen konnten. Auch diese Verfahren sind Teil der Kryptologie und werden „Kryptophonie“ (engl. auch *cyphony*) genannt.
Die erste, analog arbeitende Gerätegeneration konnte bald mit ebenso analogen Methoden kompromittiert werden. Die nachfolgenden Systeme hingegen nutzten Digitaltechnik, teilweise unter Anwendung gleicher Verfahren wie in der maschinellen Kryptologie, und wurden so zur Grundlage der späteren Sprachsignalverarbeitung, der digitalen Telefontechnik und des Mobilfunks.

Die während des Krieges gemachten Erfahrungen mit kryptanalytischer Digitalelektronik konnten Forscher nach dem Krieg verwerten, wie im Kapitel 7 an Geräten der frühen Computerentwicklung dargelegt ist. Inzwischen wurde durch Dokumentefreigaben auch bekannt, wie US-Computerforscher die Entwicklung kryptanalytischer Maschinen fortsetzten, und davon kommerzielle Versionen entstanden.
Daher ist zu fragen, welche Ergebnisse oder Erfahrungen der maschinellen Kryptologie die Computerentwicklung begünstigten. Hierzu findet man erstaunlich wenige Angaben in der Literatur, die überdies fokussiert ist auf den Rechner COLOSSUS, dessen technische Daten zwar erläutert werden, doch ohne die historischen Zusammenhänge aufzuzeigen: Wie es zum Bau dieses Gerätes kam, welche Vorgeschichte zu berücksichtigen ist und welche Auswirkungen auf die frühe Computerentwicklung daraus folgten, wurde bisher kaum diskutiert.

Dementsprechend findet man auch keine Angaben, woher die *betriebssicheren* digitalen Röhrenschaltungen stammten – deren Existenz wird offenbar als selbstverständlich vorausgesetzt. Diese informatikhistorisch interessante Frage ist leider mangels Dokumentation nicht abschließend zu beantworten, doch die Diskussion zahlreicher Indizien führt hin zu Tommy FLOWERS, dem Konstrukteur des ersten elektronischen Rechners COLOSSUS. Auch aus diesem Grund kann man die Erfahrungen der maschinellen Kryptologie als eine der Grundlagen für den späteren Bau elektronischer Computer bezeichnen: Schon aus technischen Gründen hätte die frühe Computerentwicklung ohne diese Erfahrungen wohl erheblich mehr Zeit benötigt.

Ein weiterer Anlaß für die frühe Computerentwicklung hat ebenfalls einen kryptologischen Hintergrund: Die US-Geheimdienste hatten mit kryptanalytischen Maschinen im Krieg viel Erfolg gehabt und erhielten daher auch nach dem Krieg genügend Forschungsmittel. Sie führten die Entwicklungen weiter und setzten die Entzifferungen unter strikter Geheimhaltung fort. Dieser Teil der frühen Computerentwicklung unterlag bis vor wenigen Jahren der Klassifizierung und fand dementsprechend – von Vermutungen abgesehen – noch keinen Eingang in die Literatur. Es wird dargelegt, wie auch diese geheimen Entwicklungen zum Bau kommerzieller Maschinen verwertet wurden. Freilich ist das nur eingeschränkt möglich, weil viele wichtige Dokumente dieses Forschungsgebietes klassifiziert sind. Gleichwohl kann man mit dem bisherigen Freigaben die informatikhistorisch wichtigsten Entwicklungen der frühen Computer verfolgen und die bisherige Darstellung teilweise korrigieren.

Im abschließenden Kapitel 8 sollen die Ergebnisse wissenschaftstheoretisch eingeordnet werden. Das aber ist erschwert durch den Fakt, daß in der jungen Disziplin Informatik fast alle Grundlagen immer noch, teils heftig, umstritten sind. Beispielsweise wird seit langem kontrovers diskutiert, ob Informatik eine ingenieurwissenschaftliche Disziplin ist oder eine Geisteswissenschaft. Dabei geht es nicht etwa nur um eine akademische Debatte, sondern auch um die Frage, wo die Schwerpunkte in der Ausbildung der künftigen Informatiker zu setzen sind. Dazu kann es nützlich sein zu verfolgen, welche Bedeutung in der Informatikgeschichte die Ingenieure hatten und wofür die maschinelle Kryptanalyse viele beeindruckende Beispiele bietet: Erst die Synthese aus Wissenschaft und Technik – hier Kryptologie/Mathematik und Elektromechanik – ermöglichte auf diesem Gebiet herausragende Leistungen; einige Beispiele im Kapitel 8 bestätigen das.

1.4 Quellen- und Literaturlage

Es überrascht nicht, daß bei einem mit dem Geheimdienstmilieu verbundenen Forschungsgegenstand die Aufarbeitung erschwert ist, denn diese Dienste neigen gelegentlich zu überzogener Geheimhaltungspolitik[17], besonders die britischen. In den USA erzwang die öffentliche Kritik daran ein Umdenken: Das *opendoor program*, in der Folge des *Freedom of Information Act* von 1966/74, sorgte allmählich, vor allem in 1996 und 2000, für die Deklassifizierung Tausender relevanter Dokumente, darunter auch vieler beschlagnahmter deutscher aus dem Zweiten Weltkrieg, und ermöglichten überdies online-Recherchen oder veröffentlichten Übersichtslisten im Internet. Nun konnten auch die britischen Dienste nicht mehr nachstehen und mußten ebenso Dokumente im *Public Record Office* (Kew/GB) zugänglich machen. Leider verhinderten die britischen Geheimdienste eine mit den USA vergleichbare Offenlegung. Man hielt auch

[17] Zu den Hintergründen dieser Politik s. 5.6.1.

Dokumente zurück, die für britische Sicherheitsfragen kaum wichtig sein können, beispielsweise nach dem Krieg angefertigte Befragungsprotokolle deutscher Kryptologen, die jedoch für die Forschung interessant wären.[18] Überdies wurde auch nicht mitgeteilt, welche Dokumente jeweils betroffen sind, so daß die Forschung weiter mit einem „Unschärfebereich" leben muß. Immerhin ermöglichten die bisherigen Freigaben die Klärung einiger wichtiger noch offener Vorgänge.

Der weitaus größte Teil der Literatur zu ULTRA besteht aus historischen, teils sehr ausführliche Standardwerken wie beispielsweise „Das Deutsche Reich und der Zweite Weltkrieg".[19] Besonders gründlich wurde freilich der Seekrieg untersucht, wo der Einfluß von ULTRA offenkundig war. Hierzu liegen u.a. zahlreiche Publikationen des Marinehistorikers ROHWER vor, als Standardwerk gilt „Die Chronik des Seekrieges 1939-1945".[20]

Doch sieht man einmal vom sehr gut erforschten Seekrieg ab, findet man über den für das Deutsche Reich noch wichtigeren Land- und Luftkrieg viel weniger Forschungspublikationen. Vermutlich gehört das zu den „historiographischen Lücken", die WEGNER an zahlreichen Beispielen beklagt.[21] Neben Quellenproblemen schreibt er dieses „Defizit" vor allem „...der übermäßigen Vernachlässigung aller für die Analyse des nationalsozialistischen Herrschaftssystems als wenig relevant eingeschätzten Aspekte des Krieges [zu]. Hierzu zählen [...] auch die Probleme einer kritischen Technikgeschichte..."[22], zu denen man den deutschen Teil der ULTRA-Geschichte wohl rechnen kann.

Genau das ist der Gegenstand dieser Abhandlung, und ausdrücklich nicht die bedeutende historische Seite des Phänomens ULTRA.

Zur Technikgeschichte der maschinellen Kryptologie, und damit zur Weltkriegskryptologie, findet man in der Tat nur wenige Publikationen, und überdies sind diese oft nicht auf dem aktuellen Stand, weil die erwähnten Dokumentefreigaben der letzten Jahre nicht immer berücksichtigt werden konnten. Eine Sonderstellung nimmt hierbei das Buch[23] des Mathematikers, Informatikers und Kryptologen BAUER ein: Das reich illustrierte Werk ist zwar kryptomathematisch orientiert, enthält aber auch viele technische und historische Informationen, und insbesonders fast alle Geräte zum Thema; es eignet sich daher als Nachschlagewerk. Die englische Ausgabe[24] ist neueren Datums und aktualisiert.

---

[18] Das wurde bekannt durch eine Anfrage im britischen Unterhaus nach dem Verbleib des Protokolls über die Befragung des Marine-Kryptologen Frowein (s. hierzu 5.2.3).

[19] Militärgeschichtliches Forschungsamt (Hsg.): Das Deutsche Reich und der Zweite Weltkrieg, 7 Bände, Stuttgart 1993-2001.

[20] Rohwer, J. und Hümmelchen, G.: Chronik des Seekrieges 1939-1945. Oldenburg (1968) ^{3}1992.

[21] Wegner, Bernd: Kriegsgeschichte – Politikgeschichte – Gesellschaftsgeschichte. In: Rohwer, J. und Müller, H. (Hrsg.): Neue Forschungen zum Zweiten Weltkrieg. Weltkriegsbücherei Stuttgart, Band 28. Koblenz 1990. S. 102-111.

[22] Ebd., S. 110.

[23] Bauer, F.L.: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Berlin ^{3}2000. (Zukünftig zit.: "Bauer, Geheimnisse").

[24] Bauer, F.L.: Decrypted Secrets: Methods and Maxims of Cryptology. Berlin, New York (NY) ^{3}2002.

Das vielzitierte Buch[25] des Historikers KAHN hingegen ist nur eingeschränkt brauchbar: Das Konvolut breitet auf 1180 Seiten sehr viele, auch unwichtige Details aus, dafür fehlen selbst in dieser aktualisierten Ausgabe einige wichtige Geräte und Vorgänge.
Speziell zu den herausragenden Leistungen des Mathematikers Alan TURING findet man interessante und aktuelle Erläuterungen in seiner Biographie, mit technischen Einzelheiten zu Geräten, an denen TURING in irgendeiner Weise beteiligt war.[26]

Ein Insiderwerk[27] ehemaliger Mitarbeiter in BP enthält auch technische Informationen, vor allem über die elektronischen Geräte. Aktueller jedoch – die Dokumentefreigaben 1996/2000 wurden berücksichtigt – ist ein Sammelband mit Berichten ehemaliger BP-Kryptologen, deren nun offengelegtes Insiderwissen manche bisherige Unklarheiten beseitigt.[28]
In Periodika, besonders in „Cryptologia", werden kryptologische Einzelprobleme ausführlich diskutiert, meist mit den dazu erforderlichen technischen Angaben. Viele für diese Abhandlung relevanten Artikel enthält ein Sammelband.[29]
Zum Thema „Erste Computer" gibt es zwar eine umfangreiche Literatur, die jedoch anders orientiert ist: Man untersuchte vor allem Rechnerarchitekturen und deren Vor- und Nachteile; der kryptologische Hintergrund vieler Maschinen wird nicht diskutiert – COLOSSUS ausgenommen.[30]

Viele Informationen zum Thema findet man auf Webseiten. Allerdings ist bei deren Verwendung Vorsicht geboten, denn nicht nur private Seiten enthalten Fehler. Mit einiger Erfahrung war diese Recherche dennoch erfolgreich und es konnten wenige zuverlässige, sehr informative Seiten ermittelt werden. Besonders zu erwähnen sind: Die Webseite des Museums Bletchley Park, deren technischer Teil vom früheren Kustos Tony SALE betreut wird.[31] Neuerdings offenbart eine spezielle Seite manche bisher unbekannte bzw. hartnäckig geleugnete Details aus den Archiven.[32] Leider ist sie z.Zt. nur bis März 1944 verfügbar.

---

[25] Kahn, David: The Codebreakers. The Story of Secret Writing. New York (NY) ²1996. (Zukünftig zit.: "Kahn, Codebreakers").
[26] Hodges, Andrew: Alan Turing, The Enigma. US-Edition by Walker Publishing, ²2000. Dazu ständige online-Updates. (Zukünftig zit.: "Hodges, Turing").
[27] Hinsley, F. Harry and Stripp, Allan (Eds.): Codebreakers. The Inside Story of Bletchley Park. Oxford University Press 1993. (Zukünftig zit.: "Hinsley, Codebreakers").
[28] Erskine, Ralph and Smith, Michael (Eds.): Action this Day. Bantam Press, London u.a. Orte, 2001.
[29] Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, 1990-1998. Artech House, Norwood MA/USA, 1998.
[30] Rojas, R./Hashagen, U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA und London, 2000.
[31] Sale, Tony: Codes and Ciphers in the Second World War. URL: http://www.codesandciphers.org.uk. (zukünftig zit.: „Sale, Codes and Ciphers").
[32] Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives". URL: http://www.bletchleypark.org.uk/dchistory/.

Nützlich ist die Alan-Turing-Homepage, die vom Mathematiker und Turing-Biographen Andrew HODGES betreut und ständig aktualisiert wird.[33]
Schließlich veröffentlichen und kommentieren die Mitglieder der „Crypto Simulation Group“ ggf. neue Dokumente, wenn sie freigegeben werden.[34] Ihre Seiten enthalten viele Informationen, Dokumente und Links zu anderen interessanten Seiten oder Literaturstellen.

Wenig ergiebig sind öffentliche deutsche Archive: Die (wenigen) relevanten Dokumente, welche die Vernichtungsbefehle bei Feindannäherung oder die Bombardierungen überstanden hatten, beschlagnahmten alliierte Suchtrupps. Zwar gab es nach und nach Rückführungen, gemäß Regierungsabkommen beginnend in den 60er Jahren, aber nicht vollständig, und – leider üblich – auch ohne Angaben, was sonst noch gefunden, aber zurückgehalten wurde.[35]

Deutsche Experten schrieben nach dem Krieg ihre Kenntnisse und Erfahrungen aus dem Gedächtnis auf bzw. nach privaten Unterlagen, teils im alliierten Auftrag, teils später im Auftrag bundesdeutscher Dienststellen. Die Geheimhaltung wurde für die meisten Dokumente inzwischen aufgehoben, dennoch sind sie nicht immer öffentlich zugänglich, doch einige konnten in privaten Archiven eingesehen werden.

Bei der Bearbeitung des gesamten relevanten Materials findet man häufig falsche Zuordnungen von Geräten, unzutreffende Bezeichnungen und unpräzise Definitionen, mitunter sogar reine Fiktionen, und leider nicht nur auf privaten Webseiten. Das erforderte entsprechende Sorgfalt, um diese Unklarheiten zu eliminieren; der Verf. bemühte sich, nichts wesentliches zu übersehen.

[33] URL: http://www.turing.org.uk.
[34] URL: http://frode.home.cern.ch/frode/crypto.
[35] Gemäß mdl. Auskunft des Militärarchivs Freiburg.

1.5 Definitionen, Abkürzungen

abstreifen	Eliminierung einer Verschlüsselungsebene, vor allem einer Überschlüsselung.
Bletchley Park (BP)	Ort bei London. Synonym für das dorthin verlagerte engl. Chiffrierzentrum des Geheimdienstes während des 2. WK. Auch „Station X" genannt.
Brechung (einer Chiffriermaschine)	Beherrschung der Chiffrieralgorithmen einer Maschine und regelmäßiges Entziffern, ggf. mit maschinellen Entzifferungsverfahren.
Entzifferung	Unbefugte Gewinnung des Klartextes, ohne im Schlüsselbesitz zu sein, meist durch Kryptanalyse (s. dort).
Funkaufklärung	Informationsgewinnung aus Entzifferungen des Funkverkehrs, dessen Verkehrsanalyse und aus Peilungen.
Geheimtext	Chiffrierter Klartext, auch Chiffrat.
Griechenwalze	4. Rotor in der Marine-Enigma M-4.
Grundeinstellung	Enigma-Voreinstellung nach Tabelle, täglich wechselnd: Rotorlagen, Ringstellung (s. dort) und Steckerfeld.
Klartext	Zu chiffrierender Text.
Klartextfunktion (*Autokey*)	Bestimmte vorwählbare Buchstaben des Klartextes beeinflussen den Chiffrier-Algorithmus – eine starke kryptanalytische Erschwernis.
Kompromittierung	Bloßstellung eines Geheimtextes, durch Kryptanalyse bzw. aus anderen Quellen. Auch völlige Beherrschung einer Chiffriermaschine.
Kryptanalyse	Meist mathematische und statistische Methoden zur Entzifferung von Geheimtexten, d.h. Informationen unbefugt erlangen. Diese werden nicht „entschlüsselt/dechiffriert", wie häufig zu lesen, da ja der Schlüssel nur im Besitz des rechtmäßigen Empfängers ist, sondern „entziffert".
Kryptographie	Geheimschriftkunde – *offen* versendete Nachrichten sollen durch Verschlüsselung bzw. Chiffrierung für Unbefugte nicht lesbar sein. Der berechtigte Empfänger verfügt über den Schlüssel und kann die Nachricht entschlüsseln bzw. dechiffrieren.
Kryptologie	Wissenschaft der Verfahren zur Geheimhaltung von Nachrichten, aber auch zu deren Brechung.
linguistische Krypt-analyse	Beruht darauf, daß natürliche Sprachen bestimmte Eigenschaften haben, die auch nach einer Chiffrierung vorhanden sind.
monoalphabetisch	Verschiebungen eines Alphabets (Caesar-Code).
Permutierung	Verwürfelung eines Normalalphabets, dessen Buchstaben bleiben aber erhalten. Auch als Transposition bezeichnet.
polyalphabetisch	Bei Chiffrierungen wird für jeden Buchstaben ein neues Alphabet verwendet, bei Maschinen durch Algorithmus vorgegeben.
Puls-Code-Modulation	Sprachübertragung mit kurzen Frequenzproben einer Schwingung, zur Verminderung der erforderlichen Bandbreite.
recipher (brit.), oder (US) re-encodement, re-encipher	Chiffrieren des gleichen Textes mit min. 2 verschiedenen Schlüsseln. Ermöglichte in BP häufig die Gewinnung von cribs oder dephts (s. dort).
reziprok	Eine Chiffriermaschine ist reziprok, wenn mit gleicher Einstellung chiffriert/dechiffriert wird. Erleichert die Kryptanalyse. Bekannteste Maschine war ENIGMA .

Ringstellung	Ein verdrehbarer Buchstabenring am ENIGMA –Rotor wurde jeweils fixiert zur Permutation.
Rotor, -Scheibe, -Walze	Bezeichnungen für Chiffrierrotoren, für ENIGMA-Rotoren wurde immer „Walze“ verwendet.
Rotorlage	Reihenfolge der Rotoren in der Maschine. Wechselte regelmäßig.
Spruchschlüssel	Gegenseitige Funk-Vereinbarung von Chiffriermaschinen-Einstellungen.
Stator	Unbeweglicher Kontaktring an Ein-und Ausgang von Rotormaschinen zur Übertragung auf die Rotorkontakte.
Steckerfeld	Tastaturausgang der ENIGMA wurde unterschiedlich mit 10 (vorher 6) Kabeln mit dem Eingangsstator über Stecker/Buchsen verbunden.
Steckeruhr	Die Schaltungen des Steckerfeldes wurden durch einen Mehrfach-Umschalter regelmäßig vertauscht.
Tagesschlüssel	Tägliche Voreinstellung von Chiffriermaschinen, aus Tabellen zu entnehmen.
Überschlüsselung	Auch „Überchiffrierung“ genannt, d.h. der Geheimtext wird einer weiteren Chiffrierung unterworfen.
Umkehrwalze	Setzbare Walze der ENIGMA , die den Stromfluß versetzt wieder zurück über die Rotoren lenkte. Ermöglichte Chiffrieren/Dechiffrieren mit der gleichen ENIGMA –Einstellung.
Umkehrwalze D	Wie Umkehrwalze, jedoch mit inneren Steckverbindungen schaltbar (permutierbar).
Verschlüsselung	Chiffrierung mit irgend einem Verfahren.
VIGENÈRE-Verschlüsselung	s. polyalphabetisch.
Walze	s. Rotor.
Walzenlage	s. Rotorlage

Verwendete Abkürzungen

BP	s. Bletchley Park.
BS-4	Abteilung des polnischen Geheimdienstes, für Deutschland zuständig.
Chi	Chiffrierabteilung des OKW, für Entzifferungen zuständig.
Crib	Angenommene bzw. wahrscheinliche Klartextworte/Buchstaben zur Kryptanalyse.
Depth	Hilfsmittel zur Kryptanalyse: Mit gleicher Chiffriermaschinen-Einstellung gesendete verschiedene Texte, oder gleicher Text mit verschiedener Verschlüsselungen ermöglichte Kompromittierungen (s. dort).
GC&CS	Government Code and Cypher School; Tarnbezeichnung für die Chiffrierabteilung des britischen Geheimdienstes. In der Nachkriegsliteratur „BP“.
GCHQ	wie vor, Bezeichnung nach dem Krieg.
MAGIC	Erkenntnisse („Signals Intelligence“) aus US-Entzifferungen japanischer Funksendungen im 2. WK., ähnlich ULTRA.
MI5, MI6	Britischer Inlands- bzw. Auslandsgeheimdienst, zuständig für BP.
NSA	National Security Agency der USA, 1952 gegründet aus dem Zusammenschluß von SIS (Army-Geheimdienst) und OP-20-G. (Navy-Geheimdienst).
OKH	Oberkommando des (deutschen) Heeres.
OKW/Chi	Abkürzung für: OKW/AG WNV/Chi = Oberkommando der(deutschen) Wehrmacht/Amtsgruppe Wehrmachts-Nachrichtenverbindungen, Abt. Chiffrierwesen. Nachfolgeorganisation der Chiffrierstelle des Reichswehrministeriums ab 1938.
OP-20-G	Kryptologisch-technische Abteilung des US-Navy-Geheimdienstes.
OTP	Einmal-Schlüssel-Verfahren zur Chiffrierung.
SIS	Kryptologisch-technische Abteilung des US-Army-Geheimdienstes.
SLU	Special Liaison Unit. Verteilte ausgewählte ULTRA-Informationen an alliierte Frontkommandeure. Sicherung der Übertragung per OTP oder TYPEX.
UKD	s. Umkehrwalze D
TYPEX	Brit. Weiterentwicklung der ENIGMA , kryptologisch stark verbessert.
ULTRA	Erkenntnisse („Signals Intelligence“) aus brit. Entzifferungen dt. und ital. und jap. Funksendungen in Europa, in Zusammenschau mit anderen Informationen.
XOR, -ing, -ed	Boole’sche Logikfunktion Exklusiv-Oder und deren Anwendung.
X-Service	Ursprüngliche Tarnbezeichnung für BP („Station X“).
Y-Service	Weltweiter brit. Abhör- und Peildienst.

2 kryptohistorische Grundlagen

Vermutlich seit es Schriftzeichen gab, versuchte man schriftliche Nachrichten für „Unbefugte“ unlesbar zu machen. Und bereits im 17. Jh. v. Chr. entstand die erste Geheimzeichenschrift, die auf dem „Diskos von Phaistos“ eingraviert wurde.[36]
Auch die späteren Buchstaben-Texte konnte man zunächst nur mit Geheimzeichen verschlüsseln, bis dafür spezielle Chiffrierverfahren erfunden wurden. Deren allmähliche Verbreitung entwickelte dann – analog zum Rechnen – das Bedürfnis, das mühsame und fehleranfällige Chiffrieren zu mechanisieren. Das aber gelang erst im 20. Jahrhundert.
Wie und warum entstand nun diese maschinelle Chiffriertechnik gerade im 20. Jahrhundert?

2.1 erste Chiffriergeräte

Julius CAESAR soll als Erster Texte chiffriert haben, und nach ihm wurde deshalb ein Chiffrierverfahren benannt, der „Cäsar“ (mit einigen Varianten). Neu daran war, daß er keine Geheimzeichen mehr benötigte wie bisher – jeder Buchstabe wurde durch einen anderen ersetzt, der vereinbar dahinter auftritt (bspw. A durch D, usw.). Mithin besteht der Algorithmus dieser Verschlüsselung aus dem Ersetzen der Buchstaben, und der Schlüssel aus der jeweils zu vereinbarenden Anzahl der Positionen, die dazwischen liegen. [CAESAR begnügte sich mit einer festen Verschiebung um 3 Stellen]. Die Sicherheit dieses Verfahrens beruht demnach darauf, daß es ein potentieller Entzifferer[37] nicht kennt, denn anderenfalls könnte er es leicht durch Probieren knacken, da es ja nur 26 verschiedene Schlüssel gibt.[38]

Das galt aber nur bis zur Erfindung kryptanalytische Methoden: Der Caesar-Code war ein monoalphabetisches Verfahren, d.h. es wird nur ein Alphabet verwendet, und ermöglicht demzufolge Entzifferungen durch eine Analyse der Buchstabenhäufigkeiten. Der arabische Kryptologe AL-KINDI erkannte diese Einbruchsmöglichkeit bereits im 9. Jahrhundert n. Chr.

[36] Vgl. Bauer, Geheimnisse, Farbtafel A.
[37] „Entzifferung“ ist die korrekte Bezeichnung für eine Klartextgewinnung ohne Schlüsselbesitz. Wird oft mit „Dechiffrierung“ verwechselt.
[38] Vgl. Eckert, Claudia: IT-Sicherheit. München 2003, S. 218 u. 225.

2.1.1 Chiffrierscheibe

Diese bald allgemein bekannte Schwäche der Caesar-Chiffrierung regte Kryptographen zu Verbesserungen an. Nach gründlicher Vorarbeit PORTA'S (1535-1615) und Vorschlägen von TRITHEMIUS (1462-1516) und ALBERTI (1404-1472) veröffentlichte DE VIGENÈRE (1523-1596) in 1585 ein praxisgerechtes Verfahren, eine sog. polyalphabetische Verschlüsselung, die später nach ihm benannt wurde. Die praktische Lösung benutzte dazu ein Schlüsselwort und ein Quadrat aus 26 Alphabeten, die um jeweils einen Buchstaben verschoben sind. Das Schlüsselwort gibt die jeweilige Stellung vor, anschließend wird jeder Buchstabe mit einem neuen Alphabet verschlüsselt – ein umständliches und fehleranfälliges Verfahren. Das konnte man mit Hilfsmitteln weiter verbessern; besonders erfolgreich war die 1466 von ALBERTI beschriebene Chiffrierscheibe. Sie war die Grundlage der späteren Mechanisierung.
Man mußte nun nur noch die beiden Scheibenteile mit dem Klar- und Geheimtextalphabet gegeneinander verdrehen, konnte den chiffrierten Buchstaben dann direkt ablesen und dann je nach Schlüsselwort die Scheibe neu einstellen.

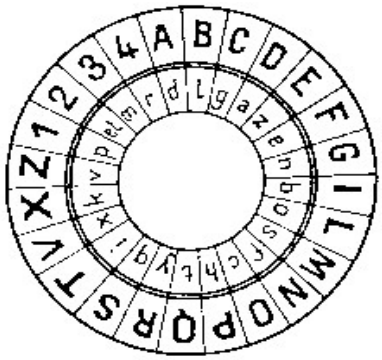


Bild 1: ALBERTI-Scheibe[39]

Statt auf einer Scheibe, ordnete man die Alphabete auch auf Linealen an, die gegeneinander zu verschieben waren. Diese Chiffrierschieber verwendete man nach 1600 in England.[40]

[39] Bild nach Bauer, Geheimnisse, S. 54
[40] Ebd.

2.1.2 Chiffrierzylinder

Die Alberti-Scheibe wurde erst nach über 300 Jahren abgelöst durch ein kryptologisch stärkeres Gerät, dem Chiffrierzylinder. Die erste Konstruktion von 1786 blieb geheim bis ins 20. Jahrhundert, weil der Erfinder, der schwedische Diplomat GRIPENSTIERNA, sie vermutlich für seinen Monarchen sichern sollte. Anschließend stellte der US-Präsident JEFFERSON um 1795 ein fast identisches Gerät vor, und danach folgten im 19. Jahrhundert weitere Erfinder, die das Gerät jedoch nicht verbesserten, bis der US-Army-Kryptologe MAUBORGNE in 1922 eine kryptologisch wirksame Änderung einführte: Die 25 Scheiben konnten nun aus 50 ausgewählt werden. Dieses M-94 bewährte sich für die Verschlüsselung taktischer Nachrichten, bis es im Zweiten Weltkrieg von der Chiffrier-Rechenmaschine M-209 (s. 3.3.1) abgelöst wurde.[41]

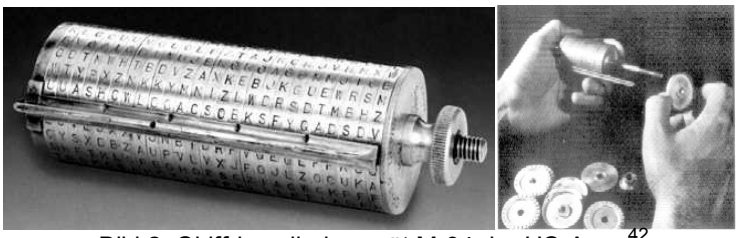


Bild 2: Chiffrierzylindergerät M-94 der US-Army[42]

Die Anordnung der Scheiben wechselte täglich, für erhöhte Sicherheitsanforderungen konnte man wechseln auch bei jeder Nachricht. (Vergleichbare Chiffriermittel gab es in der deutschen Wehrmacht im Zweiten Weltkrieg nicht; auf den unteren Ebenen mußte man wie im Ersten Weltkrieg mit Handverfahren verschlüsseln).

Andere Weiterentwicklungen des Chiffrierzylinder-Verfahrens verbesserten nicht die Sicherheit, jedoch die Anwendbarkeit. Beispielsweise erhielt 1915 der schwedische Erfinder Arvid DAMM[43] ein Patent zuerkannt für ein Chiffrierzylinder-Gerät mit automatischer Fortschaltung nach jeder Buchstaben-Verschlüsselung. Später rüstete er das Gerät mit einer Tastatur aus, die es für Büroanwendungen attraktiv machte; es konnte erfolgreich verkauft werden:[44]

---

[41] Vgl. Bauer, Geheimnisse, S. 129.

[42] Bild nach Bauer, Geheimnisse, Farbtafel D und S. 129.

[43] Identisch mit dem Rotor-Miterfinder A. Damm, s. dort.

[44] Vgl. Hagelin, Boris C.W.: The Story of the Hagelin Cryptos. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, Artech House, Norwood MA/USA, 1998, S. 481-483. (Künftig zit. "Hagelin, Cryptos").

Bild 3: Damm's A21-"Office machine" 1915[45]

Dieses Gerät markiert den Übergang zur maschinellen Kryptographie: Es enthält bereits viele Elemente einer Chiffriermaschine, jedoch fehlt ein Chiffrieralgorithmus, der vom Anwender zu erbringen war. Erst die Erfindung des Chiffrier-Rotors 1917 bewirkte einen Entwicklungssprung, ermöglicht durch die Fortschritte der Elektromechanik, aber auch, weil die Erfinder einen „Markt“ für ihre neuen Geräte sahen.

2.2 erste Chiffriermaschinen

Entscheident ist für kryptographische Maschinen die Fähigkeit, Chiffrieralphabete selbst zu generieren, damit ebenso zu verschlüsseln, und dann umgekehrt den Klartext daraus zurückgewinnen, wofür ein genau definierter Algorithmus vorhanden sein muß. Das trifft im Prinzip ebenso zu für Rechenmaschinen; kryptographische Maschinen kann man mithin als spezielle Rechenmaschinen auffassen und ebenso realisieren. Die Entwicklung der beiden Systeme verlief nicht zufällig sehr ähnlich, wenn man von zeitlichen Verschiebungen absieht.

2.2.1 Fortschritte von Wissenschaft und Wirtschaft

Nach der Mitte des 19. Jahrhunderts begann die Weltwirtschaft zu expandieren als eine Folge der Industriellen Revolution. Nicht zufällig entwickelten sich dazu parallel neue wissenschaftliche Disziplinen, vor allem auf technischem Gebiet, aber auch die Kryptologie.
Der preußische Offizier Friedrich KASISKI (1805-1881) veröffentlichte als erster

[45] Bild nach Hagelin, Cryptos, S. 482.

Kryptologe in 1863 eine Abhandlung „Die Geheimschriften und die Dechiffrierkunst." Darin beschreibt er ein Verfahren, einen polyalphabetisch verschlüsselten Text zu entziffern, das später als „Kasiski-Test" bekannt wurde. Charles BABBAGE hatte ein ähnliches Verfahren bereits 1854 entwickelt, seine Arbeit allerdings nicht veröffentlicht. Sie wurde erst im 20. Jahrhundert in seinem Nachlaß gefunden; KASISKI konnte von den kryptanalytischen Arbeiten BABBAGES daher nichts gewußt haben. Er hatte mit seiner Publikation die *öffentliche* wissenschaftliche Kryptanalyse begründet, denn bisher entzifferten Kryptologen in fürstlichen „Geheimkabinetten".

KASISKI'S Methoden wurden weiterentwickelt und die Ergebnisse publiziert durch KERCKHOFFS (1883), DE VIARIS (1893, s.u.) und DELASTELLE (1902). Dementsprechend waren um die Jahrhundertwende Methoden bekannt, polyalphabetische Chiffrierungen zu entziffern.
Die erwähnte Entwicklung von Handel und Wirtschaft, mit „Globalisierung" einhergehend, bewirkte eine entsprechende Intensivierung des Nachrichtenverkehrs im letzten Drittel des 19. Jahrhunderts. Einen weiteren Schub erzeugte die Erfindung der Funktelegraphie, deren kommerzieller Einsatz bald nach der ersten erfolgreichen Transatlantik-Übertragung (1901) begann, und einen schnellen Nachrichtenaustausch mit nicht von Telegraphen erschlossenen Gebieten ermöglichte. Deren Abhörbarkeit steigerte den Bedarf nach leistungsfähigeren Chiffrierverfahren, für welche die wirtschaftlichen und technischen Voraussetzungen nun gegeben waren. Ein Indiz dafür ist auch die große Zahl der Patente, die seit 1880 dafür zuerkannt wurden: Beispielsweise konstatierte der Experte Siegfried TÜRKEL: „Es existieren unzählige Chiffrier- und Dechiffriergeräte und –maschinen, welche Patentschutz genießen." Freilich befänden sich darunter auch „primitivste Geräte" und vermutlich nur wenige wirklich geeignete Maschinen, „[...] welche nach Art einer Schreibmaschine gebaut sind."[46]

Eine Maschine scheint ihm entgangen zu sein, denn sie war nicht patentiert, und sie war keine Schreibmaschine: Um 1888 erfand der französische Offizier Marquis de VIARIS (1847-1901) eine Chiffriermaschine, die den Geheimtext auf einen Streifen ausdruckte und auch sonst als die erste „richtige" Chiffriermaschine gelten kann.[47] Vermutlich geriet sie in Vergessenheit, weil es dafür noch keine militärischen Anwender gab. Und kommerzielle Anwender werden Schreibmaschinen bevorzugt haben.

2.2.2 Chiffrier-Schreibmaschinen

Schon bald nachdem Schreibmaschinen verwendet wurden, muß das Bedürfnis entstanden sein, damit geschriebene Texte geheim zu halten, vermutlich um sie vor dem Personal zu verbergen. So wurden bald Chiffrier-Schreibmaschinen von

[46] Türkel, Siegfried: Chiffrieren mit Geräten und Maschinen, Graz 1927, S. 44.
[47] Vgl. Kahn, Codebreakers, S. 240. Nach Kahn soll die erste druckende Chiffriermaschine bereits vor 1874 von Emile VINAY und Joseph GAUSSIN erfunden worden sein.

Erfindern angeboten, deren viele Mängel wohl eine größere Verbreitung verhinderten; Produktion und Verwendung dieser Maschinen wurden bisher nicht untersucht.
1889 wurde die erste Chiffrierschreibmaschine "Typewriter Ciphograph" von G. BOFINGER patentiert[48], eine Maschine mit Buchstabenverschiebung, die jedoch vermutlich nicht hergestellt wurde. Belegt ist die Produktion der „Merrit", im gleichen Jahr patentiert, die Text verschlüsselte, indem man bewegliche Lettern in jeweils unterschiedlicher Reihenfolge einsetzte und damit ein anderes Alphabet erzeugte.[49] Mit dem Empfänger mußte man deren Reihenfolge vereinbaren, so daß dieser den Text auf gleiche Weise dechiffrieren konnte. Das umständliche Einsetzen von Lettern vermied man später durch auswechselbare Tasten, und vereinfachte diese Methode dann durch Kappen, die auf die Tasten gesteckt wurden.[50] So ließen sich sogar vorhandene Schreibmaschinen kostengünstig umrüsten.
In der 1899 patentierten „Diskret" hingegen verwendeten die Erfinder eine modifizierte Alberti-Scheibe: Die zu druckenden Buchstaben waren auf einer Scheibe aufgetragen; eine zweite innere Scheibe mit Buchstaben konnte man dazu verdrehen und so ein anderes Alphabet erzeugen:

Bild 4: Geheimschreibmaschine "Discret"[51]

Diese einfachen Verschlüsselungen boten jedoch wenig Sicherheit, waren umständlich anzuwenden und dadurch fehleranfällig.

Erst die Erfindung der elektrischen Schreibmaschine ermöglichte Verbesserungen. Bereits 1892 wurde die erste funktionsfähige elektrische Schreibmaschine „Cahill Universal Electric" patentiert, die nach 1901 in kleinen Stückzahlen verkauft wurde.[52] Diese Maschine besaß einen speziellen Vorteil

[48] US-Patent N° 396.592 vom 22.1.1889.
[49] Vgl. Martin, Ernst: Die Schreibmaschine und ihre Entwicklungsgeschichte, 8. Aufl., Aachen 1949, S. 369.
[50] Österr. Patent Nr. 51351/ 27.12.1911 (Kanschine, Jellinek-Mercedes). Der Erfinder des Chiffrierrotors H.Hebern erhielt zusammen mit Hoffmann ein österr. Patent Nr. 70448/ 10.11.1915 für eine verbesserte Version.
Vgl. Türkel, Siegfried: Chiffrieren mit Geräten und Maschinen, S. 14-15.
[51] Bild nach Heinz Nixdorf MuseumsForum (HNF), Abteilung Kryptologie.
Ryska, Norbert.: „Weltgeschichte der Kryptologie", Vortrag in Bildern und Texten. Stand 4.12.02.
(zukünftig zit.: HNF/Ryska, Vortrag Kryptologie)
[52] Vgl. Martin, Ernst: Die Schreibmaschine und ihre Entwicklungsgeschichte, S. 370.

gegenüber anderen, nach der Jahrhundertwende angebotenen elektrischen Maschinen: Jeder Typenhebel wurde *einzeln* elektromagnetisch bewegt, d.h. die Maschine konnte auch extern angesteuert werden.
Das erkannte wohl der Erfinder Edward Hugh HEBERN (1869-1952), als Bauunternehmer ein Hobby-Kryptograph, der, wie bereits in Fußnote 50 erwähnt, schon ein Patent für eine einfache Chiffrierschreibmaschine zuerkannt erhalten hatte. Er experimentierte mit dieser diskreten Ansteuerung der Typenhebel und verdrahtete dabei die Maschine anders, so daß sie jeweils andere Buchstaben druckte und so den Text verschlüsselte; ein gleich verdrahtetes Gerät beim Empfänger wandelte ihn zurück in Klartext. Eine Umschaltmöglichkeit sorgte für Wechsel des Verdrahtungsschemas; diese Wechsel mußten vorher vereinbart werden, wenn einfache monoalphabetische Verschlüsselung nicht ausreichte. Das war umständlich und fehleranfällig, und aus diesem Grund wird HEBERN nach einer Verbesserung gesucht haben, die ihm später mit der Erfindung des Chiffrierrotors gelang.

Bild 5: erster Erfinder des Chiffrierrotors H. Hebern[53]

In der Folgezeit benutzte er zwei Schreibmaschinen, die er über schaltbare Verbindungskabel angesteuerte. Damit konnten Klar- und Geheimtext zugleich ausgedruckt und die Chiffrierung sicherer gemacht werden, weil die jeweiligen Schaltverbindungen umsteckbar waren. Damit erhielt man eine wesentlich sichere polyalphabetische Chiffrierung, die bei 26 Buchstaben $26! = \text{ca. } 4 \times 10^{26}$ theoretisch[54] mögliche Permutationen umfaßte.
Doch das umständliche und fehleranfällige Umstecken der Verbindungskabel wird potentielle Anwender ebenso nicht überzeugt haben, denn das Verfahren erlangte keine praktische Bedeutung.
Gleichwohl ist diese Vorrichtung technikhistorisch bemerkenswert, weil der Erfinder sich mangels Erfolg Gedanken machen mußte über eine automatische Umsteckung der Verdrahtungen – mithin über einen Chiffrier-Algorithmus. HEBERN kannte vermutlich nicht den Begriff Algorithmus, und kam später empirisch auf die brilliante Idee, dieses mit einem neuen elektromechanischen Bauelement zu realisieren, nämlich mit einem Chiffrierrotor, dessen Aufbau und Anwendung unter 3.1 beschrieben ist.

[53] Bild nach HNF/Ryska, Vortrag Kryptologie. © David Kahn Collection, New York.
[54] Zur Fragwürdigkeit theoretischer Schlüsselzahlen s. unter 3.2.2.

2.2.3 Chiffrier-Rotormaschinen und -Fernschreiber

Durch den Kriegsausbruch 1914, nach über 50 Jahren Frieden, entstand ein „Markt“ für alles Neue, das militärisch irgendwie verwendbar war. Vorausschauende Erfinder dachten vermutlich an den zu erwartenden sprunghaft steigenden Bedarf, militärische Nachrichten zu verschlüsseln, besonders wegen der inzwischen militärisch genutzten, abhörbaren Funkübertragung. Daher müßten militärische Stellen ein großes Interesse an Verfahren haben, die Verschlüsselungen einfacher, schneller und sicherer machen. Und das konnten nur maschinelle Verfahren leisten.

Aus der Vorkriegszeit wird HEBERN und den anderen Erfindern bekannt gewesen sein, daß sichere und einfache Verschlüsselung längerer Texte problematisch war: Die damals verbreitete Methode – Codebücher – war umständlich und fehleranfällig, und diente vor allem dazu, Telegramm-Gebühren zu sparen. Zuverlässige Verschlüsselungen waren damit schon deshalb problematisch, weil Codebücher nicht häufig gewechselt werden konnten, weshalb die Codes noch überschlüsselt werden mußten für eine ausreichend sichere Chiffrierung. Dieses umständliche Verfahren verwendeten vor allem militärische und diplomatische Dienste.
Die deutschen Militärs verschlüsselten zu dieser Zeit ihre geheimen Nachrichten mit Varianten der polyalphabetischen Chiffrierung (Heer) oder Codebücher (Marine), doch beides war fehleranfällig und entzifferbar. Letzteres freilich besonders leicht, wenn so ein Codebuch in feindliche Hände fiel. Das passierte schon bald nach Beginn des Ersten Weltkrieges nach der Versenkung des Kreuzers „Magdeburg“: Russische Taucher bargen das im Wrack befindliche Marine-Codebuch und übermittelten den Briten eine Kopie. Damit konnte schon im Ersten Weltkrieg die Royal Navy den Funkverkehr der deutschen Flotte mitlesen.
Nachdem die USA sich voraussichtlich am Krieg beteiligen würden, sah HEBERN wohl ein großes Potential für die Anwendung maschineller Kryptographie im Kriege. So intensivierte er sein Hobby, erfand dabei 1917 den Chiffrierrotor und baute damit eine erste Rotor-Chiffriermaschine. Er nutzte seine Beziehungen zur US-Navy und konnte einige Maschinen zu Versuchszwecken verkaufen.
Nach Kriegsbeginn benötigte die US-Army eine leistungsfähige Nachrichtenverbindung zu ihrem Corps nach Europa. Die damals zur Verfügung stehende Telegraphie war umständlich zu nutzen, und eine direkte Verschlüsselung nicht bekannt. Die US-Army glaubte jedoch, mit dem neuentwickelten Fernschreiber und Multiplexübertragung eine sichere Übertragung zu haben, und beauftragte die führende US-Telegraphiefirma AT&T das zu prüfen. Deren junger Ingenieur Gilbert VERNAM (1890-1960) konnte jedoch nachweisen, daß diese Fernschreib-Übertragung keine Sicherheit bot, denn ein Unbefugter könnte per Oszillograph die Impulse aufzeichnen und daraus den Text rekonstruieren. Er dachte darüber nach, und erfand das erste *online*-Chiffrierverfahren nach heutigen Begriffen (s. 4.2).

Bild 6: Erfinder der Fernschreiber-Ciffrierung G. Vernam[55]

Beide genannten Erfindungen entstanden empirisch: HEBERN war Geschäftsmann und beschäftigte sich mit Chiffriermaschinen als Hobby-Konstrukteur. VERNAM hatte Fernmeldetechnik studiert und arbeitete als Telegrapheningenieur, von wissenschaftlicher Kryptologie hatten beide sehr wahrscheinlich nichts gehört. Denn damals gab es nur wenige Wissenschaftler und einige Offiziere, die sich damit befaßten.
VERNAM hatte vermutlich ebenso empirisch die Boole'sche Operation „Exklusiv-Oder" für sein Verfahren „erfunden" und elektromechanisch realisiert, denn diese mathematischen Logikfunktionen kannten damals auch nur wenige Gelehrte.
Die jeweils ersten Geräte beider Erfinder wurden jedoch mit wissenschaftlicher Hilfe kryptologisch verstärkt: Die Schwäche von Hebern's Rotormaschine bewies die US-Navy-Kryptologin Agnes MEYER (später DRISCOLL), indem sie einige damit verschlüsselte Nachrichten entzifferte. Nach ihren Empfehlungen verbesserte HEBERN seine Maschine, blieb jedoch ohne kommerziellen Erfolg.
Nicht besser erging es VERNAM: Seine Erfindung der Fernschreiber-Chiffrierung prüfte der US-Army-Kryptologe MAUBORGNE und erkannte dessen Schwachstelle: Die wiederholte Verwendung des gleichen, relativ kurzen Schlüssel-Lochstreifens schwächte die Chiffrierung zu sehr. Er empfahl eine wichtige Verbesserung, nämlich das Schlüsselband nur einmal zu verwenden, das spätere sog. One-Time-Pad (s. 4.5). Sein Chef Parker HITT entwickelte dazu eine Vorrichtung zur Schlüsselgenerierung mit hintereinander geschalteten Stifträdern. Doch trotz dieser Verbesserungen übernahm die US-Army das Verfahren nicht, und im zivilen Bereich gab es kaum Interessenten, denn der Durchbruch des Fernschreibers stand noch bevor. VERNAM ließ seine Erfindung zwar patentieren, verlor mangels Nachfrage jedoch das Interesse an der Chiffriertechnik und machte später Karriere als Nachrichtentechniker; zahlreiche Patente auf diesem Fachgebiet zeugen von seiner Begabung.
Die geschilderten US-Entwicklungen wurden nach empirischen Anfängen umgehend kryptologisch verbessert. In Deutschland hingegen scheint der ENIGMA-Erfinder SCHERBIUS wissenschaftliche Beratung nicht erhalten und wohl auch nicht gesucht zu haben, und eine militärische Kryptologie gab es ohnehin nicht.

[55] Bild nach HNF/Ryska, Vortrag Kryptologie. © David Kahn Collection, New York.

3 Technik der Rotor-Chiffriermaschinen

Nach dem 1. Weltkrieg kam es zu einem Patentstreit um das Rotorverfahren, das sich drei europäische Erfinder patentieren ließen, die vermutlich die Erfindungen der jeweils anderen nicht kannten. Auch nicht HEBERN'S Maschine von 1917, die er damals nur den US-Militärs vorgestellt hatte, und aus unbekannten Gründen erst 1921 zum Patent anmeldete, das 1924 erteilt wurde (US-Patent 1,510,441).
Als Erster meldete Artur SCHERBIUS (1878-1929) am 23.2.1918 ein Patent an (DRP 416219), gefolgt vom Niederländer Hugo A. KOCH (1870-1928) in 1919. Doch neuerdings postuliert der niederländische Historiker Karl DE LEEUW, daß die holländische Marine bereits ab 1915 eine geheime Rotormaschine verwendet habe, auf die vermutlich Koch's Patent beruhe, und die der ENIGMA A sehr ähnlich gewesen sei. Daher wären die beiden Marineoffiziere VAN HENGEL und SPENGLER die ersten Erfinder der Rotormaschine, für die sie ebenfalls 1919 ein Patent beantragen wollten. Vom Patentanwaltsbüro soll dann KOCH, dank verwandtschaftlicher Beziehungen, von dieser Anmeldung erfahren und dann selbst genutzt haben.[56] Allerdings existiert von dieser Marine-Maschine nur eine vage Beschreibung, und DE LEEUW konnte für seine Behauptung bisher auch keine relevanten Dokumente nachweisen.

Ebenfalls 1919, drei Tage nach KOCH, meldete der Schwede Arvid DAMM (?-1928) ein Rotormaschinen-Patent an, das jedoch von den vorgenannten abwich: Es beruhte auf dem sog. „Halbrotor" (s. 3.2.5), weil der Erfinder dieses Element für die Verschlüsselung von Funk-Telegraphiesendungen für geeigneter hielt.

Es ist bezeichnend, daß die vier Erfinder unabhängig um die gleiche Zeit zum gleichen Ergebnis gelangten, vermutlich weil sie eine große Nachfrage erwarteten. Das aber war ein Irrtum: Nach dem Weltkrieg hatten die Militärs kaum Interesse, und der kommerzielle Absatz blieb gering, vermutlich weil die Maschinen relativ teuer und umständlich zu bedienen waren. Man verwendete die vorhandenen Codebücher weiter.

[56] Vgl. Leeuw, Karl de: The dutch invention of the rotor machine, 1915 - 1923. In: Cryptologia 27 (2003), 73 - 94.

3.1 Hebern-Maschinen

HEBERN erfand 1917 als erster einen maschinellen Chiffrier-Algorithmus: Eine isolierende Scheibe mit seitlichen 26 Buchstaben-Kontakten wird von beidseitig 26 Gegenkontakten abgetastet, und nach jedem chiffrierten Buchstaben einen Schritt weiter gedreht. Eine solche Scheibe, von Kryptologen als „Rotor“[57] bezeichnet, chiffriert nach jedem Schritt mit einem neuen Alphabet („rotierende Alphabete“) und erzeugt damit einen Algorithmus. Diese Konstruktion benötigt jedoch eine elektrische Ausgabe- bzw. Anzeigevorrichtung, wofür HEBERN zunächst eine der erwähnten elektrischen Schreibmaschinen mit diskreter Schreibhebelansteuerung verwendete.

Vermutlich um die Kosten für sein erstes Verfahren zu begrenzen, verzichtete HEBERN dann auf eine elektrische Schreibmaschine und wählte stattdessen ein preisgünstigeres Buchstaben-Anzeigefeld mit Glühlämpchen.
Das nachstehende Bild zeigt HEBERN'S erste kommerziell angebotene Maschine, mit Glühlampen-Anzeige und einfachen Rotor, die erste lieferbare funktionsfähige Rotormaschine überhaupt:

Bild 7: HEBERNS Rotor-Chiffriermaschine (ca.1918)[58]

[57] In Deutschland verwendete Scherbius für die ENIGMA den Begriff „Durchgangsrad“; „Walze“ verwendete später das Militär.
Vgl. dazu Bauer, F.L.: Scherbius und die ENIGMA. Informatik-Spektrum (1991) 14, S. 212.

[58] Bild nach www.math.hr/~duje/ slike/Hebern1.jpg, am 7.11.03.

Der permutierbare Rotor

Eine weitere, von HEBERN erstmals patentierte Maschine mit Schreibmaschinen-Ausgabe chiffrierte mit einem permutierbaren Rotor („*code wheel*“, N° 59). Dieser verstärkte den kryptologisch schwachen Algorithmus der Chiffrierung der Ein-Rotor-Maschinen durch eine variable Permutierung, die man durch Wechsel der inneren Verdrahtung bewirkte. Diese Variante setzte sich jedoch nicht durch, vermutlich war der Aufwand für das Umklemmen der Verdrahtungen innerhalb des Rotors zu groß.

Gleichwohl kam man im Zweiten Weltkrieg wieder auf dieses Prinzip zurück: Ab 1944 bereitete die per inneren Steckverbindungen permutierbare „Umkehrwalze D“ (UKD) in der ENIGMA I (s. 3.2.3) den Entzifferern erhebliche Probleme.

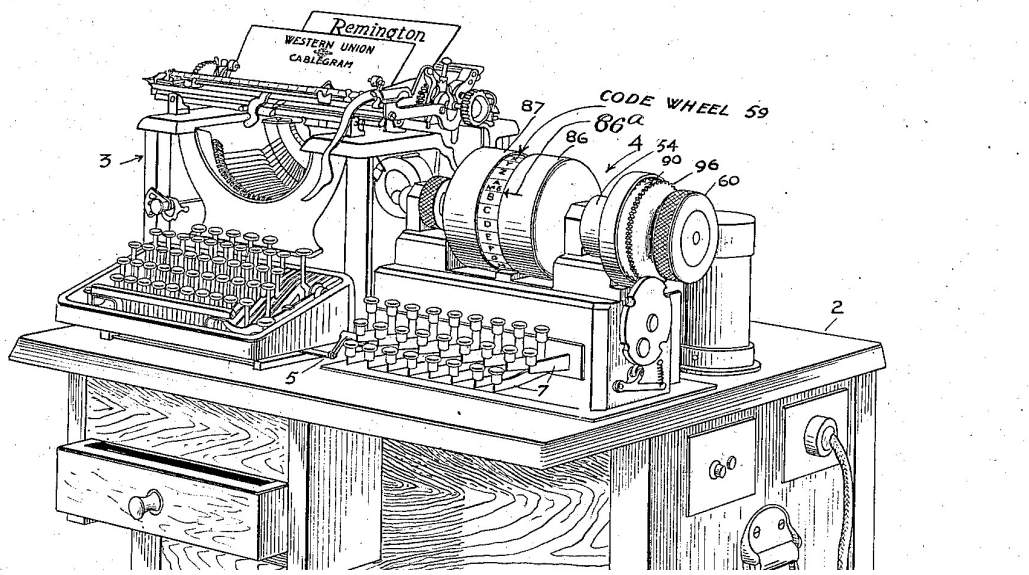


Bild 8: HEBERNS „Electric Coding Maschine“ (1921)“[59]

Der Mehrfachrotor

Der Erfinder SCHERBIUS (s.u.) ging bei der ENIGMA einen anderen Weg, um die kryptologische Schwäche des einfachen Rotor-Algorithmus zu vermeiden. Er schaltete bei seinen Maschinen mehrere Rotoren elektrisch hintereinander, deren Stellung zueinander verdrehbar war, indem ein Zahnradantrieb schrittweise Rotationen bewirkte. Das ersetzte er später durch eine weniger aufwendige Konstruktion: Jeder Tastendruck eines Klartextzeichens bewegte den ersten Rotor

[59] Bild nach US-Patentschrift 1,510,441. US- Patent and Trademark Office. Von: http://www.uspto.gov/patft/help/.htm, am 16.01.02.

einen Schritt, und nach 25 Schritten rastete eine Klinke in den Nocken des benachbarten Rotors ein. Der 26. Schritt, der letzte des deutschen Alphabets, erfolgte nun gemeinsam und drehte den zweiten Rotor einen Schritt weiter, beim dritten Rotor ebenso. Diese zählerartige Konstruktion wurde dann Standard fast aller Rotormaschinen.

Auch HEBERN übernahm dieses Verfahren für seine HCM-Maschinen, die er für die US-Navy entwickelte; vier Rotoren sind im Bild gut zu erkennen, weil der Andruck gelöst wurde:

Bild 9: Hebern's HCM-4-Rotoren-Maschine (ca. 1924)[60]

Doch 1925 bewies der berühmte US-Army-Kryptologe William FRIEDMANN (1891-1969) die Schwäche der Maschine, indem er damit verschlüsselte Nachrichten entzifferte. Daraufhin verbesserten Navy-Kryptologen, unter Beteiligung FRIEDMANNS, die Maschine mehrfach, und entwickelten 1936 nach einigen Zwischenmodellen die SIGABA-Maschine, die sicherste (und teuerste) Rotormaschine des Weltkrieges, die bis 1959 verwendet wurde für höchste Geheimhaltungsstufen.

3.2 ENIGMA

Über die ENIGMA (grch. Rätsel) gibt es zahlreiche Berichte und Geschichten höchst unterschiedlicher Qualität, aber vergleichsweise wenige korrekte Publikationen. Wie nun entstand diese historisch wichtigste Rotormaschine und wie entwickelten sich Technik und Anwendung bis nach dem Weltkrieg?

[60] US-Patent N° 1,683,072.
Bild von http://www.uni-mainz.de/~pommeren/Kryptologie/Klassisch/4_ZylRot/Hebern.gif.

Bild 10: ENIGMA-Konstrukteur A. Scherbius[61]

3.2.1 Die kommerzielle Herkunft

Der promovierte Elektroingenieur SCHERBIUS (?-1929) hatte sich bislang nicht mit Kryptologie beschäftigt, sondern erhielt als vielseitiger Erfinder Patente für Heizungen, elektrische Schalter, Motorsteuerungen usw. zuerkannt. Mit seinem Partner RITTER betrieb ein kleines Fertigungsunternehmen für Elektrogeräte, dessen Geschäfte schlecht liefen. Es ist nicht bekannt, wer oder was SCHERBIUS zu kryptologischen Überlegungen anregte, und vermutlich analog zu HEBERN hoffte er auf militärischen Bedarf. Er reichte am 23.2.1918 eine Patentschrift[62] ein über eine Chiffrier-Rotormaschine, mit dem erwähnten Mehrfachrotor-Verfahren, wobei vier aus bis zu 10 Rotoren nacheinander in die Maschine eingesetzt werden konnten.[63]
Er bot dann der damaligen Kaiserlichen Marine seine Maschine an und erhielt auch eine positive Beurteilung am 16.7.1918. Gleichwohl lehnte der Admiralstab eine Beschaffung zum damaligen Zeitpunkt ab, und empfahl stattdessen die Maschine dem Auswärtigen Amt anzubieten, doch auch dieser Versuch blieb erfolglos.[64]
So mußte SCHERBIUS auf zivile Anwendungen setzen und verkaufte 1923 mangels Kapital seine Patentrechte an die Gewerkschaft Securitas, die spätere Chiffriermaschinen AG Berlin, wo er den Posten des Cheftechnikers übernahm.[65]
Er starb 1929 bei einem Verkehrsunfall.

Die erste dort produzierte ENIGMA A war noch unhandlich und schwer, und wurde 1924 durch die leichtere ENIGMA B ersetzt; beide Geräte hatten ein Schreibwerk. Trotz großen Werbeaufwands konnten nur wenige Maschinen verkauft werden; sie waren wohl zu teuer, und das wirtschaftliche Umfeld nach dem Krieg nicht günstig.

---

[61] Bild nach http://www.uni-mainz.de/~pommeren/Kryptologie/Klassisch/4_ZylRot/HistRot.html
[62] DRP 416 219
[63] Vgl. Bauer, Secrets, S. 107.
[64] Vgl. Bauer, F.L.: Scherbius und die ENIGMA. Informatik-Spektrum (1991) 14, S. 212.
[65] Vgl. Kruh / Deavours: The Commercial ENIGMA. S. 1

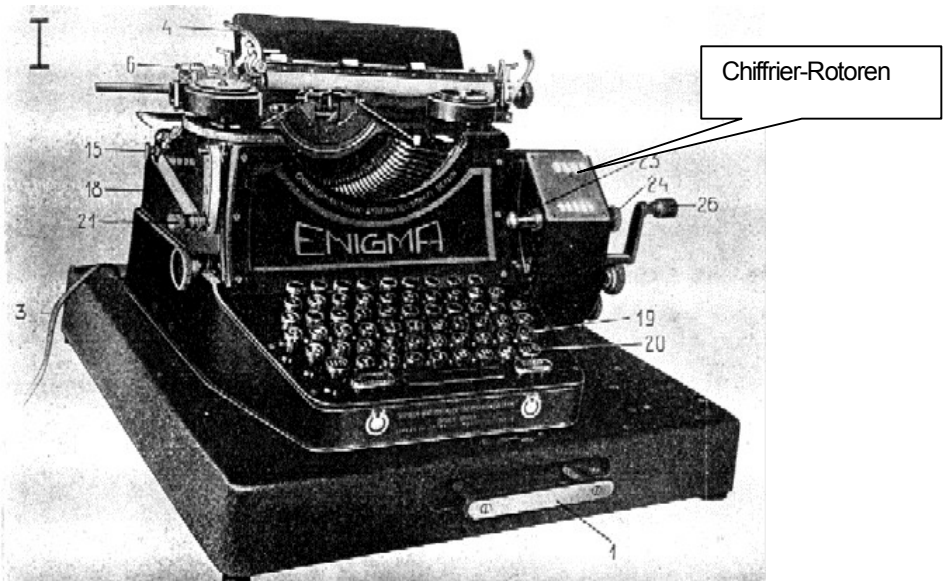


Bild 11: ENIGMA B (1924)[66]

Die ENIGMA B war eine modifizierte elektrische Schreibmaschine mit einer seitlich angebrachten Chiffriereinrichtung aus 2 x 4 [umständlich] einstellbaren Rotoren; der zu vereinbarende Schlüssel bestand entsprechend aus acht Buchstaben. Sie konnte auf Klartext umgestellt und wie eine normale Schreibmaschine verwendet werden.[67]

Militärisches Interesse

Die Chiffriermaschinen AG bewarb die ENIGMA B intensiv und präsentierte sie auf Postausstellungen als „unbrechbar“. Dort entdeckten sie Offiziere der Abteilung Chiffrier- und Nachrichtenwesen der Reichswehr, die daraufhin einige Exemplare zu Versuchen erwarb. [68]

Der Hintergrund dieser für deutsche Offiziere ungewöhnlichen Aktivitäten liegt vermutlich in deren Fehlern im Ersten Weltkrieg: Nachdem CHURCHILL seine Kriegserinnerungen *The World Crisis* 1923 publiziert hatte, und darin u.a. über die gelungene Entzifferung des "Zimmermann-Telegramms" (s. Fußnote 10) und andere kryptanalytische Erfolge berichtete, waren die deutschen Offiziere schockiert: Sie konnten darin lesen, daß der größte Teil des militärischen (und diplomatischen) Nachrichtenverkehrs von britischen und/oder französischen Experten entziffert worden war. Und daß dieser Erfolg u.a. auf der Schwäche der dilettantischen Chiffrierungen beruhte, die sich Hobby-Kryptographen unter den Nachrichtenoffizieren ausgedacht hatten – weil eine militärische Kryptologie

[66] Bild nach Türkel, Siegfried: Chiffrieren mit Geräten und Maschinen, Tafel N, Fig. II.
[67] Ebd. S. 81.
[68] Vgl. Kahn, Codebreakers. S. 972.

fehlte. Verständlicherweise suchten sie nun nach einer sicheren und leistungsfähigen Chiffriermethode für ihre militärische Kommunikation; die ENIGMA schien dafür geeignet zu sein.

ENIGMA C

Vermutlich beanstandeten die Offiziere das schwere und teure Schreibwerk der ENIGMA B, denn das erschwerte eine militärische Verwendung: SCHERBIUS ersetzte es daher durch ein Glühlämpchenfeld nach Hebern's Idee. Dazu erfand Scherbius' Konstrukteur Karl KORN eine sog. „Umkehrwalze" (DRP 452 194, angem. 21.3.1926), die es ermöglichte, mit gleicher Einstellung der Maschine zu chiffrieren und dechiffrieren, und damit die Bedienung erheblich vereinfachte. Doch wurden hierzu Kryptologen offenbar nicht konsultiert, weder von SCHERBIUS, noch von den Offizieren, denn: Diese Walze machte nämlich die Maschine reziprok, indem die Buchstaben beim Ver- und Entschlüsseln jeweils fest zugeordnet waren. Überdies konnte nun nicht mehr ein Buchstabe mit sich selbst verschlüsselt werden. Beides schwächte die Chiffriersicherheit stark und erleichterte die spätere Brechung; die Gründe dafür sind unter 5.2 eingehend beschrieben.

Die Maschine mit den genannten Änderungen erhielt die Bezeichnung ENIGMA C und wurde ab 1926 (etwas modifiziert) als „Funkschlüssel C" von der Marine auf Schiffen eingesetzt und bis 1934 verwendet. Doch bereits 1930 erkannte der Nachrichtenoffizier und Hobbykryptologe Oberleutnant z.S. LUCAN, daß diese ENIGMA „weder technisch noch kryptologisch modernen Ansprüchen genügt." Das schrieb er in einer Studie, doch es dauerte dann bis 1934, bis die Marine zur ENIGMA I wechselte.[69] Zu diesem Zeitpunkt setzte der Chef OKW/WNV (FELLGIEBEL) ein gemeinsames Wehrmachtsmodell durch, die ENIGMA I.

ENIGMA D

Die kommerzielle Weiterentwicklung ENIGMA D erhielt erstmals austauschbare Rotoren, nun offiziell als „Walzen" bezeichnet, und die Umkehrwalze konnte mitbewegt werden wie die anderen drei Rotoren. Diese Maschine wurde ein kommerzieller Erfolg, erweckte jedoch auch das Interesse der Geheimdienste, so daß sie viele Industriestaaten zu Studienzwecken kauften und manche weiter entwickelten.

[69] Neue Chiffriermaschine für die Marine. Geheime Kommandosache der Marineleitung vom 7.2.1930, dazu Schriftwechsel. BA-MA.

ENIGMA G

Die positiven Berichte der Marine über die ENIGMA C erhielt auch die Heeres-Chiffrierstelle um 1927. Man erkannte die Vorteile der Maschine für den Heeresgebrauch [kryptologische Analysen werden nicht erwähnt] und sorgte daher für Anpassungen: Standard-Tastatur, 26-er Rotoren ohne Umlaute, und ein Spruchschlüsselverfahren ohne Codebuch.[70] Dazu ebenfalls austauschbare, jedoch exklusiv für das Heer anders verdrahtete Walzen, und die Umkehrwalze kam in eine feste Position. Damit begann die Reichswehr am 15.7.1928 ein umfangreiches Versuchsprogramm. Der mit dieser Maschine verschlüsselte Funkverkehr konnte vom polnischen Geheimdienst nicht mehr entziffert werden. So suchte er nach Methoden zur Brechung dieser neuen Verschlüsselung, denn dessen deutsche Sektion BS-4 konnte bisher den deutschen militärischen Funkverkehr regelmäßig mitlesen. Diese Nachrichten hielt man wegen der latenten Kriegsgefahr für sehr wichtig.

3.2.2 Wehrmachts-ENIGMA-Versionen

Die erwähnte Studie[71] des Nachrichtenoffiziers erwähnt dann den „...neuesten Funkschlüssel, den die [Hersteller-]Firma auf Grund jahrelanger Erfahrungen herausgebracht hat." Man könne daher annehmen, „...daß die unbefugte Entzifferung auch mit dem Besitz dieses Funkschlüssels nicht möglich ist."

Dieser „neueste Funkschlüssel" erhielt später die Bezeichnung ENIGMA I (I = „Eins"), und unterschied sich von den Vorgängermodellen durch ein Steckerbrett, welches die eingetasteten Klartextbuchstaben vertauschte, und dann das durch die Walzen erzeugte Chiffrat überschlüsselte. Diese Maschine wurde 1930 Standardmodell des Heeres, und nach weiteren Verbesserungen die historisch wichtigste Rotor-Chiffriermaschine des Zweiten Weltkrieges.

Das nachstehende Schema zeigt die Funktion der Maschine:

[70] Kahn, David: Seizing the Enigma: The Race to Break the German U-Boat-Codes, 1939-1943. Houghton Mifflin, Boston MA/USA, 1991. Vermutlich verwechselt hier Kahn die „Chiffrierstelle" mit dem für Beschaffung und Erprobung zuständigen Heeres-Waffenamt.

[71] Neue Chiffriermaschine für die Marine.

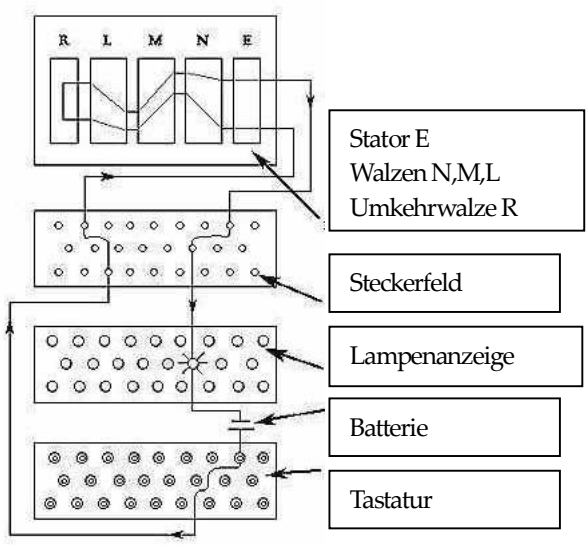


Bild 12: ENIGMA I – Stromlaufplan[72] (schematisch)

Wurde ein Buchstabe auf der Tastatur gedrückt, schloß sich der Stromkreis. Er verlief dann über das Steckerfeld, wurde dort per einzusteckendem Kabel zu einem anderen Buchstaben geleitet (= vertauscht) und kam dann in den Eingangs-Stator. Dessen Kontakte leiteten weiter über die Walzen L, M und N, wo die Chiffrierung durch vielfache Vertauschung erfolgte. In der stationären Umkehrwalze R drehte sich die Stromrichtung und der Strom floß zurück durch die Walzen bis zum Eingangs-Stator. Diese schon 1926 eingeführte Umkehrwalze erleichterte die Bedienung: Man konnte bequem mit der gleichen Walzeneinstellung chiffrieren und dechiffrieren, aber die Maschine wurde damit reziprok. Das schwächte die ENIGMA-Maschinen erheblich, weil nun kein Buchstabe mehr mit sich selbst verschlüsselbar war, und dadurch Kryptanalytiker leichter die Lage eines „wahrscheinlichen Wortes“ im Geheimtext ermitteln konnten.[73]

Vom Stator E verlief der Strom zurück über die Steckerfeld-Vertauschung wie vor, und ließ dann die jeweilige Glühbirne aufleuchten, die dem gesteckerten Buchstaben zugeordnet war. Wurde der nächste Buchstabe auf der Tastatur gedrückt, drehte sich die erste Walze N einen Schritt weiter und schaltete damit zu einem anderen Buchstaben, d.h. es wurde mit einem neuen Alphabet verschlüsselt, entsprechend einer polyalphabetischen Chiffrierung.
Nach 25 Schritten, bei insgesamt 26 Buchstaben, vollzog Walze N ihre volle Umdrehung und nahm die zweite Walze M mit, nach Art eines Kilometerzählers. Diese drehte sich dabei einen Schritt weiter, bis sie ebenfalls nach einer vollen Umdrehung die dritte Walze bewegte, usw. Der vierte „Rotor“ hingegen, die Umkehrwalze, konnte nicht bewegt sondern nur gesetzt werden. Die Mitnahme bewirkten Stoßklinken auf den Walzen und Nuten auf den Einstellringen; doch

[72] Bild nach Rejewski, M.: Mathematical Solution of the Enigma Cipher, (Transl. by Kasparek), S. 321. In: Deavours, Cipher A. et al. (Eds.): Cryptology – machines, history and methods. Artech House, Norwood MA/USA, 1989.
[73] Kryptologische Begründung s. Bauer, Geheimnisse, S. 270-273.

die Walzen der Standard-ENIGMA hatten nur jeweils eine Nut, so daß eine zyklometrische Bewegung der Rotoren entstand. Der so erzeugte Algorithmus war kryptologisch schwach, und daran änderte sich auch nichts Wesentliches, als 1938 zwei weitere Walzen hinzu kamen, so daß dann jeweils 3 aus 5 auszuwählen waren, mit Verzehnfachung der möglichen Walzenlagen.

Die Marine erhöhte bereits 1936 die Walzenzahl auf sechs (M 1), dann sieben (M 2) und schließlich acht (M 3), bis sie 1942 eine eigene Variante M 4 einführte (s. unter 3.2.2 /M 4).

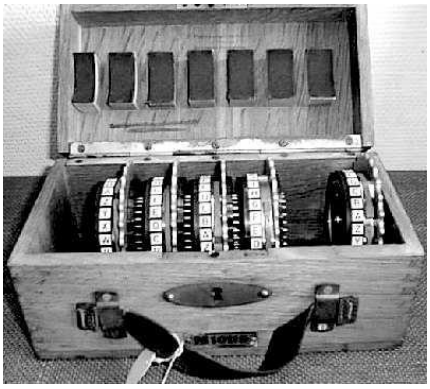


Bild 13: Walzenbox einer Marine-ENIGMA M4

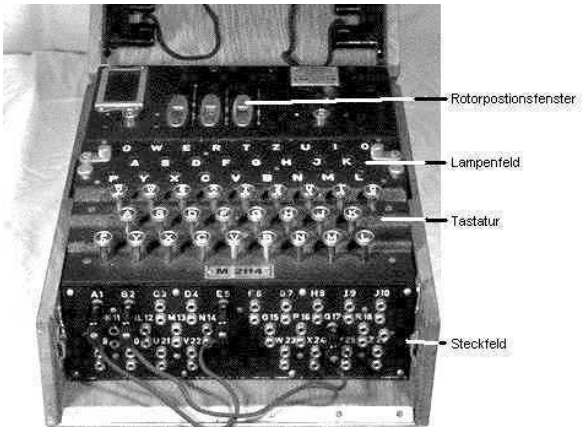


Bild 14: ENIGMA I (1938)[74]

Für die maximal möglichen Schlüsseleinstellungen der ENIGMA I, die sog. Periode, gibt es erstaunlich unterschiedliche Angaben: So bspw. $1{,}5 \times 10^{19}$ (SALE[75]), $4{,}03 \times 10^{17}$ (HODGES[76]), $1{,}074 \times 10^{23}$ (ERSKINE[77]), $1{,}59 \times 10^{20}$ (SINGH[78]), und die FH Hamburg[79] kommt mit einer theoretischen Berechnung gar auf $2{,}79 \times 10^{24}$. Diese großen Unterschiede sind die Folge unterschiedlicher theoretischer Ansätze, welche die kryptologischen Besonderheiten der Maschine mehr oder weniger, oder überhaupt nicht (FH Hamburg) einbeziehen. Besonders beachtete man dabei nicht, daß viele Einstellungen identisch bzw. quasi-identisch sind, und somit keine echte neue Verschlüsselung bewirken. Da überdies ein Buchstabe nicht mit sich selbst verschlüsselt werden kann, reduziert das die echte Schlüsselzahl weiter. Vermutlich aus diesem Grund geben wirkliche Experten keine Zahlen zur Schlüsselperiode der ENIGMA an.

---

[74] Bilder nach Universität Hamburg – Informatik: Die ENIGMA .

[75] Sale, Codes and Ciphers, The ENIGMA , Page 3. The complexity of the ENIGMA-machine.

[76] Hodges, Turing, S. 178

[77] Erskine, Ralph: ENIGMA's Security. In: Erskine, Ralph and Smith, Michael (Eds.): Action this Day. Bantam Press, London u.a. Orte, 2001, S. 372. (Zukünftig zit.: "In : Erskine/Smith, Action ").

[78] Singh, Simon: Geheime Botschaften, München 2000, S. 210-213. (Orig. „The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography", London 1999). S. 212.

[79] Zenker, Uwe: Kurzinformation über die wichtigsten Daten der ENIGMA I. Juni 1996. Von: http://users.informatik.fh-hamburg.de/~voeller/krypto/html/enigma/ENIGMA_uwe.htm, am 21.8.99.

Ein weiteres Detail dazu: Die Walzenbewegung erfolgte nicht rein zyklometrisch, bedingt durch einen konstruktiven Mangel der Fortschaltung, so daß die mittlere Walze einen Extraschritt weiterbewegt wurde, wenn sich die linke Walze bewegte. Dadurch erzeugte die ENIGMA nicht die theoretisch möglichen, in vielen Analysen angesetzten 26^3 Permutationen, sondern nur 26x25x26, also um den Faktor 26 vermindert.[80]
Doch das spielte bei der Beurteilung der realen Sicherheit der ENIGMA ohnehin nur eine geringe Rolle, denn die großen Zahlen suggerierten eine Sicherheit, die nicht wirklich vorhanden war. Denn wenn man, eigentlich selbstverständlich, nach kryptanalytischen Kriterien die Maschine als System beurteilt, kommt man zu ganz anderen Ergebnissen. Genau das aber hielten die Militärs wohl für entbehrlich bzw. wußten nicht, daß es kryptanalytische Methoden zur Brechung gibt. So ließen sie sich wahrscheinlich von diesen theoretischen großen Schlüsselzahlen beeindrucken, als sie die ENIGMA I einführten. Ob sie dabei erfahrene Kryptologen konsultierten, und gar deren Meinung berücksichtigten, ist sehr unwahrscheinlich: Dokumente[81] bestätigen, daß mindestens bis 1942 keine kryptologischen Prüfungen erfolgten, und auch danach blieben die militärischen Waffenämter zuständig.

ENIGMA I mit Umkehrwalze D

Im Verlauf des Krieges zweifelten erfahrene Offiziere die Chiffriersicherheit der ENIGMA I immer wieder an, denn der Gegner verfügte offenkundig über exzellente Informationen. Doch stets machte man dafür Verräter oder Spionage verantwortlich. Gleichwohl versuchte man mit einigen Änderungen die Sicherheit der ENIGMA zu verbessern – einer Maschine, die offiziell sicher war – woraus man folgern kann, daß die Verantwortlichen deren Sicherheit ebenfalls bezweifelten, das aber nicht offen zugestehen konnten (s. hierzu 5.4.4).

Eine kryptologisch wirksame Verbesserung erreichte man erstmals mit einer durch Steckverbindungen schaltbaren neuen „Umkehrwalze D“ (UKD), die ab Januar 1944 in einigen Luftwaffenschlüsseln verwendet wurde, um eine erwähnte Schwäche der ENIGMA I – die feste Umkehrwalze – zu vermeiden. Diese UKD ersetzte die Standardumkehrwalze B, war dazu auf deren Abmessungen abgestimmt, und wurde ebenso auf die jeweilige Position gesetzt. Doch vorher änderte man mit Steckern die Zuordnung der Buchstaben auf der Kontaktplatte; diese Schaltung wechselte alle 10 Tage. Darüber hinaus wurde zweimal täglich zu bestimmten Zeiten je eine Steckverbindung des äußeren Steckerfeldes gewechselt.

[80] Ausf. beschrieben in Hamer, D.H.: Enigma: Actions involved in the „double stepping“ of the middle rotor. In: Cryptologia; Volume XXI (1); Jan 1997.

[81] Bericht über das Chiffrierwesen in OKW/Chi, nach dem Krieg angefertigt.
Vertrauliches Dokument der Zentralstelle für das Chiffrierwesen der BRD –Nur für den Dienstgebrauch--. Aus der Sammlung Staritz.

Bild 15: Enigma-Umkehrwalze D[82]

Kontaktplatte herausgenommen

Diese Verbesserungen verhinderten zunächst Entzifferungen in BP. Nach kryptanalytischen Studien entwickelte man ein Verfahren zur Handentzifferung („Duenna"), das sich auch für maschinelle Verarbeitung eignete. Doch hierzu benötigte man sehr lange Klartextfragmente mit 10-facher Länge, verglichen mit denen der Standard-ENIGMA, und mußte viel Personal einsetzen, das nun anderswo fehlte. Und man hatte noch Glück: Viele Nachrichten wurden *re-enciphered*, d.h. wortgleich in anderen Schlüsselkreisen erneut chiffriert und gesendet, die nicht über UKD-ENIGMAs verfügten, sondern nur über ENIGMA I-Maschinen. Diese Texte las man in BP regelmäßig mit und konnte so per Klartext-Geheimtext-Kompromittierung Einbrüche in die Verschlüsselung durch UKD-ENIGMAs erzielen. Dann erbeutete man im Juli 1944 eine Schlüsselanweisung und konnte damit die UKD und deren Betriebsweise rekonstruieren.[83]

ENIGMA I mit Steckeruhr

Ab 10. Juli 1944 konnte man in BP bei routinemäßiger Entzifferung einiger Luftwaffenschlüssel überraschend nur noch eine zweistellige Zahl lesen. Alle Versuche brachten kein anderes Ergebnis und man mußte ein unbekanntes Gerät oder Zubehör annehmen. Das bestätigte sich, denn ab diesem Tag kam die „Steckeruhr" (*Uhr-Box*) mit einigen Exemplaren zum Fronteinsatz, dann häufiger ab August 1944.
Auch hier half BP die Gewohnheit deutscher Nachrichtenoffiziere, analog zur UKD manche Nachrichten *re-enciphered* an mehrere Schlüsselkreise zu senden, die

[82] Bild nach W1TP Telegraph & Scientific Instrument Museums.
Von: http://www.chss.montclair.edu/~pererat/u_108.jpg, am 10.10.03.
[83] Vgl. Ulbricht, Heinz: Uncle Dick and another Horrors of the Enigma. In: The Journal of Intelligence History, Vol 1 (1), Summer 2001, S. 45-47.

nur über Standard-ENIGMA I-Maschinen verfügten. So konnte BP durch Kompromittierung dieser Sendungen die Arbeitsweise der Steckeruhr rekonstruieren, die BOMBE-Maschinen entsprechend umrüsten, und wieder entziffern.[84]

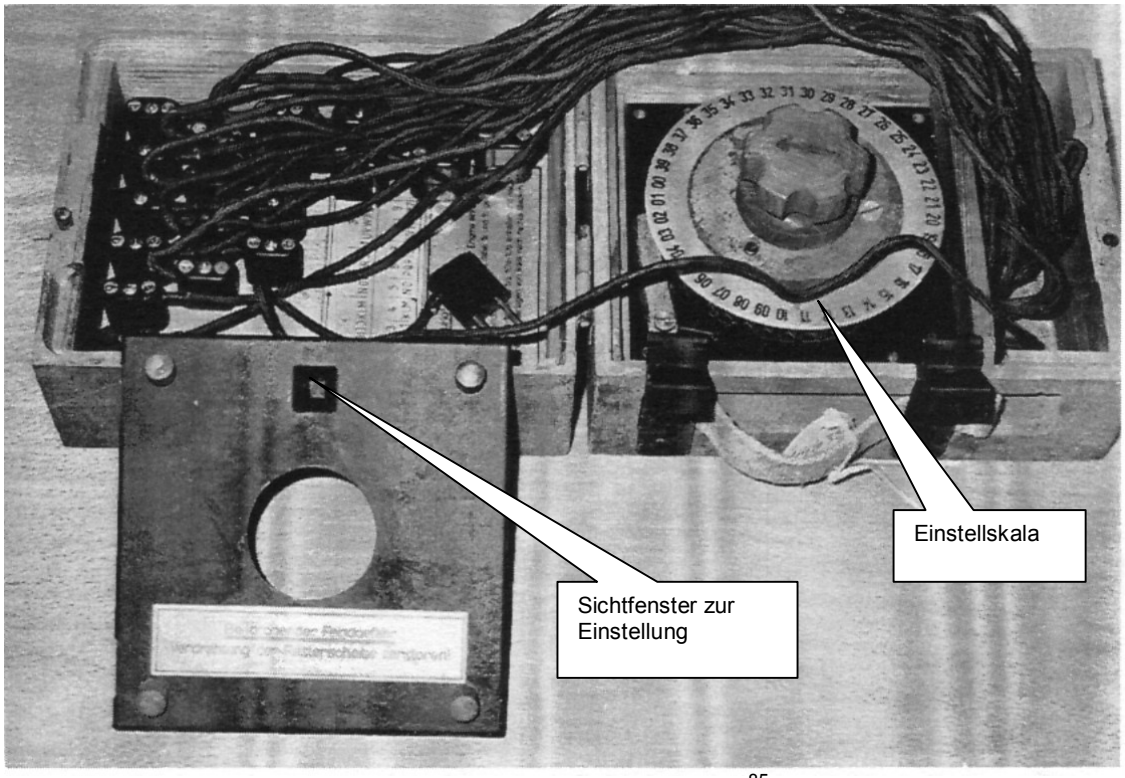


Bild 16: "Steckeruhr" zur ENIGMA I[85]
[Abdeckung der Einstellskala geöffnet]

Die Steckeruhr wurde in die Steckverbindungen der ENIGMA I eingeschleift und vertauschte so die Zuordnungen der gesteckerten Buchstaben. Das geschah durch Drehen des Mehrfach-Umschalters mit einer numerierten Einstellskala. Diese Einstellung mußte jeweils zu Beginn einer Sendung und vor der Drehung des Umschalters vereinbart werden, quasi als zusätzlicher Spruchschlüssel. Es war die erwähnte zweistellige Zahl.
Die Uhr hob die Reziprozität der ENIGMA auf und war damit ein kryptologisch wirksames Mittel, das die Entzifferungen sehr erschwerte. Allerdings verwendete die Wehrmacht nur kleine Stückzahlen, analog zur Umkehrwalze D.

ENIGMA M3

Die Marine war sicherheitsbewußter und erhöhte bei ihrer Version ENIGMA M die Anzahl der auswechselbaren Walzen der ENIGMA I nacheinander von fünf/sechs (M 1/2) auf acht (M3 in 1939), wodurch statt bisher 60 Rotorlagen nun 336 zu untersuchen waren. Diese drei zusätzlichen Walzen konnten die

[84] Vgl. Ulbricht, Heinz: Uncle Dick and another Horrors of the Enigma. S.49-52.
[85] Bild nach Ulbricht, Heinz: The Enigma-Uhr. In: Skillen, Hugh (Ed.): The Enigma Symposium 2000.

polnischen Kryptologen vor der Besetzung Polens nicht mehr rekonstruieren. Die Entzifferung von Marinesendungen war daher in BP zunächst nicht möglich, was das britische Kriegskabinett angesichts des verlustreichen U-Boot-Kriegs veranlaßte, die Beschaffung dieser Walzen und der ebenso wichtigen fehlenden Geheimunterlagen durch Kaperungen deutscher Schiffe anzuordnen (s. 5.2.3).

ENIGMA M4

Zum Februar 1942 wurde für U-Boote die ENIGMA M4 eingeführt, mit einem zusätzlichen 4. Chiffrierrotor („Griechenwalze" β, später γ), der den rechten Teil der Umkehrwalze B darstellte, der linke wurde entsprechend als „Umkehrwalze B dünn" bezeichnet. Diese gespaltene Anordnung wählte man, um die Breite der Maschine nicht ändern zu müssen; die vorhandenen Maschinen sollten weiterbenutzt werden. Der Nachteil dieser Lösung: Die Griechenwalze konnte nur in 26 Stellungen fest eingestellt und danach nicht mitbewegt werden, sie war auch nicht mit den anderen Walzen austauschbar. Mit dieser Konstruktion verzichtete man aber auf die größere Sicherheit einer echten Vierrotormaschine: Nach ERSKINE entsprach so die Zahl der zu prüfenden Walzenlagen denen einer M3-Maschine, nämlich 336, anstatt der 3024 möglichen bei einer echten Vierrotormaschine.[86]

Doch diese Maschine verhinderte Entzifferungen bis zum 13. Dezember 1942, die danach erst wieder möglich wurden, nachdem die erforderlichen Geheimunterlagen „beschafft" waren. Und zur ausreichend schnellen Entzifferung mußte BP noch BOMBE-Geräte mit vier Rotoren zur Ermittlung der jeweiligen Schlüsseleinstellungen entwickeln.

Schlüsselgerät 39

Die Maschine entwickelte die Firma Telefonbau & Normaluhr (T&N) in Zusammenarbeit mit dem Heereswaffenamt (WA Prüf 7). Ein Prototyp wurde 1939 vorgestellt, jedoch wegen angeblich mangelnder Serienreife vom Waffenamt nicht akzeptiert, obwohl es ein – verglichen mit der ENIGMA I – weit sichereres Gerät war: U.a. erzeugten drei Antriebsräder mit setzbaren Stiften an den Schlüsselwalzen eine pseudo-irreguläre Bewegung.[87]

Weitere Einzelheiten enthält ein erst 2003 publizierter NSA-Bericht. Danach soll das Gerät vom OKW/Chi-Mitarbeiter MENZER erfunden (*invented*) worden sein, eine Feststellung, die (auch für andere Geräte) unter 3.3.2 widerlegt wurde. Es sei eine elektrisch angetriebene, automatisch arbeitende Maschine gewesen, mit drei irregulär bewegten Chiffrierrotoren, und darüber hinaus mit je einem Steckerfeld zur Permutierung des Rotorein- und -ausgangs. Das Gerät verfügte über Tastatur, Drucker für Klar-und Geheimtext und einer Vorrichtung zur Umsetzung in den

[86] Vgl. Erskine, Ralph: ENIGMA's Security. S. 10.
[87] Neu- und Weiterentwicklung technischer Schlüsselmittel, Stand Januar 1944. TICOM-Dok.

Fernschreibcode. So konnte die Maschine auch mit einem Lochbandstanzer für Fernschreibsendungen gekoppelt werden, denn es sei für später geplant gewesen, damit die Fernschreib-Schlüsselmaschinen T52d und T52e zu ersetzen.[88]
Nach ERSKINE hätten die Alliierten diese Maschine nicht brechen können.[89]

Erst 1943 kam man wieder auf diese Konstruktion zurück, wohl nachdem man einräumen mußte, „daß [damit] alle z.Zt. bekannten Verfahren auch der maschinellen Entzifferung ... hierdurch ausmanövriert [sind]“ – eine indirekte Bestätigung dafür, daß Eingeweihte über die problematische Sicherheit der ENIGMA vermutlich informiert waren (s.u.). Doch die Herstellerfirma forderte – kriegsbedingt – ca. drei Jahre Anlaufzeit bis zur Serienproduktion. Dementsprechend stornierte das Waffenamt dieses Projekt, forderte aber dessen wesentliche Elemente für die geplanten neuen ENIGMA-Versionen M5 und M10 zu verwenden (s.u.).[90]
Dazu kam es aus unbekannten Gründen nicht, aber dafür lebte das Projekt im Sommer 1944 wieder auf: Am 6. Juli 1944 vereinbarte man bei OKW/GBN[91] einen Arbeitskreis aus den Firmen T & N, Wanderer-Werken und Olympia für die Herstellung des Schlüsselgerätes 39. Bis Ende 1944 sollten 10 Mustergeräte für Feldversuche zur Verfügung stehen, und die Serienproduktion mit monatlich 900 Geräten war ab September 1945 vorgesehen.[92]
Das wurde wieder relativiert, nachdem nach dem 20. Juli 1944 die SS die Kontrolle über das Chiffrierwesen allmählich erlangte:
Zwar bestätigte der „Rf SS Chef FMW“[93] den Auftrag zum Bau der Mustergeräte, doch nur „ ... um, insoweit eine Entzifferungsmöglichkeit des Gegners gegeben ist, durch [dann] angeordnete Serienfertigung von SG 39 diese Möglichkeit auszuschalten.“[94]
Mithin rechnete die SS nicht mit ENIGMA-Entzifferungen, vermutlich weil sie – verständlicherweise – nicht über die wahren Verhältnisse informiert wurde.

ENIGMA M5 und M10

Die ENIGMA M5/10 wurde offiziell nur „weiterentwickelt“ auf der Basis des vorerwähnten Schlüsselgerätes 39 und der ENIGMA M4, doch war sie eine „vollständige Neukonstruktion“, die für alle Wehrmachtsteile gleichermaßen verwendet werden sollte: Der setzbare Schlüsselradantrieb des SG39 sollte mit einer Novität kombiniert werden, einer sog. „Wahllückenwalze“, auch „Lückenfüllerwalze“ genannt. Und diese Neukonstruktion „ ... erlaubt es, an jeder Walze Schaltlücken beliebig nach Art und Zahl einzustellen.“ Diese Walzen

[88] Vgl. Mowry, David P.: German Cipher Machines of World War II, Center for Cryptologic History, National Security Agency 2003. S. 21-25.
[89] Vgl. Erskine, Ralph: ENIGMA's Security. In : Erskine/Smith, Action, S. 384.
[90] Neu- und Weiterentwicklung technischer Schlüsselmittel.
[91] GBN = Generalbevollmächtigter für Nachrichtenwesen; zu dieser Zeit noch Fellgiebel.
[92] StAC, Bestand 31030, Nr. 2846. Bericht vom 8.7.1944.
[93] Reichsführer SS, Chef Fernmeldewesen.
[94] StAC, Bestand 31030, Nr. 2846. Interne Mitteilung der Wanderer-Werke vom 23.9.1944.

könnten darüberhinaus in den „alten“ ENIGMA-Maschinen die vorhandenen Walzensätze ergänzen. Zusätzlich sollte die 4. Walze der ENIGMA M4 zu einer echten Rotorwalze aufgewertet werden; darüber hinaus waren 12 Tauschwalzen vorgesehen, so daß dann 23.760 Walzenlagen gegenüber 1.344 der ENIGMA M4 möglich wären.[95]

Die beiden Varianten unterschieden sich nur durch Druckvorrichtungen, die für die M10 geplant waren.
Es ist nicht bekannt, ob Prototypen oder wesentliche Teile dieser kryptologisch sehr starken Maschine existierten, jedoch sollen sich klassifizierte Dokumente darüber in alliierten Besitz befinden.

ENIGMA T („Tirpitz“)

Zur Kommunikation zwischen deutschen und japanischen Marinestellen und Schiffen ließ das Marine-Waffenamt 1942 eine spezielle ENIGMA-Version entwickeln, die ENIGMA T. Um diese sog. „Tirpitz-Maschine“ ranken sich zahlreiche Legenden, weil nach der Invasion die US-Truppen etwa 70 Maschinen in einem Lager an der französischen Westküste fanden, die dort zum Verschiffen per U-Boot nach Japan bereit lagen, und niemand darüber Bescheid wußte.
Die Forschung konnte jedoch inzwischen den Sachverhalt klären:[96] Gemäß deutsch-japanischem Marineabkommen vom 11. September 1942 wurde maschinelle Chiffrierung vereinbart, wofür die ENIGMA T exklusiv vorgesehen war. Davon gab es zwei Versionen: Zunächst eine ENIGMA T ohne Steckerfeld, deren erste Lieferung im August 1942 belegt ist. Im November 1943 informierte die deutsche Marine die Japaner über Sicherheitsbedenken bei längeren Texten, so daß die Maschine durch eine verbesserte Version ersetzt werden soll. Nach Beschwerden des japanischen Marineattachés, nun würden die vorhandenen Maschinen wertlos, wurde ihm versichert, daß die neue zur alten Maschine kompatibel sein werde. Diese im deutsch-japanischen Schriftverkehr so bezeichnete „02561-A-ENIGMA“ war mit einem Steckerfeld wie die ENIGMA I ausgerüstet, und – zur Kompatibilität – mit den speziellen Walzen der ENIGMA T, und damit auch mit deren 5 Nocken. Die Lieferungen per U-Boot begannen 1944; ab März 1944 wurden damit verschlüsselte Sendungen von der US-Navy erstmals identifiziert.

Die erwähnten 70 gefundenen ENIGMA T-Maschinen gehörten noch zur älteren Version. [Vermutlich wurden sie gelagert, weil die Japaner daran freilich kein Interesse mehr hatten].

---

[95] Neu- und Weiterentwicklung technischer Schlüsselmittel. Stand Januar 1944. TICOM-Dokument. Allerdings wären die 1344 Walzenlagen der M4 nur mit einer (geplanten) rotierenden 4.Walze zu erreichen gewesen.

[96] Vgl. Weierud, Frode: Tirpitz and the Japanese-German Naval War Communikation Agreement. In: Cryptologia, Vol 20, No. 3, Summer 1999, p 610.
Von: http://mad.home.cern.ch/frode/crypto/tirpitz.htm, am 14.01.03.

Die ENIGMA T unterschied sich von den Standardmaschinen in mehreren Punkten: Sie enthielt drei Walzen mit setzbarer Umkehrwalze, aus acht auszuwählen, hatte jedoch kein Steckerbrett. Diese scheinbare Schwäche kompensierte man durch speziell verdrahtete Walzen mit 5 Nocken, die quasi-irreguläre Bewegungen der Walzen erzeugten. Eine weitere Komplikation bewirkte der Eingangsstator: Entgegen der Standard-ENIGMA waren die Buchstaben nicht alphabetisch angeordnet, sondern permutiert. Dazu kam eine Tastatur mit den Zahlen 0-9, wozu die oberste Tastenreihe umschaltbar war.
Die pseudo-irregulären Walzenbewegungen hätten, zusammen mit dem permutierten Stator, die gesamte maschinelle Ausrüstung der Alliierten zur Brechung obsolet gemacht: Neue Verfahren wären zu entwickeln gewesen und das hätte viel Zeit beansprucht.[97] Mithin waren die erwähnten Sicherheitsbedenken nicht nur unberechtigt, vielmehr hätte die Maschine eine bessere Schlüsselsicherheit geboten.
Warum die deutschen Verantwortlichen, die Marine-Nachrichtenoffiziere, diese kryptologischen Stärken nicht sahen, wurde unter 5.4.3 mit deren mangelnden Sachverstand begründet. Für diese Annahme spricht auch die unnötige Ersetzung der ENIGMA T durch die A-ENIGMA.

3.2.3 sonstige ENIGMA–Versionen

Reichsbahn-ENIGMA

Die kommerzielle ENIGMA D fand später eine neue Verwendung, freilich – bei sonst gleicher Bauweise – mit neu verdrahteten Walzen: In BP registrierte man erstmals am 15. Juli 1940 Sendungen, die offenbar Bahn-Transportmeldungen betrafen. Die zugehörige unbekannte Chiffriermaschine nannte man folgerichtig „*Railway*-ENIGMA“, und dieser neue Schlüsselkreis erhielt die Tarnbezeichnung ROCKET I.[98]
Diese modifizierte ENIGMA D setzte die Reichsbahn ein in den besetzten Gebieten Osteuropas und dem Balkan, in denen es durchgehende Nachrichtenverbindungen nicht gab. Demzufolge mußte die Bahn ihre Transporte per Funk organisieren und diese Meldungen verschlüsseln.
In BP konnte man die Maschine vermutlich leicht lösen, weil genügend Material vorlag das mit gleicher Schlüsseleinstellung chiffriert war. Mit diesen *depths* gelangen die Entzifferungen mit den klassischen Methoden der Kompromittierung.[99]
Die daraus gewonnenen Informationen scheinen sehr wichtig gewesen zu sein: “*The intelligence obtained from ‚Rocket‘* [I] *traffic is of first-grade importance since it gives long-term information as to production and movement of supplies*.”[100]

---

[97] Vgl. Ebd.
[98] Vgl. Hamer, D.H., Sullivan, G., Weierud, F.: Enigma Variations. An Extended Family of Machines. In: Cryptologia; Volume XXII (3); July 1998; pp. 211-229.
[99] Vgl. Bauer, Geheimnisse, S. 378.
[100] US-Army-Kryptologe W. Friedman in: The report on his visit to GC & CS [Bletchley Park] in the period 25 April - 13 June 1943.

Im September 1942 registrierte BP eine neue Variante an der Westfront, genannt ROCKET II. Doch diese Chiffrierung widerstand allen Entzifferungsversuchen, wofür man keine Erklärung fand, und man konnte nicht einmal ermitteln, ob die gleiche Maschine wie für ROCKET I benutzt wurde. Im Mai 1944 kam eine weitere Variante „ROCKET III“ hinzu, die ebenfalls den Entzifferungsversuchen widerstand.
Nach dem Krieg stellte sich heraus, daß die Reichsbahn in westlichen Gebieten eine Standard-ENIGMA I nutzte, und diese sogar ohne jeden Walzenwechsel. Entzifferungen wären deshalb mit geringem Aufwand möglich gewesen, doch man scheiterte wegen der fehlenden Wortsequenzen (*cribs)*, die man aus Transportmeldungen nicht gewinnen konnte.[101] Und *depths* standen vermutlich auch nicht zur Verfügung, weil die Chiffrierdisziplin dort besser war.

Abwehr-ENIGMA

Die Abwehr setzte verschiedene ENIGMA-Maschinen in ihren Hauptstellen ein, darunter nach den Untersuchungen in BP zwei Versionen der ENIGMA K, mit jeweils unterschiedlicher Verdrahtung der Walzen. Als dritte Maschine identifizierte BP eine Standard-3-Walzen-ENIGMA mit Steckerbrett, wobei die Abwehr jedoch nur die Walzen I, II u.III nutzte, ohne jeden Wechsel.[102]

Schließlich identifizierte BP eine vierte, noch ältere frühere kommerzielle Version von 1926, genannt „Zählwerks-ENIGMA“, die frei verkäuflich war, wie erhaltene Angebote belegen.[103] Diese Maschine, mit neu verdrahteten Walzen, setzte die Abwehr besonders oft ein, und sie wird daher in der Literatur als „Abwehr-ENIGMA“ bezeichnet. Zur Unterscheidung zu anderen Versionen ist auch die Bezeichnung *multi-turnover machine* oder, nach der Nockenanzahl, *11-15-17-machine* gebräuchlich.

Die kryptologisch relevanten Teile der Maschine waren eine mitrotierende Umkehrwalze und drei untereinander austauschbare Mehrfachnocken-Walzen. Die zahlreichen Nocken erzeugten pseudozufällige Schrittbewegungen, deren vermeintliche Sicherheit vermutlich die Verantwortlichen überzeugten. Dementsprechend setzte die Abwehr sie in ihren Hauptstellen ein, und dort auch für die Weiterleitung der mit verschiedenen Handverfahren verschlüsselten Agentenmeldungen (das in BP beliebte *re-enciphering*). Als dann im Krieg viel mit der Maschine verschlüsseltes Material abgehört wurde, hatten die Kryptologen in BP vermutlich wenig Mühe, die Walzen der gut bekannten, weil früher frei verkäuflichen Maschine zu rekonstruieren, was bereits 1941 gelang.

---

[101] Vgl. Hamer et al.: Enigma Variations.
[102] Hamer, Sullivan, Weierud: Enigma Variations. An Extended Family of Machines. In: Cryptologia; Volume XXII (3); July 1998; pp. 211-229.
[103] Angebot Chiffriermaschinen AG, Berlin vom 16.9.1929. Sammlung Staritz.

Den ersten Einbruch erzielten die Analytiker durch eine Analyse des Spruchschlüsselverfahrens: Es bestand aus acht Buchstaben, die, wie man überrascht feststellte, die doppelt gesendeten vier Wahlstellungen der Walzen waren, eine alte Methode also, die bei der Vorkriegs-ENIGMA bis 1938 verwendet und von polnischen Kryptologen bereits ab 1932 zur Entzifferung genutzt wurde. Überdies erleichterten die Operatoren den Entzifferern in BP die Arbeit durch zahlreiche Fehler, besonders durch Verwendung stereotyper Buchstaben-Kombinationen, und durch *re-encipherings*.[104]

Die Verwendung des alten Spruchschlüsselverfahrens, vor allem aber die häufigen *re-encipherings,* deuten auf sehr mangelhafte kryptologische Kenntnisse und der dadurch fehlenden Überwachung der Chiffriersicherheit. Dazu bemerkte der frühere Abwehr-Mitarbeiter STARITZ: In der Abwehr gab es generell wenig kryptologischen Sachverstand, niemand beschäftigte sich mit der Chiffriersicherheit. Es blieb den Mitarbeitern überlassen, welche Chiffrierverfahren sie verwendeten.[105] Und für die Chiffriermaschinen war ohnehin das technikorientierte Heereswaffenamt zuständig.

Auch Militärattachés verwendeten die Abwehr-ENIGMA, allerdings nur bis 1943, weil deren Schwäche von OKW-Kryptologen erkannt worden war. Die Maschinen wurden daraufhin der Abwehr angeboten, vermutlich ohne den wahren Grund des Angebotes zu nennen.[106] Es ist nicht bekannt, doch sehr wahrscheinlich, daß die Abwehr diese Maschinen übernahm, denn es war deren Standardmaschine, und sie blieb weiter im Einsatz.

Diese Maschine hatte mit den verschiedenen ENIGMA-Versionen wenig gemein, und war wegen der vielen anders konstruierten Bauteile fast ein eigenständiges Gerät. Völlig anders war bspw. der Antrieb der Walzen ausgelegt:

[104] Vgl. Carter, Frank: The Abwehr Enigma Machine.
Von www.bletchleypark.org.uk/abwehr.pdf, am 15.9.03.
[105] Staritz, Korrespondenz mit dem Verf. (u.v.).
[106] TICOM I-77: Homework by Dr. Huettenhain and Dr. Fricke on Zaehlwerk (cyclometer) – Enigma. Ref. G5/80 – 1st Aug. 1945. POW/Kew (GB).

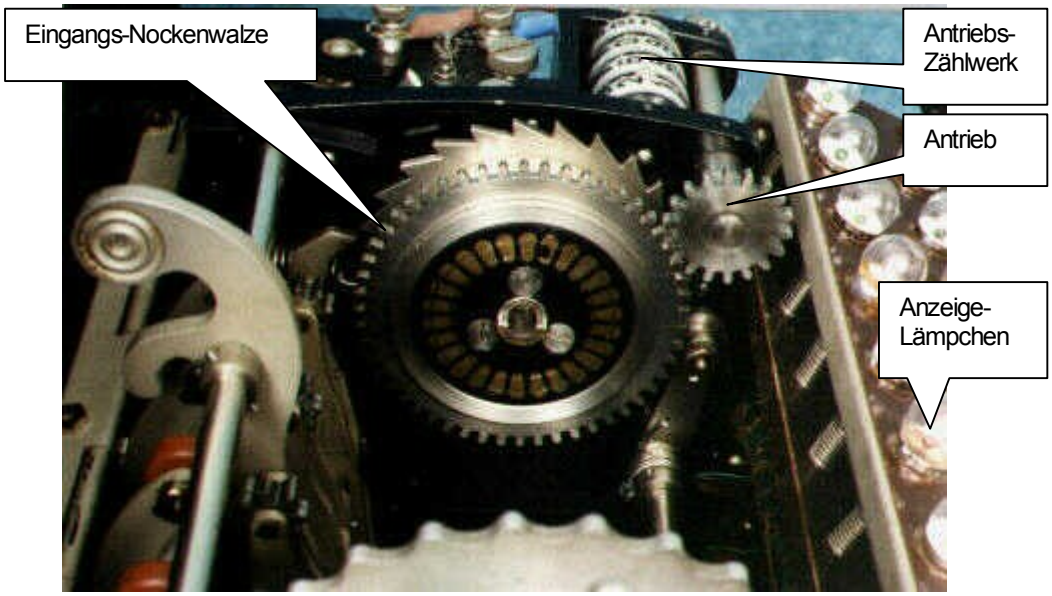


Bild 17: Schlüsselradantrieb der Abwehr-ENIGMA[107]

Die anders verdrahteten und, verglichen mit der ENIGMA I, kleineren Walzen wurden zwar gleichmäßig angetrieben, doch waren sie mit Nocken versehen, die als Primzahlen (11-15-17) ungleichmäßig auf den Walzen verteilt waren und so den gleichmäßigen Zahnradantrieb in eine pseudo-unregelmäßige Schrittbewegung wandelten. Der Antrieb ermöglichte sogar eine Rückwärtsbewegung: Man konnte bei Tippfehlern zurückkurbeln bis zum Fehler; es mußte nicht mehr alles neu eingetippt werden. Ein Zählwerk kontrollierte die Eingabe und das Rückwärtskurbeln.

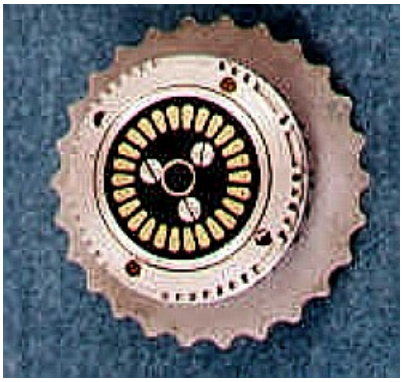


Bild 18: Primzahl-Nocken auf einer Walze[108]

Es war eine echte 4-Walzen-Maschine, d.h. die Umkehrwalze rotierte mit den anderen Walzen, im Gegensatz zur ENIGMA M4, die nur eine setzbare vierte Walze besaß, die nicht mitbewegt wurde.

[107] Bild nach Hamer, D.H.: G-312: An Abwehr Enigma.
In: Cryptologia; Volume XXIV (1); Jan 2000; pp. 41-54.
[108] Bild nach Hamer, D.H.: G-312: An Abwehr Enigma.

KD-ENIGMA

Im Herbst 1944 registrierten die Alliierten eine neue Abwehr-ENIGMA, die sie „KD-ENIGMA“ nannten, eine Variante der ENIGMA K: Diese Maschine hatte kein Steckerfeld, sondern wurde aufgerüstet mit der von der ENIGMA I bekannten schaltbaren Umkehrwalze D. Der Walzensatz bestand aus sechs mit je 9 Nocken versehenen Walzen, von denen drei täglich gewählt wurden.

Diese kryptologisch wesentlich stärkere Maschine identifizierte BP auf der Funklinie Berlin-Madrid-Lissabon. Diese wurde betrieben von der SS-Nachfolgeorganisation der Abwehr, dem „Amt Mil“ des SS-Reichssicherheitshauptamtes.[109] Andere Verwendungen sind nicht bekannt.

[109] Vgl. Hamer, D.H., Sullivan, G., Weierud, F.: Enigma Variations. An Extended Family of Machines. In: Cryptologia; Volume XXII (3); July 1998; pp. 211-229.

3.2.4 ENIGMA-Übersicht

Jahr der Einführung	Version	Bemerkungen
1923	ENIGMA A	Chiffrierschreibmaschine mit 4 hintereinandergeschalteten Rotorwalzen, mittels Schlüsselrädern gleichmäßig bewegt.
1924	ENIGMA B	wie ENIGMA A, jedoch kleiner und leichter
1926	ENIGMA C	Kein Schreibsystem mehr – nur Lampenanzeige je Buchstabe, um das Gewicht zu verringern (für Militäranwendungen). Nur 3 Rotoren, mit Umkehrwalze - mit gleicher Einstellung konnte nun chiffriert und dechiffriert werden. Mitnehmernocken auf den Rotorwalzen ersetzten die Schlüsselräder.
1926	ENIGMA C (mod.)	„Funkschlüssel C“ der Reichsmarine, mit anderer Tastatur und neu verdrahteten Walzen.
1926	Zählwerks-ENIGMA	Sondermodell mit kleineren Nockenwalzen, Zahnradantrieb, setzbarer Umkehrwalze, Buchstaben-Zählwerk, rückwärts schaltbar.
1927	ENIGMA D	Erstmals mit Austauschwalzen, viel verkaufte kommerzielle Maschine, bes. auch an Dienste anderer Staaten. Entsprechend viele Nachbauten.
1927-29	ENIGMA E /F /G /H	Versuchsmuster. Heereserprobung ENIGMA G, ENIGMA H erstmals mit Steckerbrett.
1930	ENIGMA I	Wie ENIGMA G, mit fester Umkehrwalze.
1932	ENIGMA II	Wie vor, mit Drucker. Nur wenige Exemplare im Einsatz.
1934	ENIGMA I	Gemeinsames Modell aller Teilstreitkräfte mit 3 Walzen aus 5 wählbar; Heer sperrte aber die 2 Zusatzwalzen. Setzbare Umkehrwalze A.
1936 (?)	Abwehr-ENIGMA	Wie Zählwerks-ENIGMA, jedoch Umkehrwalze rotierend, Walzen neu verdrahted.
1934-39	ENIGMA M1/2/3	Marineversion mit 3 Walzen aus 6 wählbar (M1), aus 7 (M2 1938), dann aus 8 (M3 1939).
1937	ENIGMA I	Weltkriegsmodell mit setzbarer Umkehrwalze B
1938	ENIGMA K (Swiss-K)	Wie ENIGMA D, wurde an Japan geliefert. Lieferung auch an die Schweiz, dort wurden alle Rotoren neu verdrahted (Swiss-K), und 1941 die Walzen-bewegungen verändert.
1938/39	ENIGMA I (Mob.1/2)	Wie vor, 1./2. Zusatzwalze vom Heer freigegeben
1939	Schlüsselgerät 39	ENIGMA-Konkurrenzmodell von T & N Frankfurt/M. Kryptologisch wesentlich stärker durch irregulären Schlüsselradantrieb usw.. Wegen angeblich fehlender Serienreife jedoch abgelehnt.
1940	Reichsbahn-ENIGMA	Wie ENIGMA D, mit setzbarer Umkehrwalze B. Ab 1942 auch ENIGMA I mit 3 Walzen ohne Wechsel.

Jahr der Einführung	Version	Bemerkungen
1942	ENIGMA T	„Tirpitz“-Maschine für Kommunikation mit jap. Marine. Ohne Steckerfeld, dafür mit vier Walzen und je fünf Nocken je Walze.
1942	ENIGMA M4	Für U-Boote mit zusätzlichen neuen Walzen β,γ, sog. „Griechenwalzen“, die nacheinander freige-geben wurden, aber nicht rotierten. „Dünne“ UKW.
1943	ENIGMA I-UKD	ENIGMA I mit schaltbarer Umkehrwalze D. Weiteres (z.T. früheres) Zubehör: Steckeruhr, Schreibvorrichtung, sep. Ablesevorrichtung etc.
1943	A-ENIGMA	Verbesserte Version der ENIGMA T, mit Steckerfeld. Kam 1944 zum Einsatz mit jap. Marine.
1943	ENIGMA M5	Neukonstruktion für alle Wehrmachtsteile, eine verbesserte M4 mit Teilen des „Schlüsselgerätes 39“. Sollte ab Sommer 1945 geliefert werden.
1943	ENIGMA M10	Wie M5, jedoch mit Streifenschreibern für Klar- und Geheimtext.
1944	KD-ENIGMA	Wie ENIGMA K, mit schaltbarer Umkehrwalze D, 6 Walzen mit je 9 Nocken (neu verdrahted). Eingesetzt vom Amt Mil (Nachfolger Abwehr).
1945	Norway-ENIGMA	Wie ENIGMA I, mit nach dem Krieg in Norwegen neu verdrahteten Rotoren.

3.2.5 Enigma-orientierte Chiffriermaschinen

Die nachstehend beschriebenen Maschinen von DAMM/HAGELIN waren zwar keine eigentlichen Rotormaschinen im Vergleich zu den anderen Konstruktionen. Doch deren ähnliche Verwendung und der gleiche Kundenkreis legen eine analoge Betrachtung nahe.

Halbrotor-Maschinen

Der schwedische Miterfinder des Rotorverfahrens Arvid DAMM ging bei seiner Patentanmeldung (10.10.1919) einen Sonderweg: Er brachte nicht beidseitig am Rotor Kontakte an, sondern nur einseitig, und verband diese Kontakte auf der anderen Seite mit fünf Schleifringen. Für diese Konstruktion wurde später der Begriff „Halbrotor“ üblich.

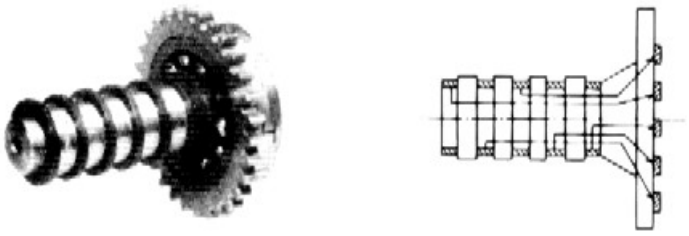


Bild 19: Damm's "Halbrotor" (1919)[110]

Für diese Version gab DAMM'S Mitarbeiter und späterer Nachfolger Boris HAGELIN (s. dazu 3.3) folgende Begründung:

Damm's Elektrocrypto B18

DAMM beabsichtigte, seine Maschinen besonders für die Chiffrierung von Funk-Telegraphiesendungen auszulegen; er glaubte dafür einen Markt zu finden, weil diese Sendungen leicht abgehört werden konnten. Die Maschine konstruierte er mit Tastatur, motorbetriebener Chiffriereinrichtung und Telegraphie-Lochbandstanzer; alternativ konnte auch eine elektrische Schreibmaschine das Chiffrat ausgeben. Die Verschlüsselung erfolgte durch zwei Halbrotoren mit ungleichmäßiger Rotation, was er durch separate Schlüsselräder erreichte. Die fünf Schleifringe der Rotoren erzeugten über eine 5 × 5 Matrix jeweils 25 mögliche Kombinationen, so daß ein Buchstabe des Normalalphabets entfallen mußte. Der Antrieb über Primzahlen-*pinwheels* (Schlüsselräder) mit einstellbaren Stiften, vergleichbar einem Sprossenrad in Rechenmaschinen, erzeugte in Kombination mit der Matrix theoretisch sehr hohe Schlüsselzahlen.[111]

[110] Bild nach Bauer, Geheimnisse, S. 113.
[111] Vgl. Hagelin, Cryptos, S. 483-487.

Bemerkenswert an dieser Konstruktion ist die mögliche *online*-Chiffrierung, denn das gestanzte Lochband konnte anschließend durch den Abtaster laufen. Das zeichnete die Maschine gegenüber der ENIGMA besonders aus und entsprach vermutlich den Vorstellungen der potentiellen Kunden. Hinzu kam die einfache Voreinstellung: Man mußte nicht wie bei der ENIGMA erst umständlich die Rotoren nach einem vereinbarten Schema einsetzen und einstellen, sondern nur eine Relais-Matrix schalten. Die *pinwheels* waren nur bei höheren Sicherheitsanforderungen einzustellen (*pin setting*), oder in größeren Zeitabständen.

Hagelin's Elektrocrypto B21 und B211

Für das schwedische Militär entwickelte der Nachfolger DAMMS, Boris HAGELIN (s. 3.3), auf der Basis der Elektrocrypto B18 die Maschine Elektrocrypto B21, mit einer Periode von [theoretisch] 10^{24}, wenn alle Möglichkeiten des *pin settings* ausgeschöpft wurden. Für den Büroeinsatz in der Privatwirtschaft konnte eine elektrische Schreibmaschine angekoppelt werden.[112]

Die B21 ähnelt äußerlich sehr der ENIGMA, mit etwa der gleichen Periode, und hat als Ausgabe ebenfalls ein Glühlämpchenfeld.

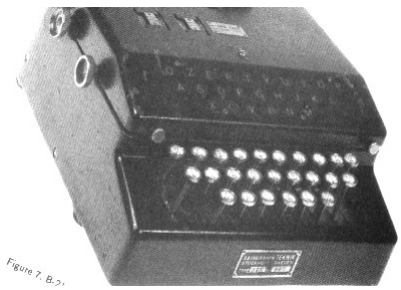


Bild 20: B21 von Damm/Hagelin[113]

Die französische Armee interessierte sich für diese Maschine, forderte jedoch statt des fehleranfälligen Ablesens des Lämpchenfeldes eine Vorrichtung zum Ausdrucken des Textes. HAGELIN ersetzte daher das Lämpchenfeld durch einen elektromechanischen Typenraddrucker, der bei Stromausfall von Hand betätigt werden konnte. Für die Relais-Chiffriermatrix genügte dann eine Taschenlampenbatterie als Stromquelle. Von dieser B211-Maschine konnte HAGELIN ca. 500 Stück an die französische Armee verkaufen – und von dem Erlös seine klamme Firma sanieren.

[112] Vgl. Hagelin, Cryptos, S. 483-487.
[113] Bild nach Ebd.

Erwähnenswert ist noch der Verkauf von zwei Maschinen an die Sowjetunion: Dort baute man die Maschinen nach, mit Modifikationen für das kyrillische Alphabet, und setzte sie im Weltkrieg erfolgreich ein.[114]
Deutsche Dienststellen waren über diese B211-Maschinen informiert und auch darüber, daß eine russische Variante mit 6 Sprossenrädern existierte.[115]

Japans Halbrotormaschine RED

Eine japanische Maschine, US-Tarnbezeichnung RED, basierte ebenfalls auf einem Halbrotor. Dieser erhielt sogar 26 Schleifringe, womit man die lateinische Buchstaben-Transliteration[116] des Japanischen abdeckte. Nach BAUER hatten dazu die Japaner die Konstruktionen anderer Länder studiert, darunter die Maschinen von DAMM/HAGELIN, und auch den Halbrotor übernommen. Allerdings verzichteten sie auf dessen ungleichmäßige Fortschaltung durch die Schlüsselräder und das *pin setting*, und erreichten so nur eine kryptologisch schwache Fortschaltung der Rotoren. Daher brachen US-Kryptologen bereits 1936 die Maschine, die im diplomatischen Dienst verwendet wurde.[117]

Japans Maschine PURPLE

Die Halbrotor-Maschine RED war bei Kriegsbeginn nicht mehr im Einsatz. Deren Nachfolgerin PURPLE (US-Tarnbezeichnung) verschlüsselte zunächst sicher, doch deren spätere Brechung unter der Tarnbezeichnung MAGIC kompromittierte den japanischen Diplomatiefunk im Kriege – das erhielt historische Bedeutung: Besonders die Sendungen der jap. Botschaft in Berlin enthielten fast alle Einzelheiten deutscher langfristiger Planungen, deren Entzifferung die alliierte Strategie beeinflußten.

Die ENIGMA-orientierte Maschine nutzte statt drei Rotoren eine neuartige Vertauscherkonstruktion, bei der drei 25er Schrittschalter die Vertauschungen bewirkten. Deren Kontakte schaltete man mittels Steckerfeld flexibel zusammen, so daß der umständliche Rotorwechsel der ENIGMA entfiel.
Nach der Analyse und Rekonstruktion der Maschine mußten die US-Kryptologen keine kryptanalytischen Maschinen dagegen entwickeln, da die sehr mangelhafte japanische Chiffrierdisziplin es den Entzifferern leicht machte. Beispielsweise übermittelten die Operatoren vor dem Schlüsselwechsel den neuen Schlüssel noch mit der alten Einstellung – die Entzifferer brauchten nur ihren elektromechanischen PURPLE-Simulator umzustöpseln.

[114] Vgl. Hagelin, Cryptos, S. 488-489.
[115] Bericht über das Chiffrierwesen in OKW/Chi.
[116] Überführung der japanischen Schriftzeichen in das lateinische Alphabet.
[117] Vgl. Bauer, Geheimnisse, S. 147-148.

3.2.6 TYPEX - Wissenschaft statt Empirie

ENIGMA – Prototyp der Empirie

Die Maschine ENIGMA war, wie bereits erläutert, ein Produkt der Empirie: Weder der Erfinder, dann die Hersteller, noch die militärischen Anwender der Maschine hielten kryptologische Prüfungen für erforderlich. Vermutlich wußten manche nicht einmal, daß es eine wissenschaftliche Kryptologie gab, erst recht nicht, welche Möglichkeiten die Kryptanalyse zur Brechung von maschinellen Chiffrierungen bietet.

TYPEX – das wissenschaftsorientierte Gegenbeispiel

Völlig anders verlief hingegen die Entwicklung der TYPEX-Maschine in England: Seit 1926 prüfte ein *Inter-Departmental Cypher Committee* alle erreichbaren Maschinen und Prototypen, verwarf diese als kryptologisch unsicher, und beendete 1934 die Arbeit mangels geeigneter Geräte. Doch Experten der Royal Air Force setzten diese Arbeit fort und beschlossen, eine kommerzielle ENIGMA D umzurüsten, und dabei einen weit höheren Sicherheitsstandard als den der ENIGMA anzustreben. Das gelang (s.u.), und nach einem erfolgreichen Einsatz der Prototypen in der Abbessinien-Krise 1935 begann in 1937 die Produktion der TYPEX Mk I. Eine verbesserte TYPEX Mk II wurde 1938 dem *Inter-Departmental Cypher Committee* präsentiert, dort akzeptiert und daraufhin in anderen Dienststellen eingeführt, bspw. in Army, Navy und CHURCHILL's War Office, jedoch – produktionsbedingt – nur in kleinen Stückzahlen.[118]

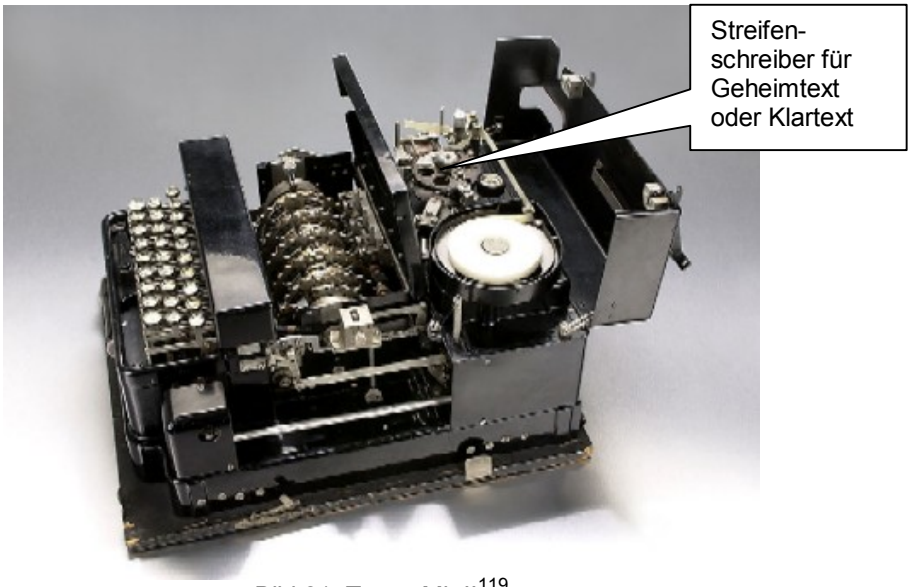


Bild 21: Typex Mk II[119]

[118] Vgl. Erskine, Ralph: The Development of Typex.
In: Kapera, Z.J (Ed.): The Enigma-Bulletin N° 2 - May 1997.

[119] Bild nach HNF/Ryska, Vortrag Kryptologie.

Die kryptologisch sehr wirksame Verbesserung der ENIGMA erforderte erstaunlich wenig Aufwand: Die Maschine erhielt bspw. Rotoren, deren Buchstabenringe je 5, 7, oder 9 Nocken aufwiesen (ENIGMA: 1 bzw. 2), und erzeugte damit quasi-irreguläre Bewegungen. Zwei stationäre, aber einstellbare Eingangsrotoren ersetzten das ENIGMA-Steckerbrett, womit man die Reziprozität der ENIGMA vermied. Und statt der festen inneren Verdrahtung der ENIGMA-Rotoren stellte ein *reversible insert* in den Rotoren die Verbindungen her, so daß man jederzeit deren Verdrahtung ändern konnte. Durch diese kostensparende Konstruktion benötigte man auch nicht jeweils neue, aufwendig herzustellende Rotoren, und konnte doch aus weitaus mehr Exemplaren auswählen, nämlich aus 120 (später 240), im Gegensatz zu fünf der ENIGMA I. So standen mehr als 20 (40) komplett verschiedene Rotorsätze zur Verfügung (ENIGMA einer), und ein gegnerischer Einbruch konnte nicht mehr die Sicherheit der anderen Schlüsselnetze gefährden, die andere Rotorsätze verwendeten.
In der Weiterentwicklung TYPEX IV kam eine zusätzliche externe Vorrichtung hinzu, die der späteren Umkehrwalze D der ENIGMA kryptologisch entsprach. Mit diesem äußeren Steckerfeld konnten ebenso neue Verbindungen geschaltet werden, doch viel bequemer als bei der ENIGMA, wo man zuvor die Umkehrwalze D demontieren mußte.

In der Summe sicherten alle diese Maßnahmen die Chiffrierung so sehr, daß deutsche Experten diese Maschinen nicht brechen konnten und es nach mehreren Versuchen aufgaben, obwohl TYPEX-Maschinen erbeutet wurden.[120]
Auch die US-Kryptologen anerkannten den hohen Sicherheits-Standard der TYPEX-Maschinen: Sie akzeptierten für den gemeinsamen intensiven Nachrichtenaustausch auf höchster Ebene eine Version „CCM“ (*Combined Cipher Machine*), der zur Kommunikation mit der US-Rotormaschine SIGABA eine *SIGABA compatibility box* nachgeschaltet war.
Die Entwicklung der TYPEX zeigt eindrucksvoll, wie eine empirisch entstandene Maschine, die ENIGMA, dank wissenschaftlicher Kompetenz zu einem weit sichereren Gerät entwickelt wurde, und das mit geringem technischen Aufwand. Und diese hohe kryptologische Sicherheit der TYPEX bot genügend Reserven gegen die im Krieg unvermeidlichen Chiffrierfehler, die überdies gering blieben, weil britische Militärs die Maschinen viel vorsichtiger verwendeten, als deren deutsche Gegner die ENIGMA.

In BP erfüllte die TYPEX sogar eine historische Mission: Die täglich bis zu dreitausend mit ENIGMA chiffrierten Nachrichten mußten zur Auswertung in den Klartext übertragen werden. Dazu ermittelte man zunächst per Turing-BOMBE die Tagesschlüsseleinstellungen der ENIGMA, und zwar für jeden der vielen Schlüsselkreise. Diese Einstellungen übertrug man anschließend auf modifizierte TYPEX-Maschinen, und erhielt dann nach Eintippen des Geheimtextes den Klartext per Streifenschreiber ausgedruckt.

[120] Vgl. Erskine, Ralph: The Development of Typex.
In: Kapera, Z.J (Ed.): The Enigma-Bulletin 2 - May 1997.

US-Maschine SIGABA

Analog zur TYPEX, entstand die aufwendige und praktisch unbrechbare US-Maschine SIGABA ebenso aus einem empirisch entwickelten Vorläufermodell: Aus HEBERN'S ECM-Maschine entwickelten die besten US-Kryptologen die sicherste Chiffriermaschine im Zweiten Weltkrieg, die bis 1959 eingesetzt wurde.

3.3 Hagelin's mechanische Chiffriermaschinen

Im Abschnitt 3.1 wurde dargelegt, wie der Chiffrierzylinder zum Chiffrierrotor mutierte, indem der Erfinder dazu eine elektromechanische Analogie nutzte. Es ist aber ebenso möglich, Chiffrieralgorithmen rein mechanisch zu erzeugen. Vorbilder dafür gab es schon lange: Mechanische Rechenmaschinen, bei denen Zahnradgetriebe und Walzen die mathematischen Algorithmen nachbildeten, bis hin zu Großmaschinen der Höheren Mathematik wie bspw. Babbage's Maschinen.

Der bereits erwähnte Ingenieur Boris HAGELIN entwickelte auf dieser Basis um 1935 eine rein mechanische Maschine, die zur erfolgreichsten Chiffriermaschine überhaupt wurde.

Bild 22: Erfinder der mechanischen Chiffriermaschine B. Hagelin[121]

Boris Caesar HAGELIN (1892-1983) war der Sohn eines Teilhabers der Firma des Miterfinders des Rotorverfahrens A. DAMM (s. 3.2.5), hatte Maschinenbau studiert und anschließend in Schweden und den USA als Ingenieur gearbeitet. Ab 1922 vertrat er als Mitarbeiter in Damm's Firma die Interessen seines Vaters. 1925 beabsichtigte die schwedische Armee ENIGMA-Maschinen zu kaufen, was HAGELIN verhinderte durch Entwicklung einer vergleichbaren Maschine, der Elektrocrypto B-21 (s. Bild 20). Nach Damm's Tod 1927 übernahm die Hagelin-Gruppe die Firma, wandelte sie um in eine Aktiengesellschaft mit Boris HAGELIN als Direktor.
Er erkannte die Schwachstelle der bisherigen Maschinen, nämlich das Ableseverfahren wie bei der ENIGMA, und begann stattdessen kompakte

[121] Bild nach HNF/Ryska, Vortrag Kryptologie.

Druckeinheiten für die Maschinen zu entwickeln. Diese Elektrocrypto B211 konnte er erfolgreich vermarkten (s. 3.2.3). Und um 1935 gelang ihm eine Innovation, die zur erfolgreichsten Chiffriermaschine entwickelt wurde.[122]
Nach eigener Darstellung[123] hatte HAGELIN Ende der 20er Jahre eine Münzwechselmaschine für schwedische Auftraggeber konstruiert, die jedoch nicht produziert wurde. Für diesen Prototyp entwickelte er ein neuartiges Maschinenelement, bestehend aus einer Trommel mit axialen Schubstangen, auf denen verschiebbare Mitnehmer von Tasten betätigt werden konnten – später Stangenkorb oder Stabtrommel (*drum bar* oder *lug cage*) genannt. Man kann hier eine Analogie zur im 18. Jahrhundert von LEIBNIZ erfundenen Staffelwalze erkennen, mit dem Unterschied, daß nicht die Walze verschiebbar ist, sondern die Mitnehmer und deren Stangen – der Effekt bleibt gleich.

HAGELIN entsann sich seiner Idee, als ihn um 1934 der französische Geheimdienst nach einer Chiffriermaschine fragte, die sehr kompakt und leicht sein sollte, und darüber hinaus den Text drucken konnte. Hierzu verwendete er diesen Stangenkorb, ersetzte die Mitnehmer-Tasten durch Schlüsselräder und baute den Typenraddrucker der B211-Maschine ein. So entstand die 1935 unter der Bezeichnung C35 vorgestellte Chiffriermaschine.

3.3.1 C38 – die erfolgreichste Chiffriermaschine

Unter Mitarbeit des schwedischen Kryptologen Yves GYLDÉN (1895-1963) wurde die Maschine erheblich verbessert, vor allem durch ein zusätzliches sechstes Schlüsselrad. Überdies konnten die Schlüsselräder nun pseudo-unregelmäßige Fortbewegungen erzeugen, weil mit einsteckbaren Pins ein jeweils wechselndes Bewegungsmuster programmierbar war. Diese Konstruktion ähnelt den Sprossenrädern in mechanischen Rechenmaschinen, ebenfalls bereits im 18. Jahrhundert erfunden von POLENI. Mithin kombinierte HAGELIN in der C36 – historisch betrachtet – eine Staffelwalze mit Sprossenrädern, und generierte damit die Chiffrier-Algorithmen.

Die schwedische Armee übernahm diese C36-Version; ein französischer Lizenzauftrag über 5000 Maschinen konnte kriegsbedingt nur teilweise realisiert werden.

---

[122] Vgl. Kahn, Codebreakers, S. 425-427.

[123] Vgl. Hagelin, Boris C.W.: The Story of the Hagelin Cryptos. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, Artech House, Norwood MA/USA, 1998. (Künftig zit. "Hagelin, Cryptos").

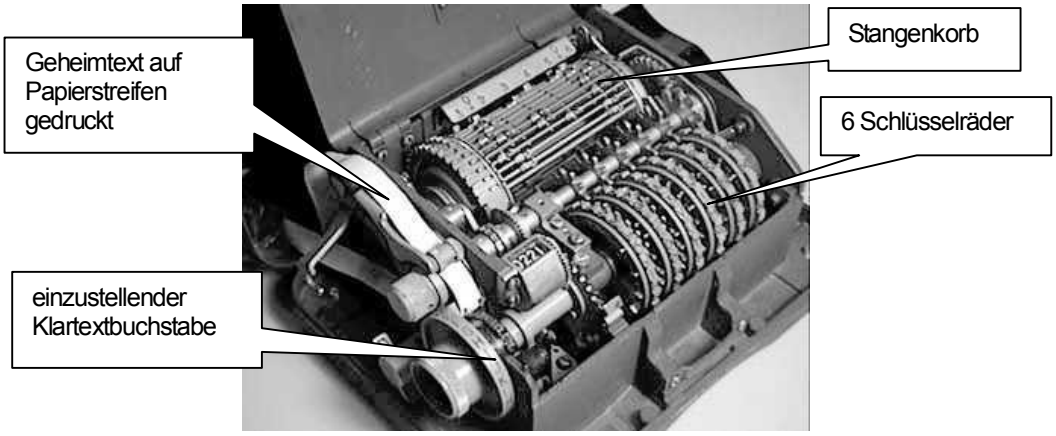


Bild 23: HAGELINS mechanische Chiffriermaschine C38 (hier US-Army-Version M-209-B) [124]

Die US-Army bezog 1940 ca. 50 Maschinen der verbesserten Version C38 für Prüfzwecke, und nach ausführlichen kryptologischen Tests wurde die Maschine für taktischen Einsatz (unterhalb Divisionsebene) akzeptiert. Daraufhin stellte in den USA die Büromaschinenfirma Smith & Corona nach HAGELIN'S Lizenz bis Kriegsende ca. 140.000 Maschinen her, die Army (als M-209) und Navy (CSP-1500) einführten.[125]
Es war die kommerziell erfolgreichste Chiffriermaschine, auch weil sie sich besonders gut für militärischen Einsatz eignete: Sie war leicht und tragbar, erforderte nur Einmannbedienung, und benötigte keine Stromversorgung. Die bewährten Maschinen wurden sogar noch im Koreakrieg verwendet.

Sicherheit der C38

Die erwähnten Verbesserungen der C36 bewirkten eine große Verlängerung der Schlüsselperiode der C38. HAGELIN gibt dazu Beispiele für die Wirkung der vielen Einstellmöglichkeiten, die, miteinander kombiniert, eine astronomische Schlüsselzahl von über 10^{100} ergeben sollen.[126] Nach dieser unrealistischen Schätzung – ein Druckfehler? – kann man jedoch nicht die effektive Sicherheit der Maschine beurteilen, denn von der großen Zahl von theoretisch möglichen Kombinationen sind viele nicht realisierbar, andere wiederum sind identisch oder ähnlich, so daß keine neue Chiffrierung entsteht. Das aber ist ein Problem aller Chiffriermaschinen, auch der ENIGMA, wie unter 3.2.2 mit Zahlenbeispielen dargelegt wurde.

Gleichwohl muß die Sicherheit der Maschine C38 bedeutend höher als die der ENIGMA sein, wenn *alle* Einstellmöglichkeiten genutzt werden. Das bestätigte der Kryptologe Hans ROHRBACH (1903-1993), ein ins Auswärtige Amt bis 1945

[124] Bild nach International Association for Cryptologic Research: The Hagelin M-209-B Rotor Machine.
[125] Vgl. Hagelin, Cryptos, S. 492-495.
[126] Vgl. Hagelin, Cryptos, S. 500.

dienstverpflichteter Mathematiker, als er nach dem Krieg schrieb: „Variabilität von Stangenkorb und Rädersystem gibt in stärkerem Maße als bei der ENIGMA die Möglichkeit zu Sicherungen, deren volle Ausnutzung einem Hagelin-Verfahren ein besonderes Maß von Sicherheit verleiht.“ [127]

Doch manche Autoren scheinen diese Kombinationsmöglichkeiten übersehen zu haben, denn sie beziehen sich nur auf die sechs „Antriebsräder“, die allein freilich eine Periode von nur knapp über 10^8 erzeugen. Demzufolge gelangen sie zum Ergebnis, die Sicherheit der Maschine sei erheblich niedriger gewesen als die der ENIGMA I.
Diese und ähnliche Bewertungen der C36/38-Maschinen orientierten sich womöglich an Berichten über die Brechung der C38m der italienischen Marine und der M-209 der US-Army. Denn sowohl BP, deutsche Entzifferer in Nordafrika, Italien und an der Westfront als auch die US-Amerikaner waren erfolgreich und lasen Nachrichten der Schweden, Finnen und Norweger. Die Autoren erklären das mit mangelhafter Chiffrierdisziplin der Operatoren.[128]

Den Widerspruch in den Beurteilungen der Maschine und deren scheinbar mühelose Brechbarkeit klärte der frühere Mitarbeiter des italienischen kryptographischen Dienstes der Marine, der spätere Admiral L. DONINI: In einem ausführlichen Bericht erläuterte er die Gründe, die es erleichterten diese Maschinen zu brechen, obgleich deren Sicherheit mit den erwähnten Kombinationsmöglichkeiten sehr hoch war.

Er verweist vor allem auf die Kompliziertheit der „inneren“ Einstellung: Um die theoretisch möglichen 10^{60} „inneren“ Schlüssel zu nutzen, eine ebenso unrealistische Schätzung wie vor (vermutlich übernommen), mußten z.B. bis zu 131 Pins der Schlüsselräder gesetzt werden, dann waren 32 Mitnehmer des Stangenkorbs in je 6 Positionen zu arretieren, usw. In der eng gebauten Maschine erforderte das viel Fingerspitzengefühl und Geduld, was unter Frontbedingungen schwer zu realisieren war. So entschloß man sich, diese Prozedur nur monatlich vorzunehmen und nahm damit in Kauf, daß die Chiffriersicherheit dann nur noch vom Spruchschlüssel für die sechs Einstellräder abhing, wenn ein Einbruch gelungen und damit die jeweilige Einstellung gefunden war – die erwähnten 10^8 Einstellmöglichkeiten. DONINI bezeichnet das als akzeptabel im ersten Kriegsjahr mit relativ wenig Funkverkehr. Als dann aber im Krieg bis zu 4000 Funksendungen täglich anfielen, die Entzifferer entsprechend viel Material hatten, waren Einbrüche quasi programmiert. Überdies erleichterten die Operatoren den Entzifferern die Arbeit: Sie verwendeten oft den gleichen „äußeren“ Schlüssel für zwei oder gar mehrere Nachrichten.[129]

---

[127] Rohrbach, Hans: Chiffrierverfahren der neuesten Zeit. In: A.E.Ü. 2 (1948), S. 362-369.

[128] Vgl. Deavours, C.A./Kruh, L.: Machine Cryptography and modern Kryptanalysis, Artech House, Norwood MA/USA, 1995.

[129] Vgl. Donini, L.: The Cryptographic Services of the Royal (British) and Italian Navies. Transl. by

Der ehemalige Chef des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Otto LEIBERICH, äußerte sich ähnlich: Danach konnten die Experten des OKW/Chi die Maschine M-209 täglich kompromittieren, „weil die Alliierten ihre Schlüssel ungeschickt handhabten.“[130] Dazu erläuterte er ausführlich die Methoden der Entzifferer und bestätigte im Wesentlichen die vorerwähnten Ausführungen DONINI'S.

Diese Entzifferungen endeten jedoch in 1942, so LEIBERICH, weil BP in entzifferten italienischen Marinesendungen Hinweise auf die deutsche Kompromittierung der M-209 fand. Eine daraufhin erfolgte „Verfahrensänderung“ [LEIBERICH nennt diese nicht] verhinderte weitere deutsche Erfolge.[131] Doch diese Darstellung wird von anderen Quellen nicht bestätigt:
Nach einem Bericht des ehemaligen Soldaten Reinhold WEBER entzifferte er und seine Einheit FNAST 5 „bis Anfang 1945“ Funksendungen der US-Truppen an der Westfront, bis zur Flucht vor den heranrückenden Amerikanern.[132]
Ebenso BAUER: Deutsche Stellen „... entzifferten ... bis 1944 in Nordafrika und Italien.“[133]

Da die M-209 weiter im Einsatz blieb, sogar noch im Koreakrieg, und offenbar nicht verändert wurde – Modifikationen sind nicht bekannt – ist anzunehmen, daß man die erwähnten „inneren“ Einstellmöglichkeiten nun nutzte und/oder die Chiffrierdisziplin verbesserte.

3.3.2 Wanderer-Werke und „Menzer-Geräte“

Ein erst 2003 veröffentlichter NSA-Bericht[134] über deutsche Chiffriermaschinen enthält einen Abschnitt *The Menzer Devices,* benannt nach dem im OKW/Chi beschäftigten Oberinspektor Fritz MENZER. Danach sei MENZER verantwortlich gewesen (*responsible*) für eine Anzahl Verbesserungen kryptographischer Maschinen, insbesonders indem er Hagelin-Schlüsselräder mit [pseudo-]irregulären Bewegungen[135] versah und in Chiffriermaschinen verwendete. Sogar die Erfindung (*invention*) des Schlüsselgerätes 39, -41 und eines „Schlüsselkastens“ (s.u.) schrieb der Autor ihm zu, und benannte nach ihm eine

---

Buonafalce. (Orig. in: Rivista Marittima, Rom, Jan. 1983). In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIV, Nr. 2, April 1990, Artech House, Norwood MA/USA, 1998. S. 11-31.

130 Leiberich, Otto: Vom diplomatischen Code zur Falltürfunktion. Hundert Jahre Kryptographie in Deutschland. In: Spektrum der Wissenschaft 4/2001, S. 14-16.

131 Ebd.

132 Vgl. Schmeh, K.: Als deutscher Code-Knacker im Zweiten Weltkrieg. Von: http://www.heise.de/tp/r4/artikel/18/18371/1.html, am 23.12.04.

133 Vgl. Bauer, Geheimnisse, S. 224.

134 Mowry, David P.: German Cipher Machines of World War II, Center for Cryptologic History, National Security Agency 2003. S. 17 ff.

135 Bereits 1936 vom schwedischen Kryptologen Gyldén empfohlen; wurde in Hagelin's C-36 realisiert.

Geräteklasse, die „*Menzer devices*." In einer anderen Publikation lobte er MENZER im Titel gar als „Cryptographic Inventor Extraordinaire."[136]

Ist diese ungewöhnlich hohe Bewertung eines relativ untergeordneten OKW-Mitarbeiters realistisch, mindestens glaubhaft? Und wie ist das zu interpretieren im Zusammenhang mit den Chiffriermaschinen der Wanderer-Werke?

Der Bericht nennt als Quellen TICOM-Reports, die nicht allgemein zugänglich sind, und, neben den Gerätebeschreibungen, überwiegend aus Protokollen von Verhören unmittelbar nach dem Krieg bestehen. Ob dabei MENZER seine Rolle im OKW etwas „überhöhte", und/oder die verhörenden Offiziere zu Mißverständnissen neigten, ist nachträglich nicht mehr zu klären. Und ob der Autor MOWRY bzw. die Verhöroffiziere den deutschen Beamtentitel MENZERS richtig (als subaltern) einzuschätzen vermochten, ist sehr fraglich. Denn dieser wurde mit für amerikanische Ohren vermutlich sehr bedeutend klingenden „*superior government inspector*" wörtlich übersetzt.

Fritz MENZER (1908-?) diente, folgt man MOWRY'S Bericht, ab 1926 als *mecanic* in der Reichswehr in einer Fahrzeugeinheit, wurde 1935 zum OKW in die Abt. Chi versetzt und erhielt dort eine Ausbildung (*formal training in the field*). Nach Ablauf seiner Militärdienstzeit 1938 arbeitete er dort weiter als Beamter (ab 1940 Oberinspektor) und war technischer Berater der Abwehr bis 1945.[137]
Mithin war MENZER kein wissenschaftlicher Kryptologe, sondern befaßte sich wahrscheinlich mit technischen Anforderungen an Chiffriermaschinen, speziell mit den rein mechanischen Hagelin-Maschinen. Denn es war üblich, daß Militärbehörden den Rüstungsbetrieben zwar Vorgaben machten, es ihnen jedoch überließ, welche technische Lösung sie fanden. MENZER könnte demnach im OKW/Chi verantwortlich gewesen sein etwa als technischer Sachbearbeiter; und ohnehin konnte OKW/Chi nur beraten, denn federführend waren in der Wehrmacht stets die Waffenämter.
Indirekt bestätigt das ein Dokument mit „...das Schlüsselgerät T41, das nach Angaben von OKW/Chi [Menzer] von Wa Prüf 7 [Heereswaffenamt] mit den Wandererwerken entwickelt wurde."[138] Mithin war MENZER nicht der *inventor*, wie der Verfasser des NSA-Berichts meint, doch als technischer Sachbearbeiter formulierte er die Vorgaben, wie ein weiteres Beispiel zeigt:

Schlüsselgerät 41

HAGELIN offerierte bereits vor dem Krieg eine C38-Variante mit Tastatur und Elektroantrieb, vermutlich für zivile Büroanwendungen entwickelt, nämlich die Maschine BC38. Eine ähnliche Maschine sollten oder wollten[139] die Wanderer-

[136] Mowry, David P.: Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire, Cryptologic Quarterly, Vol. 2, Nos. 3-4, Fall/Winter 1983-84, 21-36.
[137] Vgl. Mowry, David P.: Regierungs-Oberinspektor Fritz Menzer. S. 17-18.
[138] Neu-und Weiterentwicklung technischer Schlüsselmittel. Stand Januar 1944. S. 3.
[139] Die Vorgänge der Auftragserteilungen konnten bisher nicht geklärt werden mangels Dokumente.

Werke Chemnitz konstruieren, und MENZER formulierte dazu die zusätzlichen Anforderungen: „Es soll noch während der Ver- bzw. Entschlüsselung eine Verschiebung zwischen den Bolzenrädern und der Zahnstange (Schieberzunge) stattfinden. Es ist dabei gleichgültig, ob die Zahnstange oder die Bolzenräder (bei gegebenen Befehl von den Bolzenrädern) um eine Teilung voreilen. Der Befehl für die Voreilung wird von den Bolzenrädern, genau wie der Haltebefehl, abgetastet, jedoch um 180° versetzt.“[140]

Die Realisierung dieser Vorgabe durch die Wanderer-Konstrukteure konnte vom Verf. an einer restaurierten und funktionstüchtigen Maschine überprüft und bestätigt werden.[141] Und diese Modifikation erwies sich als kryptologisch wirksam: Es gelang in BP zwar einige Nachrichten zu entziffern mit Hilfe von *depths*, doch die Maschine SG41 konnte man nicht rekonstruieren und dementsprechend keine Entzifferungsverfahren entwickeln.[142] Das ist erstaunlich, denn die original Hagelin-Maschine war in BP genau bekannt und dementsprechend sollte der davon abweichende Algorithmus der modifizierten Maschine analysierbar gewesen sein. Mithin hatten die Wanderer-Konstrukteure exzellente Arbeit geleistet – und MENZER die Vorgaben richtig formuliert.

In der Literatur wird unterstellt, die Maschine sei ein reiner Nachbau der BC38 gewesen; diese und ähnliche Darstellungen beruhen vermutlich auf HAGELIN’S Bericht.[143]

Bild 24: Original Hagelin BC38[144]

angeblicher Nachbau Wanderer SG-41[145]

[140] StAC, Bestand 31030, Nr. 2846, Bericht 29.1.1944.
[141] Zusammen mit K. Kopacz, der die Maschine restaurierte und analysierte.
[142] Erskine, Ralph: ENIGMA’s Security. In : Erskine/Smith, Action, S. 384.
[143] Vgl. Hagelin, Cryptos. Hagelin nennt hierzu keine Quellen.
[144] Bild: John Alexander, Leicestershire UK.
Von: http://webhome.idirect.com/~jproc/crypto/menu.html, am 24.10.03.
[145] Bild: Kopacz, Stuttgart.

Das aber kann nach Auswertung von Dokumenten nicht bestätigt werden:
Die Maschine wurde im Auftrag des Heereswaffenamtes (OKH/Wa Prüf 7/IV) von den Wanderer-Werken in Chemnitz entwickelt, deren Continental-Werk über umfangreiche Erfahrungen in Konstruktion und Bau mechanischer Geräte verfügte. Lieferaufträge des Heeres wurden am 8.8.1942 (1000 Stck.) und am 30.11.1942 (10.000 Stck.) erteilt.[146] Ein Mustergerät wurde im Mai 1943 vorgeführt, jedoch verschob sich der Produktionsbeginn auf Ende 1943, weil das Heereswaffenamt Modifikationen forderte.
Die Kontrukteure entwickelten die Maschine zwar auf der Basis von HAGELIN'S Erfindung mit Stangenkorb („Stabtrommel") und Sprossenrad („Bolzenrad"), verbesserten sie jedoch kryptologisch stark nach der erwähnten Vorgabe MENZERS.

Doch die Wanderer-Werke produzierten nur ca. 1.500 Maschinen mit der internen Bezeichnung „Artikel 410 bzw. M41", in der Literatur (fehlerhaft) „C41", OKW-offiziell „Schlüsselgerät 41".[147] HAGELIN und andere Autoren unterstellen, daß diese geringe Produktion mangels Ressourcen nicht die geplante Stückzahl erreichte.[148] Das aber hatte ganz andere Gründe: Bei einer Besprechung im OKW/WNV mit General THIELE[149] am 8.12.43 wurde festgelegt: Nur 1.000 Maschinen sind bis Ende 1944 herzustellen, da sie mit 13,5 kg zu schwer für den Fronteinsatz sind.[150] Bis April 1945 wurden weitere 550 Stück produziert, vermutlich die Version SG-41Z (mit Zifferntastatur) für die Luftwaffe, die sie für ihr Wetternachrichtennetz eingesetzt haben soll.[151]

Das „kleine Gerät"

Die schwere Maschine SG-41 sollte durch ein wesentlich leichteres Gerät ersetzt werden, dessen Gewicht das OKH mit max. 3,5 kg festlegte. Es sei für die Verwendung durch vorderste Einheiten vorgesehen, ohne Tastatur, und nur einem Schreibwerk [analog M-209, s. Bild 21].[152] Es wurde zunächst diskutiert, die Maschine M-209 nachzubauen, auch wenn deren Sicherheit geringer als die des SG-41 sei, „....um die Truppe in kürzester Zeit mit einem kleinen Gerät auszurüsten." Der Kryptologe KEHREN von OKW/Chi bemerkte dazu, daß man dann auch die geringere Schlüsselsicherheit dieser Maschine in Kauf nehmen würde, und „...von diesem kleinen Gerät kämen schätzungsweise 100.000 Stück in Frage."[153]

---

[146] StAC, Bestand 31030, Nr. 2846.
[147] StAC, Bestand 31030, WW 929, Zentralstatistik.
[148] Vgl. Hagelin, Cryptos, S. 496.
[149] Nachfolger General Fellgiebels, wurde nach 4 Wochen ebenfalls verhaftet und hingerichtet.
[150] StAC, Bestand 31030, WW 2846, Bericht vom 10.12.1943.
[151] Ebd., WW 929, Zentralstatistik. Die Verwendung für Wetternachrichten wurde erstmals erwähnt in einem internen Bericht (Ebd., Nr. 2846) vom 22.2.44.
[152] Ebd., WW 2846, Bericht vom 10.12.1943.
[153] Ebd., Inoffizielle Besprechung OKW/WW am 9.10.1943. Diese Zahl entspricht den vermutlich insgesamt eingesetzten ENIGMA –Maschinen.

Diese Schätzung kann man, in Zusammenhang mit anderen Äußerungen wie „... jetzt muß die ENIGMA sterben“[154] als Versuch der Abteilung Chi interpretieren, einen Ersatz der ENIGMA wegen Sicherheitsbedenken längerfristig anzustreben, wofür allerdings das OKW und dessen Waffenamt erst überzeugt müßten – ein Versuch dazu ist nicht bekannt, zumal die ENIGMA offiziell weiter als sicher galt.
Ein Nachbau der Maschine M-209 wurde dann nicht mehr verfolgt und stattdessen ein „kleines Gerät“ von den Wanderer-Werken konstruiert, das erstmals am 20.5.1943 in einem Dokument[155] erwähnt wird. Gemäß Vorstandsbericht sollte dessen Konstruktion bis Ende Februar 1944 abgeschlossen sein, und dieses „... vereinfachte und viel leichtere Gerät wird dann in großer Auflage aufgelegt werden.“[156] Das korrespondiert mit den erwähnten Angaben des Kryptologen KEHREN von OKW/Chi.
Produziert wurde die Maschine jedoch nicht, vermutlich weil ab 6.7.1944 das „Schlüsselgerät 39“ favorisiert wurde, das der NSA-Bericht (unzutreffend) den „Menzer-Geräten“ zuordnet (s. 3.2.3).
Über dieses neu konstruierte „kleine Gerät“ sind keine Dokumente verfügbar.

Schlüsselkasten 43

Der NSA-Bericht enthält auch den „Schlüsselkasten“ („*Cipher Box*“), ein Gerät, das bisher nicht in der Literatur erwähnt wurde. Es sollte die ENIGMA ersetzen („*substitute or backup*“), und wird als eine mechanische Chiffriervorrichtung beschrieben mit gegeneinander verschiebbaren beschrifteten Schieberzungen, die mit einem Federantrieb pseudo-irregulär bewegt wurden, gesteuert von setzbaren Schlüsselscheiben. Vermutlich wurde diese Technik von MENZER entwickelt, denn der Bericht zeigt zwei Bilder eines Holzmodells „made by Fritz MENZER.“
Der Schlüsselkasten 43 sollte massenhaft produziert werden und die ENIGMA unterhalb der Divisionsebene ersetzen; beginnend mit 1.000 Geräten im Oktober 1945, dann ab Januar 1946 mit monatlich 10.000 Stück.
Der Autor scheint von dem Entwurf sehr beeindruckt gewesen zu sein, denn er schrieb „*... if it had been introduced in 1942, it could have changed the course of the war.*“[157]
Der Zusatz „43“ ist vermutlich analog zu anderen Wanderer-Geräten als Entwicklungs- oder Auftragsjahr 1943 zu interpretieren. Das korrespondiert mit der Vorführung eines Mustergerätes der Wanderer-Werke im Februar 1944 vor Vertretern des federführenden Heereswaffenamtes und OKW/Chi [ohne MENZER!]. Diese verlangten zahlreiche Änderungen, mit der Folge, daß die Wanderer-Vertreter für den Produktionsbeginn keinen Termin nennen konnten.[158]

---

[154] Ebd. Besprechung am 4.10.1943 im OKH.
[155] Ebd. Brief Wanderer-Werke an Wa Prüf 7 vom 20.5.1943.
[156] StAC, Bestand 31030, neu 243, Protokoll 5.1.1944.
[157] Vgl. Mowry, David P.: German Cipher Machines of World War II, S. 27-30.
[158] StAC, Bestand 31030, Nr. 2846, Bericht 22.4.1944.

Die Schlüsselscheibe

Dieses Gerät unbekannter Konstruktion muß man ebenfalls den „Menzer-Geräten“ zuordnen, denn diese Schlüsselscheibe sollte ausgeführt werden „...wie schon durch Beschreibung von Herrn Oberinsp. Menzer festgelegt.“[159]
Leider sind keine Angaben verfügbar, und auch der NSA-Bericht erwähnt das Gerät nicht, obwohl es offenkundig eine *Menzer device* war.

3.3.3 Weitere mechanische Chiffriergeräte

Nach dem Krieg steigerte HAGELIN die ohnehin große Sicherheit der C-Maschinen durch verschiedene Verbesserungen: Auswahl der sechs Schlüsselräder aus 12, Erhöhung der Zahl der einstellbaren Mitnehmer im Stangenkorb, usw. Ferner bot er zahlreiches Zubehör für die Maschine an, wie Tastaturen, elektrische Drucker usw.; diese CX52-Maschinen verkaufte die Crypto AG in 50 Länder.[160] Eine technisch verbesserte Version stellte eine deutsche Firma[161] her unter der Bezeichnung H54, die von der deutschen Bundeswehr 1954-1975/76 eingesetzt wurde.
Ein kryptologisch wesentliche Verbesserung erreichte HAGELIN durch eine Pseudo-Irregularität der Schlüsselradbewegungen bei der späteren Version M, nachdem seine bisherigen Maschinen einen fest eingestellten Antrieb hatten.[162]

[159] Ebd.
[160] Vgl. Hagelin, Cryptos, S. 496-497.
[161] Nicht die westdeutsche Nachfolgefirma der enteigneten Wanderer-Werke, die noch heute existiert, sondern die Firma Dr. Hell KG, Kiel. (ehem. Hersteller des „Feldfernschreibers“).
[162] Korrespondenz mit Kopacz (uv.)

4 Technik der Chiffrier-Fernschreiber

Der Fernschreiber beendete die jahrzehntelangen Bemühungen, die zeitaufwendige Telegraphie zu vereinfachen, denn nun konnte man Text seitenweise direkt von Teilnehmer zu Teilnehmer übertragen. Die hierzu erforderliche Codierung eignete sich sehr gut auch für ein Chiffrierverfahren, das noch während der Entwicklungsphase der Fernschreiber entstand, weil die US-Army im Ersten Weltkrieg daran interessiert war. Mithin muß man die Geschichte der Chiffrier-Fernschreiber mit der des Telegraphen gemeinsam betrachten.
Aber noch wichtiger wird die Beantwortung folgender Fragen sein:
Warum eignete sich die Fernschreiber-Codierung optimal für ein Chiffrierverfahren? Bietet das Verfahren besondere Chiffriersicherheit im Vergleich zur ENIGMA?

4.1 Vom Telegraph zum Fernschreiber

Die Verfügbarkeit des elektrischen Stromes setzte eine stürmische Entwicklung der Telegraphie in Gang, die nicht zufällig parallel zur Industrialisierung im 19. Jahrhundert verlief. Treibende Kraft dabei waren zunächst die Eisenbahnen, die Telegraphen für den Zugbetrieb benötigten, wofür verschiedene Nadel- und Zeigertelegraphen entwickelt wurden. Aber erst Schreibtelegraphen boten auch öffentliche Möglichkeiten der Informationsübertragung: Bereits 1836 stellte STEINHEIL ein erstes Gerät vor, doch Samuel MORSE'S 1840 weiterentwickeltes Gerät setzte sich dann durch. Weitere Verbesserungen brachten Drucktelegraphen, etwa von Siemens & Halske (1850), welche die empfangenen Impulse in lesbare Schrift verwandelten. Und das 1855 von HUGHES' erfundene Typendruckrad konnte nach einigen Verbesserungen sogar noch im 20. Jahrhundert in Fernschreibern verwendet werden. Der nächste wichtige Entwicklungsschritt brachte auch eine bedeutende Steigerung der Übertragungsgeschwindigkeit: WHEATSTONE erfand 1867 das Morsecode-Lochband, das elektromechanisch abgetastet wurde.

4.1.1 Das Baudot-Verfahren

Mit den genannten Verbesserungen gelangten die Telegraphieverfahren jedoch an ihre technischen Leistungsgrenzen. Eine Steigerung der Übertragungsleistung war nur noch möglich, wenn die Fernleitungen besser ausgenutzt, d.h. mehrfach mit Signalen belegt würden. Erste Versuche dazu mit einem drehbaren Verteiler, nach heutigen Begriffen ein Zeitmultiplexverfahren, unternahm B. MEYER um 1871.[163] Sie scheiterten, weil die Synchronisation nicht sichergestellt werden

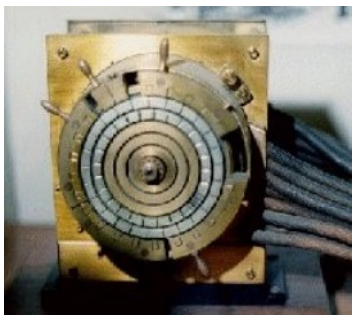
[163] Vgl. Hobbs, Alan G.: Fiveunit codes. (NADCOMM -Museum 1999). S. 2.
Von: http://www.nadcomm.com/fiveunit/fiveunits.htm, am 21.10.01.

konnte, denn die unterschiedliche Länge und Zahl der Morseimpulse je Buchstaben verhinderte einen gleichmäßigen Betrieb. Doch der französische Telegrapheningenieur Emile BAUDOT konnte 1874 dieses Problem lösen und entwickelte ein Verfahren, das zum Standard für fast 100 Jahre wurde.

Bild 25: Erfinder der Telegraphie-Codierung E. Baudot[164]

Er erkannte, daß der Meyer'sche Drehverteiler dann funktionieren würde, wenn die Impulse für die Buchstaben jeweils gleiche Länge hätten. Das erreichte er durch Codierung mit einem 5-Kanal-Code, der $2^5 = 32$ Möglichkeiten umfaßte, also für die 26 Buchstaben und Steuerzeichen genügte.[165] Das nachstehende Bild 26 zeigt, wie BAUDOT'S Code 60 Jahre später international genormt wurde, ergänzt für den Fernschreiberbetrieb durch Umschalter für Groß- und Kleinschreibung.
Diese Impulscodierungen wurden vor der Sendung in ein Band gestanzt; eine quasi-Klaviatur ermöglichte dabei den Operatoren die Bänder rasch zu lochen.

Über den Drehverteiler konnten bis zu fünf Apparate auf eine Leitung geschaltet werden, die nacheinander sendeten/empfingen. Zur Synchronisierung enthielt der Verteiler ein zusätzliches Segment, das einen Summer als Taktgeber schaltete, der den Operatoren den Rhythmus vorgab. In der Empfangsstelle wurden die Impulsfolgen elektromechanisch gespeichert und auf einem Druckstreifen ausgegeben.



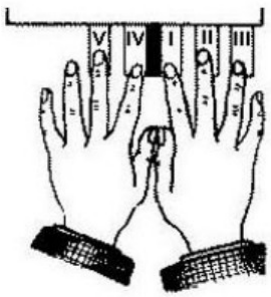


Bild 26: Baudot-Drehverteiler, Keyboard zur 5-Kanal-Lochung[166]

[164] Bild nach Hobbs, Alan G../Hallas, Sam: A Short History of Telegraphy 1987, Part 2. Von www.samhallas.co.uk, am 10.5.03.
[165] Vgl. Hobbs, Fiveunit codes, S. 1.
[166] Bild nach Hobbs./Hallas: A Short History of Telegraphy 1987, Part 2.

Auf beiden Seiten benötigte man dazu je bis fünf Telegraphisten, die in dem vorgegebenen Zeitrhythmus die jeweiligen kanalweise erforderlichen Kontaktgeber betätigten. Meist wurden Doppel- oder Vierfachsysteme eingesetzt, wobei die Geräte auch in verschiedenen Städten gleichzeitig senden/empfangen konnten [nach heutigen Begriffen eine *multipoint transmission*].
Das Verfahren bewährte sich sehr; es war bis Mitte des 20. Jahrhunderts in zahlreichen Postverwaltungen im Einsatz.[167]

BAUDOT'S Verfahren umfaßte zwei informatikhistorisch bedeutende Elemente:
Es war die Vorstufe der binär-digitalen Datenverarbeitung, denn die generierten Impulse wurden nicht nur übertragen, sondern nach Empfang elektromechanisch gespeichert und automatisch wieder in lesbare Schrift umgesetzt. Und es war das erste betriebssichere Mehrfach-Übertragungsverfahren.[168]
Die Codierung war optimal, mit geringen Anpassungen erfüllte sie fast 100 Jahre alle Anforderungen der Nachrichtentechnik, besonders der Fernschreibtechnik.

4.1.2 Erste Fernschreiber

Anfang des 20. Jahrhunderts übertrugen in Post- und Telegraphenämtern installierte sog. Maschinen- bzw. Schnelltelegraphen Nachrichten mit hoher Geschwindigkeit, die meist nicht ausgenutzt werden konnte. Denn es blieb der zeitraubende Umstand, daß die Sendungen erst zu einem Telegraphenamt zu bringen, und, nach Empfang, durch Boten auszutragen waren. Das relativierte die Übertragungsleistung des gesamten Systems erheblich. Hinzu kamen die hohen Kosten, da jedes Wort bei der Gebührenberechnung zählte.
So dachten kommerziell orientierte Erfinder über Lösungen nach, wie dem abzuhelfen sei, und entwickelten über einige Zwischenstufen den Fernschreiber. Dessen Hauptvorteile waren: Eigenes Gerät im Hause, Bedienung durch Büropersonal, Empfang auch ohne Personal, Online-Betrieb, Ausgabe von Textseiten.

Eine solche Erfindung hatte wohl nur in den USA Aussicht auf Erfolg: Denn nur dort gab es dafür einen „Markt", weil jedermann gegen Gebühr Leitungskapazität mieten und darüber private Fernschreiber betreiben konnte. In Europa hingegen verhinderten bis 1929 Postmonopole jeden direkten privaten Informationsaustausch; die neuen Fernschreiber mußten in Postämtern installiert werden.

Der Australier Donald MURRAY stellte 1901 als Erster einen Fernschreiber vor: Er kombinierte das Baudot-Verfahren mit einem von ihm erfundenen automatischen Lochbandstanzer-Sender. Diesen versah er mit Tastatur und Blattschreiber, und zur Synchronisation der Übertragung diente ein Start-Stop-Verfahren. Damit

[167] Vgl. Müller, Telegraphie, S. 275.
[168] Zur gleichen Zeit (1874) erfand Edison ein Quadruplex-Verfahren, das sich jedoch nicht durchsetzte.

erfolgte die Synchronisation zwischen beiden Geräten automatisch bei jedem Start einer Zeichengenerierung. Das aber war die Voraussetzung für den Betrieb ohne Fachpersonal, das sonst für die Synchronisation zu sorgen hatte.
Ferner modifizierte er den für die 5er Fingerklaviatur optimierten Baudot-Code, weil er eine Schreibmaschinen-Tastatur für die Eingabe verwenden wollte und dazu die Lochung quer anordnete. Diese Modifikation bezeichnet man oft als „Baudot-Murray-Code."[169]

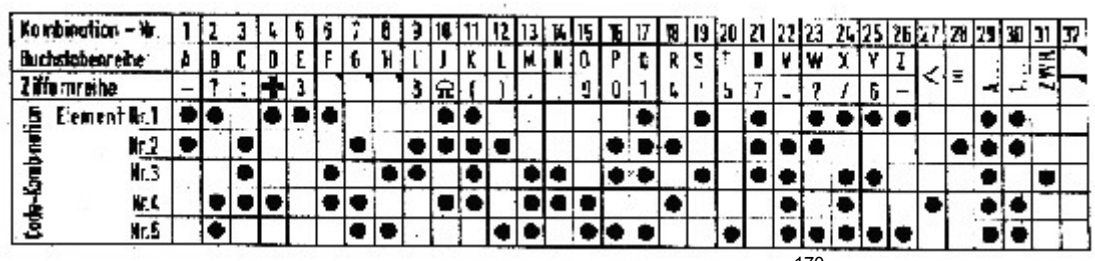


Bild 27: Baudot-Murray-Fernschreibcodierung[170]

Bild 27 zeigt einen vergrößerten Standard-Lochstreifen mit den 32 Codierungen nach der internationalen Norm CCITT-2 (ITA-2) von 1931.
Damit erhält man folgende Entsprechungen:

Code	Buchstabe	Zeichen (mit Shift)
11000	A	
10011	B	?
01110	C	:
usw.	usw.	usw.
10111	X	/
10101	Y	6
10001	Z	+
00010		Wagenrücklauf
01000		Zeilenvorschub
11111		Shift Buchstaben
11011		Shift Zeichen

MURRAY hatte keinen Erfolg mit seinen Erfindungen, vermutlich weil er die kommerziellen Umstände nicht erkannte, denn, wie erwähnt, nur in den USA konnte der Fernschreibers erfolgreich sein, weil kein Postmonopol dagegen stand. Er versäumte es, seine Erfindung in den USA patentieren zu lassen und konnte nur wenige Geräte an europäische Postverwaltungen verkaufen.

In den USA konkurrierten zwei Erfinder, deren jeweilige Patente beide für einen erfolgreichen Fernschreiber benötigt wurden: 1910 beantragte Howard KRUM ein Patent für das Start-Stop-Verfahren (das MURRAY bereits 1901 erfunden hatte,

[169] Vgl. Hobbs, Alan G.: Fiveunit codes. (NADCOMM -Museum 1999).
Von: http://www.nadcomm.com/fiveunit/fiveunits.htm, am 21.10.01.
[170] Bild nach Kuhlenkamp (Hrsg.): Lexikon der Feinwerktechnik. S. 319

s.o.), und 1916 E.E. KLEINSCHMIDT für einen Blattschreiber mit Tastatur, der mit Baudot-Murray-Code betrieben wurde. Beide Erfinder gingen zunächst getrennte Wege und entwickelten eigene Geräte, deren jeweilige Mängel einen Durchbruch verhinderten. Als 1918 KRUM'S Patent publiziert wurde, erkannte KLEINSCHMIDT dessen Vorteile und modifizierte sein Gerät entsprechend. Das führte zu einem Patentstreit, bis beide einsahen, daß nur die Kombination beider Erfindungen erfolgreich sein könne. So kam es zur Zusammenarbeit und Gründung der Morkrum-Kleinschmidt Co. in Chicago, die ab 1924 den ersten kommerziell erfolgreichen Fernschreiber „Teletype 14" herstellte.[171] Damit erst begann der Siegeszug des Fernschreibers, der bis in die 80er Jahre des 20. Jahrhunderts anhielt.

4.1.3 Deutsche Fernschreiber

In Deutschland verhinderte das bereits erwähnte Postmonopol zunächst weitere Entwicklungen. Die Lorenz AG importierte nach 1924 einige Teletype14-Geräte, installierte sie in Postämtern, und erwarb die Lizenzrechte für eine Produktion in Deutschland. Die Masse der Sendungen wurde jedoch wie bisher per Schnelltelegraphie übertragen.

Die zunehmende Besserung der wirtschaftlichen Verhältnisse vor der Weltwirtschaftskrise, und das US-Vorbild, erhöhten den Druck auf die Postmonopole. Das erzwang schließlich, in Deutschland 1929, die Freigabe der Fernschreibkanäle für private Nutzer. Zur gleichen Zeit verhandelte man auch die internationalen Normungen des Baudot-Murray-Codes. Nach Vornormen wurde in 1931 die internationale Norm CCITT-2 so vereinbart, daß man Fernschreibsendungen problemlos international austauschen konnte. Mithin war der Weg frei für den sog. TELEX-Verkehr, der sich bald durchsetzte.

Die bevorstehende Freigabe der Fernschreibkanäle veranlaßte vermutlich die Telegraphenbaufirma Siemens & Halske, die Produktion von Fernschreibern einzuplanen. Dazu begann man Verhandlungen mit der deutschen Lizenzinhaberin der Morkrum-Kleinschmidt Co., der Lorenz AG, doch man einigte sich nicht. So umging Siemens & Halske deren Patente mit der Entwicklung eines relaisgesteuerten Fernschreibers, als Alternative zum mechanischen Lorenzgerät. Dieses „Ttype 25"-Gerät präsentierte sie erstmals 1927.[172]

Die Lorenz AG stellte die in den USA weiterentwickelten Teletype 15-Geräte her, die als „Lo15" (T36) in 1932 als Standardgerät des Heeres übernommen und 1940

---

[171] Vgl. Nelson, A./Lovitt, K.M. (Ed.): History Of Teletype Development (Oct. 1963).
Von: http://www.thocp.net/hardware/history_of_teletype_development_.htm, am 13.3.02.

[172] Vgl. Mache, Wolfgang: The Siemens Cipher Teletype in the History of Telecommunationes.
In: Deavours, Cipher A. (Ed.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, S. 437-438.
(zukünftig zit.: "Mache, Siemens Cipher").

durch den Chiffrier-„Schlüsselzusatz“ Lorenz SZ40/42 ergänzt wurden. Diese Kombination erhielt im Krieg eine herausragende Bedeutung, die noch ausführlich zu diskutieren sein wird.

4.2 Das VERNAM-Verfahren

Der wahrscheinliche Kriegseintritt der USA (1917) veranlaßte die US-Army nach einer leistungsfähigen Nachrichtenverbindung mit Europa zu suchen, zu ihren dann dort zu stationierenden Truppen. Die damals verfügbare Funktelegraphie war dazu nicht geeignet, zu unsicher und leistungsschwach waren die Verbindungen. Die mögliche Telegraphie über das Unterseekabel war ebenso in der Leistung begrenzt und man mußte außerdem die Nachrichten umständlich per Hand verschlüsseln, da man Anzapfungen des Kabels befürchtete.

4.2.1 Die Fernschreiber-Chiffrierung

Die damals größte US-Fernmeldegesellschaft, die American Telegraph & Telefon Co. (AT&T) sollte daher prüfen, ob einer der neuen Fernschreiber[173] für die Army geeignet und abhörsicher sei, und insbesonders umständliche Verschlüsselungsprozeduren damit entfallen könnten. Mit dieser Untersuchung beauftragte AT&T den jungen (27jährigen) Fernmeldeingenieur Gilbert VERNAM. Bald konnte er nachweisen, daß die Fernschreibimpulse per Oszillograph aufgezeichnet und rekonstruiert werden können, auch wenn Multiplex-Übertragung angewendet würde.
Er befaßte sich intensiv mit den Anforderungen der Army und hatte dann die Idee, dafür eine sichere Übertragung (*secret signaling*) zu entwickeln, die er 1918 zum Patent anmeldete.[174]
Dazu verknüpfte er elektromechanisch die Baudot-Codierung des Klartextes mit einem Schlüsseltext, und erhielt so einen Geheimtext. Das erreichte er durch gleichzeitige Abtastung von zwei Fernschreiber-Lochbändern, von denen das eine den Klartext, das andere (als Endlosschleife) den Schlüsseltext enthielt. Das Ergebnis nach der Umsetzung per Relaislogik – den Geheimtext – stanzte ein Bandlocher in ein drittes Band, das direkt gelesen und gesendet werden konnte.
Dieses Verfahren, später nach VERNAM benannt, beruhte auf der technischen Umsetzung der Boole’schen Logikoperation „Exklusiv-Oder“, die in der Literatur überwiegend mit XOR, XORing, bzw. XORed. (engl.) abgekürzt wird. Sie beruht auf einem Sonderfall der polyalphabetischen Verschlüsselung: Der Fernschreibcode bestand aus einem binären Alphabet, das bitweise verarbeitet

[173] In der Literatur wird nirgends angegeben, welches Gerät geprüft wurde. Nach Meinung des Verf. kam wegen der Baudot-Codierung nur das Kleinschmidt-Gerät in Frage, dessen Synchronisierung allerdings Fachpersonal erforderte.

[174] US-Patent and Trademark Office, US-Patentschrift 1,510,441.
Von: http://www.uspto.gov/patft/help/.htm, am 16.01.02.

werden konnte. Da es im binären System nur die Werte 0 und 1 gibt, müssen bei der Addition der Impulse höhere Werte umgesetzt werden. Das erreicht man mit modularer Addition, bei der 1+1 nicht 2 ergibt, sondern – bei modulo 2 – nur 0, eine Methode, die beispielsweise bei der Summierung von Uhrzeiten ebenso angewendet wird.[175] Diese binäre Addition modulo 2 fällt aber genau mit Boole's Logikoperation „Exklusiv-Oder" zusammen, die sich elektromechanisch nachbilden läßt.

Freilich wird VERNAM dieser theoretische Hintergrund kaum bekannt gewesen sein, denn mit Boole's Algebra und modularer Arithmetik befaßten sich damals nur wenige Gelehrte. So entwickelte er die dazu erforderliche Relaislogikschaltung empirisch, und das so perfekt, daß sie ebenso in den späteren Chiffriermaschinen und deren kryptanalytischen Gegengeräten verwendet werden konnte.

Die Schaltlogik (0 = Strom aus, 1 = ein) lautet:

```
0 XOR 0  =  0
0 XOR 1  =  1
1 XOR 0  =  1
1 XOR 1  =  0
```

Nach Vernam's Verfahren werden zwei Fernschreiber-Lochstreifen gleichzeitig gelesen, die Impulse mit dieser Logikoperation verknüpft und damit chiffriert.

Sender:

```
   Klartext: 00101100010.......11011100101011 1. Lochstreifen
  Schlüssel: 01110111010.......10001011101011 2. Lochstreifen(Schleife)
       XOR : ----------------------------------------------------------
Geheimtext: 01011011000.......01010111000000 3. Lochstreifen/Senden
```

Dieser Geheimtext wird nun gesendet. Die Entschlüsselung beim Empfänger ist einfach, weil die XOR-Operation völlig reziprok ist, denn die empfangene Sendung wird in gleicher Weise mit dem Schlüssel XORed.

Empfänger:

```
Geheimtext: 01011011000.........01010111000000  1. Lochstreifen
 Schlüssel: 01110111010.........10001011101011  2. Lochstreifen
      XOR :-----------------------------------------------------
  Klartext: 00101100010.........11011100101011        Ausdruck
```

Für dieses empirisch entwickelte Verfahren interessierte sich die US-Army und ließ es bald wissenschaftlich prüfen und verbessern:

[175] Eine gut verständliche Erläuterung der Modul-Arithmetik bietet Singh, Geheime Botschaften, S. 316 ff.

4.2.2 Die Schlüsselgenerierung

Vernam's Verfahren bot zwar eine technisch elegante Lösung des Chiffrierproblems, weil die automatische Verschlüsselung Fehler verhinderte und überdies online nutzbar war. Doch eine Schwierigkeit blieb, nämlich die Bereitstellung geeigneter Schlüsselbänder. VERNAM glaubte zunächst, er könne eine Endlosschleife mit Zufallstext immer wieder als Schlüssel verwenden, die bei Sender und Empfänger vorhanden sein mußte. Doch sein Army-Gesprächspartner Major MAUBORGNE, ein erfahrener Kryptologe (und später *Chief Signal Officer* der Army), konnte ihn jedoch überzeugen, daß selbst ein echter Zufallstext die Chiffrierung schwächt, wenn er mehrfach verwendet wird. Abhilfe schien ein Verfahren zu bringen, das Vernams Kollege MOREHOUSE vorschlug: Die Hintereinanderschaltung von zwei Schlüsselbändern, mit entsprechender Verlängerung der Schlüsselsequenz. Doch bei Versuchen bewies der Army-Kryptologe William FRIEDMAN die Schwäche auch dieser Methode und entzifferte rasch die Geheimtexte.

Bild 28: US-Army Kryptologe Friedman prüft das Vernam-Verfahren[176]

Doch ein Geheimtext widerstand allen seinen Versuchen: Dieser war chiffriert mit einem Schlüsselband, das nur für diese spezielle Verschlüsselung verwendet worden war. Es war die erste Einmalschlüssel-Chiffrierung.[177]

William FRIEDMAN (1891-1969) gilt als bedeutendster Kryptologe seiner Zeit. Er wurde im Ersten Weltkrieg Army-Kryptologe und 1929 Mauborgne's Nachfolger als *Chief Signal Officer*, hatte sehr wichtige (teils geheime) theoretische Beiträge zur Kryptologie erarbeitet und US-Chiffriermaschinen nahezu unbrechbar verbessert.

Welcher der Beteiligten an den Versuchen dann vorschlug, das Schlüsselband nur einmal zu nutzen und dann sicherheitshalber nach Gebrauch zu vernichten, ist

[176] Bild nach HNF/Ryska, Vortrag Kryptologie. © The Friedman Collection, George C.Marshall Research Foundation.
[177] Vgl. Kahn, Codebreakers, S. 401.

nicht genau bekannt; KAHN schreibt das Major MAUBORGNE zu.[178] Es war die Erfindung des unbrechbaren „One-Time-Pad"-Verfahrens (OTP), wie es später genannt wurde, und unter 4.5 näher erläutert ist. Das wurde freilich wegen der aufwendigen Schlüssel-Logistik von der Army als nicht verwendbar angesehen, ebenso konnte es AT&T nicht erfolgreich vermarkten.

Doch MAUBORGNE'S Chef, Col. Parker HITT[179], fand für das Problem der Schlüssel-Generierung eine praktikable Lösung: Er erzeugte Pseudo-Zufallsfolgen durch ein Rad, in das Stifte vom Operator beliebig eingesteckt werden konnten, und das mit jedem vom Fernschreiber generierten Buchstaben einen Schritt weiter geschaltet wurde, vergleichbar einem Hagelin-Schlüsselrad. Diese Stifte betätigten einen Schalter, der entsprechend dem Muster der gesetzten Stifte eine Bitfolge erzeugte. Um die erforderliche Schlüssellänge zu erreichen, schaltete HITT zwei Räder mit Primzahl-Stiftfolgen hintereinander, und für jeden der fünf Kanäle des Baudot-Codes einen Radsatz. Damit erhält man eine Schlüsselperiode von $6{,}21 \times 10^{16}$ nach GOEBEL.[180] Dieser Wert entspricht ungefähr dem einer ENIGMA-Maschine.

4.2.3 XOR und aktuelle Computer-Kryptologie

Die XOR-Operation ist auch eine Grundlage der heutigen Computer-Kryptologie: Aktuelle Chiffrierverfahren, wie z.B. Stromchiffrierungen, sind, informatikhistorisch betrachtet, Weiterentwicklungen des Vernam-Verfahrens, denn in gleicher Weise wird ein Schlüssel mit dem Klartext XORed, und ebenso der Klartext aus dem Geheimtext per XOR zurückgewonnen. Der Unterschied liegt in der Schlüsselgenerierung und -verarbeitung, die heute computerunterstützt freilich weitaus mehr leistet, denn sehr komplizierte mathematische Operationen sorgen für kryptologisch sichere Algorithmen. Beispielsweise gelten 128bit-Chiffrierungen wie IDEA (u.a. Bestandteil von PGP zur eMail-Verschlüsselung) als derzeit praktisch nicht brechbar: Eine *brute-force-attack* (Durchtesten aller Schlüssel) zur Entzifferung würde mit einem aktuellen Hochleistungs-Parallelrechner ca. 10^{13} Stunden dauern.[181]

Gleichwohl besteht theoretisch die Möglichkeit zur Kryptanalyse, denn SHANNON'S Bedingung, nämlich die *echt zufällige* Schlüsselgenerierung, ist nicht erfüllt, und überdies könnten auch Informationen zum Text auf anderen Wegen beschafft werden (s. 4.5.1). Die Geheimdienste, besonders die NSA, stehen deshalb immer unter Verdacht, möglicherweise mehr zu wissen und/oder zu können, als öffentlich bekannt ist.

---

[178] Vgl. Kahn, Codebreakers, S. 397.
[179] Er publizierte 1916 das erste grundlegende Buch über Kryptologie in den USA.
[180] Vgl. Goebel, G.: Codes, Ciphers, & Codebreaking, [9.1] Telecipher Systems.
[181] Vgl. Eckert, Claudia: IT-Sicherheit. München 2003.

4.3 Der „Geheimschreiber“ Siemens T52

Die Online-Chiffrierung

Nachdem der erste deutsche Fernschreiber von Siemens & Halske angeboten wurde, meldete sich auch der erste Interessent: Die deutsche Marine. Doch deren Verantwortliche waren wohl immer noch betroffen von den Entzifferungserfolgen der Briten im Ersten Weltkrieg und forderten deshalb eine Chiffriervorrichtung für die Maschine. Das war damals ein völlig neuer Gedanke, denn alle Nachrichten wurden vorher separat und manuell chiffriert, und erst dann gesendet. Nach MACHE war es die erste bekannte Idee einer online-Chiffrierung.[182] Doch konnte bereits VERNAM mit seinem Verfahren online chiffrieren, ohne daß damals diese Möglichkeit expressis verbis angegeben wurde.

Als ersten deutschen Fernschreiber mit Chiffriervorrichtung baute Siemens & Halske den „Doppelabtaster mit Mischer“, über den kaum etwas bekannt ist. Nach BAUER[183] wurde VERNAM'S Idee „aufgegriffen“; man muß demnach einen Nachbau des Vernam-Verfahrens annehmen, der dem neuen Siemens-Fernschreiber Ttyp 25 angepaßt war. Ob dabei ein OTP-Verfahren angewendet wurde, oder aber die Schlüsselbänder mehrfach genutzt wurden, ist nicht bekannt.

Die umständliche Schlüsselgenerierung und -verwaltung dieses Systems wurde vermutlich von den potentiellen Kunden nicht akzeptiert, was der Siemens-Entwickler A. JIPP bei Gesprächen mit den Interessenten wohl erfahren haben wird. Das brachte ihn und seinen Kollegen ROSSBERG auf die brillante Idee, einen Fernschreiber mit *eigener* Schlüsselgenerierung zu konstruieren, der *online* nutzbar war. Davon versprach man sich eher einen kommerziellen Erfolg, der sich später aber nicht wie gewünscht einstellte, da die Sicherheitsbehörde 1934 die Maschine unter Geheimschutz stellte und danach nur noch militärische bzw. hoheitliche Verwendung möglich war.

Der erste Geheimschreiber

Das Siemens-Entwicklungsteam unter JIPP und ROSSBERG konnte bereits am 18.7.1930 das erste offene Patent[184] für eine „Anordnung zur Nachrichten-übermittlung in Geheimschrift über Telegraphenanlagen“ anmelden. Es bestand aus einer separaten Chiffriereinrichtung, die mit dem Fernschreiber Ttyp 25 gekoppelt wurde, jedoch nur eine einfache Tauschoperation der Buchstaben ausführen konnte. Das aber genügte dem von der Reichswehr – einem wichtigen Interessenten – zu Siemens & Halske abgeordneten Nachrichtenoffizier HETTLER

[182] Vgl. Mache, Wolfgang: The Siemens Cipher Teletype in the History of Telecommunationes. In: Deavours, Cipher A. (Ed.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, S. 442.
[183] Vgl. Bauer, Geheimnisse, S. 137.
[184] DRP 615016 vom 18.7.1930.

nicht, er forderte und erreichte ein zusätzliches Verwürfeln des Chiffrats, wofür er ein Nebenpatent[185] erhielt. Diese verbesserte Maschine meldeten die drei Erfinder sogleich in den USA zum Patent[186] an, weil man sich vom großen US-Markt gute Geschäfte versprach. Und nach einigen weiteren Verbesserungen entstand 1932 der erste T52 als Kompaktmaschine, indem der Chiffrierzusatz um den ebenfalls neuen Fernschreiber Ttyp 36 angeordnet wurde.[187] Die Maschine war zunächst frei verkäuflich, wurde aber 1934 unter Geheimschutz gestellt.[188]

Für die Maschine findet man in der Literatur verschiedene Bezeichnungen: Populär wurde der inoffizielle Begriff „Geheimschreiber", auch „G-Schreiber", der freilich in Dokumenten nicht zu finden ist. Das Herstellerwerk selbst verwendete „Geheimfernschreibmaschine Ttyp 52", und ab 1934 lautete die amtliche Bezeichnung der Sicherheitsbehörden in Druckschriften „Geheimzusatz der Siemens-Fernschreibmaschine T.typ.52". Schließlich wurde 1942 die Bezeichnung „Schlüsselfernschreibmaschine bzw. SFM T52" vorgeschrieben und einheitlich verwendet.[189]

Die Marine übernahm bereits 1932 als erste Militäreinheit die Maschine, beanstandete jedoch Störimpulse, die deren zahlreichen Relais erzeugten und den Funkverkehr beeinträchtigten, denn die Maschine wurde auch an Bord von Schiffen in Häfen verwendet, und war dort an das Fernschreibfestnetz per Verlängerungskabel angeschlossen. Dementsprechend erhielt die Maschine eine Funkentstörung und die Bezeichnung T52b, um sie besser unterscheiden zu können von der T52a, dem kryptologisch identischen Gerät. Später verwendete OKW/Chi die einheitliche Bezeichnung T52a/b in den entsprechenden Vorschriften, die ebenso in der Literatur üblich wurde, obwohl es a- bzw. b-Maschinen bis Kriegsende gab.[190]

Die Luftwaffe beabsichtigte die T52 ebenfalls zu übernehmen, forderte aber einige Verbesserungen, die sie 1936 für das spätere Modell T52c spezifizierte, das aber erst ab 1941 ausgeliefert und später auch vom Heer eingesetzt wurde.[191]
Zu ergänzen ist hierzu, daß die Maschine T52 für die Verwendung auf Kabelstrecken ausgelegt war und sich auch nicht für Funkübertragungsverfahren eignete. Denn diese erzeugten damals viele Störkomponenten, die den kryptologischen Prozeß beim Empfang der Sendung außer Tritt bringen konnten. Dieses Synchronisationsproblem konnte später (in 1942) mit einer optimierten Lochstreifenabtastung in der T52c besser beherrscht werden, deren gleichmäßige Impulse durch Störungen nicht mehr leicht außer Takt gebracht werden

[185] DRP 591974 vom 11.10.1930.
[186] US-Patent 1,912,983 vom 16.7.1931.
[187] Vgl. Mache, W.: Der Siemens-Geheimschreiber – ein Beitrag zur Geschichte der Telekommunikation. Archiv für deutsche Postgeschichte 1991, S. 86-88. (zukünftig zit.: „Mache, Geheimschreiber").
[188] Gem. § 88 RGB, Fassung vom 24.April 1934. Nach Mache, Korrespondenz.
[189] HDvg 422 „Schlüsselfernschreibvorschrift" des OKW, gültig ab 1.12.42. Archiv Mache.
[190] Nach Mache, Korrespondenz: Es wurden nicht alle a/b-Maschinen zu T52d umgebaut.
[191] Vgl. Mache, Siemens Cipher, S. 445.

konnten.[192] Diese Maschinen kamen im Sommer 1942 zum Einsatz; gleichzeitig registrierte man in BP die ersten T52c-Funkfernschreibsendungen, deren Chiffrierung „STURGEON“ genannt wurde.[193] Diese Bezeichnung verwendete BP dann für den Verkehr aller T52-Varianten, die im Funkfernschreibdienst eingesetzt wurden.

Varianten

Die Schlüsselperiode der T52 betrug 8,9 x 10^{17}, lag also in der Größenordnung einer ENIGMA I. Doch analog zur ENIGMA besagen diese theoretischen Werte wenig über die tatsächliche Sicherheit: So soll in der Abteilung Chi des Heeres ein dienstverpflichteter Mathematiker („Gefreiter SCHULZ“) den Algorithmus der Maschine mathematisch analysiert haben.[194] Und kurz vor Kriegsbeginn beanstandete der OKW/Chi-Kryptologe HÜTTENHAIN (s.u.) die mangelhafte Sicherheit der Maschine).
Die späteren Verbesserungen der Maschine durch das Herstellerwerk erhöhten nur wenig die Sicherheit, wie die Entzifferungen zeigen, und kryptologische Beratung scheint dazu ebenso nicht angefordert worden zu sein: Das Luftwaffenmodell T52c („Cäsar“) rüstete man auf mit einer Relaislogik, mit der man den Ausgangswert der 10 Nockenräder permutieren konnte, sowie eine Vorrichtung zur Eingabe eines Spruchschlüssels. Doch die starre Anordnung und Bewegung der Nockenräder blieb unverändert. Diese Maschine wurde ausdrücklich zugelassen für Kabelsendungen über das neutrale Ausland, ebenso wie die Maschine SZ42. Der Hintergrund dieser Anordnung war: Nachdem über den finnischen Militärattaché die schwedische Brechung der T52a/b bekannt wurde (Juni 1942), durfte diese Maschine nur noch in von der Wehrmacht kontrollierten Gebieten verwendet werden, so die in der Literatur bisher übliche Darstellung.[195] Doch OKW/WNV wußte bereits Anfang Februar 1942 von der „...mangelnden Schlüsselfestigkeit des derzeit verwendeten Geheimschreibers“, und man ließ deshalb die [T52a/b]-Verbindung nach Bukarest stillegen.[196] Das hielt man offenbar geheim gegen andere Dienststellen (s. dazu 5.4.3), denn Reaktionen darauf sind nicht bekannt – die Maschine blieb bis Juli 1942 im Einsatz für Geheimsendungen.

Der größte Teil der T52a/b-Maschinen wurde dann ab 1943 umgebaut zur „Dora“-Maschine T52d mit pseudo-unregelmäßiger Walzenfortschaltung, wobei die Weiterschaltung eines Nockenrades von der Polarität der vorherigen abhing. Eine verbesserte unregelmäßige Fortschaltung per Relaislogik erhielten dann

[192] Nach Mache, Korrespondenz. Es ist nicht bekannt, wie dieser Zusatz arbeitete. Vermutlich war es ein sog. „Entzerrer“, der die Impulse synchronisierte.
[193] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 1.
In: Proceedings on Coding Theory and Cryptography, New York (NY) 2000.
[194] Vgl. Mache, W.: Der Siemens-Geheimschreiber, S. 88.
[195] So auch Weierud in: Sturgeon, The Fish BP Never Really Caught, S. 16.
[196] Nach einer Notiz des Präsidenten der Reichspost-Forschungsanstalt vom 17.2.1942.
BArch, R 4701/18314.

1944 die T52c-Maschinen beim Umbau zur T52e („Emil“). An beiden Maschinen konnte eine zuschaltbare, fest verdrahtete Klartextfunktion aktiviert werden, wobei je nach Polarität des dritten Klartextschrittes die Fortschaltung von zwei Nockenwalzen gestoppt wurde.[197] Allerdings verwendeten die Operatoren diese Funktion selten, denn schon durch geringe Störungen der Übertragung auf Funkstrecken konnte die Synchronisation dabei verlorengehen; ab September 1944 wurde deren Verwendung sogar untersagt.

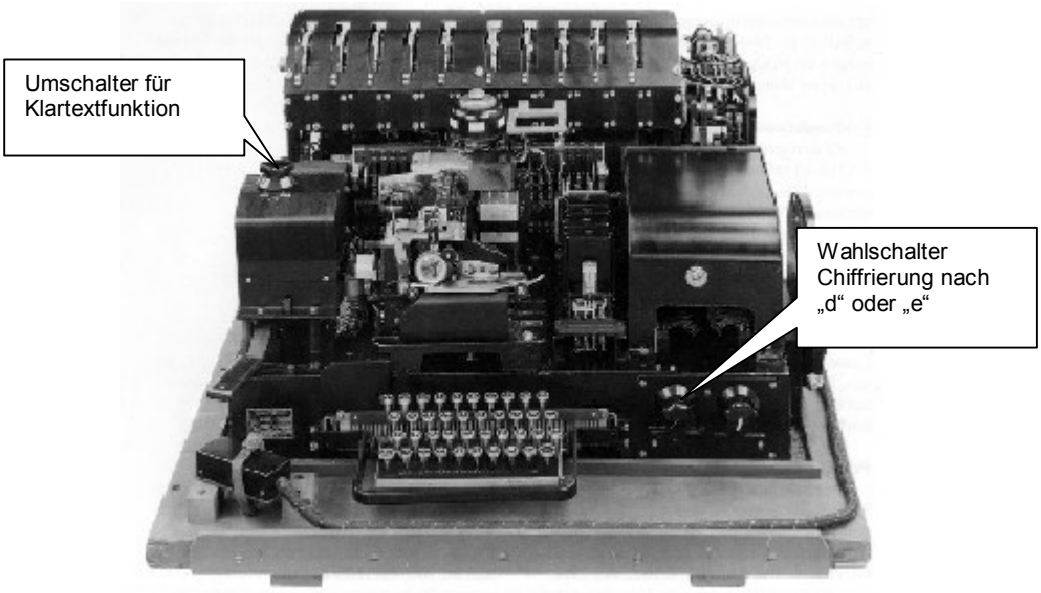


Bild 29: Siemens SFM T52(c)e[198]

Weitere Funktionsvarianten

Der elektromechanische Aufbau der Maschine eignete sich sehr gut für Modifikationen, weil man die innere Verdrahtung mühelos verändern konnte. Eine solche Variante registrierte BP im März 1943, die als „adaptierte“ T52c bezeichnet und dementsprechend „T52ca“ im entzifferten Nachrichtenverkehr genannt wurde; diese Bezeichnung änderte sich jedoch im Juni 1943 wieder zu T52c.[199] Nach MACHE änderte man dazu in der Maschine T52c die feste Verdrahtung der mit dem Steckerfeld des „Grundschlüssels“ verbundenen Relais.[200] Diesen Grundschlüssel bildete ein 10er Steckerfeld, womit die Zuordnung zu den Relais durch Stecker monatlich gewechselt wurde.

In gleicher Weise sollen auch andere Dienststellen des Dritten Reiches die Maschinen verändert haben, darunter HITLERS Sekretär BORMANN für sein geheimes Nachrichtennetz, nachdem 1943/44 in HITLERS Hauptquartier

[197] Vgl. Mache, Geheimschreiber, S. 88-90.
[198] Bild nach Weierud, F.: Frode's Crypto Page, The Siemens and Halske T52d. (Diese Bezeichnung ist nicht korrekt, es handelt sich um eine T52c-Maschine, die nach e umgebaut wurde).
[199] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 15.
[200] Mache, Korrespondenz, mit Bezug auf B. Beckmann, „Svenska Kryptobedrifter“, 1996.

„Wolfsschanze“ eine undichte Stelle vermutet wurde. Der Schutz gegen den „inneren Feind“ – den zunehmenden Widerstand – und die Abschottung gegen andere Organisationen erhielt damals eine immer größere Bedeutung im Dritten Reich.[201]

Nach dem Krieg wurden zahlreiche erbeutete T52-Maschinen von einer deutschen Fachfirma in Trier instant gesetzt und bis mindestens 1960 weiterverwendet, vor allem in Frankreich. Die T52e-Maschinen erhielten dabei eine bereits während des Krieges entwickelte erweiterte Klartextfunktion (T52f), wobei nun fünf Stellungen wählbar waren.[202]
Es gab auch eine norwegische Modifikation, ähnlich verändert, die vom norwegischen Sicherheitsdienst bis in die 60er Jahre benutzt wurde.[203]

4.4 Schlüsselzusatz (G-Zusatz) SZ42

Diese Maschine erlangte insofern besondere technikhistorische Bedeutung, weil zu deren Brechung die ersten betriebssicheren elektronischen Rechner entwickelt wurden. Das rechtfertigt eine ausführlichere Betrachtung.

Geschichte

Die geheime Entwicklung der Maschine begann vermutlich mit der Absicht, ein Zusatzgerät zu den bereits in großer Zahl beim Heer verwendeten mechanischen Fernschreibern Lorenz Lo15 zu bauen, und dieses sollte ebenso mechanisch arbeiten. Wie im deutschen Heer üblich, formulierte das Heeres-Waffenamt (Abt. WA Prüf 7) in 1937 die Vorgaben, und nicht etwa die sachkundigen Kryptologen von OKW/Chi.[204] Und die Firma Lorenz AG übernahm den Entwicklungsauftrag, obgleich auch sie über keine kryptologische Kompetenz verfügte.

Diese Vergabe lag nahe, denn die Lorenz AG stand in der Tradition mechanischer Fernschreiber, die sich beim Heer bewährt hatten. Diese Geräte baute die Lorenz AG ab 1925 unter Lizenz der Morkrum-Kleinschmidt Corp./USA (s. dazu 4.1.2). Überdies sparte das Heer mit dieser Entwicklung Kosten, denn neue Schlüsselfernschreibmaschinen T52a/b wären erheblich teurer gewesen. Aber auch deren Eigenschaften könnten die Neuentwicklung mit veranlaßt haben:
Das deutsche Heer setzte die Maschine T52a/b nur auf Kabelstrecken ein, weil Versuche ergeben hatten, daß diese für Drahtverbindungen konstruierte

[201] Nach Mache, Korrespondenz.
[202] Stichwort „Geheimschreiber“ in: Mache, W. (Hrsg.): Lexikon der Text- und Daten-Kommunikation, S. 185-186. Zusätzliche Angaben Mache, Korrespondenz.
[203] Vgl. Selmer, E.S.: The Norwegian Modification of the Siemens T52e. In: Cryptologia Vol. XVIII (2), April 1994.
[204] TICOM 1-45: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines. Written by Huettenhain and Fricke, 1.8.1945.

Maschine bei der im Heeresdienst wichtigen Funkübertragung zu Synchronisationsfehlern neigte. Die Marine verwendete sie ebenso nur in ihren durch Kabel verbundenen Hauptstellen (Kommandostellen, Häfen etc.).

Um dennoch die neue Maschine auf Funkstrecken einsetzen zu können, erhielt sie eine Synchronisiereinrichtung („Gleichlaufzusatz"), und war vorgesehen für die Kommunikation der obersten Führungsebene (Führerhauptquartiere, OKW, OKL, Heeresgruppen, Luftflotten). Dementsprechend sollte sie für „Geheime Kommandosachen" sicher sein. Die offizielle Bezeichnung lautete „Schlüsselzusatz" (= SZ40), im Truppendienst auch „Geheimzusatz" oder „G-Zusatz", da das Gerät, wie erwähnt, nur ein Zusatz zum vorhandenen Lo15-Fernschreiber war.

Das Entwicklungsteam der Lorenz AG, unter Leitung des Physikers GRIMSEN, bestand aus Fernmeldeingenieuren, die eine technisch exzellente Maschine konstruierten. Doch diese muß aus kryptologischer Sicht der Empirie zugeordnet werden, denn wissenschaftlich-kryptologische Beratung hielt man scheinbar für entbehrlich, zumindest fehlte sie bei der nachstehend beschriebenen ersten Variante „SZ40 alt" .

Der erwähnte Bericht[205] beschreibt verschieden Varianten, die im Laufe der Zeit entwickelt und in Dienst gestellt wurden, über die aber wenig bekannt ist. Daher beziehen sich alle weiteren Angaben stets auf die Version SZ42, die untersucht werden konnte, da drei dieser Maschinen dem Zerstörungsbefehl am Kriegsende entgingen und von alliierten Truppen erbeutet wurden. Die Bezeichnung SZ42 ist in der Literatur üblich, stimmt jedoch nicht mit der offiziellen deutschen überein (s. „Varianten").

[205] TICOM 1-45: OKW/Chi Cryptanalytic Research.

Bild 30: LORENZ SZ42 – Chiffrierzusatz zum LORENZ-Fernschreiber[206]
(Schlüsselräder-Abdeckung offen)

Technik

Die Maschine wurde in die Verbindungsleitung des Fernschreibers zur Anschlußstelle eingeschleift. Sie verarbeitete die Signale fast ausschließlich mechanisch, im Gegensatz zur vorbeschriebenen T52, die eine Relaismaschine war. Die Impulsfolgen mußten für den online-Betrieb genau eingehalten werden, dafür sorgten abgestimmte mechanische Speicher und Kupplungen, die diskontinuierlich arbeiteten. Man kann sich vorstellen, wie diffizil diese Konstruktion aufgebaut war, und mit welcher Sorgfalt die Wartung und Justierung der komplizierten Mechanik vorgenommen werden mußte.[207]

[206] Bild nach Sale, Codes and Ciphers, The Lorenz Cipher, Page 1.
[207] Detaillierte Beschreibung s. Davies, The Lorenz Cipher Machine SZ42, S. 517-537.

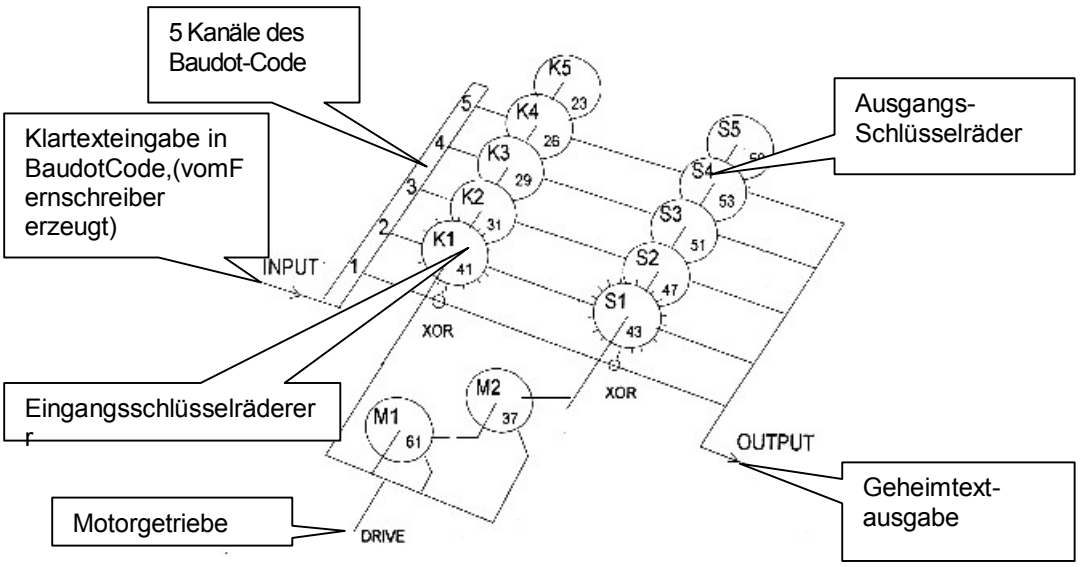


Bild 31: mechanisches Schema des SZ42-Schlüsselerzeugers[208]

Die Maschine verarbeitete die im Fernschreiber generierten Klartextimpulse des Baudot-Codes kanalweise in 2 Stufen: In der ersten setzten die Schlüsselräder K1-K5 (*Chi-wheels*) mit unterschiedlichen Primzahlen die Buchstabenimpulse per XOR um, sie bewegten sich nach jedem Buchstaben einen Schritt weiter. Die zweite Reihe Schlüsselräder S1-S5 (*Psi-wheels*) wiederholte diese Operation, jedoch mit den nachstehend beschriebenen pseudo-zufälligen Unterbrechungen.

Jedes Rad hatte 50 Einstellmöglichkeiten: 50 Schaltstifte auf dem Rad waren wahlweise „aktiv" oder „aus" zu setzen und generierten damit eine Binärsequenz, welche die XOR-Operation jedes Rades bestimmte. Diese Einstellungen wurden in bestimmten Intervallen geändert: K-Räder monatlich, ab 1.9.1944 täglich, S-Räder vierteljährlich, dann monatlich.
Damit konnten nach SALE[209] bis zu 10^{19} Schlüssel [theoretisch] generiert werden.
Zur Verbesserung der Sicherheit diente ein Motorgetriebe, das pseudozufällige Schrittbewegungen der 2. Schlüsselradgruppe bewirkte über zwei ebenso einstellbare Schlüsselzahnräder M1/61 und M2/37 („*motor-wheels*"): Das größere Rad M1/61 bewegte sich gemeinsam mit der ersten Schlüsselradgruppe K1-K5, bis der aktiv gesetzte Schaltstift auf dem 61er Rad schaltete, und damit das kleinere M2/37 in Bewegung setzte, bis dessen aktiv gesetzter Schaltstift die Ausgangsräder S1-S5 *gemeinsam* einen Schritt bewegte. Die Getriebeübersetzung wurde täglich gewechselt, weil man glaubte, Analysen damit besser verhindern zu können. Das war ein Irrtum, denn die Pseudo-Irregularität in der Bewegung der Schlüsselräder war tatsächlich definiert periodisch und konnte jeweils mathematisch rekonstruiert werden.[210]

[208] Bild nach Sale, Codes and Ciphers, The Lorenz Cipher, Page 1.
[209] Sale, Codes and Ciphers: Colossus, Lecture given at the IEEE, 18th February 1999.
[210] S. dazu 5.3.2.

Beim Empfang durchlief der Geheimtext dieselbe Prozedur; mit der gleicher Einstellung der Schlüsselräder wurde der Klartext zurückgewonnen – die Maschine war reziprok. Die Räder wurden vor jeder Chiffrierung eingestellt und diese Einstellung dann per Spruchschlüssel zur Gegenstelle gesendet, wo vor Empfang die gleiche Einstellung vorzunehmen war.

Varianten

Nach dem Bericht[211] der OKW/Chi-Kryptologen durchlief die Maschine mehrere Entwicklungsphasen, die bisher nur z.T. bekannt waren und hier erstmals im Zusammenhang dargelegt werden. Die darin verwendeten Bezeichnungen der Varianten stimmen nicht immer mit denen in der Literatur verwendeten überein:

- „SZ 40 (alt)“

Diese erste Version verschlüsselte die Impulse des Baudot-Codes durch je zwei hintereinandergeschaltete Schlüsselräder, die wie vorbeschrieben angeordnet waren. Die vorderen Räder bewegten sich mit jedem Buchstaben einen Schritt weiter, die hinteren ebenso, denn es gab keine pseudo-zufällige Bewegungen der Schlüsselräder per Getriebeübersetzung, wie bei den Folgemodellen. Diese Anordnung ist kryptologisch schwach, denn ein Geheimtext bereits ab 1000 Buchstaben war entzifferbar. [Das demonstriert die mangelnden kryptologischen Kenntnisse der Entwickler aus der Fernmeldetechnik, die empirisch vorgingen, und ebenso die fehlende Einsicht des Auftraggebers, des Heereswaffenamtes, hierzu wissenschaftliche Beratung durch Kryptologen anzuordnen].
Es sollen davon nur ca. 40 Maschinen produziert und eingesetzt worden sein, und nach Erkenntnis ihrer Schwäche nur auf kontrollierten Kabelstrecken.

- „SZ 40“

Diese Variante ist lt. Bericht[212] identisch mit der vorbeschriebenen SZ 42. Das erklärt auch, warum in der Schlüsselfernschreibvorschrift[213] vom 1.12.1942 ebenfalls die Bezeichnung „SZ 40“ verwendet wurde. Mithin scheint die falsche Bezeichnung SZ42 erst in der Literatur üblich geworden zu sein.
Der Wechsel von SZ40alt zu SZ40(42) erfolgte offenbar Ende 1941, denn zu diesem Zeitpunkt registrierte man in BP eine wesentliche Erschwernis des TUNNY-Algorithmus, wie diese Verschlüsselung genannt wurde, die man jedoch mit den inzwischen gemachten Erfahrungen bewältigen konnte.[214]

---

[211] TICOM 1-45: OKW/Chi Cryptanalytic Research.
[212] Ebd.
[213] S. Anm 189.
[214] Vgl. Wylie, Shaun: Breaking Tunny and the Birth of Colossus. In: Erskine, Ralph and Smith, Michael (Eds.): Action this Day.

• „SZ 42a“ und b

Die Schwäche der SZ 40/42-Konstruktion – pseudoirreguläre *gemeinsame* Bewegung aller Ausgangs-Schlüsselräder – erkannte man später und entwickelte Funktionsvarianten zur Verbesserung: Verschiedene Klartextfunktionen beeinflußten die Bewegung der nachgeschalteten Schlüsselräder, analog der Beeinflussung durch die Getrieberäder. (Der Wechsel von SZ42a zu 42b hatte – folgt man dem Bericht[215] – keine kryptologische Bedeutung, sondern erfolgte aus technischen Gründen).

In BP nannte man diese Klartextfunktionen *limitations*: Nach DAVIES registrierte BP die erste *limitation* („Chi-2“) im Februar 1943.[216] Doch das scheint keine Klartextfunktionen gewesen zu sein, nur eine Verbesserung des Stopverfahrens des Motorgetriebes wurde eingeführt, dessen Details nicht bekannt sind.[217]

Die nächste Erschwernis („P5“) war eine echte Klartextfunktion, wobei der 5. Klartext-Buchstabe die Bewegung der Schlüsselräder beeinflußte. Diese *limitation* wurde erst allmählich bei den Funkfernschreiblinien eingeführt: Die erste Verwendung stellte BP fest im März 1943, dann weitere im Dezember 1943, und schließlich auf allen Strecken im Februar 1944. Diese Funktion erschwerte erheblich die Entzifferung, die aber mit Hilfe des COLOSSUS I allmählich wieder gelang. Doch die Synchronisationsprobleme bei der Verwendung der P5-Funktion, die immer wieder die Übertragungen behinderten, zwangen die Verantwortlichen zur Anordnung, P5 ab Ende ab September 1944 nicht mehr zu verwenden.

Im Juni 1944, nach der Invasion, registrierte BP eine erneute *limitation* („Psi-1“) auf zwei Linien, eine dritte Linie kam im Januar 1945 hinzu; die Überwindung von Psi-1 gelang mit Hilfe des COLOSSUS II im September 1944.[218]

• „SZ 42c“

Schließlich plante man, in der SZ42 die *gemeinsame,* nur pseudozufällig unterbrochene Schlüsselradbewegung der zweiten Schlüsselradgruppe durch eine individuelle Bewegung zu ersetzen, gesteuert von der ersten Schlüsselradgruppe, und ohne Motorgetriebe. Diese Verbesserung (SZ42c) wurde in 1944 geprüft, kam aber nicht mehr zum Einsatz.[219]

---

[215] TICOM 1-45: OKW/Chi Cryptanalytic Research.
[216] Vgl. Davies, Donald: The Lorenz Cipher Machine SZ42. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIX, Nr. 1, January 1995, Artech House, Norwood MA/USA, 1998.
[217] TICOM 1-45: OKW/Chi Cryptanalytic Research.
[218] Vgl. Davies, Donald: The Lorenz Cipher Machine SZ42.
[219] TICOM 1-45: OKW/Chi Cryptanalytic Research.

Folgt man WEIERUDS Bericht, ging diese Verbesserung zum SZ42c sogar darüber hinaus: Der Verschlüsselungs-Algorithmus der Maschine soll direkt auf das Funksignal gewirkt haben, das kontinuierlich gesendet und mit der Empfangsstation synchronisiert wurde per quarzgesteuertem Oszillator.[220] WEIERUD nennt hierfür keine Quelle; doch gibt es für diese Angaben eine indirekte Bestätigung. Nach ROHRBACH entwickelte man wegen der „Schwächen" der bisherigen Verfahren [Schlüsselerzeugung mit Walzen-Drehbewegungen] neue Methoden: Entweder „auswechselbare Überschlüsselungsstreifen" [realisiert in der T43, s. 4.5.3], oder man „...sendet die Additionsreihe ständig ohne Unterbrechung".[221]

Fazit
Die Lorenz SZ40/42 ist ein klassisches Beispiel für den Algorithmus einer maschinellen Schlüsselgenerierung, von dem die Verantwortlichen glaubten, daß eine Entzifferung praktisch auszuschließen sei, denn: Eine theoretisch sehr hohe Zahl der Einstellmöglichkeiten, kombiniert mit der (Pseudo-) Irregularität der Schlüsselradbewegungen, schienen, wenn nicht unbrechbar, mindestens jedoch nicht in absehbarer Zeit entzifferbar zu sein. Diese Überzeugung hatte sich im militärischem, aber auch ingenieurmäßigem Denken gebildet, und war die Folge deren empirischen Entwicklung. Und als ausnahmsweise einmal eine kryptologische Untersuchung (HÜTTENHAIN in
1939, s. 4.3) vorlag, wurde deren Ergebnis ignoriert – es offenbarte wohl zu viele Schwächen der Maschine.

4.5 Das One-Time-Pad (OTP)-Verfahren

In der Geschichte der Kryptographie finden sich immer wieder Beispiele dafür, daß noch so scheinbar raffinierte Chiffrierungen früher oder später geknackt wurden.[222] Verständlich daher die lange Suche nach einem Verfahren, welches absolut sicher ist. Man entdeckte es zufällig, konnte jedoch dessen Unbrechbarkeit nur vermuten, die erst später mathematisch bewiesen wurde: Der US-Army-Kryptologe MAUBORGNE schlug dazu bereits 1918 vor, den Schlüssellochstreifen des Vernam-Verfahrens nur einmal zu benutzen, um eine Entzifferung auszuschließen (s. 4.5). Doch die Schlüsselbänder mußten dann gleichzeitig an den beiden Stationen vorliegen, und dementsprechend gelang es MAUBORGNE nicht, dieses Verfahren in der Army durchzusetzen, trotz der unbestreitbaren Sicherheit – die Schlüssellogistik war zu aufwendig.

Das später so genannte One-Time-Pad (OTP)-Verfahren ist weder an das Fernschreibsystem gebunden, noch setzt es ein binäres Zahlensystem voraus: Beispielsweise ist das Dezimalsystem anwendbar, wobei zunächst die Buchstaben

[220] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 2.
[221] Vgl. Rohrbach, Hans: Chiffrierverfahren der neuesten Zeit, S. 368.
[222] Viele Beispiele, teils vergnügliche, sind zu finden in Bauer, Geheimnisse.

in Zahlen umgesetzt und dann mit dem Schlüssel addiert werden. In Deutschland wurde dieses dezimale OTP-Verfahren in 1921 von KUNZE, SCHAUFFLER und LANGLOTZ für den diplomatischen Dienst entwickelt. Dort verwendete man (Pseudo-)Zufallszahlen, die eine Maschine auf Blöcke druckte, und die nur einmal zur Addition verwendet werden durften; vermutlich stammt der Begriff One Time Pad = Einmalblock von dieser Methode. Damit überschlüsselte man die Zahlencodes, die den Codebüchern des Auswärtigen Amt entnommen wurden.[223]

Wegen der problematischen Schlüsselverteilung und -Verwaltung kam das Verfahren jedoch nur für besonders wichtige Anwendungsfälle der obersten Sicherheitsstufe (Diplomatie, Top-Spionage etc.) in Betracht. Da man den nachstehend erläuterten SHANNON'schen Hauptsatz noch nicht kannte und dementsprechend ein Sicherheitsproblem nur zu vermuten war, nahm man es mit der Einmalverwendung nicht immer so genau, und demzufolge kam es durch Mehrfachverwendung der Blöcke und/oder maschineller Schlüsselerzeugung zu Entzifferungen, wenn genügend Material und Zusatzinformationen vorlagen.

4.5.1 C.E. Shannon und die Kryptosicherheit

Die Unbrechbarkeit des OTP-Verfahrens konnte man zunächst nur vermuten, weil alle Entzifferungsversuche scheiterten. Doch womöglich wußten die alliierten Geheimdienste bereits im Krieg mehr, denn man benutzte schon das OTP-Verfahren für die unbrechbaren ROCKEX- und SIGTOT-Systeme (s.u.): Dieses Wissen könnte der Informationstheoretiker Claude SHANNON (1916-2001) erarbeitet haben, als er während des Krieges (ab 1942) in den *Bell Labs*[224] mathematisch-theoretische Untersuchungen durchführte, die mit anderen Arbeiten der *Bell Labs* immer noch der Geheimhaltung unterliegen.

Vor dem Krieg wurde SHANNON bekannt durch den Nachweis der Analogie zwischen Boole'scher Algebra und (digitalen) Relaisschaltungen für Telefonvermittlungen. Dabei entdeckte er das „Bit" als Informationseinheit und als Fundament der Informationstheorie, die er nach dem Krieg (1948) in einer fundamentalen Schrift „A mathematical theory of communication" begründete. Danach übernahm er eine Professur für Mathematik.

SHANNON stellte als Erster ein mathematische Modell der Kryptologie auf und entwickelte die Analyse von Geheimtexten mit informationstheoretischen Methoden, also nicht mit praktischen kryptanalytischen Mitteln. Die grundlegende Frage dieser Theorie ist:
Wieviel Information über den Klartext ist im Geheimtext enthalten?

---

[223] Ausf. in Kahn, Codebreakers, S. 403.
[224] Zentrale Forschungseinrichtung der American Telephone&Telegraph Co.

Dazu zählen alle Informationen, wie Kenntnis des Geheimtextes und seines Verschlüsselungsverfahrens, Teilinformationen über den Klartext („wahrscheinliches Wort"), und besonders die verwendete Sprache: Denn jede natürliche Sprache enthält bestimmte Gesetzmäßigkeiten (Redundanzen), die auch im Geheimtext (verborgen) enthalten und analysierbar sind.

Seine Erkenntnisse faßte SHANNON zusammen in einer „*Communication Theory of Secrecy Systems*"[225], die zwar zum Kriegsende fertiggestellt war, aber erst 1949 publiziert wurde. Darin beschrieb er ein mathematisches Modell der Kryptologie, das es ermöglichte, quantitativ zu ermitteln, wieviel Information über den Klartext im Geheimtext noch enthalten ist. Und wenn diese dann nicht mehr ausreicht, den Klartext zu rekonstruieren, ist das Verfahren sicher.
Diese Analyse ermöglichte die erste (und bisher einzige) quantitative Beurteilung der Sicherheit von Chiffrierverfahren, und sie zeigte auch, daß das OTP-Verfahren die einzige *beweisbar sichere* Chiffrierung ist.

Für die hier zu berücksichtigenden Zusammenhänge kann man den sog. Shannon'schen Hauptsatz vereinfachend so zusammenfassen:
Das Vernam-Verfahren (und nur dieses eignet sich dafür) ist unbrechbar unter folgenden Bedingungen:

- Der Schlüssel muß *mindestens so lang* sein wie der Klartext.
- Der Schlüssel darf *nur einmal* verwendet werden.
- Der Schlüssel muß *echt zufällig* generiert sein.

Die letzte Bedingung stellte der maschinellen Kryptographie eine unüberwindbare Aufgabe: Alle Chiffriermaschinen verschlüsselten mit einem implementierten Algorithmus, der immer gleich blieb, und daher keine echt zufälligen Schlüssel erzeugen konnte. Man behalf sich daher mit verschiedenen Pseudozufälligkeiten, die jedoch von einem Sub-Algorithmus generiert wurden, und dieser konnte oft durch kryptanalytische Verfahren aufgedeckt werden, wie die Entzifferungen im Zweiten Weltkrieg zeigten.
Daher müssen alle Chiffrierverfahren, die dem Shannon'schen Hauptsatz nicht vollständig entsprechen, so konzipiert sein, daß der Aufwand zur Brechung so groß wird, daß Entzifferungen unrealistisch sind (wenn auch theoretisch möglich). Das war bei den meisten maschinellen Systemen des Krieges nicht der Fall, und daher konnten die ausgeklügelten deutschen (und japanischen) Chiffriermaschinen kompromittiert werden.

Auch die heutige computerbasierte Kryptographie arbeitet mit Pseudo-Zufallszahlen, deren elektronische Generierung allerdings nach mathematisch sehr komplizierten Algorithmen erfolgt und so konzipiert ist, daß deren Kryptanalyse mit *bekannten* derzeitigen Methoden äußerst aufwendig sein würde.

[225] Shannon, C. E.: Communication theory of secrecy systems.
Bell System Technical Journal 28 (1949), 656 - 715.

Sie gelten daher als praktisch unbrechbar. Das schließt keineswegs Entzifferungen aus, denn Geheimdienste können über unbekannte kryptanalytische Verfahren und/oder Computer verfügen, deren Leistungen weit über dem aktuellen Standard liegen. Und sie könnten sich aus anderen Quellen zusätzliche Informationen zum Geheimtext beschaffen, die den kryptanalytischen Aufwand erheblich mindern würden. Beides unterstellt man vor allem der NSA, deren Vorsprung auf diesem Gebiet von Experten auf 10-20 Jahre geschätzt wird, und die Folge der intensiven Förderung gleich nach dem Krieg ist, wie unter 7.5 ausgeführt wurde.

4.5.2 ROCKEX und SIGTOT– Verfahren

Keine Risiken ging man während des Krieges in England ein: Der umfangreiche (bis eine Mio Worte pro Tag) und militärisch wichtige Nachrichtenaustausch mit den USA war wegen der großen Länge der Texte durch Kryptanalyse besonders gefährdet. Um diesen Nachrichtenverkehr zu sichern, entwickelte eine Sonderabteilung des britischen Geheimdienstes MI6 eine besonders sichere Version des OTP-Verfahrens, genannt ROCKEX. Dessen Schlüssel erzeugte man nicht maschinell, sondern tastete elektronisches Rauschen ab, eine Methode, die ebenso für das OTP-Sprachverschlüsselungsverfahren SIGSALY angewendet wurde (s. 6.4.2). Darüber hinaus verschleierte man elektronisch die Betriebszeichen der Fernschreiber (Zeilenvorschub usw.), um jegliche Möglichkeit der Schlüsselanalyse auszuschließen.[226]

Ein ähnliches Verfahren mit der Kurzbezeichnung SIGTOT benutzte das US-Außenministerium ab 1944 für seine Kommunikation mit den Außenstellen. Es löste das bis dahin verwendete O2-Verfahren ab, das von Kryptologen des deutschen Auswärtigen Amtes gebrochen war.[227]

4.5.3 Siemens T43

Die deutschen Verantwortlichen zweifelten an der Sicherheit der SZ42- und T52-Maschinen wohl stärker als sie offiziell einräumen konnten, denn anders ist die zusätzliche Einführung der sicheren OTP-Maschine T43 kaum zu erklären: Vor allem das OKH, aber auch Marine[228] und Auswärtiges Amt[229] übernahmen ab Anfang 1944 die von Siemens & Halske entwickelte Schlüsselfernschreibmaschine

---

[226] Vgl. Hodges, Andrew: Alan Turing, The Enigma. US-Edition by Walker Publishing ²2000, S. 270-271. (künftig zit.: Hodges, Turing).

[227] Vgl. Bauer, Geheimnisse, S. 130.

[228] Stichwort SFM T43 in: Mache, W. (Hrsg.): Lexikon der Text und Daten-Kommunikation.

[229] Vgl. Beckman, B.: Svenska kryptobedrifter. Danach wurde eine T43-Maschine in der deutschen Botschaft Stockholm bei einer illegalen Aktion im Dez. 1944 gefunden.

T43. Diese bestand aus dem serienmäßigen S&H-Fernschreiber Ttyp 34n, dem ein Abtaster für das Schlüsselband und ein Mischer zur binären Addition der Impulse hinzugefügt wurde. Zur Chiffrierung dienten Einmalschlüsselbänder gemäß OTP-Verfahren, die an zentraler Stelle in Berlin hergestellt wurden, wo maschinell eine pseudozufällige Binärzahlensequenz („Störtext") durch Hintereinanderschaltung von zwei T52e-Maschinen erzeugt und in Schlüsselbänder gestanzt wurde.[230] Um die einmalige Verwendung der Schlüsselbänder sicherzustellen, durchlief das Band nach der Abtastung den Lochstanzer und wurde so automatisch vernichtet.

Die Logistik für Herstellung und Verteilung der Schlüsselbänder, die an beiden Stationen vorhanden sein mußten, wird in der Spätphase des Krieges problematisch gewesen sein und den Einsatz der Maschine limitiert haben. Möglicherweise blieben aus diesem Grund die Maschinen SZ42 und T52 weiter im Einsatz und für die Übertragung geheimer Kommandosachen zugelassen. Es konnte aber bisher nicht geklärt werden, warum zu diesen offiziell sicheren Maschinen eine weitere damals praktisch unbrechbare Maschine hinzu kam, die überdies großen Aufwand erforderte.

Der Wiener Historiker LANGER versuchte die Geschichte dieser Maschine zu erforschen und hat dazu Zeitzeugen und Forscher befragt sowie die wenige relevante Literatur ausgewertet.[231] Leider übernahm er unkritisch einige der Legenden, die sich um diese Maschine gebildet hatten, und interpretierte manche technische Details unrichtig. Und die interessante Frage, warum denn die Maschine T43 überhaupt eingeführt wurde, obwohl man die „sicheren" Maschinen SZ42 und T52 weiter verwendete, scheint Langer übersehen zu haben.

LANGER bezeichnet das Verfahren als „nicht entschlüsselbar". Das ist jedoch nach Shannon's Hauptsatz so nicht richtig: Die Schlüsselgenerierung erfolgte maschinell, unterlag mithin einem Algorithmus, der mit entsprechend großem Aufwand analysierbar gewesen wäre. Ob man das in BP versuchte, war nicht bekannt, doch nun enthält ein erst in 2000 freigegebenes Originaldokument[232] auch einen Abschnitt über „THRASHER", so die BP-Tarnbezeichnung für Verschlüsselungen durch die T43. Diese „Fischbezeichnung" wurde gewählt, weil die Kryptanalytiker zunächst vermuteten, die Schlüsselbänder würden mit einer SZ42-Maschine erzeugt, mithin zu den FISH-Chiffrierungen gehören. Bei der Analyse fanden sie einige Regelmäßigkeiten, darunter einen sehr kurzen Schlüsselwechsel aller 2000 Buchstaben, der Entzifferungen mit der Standardmethode ausschloß. Auch mit der statistischen Methode hatten sie keinen Erfolg; weitere Versuche unterblieben daher. Und sie stellten fest, daß „*at*

[230] Mache, Korrespondenz. Er beruft sich dabei auf H. Wüsteney/Siemens.

[231] Vgl. Langer, Josef: SFM T 43. (Letztes Update Dez. 2002).
Von: http://www.eclipse.net/~dhamer/downloads/SFMT43neu.PDF, am 8.4.03.

[232] Vgl. Good/Michie/Timms: General Report On Tunny: With Emphasis on Statistical Methods (1945), S. 494-495. Public Record Office, Kew/GB.

various times“ sogar Klartext gesendet wurde, wofür sie Maschinendefekte vermuteten. Doch eher wird Mangel an Schlüsselbändern der Grund gewesen sein, deren Nachschub in den letzten Kriegsmonaten problematisch gewesen sein dürfte.
Man hatte demnach Entzifferungen versucht, wollte oder konnte jedoch in BP die für intensivere Analysen notwendigen Ressourcen nicht einsetzten, zumal der Erfolg beim damaligen technisch-wissenschaftlichen Stand eher unwahrscheinlich war. Außerdem benötigte man diese Entzifferungen nicht unbedingt, denn es lagen ja genug Informationen aus der SZ42- und ENIGMA-Entzifferung vor.

Anzumerken wäre hierzu eine bisher unbekannte Schwäche der Maschine: Die Kryptologen von OKW/Chi gaben in ihren Verhören nach dem Krieg zu Protokoll, daß die T43 gleichwohl brechbar war, weil es wegen der Langsamkeit der Verschlüsselungs-Relais zu Phasenverschiebungen zwischen Klar- und Geheimtext kam, die sie oszillographisch aufzeichnen konnten. Diese Phasendifferenz ermöglichte die buchstabenweise Rekonstruktion des Klartextes und sie hatten daher gefordert, alle T43-Maschinen nur über einen „Entzerrer“ zu betreiben, der diesen Mangel behob. Sie konnten jedoch nicht angeben, wo T43-Geräte eingesetzt und ob jeweils Entzerrer verwendet wurden.
Diese Entdeckung veranlaßte die Herstellerfirma zu einer Konstruktionsänderung, doch die verbesserten Maschinen kamen nicht mehr zum Einsatz.[233]

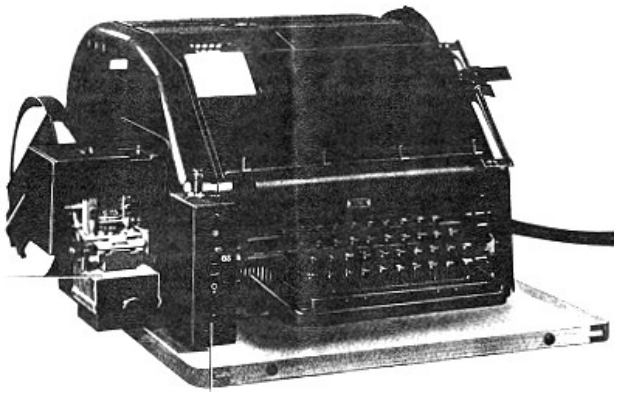


Bild 32: Schlüsselfernschreibmaschine Siemens T 43[234]
[Basismaschine Siemens Ttyp 34n]

In der Literatur, bspw. bei LANGER, wird die Blattschreiberversion der T43 abgebildet. Nach MACHE ist das nicht ganz korrekt, denn im militärischen Bereich wurde fast ausschließlich der hier abgebildete Streifenschreiber verwendet.[235]

[233] TICOM 1-45: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines.
[234] Bild nach Mache, Korrespondenz.
[235] Mache, Korrespondenz.

4.5.4 Der mechanische OTP-Schlüsselgenerator

Um die hohen Kosten der Generierung echt zufälliger Schlüssel zu vermeiden, die nur für höchste militärische bzw. diplomatische Geheimhaltung vertretbar waren, entwickelte man dazu Pseudo-Zufallsgeneratoren.Neben maschinellen Verfahren, die ähnlich wie Chiffriermaschinen Schlüssel erzeugten, gab es auch arbeitsintensive Handmethoden: Beispielsweise berichtet HAGELIN von Methoden, die er als „*laboriously rolling dice*" charakterisiert, und davon, daß man auf Schreibmaschinen beliebige Zahlenfolgen tippen ließ.[236]

Doch das ist eine gefährliche Methode: Sie unterliegt gleichwohl einem schwachen Algorithmus, weil die Finger nicht exakt zufällig tippen, und daher bei genügend viel Geheimtext-Material analysierbar ist. Sowjetische Geheimdienste ließen so ihre OTP-Schlüsselblöcke tippen, die überdies gelegentlich mehrfach verwendet wurden. Daher konnten sowjetische Agentensendungen später von der NSA entziffert und die meisten Atomspionage-Agenten enttarnt werden (*VENONA-Breaking*).

HAGELIN bewies auch hier seine geniale Fähigkeit, komplizierte Algorithmen mechanisch zu generieren, und – fast genau so wichtig – in eine kommerziell nutzbare Maschine zu integrieren. Überdies erreichte er mit relativ geringem Aufwand eine fast perfekte Zufallswahrscheinlichkeit. Dementsprechend wird das Verfahren noch heute im Prinzip zur Ausspielung der Lottozahlen im Fernsehen eingesetzt:

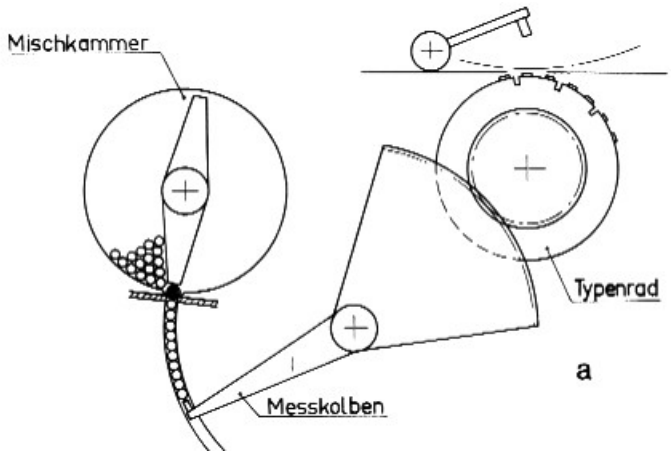


Bild 33: Schema „Random Number Generator" CBI53[237]

[236] Vgl. Hagelin, Cryptos, S. 509-510.
[237] Bild nach Hagelin, Cryptos, S. 510.

In dieser Maschine steuerten acht Mischkammern mit je 26 Stahlkugeln über Taster („Messkolben“) die acht Typenräder, die mit je einer 5-Buchstabensequenz versehen waren. Eine Kugel von den 26 war etwas größer und blockierte nach dem Mischvorgang in zufälliger Folge das jeweilige Ausgangsrohr.
Die Zufallsfolge entstand durch die in der Zwischenzeit ausgetretenen Kugeln; deren Anzahl bewegte entsprechend ihrem Gewicht einen Taster, dessen Winkelstellung proportional ein Typenrad steuerte. Und nach jedem Durchlauf druckte das Typenrad eine Sequenz von 8x5 Zufallsbuchstaben oder -zahlen.

Es wurden nur etwa 10 Maschinen gebaut, weil Computer das Verfahren ersetzten, doch „… die meisten sind noch heute [1994] in Betrieb.“[238]

[238] Vgl. Hagelin, Cryptos, S. 510.

5 Brechung der Chiffriermaschinen

Der Begriff „Brechung“ eines Chiffrierverfahrens (*codebreaking*) ist hier zu verstehen als maschinelle Entzifferung von Geheimtexten, die Teil des Untersuchungsgegenstandes „maschinelle Kryptologie“ ist (mathematisch-kryptologische Analysen siehe einschlägige Fachliteratur). Denn die herkömmlichen nichtmaschinellen kryptanalytischen Methoden hätten selbst mit enormen Personaleinsatz im Krieg nicht ausgereicht und wären überdies bei manchen Chiffrierungen undurchführbar gewesen, so daß sie hier außer Betracht bleiben können.
Mithin konnten nur maschinelle Entzifferungsverfahren im Zweiten Weltkrieg erfolgreich sein, weil die große Zahl der Funknachrichten – mehrere Tausend täglich – nur maschinell zu bewältigen war. Und erst die aus dieser Menge gewonnenen Informationen und deren intensive Weiterverarbeitung erbrachten in der Zusammenschau die *intelligence*, ULTRA genannt, die mehr war als die deutsche „Funkaufklärung“.

Ohne kryptanalytische Maschinen wäre demnach ULTRA nicht möglich gewesen, und die Alliierten hätten ihre informationelle Überlegenheit nicht erlangen können. Wie aber konnten sie diese damals ganz neuartigen Maschinen bauen und einen so großen technologischen Vorsprung über Deutschland erringen? Und welche Informationen und Textmaterial benötigten sie zum erfolgreichen Betrieb dieser Maschinen? Wurden da etwa deutsche Fehler gemacht, und wenn ja, welche und aus welchen Grund?

5.1 wissenschaftlich-technische Grundlagen

Bevor ein maschinelles Chiffriersystem gebrochen werden konnte, bedurfte es intensiver wissenschaftlicher Vorarbeit, denn die Algorithmen des Verfahrens mußte man als erstes kryptomathematisch analysieren. Das war generell möglich, weil die von der deutschen Wehrmacht verwendeten Chiffriermaschinen mechanisch bzw. elektromechanisch die Verschlüsselungsalgorithmen generierten, aber während des Krieges nicht oder nur unwesentlich kryptologisch wirksam verändert wurden, wie beispielsweise die britische TYPEX-Maschine.
Doch bevor Kryptanalytiker die Algorithmen der Maschinen ermitteln konnten, benötigten sie neben den abgehörten und aufgezeichneten Geheimtexten auch genügend dazu passendes Klartextmaterial, zu beschaffen durch Spionage, Diebstahl und besonders durch Kompromittierungen: Für diese bewährte kryptanalytische Methode nutzte man, wenn verfügbar, *re-enciphered* (auch *re-encodet*) *material*, Texte also, die ganz oder teilweise auch mit anderen, bereits

gebrochenen Chiffrierverfahren verschlüsselt worden waren. Damit erhielt man einen passenden Klartext für die Analyse des zu entziffernden Geheimtextes, und erreichte eine „Klartext-Geheimtext-Kompromittierung“ (ein „*kiss*“ in BP). Eine weitere Analysemöglichkeit bot die „Geheimtext-Geheimtext-Kompromittierung“, die voraussetzte, daß der gleiche Klartext mit verschiedenen Schlüsseleinstellungen chiffriert wurde. Schließlich gab es noch eine andere „Geheimtext-Geheimtext-Kompromittierung“, die möglich wurde, wenn verschiedene Klartexte mit demselben Schlüssel chiffriert wurden. Diese Kompromittierungsvarianten nannte man in BP „*depths*“.
Mit all diese Angriffsmöglichkeiten mußte unter Kriegsbedingungen gerechnet werden.

Diese kryptanalytischen Methoden wurden ergänzt bspw. durch linguistische Studien über Eigenheiten der zu analysierenden Sprache und besonders deren Ausdrucksweise im militärischen und diplomatischen Sprachgebrauch. Denn die Vertreter dieser beiden Berufsgruppen verwenden häufig stereotype Redewendungen und Floskeln, die den Analytikern viele Möglichkeiten zur Gewinnung von Klartextfragmenten bieten. Ebenso dienen dazu plötzliche Ereignisse, für die geläufige Wörter, Ortsnamen usw. im Geheimtext anzunehmen sind, und die man gelegentlich provozierte (in BP *gardening* genannt).
Längere Klartexte ermöglichten es sogar, den Algorithmus einer Chiffriermaschine mathematisch zu bestimmen, auch wenn die Maschine unbekannt war. Dann konnte man anschließend diese Maschine rekonstruieren und einen Simulator bauen, mit dem dann die Klartexte erzeugt wurden. Dazu mußten man freilich vorher die jeweilige Schlüsseleinstellung kryptanalytisch bestimmen. Für diese täglich erforderliche Arbeit genügten im Kriege nicht mehr zeitaufwendige Handverfahren, es mußten hierzu maschinelle Methoden entwickelt werden. Dazu implementierten Ingenieure die mathematisch abgeleiteten Algorithmen in Maschinen, mit denen man die Schlüsseleinstellungen bestimmen konnte. Um aber damit schnell genug entziffern zu können, benötigte man zu den täglichen, später teilweise 8-stündlichen Schlüsselwechseln jeweils zugehörende Klartextfragmente, sog. *cribs*, eine weitere kryptanalytische Aufgabe.

Mithin benötigte man Mathematiker für die Analysen, und Ingenieure für die Konstruktion kryptanalytischer Maschinen, die überdies im Krieg unter enormen Zeitdruck betriebsfertig zu bauen waren. Ferner weitere Wissenschaftler, wie Linguisten, Dolmetscher, Militärexperten, sowie zahlreiche sonstige Mitarbeiter zur Sortierung, Auswertung, Archivierung und Maschinenbedienung. Dieser enorme Aufwand – zuletzt arbeiteten bis zu 10.000 Personen[239] in BP – war nur durchsetzbar, weil wenige weitsichtige Verantwortliche der Alliierten, besonders CHURCHILL, den „Ertrag“ richtig einschätzten: Die aus den Entzifferungen gewonnene *intelligence* – später ULTRA genannt – würden im Krieg eine sehr wirksamen Waffe sein.

[239] Nach Smith beschäftigte BP 8.995 Mitarbeiter im Jan. 1945.
Vgl. Smith, Michael: Enigma entschlüsselt, S. 272.

5.2 Beherrschung der Wehrmachts-ENIGMA

Über die ENIGMA-Geschichte kann man immer noch erstaunliche, teilweise aberwitzige Geschichten lesen, vor allem auf Internetseiten und besonders über die Vorkriegszeit, nachdem bekannt wurde, daß polnische Kryptologen die ENIGMA bereits 1932 gebrochen hatten.
Das ist unverständlich, denn die Forschung ermittelte längst den wahren Sachverhalt, bis auf wenige ungeklärte, jedoch unwesentliche Punkte.

5.2.1 Polnische ENIGMA-Analyse

Polen war sich der latenten Kriegsgefahr nach dem 1. Weltkrieg stets bewußt: Die beiden Nachbarn Deutschland und Sowjetunion wollten ihre 1919 an Polen verlorenen Gebiete zurück. Um nicht überrascht zu werden, zeichnete man deren Funkverkehr auf und entzifferte ihn. Der polnische Geheimdienst hatte darin Erfahrungen gesammelt, die schon im polnisch-sowjetischen Krieg 1919/20 halfen, den Krieg zu gewinnen. So war man sehr besorgt, als bereits im Februar 1926 nach Einführung der ENIGMA C („Funkschlüssel C“) die Sendungen der deutschen Marine, und im Juli 1928 nach Einführung der ENIGMA G ebenso die des Heeres nicht mehr entziffert werden konnten. Die Chiffrierung dieser Funksendungen widerstand allen damals bekannten kryptanalytischen Methoden.

Bald vermutete die zuständige Abteilung des polnischen Generalstabes (BS4) eine maschinelle Chiffrierung; der Verdacht richtete sich auf die ENIGMA, deren kommerzielle Version bekannt war. Der Geheimdienst forschte nach und bestätigte dann Informationen, daß das deutsche Heer eine modifizierte ENIGMA verwende, ab 1. Juni 1930 die ENIGMA I.

Alle Versuche der militärischen Experten, damit chiffrierte Nachrichten zu entziffern, scheiterten. Selbst die Lieferung geheimer ENIGMA-Dokumente[240] durch den deutschen Agenten H.T. SCHMIDT (Deckname „Asche“) via französischen Geheimdienst brachte keinen Erfolg. Man kam zum Ergebnis, daß nur noch wissenschaftliche Kompetenz weiterhelfen könne, und stellte zum September 1930 drei geeignete Mathematiker zur Kryptanalyse ein: REJEWSKI, der auch in Göttingen studiert hatte, ROZYCKI und ZYGALSKI. Sie waren die erfolgreichsten Teilnehmer an einer vom Chiffrierdienst organisierten kryptologischen Ausbildung an der Universität Posen, und sprachen fließend Deutsch. [241]

[240] Besonders wertvoll waren: Gebrauchs-und Schlüsselanweisungen, und die täglichen ENIGMA-Einstellungen für zwei Monate.

[241] Vgl. Bloch, Gilbert: ENIGMA before ULTRA – Polish Work and the French Contribution. (Translation by Deavours, C.A.). In: Deavours, Cipher A. (Eds.), Selections from Cryptologia, Volume XI, Nr. 3, July 1987. (Künftig zit.: “Bloch, Polish Work”).

Bild 34: M. Rejewski[242]

REJEWSKI (1905-1980) war bereits nach 10 Wochen erfolgreich: Er erarbeitete eine „ENIGMA-Gleichung“ und zeigte damit, wie die unbekannte innere Verdrahtung der Maschine rekonstruiert und damit eine Entzifferung ermöglicht werden könnte. Doch das Gleichungssystem enthielt zu viele Unbekannte, war so nicht lösbar, und bedurfte dazu weiterer Angaben. Die fand REJEWSKI in den vom französischen Geheimdienst beschafften ENIGMA-Geheimdokumenten, welche die polnischen Kollegen ebenfalls erhielten.

Die Bedeutung dieser von H.T. SCHMIDT entwendeten Dokumente wurde und wird von polnischen Verfassern (aus nationalistischen Gründen?) stets heruntergespielt. Dabei hätte REJEWSKI diese „Aufwertung“ bestimmt entbehren können; er selbst schrieb bescheiden: „*...the intelligence material furnished to us should be regarded as having been decisive in the solution of the machine*.“[243]

Diesen Dokumenten war u.a. zu entnehmen, wie die ersten drei Buchstaben des Spruchschlüssels verdoppelt und dann verschlüsselt wurden. Während dieser Prozedur bewegte sich fast nur die erste Rotorwalze, alle anderen variablen Einstellungen blieben konstant. Weiteren Geheimdokumenten entnahm er die jeweiligen Tagesschlüssel, wozu korrespondierende, abgehörte Geheimtexte vorlagen, und konnte damit die innere Verdrahtung der ersten Walze rekonstruieren; die anderen beiden folgten nach dem Wechsel der Walzenlage.[244]
Schließlich „erriet“ er noch intuitiv die Verdrahtung des Eingangsstators mit der Tastatur, und mit diesen gesamten Erkenntnissen gelang ihm die Brechung der ENIGMA-Verschlüsselung. Und die Überschlüsselung durch das Steckerfeld umging REJEWSKI durch Analyse von „ungesteckerten“[245] Buchstaben.
Mit diesen Ergebnissen konnte man ENIGMA-Nachbauten in Auftrag gegeben, den die AVA-Werke Warschau ausführten.[246]

---

[242] Bild nach HNF/Ryska, Vortrag Kryptologie. © W. Kozaczuk: Im Banne der Enigma.
[243] Zit. nach Kahn, Codebreakers, S. 974.
[244] Die Walzen wurden nach Tabellen regelmäßig wechselnd in die Maschine eingesetzt: Damals aller 3 Monate, dann ab 1936 monatlich, im Kriege täglich.
[245] Es wurden damals nur 6 Buchstabenpaare “gesteckert”, später bis 10.
[246] Vgl. Bloch, Polish Work, S. 378-382

Ab Anfang 1933 war die ENIGMA I gebrochen, mit der Einschränkung, daß dies nur für das damalige ENIGMA-Betriebsverfahren galt, denn spätere Änderungen erforderten neue kryptanalytische Methoden, die noch eingehender zu diskutieren sind. Es war auch der erste Beweis dafür, daß zur erfolgreichen Kryptanalyse maschineller Chiffrierungen *intelligence* erforderlich ist: Diese beschaffte man durch Diebstahl oder Kopie, wie „Asches" Material, und durch Kompromittierung (Spruchschlüssel-Verdoppelung). Gleichwohl mindert das nicht REJEWSKI'S Verdienst, die erste wissenschaftliche Kryptanalyse einer maschinell generierten Chiffrierung erarbeitet zu haben.

Mit den ENIGMA-Nachbauten allein war regelmäßiges Entziffern freilich nicht möglich: Täglich wechselte die ENIGMA-Einstellung, der sog. Tagesschlüssel: Walzenlage (ab 1936), Ringstellung, Steckerbrett-Verbindungen und Grundstellung (Startposition der Walzen) wurden in geheimen Tabellen[247] vorgegeben. Und für jede Nachricht wurden die Walzen per Spruchschlüssel neu eingestellt. Der ENIGMA-Operator vereinbarte diesen mit seinem Gegenpart, indem er zunächst drei beliebige Buchstaben wählte, diese dann verdoppelte als Sicherheit gegen Übertragungsfehler, und schließlich per Tagesschlüssel chiffrierte, wie den übrigen Text. Damit wurde die Stellung der Walzen vereinbart und mit dieser Einstellung dann der Geheimtext gesendet. In der empfangenden Station konnte der Operator entschlüsseln, nachdem er zuvor mit Hilfe des ihm ebenfalls vorliegenden Tagesschlüssels den Spruchschlüssel entschlüsselt hatte.

Die ersten sechs Ziffern einer solchen Sendung boten somit eine Einbruchsmöglichkeit durch „Geheimtext-Geheimtext-Kompromittierung".[248] REJEWSKI beobachtete dazu eine Häufung bestimmter Schlüssel durch schlechte Gewohnheiten der Operatoren, und Rotorzyklen, die von den Steckerverbindungen unabhängig sind. Dazu ermittelte er, daß diese Zyklenlängen (ein Begriff der mathematischen Gruppentheorie) von den Steckerverbindungen unabhängig sind.[249]

Allerdings waren dazu 105.456 Möglichkeiten zu untersuchen. Das aber konnte vereinfacht werden, weil eine sog. Mustersuche möglich war, für die ein Katalog erstellt werden mußte. Für dessen Anfertigung konstruierte REJEWSKI zusammen mit dem Ingenieur PALLUTH (AVA-Werk) die erste kryptanalytische (Hilfs-)Maschine mit der Tarnbezeichnung CYCLOMETER, die 1937 in Betrieb ging.[250] Nach einiger Zeit war der Katalog fertig und man konnte nun den Tagesschlüssel innerhalb ca. 20 min ermitteln.

---

[247] Agent H.T. Schmidt („Asche") lieferte die meisten dieser Tabellen, die jedoch den Kryptologen nicht übergeben wurden. Die Offiziere kontrollierten damit deren Arbeit. Vgl. Bloch, Polish Work, S. 383.

[248] Ausf. in Bauer, Geheimnisse, S. 411.

[249] Ebd., S. 416.

[250] Vgl. Bloch, Polish Work, S. 389. Ausführliche technisch-mathematische Erläuterungen der Enigma-Kryptanalyse s. Rejewski, M.: Mathematical Solution of the Enigma Cipher , S. 310-324.

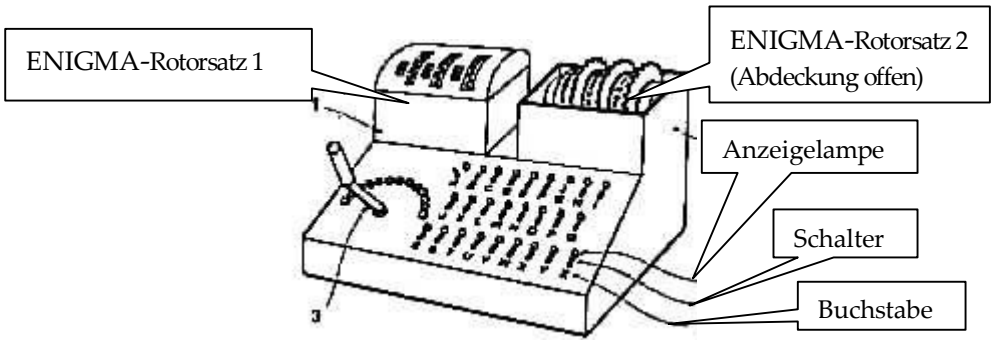


Bild 35: Cyclometer[251]

Ein Jahr vor Kriegsbeginn, am 15.9.1938, änderte die Wehrmacht die Betriebsvorschrift der ENIGMA: Der Tagesschlüssel entfiel, dafür mußte für jede Sendung eine eigene ENIGMA-Grundstellung vereinbart, und mit dieser dann der folgende Spruchschlüssel chiffriert und wiederholt werden. Damit waren die bisherigen polnischen Entzifferungsverfahren nun wirkungslos. REJEWSKI erarbeitete zur Lösung[252] dieses Problems einen Algorithmus, basierend auf der beibehaltenen Spruchschlüsselverdopplung, und PALLUTH konstruierte eine Maschine mit der Tarnbezeichnung „BOMBA“ (poln. = Bombe), wohl wegen des ständigen Tickens der Kontakte so genannt. Entsprechend den sechs möglichen Walzenlagen wurden sechs Maschinen in Auftrag gegeben, mit je drei Paaren Rotorsätzen, die um jeweils drei Positionen gegeneinander versetzt waren:

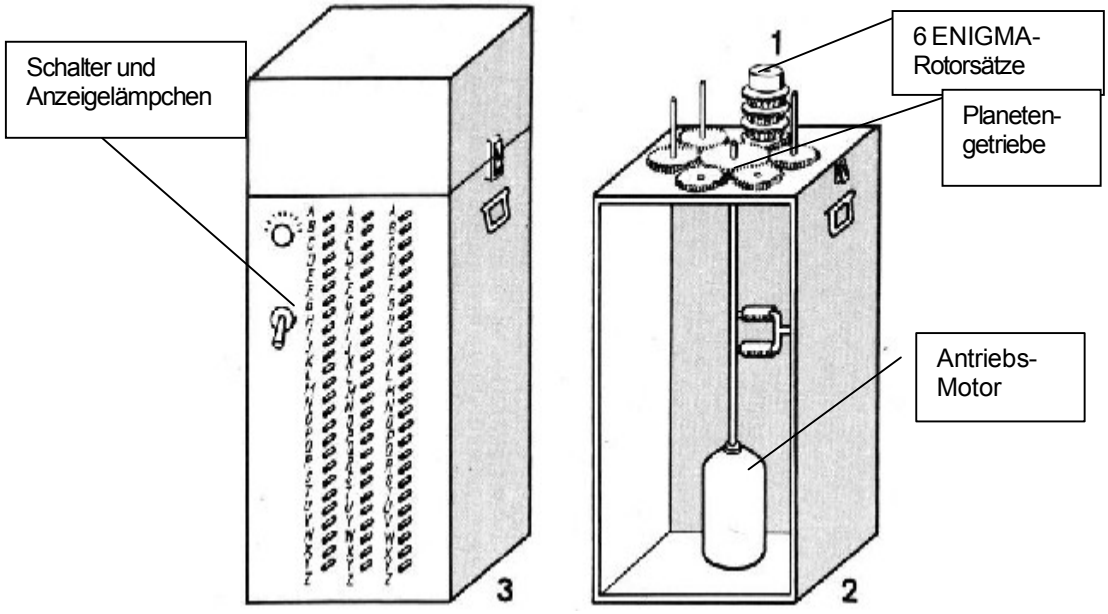


Bild 36: Polnische “BOMBA” [253]

[251] Bild nach Bloch, Polish Work, S. 321.

[252] Eine andere Lösung wurde von Zygalski entwickelt – ein Lochkartenverfahren („Zygalski-sheets“), bevor die BOMBA einsatzbereit war. Es wurde später in BP von Turing weiterentwickelt, s. 5.2.2.

[253] Bild nach HNF/Ryska, Vortrag Kryptologie. © W. Kozaczuk: Im Banne der Enigma.

Im November 1938 standen die sechs Maschinen zur Verfügung, mit denen man die jeweiligen Einstellungen der Walzen und deren Ringstellungen innerhalb von zwei Stunden bestimmten konnte, sobald genügend Material vorlag.[254] Anschließend konnten damit auf einer nachgebauten ENIGMA auch die Verbindungen des Steckerbretts ermittelt und dann die aufgezeichneten Sendungen dieses Tages mitgelesen werden.

Am 15. Dezember 1938 erschwerte die Wehrmacht erneut die Entzifferung: Sie führte zwei zusätzliche Walzen ein, so daß nun die drei Walzen aus fünf auszuwählen waren, was die möglichen Walzenlagen verzehnfachte. Die beiden neuen Walzen konnten jedoch umgehend rekonstruiert werden, dank eines Chiffrierfehlers einer SS-Dienststelle, denn die SS verwendete die gleiche Maschine, kombiniert mit einer den Polen bekannten Vorverschlüsselung.
Aber: Entzifferungen benötigten nach der Verzehnfachung der Walzenlagen mit der vorhandenen Ausrüstung sehr viel mehr Zeit und waren nicht immer möglich. Man benötigte zur Lösung des Problems eine entsprechende Aufstockung an Geräten: 60 BOMBA-Maschinen statt sechs, dazu das erforderliche Fachpersonal. Doch das überforderte die Ressourcen des polnischen Dienstes.

Eine weitere Erschwernis kam hinzu am 1. Januar 1939: Zusätzliche Steckerverbindungen (10 statt bisher 6) wurden befohlen. Das erschwerte die Entzifferungen so sehr, daß die Verantwortlichen nicht mehr auf Besserung hoffen konnten.[255] Man entschloß sich daher zur engen Zusammenarbeit mit den Alliierten, denen man bisher nichts mitgeteilt hatte, was aber angesichts der offenkundigen Kriegsgefahr ohnehin ratsam war. Am 25. Juli 1939 übergab man daher in Pyry (nahe Warschau) den verblüfften Experten Englands und Frankreichs alle Unterlagen, Lochkarten-Kopien, und vor allem je eine nachgebaute ENIGMA I samt allen fünf rekonstruierten Walzen. (Die anderen polnischen Geräte mußten nach Kriegsbeginn und drohender Erbeutung vernichtet werden). Das polnische Material erreichte London via Frankreich am 16.8.1939, und sogleich begannen die Experten im gerade eingerichteten Entzifferungszentrum BP mit dem polnischen „Geschenk“ zu arbeiten.

5.2.2 Turing und die britische ENIGMA-Beherrschung

Dillwyn „Dilly“ KNOX

Die britischen kryptanalytischen Dienste waren nach dem Ersten Weltkrieg stark verkleinert und zusammengelegt worden; sie arbeiteten nun unter der Tarnbezeichnung GC&CS überwiegend für das Außenministerium. Der bereits

[254] Vgl. Bauer, Geheimnisse, S. 417-419.
[255] Vgl. Bloch, Polish Work, XII/3, S. 396-397.

1915 noch für den *room 40* eingestellte Altphilologe Alfred Dillwyn „Dilly" KNOX (1885-1943) blieb jedoch im Dienst, wohl wegen seiner überragenden Fähigkeiten. In den 30er Jahren übertrug man ihm eine kleine Abteilung, die Methoden zur Entzifferung von ENIGMA-Sendungen erarbeiten sollte, aktuell für die im spanischen Bürgerkrieg verwendete ENIGMA D ohne Steckerbrett. Das gelang ihm, und KNOX übertraf diesen Erfolg später noch mit der Rekonstruktion der Abwehr-ENIGMA 1941 (s. hierzu 5.2.4). Doch mit seinen Methoden der linguistischen Kryptanalyse konnte er keinen Einbruch erzielen in die ENIGMA I-Chiffrierung, da das Steckerbrett eine zu große Hürde war, auch nicht, als er ebenfalls wie seine polnischen Kollegen die vom französischen Geheimdienst beschafften Geheimdokumente erhalten hatte. In 1938 intensivierte die GC&CS die Zusammenarbeit mit Frankreich und erhielt zusätzliche Dokumente, darunter die vom Agenten H.T. SCHMIDT gelieferten monatlichen Einstelltabellen der ENIGMA I.[256] Dennoch konnte KNOX die Maschine nicht überwinden, und man kam zum Ergebnis, daß gegen diese neuartigen Maschinenchiffrierungen wohl nur mathematische Methoden erfolgversprechend sind.

Zu dieser Zeit besuchte der schon als Schüler kryptologisch interessierte Cambridge-Mathematiker Alan TURING Kryptologie-Kurse der GC&CS, zuletzt Ende 1938. Er assistierte Dilly KNOX bei dessen Versuchen, die ENIGMA I zu attackieren.[257]

Bild 37: A.M. Turing (1951)[258]

Sein Biograph A. HODGES bezeichnete TURINGS dortige Tätigkeit als „*the first scientific input into a hitherto arts-based department*".[259] Denn die wenigen Kryptologen der GC&CS waren wie „Dilly" KNOX zwar sehr erfahren, jedoch

[256] Vgl. Bloch, Polish Work, XII/3, S. 395-396.

[257] Kahn, David: Seizing the Enigma: The Race to Break the German U-Boat-Codes, 1939-1943, S. 93. Houghton Mifflin, Boston MA/USA, 1991.

[258] Bild nach Hodges, M.: Alan Turing Archives and Photographs, © National Portrait Gallery. Von: http://www.turing.org.uk/sources/archive.html, am 25.10.02.

[259] Hodges, Andrew: Alan Turing – a short biography, Part 4 – The Second World War, 1999. Von http://www.turing.org.uk/turing/index.html, am 16.2.02.

Linguisten, und hatten daher Probleme bei der Entzifferung der neuartigen Maschinenchiffrierungen. Denn diese veränderten die inneren Gesetzmäßigkeiten einer Sprache, die sonst auch im Geheimtext verborgen sind, und nun kaum mehr mit linguistischer Kryptanalyse rekonstruiert werden konnten.
Nun hofften die Verantwortlichen auf Erfolge mit TURINGS wissenschaftlicher Kompetenz, genauer mit seinen Fähigkeiten als mathematischer Logiker, die er in einer berühmt gewordenen Schrift publiziert hatte: „*On Computable Numbers, with an Application to the Entscheidungsproblem*."[260] Darin diskutierte er u.a. eine später nach ihm benannte hypothetische „Turing-Maschine", ein Modell zur Untersuchung von Fragen der Berechenbarkeit. Berechenbar heißt in diesem Sinne, daß ein Algorithmus zur Lösung des Problems existieren muß. Doch den Begriff „Algorithmus", damals mehrdeutig, mußte TURING zunächst präzisieren, und kam dann zu folgendem Ergebnis: „[...] alle algorithmisch lösbaren Probleme – und zwar genau diese – können prinzipiell von einer Rechenmaschine bearbeitet werden." Ferner lassen sich damit „[...] beliebige Rechenautomaten nicht nur definieren, sondern auch technisch realisieren."[261]

TURING bewies bei seiner Tätigkeit in BP, daß diese Erkenntnis auch und gerade auf kryptanalytische Maschinen zutrifft (s. 5.2.2). Deren Algorithmus mußte nur dem der jeweiligen Chiffriermaschinen reziprok sein, um Lösungen zu finden. Und Chiffriermaschinen wiederum mußten mit einem präzise definierten Algorithmus verschlüsseln, da ja sonst die Gegenstelle nicht zuverlässig entschlüsseln konnte, die den gleichen Algorithmus verwendete. Mithin eigneten sich alle kryptologischen Maschinen, sei es zur Chiffrierung, sei es zur Dechiffrierung und auch zur Entzifferung, ideal für eine maschinelle Realisierung im Sinne TURINGS, denn sie arbeiteten ausschließlich algorithmisch.
Das aber prädestinierte den Logiker und Algorithmus-Experten TURING zum Kryptanalytiker und vor allem zum Entwickler kryptanalytischer Maschinen.
Kurz vor Kriegsbeginn verpflichtete man daher TURING als hauptberuflichen BP-Mitarbeiter, zusammen mit anderen Wissenschaftlern, darunter den Mathematiker Gordon WELSHMAN (1906-1995), die am 4.9.1939 ihren Dienst antraten.

TURING wurde dann KNOX' Abteilung zugeordnet und erhielt den Auftrag nach Methoden zu suchen, die eine Schwäche des polnischen Entzifferungsverfahrens vermied: Es war völlig abhängig von der Analyse der doppelt gesendeten Start-Walzenpositionen, dem Spruchschlüssel, denn bei einem Verfahrenswechsel würden die polnischen Methoden wertlos. Und mit einem solchen Wechsel mußte man jederzeit rechnen.
Dieser erfolgte zum 1. Mai 1940: Es entfiel die Verdoppelung der Walzenstellungen beim Senden des Spruchschlüssels, so daß kein Klartextfragment mehr zur Verfügung stand. Doch TURING fand eine Lösung: Er ersetzte den fehlenden Klartext durch die Annahme eines Wortes, das im Text wahrscheinlich vorkam

[260] In den „Proceedings of the London Mathematical Society" (2) 42S, 1937.
[261] Naumann, Informatik, S. 248.

und dessen Stellung ungefähr bekannt war. Diese Hypothese sollte durch die Unterstellung geprüft werden, das Wort sei im Suchbereich des Geheimtextes für jede der eingestellten Walzenpositionen richtig, und wenn nicht, dann war nach der mathematischen Logik „reductio ad absurdum“ = Beweis durch Widerspruch, diese Position zu verwerfen. Das galt ebenso, wenn das Wort selbst unrichtig war. Vermutlich analog zu seiner hypothetischen Maschine plante TURING dazu eine maschinelle Lösung zu entwickeln, eine Maschine, die diesen Testalgorithmus ausführte. Diese nannte man später in BP nach dem polnischen Modell „BOMBE“.

Folgt man SINGH, fielen TURING in vielen [mit polnischen Verfahren] entzifferten deutschen Funksendungen Strukturen auf, nach denen man teilweise voraussagen konnte, welche Inhalte wo im Text vorkamen, wenn man wußte, wann und woher sie gesendet wurden.[262] Beispielsweise sendeten manche deutsche Dienststellen täglich nach 6 Uhr einen verschlüsselten Wetterbericht. Demzufolge mußten die kurz nach 6 Uhr abgehörten Nachrichten fast sicher das Wort *wetter* enthalten, und, da ja strenge deutsche militärische Vorschriften galten, mußte dieses auch an einer bestimmten Position zu finden sein. Somit konnte man das Klartextfragment *wetter* mit dem zugehörenden Geheimtext verknüpfen. Diese Klartextfragmente nannte man im BP-Jargon „*crib*“, deren Erarbeitung aus den Geheimtexten unter 5.4.2 näher erläutert ist.

TURING ging nun davon aus, daß mit Hilfe dieser *cribs* der jeweilige ENIGMA-Schlüssel rekonstruierbar sein müßte. Freilich konnten dazu nicht alle (nach SINGH) theoretisch möglichen $1{,}59 \times 10^{20}$ Einstellungen probiert werden, besonders mußte ein Weg gefunden werden, die Überschlüsselung durch das Steckerbrett abzustreifen, das davon mit rd. $1{,}5 \times 10^{14}$ bzw. ca. 70% den weitaus größten Anteil hatte.[263]

[262] Vgl. Singh, Simon: Geheime Botschaften, S. 211-214.
[263] Vgl. Bauer, Geheimnisse, S. 50, berechnet für 10 Steckerpaare.

Nach TURINGS Idee kann man ein *crib* nahezu beliebig mit dem zugehörenden Geheimtext verknüpfen, und nicht jeder Buchstabe des *cribs* muß dazu genommen werden, denn bereits ein „falscher" führt den logischen Widerspruch herbei. SINGH gibt dazu das folgende Beispiel:[264]

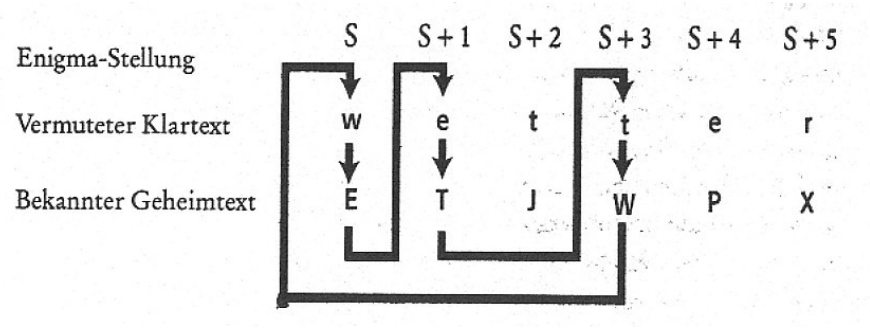


Bild 38: Turings crib-Methode mit Schleifenbildung[265]

Das vermutete Klartextwort *wetter* wird über drei hypothetische Schleifen mit dem Geheimtext verknüpft. Die unbekannte Walzenstellung S verändert sich mit jeden Buchstaben, da die ENIGMA bei jeden Buchstaben einen Schritt weiterschaltet, also S+1, usw. Damit erhält man folgende drei hypothetische Verschlüsselungsergebnisse:

In Stellung S verschlüsselt ENIGMA w als E,

" S+1 " " e als T,

" S+3 " " t als W.

TURING hatte nun eine weitere geniale Idee: Man könnte die hypothetischen Buchstaben-Schleifen elektrisch realisieren und drei ENIGMA-Maschinen ebenso elektrisch miteinander verbinden, und zwar so, daß sich die Wirkung der Steckerbretter aufhebt und überdies eine aufleuchtende Glühbirne im Stromkreis anzeigt, wenn die passenden Walzenstellungen eingerastet sind, das *crib* also nicht mehr widersprüchlich ist:

[264] Vgl. Singh, Simon: Geheime Botschaften, S. 212-213.
[265] Bild nach Singh, a.a.O., S. 212.

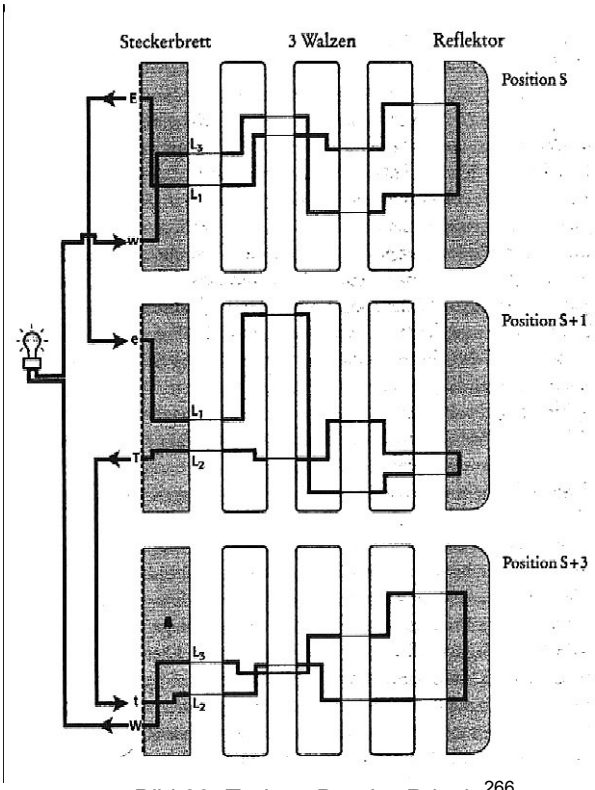


Bild 39: Turings Bombe-Prinzip[266]

Im Bild ist die Stellung der drei ENIGMAs des Beispiels so dargestellt, daß die *crib*-Schleifen einen durchgehenden Stromkreis bilden, der die Glühbirne aufleuchten läßt. Das wäre das Endergebnis eines Testlaufes. Bei genauer Betrachtung erkennt man die Neutralisierung der Steckerbretter: Der Strom fließt am Buchstaben w in die erste ENIGMA und verläßt die Rotoren am unbekannten Buchstaben L_1, den das Steckerbrett wieder in den Buchstaben E wandelt. Dieser Kontakt E ist nun per Draht mit dem des Buchstaben e der zweiten ENIGMA verbunden, der per Steckerbrett wieder in L_1 zurückverwandelt wird – die Vertauschung hebt sich also auf. Ebenso fließt dann der Strom aus den Rotoren der zweiten ENIGMA bei L_2 über das Steckerbrett nach T, und von dort in den korrespondierenden Buchstaben t/L_2 der dritten ENIGMA, wo er wieder als L_3/w austritt und via Glühbirne nach w der ersten ENIGMA gelangt.

Mit anderen Worten: TURING zeigte mit diesem hypothetischen Modell, wie für ein bestimmtes *crib* der zugehörende ENIGMA-Schlüssel ermittelbar ist, weil sich die Wirkung der ENIGMA-Steckerbretter gegenseitig aufhebt. Er konnte sie daher in der geplanten Maschine weglassen; es genügte, den Ausgang der ersten Rotorenreihe L_1 direkt mit dem Eingang L_1 der zweiten zu verbinden, und ebenso L_2 mit L_2 der dritten ENIGMA, usw. Da aber der Buchstabe L_1 unbekannt war, und alle 26 Buchstaben in Frage kamen, mußten alle 26 Walzenausgänge der ersten ENIGMA mit allen korrespondierenden Eingängen der zweiten Maschine verbunden werden, usw. So entstanden 26 Stromkreise, die, mit einer Glühbirne

[266] Bild nach Singh, Simon: Geheime Botschaften, S. 216.

als Indikator versehen, dann aufleuchten würden, wenn der jeweilige Kreis geschlossen und die gesuchte Einstellung gefunden war.

Die drei Schleifen des Beispiel-*cribs* können nun mit dieser Schaltung hypothetisch durchgetestet werden, wozu max. 17.576 [267] Walzenstellungen zu prüfen sind in max. 5 Stunden, unterstellt man pro Sekunde eine Testung. Hinzu kommen noch 60 mögliche Walzenlagen, die bei Auswahl der drei aus fünf Tauschwalzen möglich sind, mithin läge in maximal 300 Stunden, im Mittel also in einer Woche, die Entzifferung vor. Anschließend mußte man noch durch Probieren auf einer ENIGMA herausfinden, welche Steckerverbindungen geschaltet waren, doch das erforderte nur geringen Aufwand, weil Klar- und Geheimtext ja nun vorlagen.[268]

Diese hypothetische Betrachtung SINGHS berücksichtigt jedoch nicht, daß längst nicht jede Walzenstellung zu testen ist, weil die reziproke ENIGMA einen Buchstaben nicht mit sich selbst verschlüsseln kann, und ferner die Lage des Klartextwortes im Geheimtext ungefähr bekannt, der Suchraum entsprechend eingeschränkt ist. Überdies schaltet jeder Widerspruch, d.h. jede Verwerfung einer Rotorstellung bereits durch nur eine Schleife die Maschine zur nächsten möglichen Stellung weiter. Das reduziert drastisch die erforderlichen Testungen, und genau das ist ein wesentlicher Teil des Turing'schen Verfahrens.

Der Turing-Biograph A. HODGES kommentierte die geniale Idee TURINGS mit *„It was he [TURING] who first formulated the principle of mechanizing a search for logical consistency based on a ‚probable word'."*[269] Man sollte hinzufügen, daß die Neutralisierung der Steckerbrett-Überschlüsselung mindestens dieselbe Bedeutung hatte, jedoch aus unbekannten Gründen in der Literatur meist „vergessen" wird.

Und für den Fall, daß die Methode des wahrscheinlichen Wortes einmal nicht zum Ziel führte, hatte TURING die polnische Lochkartenmethode (*Zygalski sheets*) vervollkommnet (*Banburism*), und eine kryptologische Bewertung der gefundenen Parallelstellen entwickelt (*weight of evidence*). Damit konnten nach HODGES die zu testenden Walzenlagen stark verringert werden.[270]

Turing-BOMBE

Nach dem vorerwähnten hypothetischen Beispiel plante TURING eine BOMBE-Maschine zunächst mit 12 elektrisch gekoppelten ENIGMA-Simulatoren, so daß 12 Suchschleifen zur Verfügung standen. Damit konnte man auch längere Klartextsequenzen als *crib* nutzen und/oder den Suchbereich für die Lage des

[267] Singh gibt hier einen falschen Wert an, einem verbreiteten Irrtum folgend. Richtig ist 16.900 (s. 3.2.2).
[268] Vgl. Singh, Simon: Geheime Botschaften, S. 211-215.
[269] Zit. nach Hodges, Turing, S. 424
[270] Hodges, Turing, S. 424.

cribs im Geheimtext verbreitern, wodurch schnellere bzw. zuverlässigere Ergebnisse zu erwarten waren.

Anfang 1940 schloß TURING seine Planung ab, und es bedurfte nun es eines hervorragenden Ingenieurs, der aus diesen Ideen eine gut funktionierende Maschine konstruierte und schnell baute. Das gelang Harold KEEN und seinem kleinen Arbeitsteam in der mit dem Bau beauftragten Firma British Tabulating Machine Co. (BTM). Bereits im Mai 1940 ging die erste elektromechanische BOMBE in Betrieb, nach nur knapp 4 Monaten Konstruktions- und Bauzeit für dieses aufwendige Gerät.

Die zu dessen Betrieb erforderlichen *cribs* waren nicht schwer zu finden: Die Sprache der deutschen Funksendungen war sehr schematisch, bestimmte Strukturen, Worte und Wortkombinationen wiederholten sich in den alltäglichen Routinemeldungen. Und die deutschen Offiziere sorgten – unfreiwillig – für ständigen Nachschub, weil sie elementare kryptologische Grundlagen nicht beachteten, wie im Abschnitt 5.4.1 näher ausgeführt ist.

Die Militärs (und besonders CHURCHILL) forderten nach Kriegsbeginn dringend Informationen aus Entzifferungen, daher blieb zunächst nur das Lochkartenverfahren bis zum Betriebsbeginn der BOMBE. Dieses Verfahren mußte jedoch erst den neuen ENIGMA-Betriebsvorschriften angepaßt werden. Ein Arbeitsteam unter Leitung des Mathematikers JEFFREY (daher *Jeffrey sheets*) hatte bis Ende Dezember 1939 die neuen Lochkarten komplettiert und Sätze davon den in Frankreich arbeitenden polnischen Kollegen übergeben, denen damit am 17. Januar 1940 die ersten Entzifferungen der ENIGMA I gelangen. Bis zur Besetzung Frankreichs am 22. Juni 1940 sollen über 4000 Sendungen entziffert worden sein, die meisten davon in BP.[271] Wieviel davon der am 14. Mai 1940 installierten ersten Turing-BOMBE zuzuordnen sind, ist nicht bekannt.

Nach SINGH arbeitete die inzwischen installierte BOMBE-Maschine unerwartet langsam und benötigte bis zu einer Woche, um eine passende ENIGMA-Einstellung zu finden.[272] Die Gründe für die mangelnde Leistung dieser ersten Maschine nannte SALE: Man hatte wenig Erfahrungen mit *cribs* und es kam daher zu häufigen Fehlstops der Maschine. Dementsprechend benötigte man zusätzliche Suchschleifen; man installierte dann davon 36 im verbesserten Nachfolgemodell (August 1940), statt nur 12 wie bisher. Eine weitere wesentliche Verbesserung war, nach einer Idee des Mathematikers WELSHMAN, ein sog. *diagonal board,* das es ermöglichte, den Ein- und Ausgang der BOMBE-Schaltung gleichzeitig zu testen. Damit stieg die Effizienz der Suche drastisch und überdies reichten kürzere *cribs* aus. Die später für die Maschine (s. Bild 41) übliche

[271] Vgl. Bloch, Polish Work, S. 397-399. Vgl. hingegen Smith, Michael: Enigma entschlüsselt, S. 63, der die ersten Entzifferungen den britischen Kryptanalytikern zuschreibt.

[272] Vgl. Singh, Simon: Geheime Botschaften, S. 218.

Bezeichnung „Turing-Welshman-Bombe“ scheint insoweit gerechtfertigt.[273]
Der prinzipielle Unterschied beider BOMBE-Varianten bestand darin, daß TURINGS Entwurf universell anwendbar war und nicht auf dem reziproken[274] ENIGMA-Verfahren beruhte, während WELSHMANS Ergänzung genau das voraussetzte. Dieser scheinbar unwesentliche Unterschied wurde 1944 wichtig, als „Umkehrwalze D“ und „Steckeruhr“ (s. 3.2.3) die ENIGMA-Reziprozität aufhoben und die BOMBE-Maschinen bei damit chiffrierten Sendungen versagten.[275]

Bis Kriegsende installierte man 211 Turing-Welshman-BOMBEN in verschiedenen Versionen in BP und dessen Außenstellen; deren 24-Stunden-Betrieb sicherten 265 Mechaniker, und dazu benötigte man 1675 weibliche Hilfskräfte (*WRENS*) zur Bedienung.[276]

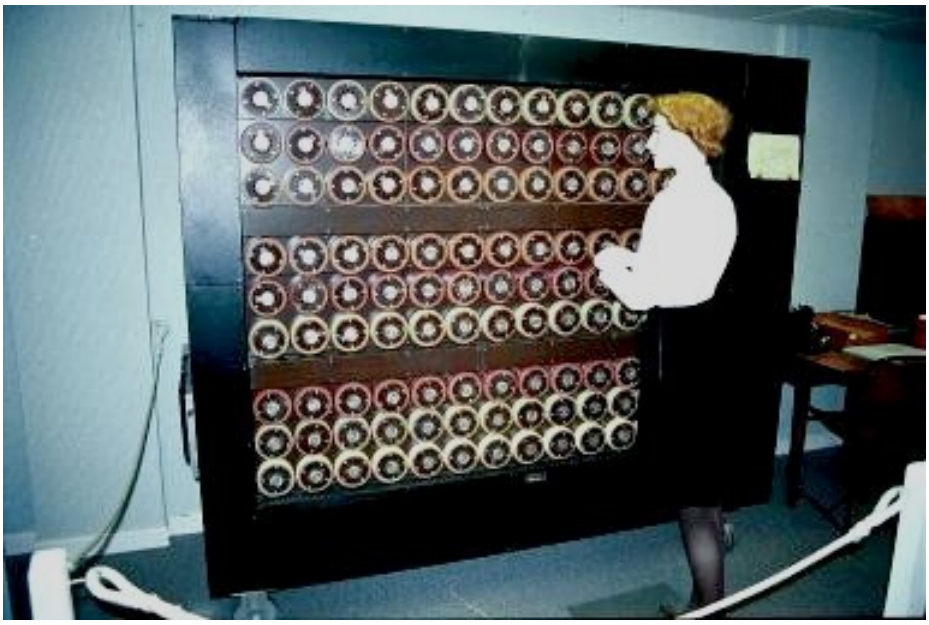


Bild 40: Turing-Welshman-Bombe[277]

Die Leistungen des Ingenieurs KEEN und dessen Team bei Konstruktion und Bau der verschiedenen BOMBE-Varianten offenbart sich erst in den letzten Jahren, seitdem versucht wird, eine BOMBE zu rekonstruieren. Dabei sind diffizile Probleme zu lösen, so daß auch nach mehreren Jahren die Arbeit noch nicht abgeschlossen werden konnte.

---

[273] Vgl. Sale, T.: Virtual Wartime Bletchley Park. In: Codes and Ciphers.
[274] Feste Zuordnung der Buchstaben beim Ver- und Entschlüsseln. Die Umkehrwalze hatte ENIGMA bereits reziprok gemacht; das Steckerfeld bewahrte diese Eigenschaft.
[275] Vgl. Deavours, C.A./Kruh, L.: The Turing Bombe: Was it enough? ,In: Deavours, Cipher A. (Eds.), Selections from Cryptologia, Volume XIV, Nr. 4, October 1990.
[276] Vgl. Erskine, Ralph: Breaking Air Force and Army Enigma. In: Erskine/Smith, Action, S. 58.
[277] Bild nach Hamer, D.: Bombe Rebuild Project, Versions of the Bombe.

TURING beschrieb dann die Methoden zur Brechung der ENIGMA-Verschlüsselung in einer ausführlichen Abhandlung[278] in 1940, wohl um den Kryptologen in BP quasi ein Handbuch zur Verfügung zu stellen, das auch ihre US-Kollegen – vermutlich 1942 – erhielten. Es enthält die Methoden zur Rekonstruktion der Verdrahtungen der ENIGMA-Walzen, das von ihm verbesserte Lochkartenverfahren, und das von ihm entwickelte maschinelle BOMBE-Verfahren. Auch erste Überlegungen zur Brechung der Marine-ENIGMA M3 sind enthalten, was aber erst 1941 gelang. Dieses für die ENIGMA-Brechung grundlegende Dokument wurde erst 1996 deklassifiziert.
TURING'S Biograph A. HODGES bezeichnet es als "*…perhaps his [Turings] greatest individual contribution to history*", wobei man einschränken muß, daß noch manches über TURINGS Leistungen in BP und den USA mangels zugänglichen Dokumenten ungeklärt ist.

TURINGS Methode des wahrscheinlichen Wortes, die Gewinnung und Verwendung von *cribs,* wird im Prinzip auch heute noch angewendet, obwohl leistungsstarke Computer zur Verfügung stehen. Doch die damit üblichen *brute force attacks*, dem Durchtesten aller Schlüssel, sucht man zu vermeiden wegen hoher Kosten bzw. langer Rechenzeit, und benutzt, wenn immer möglich, bewährte kryptanalytische Methoden, die auf TURING zurückgehen:

Nach ECKERT ist ein „Angriff mit bekanntem Klartext" [= *crib*] (*known plaintext attack*) möglich, wenn der Angreifer sich auf anderen Wegen Informationen über den Geheimtext beschaffen kann bzw. diese im Kontext der Nachricht verborgen sind. Darüber hinaus kann der Angreifer sich sogar passende Geheimtexte „verschaffen", indem er ausgewählten Klartext mit dem Verfahren verschlüsseln läßt, dem sog. „Angriff mit gewähltem Klartext" [= *depth*] (*chosen plaintext attack*), um den Schlüssel bloßstellen zu können.[279]

Auch diese Methode verwendeten die Entzifferer bereits in BP, indem sie deutsche Dienststellen veranlaßten, bekannte Begriffe unfreiwillig zu verschlüsseln (Tarnbezeichnung *gardening*): Sie ließen bspw. eine Markierungs-tonne einer Hafeneinfahrt zerstören, und konnten dann sicher sein, sehr bald chiffrierte Warnmeldungen zu erhalten wie „Markierungstonne Einfahrt Calais zerstört" usw. Überdies verbreiteten die deutschen Dienststellen diese Warnmeldungen fast immer mit verschiedenen Verfahren verschlüsselt (etwa Werftschlüssel und ENIGMA M3 und/oder M4), dazu wortgleich, womit BP dann per Klartext-Geheimtext-Kompromittierungen etwaige Probleme mit einem dieser Verfahren lösen konnte.

---

[278] Turing, A.M.: Treatise on Enigma. NARA-Dokument Record Group 457, NSA Coll. Box 201, Nr. 964. Rekonstruiert und editiert von Erskine, R., Marks, P. und Weierud, F., Febr. 1999. Von: http://mad.home.cern.ch/frode/crypto.htm, am 14.01.03.

[279] Vgl. Eckert, Claudia: IT-Sicherheit, S. 280.

5.2.3 Turing und die Marine-ENIGMA M3/M4

Nachdem die BOMBE-Maschinen zufriedenstellend arbeiteten und vor allem Sendungen der deutschen Luftwaffe entziffert werden konnten (das Heer hielt bessere Chiffrierdisziplin), übernahm TURING die dringende Aufgabe, auch für die Marine-ENIGMA M3 eine Entzifferungsmethode zu finden. Er suchte nach einer Lösung, zusammen mit weiteren Mathematikern und anderen Wissenschaftlern, einer „*...aristocracy of intelligence*...“[280], die sich in der „Hut 8“, wie die Marinesektion in BP hieß, zusammenfand.

Doch die Lösung war alles andere als einfach:
Die M3-Operatoren verwendeten nach Kriegsbeginn acht Walzen, von denen jeweils drei in die Maschine einzusetzen waren, statt drei aus fünf wie bei der ENIGMA I, womit nun 336 Walzenlagen gegenüber den 60 der ENIGMA I zu prüfen waren. Darüber hinaus wurde die Spruchschlüsselvereinbarung seit 1937 jeweils mit „Bigramm-Tabellen“ überschlüsselt.[281] Hinzu kam eine Überschlüsselung der Positionskoordinaten mit einer geheimen Seekarte („Quadratkarte“), welche die im Seekrieg besonders wichtigen Positionsangaben bei etwaigen Entzifferungen unlesbar machen sollte.

Der für Großbritannien ungünstige Kriegsverlauf mit hohen Verlusten durch den U-Boot-Krieg konnte besonders durch die Entzifferung des U-Boot-Nachrichtenverkehrs positiv beeinflußt werden. Denn mit den entzifferten Nachrichten ließen sich im *U-Boat-tracking room* in London die Boot-Positionen, -Kurse und -Zielgebiete viel besser verfolgen, teilweise im voraus, und damit konnte die Admiralität Konvois umleiten oder Zerstörer und Bombenflugzeuge gezielt einsetzen.

Für eine zeitaufwendige Kryptanalyse der ENIGMA M3 blieb keine Zeit, denn dafür hätte man viele Monate benötigt. Überdies fehlten dazu wichtige Geheimunterlagen: Neben den unbekannten drei zusätzlichen Walzen benötigte man „Quadratkarte“, „Kurzsignalheft“ (für taktische Berichte verwendet) und „Wetter-Kurzschlüssel“ zur Gewinnung von *cribs*. Dieses Material konnte in kurzer Zeit nur durch Aufbringungen beschafft werden und so erhielt die Royal Navy den Auftrag, das durch gezielte Angriffe zu versuchen. Freilich wurde das lange bestritten, weil manche Aktionen beinahe Kriegsverbrechen waren, doch inzwischen bestätigten sogar britische Historiker die nicht mehr zu kaschierenden Kaperungen. Beispielsweise räumte ERSKINE ein, daß die geheimen Chiffrierunterlagen „[...] in eigens geplanten Überfällen auf die Wetterschiffe München und Lauenburg erbeutet wurden.“[282]
Ein anderer Beleg dafür stammt vom Turing-Biographen A. HODGES, der sich auf

[280] Hodges, Turing, S. 204.
[281] Ausf. in: Bauer, Geheimnisse, S. 63.
[282] Erskine, Ralph: Der Krieg der Code-Brecher. In: Akademie aktuell Nov. 2002, Zeitschrift der Bayerischen Akademie der Wissenschaften, S. 9. Übers.: J. Müller. Bearbeitet von F.L. Bauer.

ein erst 1996 deklassifiziertes Dokument beruft: Danach hatten in 1940 die Kryptanalytiker in BP Probleme, denn: „*... the Banburismus method*[283] *could not be brought into use for lack of sufficient captured material, and that the analysts pressed the navy to undertake captures*."[284]

Die Royal Navy meldete bald Erfolge: Die Walzen 6 und 7 (die ersten 5 waren identisch mit denen der ENIGMA I und bereits von den polnischen Kryptologen rekonstruiert, s. 5.2.1) erbeutete man im Februar 1940 durch Aufbringung von U-33, die letzte 8. Walze im August 1940.[285] Erste Entzifferungen gelangen damit ab Mai 1940 gelegentlich, doch erst am 9. Mai 1941 brachte eine U-Boot-Kaperung eine komplette ENIGMA M3 sowie alle Geheimunterlagen in britische Hand.[286] Damit konnte BP die Sendungen des laufenden Monats direkt entziffern, und ab August 1941 beherrschte man die ENIGMA M3 nach Anpassung der BOMBE-Maschinen. Man benötigte ca. 36 Stunden für die Entzifferungen nach dem Schlüsselwechsel (aller 2 Tage), sonst weniger als 17 min.[287]
Die damit ermöglichten Erfolge der Royal Navy konnte sich die deutsche Seekriegsleitung nur durch Verrat erklären. Die freilich ebenso mögliche Funkentzifferung wurde hingegen stets bestritten (s. ausf. unter 5.2.3).

Blackout nach Einführung der M4

Dennoch mißtrauten einige Verantwortliche der Sicherheit der ENIGMA-Chiffrierung und sorgten für die Beschaffung einer verbesserten Maschine: Diese am 1.2.1942 eingeführte ENIGMA M4 machte das bisherige Entzifferungsverfahren in BP obsolet, denn eine zusätzliche vierte Walze "ß" („Griechenwalze") bewirkte eine zunächst nicht zu überwindende Erschwernis. Überdies verhinderte ein neu eingeführtes Wetterkurzschlüsselheft, daß die aus den Wettermeldungen bisher gewonnenen *cribs* weiter zur Verfügung standen.

TURING und seine Kollegen arbeiteten intensiv an einer Lösung und wußten bald, welche Verfahrensänderungen erfolgversprechend waren: Sie hatten bereits die innere Verdrahtung der neuen Walze rekonstruiert, weil sie einen (typisch?) deutschen Fehler nutzen konnten: Noch vor der Einführung der 4. Walze (am 1.2.1942) sendeten einige Funkstellen irrtümlich Nachrichten unter Verwendung der neuen Walze, denn das neue Verfahren mußte ja über den Äther geübt werden, nach Meinung deutscher Nachrichtenoffiziere. Doch einmal konnte die Gegenstelle nicht entschlüsseln, sie hatte die 4. Walze noch nicht, und daher wurde der Text erneut gesendet, diesmal korrekt mit der 3-Walzen-Einstellung –

[283] Das von Turing verbesserte Lochkartenverfahren.
[284] Mahon, A. P.: The History of Hut Eight, a report of 1945 released by the National Security Agency, Washington DC, 1996; reference NR 4685, box 1424, RG 457, National Records and Archives Adminstration. Von: http://www.turing.org.uk/publications/profsbook.html, am 3.10.03.
[285] Vgl. Erskine, Ralph: Der Krieg der Code-Brecher, S. 8.
[286] Nach Ansicht deutscher Autoren durch ein Kriegsverbrechen. Ausführlich in: Brennecke, J.: Die Wende im U-Boot-Krieg, S. 77 ff. Der Vorfall konnte 13 Jahre geheim gehalten werden.
[287] Vgl. Erskine, Ralph: Der Krieg der Code-Brecher, S. 9.

und „Hut 8“ konnte per Klartext-GeheimtextKompromittierung allmählich die Verdrahtung rekonstruieren – denn den alten M3-Modus beherrschte BP inzwischen.[288]

Damit konnte BP jedoch noch nicht maschinell entziffern, denn es fehlten modifizierte, d.h. schnellere BOMBE-Maschinen, und nur Elektronik konnte nach TURINGS Überzeugung die geforderte Geschwindigkeit bieten, Relais waren zu langsam. Man konsultierte also Elektroniker, zuerst den TURING gut bekannten Cambridge-Physiker WYNN-WILLIAMS (s. 6.2.3), der inzwischen Radarelektronik entwickelte. Doch sein Entwurf eines schnellen Zusatzes zur BOMBE, ein *high speed rotor*, bewährte sich nicht. Inzwischen hatte man auch Tommy FLOWERS (s. 6.2.1) angesprochen, der dem BOMBE-Konstrukteur Harold KEEN vorschlug, die Maschine mit elektronischen Modulen aufzurüsten. Das aber wurde zurückgewiesen, man hielt Digitalelektronik für unzuverlässig.[289]
Abgesehen von den zu langsamen BOMBE-Maschinen – es fehlten auch die zu deren Betrieb erforderlichen *cribs*, doch bei der Aufbringung von U-559 am 30.10.1942 erbeutete die Royal Navy auch das neue Wetterkurzschlüsselheft. In BP stellte man bei dessen Analyse fest, daß die Maschine M4 für Wettersendungen im bisherigen M3-Modus betrieben wurde, damit diese Nachrichten auch von den Küstenstationen und sonstigen Schiffen – die nur über von BP geknackte M3-Maschinen verfügten – gelesen werden konnten.[290] Dieser grobe Fehler kompromittierte die M4-Chiffrierung, denn nun verfügte BP wieder über *depths*; und damit gelang bereits am 13.12.1942 die erste M4-Entzifferung: Man präsentierte der Admiralität „... die Positionen von mehr als 12 U-Booten im Atlantik ....“ [291]

Den Wetter-Modus der M4 – identisch mit der M3-Verschlüsselung – erreichte man durch Neutralstellung der 4. Walze, die in „Lage Null“ gesetzt wurde. Damit zahlte man einen hohen Preis für die Herstellung der Kompatibilität beider Maschinen, denn nun konnte BP die jeweiligen Einstellungen der drei Walzen ermitteln, mit dem Entzifferungsverfahren der völlig gebrochenen ENIGMA M3. War aber damit diese Walzeneinstellung ermittelt, hatte man keine Problem mehr: Die deutsche Marine verwendete genau diese Einstellung auch für den reinen U-Boot-Verkehr, und ließ dazu lediglich die 4. Walze in Position setzen. Diese war unbeweglich, wurde also bei der Walzenweiterschaltung nicht mitgenommen, und so mußten zusätzlich „nur“ deren 26 Positionen getestet werden.
Dieser kaum zu begreifende Fehler der deutschen Marineoffiziere bewirkte dann die Kompromittierung der ENIGMA M4, und zur geforderten schnellen Entzifferung benötigte man „nur“ noch schnelle BOMBE-Maschinen. Daran

[288] Vgl. Smith, Michael: Enigma entschlüsselt, S. 174.
[289] Vgl. Hodges, Turing, S. 226-228.
[290] Vgl. Bletchley Park Museum: “Historical information gathered from the Bletchley Park archives”, Oct. 1942.
[291] Erskine, Ralph: Der Krieg der Code-Brecher, S. 10.

konnte TURING nicht mehr mitarbeiten, da er sich inzwischen am 7.11.1942 zu einer US-Reise eingeschifft hatte.

Turings US-Reise 1942/43

TURING reiste in die Staaten am 7. 11.1942 im geheimen Regierungsauftrag und befaßte sich dort zunächst mit Entwicklungen zur Sprachverschlüsselung (ausf. unter 6.4), die in den Bell-Laboratorien bereits weit gediehen waren. Dort stellte man ihn vor als „*the top cryptanalyst of England*" – zurecht aus heutiger Sicht – und machte ihn mit dem digitalen „Projekt X" vertraut, dem späteren SIGSALY-System. Anfang März hatte TURING seine Empfehlungen zum Projekt X zusammengestellt, und die Endmontage begann.[292] Die ersten beiden Einheiten sollten dann in Washington und London installiert werden zur Sicherung der hochgeheimen Telefongespräche CHURCHILLS mit dem US-Präsidenten.

Zwischendurch und nochmals Mitte März beriet TURING den US-Navy-Geheimdienst, der den Bau einer schnellen teilelektronischen US-BOMBE gegen die ENIGMA M4 plante (s. 6.3.3), und die in 1943 realisiert wurde. Anschließend (am 23.3.1943) fuhr er zurück nach England und nahm seine Arbeit in der Hut 8 in BP wieder auf. Da aber inzwischen die ENIGMA M4-Entzifferungen keine grundlegenden Probleme mehr bereiteten, befaßte sich TURING zunehmend mit einer britischen Sprachverschlüsselung, die weit weniger aufwendig sein sollte als das US-SIGSALY-System (s. 6.4.3). Er verließ daher im Herbst 1943 BP und begann mit deren Entwicklung in Hanslope Park, einer Station des Geheimdienstes MI6. Das Gerät war zum Kriegsende nahezu fertig, doch wurde das Projekt nicht mehr fortgesetzt. TURING ging dann zum National Physical Laboratory und begann dort einen speicherprogrammierbaren Rechner zu entwerfen, das sog ACE-Projekt (s. 7.3.2).

Die 4-Rotoren-BOMBE

Nachdem die erwähnten Versuche gescheitert waren, mit 3-Rotoren-BOMBS und Zusatzgeräten die M4-Sendungen zu entziffern, entwickelte BP (ohne den abwesenden TURING) die nun erforderliche 4-Rotoren-BOMBE, die dann aber mangels Ressourcen nicht in genügender Stückzahl gebaut wurde. Überdies erbrachte diese teilelektronische Maschine nicht die geplante Leistung, und ließ sich auch nicht mehr verbessern (s. 6.3.4).
Der US-Navy-Dienst OP-20-G konnte hingegen reichlich Mittel einsetzen und baute (mit TURINGS Beratung) leistungsstarke teilelektronische Desch-BOMBs (s. 6.3.3) in ausreichender Zahl, so daß er die M4-Entzifferungsarbeit ab Spätherbst 1943 vollständig übernehmen konnte.
Damit war die ENIGMA M4 endgültig gebrochen.

[292] Vgl. Hodges, Turing, S. 245-252.

5.2.4 wichtige ENIGMA-Varianten

Reichsbahn-ENIGMA
Die Reichsbahn verfügte über kommerzielle Vorkriegs-ENIGMA D-Maschinen, deren Walzen sie neu verdrahten ließ. Diese Maschinen setzte sie im besetzten Gebiet Osteuropas und des Balkans ein, denn dort gab es keine funktionierenden Eisenbahn-Telefonlinien, so daß Transportnachrichten gesendet werden mußten. BP registrierte erstmals am 15. Juli 1940 damit verschlüsselte Sendungen, die offenbar Bahn-Transportmeldungen betrafen. Die zugehörige Chiffriermaschine nannte man daher „*Railway*-ENIGMA", und dieser neue Schlüsselkreis erhielt die Tarnbezeichnung „ROCKET I".[293] Es gelang bald, diese neuen Rotoren zu rekonstruieren und die relativ einfache Chiffrierung zu brechen, obwohl *cribs* zunächst fehlten. Und man erkannte die große Bedeutung dieser regionalen Transportmeldungen für längerfristige Planungen.

Im September 1942 registrierte man eine neue Variante an der Westfront, welche die Tarnbezeichnung „ROCKET II" erhielt. Doch diese Chiffrierung widerstand allen Entzifferungsversuchen, wofür man keine Erklärung fand. BP konnte nicht einmal ermitteln, welche Maschine benutzt wurde. Und im Mai 1944 kam eine weitere Variante „ROCKET III" hinzu, die ebenfalls nicht zu entziffern war. Schließlich bat man den US-Navy-Dienst um Hilfe, der eine dafür geeignete neue Hochleistungs-Entzifferungsmaschine namens HYPO in Betrieb genommen hatte. Doch selbst ein 90-Stunden-Suchlauf dieser Maschine brachte keinen Erfolg. Immerhin konnte man damit klären, daß die ROCKET II/III-Chiffrierungen nicht durch eine „alte" Reichsbahn-ENIGMA (ROCKET I) erzeugt wurden, sondern einer unbekannten Version der ENIGMA I zuzuordnen war.
Nach dem Krieg stellte sich heraus, daß die von der Reichsbahn in Westeuropa eingesetzte Maschine eine Standard-ENIGMA I war, die jedoch ohne Walzenwechsel betrieben wurde, im Gegensatz zum täglichen Wechsel bei der Heeres-ENIGMA. Die für diese kryptanalytisch „einfache" Betriebsweise erstaunlichen Entzifferungsprobleme hatten drei Ursachen:
▪ Die Art der Nachrichten – Bahn-Transportinformationen – waren für BP „*obscur*". [Vermutlich konnte man sie nicht wie Militärnachrichten interpretieren].
▪ Man gewann daher kaum *cribs* und konnte nicht BOMBE-Maschinen einsetzen.
▪ Und ohne *cribs* und gelegentliche *re-encodements* war BP meist nicht in der Lage, in neue Verschlüsselungen einzubrechen.[294]
Dieses Beispiel demonstriert eindrücklich, daß die maschinellen Entzifferungen nicht nur die Folge sicherheitstechnischer Mängel der ENIGMA waren, wie immer wieder zu lesen ist. Vielmehr benötigte BP unbedingt dazu *cribs*, und dafür sorgten unfreiwillig die deutschen Militärs mit ihrer Nichtbeachtung kryptologischer Grundlagen, wie unter 5.4.1 näher erläutert wird.

---

[293] Vgl. Hamer, D.H., Sullivan, G., Weierud, F.: Enigma Variations. An Extended Family of Machines. In: Cryptologia; Volume XXII (3); July 1998; pp. 211-229.
[294] Vgl. Ebd.

Abwehr-ENIGMA

Diese Maschine hatte kein Steckerbrett wie die ENIGMA I, überdies war die kommerzielle Version seit 1926 bekannt, und dennoch hatten die Analytiker in BP große Probleme: Die „*very high turnover rate*“[295] der mit vielen Nocken versehenen Walzen erzeugte pseudo-irreguläre Walzenbewegungen und das zwang zur Entzifferung per Hand, die erstmals im Oktober 1941 gelang. BOMBE-Maschinen mit vier Rotoren konnte man nicht einsetzen, weil dafür zykloide Walzenbewegungen vorausgesetzt wurden, die nur die anderen ENIGMA-Varianten aufwiesen. Daher entwickelte man eine neue Maschine, eine spezielle Variante der BOMBE, genannt FUNF.[296] Wie aber damit die nicht-zykloiden, pseudo-zufälligen Bewegungen der Walzen simuliert wurden, ist unbekannt; diese Spezialmaschine unterliegt weiter strikter Geheimhaltung.

Die Schwächen der Abwehr-ENIGMA kannten auch die OKW/Chi-Kryptologen: Sie beschrieben nach dem Krieg die detaillierten Entzifferungsmöglichkeiten, die sie erarbeitet hatten. Daraufhin zog das OKW/WNV/Fu die von Militärattachés verwendeten ca. 100 Maschinen ein, und bot sie 1943 der Abwehr an. Die Verfasser konnten aber nicht sagen, ob die Schwächen offenbart wurden und die Abwehr die Maschinen auch nutzte.[297] Letzteres ist sehr wahrscheinlich, weil die Abwehr ENIGMA-Maschinen bis zum Kriegsende verwendete.

ENIGMA mit schaltbarer Umkehrwalze D

Eher weniger bekannte Maschinen zur ENIGMA-Brechung sind die Varianten der *Scritchers*.[298] Sie wurden entwickelt, nachdem Anfang 1944 in einigen Luftwaffen-Funknetzen die ENIGMA I mit schaltbarer Umkehrwalze D (UKD) eingesetzt wurde, und daraufhin Entzifferungen mit BOMBE-Maschinen nicht mehr möglich waren: Denn dazu wurde eine reziproke ENIGMA vorausgesetzt, wie unter 5.2.2 dargelegt wurde, und alle internen Stromkreise der Maschine mußten bekannt sein. Nach Einführung der UKD änderte sich jedoch diese Schaltung alle 10 Tage durch variable Steckerverbindungen, und damit die interne Verdrahtung der ENIGMA.
Nach ERSKINE hatte das zur Folge, daß man nun jeweils $3{,}2 \times 10^{11}$ mögliche innere Verbindungen aufwendig per Hand und Lochkarten analysieren mußte.[299]

---

[295] Vgl. Hamer, D.H., Sullivan, G., Weierud, F.: Enigma Variations.

[296] Vgl. Bletchley Park Museum: “Historical information gathered from the Bletchley Park archives”, Dec. 1942.

[297] TICOM I-77: Homework by Dr. Huettenhain and Dr. Fricke on Zaehlwerk (cyclometer) – Enigma. Ref. G5/80 – 1st Aug. 1945. POW/Kew (GB).

[298] Scritching = In BP verwendeter Begriff für sequentielle Testungen von Annahmen gegen andere Annahmen.

[299] Vgl. Erskine, Enigma’s Security, S. 381-382.
Ausf. in: Alexander, C.H.O’D.: Stecker Knock-Out. In: Weierud, Frode (Ed.): Frodes Kryptopage, The Alexander Papers, (Orig. BP-Dokument o.D., ca. März 1944). Von: http://mad.home.cern.ch/frode, am 29.11.02.

Doch diese Angabe ERSKINES ist unrichtig: Die genannte große Anzahl der möglichen Schaltungen der UKD, entsprechend theoretischen Berechnungen, ist jedoch nicht kryptologisch relevant, da ja immer nach dem gleichen Schema geschaltet wird. Demzufolge muß sie nicht analysiert werden, sondern, nach BAUER, „nur" die 26^3 (= $1{,}75 \times 10^4$) Anfangsstellungen, also nur ein Bruchteil.[300]

Man befürchtete in BP eine allgemeine Einführung der UKD zum 1.8.1944, wofür es Hinweise in entzifferten Meldungen gab, und traf umfangreiche Vorbereitungen, darunter die Entwicklung einer neuen Maschine. Diese erhielt den Namen GIANT, bestand im wesentlichen aus vier zusammengeschalteten BOMBE-Maschinen mit Steuerelektronik, erbrachte dann jedoch nicht die gewünschte Leistung.[301]

Der zuständige US-Army-Dienst SIS (*Signal Intelligence Service*) hingegen ließ spezielle Relaismaschinen[302] namens AUTOSCRITCHER bauen, die Ende 1944 in Betrieb gingen, deren langsames Arbeiten jedoch nicht genügte. Sie wurden daher in 1945 durch die elektronischen SUPERSCRITCHER ersetzt (s. 6.3.5).
Auch die US-Navy blieb nicht untätig: Ihr kryptanalytischer OP-20-G-Dienst entwickelte eine vergleichbare Maschine, genannt DUENNA.[303]
Beide Maschinen unterliegen weiter der Geheimhaltung, es sind keine Informationen verfügbar.

[300] Vgl. Bauer, Geheimnisse, S. 288-290.
[301] Vgl. Erskine, Enigma's Security.
[302] Der SIS mißtraute noch 1944 der Elektronik, obwohl der OP-20-G mit seiner teilelektronischen Desch-BOMBE gute Erfahrungen gemacht hatte, erst recht BP mit dem COLOSSUS.
[303] Vgl. Bauer, Geheimnisse, S. 290.

5.3 Brechung der Chiffrier-Fernschreiber

Man kann sich vorstellen, daß die Entzifferung der Kommunikation der obersten deutschen Führungsebene (HITLER, OKW, Heeresgruppen) den Alliierten kaum abschätzbare Vorteile für ihre strategischen Planungen brachte. Denn diese Sendungen enthielten oft „Geheime Kommandosachen", strategische Überlegungen und Planungen, und die daraus gewonnene *high grade intelligence* ermöglichte – zusammen mit den ENIGMA-Entzifferungen – die Optimierung der alliierten Strategie.
Diese Funksendungen[304] wurden überwiegend mit dem „Schlüsselzusatz" SZ40/42 (im Heeresdienst meist „Geheimzusatz" oder „G-Zusatz" genannt) chiffriert, weshalb BP seine Ressourcen auf die Brechung dieser Maschine konzentrierte. Man entwickelte dazu erstmals elektronische Komponenten und sammelte Erfahrungen mit binär-digitaler Datenverarbeitung. Schließlich baute man elektronische Maschinen, bis zu ersten Rechnern, und konnte nach dem Krieg dieses *know how* für die frühe Computerentwicklung nutzen.
Um so mehr interessiert hier die Frage: Wie konnten die Alliierten diese damals ganz neuartigen Maschinen bauen und einen so großen technologischen Vorsprung über Deutschland erringen?

5.3.1 Siemens-Geheimschreiber T52

Schwedischer Erfolg

Nach der deutschen Besetzung Norwegens 1940 verlief die gesamte militärische Kommunikation über gemietete Kabelkanäle via Schweden, so daß keine Funkübertragung benötigt wurde. Gleichwohl befürchtete man Kabelanzapfungen und sicherte daher die Übertragungen mit Schlüssel-fernschreibmaschinen Siemens T52a/b, die für Kabelbetrieb üblich und geeignet waren. Der schwedische Geheimdienst zeichnete diese Sendungen auf und schon im Juni 1940 konnte sie der zum Militär dienstverpflichtete Mathematiker Arne BEURLING entziffern. Er nutzte dazu u.a. die Fehler der deutschen Operatoren, die wiederholt mehrere Texte mit gleicher Schlüsseleinstellung sendeten, die erwähnten *depths*.[305]
Der britische Militärattaché DENHAM hatte Zugang zu diesen Entzifferungen, und übermittelte die Inhalte nach London.[306] Dort erkannte man daraus die enorme Bedeutung militärischer Fernschreibsendungen der obersten Führungsebene, und ordnete an, die Arbeiten zur Aufzeichnung und

[304] Kabelsendungen waren außerhalb des Reichsgebietes selten möglich und später im Krieg innerhalb auch begrenzt (Störungen durch Bombenschäden); hierfür wurden oft T52-Maschinen eingesetzt.
[305] Vgl. Beckman, B.: Svenska kryptobedrifter , The Siemens and Halske Geheimschreiber T52.
[306] Vgl. Mache, W.: Der Siemens-Geheimschreiber – ein Beitrag zur Gesch. der Telekomm. S. 90.

Entzifferung von FISH zu intensivieren, wie chiffrierte Funkfernschreibsendungen nun zur Tarnung genannt wurden.
Von den Entzifferungen erfuhr auch der finnische Militärattaché, der im Juni 1942 deutsche Kameraden warnte. Nachdem das in Berlin wenigen Eingeweihten bekannt wurde, ersetzte man diese Maschine ab 21. Juli 1942 durch die verbesserte Variante T52c (aber auch durch den SZ42); die Verwendung der T52a/b auf Funkstrecken wurde untersagt, und auf Kabelstrecken nur in von der Wehrmacht kontrollierten Gebieten gestattet. Doch beide Geräte konnten ebenso gebrochen werden: Die T52c bereits ab 13. September 1942, die SZ42 dann am 9.April 1943, und das jeweils „*fully broken*."[307]
Der schwedische Geheimdienst konnte daher Texte mit beiden Verschlüsselungen bis Ende 1943 mitlesen. Ab 1944 setzte die Wehrmacht neben dem SZ42 auch die Maschine T52d ein, die mit dem schwedischen Verfahren nicht zu brechen war.
Das große schwedische Interesse an den deutschen Geheimsendungen war vermutlich historisch bedingt: Im Ersten Weltkrieg versuchte das damalige Deutsche Reich wiederholt Schweden als Verbündeten zu gewinnen, beinahe mit Erfolg, und erreichte immerhin eine gute Zusammenarbeit für kriegswichtige Lieferungen.
Das wiederholte sich im Zweiten Weltkrieg, doch Schweden beschränkte sich auf Erzlieferungen und wollte vermutlich abwarten, wie sich die Kriegslage entwickelte. Mit Kenntnis der strategisch wichtigen Geheimen Kommandosachen der obersten deutschen Führung konnte man dies freilich zuverlässiger abschätzen.

Britische Brechung der T52c-Maschine

Da die deutsche Wehrmacht T52a/b-Maschinen fast ausschließlich auf Kabelstrecken einsetzte, wofür diese, da ohne Gleichlaufzusatz, auch konstruiert waren, konnte BP mangels abhörbarer Sendungen zunächst nichts entziffern. So registrierte BP erst im Sommer 1941 Funkfernschreib-Sendungen, mit einer Maschine verschlüsselt, die man noch nicht kannte. Daß es eine modifizierte T52a/b war, nämlich eine T52c, stellte man erst später fest. Man erkannte bald, daß es verschlüsselte Fernschreibsendungen waren, deren Bedeutung in BP bekannt war aus schwedischen Entzifferungen.
Wiederum erleichterten deutsche Chiffriergewohnheiten den Analytikern die Arbeit: WEIERUD berichtet, daß bspw. die Operatoren die Gewohnheit hatten, viele Sendungen mit der gleichen Maschineneinstellung zu senden. Darüber hinaus verständigten sie sich jeweils anschließend in Klartext („*operator chat*") mit ihren Kollegen der Empfangsstelle, gaben dann das Umschaltsignal, und schalteten zur Ausgangs-Schlüsselstellung zurück. Dementsprechend sammelten sich in BP die *depths,* und schließlich standen unglaubliche 40 *depths* für die erste Brechung zur Verfügung; die Analytiker konnten so problemlos die Maschine rekonstruieren.[308]

---

[307] Vgl. Beckman, B.: Svenska kryptobedrifter. Kurzfassung in: Teleprinter Ciphers, „The Siemens and Halske Geheimschreiber T52." Von: http://hem.passagen.se/tan01/tele.html, am 15.02.02.
[308] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 2-4.

Dabei konstatierten sie, daß es sich um eine kryptologisch schwache Maschine handelte wegen der festen Anordnung der Schlüsselwalzen („*fixed code wheels pattern*"), die darüber hinaus noch mit dem ENIGMA-Fehler behaftet war, nämlich daß kein Buchstabe mit sich selbst verschlüsselt werden konnte. Das half sehr bei der Auswertung der *depths* und der Plazierung von *cribs*.[309]

Doch letztlich entscheident für die Gewinnung der zahlreichen *depths,* der Ursache für diese „leichte" Brechung der T52c, war ein Schalthebel, womit die Schlüsselwalzen in ihre Ausgangsposition zurückgesetzt wurden. WEIERUD nennt das „*a blunder of some magnitude*".[310] Denn damit waren *depths* vorprogrammiert, weil die offenbar nicht entsprechend unterwiesenen Operatoren diese Betriebsart häufig anwendeten. Überdies wäre dieser Hebel für die T52c gar nicht erforderlich gewesen: Er stammte aus der T52a/b-Maschine, die keine Spruchschlüssel-Einstellvorrichtung besaß, und dort zum Setzen des Spruchschlüssels diente, indem zuvor die Schlüsselradstellung zurückgesetzt wurde.
Diese offenkundige Schwäche der T52c bemerkten dann auch Verantwortliche der Luftwaffe, denn am 17. Oktober 1942 wies die Luftflotte 2 den Fliegerführer Afrika an, wegen Sicherheitsmängeln alle Geheimsachen vor der Sendung mit T52c-Maschinen per ENIGMA vorzuschlüsseln.[311] Das aber steht im Widerspruch zu der auch für die Luftwaffe gültigen „Schlüsselfernschreibvorschrift" des OKW vom 1.12.1942, wonach T52c-Maschinen (neben SZ40) zur Übermittlung von Geheimsendungen über Funklinien zulässig waren, und zwar ohne Vorverschlüsselung.[312] Mithin hatte die Luftwaffe das OKW/Chi nicht über ihre Sicherheitsbedenken informiert.

Doch diese Anweisung beachteten die Operatoren ohnehin nicht, vermutlich weil ihre Vorgesetzten das mangels kryptologischer Grundkenntnisse nicht kontrollierten, denn BP entzifferte weiter T52c-Sendungen. Dabei halfen Übungssendungen auf drei Linien mit T52a/b-Maschinen: WEIERUD wundert sich darüber, daß die Luftwaffen-Nachrichtenführer nicht die engen kryptologischen Gemeinsamkeiten der beiden Maschinentypen erkannten, und so den Entzifferern die Arbeit sehr erleichterten.[313] Er konnte jedoch nicht wissen, daß diese – er nennt sie „*cipherofficers*" – kaum etwas von Kryptologie verstanden, ein Problem, das im Abschnitt 5.4.3 näher beleuchtet wird. Offenbar erst im Februar 1943 erkannten auch andere Dienststellen die Schwäche der T52c: Sie sei „*badly compromised*", wie entzifferten Abwehrnachrichten der Verbindung von Madrid nach Paris zu entnehmen war. In der Folge erließ man strenge Vorschriften (18.2.1943), die u.a. eine neue Spruchschlüsselprozedur anordneten und [– nun

[309] Ebd. Weierud beruft sich dabei auf einen „Unknown Author": Sturgeon Type Ciphers (Research Section, November 1944). Addendum to Captain Walter J. Fried's report No. 116 of 17 Nov. 1944.
[310] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 9.
[311] Ebd. S. 14, nach in BP entzifferten Nachrichten. Weierud konnte jedoch bisher nicht den Wortlaut dieser Nachrichten an die T52c-Funkstellen einsehen.
[312] S. Anm. 189.
[313] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 15.

erst sah man den groben Fehler –] befahlen, den Hebel zum Zurücksetzen der Schlüsselräder zu entfernen. Vorläufig mußten Geheimsachen mit einer ENIGMA vorverschlüsselt werden, bis die „adaptierte" T52ca-Maschine zur Verfügung stand.[314] Bei dieser hatte man den Grundschlüssel, den die innere Verdrahtung der Relais darstellte, wesentlich verändert. Die Bezeichnung T52ca wurde im Juli 1943 wieder ersetzt durch T52c.

Schwächen der T52c waren längst bekannt

Die Brechung der T52c-Maschine hatte eine Vorgeschichte: Bereits 1939 prüfte der OKW/Chi-Kryptologe HÜTTENHAIN (s. 5.5) die Maschine T52a/b und konstatierte einen sehr geringen Sicherheitsgrad („*extraordinary low degree of security*"), weshalb die Maschine leicht zu brechen sei.[315]
Daraufhin habe, nach WEIERUD, das OKW/Chi Veränderungen gefordert, vor allem unregelmäßige Schlüsselradbewegungen, was jedoch vom Herstellerwerk aus konstruktiven Gründen abgelehnt wurde. Stattdessen lieferten Siemens & Halske das modifizierte Modell T52c, das jedoch aus den geschilderten Gründen ebenso kryptologisch schwach war.[316]

Diese Darstellung WEIERUDS überzeugt nicht, denn bereits 1934 erhielt das Werk ein Patent[317] zuerkannt für die unregelmäßige Walzenfortschaltung, und baute nach Anforderung damit in 1943 das Modell T52d. Vielmehr ist anzunehmen, daß man im zuständigen Waffenamt (Abt. Wa Prüf 7) die Meinung des Beamten HÜTTENAIN damals nicht ernst nahm, eine deutsche Besonderheit, die WEIERUD sich wohl nicht vorstellen konnte. (s. dazu 5.4).

Ebenso wenig überzeugend berichtet WEIERUD über das weitere Vorgehen:
Die neue Maschine T52c soll der Kryptologe DÖRING geprüft haben, der dem OKH/Gen d Na (General der Nachrichten-Aufklärung) unterstand. Er konnte zeigen, daß bereits ein Text mit 1000 Buchstaben zur Brechung ausreichte; zur Analyse soll er kryptanalytische Maschinen des OKW/Chi [Dehomag D11] genutzt haben; die Mitarbeit HÜTTENHAINS sei unbekannt. Diese Untersuchung habe dann zur Entwicklung und Produktion der Maschine T52d geführt, die DÖRING dann ebenfalls prüfte und bereits „*early in 1943*" zeigte, die Maschine sei unsicher. Das resultierte dann in der „*production*" des Modells T52e.[318]

WEIERUD nennt hierzu keine Quellen, und auch sonst ist sein Bericht an dieser Stelle wenig wahrscheinlich, denn: Die OKW-Abt. Nachrichten-Aufklärung war nicht zuständig für Chiffriermittel, verfügte allerdings zur Entzifferung über Dehomag D11-Maschinen und mußte mithin nicht die des OKW/Chi nutzen, was

[314] Ebd., S. 16.
[315] Vgl. TICOM I-45: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines. Written by Huettenhain and Fricke, 1.8.1945.
[316] Vgl. Weierud a.a.O.
[317] DRP 641560 vom 3.12.1934, Archiv Mache.
[318] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, S. 16-17.

auch kaum vorstellbar ist. Ebenso unrealistisch ist die Prüfung der T52d im frühen 1943, denn damals begann vermutlich gerade deren Entwicklung; erste Maschinen sollen im Oktober 1943 eingesetzt worden sein.

Konnte BP die T52d/e-Maschinen nicht brechen?

Diese Meinung ist besonders bei „Ehemaligen" verbreitet, mit der Begründung, es gäbe ja keine entzifferten T52d/e-Sendungen unter den im *Public Record Office (Kew)* zugänglichen Dokumenten. Aber: Diese Dokumente sind nicht danach gekennzeichnet, mit welcher Maschine jeweils die Sendung verschlüsselt wurde. Man muß daher zur Klärung dieser Frage auf interne BP-Dokumente bzw. Berichte damaliger BP-Mitarbeiter zurückgreifen, die inzwischen teilweise einsehbar sind.

Vorab ist festzuhalten, daß T52-Sendungen in BP weniger intensiv bearbeitet wurden als die der SZ42, denn: London interessierte sich wesentlich mehr für die strategisch wichtigen Informationen aus HITLERS Hauptquartier und den Heeresgruppen-Kommandos und entschied daher im Frühjahr 1942, die Ressourcen auf die *TUNNY-links*, den vom Heer betriebenen SZ42-Linien, zu konzentrieren. Ohnehin genügten die Informationen aus dem Heer nicht, im Gegensatz zu Luftwaffe und Marine, wo ein „*immense amount*" aus Entzifferungen von ENIGMA-Sendungen anfiel. Vor allem aber enthielten die Entzifferungen der mit TUNNY [SZ42] verschlüsselten Sendungen viele Informationen über die Gedanken, Planungen und strategischen Diskussionen der obersten Führung, deren *intelligence* auch dann nützlich war, wenn sie mit Verzögerung entziffert wurde.[319]

Man wollte aber auch den sowjetischen Verbündeten mit Informationen unterstützen, die ein geheimes Verbindungsbüro in Moskau übermittelte.[320] Das war in London sehr umstritten, weil man die Enttarnung des ULTRA-Geheimnisses fürchtete, doch CHURCHILL ordnete es an, denn sowjetische Erfolge würden unmittelbar den westlichen Kriegssschauplatz entlasteten.

Diese lange unbekannte, jedoch nachvollziehbare strategische Entscheidung Londons, nämlich die Ressourcen auf die SZ42 zu konzentrieren, begünstigte später die Meinung, die Maschinen T52d und T52e seien „damals unbrechbar" gewesen, weil scheinbar den Briten deren Brechung nicht gelang. Inzwischen bestätigt ein freigegebenes Dokument, daß die BP-Analytiker die T52d-Maschine brachen: Im Juli 1944 gelang mit einem *depth* aus 5 Sendungen der Durchbruch.[321]

---

[319] Vgl. Hinsley, F.H.: An Introduction to Fish. In: Hinsley, F.H. and Stripp,A (Eds.):Codebreakers. The inside story of Bletchley Park. Oxford (GB) 1993. S. 142-143.

[320] Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", March 1942.

[321] Vgl. Fried, Walter J.: Fish Notes (Sturgeon). Fried Report No. 68 of 29 July 1944. NARA RG 457, NSA Hist. Col. Box 880 Nr. 2612. Zit. nach Weierud: Sturgeon, The Fish BP Never Really Caught, S. 10.

Man fragt sich, wieso eine derart komplizierte Maschine so „leicht“ zu brechen war. Doch die Antwort ist einfach: Weil man bereits die vorherigen Varianten beherrschte, und auch die Schlüsselräder der T52d gleich geblieben waren („....*the same patterns as on the T52a/b and T52c machines.*“).[322] So blieben noch die pseudo-irregulären Drehbewegungen zu analysieren, die jedoch einfacher strukturiert waren als die der SZ42-Maschine: Die Bewegung eines jeweiligen Schlüsselrades determinierte die der benachbarten Räder elektromechanisch, denn es gab keinen pseudozufälligen Motorantrieb wie in der SZ42. Man konnte daher per Hand entziffern, unter Verwendung von Tabellen und Hilfsmitteln, und benötigte keine maschinellen Methoden.

Ob man in BP auch mit T52e verschlüsselte Sendungen entzifferte, kann nicht so eindeutig beantwortet werden. Nach WEIERUD empfing man keine derartigen Sendungen bzw. konnte sie nicht als solche identifizieren, und dementsprechend blieb die Maschine unidentifiziert bis zum Kriegsende.[323] Dagegen wäre einzuwenden, daß die T52e mit einem T52d-ähnlichen Algorithmus verschlüsselte, denn Anordnung und pseudo-irreguläre Bewegung der Schlüsselräder waren dieselben, sie unterschieden sich nur durch die relaisbasierte Verwürfelung des Zwischentextes der T52e. Überdies sollte gemäß Kommissionsempfehlung[324] wegen Funkstörungen die Klartextfunktion der T52e nicht verwendet werden, die immerhin *depths* verhinderte.

Aus diesen Gründen können T52e-Entzifferungen nicht allzu schwierig gewesen sein. Daß man sich dazu in BP nicht bekennen will, könnte eine Täuschung sein um zu kaschieren, daß man Nachkriegssendungen der verbündeten Länder Frankreich und Norwegen entzifferte, welche die T52e-Maschinen bis in die 60er Jahre verwendeten.

Hinweise für die Brechung der T52e geben auch deutsche Quellen: ROHRBACH beispielsweise erwähnt hierzu „Periodizitätsuntersuchungen“, weil „...die Bewegung... der... Nockenräder... von allen vorangehenden Rädern....“ abhängt.[325] Diese Untersuchungen waren offenbar erfolgreich, denn v. d. MEULEN berichtet, daß die Meldungen von Militärattachès, die mit T52e verschlüsselt waren, von der kryptologischen Abteilung des AA (Tarnbezeichnung „Pers Z“, Leiter ROHRBACH) entziffert wurden.[326] Das bestätigt ebenso BAUER.[327]
Hintergrund: Die Militärattachès unterstanden nicht dem AA, sondern dem OKW, kommunizierten aber über Kanäle des AA. Und dessen Chef RIBBENTROP soll diese Entzifferungen angeordnet haben, um für den internen Machtkampf im Dritten Reich besser informiert zu sein.

---

[322] Vgl. Fried, Walter J.: Fish Notes (Sturgeon).
[323] Vgl. Weierud: Sturgeon, The Fish BP Never Really Caught, S. 17.
[324] S. dazu Bericht über das Chiffrierwesen in OKW/Chi.
[325] Vgl. Rohrbach, Chiffrierverfahren der neuesten Zeit, S. 368.
[326] Vgl. Van der Meulen, M.: The Road to German Diplomatic Ciphers – 1919 to 1945. In: Cryptologia, Vol XXII (2), April 1998.
[327] Vgl. Bauer, Decrypted Secrets, S. 435.

Fazit

In seinem Bericht schreibt WEIERUD zur Sicherheit der T52-Maschinen, sie wären wahrscheinlich ohne die deutschen Fehler („*security blunders*“) nicht zu brechen gewesen.[328] Doch wiederum verkennt er deutsche Besonderheiten: Er beschuldigt gleichermaßen die Operatoren und die Konstrukteure der Maschinen, dafür verantwortlich zu sein, und besonders letztere, nicht auf den Rat der Kryptologen gehört zu haben. Dagegen zeigt Abschnitt 5.4 die wahren Hintergründe, nämlich die problematische Beziehung der deutschen Militärs zur Kryptologie bzw. den Kryptologen, ein Phänomen, das wohl nicht nur ausländischen Autoren unverständlich ist.

[328] Vgl. Weierud: Sturgeon, The Fish BP Never Really Caught, S. 29.

5.3.2 Schlüsselzusatz SZ40/42

Rekonstruktion

Da diese von der Lorenz AG entwickelte SZ40/42-Maschine geheim war, im Gegensatz zur offen patentierten Siemens T52, mußte BP zuerst deren unbekannte Funktion, d.h. deren Schlüsselalgorithmus, rekonstruieren.

BP nutzte zur Analyse eine Eigenschaft des VERNAM-Verfahrens: Chiffriert man zwei Texte mit der gleichen Schlüsselsequenz, d*epth* in BP, erhält man nach GOEBEL beispielsweise für zwei Buchstaben folgende Resultate:[329]

```
Buchstabe           D       W
Baudot-Code      10010   11001
Schlüssel         01110   01110
             XOR ------   ------
                 11100   10111
```

Wendet man dann auf diese beiden Zwischenresultate die XOR-Operation an,

```
          11100
          10111
XOR       -----
          01011
```

dann ist das Resultat dasselbe wie das XOR der beiden Ausgangsbuchstaben:

```
          10010
          11001
XOR       -----
          01011
```

Der Schlüssel wurde mithin eliminiert und die beiden Buchstaben sind entziffert. Kennt man nun die Lage der Buchstaben im Klartext durch *cribs*, ist die Schlüsselsequenz mit dieser Methode bestimmbar.[330]

1940/41 registrierte BP viele d*epths* in SZ40-Sendungen, ohne daß Wesentliches entziffert werden konnte. Das überrascht nicht, denn mangels vorhergehender Entzifferungen verfügte man nicht über *cribs*, und es konnten nur kurze Startsequenzen entziffert werden. Dementsprechend gelang es der dazu neu gebildeten Abteilung zunächst nicht, die Schlüsselsequenz weiter zu analysieren.
Am 30.8.1941 jedoch passierte ein schwerwiegender Fehler bei Testsendungen, die per SZ40 verschlüsselt waren: Wegen eines Übertragungsfehlers wiederholte der Operator eine verschlüsselte Nachricht, aber mit der unveränderten

[329] Vgl. Goebel, G.: Codes, Ciphers, & Codebreaking, [9.2] The Lorenz Sx40/42 Telecipher Machines.
[330] Ausf. in Bauer, Geheimnisse, S. 385 ff.

Schlüsseleinstellung der SZ40-Maschine. Somit erhielt BP einen Text zweimal mit gleichem Spruchschlüssel, lang genug (ca. 4000 Zeichen) und darüber hinaus bei der zweiten Übermittlung um 500 Zeichen verkürzt, weil der Operator nicht noch einmal alles eingeben wollte. Das ermöglichte dem BP-Kryptologen TILTMAN diesen Text vollständig zu entziffern, und anschließend gelang dem Mathematiker TUTTE mit seinem Team die Rekonstruktion der Schlüsselerzeugung. Im Januar 1942 lag dann die mathematische Definition des Algorithmus der Chiffrierung der unbekannten Maschine vor, in BP genannt „*German TUNNY*".[331]

Gleichwohl mußte man einen Rückschlag hinnehmen: Zu Beginn 1942 ging die verbesserte Version SZ42 der Maschine in Betrieb (s. 4.4), und man benötige entsprechend Zeit, auch diesen Algorithmus zu rekonstruieren.

TUNNY-machine

Mit dem nun bekannten SZ42-Algorithmus konnte man dann den Klartext erzeugen, wenn man vorher die jeweiligen Einstellungen der SZ42 aufwendig von Hand analysiert hatte. Es bot sich an, den Algorithmus maschinell zu erzeugen, um dann mit der analysierten SZ42-Einstellung schneller zum Ziel zu gelangen.

Das Forschungslaboratorium der Britischen Post in Dollis Hill[332] übernahm diesen Auftrag und konstruierte eine elektromechanische *TUNNY-machine* mit dem implementierten Chiffrier-Algorithmus. Diese bestand aus Logikschaltungen, vorwiegend aufgebaut aus Telefon-Hebdrehwählern (*uniselectors*) und Relais, und benötigte einen kleinen Zwischenspeicher, da die fünf parallelen Buchstabenimpulse nur seriell verarbeitet werden konnten.[333]
Das erste, Mitte 1942 betriebsfähige Gerät war umständlich mit Steckfeldern zu programmieren. Später folgten diverse verbesserte Modelle mit Zusatzfunktionen.

[331] Vgl. Sale, Tony: The Colossus of Bletchley Park. In: Rojas, R./Hashagen,U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA und London 2000, S.352-354.
[332] Zukünftig "Dollis Hill" genannt, analog der in der Literatur üblichen Bezeichnung.
[333] Vgl. Sale, Codes and Ciphers: The rebuild of Heath Robinson, Page 376, 56J.

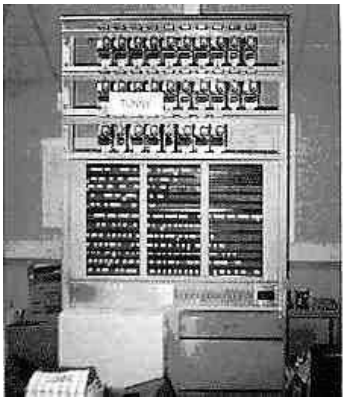


Bild 41: TUNNY-Maschine[334]

Die TUNNY-Maschinen waren keine „Dechiffriergeräte“, wie manchmal zu lesen ist, sondern SZ42-Simulatoren: Sie wandelten den auf Lochstreifen gespeicherten Geheimtext kanalweise (seriell) in Klartext mit Hilfe des implementierten SZ42-Schlüsselalgorithmus und der jeweiligen, mit Steckern und Schaltern programmierten SZ42-Einstellung. Und diese mußte zuvor von Hand kryptanalytisch ermittelt werden, wofür die Experten Wochen benötigten: Das ist verständlich, denn zu bestimmen waren die Anfangsstellungen der Schlüsselräder, der sog. Spruchschlüssel (*wheel setting*) für jede Sendung, dann täglich die Getriebeübersetzung (*motor wheels*), und schließlich monatlich die Schaltstift-Einstellungen (*wheel patterns*).
Gleichwohl nutzten die Kryptanalytiker die Maschinen gelegentlich auch zum teilweisen Entziffern: Denn wenn bereits der erste SZ42- Walzensatz bestimmt war, die Analyse des zweiten aber Probleme bereitete, konnte man durch Probieren verschiedener Einstellungen die Lösung finden.[335]

ROBINSON-Maschinen

Die erwähnten Einstellungen der SZ42-Schlüsselräder ließen sich auch deshalb nur mit großem personellen Aufwand kryptanalytisch ermitteln, weil die wissenschaftlichen Grundlagen unvollständig waren. In BP hatte man zwar Verfahren entwickelt, die sich für die Analyse der SZ40 eigneten, jedoch mit der erwähnten Einführung der verbesserten SZ42 Ende 1941 nicht mehr genügten. Diese Hürde konnte man noch mit neuen statistischen Methoden überwinden und bald wieder entziffern, wenn auch nicht alle Sendungen. Doch im August 1942 ersetzte die Wehrmacht die Spruchschlüssel, die *cribs* in BP waren, durch ein Nummernsystem, und die nun fehlenden *cribs* konnten nicht ersetzt werden. In dieser prekären Situation wußte man sich aber zu helfen: Den inzwischen zum *senior adviser* berufenen TURING beauftragte man mit der Suche nach einer Lösung. Er entwickelte eine neue Entzifferungsmethode namens „*Delta-K*“, intern „*Turingery*“ genannt, bevor er seine mehrmonatige US-Reise antrat. TUTTE erweiterte später das Verfahren, nun „*statistical method*“ genannt.[336]

---

[334] Bild nach Sale, Codes and Ciphers: The Lorenz Cipher and how Bletchley Park broke it.
[335] Vgl. Smith, Michael: Enigma entschlüsselt, S. 240.
[336] Vgl. Wylie, Shaun: Breaking Tunny and the Birth of Colossus. In: Erskine/Smith, Action, S. 326-331.

Einen ersten Großerfolg erzielte die *Fish*-Abteilung damit im Januar 1943: Es gelang, die Sendungen über die neue SZ42-Fernschreiblinie zwischen Rom und ROMMELS Hauptquartier in Tunesien zu entziffern, und BP konnte mit diesen Informationen die Entscheidungskämpfe an der Afrikafront günstig beeinflussen. Allerdings erforderte das einen enormen personellen Aufwand, da damals nur Tabelliermaschinen als Hilfsmittel zur Verfügung standen, um die Tagesschlüssel der SZ42-Maschinen zu bestimmen.[337]

Der Mathematiker und Leiter der *Tunny*-Abteilung Max NEWMAN (S. 6.3.2) schlug zur Abhilfe vor, die erforderlichen umfangreichen Zählprozesse durch elektronische Zählschaltungen zu beschleunigen, die er von seiner Tätigkeit in Cambridge kannte. Er war dort auch TURINGS Hochschullehrer gewesen und mit dessen Gedanken vertraut, insbesonders mit TURINGS Erkenntnis, daß algorithmisch definierbare Probleme, wie es alle kryptologischen sind, sich auch maschinell lösen lassen. Vermutlich regte das NEWMAN zu Gedanken über die Mechanisierung dieses Entzifferungsprozesses an, und zu entsprechenden Vorgaben für die Entwickler.

NEWMAN kannte auch den Cambridge-Physiker WYNN-WILLIAMS (s. 6.2.3), der zur Mitarbeit bereit war. Dieser entwickelte eine teilelektronische digitale Zählschaltung, und zu deren Auswertung konstruierte Tommy FLOWERS (s. 6.2.1) eine „*combining unit*" mit elektronischen Komponenten, die Logikoperationen ausführten. Der Entwicklungsauftrag wurde im Januar 1943 erteilt, und bereits ab Juni 1943 arbeitete die Maschine zunächst zufriedenstellend; man nannte sie später „HEATH ROBINSON".[338]

Die Maschine las gleichzeitig zwei Lochbänder photoelektrisch mit je ca. 1000 Zeichen/sec, eines mit der Schlüsselsequenz, das andere mit dem Geheimtext, und beides als Endlosschleife verklebt. Der Leseprozeß startete mit einem Versatz um ein Zeichen, so daß nach jedem Umlauf eine andere Phasenlage entstand.
Die gelesenen Impulsfolgen steuerten eine elektronische Logikeinheit, die erwähnte *combining unit,* deren Algorithmus auf einem Steckfeld geschaltet wurde. Diese Einheit verglich die beiden Impulsströme per Boole'scher Algebra, die resultierenden Übereinstimmungen der 2x5 Kanäle zählte dann die teilelektronische digitale Zählvorrichtung und gab das Ergebnis in einem Anzeigefeld aus (später per Drucker). Die Zählelektronik umfaßte vier Dekaden, benötigte aber nur 24 *valves*[339], weil Thyratrons in der Zählschaltung nur in der schnellen Eingangsstufe angeordnet waren. Die weiteren Stufen bestanden hingegen aus Relais; der Grund dafür war der Nachbau einer älteren

[337] Vgl. Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", Jan. 1943.
[338] Vgl. General Report On Tunny: With Emphasis on Statistical Methods (1945), 15A, S. 33.
[339] Dieser Begriff wurde in Großbritannien gleichermaßen für Thyratrons und Vakuumröhren (US: „tubes") verwendet, aber auch „thermionic valves" für Thyratrons.

„Sparschaltung“ von WYNN-WILLIAMS.[340] Die Maschine arbeitete dadurch unnötig langsam, *„... because the relays slowed everything down“*.[341]
Besondere Probleme bereiteten häufige Bandrisse wegen der erforderlichen vielen schnellen Umläufe. Überdies brachten Synchronisationsfehler infolge Lochbanddehnungen den kryptanalytischen Prozeß außer Tritt.[342]
Daraufhin entwickelte man leistungsfähigere Varianten: OLD ROBINSON, und einen teilelektronischen Vorläufer des COLOSSUS namens SUPER ROBINSON (s. 6.3.1). Gleichwohl blieben die Synchronisationsprobleme, die erst mit dem Einsatz des vollelektronischen COLOSSUS eliminiert werden konnten (s. 6.3.2).

SZ42-Entzifferungsverfahren

Nach KEN HALTON[343] arbeiteten die Entzifferer in zwei Schritten, analog der zweistufigen Chiffrierung in der SZ42-Maschine: Zunächst setzte man die vorerwähnten Maschinen ein, um per *statistical method* die Einstellungen der ersten SZ42-Stufe (*Chi-wheels*) zu ermitteln, also die Stellung der ersten fünf Schlüsselräder und deren Schaltstifte. Anschließend las man diesen *Chi-stream* ein in eine speziell dafür programmierte TUNNY-Maschine, wo er vom Geheimtext abgestreift[344] wurde; das Resultat nannte man *de-Chi*.
Danach waren die Einstellungen der zweiten Schlüsselradgruppe (*Psi-wheels*) zu ermitteln, und die der *motor wheels* des Getriebes. Dafür standen zunächst keine Geräte zur Verfügung, so daß sehr aufwendige Handarbeit erforderlich war. Doch man hatte manchmal Glück: Da, wie erwähnt, die erste Chiffrierstufe ja abgestreift war, erschien deutscher Klartext, wenn die *Psi-wheels* infolge der „zufälligen“ Getriebeschaltung sich nicht bewegten. Wenn doch, blieb die bewährte Methode, *cribs* in sukzessiven Positionen zu analysieren usw. Schließlich waren noch die Startpositionen der Schlüsselräder der zweiten Gruppe zu bestimmen, ebenfalls aufwendig per Hand.
Doch im November 1944 kam Hilfe: Der US-Dienst SIS hatte eine Relaismaschine namens DRAGON entwickelt, die in BP installiert wurde, und in der Lage war, die Position eines *cribs* im erwähnten *de-Chi*-Text zu bestimmen. Damit standen die relativen Positionen aller Schlüsselräder fest und anschließend konnte man deren Startpositionen ermitteln.

Anfang 1945 erhielt man eine verbesserte Maschine DRAGON II, die das Postlabor in Dollis Hill konstruiert hatte, und schließlich kurz vor Kriegsende die teilelektronische Version DRAGON III. Hierüber konnte HALTON nichts berichten und vermutet, die Maschine sei [im Krieg] nicht mehr genutzt worden.
Auch der inoffizielle BP-Bericht[345] enthält wenig zu dieser Maschine. Danach

[340] Vgl. Sale, Codes and Ciphers: The rebuild of Heath Robinson, page 23.
[341] Copeland, Computer Age, S. 360.
[342] Vgl. Goebel, G.: Codes, Ciphers, & Codebreaking, [9.3] Heath Robinson & Colossus.
[343] Korrespondenz mit Mache (u.v.). Halton arbeitete damals in BP als Tunny-Codebreaker.
[344] Kryptanalytischer Begriff. Wird verwendet für die Eliminierung einer Verschlüsselungsebene.
[345] Vgl. General Report On Tunny: With Emphasis on Statistical Methods (1945), 55B, S. 364.

reichte sogar ein 16-Buchstaben-*crib*, um erfolgreich zu sein, und man konnte damit Lücken im Text bis zu fünf Buchstaben überbrücken.
Hierzu wäre zu fragen, was denn so nach dem Krieg damit entziffert wurde, doch es gibt – kaum verwunderlich – darüber keine Auskunft. Bekannt wurde dazu nur, daß die offiziell sicheren T52e-Maschinen nach dem Krieg von den französischen und norwegischen Verbündeten verwendet wurden – und daß die COLOSSUS-Maschinen bis in die 60er Jahre in Betrieb waren.

Schwedische Brechung des SZ42

Nachdem die schwedische Brechung der T52a/b in Berlin bekannt wurde, ersetzte man diese Maschine am 21.Juli 1942 durch die verbesserte Variante T52c, aber auch durch den SZ42; die Verwendung der T52a/b wurde außerhalb des von der Wehrmacht kontrollierten Gebietes untersagt. Doch beide Geräte konnten ebenso gebrochen werden („*fully broken*"); die Brechung der T52c wurde bereits unter 5.3.1 angesprochen.

Die ersten, mit dem SZ42 verschlüsselten Sendungen registrierte der schwedische Geheimdienst im Dezember 1942 in den abgehörten Kabelverbindungen Deutschland-Schweden-Norwegen/Finnland; am 9. April 1943 gelang der Einbruch. Und ab Juni 1943 sollen sogar abgehörte SZ42-Funkfernschreiben entziffert worden sein, bis Ende 1943 eine Änderung des SZ42 (Klartextfunktion „P5 ", s. 4.4) das unbekannte schwedische Entzifferungsverfahren obsolet machte, ebenso wie die Einführung der T52d zur gleichen Zeit.[346]

5.4 ULTRA – Folge systematischer deutscher Fehler ?

Zum effektiven Betrieb kryptanalytischer Maschinen benötigte man – wie gezeigt – mehr oder weniger umfangreiches Klartextmaterial. Also hätte BP ohne Klartextfragmente die Entzifferungsmaschinen nicht nutzen und keine ULTRA-Informationen erarbeiten können, denn: ULTRA entstand erst nach der maschinellen Verarbeitung von täglich Tausenden Funknachrichten und deren anschließenden Auswertung. Mithin mußten täglich für jeden Schlüsselkreis geeignete Klartextfragmente erarbeitet werden, und das gelang meistens, weil die deutsche Gegenseite unfreiwillig mitarbeitete – sie „lieferte" dazu stets genügend Chiffrierfehler. Waren also die deutschen Militärs letztlich selbst verantwortlich für die maschinelle Entzifferung ihrer Geheimnachrichten ? Und wenn ja, wie konnte das passieren und welche Fehler wurden gemacht, gar systematische ?

Zu diesen scheinbar provozierenden Fragen findet man kaum Antworten in der Standardliteratur, erst recht keine Forschungsberichte. Beispielsweise erklärt die umfangreiche Marine-Historiographie die Brechung der Maschine ENIGMA M3 und der späteren M4 vor allem mit der Erbeutung von Maschinen und

[346] Mache, Korrespondenz.

Schlüsselunterlagen, was dementsprechend ausführlich erforscht wurde. Doch das waren nur Voraussetzungen dafür, daß die BP-Analytiker die Entzifferungsalgorithmen schnell genug entwickeln konnten, quasi die „Hardware“. Mindestens genauso wichtig waren jedoch die ständigen deutschen Chiffrierfehler, also die „Software“ dazu, die erst die Gewinnung von Klartextmaterial ermöglichten, und das für täglich zahlreiche Schlüsselkreise. Und nur damit konnten die Codebrecher BOMBE-Maschinen programmieren und täglich Tausende Sendungen entziffern.

Lag also der Fehler im System, in Struktur und Mentalität des deutschen Militärs? Oder muß man nur Nachlässigkeiten annehmen? Diese Fragen können hier nicht ausführlich beantwortet werden, und aussagekräftige Literatur darüber ist nicht bekannt. Allerdings kann bei einer technikhistorischen Analyse die „Software“ für die kryptanalytischen Maschinen nicht ausgespart werden, die überdies in ständiger Wechselwirkung mit den technischen und organisatorischen Bedingungen steht – mithin Teil eines zu diskutierendes „Systems Chiffriermaschine“ ist.

5.4.1 Routinesendungen und Klartextfragmente

Wie unentbehrlich für BP das Klartextmaterial war, die *cribs* und *depths*, zeigt beispielsweise für die SZ42-Entzifferung ein erst in 2000 freigegebener interner BP-Bericht.[347] Danach „lieferten“ deutsche Dienststellen mit verblüffender Selbstverständlichkeit geeignetes Material, das überdies besondere Qualitäten aufweisen mußte: Für die – gegenüber ENIGMA-Sendungen – schwierigere SZ42-Entzifferung forderten die BP-Analytiker u.a.: Die Nachricht mußte wiederholt gesendet und dazu auch noch exakt gleich sein, was nur bei maschinell gesendeten Nachrichten des gleichen Lochstreifens der Fall war. Sie sollte sich überdies auf eine vorangegangene, bereits entzifferte Nachricht beziehen [und somit eine Kompromittierung ermöglichen]. Doch an diesen speziellen Nachrichten mangelte es offenbar nicht, denn beispielsweise sendete das OKH regelmäßig Routine-Nachrichten wortgleich an mehrere Truppenteile, die eine zur Kryptanalyse geeignete Länge von 3.000-10.000 Buchstaben aufwiesen. Ebenso konnte BP die meist täglichen Lageberichte des OKH nutzen, die ebenfalls wortgleich an mehrere Adressen gingen. Dazu kam noch der „Lagebericht West“ in gleicher Regelmäßigkeit; einmal ließ der OB-West gar 16 Stunden ununterbrochen senden, nämlich 72 Berichte. Schließlich trug auch die Marine zur Klartextgewinnung bei: Sie sendete[348] ihre „Kurzlage“ ebenfalls teils täglich und wortgleich an verschiedene Dienststellen.
Diese Vielzahl von geeigneten Sendungen ermöglichte es den Kryptologen auch, die häufigen Empfangsfehler zu korrigieren und Erschwernisse durch Klartextfunktionen leichter zu überwinden. Aber auch sonstige deutsche „*most*

[347] Vgl. General Report On Tunny: With Emphasis on Statistical Methods (1945), 27A, S. 234-337.

[348] Die Marine bevorzugte aus Sicherheitsgründen abhörsichere Kabelverbindungen, die aber in der zweiten Kriegshälfte immer öfter gestört waren, so daß gefunkt werden mußte.

useful practices“ halfen, beispielsweise die Klartextprozedur der Operatoren beim Abschluß einer Übertragung.[349]

Anzumerken ist hierzu, daß kryptologisch fundierte Vorschriften für die Verwendung der Schlüsselfernschreibmaschinen[350] diese erwähnten Routinesendungen eigentlich verhindern bzw. modifizieren sollten. Doch das scheint nicht durchsetzbar gewesen zu sein; die Ursachen dafür sind ebenfalls Teil des zu diskutierenden Systems.

Weniger hohe Ansprüche mußten Sendungen erfüllen, aus denen *cribs* zur ENIGMA-Entzifferung zu gewinnen waren, denn es genügten meistens nur ca. 20 Buchstaben, wenn man deren ungefähre Lage im Text kannte. Doch das scheint kein Problem gewesen zu sein: Die Nachrichten enthielten häufig stereotype Formulierungen in Routinesendungen, wie Grußformeln, Lagerbestandsmeldungen, Reparaturanforderungen usw. Und besonders unsinnig war es, die regelmäßigen Wetterberichte zu verschlüsseln, noch dazu schematisch, und immer mit der gleichen ENIGMA-Maschine, die auch für geheime Kommandosachen eingesetzt wurde. Man hätte Wetterberichte auch im Klartext senden können – die Alliierten verfügten dank weltweiter Wetterbeobachtung über weit bessere Wetterprognosen, die deutschen Berichte hätten ihnen keine Vorteile gebracht.
Doch damit verfügte BP über eine regelmäßige *crib*-Quelle zur Bestimmung der ENIGMA-Einstellungen. Wie man das vermeidet, zeigten die Alliierten: Sie verwendeten nämlich für Routinemeldungen andere Chiffriermethoden, um das übergeordnete Verfahren für Geheimsendungen zu sichern. Beispielsweise benutzte dafür die US-Army das Zylindergerät M-94 (s. 2.1.2) für taktische Nachrichten, dann für höhere Sicherheit die Chiffrier-Rechenmaschine M-209 (s. 3.3.1), und schließlich für strategische Informationen der obersten Führung die SIGABA-Maschine, die sicherste (und teuerste) Rotormaschine des Weltkrieges, die bis 1959 verwendet wurde für die höchste Geheimhaltungsstufe.

Selbst die aus Sicherheitsgründen eingeführte große Zahl der ENIGMA-Schlüsselkreise, für die jeweils täglich (später z.T. 8-stündlich) geeignete *cribs* bereitzustellen waren, wurde von BP bewältigt: Fast immer gab es genügend *cribs* zur Programmierung der BOMBE-Maschinen, und fehlten diese doch einmal, was mit zunehmender Kriegsdauer immer seltener vorkam, konnte man sich mit TURINGS Lochkartenmethode *Banburismus* behelfen (s. 5.2.2).

Ein weiterer, nach BP-Unterlagen häufiger deutscher Fehler war es, denselben Text wortgleich mit anderen bekannten Verfahren zu chiffrieren, das *re-enciphering*: So sorgte beispielsweise die Abwehr mit dieser Methode für die Kompromittierung ihrer Maschinen, denn deren Hauptstellen übermittelten per

[349] Vgl. General Report On Tunny: With Emphasis on Statistical Methods (1945), 27A, S. 234-337.
[350] HD/LDv/MDv „Schlüsselfernschreibvorschrift“ des OKW/Chef WNV, gültig ab 1.12.42. Archiv Mache.

Abwehr-ENIGMA wortgleich die eingegangenen Agentenmeldungen, die – mit einfachen Hilfsmitteln verschlüsselt – umgehend in BP entziffert wurden. Hinzu kamen zahlreiche weitere Chiffrierfehler, so daß die Entzifferer wohl wenig Mühe hatten. Diese Leichtfertigkeit im Umgang mit der sensiblen Chiffriertechnik überraschte den ehemaligen Abwehr-Mitarbeiter STARITZ nicht: Nach seiner Kenntnis verfügte die Abwehr nicht über kryptologischen Sachverstand – und vermißte ihn wohl auch nicht. So gab es bspw. keine einheitlichen, geprüften Chiffrierverfahren für die Agenten, jeder Agentenführer „bastelte" sich seine eigenen Methoden, die den professionellen BP-Kryptologen freilich keine Mühe bereiteten.[351]

Ebenso scheinen die Nachrichtenoffiziere der Marine kryptologischen Sachverstand nicht vermißt zu haben, denn das von ihnen verschuldete quasi-*reencipher*ing zwischen den Wetternachrichten und dem U-Boot-Funk ermöglichte BP regelmäßig die Gewinnung von *cribs*: Sie veranlaßten die Verwendung der U-Boot-ENIGMA M4 für Wettersendungen im bisherigen M3-Modus, damit Wetterberichte auch von den Küstenstationen und sonstigen Schiffen – die nur über M3-Maschinen verfügten – gelesen werden konnten. Und diese ENIGMA M3 beherrschte BP inzwischen, und konnte mit Hilfe des bei der Aufbringung von U-559 am 30.10.1942 erbeuteten Wetterkurzschlüsselheft die M3-Walzeneinstellung ermitteln – und hatte so gleichzeitig die der M4-Maschine, die ja im M3-Modus betrieben werden mußte.
Abgesehen davon, daß – wie bereits erwähnt – die Verschlüsselung der Wetterberichte unnötig war, die Marineoffiziere handelten auch unlogisch: Die Maschine M4 wurde ja eingeführt, weil (inoffiziell) Sicherheitsbedenken gegen den „Schlüssel M3" geäußert wurden; die Einführung wäre sonst ja überflüssig gewesen. Wenn aber Bedenken gegen die M3 bestanden, wieso verknüpfte man beide Maschinen über den Wettermodus? Denn nun hing die zusätzliche Sicherheit der M4-Verschlüsselung von der Geheimhaltung des Wetterkurzschlüsselheftes ab, das im Krieg nie sicher war – Erbeutung, Beschaffung durch Verrat usw. drohten, und Rekonstruktion aus entzifferten Meldungen. Und das war kryptologisches Standardwissen: Bereits 1883 hatte der Kryptologe KERCKHOFFS gefordert, die Sicherheit der Verschlüsselung dürfe nur auf dem Schlüssel selbst beruhen, nicht aber auf dem Gerät bzw. Schlüsselmittel, oder dem Verfahren.[352]

Nun wird niemand eine kryptologische Ausbildung der Nachrichtenoffiziere gefordert haben, aber doch wenigstens die Bereitschaft, Kryptologen zu konsultieren. Dann hätten sie viele Chiffrierfehler vermeiden können, bestimmt aber den vermutlich gröbsten des Krieges: Karl DÖNITZ ließ am 30.1.1943 seine Beförderung zum Großadmiral und Oberbefehlshaber allen Marinedienststellen mitteilen, den Schiffen per Funk. Die zuständigen Nachrichtenoffiziere ließen den Text *wortgleich* mit *allen* relevanten Verfahren verschlüsseln und dann senden,

[351] Korrespondenz mit Staritz (uv.).
[352] In seinem Hauptwerk „La cryptographie militaire" 1883.

und lieferten so den Kryptologen in BP für *alle* Marine-Chiffrierverfahren eine Klartext-Geheimtext-Kompromittierung, ein Super-*depth*. Überdies war die Verschlüsselung unsinnig, denn es war keine Geheimnachricht – sie stand am nächsten Tag in den Zeitungen.

5.4.2 Chiffriermaschinen – Empirie vs. Wissenschaft

Die vorerwähnten Chiffrierfehler standen auch in einer Wechselwirkung mit den eingesetzten Chiffriermaschinen: Die im Krieg praktisch unvermeidbaren Chiffrierfehler können aber – wie nachfolgend dargelegt – kompensiert werden durch entsprechend konzipierte Chiffriermaschinen. Denn wenn beispielsweise die Zahl der kryptanalytisch zu prüfenden Varianten zu groß ist und diese häufig gewechselt werden, wie bei der britischen TYPEX-Maschine (s. 3.2.6), dann hat ein einmalig erzielter Einbruch in die Verschlüsselung keine Folgewirkung. Die ENIGMA hingegen verschlüsselte nur mit einem Rotorwalzensatz, der seit 1930 (1938 kamen zwei Rotoren hinzu) bis zum Kriegsende nicht verändert wurde. Ebenso änderte sich nicht die immer gleiche zyklometrische Bewegung der Rotorwalzen. Mithin konnten die Analytiker immer dann von diesem bekannten Walzensatz ausgehen, wenn es Probleme gab durch Änderungen des ENIGMA-Verfahrens.
Diese Gefahren waren den deutschen Experten durchaus bekannt, doch sie konnten mangels Zuständigkeit nichts bewirken (s.u.). Aus eben diesem Grund blieb es auch bei den von den Herstellern empirisch entwickelten Maschinen.
Diese empirische Entwicklung der ENIGMA (und später der Chiffrier-fernschreiber) hatte historische Ursachen: Als die alliierten Entzifferungen im Ersten Weltkrieg bekannt wurden, nachdem CHURCHILL seine Memoiren publiziert hatte (1923), kann man sich die Verlegenheit der deutschen Offiziere vorstellen, deren fehlende kryptologische Kenntnisse nun offenbart waren. Doch nun schien das Problem gelöst: Auf Postausstellungen entdeckten sie eine als unbrechbar bezeichnete Chiffriermaschine namens ENIGMA, deren Chiffriersicherheit ihre Probleme wohl lösen würde. Die Offiziere glaubten, eine Maschine mit dieser (theoretisch) sehr großen Schlüsselperiode könne schon deshalb nicht gebrochen werden, weil ein potentieller Entzifferer viel zu viel Zeit benötigen würde. Man stellte als „Beweis“ dafür Berechnungen an, wieviel Zeit Entzifferer benötigen würden, um alle Einstellungen der Maschinen durchzutesten – eine empirisch orientierte Beurteilung. Und das glaubten sie sogar noch im Krieg, so beispielsweise eine nicht direkt genannte “Kapazität der Nachrichtentechnik“: „Die bekannten Methoden der mathematischen Analysen und ... Berechnungen verlangen einen sich auf Monate, ja Jahre erstreckenden Aufwand, um nur eine der vielen möglichen Schlüsseleinstellungen des Marineschlüssels M aufzubrechen.“[353] Warum aber dazu nicht wissenschaftlich

[353] Zit. nach Brennecke, S. 34. Aus dem Text kann man folgern, daß der Nachrichtenoffizier Kap. Heinz Bonatz gemeint ist, damals Chef des xB-Dienstes der Marine.

orientierte Kryptologen konsultiert wurden, zumindest nicht vor 1944, gehört zu den unerforschten Bereichen diese Themas.

Und mit eben dieser Begründung pries der Erfinder bereits 1923 seine Maschine an, denn auch er schien die Konsultation von Kryptologen für überflüssig zu halten – die Offiziere ohnehin. So beschafften militärische Dienststellen erste ENIGMA-Maschinen und begannen diese versuchsweise ab 1926 einzusetzen als „Funkschlüssel C", wohl in der Überzeugung, mit ausgiebigen Praxistests deren Sicherheit beurteilen zu können.

Ein Hobbykryptologe, der Nachrichtenoffizier Oberleutnant z.S. LUCAN erkannte dann, daß diese ENIGMA „weder technisch noch kryptologisch modernen Ansprüchen genügt." Das schrieb er 1929/30 in einer Studie, doch es dauerte bis 1934, bis die Marine zur ENIGMA I wechselte.[354]

Vermutlich auch mit der Begründung einer weit größeren Periode – Dokumente hierzu sind nicht bekannt – bot das Herstellerwerk eine verbesserte Maschine an (ENIGMA G dann I), die dazu erstmals mit einer Steckerbrett-Überschlüsselung ausgerüstet war, ansonsten jedoch unverändert blieb. Doch auch das scheint eine empirische Entwicklung gewesen zu sein: Diese Überschlüsselung war so konzipiert, daß die Maschine weiterhin reziprok chiffrierte – und damit Entzifferungen durch BOMBE-Maschinen später ermöglichte.
Ebenso entstanden die Chiffrierfernschreiber empirisch, wie bereits dargelegt, und man änderte auch nie die Schlüsselräder der Chiffrierfernschreiber, so daß spätere Modifikationen durch pseudoirreguläre Bewegungen leichter überwunden werden konnten.

5.4.3 Die deutschen Zuständigkeiten als Problem

Die offenkundige Empirie bei Konstruktion und Weiterentwicklung der deutschen Chiffriermaschinen könnte Folge einer (typisch?) deutschen Besonderheit gewesen sein: Für Chiffriermaschinen waren nämlich die technisch orientierten Waffenämter zuständig, und in denen gab es keine Kryptologen. Diese Behörden formulierten die Anforderungen, schrieben aus und prüften anschließend die produzierten Maschinen – die sog. Abnahme – und übergaben sie dann zum „Feldversuch". Die Mitarbeit von Kryptologen ist hierzu nicht bekannt, und auch nicht wahrscheinlich; ein Dokument belegt das zumindest bis Ende 1942:
Nachdem Frontoffiziere immer wieder an der Sicherheit der Chiffrierungen zweifelten, auf sonst nicht erklärbare Informationen des Feindes verwiesen, errichtete man erstmals ein Referat „Prüfung der Sicherheit der eigenen Geheimschriften" bei OKW/Chi. Denn dort hatte man, nach inzwischen drei

[354] Neue Chiffriermaschine für die Marine. Geheime Kommandosache der Marineleitung vom 7.2.1930, dazu Schriftwechsel. BA-MA.

Kriegsjahren, den „unhaltbaren Zustand“ erkannt[355], nämlich daß „... die Überprüfung der Sicherheit [...] entweder überhaupt nicht oder von den entwickelnden Stellen [Hersteller] selbst“ erfolgte. Und: „Eine unabhängige, neutrale Überprüfung war bis zur Einrichtung des Referates [...] nicht möglich“.[356] Mithin räumte man indirekt ein, daß das Waffenamt nicht in der Lage war, „neutral“ (d.h. kryptologisch) zu prüfen, eine sehr wohlwollende Bezeichnung für den Fakt, daß dieses Amt nicht über kryptologisch-wissenschaftlichen Sachverstand verfügte.

Warum aber die Waffenämter für ein so sensibles Gerät wie eine Chiffriermaschine zuständig blieben, und auch kryptologische Beratung wohl nicht für erforderlich hielten, kann mangels relevanter Forschung hier nicht beantwortet werden. Ebenso fehlen Forschungsberichte zu den Ursachen der erwähnten systematischen Fehler, welche die Verantwortlichen scheinbar nicht als solche erkannten. Dabei hätte ein Blick in die Geschichte der Wissenschaft Kryptologie den Offizieren ein anderes Vorgehen nahegelegt:
Bereits Ende des 19. Jahrhunderts erkannten Kryptologen, daß auch vermeintlich perfekte Chiffrierverfahren keineswegs sicher sein müssen. Daher dürfe die Sicherheit der Verschlüsselung nur auf dem Schlüssel selbst beruhen, nicht aber auf dem Gerät bzw. dem Verfahren. Denn diese könnten den Gegnern in die Hände fallen, womit im Krieg immer zu rechnen ist, und auch durch Verrat oder Diebstahl „besorgt“ werden. Diese Erkenntnisse und die dazu untersuchten Gründe wurden keineswegs geheim gehalten, sondern publiziert und öffentlich diskutiert, nachdem die Kryptologie sich als Wissenschaft etabliert hatte. Für die hier betrachteten Zusammenhänge formulierte bereits 1883 der Kryptologe KERCKHOFFS eine Maxime: „Nur der Kryptanalytiker, wenn überhaupt jemand, kann die Sicherheit eines Chiffrierverfahrens beurteilen.“[357] Denn dieser beurteilt ein Verfahren aus der Perspektive des Entzifferers und unterstellt dabei die Kenntnis des Verfahrens bzw. der Maschine, gründliche Kenntnis der gegnerischen Sprache und deren militärischen Jargon, dazu den Besitz vieler abgehörter Geheimtexte, jedoch nicht den jeweiligen Schlüssel, den es zu knacken gilt.
Mit anderen Worten: Man kann nicht nur Chiffriermaschinen, sondern alle Chiffrierverfahren nur dann richtig beurteilen, wenn neben der Technik sämtliche Einsatzbedingungen bekannt sind, denn sie stehen zueinander in Wechselbeziehungen – sie bilden ein System. Und dazu gehören auch die Anwender und deren Gewohnheiten, sie sind nämlich Teil des Systems Chiffriermaschine. Denn man muß beim Einsatz von Chiffriermaschinen unter häufig extremen Kriegsbedingungen damit rechnen, daß Befehle zu deren Bedienung nicht immer korrekt ausgeführt werden (können) und überdies den Operatoren dabei gelegentlich kryptologisch schwerwiegende Fehler unterlaufen.

---

[355] Was OKW/Chi inoffiziell schon wußte, ist nicht dokumentiert; Befragungen nach dem Krieg lassen auf manche Erkenntnisse schließen, die vermutlich nicht geäußert werden „durften“.
[356] Bericht über das Chiffrierwesen in OKW/Chi.
[357] Ausf. in Bauer, Geheimnisse, S. 211-226.

Das aber muß man diesen einfachen Soldaten zubilligen, denn ihnen fehlte der kryptologische Hintergrund zum Verständnis, hätte sie wohl auch überfordert, und ihre Vorgesetzten, die Nachrichtenoffiziere, wohl ebenso. Diese unvermeidbaren, mithin systematischen Fehler begünstigten, ja ermöglichten oft erst den gegnerischen Kryptanalytikern Einbrüche in die Chiffrierung und/oder die Gewinnung von Klartextfragmenten.
Im Gegensatz zu ihren deutschen Kameraden hatten beispielsweise die Verantwortlichen der US-Army die Publikationen von KERCKHOFFS et al. nicht nur gelesen, sondern praktisch umgesetzt: Sie ließen Offiziere zu Kryptologen ausbilden und veranstalteten noch vor dem ersten Weltkrieg regelmäßige Seminare zu deren Weiterbildung. Dazu gehörten die bereits unter 4.2 erwähnten Militärkryptologen MAUBORGNE und HITT; letzterer publizierte 1916 ein Buch über militärische Kryptanalyse. Berühmt wurde später FRIEDMAN, als Theoretiker (erste Publikation 1922), als genialer Kryptanalytiker und als Konstrukteur von Chiffriermaschinen.
Die Verantwortlichen Englands und Frankreichs zogen bald nach, doch im Deutschen Reich scheinen die Verantwortlichen eine Militärkryptologie für überflüssig gehalten zu haben. So blieb den für die Übermittlung von Geheimsendungen zuständigen Nachrichtenoffizieren im Weltkrieg nur die Möglichkeit, selbst Chiffrierungen zu konzipieren, was sie – gezwungenermaßen – auch taten. Mithin verwendete das deutsche Heer im Ersten Weltkrieg von Hobby-Kryptologen entwickelte Verschlüsselungen – mit entsprechendem Ergebnis: Nahezu alle Funksendungen des deutschen Heeres entzifferten französische Kryptologen, meist innerhalb eines Tages.[358]
Warum nun die deutschen Militärs die Chiffriertechnik, immerhin ein wichtiges militärisches Instrument, so wenig beachteten und als Sache der Nachrichtenoffiziere ansahen, wurde bisher nicht erforscht.

Daran änderte sich auch nichts in der Zwischenkriegszeit, denn die Militärs scheinen nicht nur nicht die systemischen Zusammenhänge der Chiffrierung erkannt zu haben, sondern beachteten auch elementare kryptologische Grundlagen nicht: Etwa daß eine Chiffriermaschine und/oder deren Schlüsselunterlagen im Krieg wahrscheinlich dem Gegner bekannt werden, oder daß mit kryptanalytischen Methoden das Verfahren rekonstruiert werden kann. Doch die hierzu erforderlichen Kenntnisse erwartete ja niemand von den Militärs, sondern „nur“ die Bereitschaft, sich von Sachkundigen beraten zu lassen – und deren Ratschläge auch zu befolgen. Das war in den alliierten Streitkräften selbstverständlich, zumal sie über Offiziers-Kryptologen verfügten.

Aber, so könnte hiergegen eingewendet werden, es gab doch bereits in der Reichswehr die „Chistelle“, und später in allen deutschen Wehrmachtsteilen Entzifferungsstellen, und eine „Amtsgruppe Wehrmachtsnachrichten-Verbindungen“ mit der Abt. Chiffrierwesen, unter der Leitung des anerkannten Nachrichtenoffiziers General FELLGIEBEL?

[358] Ausf. in Bauer, Geheimnisse, pass.

Freilich gab es diese Stellen, aber sie waren gemäß deutscher Militärtradition nur zuständig für die Entzifferung von Feindnachrichten, und in den Truppenteilen Gehilfen der militärischen Aufklärung unter der Leitung des „Stabsoffiziers Ic". Entsprechend wurde die Abt. Chi im OKW als Stabsabteilung betrachtet, sie erhielt keine Kompetenzen zur Prüfung und ggf. Ablehnung von Chiffriermaschinen, das lag in der Zuständigkeit der Waffenämter. Diese fachlich falschen Zuständigkeiten illustriert folgendes Beispiel:
Anfang 1942 wurde OKW/HNV/Fu (Abt. Funknachrichten) offiziell über die mangelhafte Sicherheit der Schlüsselfernschreibmaschine T52a/b informiert, und zwar von der Reichspost [!]: Die Post, und nicht die Wehrmacht, hatte eine neue militärisch genutzte Funklinie nach Bukarest installiert und in Probebetrieb genommen, mit Verschlüsselung durch T52a/b-Maschinen. Die Post beklagte aber bald, daß „....die Verbindungen mit Bukarest stillgelegt werden [mußten], weil das OKW Bedenken gegen die Schlüsselfestigkeit des derzeit verwendeten Geheimschreibers [T52a/b] angemeldet hatte." Dementsprechend fragte die Postdienststelle, ob das Postministerium beim OKW veranlassen kann, „....unbedenklich zu verwendende G-Schreiber...." zur Verfügung zu stellen.[359]
Die daraufhin erfolgte offizielle Anfrage des Reichspostministers beantwortete OKW/WNV/Fu IIa am 8.5.1942: „.... daß über Wa Prüf 7 [Heereswaffenamt] die Bearbeitung aller damit zusammenhängenden Fragen....erfolgt. Ebenso ist die Beschaffung des ggf. erforderlichen Gerätes, wie G-Zusatz 40 [=SZ42] usw., Angelegenheit des Heeres[-Waffenamtes]."[360]

Diese Dokumente belegen u.a., daß zumindest bis zu diesem Zeitpunkt die Schlüsselsicherheit nicht von der fachlich kompetenten Abteilung OKW/Chi kontrolliert wurde, denn den Vorgang bearbeitete zunächst die Post, dann die funktechnische Abteilung Fu, schließlich das Waffenamt, das ohnehin für Beschaffung und Abnahme der Chiffriermaschinen zuständig war und blieb. Chi war danach nicht zuständig, und ob diese Stelle überhaupt über diesen Vorgang informiert wurde, ist fraglich, denn es gibt hierzu keine Hinweise im Schriftwechsel.

„Bedenken" gegen die Maschine T52a/b hatte Chi bereits 1939 geäußert:
Das zeigt ein heute kaum verständlicher Vorgang: Kurz vor Kriegsbeginn erhielt der im OKW/Chi als Referent beschäftigte Mathematiker und Kryptologe Erich HÜTTENHAIN (S. 5.5) den Auftrag, die Chiffriersicherheit der Maschinen SZ40 und T52a/b zu prüfen. [Für ENIGMA hatte er keinen Auftrag, die Maschine galt „... längst als überprüft und sicher"[361]]. Er kam zum Ergebnis, daß keine Maschine *„.. up to the security Standards then in force"* war, und besonders die

[359] Schreiben des Präsidenten der Forschungsanstalt der Reichspost vom 17.2.1942 an sein Ministerium. BArch, R 4701/18314.
[360] Schreiben OKW/WNV/Fu IIa vom 6.5.1942 an das Reichspostministerium. BArch, R 4701/18314.
[361] Leiberich, Otto: Vom diplomatischen Code zur Falltürfunktion. In: Spektrum der Wissenschaft 4/2001, S. 16. Allerdings erwähnt Leiberich nicht das Eingeständnis des OKW von 1942, den „unhaltbaren Zustand", daß die Chiffriermnaschinen nicht geprüft waren.

T52a/b durch einen „*...extraordinary low degree of security*“ gefährdet sei.[362] Doch es blieb gleichwohl beim Einsatz der bereits vom Waffenamt bestellten oder inzwischen bezogenen Maschinen auch für „Geheime Kommandosachen“, obwohl ein Wehrmachts-Kryptologe deren Sicherheit bezweifelte.

Das OKW konnte jedoch nur warnen (wie vor) und/oder über entsprechende Betriebsvorschriften das Schlimmste verhindern. Zu diesem Zweck gab OKW/WNV zum 1.12.1942 eine neue „Schlüsselfernschreibvorschrift“[363] heraus, deren Beachtung die Teilstreitkräfte jeweils extra anordnen mußten, da das OKW keine Befehlsgewalt über die Teilstreitkräfte hatte. Diese enthielt, neben dem Verbot, T52a/b-Maschinen im Funkverkehr einzusetzen, zahlreiche teils strenge Bestimmungen, die offensichtlich die bisherigen Erfahrungen, und vor allem kryptologischen Sachverstand, einbezogen. Die kryptologisch fundierten Einzelvorschriften kompensierten zwar teilweise die bekannten Schwächen der Maschinen, und es sollte durch „ständige Beaufsichtigung des Fernschreibpersonals“ sichergestellt werden, daß die Anordnungen sorgfältig befolgt werden, „ ... da davon die Schlüsselsicherheit in hohem Maße abhängt.“[364]

Beim Studium dieser Vorschrift drängt sich aber der Verdacht auf, daß die geforderten, teils umständlichen Prozeduren unter Frontbedingungen wohl kaum durchsetzbar waren, zumal die Operatoren 155 Einzelvorschriften beachten mußten. Man könnte sie daher als ein Alibi für OKW/WNV betrachten, um im „Bedarfsfall“ beweisen zu können, das Erforderliche getan zu haben. Ohnehin war OKW/WNV für die Einhaltung der Vorschriften nicht zuständig, es besaß dementsprechend auch keine Möglichkeit zur Kontrolle.

Zur Sicherheit der ENIGMA äußerte sich OKW/WNV wohlweislich nicht, denn die Experten von OKW/Chi hatten die kryptologischen Schwächen der ENIGMA I bereits analysiert, die nur sicher war, wenn die Maschine vorschriftsmäßig verwendet wurde.[365] Doch das war unter Kriegsbedingungen eine unrealistische Forderung, wie bereits erwähnt, so daß man lieber schwieg, zumal man es nicht überwachen konnte.

Aber selbst wenn die Militärs Kryptologen für eine systemische Analyse konsultiert und diese dann von bestimmten Chiffriermaschinen abgeraten bzw. Veränderungen empfohlen hätten, ist es fraglich, ob die Fehlentscheidungen der Vorkriegszeit korrigiert worden wären, etwa die Beschaffung der ENIGMA und

---

[362] Vgl. Weierud, Frode: Sturgeon, The Fish BP Never Really Caught, nach einem TICOM-Bericht in: Europan Axis Signal Intelligence in World War II-Vol 3, 1.May 1946. Vgl. ebenso Davies, Donald: The Lorenz Cipher Machine SZ42. In: Deavours, Cipher A. (Ed.), Selections from Cryptologia, Volume XIX, Nr. 1, January 1995. S. 519.

[363] HD/LDv/MDv „Schlüsselfernschreibvorschrift“ des OKW/Chef WNV, gültig ab 1.12.42. Archiv Mache.

[364] Schlüsselfernschreibvorschrift des OKW/Chef WNV.

[365] TICOM I-45: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines. Written by Huettenhain and Fricke. POW/Kew (GB).

des Schlüsselzusatzes SZ40/42.
Die potentiellen Gegner hingegen hatten aus dem Ersten Weltkrieg gelernt und verstanden Kryptologie als eine Waffe, die in einem von Funksendungen geleiteten künftigen Krieg noch wirksamer werden mußte. Dementsprechend prüften Fachgremien sehr kritisch alle Chiffrierverfahren, insbesonders die maschinellen, die zumeist verworfen wurden, wie das Beispiel der TYPEX-Maschine zeigt. Ebenso verlangten US-Gremien Verbesserungen der ECM-Maschinen, die dann auch erfolgten. Und die Alliierten bauten ihre im Frieden verkleinerten kryptanalytischen Dienste nach Kriegsbeginn stark aus und rekrutierten dafür geeignete Wissenschaftler und Ingenieure, die vom Kriegsdienst freigestellt wurden.
Doch die (wenigen) deutschen Kryptologen waren nur für Entzifferungen zuständig: Sie konnten die Beschaffungen der Chiffriermaschinen nicht beeinflussen, und auch nicht deren Anwendung. Sie erhielten dementsprechend nicht einmal Zugang zu korrespondierenden militärischen Klar-und Geheimtexten, da diese ja geheim waren.[366]
Unter dem Zwang der Kriegsereignisse scheinen die Waffenämter jedoch ab 1943 immer öfter OKW-Kryptologen konsultiert zu haben, wie beispielsweise unter 3.3.2 dargelegt wurde, demonstrierten dabei freilich ihre Zuständigkeit.

Diese immer bessere Zusammenarbeit zwischen Waffenamt und OKW/Chi gab es hingegen nicht in der Marine – obwohl diese Teilstreitkraft eine erhöhte Chiffriersicherheit benötigte und immer auch anstrebte: Den Seekrieg mußte sie nicht nur per Funk führen, sondern überdies die gesendeten Nachrichten ausreichend lange geheimhalten können, denn Schiffe waren lange unterwegs. Alle Nachrichten von und nach Schiffen auf See konnten noch nach Wochen, manchmal Monaten von operativer Bedeutung sein und taktische oder strategische Maßnahmen beeinflussen. Ob aber die Maschine ENIGMA M dafür ausreichend sicher sei, bezweifelten einige Experten der Marine vor dem Krieg, darunter der Marinebeamte und Kryptologe TRANOW. Gleichwohl befahl man deren Einführung, und vermutlich deshalb galten aufwendigere ENIGMA-Betriebsvorschriften.

Gleichwohl unterliefen den Marineoffizieren erstaunliche Fehler wegen fehlender elementarer kryptologischer Kenntnisse: Sie ließen bspw. wörtlich gleiche Informationen an mehrere, bisweilen Dutzende Empfänger senden, und mit deren jeweiligen Chiffrierverfahren verschlüsseln. Den Anlaß hierfür hatten sie selbst herbeigeführt: Sie richteten immer mehr Schlüsselnetze ein im Glauben, Entzifferungen damit erschweren zu können. So mußte man häufig Routinenachrichten an mehrere Schlüsselkreise mit verschiedenen Chiffrierungen senden, wodurch BP-Analytiker per Geheimtext-Geheimtext-Kompromittierung entziffern oder gar den Klartext durch eine Klartext-Geheimtext-Kompromittierung gewinnen konnten.

[366] Vgl. TICOM I-45: OKW/Chi Cryptanalytic Research.

Ein weiteres Beispiel hierzu berichtet BRENNECKE: Der sehr erfahrene Kapitän ROGGE kam bei seinen Hilfskreuzeraktionen aufgrund scharfsinniger Beobachtung gegnerischer Reaktionen zum Ergebnis, der Feind müsse – und zwar nach relativ kurzer Zeit – seine Positionen gekannt haben. ROGGE argumentierte, nur durch Entzifferung der an ihn gesendeten Funksprüche sei das erklärbar, denn er selbst habe Funkstille gehalten, konnte also nicht eingepeilt werden.[367] Doch beim Vortrag dieser Erkenntnisse vor DÖNITZ wies eine „Kapazität der Nachrichtentechnik"[368] – [und nicht der Kryptologie!] – alle Einwände gegen die ENIGMA-Sicherheit zurück, erklärte ausführlich, daß und warum es unmöglich sei, in dieses System einzubrechen; die Bedenken seien „absolut irrelevant". Daraufhin verbot DÖNITZ einen entsprechenden Eintrag ROGGES in sein Kriegstagebuch.[369]

Doch die verdächtigen Ereignisse veranlaßten DÖNITZ gleichwohl, eine Überprüfung der Schlüsselsicherheit zu fordern. Seine Experten kamen jedoch zum Schluß, daß „...die auf dem Schlüssel M beruhendenVerfahren als die mit Abstand als kriegsstandfestesten überhaupt [...] angesehen werden."[370]
Hierzu ergänzend RAHN, dem auffiel, „daß offenbar kein Versuch gemacht wurde, die Schlüsselsicherheit von unabhängigen Experten untersuchen zu lassen, die nicht in die militärische Hierarchie eingebunden waren." Denn die „...Überprüfung erfolgte durch Experten, die [...] von der Überlegenheit des eigenen Systems so überzeugt waren, daß sie die Fähigkeit zur nüchternen Analyse [...] weitgehend eingebüßt hatten."[371]
Doch die naheliegende Frage, warum denn unabhängige Experten nicht konsultiert wurden, stellte RAHN nicht.

Als später nicht mehr zu übersehen war, daß die alliierten Seestreitkräfte über Kenntnisse der U-Boot-Positionen verfügten, ordnete DÖNITZ eine erneute Sicherheitsüberprüfung an, im Februar 1943, zu einem Zeitpunkt also, an dem sich die Brechung der ENIGMA M4 im Dezember 1942 auszuwirken begann. Seine Experten unter der Leitung des Chefs Marinenachrichten, Vizeadmiral MAERTENS, kamen zum Ergebnis, der Gegner müsse seine Informationen aus Peilungen oder Verrat gewinnen, und verfüge neuerdings über Ergebnisse aus Beobachtungen mit einem verbesserten RADAR-Gerät. Dementsprechend sei „....eine Unterstellung des Mitlesens oder der Entzifferung durch den Gegner *kaum vertretbar.*" Zwar sei Mitlesen „....durch geniale Entzifferung, besonders

[367] Nach dem Krieg stellte sich heraus, daß sein spezieller Schlüsselkreis mangels genügend Sendungen in BP nicht entziffert wurde, jedoch die Nachrichten von und nach den an seinen Aktionen beteiligten U-Booten, wodurch Rogges Positionen ebenfalls bekannt wurden.

[368] Brennecke nennt ihn nicht, wohl um den damals noch Lebenden zu schonen. Nach dem Textzusammenhang könnte es Kap. Bonatz gewesen sein, damals Chef des xB-Dienstes, der noch 1970 von der Unbrechbarkeit des Schlüssels M überzeugt war.

[369] Vgl. Brennecke, J.: Die Wende im U-Boot-Krieg, S. 29 ff.

[370] Skl/Chef MND 02.10.1941, Prüfung der operativen Geheimhaltung, BA-MA, RM 7/845, Bl. 187 ff.

[371] Rahn, Werner: Der Seekrieg im Atlantik und Nordmeer. In: Das Dt. Reich und der Zweite Weltkrieg, Band 6, S. 320-322.

unter Anwendung maschineller Mittel *denkbar*, jedoch unwahrscheinlich." Denn: Der [hohe] Stand der eigenen Entzifferungsmethoden belege das, und damit sei der „...grundsätzliche *Beweis* [?] erbracht..., daß der Gegner nicht mitliest, nicht entziffert, auch nicht teilweise entziffert".[372] [Hervorh. durch Verf.].
Mit anderen Worten: Wenn wir es nicht können, ist der Gegner dazu auch nicht in der Lage – Überheblichkeit oder Schutzbehauptung? Zu vermuten ist letzteres, denn MAERTENS hatte vor dem Krieg[373] die Verwendung der ENIGMA in der Marine empfohlen und nun freilich nicht den Mut, diese Fehlentscheidung einzuräumen. Und seine merkwürdig gewundenen Formulierungen kann man durchaus als indirektes Eingeständnis interpretieren. Verdächtig ist ebenso, daß MAERTENS wiederum für eine *interne* Überprüfung sorgte, unter seiner Kontrolle nämlich, statt externe bzw. unabhängige Kryptologen zu konsultieren, die womöglich zu für ihn peinlichen Erkenntnissen kommen könnten. So wendete er die Gefahr für sich ab und überzeugte den zweifelnden DÖNITZ, der es schließlich notgedrungen „als so gut wie sicher" erwiesen sah, daß der Gegner seine Informationen durch „Flugzeug-Funkmeßortung" [= RADAR] gewinnen müsse.[374]

Doch DÖNITZ' Mißtrauen blieb: Er versetzte MAERTENS auf einen einflußlosen Posten und befahl zum 1. Juli 1943 den Austausch der ersten, seit Einführung der ENIGMA M4 verwendeten „Griechenwalze" β gegen eine neue Walze γ, zusammen mit einer neuen Umkehrwalze C „dünn".[375] Daraufhin konnte BP nicht mehr entziffern und mußte erst einmal die innere Verdrahtung der neuen Walzen rekonstruieren. Dazu benötigte man ein ausreichend langes *crib*, das erfahrungsgemäß nicht lange auf sich warten lassen würde, denn die häufigen *re-encipherments* zwischen den Verfahren der ENIGMA M4 und M3 ermöglichten Klartext-Geheimtext-Kompromittierungen, wie unter 5.2.3 dargelegt ist. Und mit dieser Methode hatte BP nach wenigen Wochen das Problem gelöst und entzifferte ab 12. September 1943, zusammen mit den US-Kollegen, regelmäßig die meisten ENIGMA M4-Nachrichten. Überdies sorgte die deutsche Marine für Arbeitserleichterungen, die viel BOMBE-Laufzeit sparten: Beispielsweise „lieferte" sie regelmäßig ab 24. Oktober 1943 das *Biscay Weather crib* (BP-Jargon), weil die täglichen Berichte einer dortigen Marine-Wetterstation stets mit WETTERVORHERSAGEBISKAYA begannen, und das immer an gleicher Stelle. Dieses ideale *crib* stand bis zur Zerstörung der Station im Juni 1944 zur Verfügung.[376]

---

[372] OKM/SKL/Chef MND B.Nr. 441/43, gKdos 13.2.1943. BArch-MA, RM 7/107, Bl. 3-76.

[373] Er war u.a. 1939 Chef Nachrichtenmittelversuchskommando, dann nach Kriegsbeginn Chef der Amtsgruppe Technisches Nachrichtenwesen im Marinewaffenhauptamt.

[374] In seinem Kriegstagebuch vom 5.3.1943. BArch-MA, RM 87/26, Bl. 19.

[375] Analog zur Umkehrwalze B "dünn". Beide dünne Walzen passten zusammen mit den jeweiligen Griechenwalzen in die ENIGMA M4, da so die Breite der „normalen" Umkehrwalzen eingehalten wurde, um die M4-Maschinen weiter verwenden zu können.

[376] Vgl. Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", Oct 1943.

MAERTENS' Nachfolger STUMMEL sorgte nicht einmal dann für Änderungen der Chiffrierung, als die Abwehr einen Bericht des schweizer Geheimdienstes vorlegte, wonach „*A special office in England* [nämlich BP] *has dealt exclusively with solving German codes. It has succeeded for some months in reading all orders by the German Navy HQ to U-boat commanders ...*".[377] Zwar löste diese Information Aufträge aus, einmal an die Abwehr zur Verifizierung der Nachricht, zum anderen an die *eigenen* Nachrichtenexperten zur erneuten Überprüfung der Chiffriersicherheit. Doch wie sonst immer blieb auch STUMMEL bei der Überzeugung, die ENIGMA-Sicherheit „steht außer Frage". Man diskutierte überhaupt nicht einmal die Möglichkeit einer alliierten Entzifferung von ENIGMA-Verschlüsselungen, sondern nur die Wahrscheinlichkeit, alliierte Verbände könnten eine komplette ENIGMA zusammen mit den Schlüsseln für einen Monat erbeutet haben.[378]

Doch in der zweiten Hälfte 1943 und Anfang 1944 verlor die Marine eine so große Anzahl U-Boote, daß die Frage „Ist die ENIGMA M4 noch sicher?" nicht mehr überhört werden konnte. Überdies bestätigten Entzifferungen von operativen Sendungen des britischen Peildienstes den Verdacht. Doch erst im Juli 1944 wurde der [quasi-externe] Kryptologe FROWEIN mit zwei Assistenten von der Admiralität „ausgeliehen" und mit der Prüfung beauftragt. Er konnte bis Dezember 1944 nachweisen, wie die ENIGMA-M4 kryptanalytisch brechbar ist, und zwar – günstige Bedingungen unterstellt – mit Hilfe eines *cribs* von nur 25 Buchstaben. Mit *cribs* von max. 78 Buchstaben und Lochkartentechnik könnten auch die Walzenverdrahtungen rekonstruiert werden, doch das untersuchte FROWEIN nicht praktisch, da man ohnehin annahm, der Feind verfüge über eine Maschine M4.[379]

Das einzige Ergebnis dieser Prüfung: Es durften ab Dezember 1944 nur noch ENIGMA-Walzen mit zwei Nocken in der rechten (schnellen) Position eingesetzt werden, da sonst, wie erwähnt, ein crib von 25 Buchstaben zur Entzifferung reichen würde.[380] Und in dem späteren Bericht[381] wurde die ENIGMA M4 weiterhin als „ausreichend sicher" bezeichnet.
STUMMEL scheint dennoch nicht überzeugt gewesen sein, denn er führte zusätzliche „Sonderschlüssel" ein, d.h. jedes Boot erhielt seine eigene spezielle Schlüsselgruppe. Das erschwerte zwar zunächst die alliierte Entzifferung, weil nun *cribs* fehlten, erforderte jedoch andererseits häufig Mehrfachsendungen des gleichen Textes für U-Bootgruppen – und lieferte den Entzifferern die benötigten *depths*.

---

[377] Vgl. Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", Oct 1943. Im Logbuch des BdU im August 1943 registriert. (BdU Log 1-15/8/43).
[378] Ratcliff, R.A.: Searching for Security: The German Investigations into Enigma's Security.
[379] Report on Interrogation of Lt. Frowein of OKM/ 4 Skl III.
TICOM-Bericht I-38 (14.July 1945), S. 2, Ziff. 6. Public Record Office, Kew (GB).
[380] Vgl. Report on Interrogation of Lt. Frowein of OKM/ 4 Skl III. S. 4, Ziff. 31.
[381] OKW/Chi, Chiffrierwesen.

Zusammenfassend ist zu sagen, daß die Marineoffiziere es verstanden, bis zum Kriegsende ihre groben Fehler zu vertuschen, wobei fraglich ist, ob sie diese überhaupt als solche erkannten. Beispielsweise hielt der letzte Chef des xB-Dienstes, der Nachrichtenoffizier Kapitän z.S. BONATZ, eine Brechung der ENIGMA M4 noch bis nach 1970 für nicht möglich. Erst Winterbotham's Buch[382] öffnete ihm die Augen und er mußte nun seine Publikationen umschreiben.
Und wurden die ausgezeichneten Kryptologen des xB-Dienstes hierzu konsultiert, etwa TRANOW? Darüber gibt es keine Hinweise in der Dokumentation, und das überrascht auch nicht, denn er und seine Kollegen waren ja nicht zuständig.

5.4.4 Die SS erlangt die Kontrolle über das Chiffrierwesen

Die Kryptologen im erwähnten Referat des OKW, das 1942 eingerichtet wurde, nahmen sich viel Zeit, denn erst nach weiteren zwei Jahren, als nach dem mißglückten Attentat auf HITLER die SS allmählich[383] die Kontrolle über das Chiffrierwesen erlangte, trat ein „interministerieller Sonderausschuß zur Überprüfung der Sicherheit eigener Geheimschriften" zusammen, erstmals am 25. August 1944 zur Prüfung der Sicherheit der ENIGMA.[384] Ob das ein zeitlicher Zufall war oder aber das SS-Reichssicherheitshauptamt es verlangte, ist nicht bekannt; es gibt es hierzu keine Dokumente oder gar Forschungsberichte.
Der Sonderausschuß befaßte sich als erstes mit der ENIGMA I und schlug „Zur Erhöhung der Sicherheit" [sie galt doch offiziell als sicher?] drei Maßnahmen vor:
a) Verstellen der linken Walze nach je 70 – 130 Buchstaben, jedoch nicht für die Luftwaffe, wo „überall D-Walzen[385] vorhanden sind".
[Diese Verstellmethode, in BP „CY" genannt, wurde ab 15. September 1944 teilweise eingeführt.[386]]
b) Einführung von „Lückenfüllerwalzen"
[s. 3.2.2, Enigma M5/M10; eine Neukonstruktion, die nicht lieferbar war].
c) Einführung der Stecker-Uhr.[387]
Doch die naheliegende Frage, wieso seit 1930 die innere Verdrahtung der Walzen I-III (IV-V kamen neu hinzu in 1938) nie geändert wurde, ebenso nicht die des Eingangsstators, wurde wohl sicherheitshalber nicht angesprochen.

---

[382] S. Fußnote 5.
[383] Offiziell durch Führerbefehl im November 1944.
[384] Bericht über das Chiffrierwesen in OKW/Chi, nach dem Krieg angefertigt.
Vertrauliches Dokument der Zentralstelle für das Chiffrierwesen der BRD. Sammlung Staritz.
[385] Gemeint sind die schaltbaren Umkehrwalzen der ENIGMA I., s. dazu 3.2.2. Es wurden nur relativ wenige Maschinen damit ausgerüstet, und zudem kompromittiert, weil gleiche Texte oft für beide Systeme gesendet werden wurden – ein typisch deutscher Fehler.
[386] Vgl. Ulbricht, Heinz: Uncle Dick and another Horrors of the Enigma. S. 52. Es ist jedoch nicht bekannt, ob diese Methode oft angewendet wurde bzw. wie lange. Überdies erschwerte sie die Entzifferung wenig.
[387] Umschaltvorrichtung für das Steckerfeld, s. dazu 3.2.2, Enigma I. War vermutlich mangels Produktionskapazität nur in geringen Stückzahlen verfügbar.

In gleicher Weise bewertete der Ausschuß am 26. September 1944 die Sicherheit der Schlüsselfernschreibmaschinen:
a) Die SFM T52c genügt nicht den Anforderungen [war seit 1942 bekannt!].
b) Die SFM T52d und e sind ausreichend sicher mit bestimmten Auflagen, auch für „Geheime Kommandosachen".
c) Bei den SZ40/42-Schlüsselzusätzen sah die Kommission – man formulierte aus verständlichen Gründen sehr vorsichtig – „Einbruchsmöglichkeiten", und forderte daher begrenzende Auflagen, gleichwohl blieb die Maschine für „Geheime Kommandosachen" zulässig, wenn auch „nur auf Linienverbindungen."[388]
d) Für einen verbesserten SZ42c – wohl ebenfalls für erforderlich erachtet – habe man die Sicherheitsüberprüfungen noch nicht abgeschlossen.

Die ebenso naheliegende Frage, wieso seit 1932 (T52) bzw. 1939 (SZ40/42) Art und Anordnung der Schlüsselwalzen dieser Maschinen nie geändert wurde, diskutierte man auch hier sicherheitshalber nicht.
Und besonders merkwürdig: Die sichere OTP-Schlüsselfernschreibmaschine T43, die bereits ab Anfang 1944 im Einsatz war, erwähnt der Bericht überhaupt nicht. Wollte man etwa verhindern, daß die SS mißtrauisch wurde, wenn so ein weit sichereres Gerät zur Verfügung stand? Oder gar fragte, warum denn die T43 eingeführt wurde, wenn bewährte „sichere" Maschinen wie die T52 bzw. SZ42 zur Verfügung standen?
Zu diesen Unklarheiten sind Forschungsberichte leider nicht bekannt.

Das Dokument berichtet auch über einen Vortrag im November 1944 über den „Stand der Sicherheit der eigenen Geheimschriften". Danach zeige „Die Überprüfung der in der Wehrmacht eingeführten Verfahren und Schlüsselmaschinen ..., daß alle strengen Sicherheitsanforderungen nicht immer erfüllt sind. Ein großer Teil der eigenen Verfahren ist nicht kompromißsicher." [!]

Ein anderes Dokument[389] bestätigt später diese Angaben: Darin bezeichnete man bspw. ENIGMA I und M4 zwar als „ausreichend sicher", gleichwohl befand sich „zur weiteren Erhöhung der Sicherheit" eine „Lückenfüllerwalze" in der Fertigung [wie vor]. Die „Steckeruhr" konnte wegen „Fertigungsschwierigkeiten nicht eingeführt werden". [Das ist unrichtig, eine unbekannte Anzahl war bereits ab Juli 1944 im Einsatz]. Die schaltbare Umkehrwalze D erwähnt das Dokument

[388] Unter „Linienverbindungen" versteht man Draht- und Richtfunkverbindungen, aber auch den abhörbaren „Funk-Linienverkehr" als Gegensatz zum „Stern-und/oder Netzverkehr". Der Bericht unterscheidet nicht klar zwischen (abhörbaren) „Funkfernschreiblinien" und (Draht)-„Linienverbindungen" und kann so interpretiert werden, daß „Funkfernschreiblinien" gemeint waren. Dementsprechend blieb der SZ42 im Funkfernschreib-betrieb bis Kriegsende.
Mache nimmt auf Grund der damaligen Situation an, daß der Ausschuß mit der mißverständlichen Bezeichnung „Linienverkehr" die erkannte Schwäche des SZ42 vor der SS kaschieren wollte.
Mache, Korrespondenz.

[389] Interner Bericht (o. N.) OKW/Chi: Der Stand des Chiffrierwesens in der Wehrmacht, 15. Febr. 1945. Bundesarchiv-Militärarchiv, RW 4/920.

nicht, obwohl eine unbekannte Anzahl seit Anfang 1944 verwendet wurde. Schließlich sei eine „neue Schlüssel- und Gebrauchsanleitung in Vorbereitung."

Den Schlüsselzusatz SZ42 hielt man ebenso für „ausreichend sicher auf Linienverbindungen", eine unklare Vorschrift, wie bereits erwähnt. Dennoch bestanden wohl weiterhin Zweifel, denn es „...wird ein neuer SZ42c von höherem Sicherheitsgrad entwickelt" – obwohl er bereits fertig und in der Prüfung war.
Ebenso waren die ab Armeeoberkommando eingesetzten Schlüsselfernschreibmaschinen SFM T52 d und e „ausreichend sicher"; Typ T52 c „genügte nicht" und werde daher „z.Zt. zum Typ T52 e umgebaut".
[Die Experten des Auswärtigen Amtes (Abt. Pers Z) wußten dazu besser Bescheid, sie entzifferten mit T52e verschlüsselte Nachrichten der Militärattachès, die über Kanäle des AA gesendet wurden.[390] Das wurde freilich geheimgehalten, wie damals üblich, und weder OKW/Chi noch der erwähnten Kommission mitgeteilt].

Die sehr sichere OTP-Schlüsselfernschreibmaschine Siemens T43 erwähnt dieses Dokument ebenso nicht, obwohl die Geräte bereits seit Anfang 1944 bei einigen Heeresfunkstellen, in der Marine und dem AA eingesetzt wurden.

Es liegt nahe, die Ergebnisse der Kommission als Kaschierung der wahren Verhältnisse zu interpretieren, denn die Militärs mußten um ihr Leben fürchten, wenn ihre Versäumnisse erkannt würden. So vermied man bspw. jegliche Diskussion über die nie geänderten Schlüsselwalzen der ENIGMA und der Schlüsselfernschreibmaschinen, ebenso über die sichere Maschine T43 – die SS hätte womöglich gefragt, wer dafür die Verantwortung trägt.

5.5 Was wußten die deutschen Experten ?

Der erwähnte Bericht enthält auch einen Vermerk über einen Vortrag im November 1944 über den „Stand der Sicherheit der eigenen Geheimschriften", vermutlich gehalten vom OKW/Chi-Kryptologen HÜTTENHAIN (s.u.). Danach zeige „Die Überprüfung der in der Wehrmacht eingeführten Verfahren und Schlüsselmaschinen ..., daß alle strengen Sicherheitsanforderungen nicht immer erfüllt sind. Ein großer Teil der eigenen Verfahren ist nicht kompromißsicher."
Damit wird erstmals offiziell eingeräumt, daß die Schlüsselsicherheit problematisch ist – was vermutlich schon viel länger bekannt war. Denn daß man im OKW sehr viel mehr wußte, geht aus einem Bericht hervor, den die OKW/Chi-Kryptologen HÜTTENHAIN und FRICKE unmittelbar nach dem Krieg erstatteten: Sie beschrieben für alle deutschen Chiffriermaschinen Methoden zur Entzifferung, die OKW/Chi erarbeitet hatte. Und daß und warum bei deren „nicht vorschriftsgemäßer Verwendung" – die sie „als im Krieg normal"

[390] Vgl. van der Meulen, M.: The Road to German Diplomatic Ciphers – 1919 to 1945. In: Cryptologia, Vol XXII (2), April 1998, S. 163.

bezeichneten – die Entzifferung besonders einfach sei. Sie konnten das jedoch mangels Zugang zu authentischen Klar- und Geheimtexten nicht überprüfen, den sie nicht erhielten, weil sie nicht zuständig waren.[391]
Leider äußerten sie sich nicht dazu, warum diese Erkenntnisse, nämlich die offenkundige Gefahr von Entzifferungen, nicht umgehend Konsequenzen zeitigten bzw. welche zuständigen Dienststellen nicht reagierten und aus welchem Grund.

Der bereits mehrfach erwähnte Kryptologe Erich HÜTTENHAIN (1905-1990) begann nach einem Mathematikstudium 1935 seinen Dienst als Referent im OKW/Chi. Er avancierte später zum Regierungsrat und Abteilungsleiter „Analytische Kryptologie", wozu auch die Überprüfung eigener Chiffrierverfahren gehörte. Nach dem Krieg übernahm er zunächst eine Professur für Mathematik, und wurde dann 1953 der erste Leiter der „Zentralstelle für das Chiffrierwesen" (ZfCh) des Bundesnachrichtendienstes. Diese Einrichtung sorgte für sichere Chiffrierverfahren für alle Dienststellen des Bundes, und wurde später zum „Bundesamt für die Sicherheit in der Informationstechnik" (BSI). Laut LEIBERICH, dem Nachfolger HÜTTENHAINS, zählte die ZfCh „... innerhalb der NATO zu den angesehendsten Behörden", deren Entwicklungen auch in der NATO eingesetzt wurden, teils „... nach heftiger Konkurrenz".[392] Und in dieser ZfCh arbeiteten überwiegend die erfahrenen Kryptologen des OKW, der Marine und des Auswärtigen Amtes, die nun die Kompetenz der deutschen Weltkriegskryptologen zeigen konnten. Doch das konnten sie kaum während des Krieges, die berichteten Zuständigkeiten verhinderten das zumindest bis 1944. Das ihnen gelegentlich unterstellte unkritische Vertrauen in die eigenen Chiffrierungen hatten hingegen die Waffenämter und andere militärische Dienststellen.

Die Alliierten versuchten nach dem Krieg, das deutsche Phänomen des scheinbar übergroßen Vertrauens in die maschinellen Chiffrierungen zu klären und beauftragten dazu ein *Technical Intelligence Committee* (TICOM). Dessen lange geheimer Bericht[393] über erbeutete Geräte, Befragungen deutscher Verantwortlicher, Auswertung von Dokumenten usw. wurde inzwischen auszugsweise freigegeben; ERSKINE faßt die ENIGMA betreffenden Teile so zusammen:

• Das Auswärtige Amt lehnte die Verwendung der ENIGMA ab, weil deren Sicherheit ungenügend sei.

• Die Kriegsmarine hatte die Maschine in einer kryptologisch stärkeren Version (M1/2/3) zwar übernommen, jedoch bezweifelten nach Kriegsbeginn sogar eigene

[391] TICOM I-45: OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines.
[392] Vgl. Leiberich, Otto: Vom diplomatischen Code zur Falltürfunktion. Hundert Jahre Kryptographie in Deutschland. In: Spektrum der Wissenschaft 4/2001, S. 16.
[393] Ein neunbändiges Konvolut vom 1.5.1946.

Experten die Sicherheit der Maschine. Beispielsweise empfahl der Kryptologe des B-Dienstes, W. TRANOW, statt der ENIGMA ein Codebuch-System mit Überschlüsselung zu verwenden. [Die Maschine wurde gleichwohl beschafft – TRANOW war ja nur ein unzuständiger Beamter[394]].[395]

Nach dem Krieg bestätigte TRANOW bei der TICOM-Befragung, daß vor Juli 1944 keine Sicherheitsüberprüfung der ENIGMA M4 erfolgte. Und daß die dafür verantwortlichen Marineoffiziere allenfalls prüften, was die Feinde womöglich mit dem Besitz einer ENIGMA machen könnten, und das gar als kryptanalytische Attacke verstanden. Sein vernichtendes Urteil: „*...these sort of people* [die Marineoffiziere] *were no use*."[396] Da hatte er womöglich auch an seinen Chef während des Krieges gedacht, den Kapitän z.S. H. BONATZ, der, wie bereits erwähnt, sogar noch 1970 von der Unbrechbarkeit der ENIGMA M4 überzeugt war.[397]

Zu ähnlichen Ergebnissen kommt BAMFORD in seiner TICOM-Auswertung:
Er berichtet u.a. von der Überraschung der alliierten Experten bei den Verhören der deutschen Kryptologen, wonach „.... die Deutschen die ganze Zeit darüber im Bild waren, dass ENIGMA nicht sicher war ... und genau wussten, wie ENIGMA geknackt werden konnte...", so der spätere NSA-Forschungsdirektor H. CAMPAIGNE.[398]

Hier zeigte sich ein weiteres Problem der militärisch dominierten Entscheidungsprozesse: Es waren immer *militärische* Experten, die sowohl die angebotenen Maschinen prüften und beschafften, als auch später deren Sicherheit zu beurteilen hatten, mithin sich selbst beurteilten. Ob und welche wissenschaftliche Analysen sie dazu anforderten bzw. diese berücksichtigten, blieb ihnen überlassen. Externe Prüfungen, gar durch zivile Wissenschaftler, kamen nach damaligem Verständnis wohl überhaupt nicht in Frage.

Doch wurden nicht nur die Erkenntnisse externer Wissenschaftler nicht eingeholt, auch die eigenen Experten im OKW/Chi und in anderen Teilstreitkräften konnten sich mit ihren Bedenken nicht durchsetzen, denn: Sie waren nicht zuständig, wohl das wichtigste Kriterium beim deutschen Militär, und überdies Beamte oder allenfalls Reserveoffiziere, deren Meinung traditionell wenig galt. Leider wurde dieses Phänomen bisher kaum erforscht, doch die bekannten Fakten im Zusammenhang mit deutscher militärischer Kryptologie sprechen eine deutliche Sprache.

---

[394] Er diente im Ersten Weltkrieg als Marinefunker, später als Marinebeamter (Oberregierungsrat).
[395] Erskine, Ralph: Enigma's Security: What the Germans Really Knew.
[396] Report on Interrogation of Lt. Frowein of OKM/ 4 Skl III. TICOM-Bericht I-38, S. 4, Ziff. 33.
[397] Vgl. Bauer, Geheimnisse, S. 221.
[398] Vgl. Bamford, James: NSA - Die Anatomie des mächtigsten Geheimdienstes der Welt. S. 31.
Dt. Ausgabe, München 2001. Übers.: Bonn, Dierlamm, Ettinger u. Maass.
Orig.: Body of Secrets, New York (NY) 2001., S. 31.

Alliierte Historiker scheinen diese Zusammenhänge nicht immer richtig zu verstehen, sogar ein Kenner deutscher Verhältnisse wie D. KAHN nicht, denn er schrieb dazu: „*... the very fact that the German ... government had adopted a cryptographic system for official use…*".[399] Das aber ist falsch, denn Regierungsstellen waren nicht zuständig für militärische Verwendungen, sondern ausschließlich die jeweiligen Waffenämter, und KAHN gelangt daher zum ebenso falschen Ergebnis: „*...neither country* [hier Deutschland und Japan im Sinne von Regierung] *ever made a serious ... cryptanalytic study of their machines*...", was zwar formal richtig ist, aber an der falschen Stelle ansetzt. Und mit den „*totalitarian regimes*" hat das auch nichts zu tun, denn deren „*official use*", den es wie erwähnt nicht gab, konnte mithin keine „ ... *extra aura of infallibility to the security*..." der Chiffriermaschinen erzeugen. Vielmehr waren die deutschen Militärs der Meinung, daß sie mit militärischen Prüfungen durch Waffenämter und im „Feldversuch" beurteilen konnten, ob eine Maschine geeignet war. Überdies scheinen sie unkritisch den Angaben der Hersteller geglaubt zu haben, daß eine große Schlüsselperiode als Sicherheitskriterium ausreichend und entscheident sei. Sie haben diesen Fehler ausschließlich selbst zu verantworten, denn die Vertreter des *totalitarian regimes*, nämlich das Reichssicherheitshauptamt, befaßten sich erst nach dem 20. Juli 1944 damit. Und dessen SS-Offiziere verfügten selbst kaum über kryptologische Kompetenz; ob sie ihre „erbeuteten" österreichischen und ungarischen Kryptologen[400] dazu konsultierten ist mangels Forschung nicht bekannt.

5.6 Exkurs: Bletchley Park, Y-Service und ULTRA

Die erwähnten hervorragenden wissenschaftlich-technischen Leistungen erbrachten bis zu 10.000 Mitarbeiter in der zentralen Entzifferungsabteilung des britischen Geheimdienstes M.I.6 (*Secret Intelligence Service*) und des M.I.8 (*Signals Intelligence Service = Y-Service*. Es liegt nahe, diese Einrichtung näher zu beleuchten, um deren Arbeitsweise besser einschätzen zu können, denn sie war das weltweite Zentrum der maschinellen Kryptanalyse.

ULTRA war das „Produkt" dieser bis 1974 geheimgehaltenen Organisation mit verschiedenen Tarnbezeichnungen: Offiziell war sie eine Abteilung des Außenministeriums, Tarnbezeichnung *Government Cypher & Code School* (GC&CS), gehörte aber zu den genannten Geheimdiensten. Kurz vor Kriegsbeginn verlagerte man die Abteilungen als „Station X" nach BP.
Diese Einrichtung entzifferte fast *alle erreichbaren* Funksendungen nicht nur der deutschen Wehrmacht, sondern auch die der Abwehr, der Reichsbahn, der SS, der Polizei usw., Dazu kamen italienische Militärsendungen, die für den Mittelmeerkrieg sehr wichtig waren, und die häufigen, meist sehr informativen

[399] Vgl. Kahn, David: Seizing the Enigma: The Race to Break the German U-Boat-Codes, 1939-1943, S. 315. Houghton Mifflin, Boston MA/USA, 1991.
[400] Ausf. in: Bauer, Geheimnisse, S. 63.

Sendungen der japanischen Botschaft Berlin. Das Codewort ULTRA für die daraus gewonnene *intelligence* wurde im Juli 1942 eingeführt und löste das bisherige inoffizielle SPECIAL ab.[401] Diese *intelligence* bestand nicht nur aus Informationen für die taktische Kriegsführung, so wichtig diese auch waren, beispielsweise für den U-Boot-Krieg oder die Luftschlacht um England. Vielmehr verschaffte die Sammlung und Auswertung *aller* Informationen, auch verspätet entzifferter, eine einmalige informationelle Überlegenheit: Sie ermöglichte u.a. durch scharfsichtige Zusammenschau eine umfassende *Order of Battle* zu entwickeln, die den Alliierten auch vorausschauende Planungen ermöglichte. Das ging soweit, daß vor kritischen militärischen Ereignissen etwa das Führungsverhalten der dabei kommandierenden deutschen Offiziere meist richtig prognostiziert werden konnte, weil deren Persönlichkeitsprofile im Laufe des Krieges erarbeitet worden waren. Dazu kamen die ebenfalls regelmäßig ermittelten Versorgungslagen, und schließlich die in entzifferten Fernschreiben diskutierten Pläne der obersten deutschen Führung. Mit dieser *intelligence* konnten die Auswerter in BP fast immer richtig die voraussichtlichen Maßnahmen des Gegners einschätzen.

5.6.1 Die Sicherung des ULTRA-Geheimnisses

Die Existenz von BP und der ULTRA-Informationen wurden erst 1974 teilweise offenbart.[402] Und erst durch US-Dokumentefreigaben in 1996 und 2000, sowie nachfolgend im *Public Record Office*, Kew/GB, sind viele wichtige Informationen zugänglich. Daß diese Geheimhaltung im Krieg erforderlich war, und zwar mit höchster Sicherheitsstufe, bezweifelte niemand, doch wurde oft gefragt, warum sie so ungewöhnlich lange aufrecht erhalten wurde.
Aber dafür gibt es einen wichtigen Grund: Die Entzifferungen wurden nach dem Krieg fortgesetzt, wie nachstehend dargelegt ist. Und zwar gegen ehemalige Verbündete wie Frankreich und Norwegen, gegen koloniale Befreiungsbewegungen bzw. Regierungen, und zunehmend gegen die Sowjetunion und deren Verbündete. Der Hintergrund dafür dürfte der beginnende kalte Krieg gewesen sein, und dann das Atomprogramm der Sowjetunion.
Die angloamerikanischen Geheimdienste unterstützten überdies mit einer perfiden Methode die Fortsetzung der Entzifferungen: Zahlreiche erbeutete ENIGMA-Maschinen, aber auch TYPEX- und M209-Maschinen verschenkten sie gezielt an die interessierenden Länder – und konnten dann alles mitlesen, denn die Entzifferungsmaschinen waren ja noch vorhanden und wurden für den neuen Zweck sogar mit Elektronik leistungsgesteigert (s. dazu 7.5).

Freilich wurde das stets bestritten, doch nun bestätigte der Politikwissenschaftler und Geheimdienstexperte Richard ALDRICH diese Maßnahmen nach

[401] HW 14/43, July 1942. PRO/Kew
[402] Durch: Winterbotham, F.W.: The Ultra Secret, New York, Harper, 1974.

einschlägigem Dokumentenstudium.[403] Danach setzte die britische GCHQ (BP-Nachfolgeorganisation) die Entzifferungsarbeit fort, nachdem sie zahlreiche Staaten überredet hatte, die offiziell sicheren ENIGMA- Maschinen für ihre geheime Kommunikation zu verwenden. Und diese sollen in manchen Ländern bis 1974 im Einsatz gewesen sein, bis ULTRA und damit die Kompromittierung der mit diesen Maschinen verschlüsselten Nachrichten allgemein bekannt wurde.
Ebenso weiß man erst seit wenigen Jahren ungefähr, mit welchem Aufwand die US-Geheimdienste die Entzifferungsarbeit nach dem Kriege fortsetzten. So wurde beispielsweise bei der Gründung der Vereinten Nationen 1945 der Nachrichtenverkehr fast aller Delegationen mit ihren Regierungen entziffert, darunter auch verbündeter Staaten wie beispielsweise Frankreich: Die französische Delegation verschlüsselte mit einer Hagelin C-38 [=M209], die den Entzifferern freilich keine Probleme bereitete.
Dieser Erfolg demonstrierte den US-Verantwortlichen die Bedeutung der Kryptanalyse auch in Friedenszeiten. Die dadurch erreichbaren Vorteile für die Verhandlungsführung gedachte man auch zukünftig zu nutzen, und so setzten die USA durch, den endgültigen Sitz der UNO in den USA festzulegen, denn so hatte man unmittelbaren Zugriff auf die per Kabel gesendeten Nachrichten der Delegationen.[404]

Hierzu gibt es auch eine indirekte Bestätigung: Die Weiterverwendung bzw. -entwicklung von Entzifferungsmaschinen in den US-Geheimdiensten. Darüber berichtet bspw. DEAVOURS *„....the SUPERSCRITCHER was in use from early 1946."*[405] Diese Maschine war die elektronische Weiterentwicklung des elektromechanischen AUTOSCRITCHERs, den man 1944 gegen die ENIGMA-Variante mit schaltbarer Umkehrwalze D gebaut hatte, weil dadurch die BOMBE-Maschinen wirkungslos wurden. Wenn aber eine so aufwendige Maschine nach dem Krieg weiterentwickelt wurde (BOMBE-Maschinen waren ohnehin vorhanden), kann das nur heißen, daß ENIGMA-Varianten von anderen Ländern genutzt und deren Nachrichten entziffert wurden.

Zu diesen Drittländern zählten vermutlich sogar NATO-Länder: Sie erhielten eine abgespeckte Version der sicheren und geheimen US-Maschine SIGABA[406] namens KL-7, und wahrscheinlich sorgte der US-Geheimdienst bei der Vorbereitung der Aktion dafür, daß er diese Maschine brechen konnte. Wie problematisch solche Methoden sein können zeigte sich, als 1982 der sowjetische Agent und US-Offizier HELMICH verhaftet wurde, der seit 1962 den Sowjets wiederholt Unterlagen über Walzen und Schlüssel der Maschine verkauft hatte.[407] So

[403] Vgl. Aldrich, Richard D.: Cold War Codebreaking and Beyond. In: Erskine, Ralph and Smith, Michael (Eds.): Action this Day. Bantam Press, London u.a. Orte, 2001, S. 408.
[404] Vgl. Bamford, James: NSA - Die Anatomie des mächtigsten Geheimdienstes der Welt. S. 36-39.
[405] Deavours, C.A.: The Autoscritcher. In: Deavours, Cipher A. (Eds.), Selections from Cryptologia, Volume XIX, Nr. 2, April 1995, S. 541.
[406] Die weltweit teuerste und äußerst sichere US-Rotormaschine (15 Rotoren) wurde stets bewacht und geheimgehalten. Sie war für Kommunikation der höchsten Führungsebene zugelassen.
[407] Vgl. Bauer, Geheimnisse, S, 144.

konnten vermutlich beide Supermächte den geheimen Nachrichtenaustausch der NATO-Länder verfolgen.

Hauptziel der britischen und US-Dienste war bald nach Kriegsende jedoch die Sowjetunion, besonders deren Atomwaffenprogramm, und die Enttarnung der zahlreichen Sowjetagenten. Durch ein 1996 deklassifiziertes Dokument (*Venona breaks*) wurde bekannt, daß man den umfangreichen sowjetischen Agentenfunkverkehr teilweise entziffert hatte und so Agenten enttarnen konnte. Darüber hinaus lieferten die Entzifferungsdienste „...ein vollständiges Bild des nationalen Sicherheitsapparates der Sowjetunion...", denn sie knackten alle relevanten Sendungen des Militärs, der Polizei und der Industrie.
In 1948 versiegten plötzlich diese Informationsquellen: Der im US-Geheimdienst tätige Sowjetagent WEISBAND hatte den Sowjets die Entzifferungen gemeldet, die daraufhin radikal ihre Chiffriersysteme änderten.[408]

Das erzwang intensive Forschungen und forcierte den Bau von leistungsstarken Computern und anderen „*high speed analytical equipment*"[409] – und stärkte die Kompetenz der US-Dienste auf diesem zukunftsträchtigen Gebiet.

5.6.2 ULTRA = Funkaufklärung ?

ULTRA war demnach ein Tarnname für Erkenntnisse, die der deutsche Begriff „Funkaufklärung" nur unzureichend abdeckt, denn dieser bezieht sich auf die rein militärische Aufklärung. Die *intelligence* hingegen, die den militärisch und politisch Verantwortlichen der Westmächte zur Entscheidungsfindung diente, bestand aus mehreren Komponenten: Entzifferungen aller erreichbaren militärischen, diplomatischen und reichsinternen Sendungen (s.u.), ergänzt durch Luftaufklärung und Agentenberichte, die zentral ausgewertet wurden in einer „intelligenten" Zusammenschau.
Welche Bedeutung anglo-amerikanische Historiker dieser *intelligence* zumessen, zeigt die Bezeichnung „*the missing dimension*" im Sinne von dem fehlendem Hintergrund, ohne dessen Kenntnis die Handlungen der Verantwortlichen nicht richtig beurteilt werden können.[410]

Die in BP erarbeiteten, taktisch und strategisch nutzbaren Informationen gingen direkt an die jeweiligen Oberkommandos in London und/oder an das *War Office* des Premierministers. Später wurden vom Geheimdienst ausgewählte Nachrichten – zur Geheimhaltung der Quelle als „Agentenberichte" getarnt – durch speziell ausgesuchte Nachrichtenoffiziere (*Special Liaison Units* – SLU) direkt an die alliierten Frontkommandeure übermittelt. Dazu sicherte man die

[408] Vgl. Bamford, James: NSA , S. 36-39.
[409] Vgl. Deavours, C.A.: The Autoscritcher. In: Deavours, Cipher A. (Eds.), Selections from Cryptologia, Volume XIX, Nr. 2, April 1995, S. 406-409.
[410] Vgl. Copeland, Computer Age, S. 342.

Übertragung per OTP-Verschlüsselung, und später im Krieg ab Juli 1942, vermutlich wegen der aufwendigen OTP-Logistik, per TYPEX-Maschinen.[411] Diese Offiziere waren zur Verschwiegenheit gegenüber den alliierten Kommandeuren verpflichtet; das ULTRA-Geheimnis durfte niemals offenbart werden.

Anzumerken ist noch, daß die einschlägige Literatur die von BP ebenso entzifferten Sendungen aus dem Reichsinnern scheinbar nicht ausgewertet hat. Doch diese Funksendungen nahmen im Verlauf des Krieges immer mehr zu, weil mangels funktionierender bzw. wegen überlasteter Kabelverbindungen immer mehr Nachrichten gesendet werden mußten, nicht etwa nur militärische. Beispielsweise gab es auf dem südlichen und östlichen Kriegsschauplatz keine durchgehenden Drahtverbindungen entlang der Schienenstrecken, geschweige ein funktionierendes Bahn-Telephonnetz, so daß die Reichsbahn dort ebenfalls ihre Transportvorbereitungen und –meldungen funken mußte. Später wurde das auch auf dem westlichen Kriegsschauplatz erforderlich, teilweise sogar innerhalb des Reichsgebietes, weil auch das deutsche Bahn-Telefonnetz immer häufiger durch Bombenschäden unterbrochen wurde.
So konnte BP die meisten wichtigen Transportmeldungen entziffern, wobei sich zeigte, daß diese Informationen hohen strategischen Wert besaßen.

5.6.3 Der Y-Service

Ohne diese Organisation hätte BP nicht genügend Material entziffern können und ULTRA wäre nicht möglich gewesen: Die Funkabhörstationen und deren Arbeit zur Bereitstellung von zur Kryptanalyse geeignetem Material, mit der Tarnbezeichnung *Y-Service*, eine Organisation, die CHURCHILL bereits zu Beginn des Ersten Weltkrieges aufbauen ließ. Nach der Verkleinerung in der Zwischenkriegszeit wurde sie im Zweiten Weltkrieg zu einer Organisation mit Tausenden Mitarbeitern erweitert: Abhör- und Peilstationen errichtete der *Y-Service* weltweit, wozu das damalige ausgedehnte britische Imperium genügend Stützpunkte bot (ausgenommen in den USA, mit denen man zusammenarbeitete). So konnten alle erreichbaren Sendungen eingepeilt, abgehört und aufgezeichnet werden.

Der Personalbedarf dafür war immens, so arbeiteten beispielsweise auf einer Station [Beaumanor (GB)] 1200 Personen in vier Schichten.[412]
Dieser Aufwand war erforderlich für das Abhören aller Frequenzen, Überwachung deren Funkaktivitäten usw. und die korrekte Aufzeichnung der Sendungen. Beispielsweise kam es wegen der weiten Entfernungen und/oder geringer Senderleistungen häufig zu Empfangsstörungen. Zur Rekonstruktion

[411] Vgl. Momsen, B.: Codebreaking and Secret Weapons in World War II, Chapter II. (Diese Angaben bestätigt das inzwischen freigegebene Dok. HW 14/43 im PRO vom 20.11.1942).
Anm.: Die TYPEX-Verschlüsselung konnte von deutschen Entzifferern nicht gebrochen werden.
[412] Vgl. Smith, Michael: Enigma entschlüsselt, S. 136.

des Textes mußten dann die Protokolle verschiedener Stationen verglichen und versucht werden, einen zur Kryptanalyse noch geeigneten Text zu rekonstruieren. Ferner war durch Peilung der jeweilige Senderstandort zu ermitteln und mit der Rufzeichenliste zu vergleichen, um die Schlüsselkreise zu identifizieren, deren Kenntnis zur Kryptanalyse wichtig war. Bei täglich bis zu mehreren Tausend abzuhörenden Funksendungen kann man sich die Größenordnung des erforderlichen Aufwands vorstellen.

Für den besonders wichtigen Fernschreib-Funkverkehr der deutschen Wehrmacht benötigte man speziell ausgerüstete Abhörstationen, die alle auf der britischen Insel errichtet wurden. Die erste davon war Knockholt, wo man die Telegraphie-Sendungen aufzeichnete mit Spezialgeräten (*undulator* = ein schneller Linienschreiber). Dessen Ausschläge markierten eine logische 1, die für jeden Kanal ausgewertet und auf Lochbänder zu übertragen waren. Fehler entstanden dabei vor allem durch Empfangsstörungen, aber auch Übertragungsfehler waren bei der großen Impulsmenge unvermeidbar, so daß man erst nach aufwendigen Vergleichsoperationen – ggf. auch mit anderen Stationen – und anschließenden Korrekturen Lochbänder anfertigen konnte, die für kryptanalytische Zwecke geeignet waren. Diese wurden dann nach BP zweifach über getrennte Leitungen geschickt, dort wieder verglichen und ggf. korrigiert: Man hatte aus der Anfangszeit gelernt, daß keine Buchstaben fehlen oder hinzu kommen durften, weil sonst der kryptanalytische Prozeß „außer Tritt“ fiel.[413]

Für diese aufwendigen Arbeiten benötigte man 600 Mitarbeiter in jeder Abhörstation.

[413] Vgl. General Report On Tunny: With Emphasis on Statistical Methods (1945), 31A.

6 Kryptanalytische Maschinen und Digitalelektronik

Die Grundlagen digital-elektronischer Maschinen, nämlich elektronische Logikschaltungen, untersuchte man bald nachdem dafür Schaltelemente – Elektronenröhren – verfügbar waren. Doch konnte man bereits Logikschaltungen realisieren – mit Relais, wie bspw. K. ZUSE in seinen Rechnern. Die theoretischen Grundlagen hierzu hatte 1938 der spätere Informationstheoretiker SHANNON in seiner Masterarbeit "*A Symbolic Analysis of Relay and Switching Circuits*" erarbeitet und gezeigt, daß sich Boole's Algebra zum Entwurf dieser Logikschaltungen eignet.[414]

Die vorhandenen technischen Möglichkeiten gestatteten jedoch scheinbar nicht die Realisierung betriebssicherer elektronischer Schaltungen, denn Elektronenröhren eigneten sich nur sehr eingeschränkt dafür, wie man glaubte. Vor allem hatte man deren technische Nutzbarkeit für digitale Anwendungen noch nicht erprobt und zweifelte dementsprechend an deren Zuverlässigkeit. Um dennoch betriebssichere Maschinen bauen zu können, blieb man bei der bewährten Relaistechnik, denn damit konnten digitale Schaltkonzepte ebenso realisiert werden. Überdies hatte man mit diesen Bauelementen jahrzehntelang Erfahrungen bei Bau und Betrieb von Telefonvermittlungen gesammelt, und für jeden Anwendungsfall standen geeignete Relais zur Verfügung.
Erst im Krieg bereitete die Langsamkeit der Relaisschaltungen Probleme, als bei einigen kryptanalytischen Maschinen die Arbeitsgeschwindigkeit nicht mehr ausreichte. Der Erfolgsdruck erzwang nun – trotz vieler Bedenken – die Verwendung von elektronischen Digitalschaltungen, obwohl es dafür keine erprobten Bauteile und Schaltungen gab. Erst diese Verwendung in kryptanalytischen Maschinen, und die dabei gemachten Erfahrungen, demonstrierte die Zuverlässigkeit der Elektronik unter Dauerbetrieb, was als Grundvoraussetzung zum Bau von elektronischen Rechnern anzusehen ist.

Mithin verlief die Entwicklung, ausgehend von Chiffriermaschinen, über deren Kryptanalyse zu kryptanalytischen Maschinen. Und deren Aufrüstung mit Digitalelektronik, für die erst noch betriebssichere Module zu entwickeln waren, bildete die Voraussetzung zum Bau von Rechnern; der erste vollelektronische Rechner entstand daher als kryptanalytische Maschine.

[414] Shannon, C. E., "A symbolic analysis of relay and switching circuits," Trans. AIEE, Vol. 57, 1938, p. 713-723.

6.1 Bauelemente für digitale Elektronik

Elektronische Schalter, welche die langsamen Relais ersetzen konnten, mußten erst entwickelt werden. Dabei zeigte sich, daß man nicht einfach die Relais durch Elektronenröhren ersetzen konnte, sondern deren sehr unterschiedliche technische Parameter spezielle Schaltungsentwürfe erforderten:

6.1.1 Vakuum-Röhren

Die Funk- und Radiotechnik hatte die Entwicklung von Vakuumröhren sehr gefördert, denn erst die Verbesserungen der Röhrentechnik ermöglichten bspw. den Durchbruch des Rundfunks in den 20er Jahren und die folgenden Fortschritte des Fernsehens. Dazu lieferte eine spezialisierte Industrie geeignete und preiswerte Vakuumröhren, als deren Qualitätsmerkmal eine möglichst lineare Kennlinie galt, die für die Analogtechnik wichtig war. Um die Herstellkosten niedrig zu halten, beachtete man weniger das Kriterium „Zuverlässigkeit“, denn es war kein Problem, eine ausgefallene Röhre zu erkennen: Entweder verstummte das Ausgangssignal, oder es wurde durch Rauschen ersetzt.

Einen weiteren, und wohl noch wichtigeren Grund dafür, daß Anfang der 30er Jahre Vakuumröhren als unzuverlässig galten und daher für größere Digitalschaltungen nicht in Betracht gezogen wurden, nennt der Computerhistoriker COPELAND: „Diese [vorerwähnte] Meinung bildete sich nach den Erfahrungen mit den vielen [analogen] Radioempfängern, die häufig aus- und eingeschaltet wurden.“[415] Genau diese Betriebsweise war der wichtigste Grund für die mangelhafte Zuverlässigkeit der Röhren, wie erst später die Erfahrungen mit Digitalelektronik in kryptanalytischen Maschinen zeigten.

So konnte man sich bis lange in den Zweiten Weltkrieg hinein nicht vorstellen, Schaltungen mit vielen Vakuumröhren zuverlässig betreiben zu können.
Erst recht galt das für elektronische Digitalschaltungen. Denn dort würden Röhrenausfälle ganz unterschiedliche Fehler verursachen, je nachdem, an welcher Stelle der Schaltung die Röhre arbeitete, und dementsprechend war es ungewiß, ob der Fehler gleich bemerkt werden würde. Man befürchtete im Extremfall stundenlanges Arbeiten einer Digitalschaltung ohne Fehlererkennung, und erst die dann falschen Rechenergebnisse würden den Fehler offenbaren. Schon aus diesem Grund könnten die Röhren der Analogtechnik nicht ohne weiteres für Digitalschaltungen verwendet werden, so die herrschende Meinung.

Erschwerend kam hinzu, daß Vakuumröhren systembedingt keine klar definierten Schaltzustände aufweisen: Der Stromfluß durch eine Röhre ist abhängig von der Gitterspannung, die Schwankungen unterliegen kann, etwa

[415] Copeland, Computer Age, S. 351.

durch Alterung der aktiven und passiven Bauteile, die Kennlinien änderten sich aus dem gleichen Grund, usw.[416]

In Logikschaltungen muß aber klar zwischen „Stromfluß“ (= logisch 1) und „kein Strom“ (= logisch 0) unterschieden werden. Das gewährleistete die bereits 1919 konzipierte FlipFlop-Schaltung (heute „bistabiler Multivibrator“) mit Vakuum-Trioden, deren Verwendung sich jedoch auf Experimente beschränkte, denn aus schaltungstechnischen Gründen (Streukapazitäten usw.) waren damit nur unzureichende Schaltgeschwindigkeiten zu erzielen. Erst nach Weiterentwicklung der Schaltung und Ergänzung durch einen „Kathodenfolger“ – einer dritten Röhre nach dem FlipFlop – eignete sich diese aufwendige Anordung für schnelle Logikschaltungen, und wurde erstmals in großer Zahl im ENIAC verwendet.[417] Bei dieser von der US-Army finanzierten Maschine spielte der Aufwand keine Rolle: Man entwickelte dafür spezielle Doppeltrioden, um mit je zwei Röhren pro Digit auszukommen, und benötigte dennoch für jede Zähldekade 20+4 Röhren, als Folge der Dezimalstruktur dieser Maschine.

6.1.2 Thyratron-Röhren

Die erwähnten Stabilitätsprobleme der Vakuumröhren haben gasgefüllte Röhren[418] nicht: Es gibt nur die Zustände ‚gesperrt‘ oder ‚gezündet‘, und sie wurden und werden daher als elektronische Leistungsschalter eingesetzt [und sind heute in der RADAR- und LASER-Technik unentbehrlich]. Nachdem diese Röhre einmal gezündet hat, kann sie durch das Gitter nicht mehr beeinflusst werden, d.h. der Zustand logisch 1 bleibt solange erhalten, bis gelöscht wird = logisch 0. Diese Eigenschaft ist für elektronische Speicher gut geeignet, besonders für Schieberegister.
Erstmals wurden Thyratronschaltungen 1931 von E.W. PHILLIPS[419] vorgeschlagen, und 1932 von WYNN-WILLIAMS in Zählschaltungen realisiert.[420]

Ebenfalls gasgefüllt sind Glimmlampen, die mit den Thyratronröhren verwechselt werden könnten, jedoch ein anderes Schaltverhalten aufweisen. Man verwendete sie in den 30er Jahren als Dioden; bspw. stabilisierte ZUSE’S Freund SCHREYER in seinen Experimentierschaltungen damit den Betrieb der Vakuumröhren (s. 6.2.2).

---

[416] Vgl. K. Zuse, Internetarchiv, Schaltungen bekannter Schaltmittel, Elektronenröhre als Relais.

[417] Vgl. Huskey, Harry D.: Hardware Components and Computer Design. In: Rojas, R./Hashagen, U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA und London, 2000, S. 72.

[418] Übliche Bezeichnungen: Thyratron, Stromtor (deutsch), gas filled tube, thyratron (USA), thermionic valve (engl.).

[419] Vgl. Naumann, F. in: Geschichte der Technikwissenschaften, S. 415.

[420] Deutsches Museum München, Abt. Rechentechnik und Informatik, Erläuterungen.

6.2 Versuchsschaltungen

Für die erwähnten Bauelemente gab es keine erprobte digitale Schaltungstechnik. Die wenigen Wissenschaftler bzw. Ingenieure, die sich damals Elektronik für digitale Anwendungen vorstellen konnten, mußten zunächst mit Versuchen die Grundlagen dieser Technik erarbeiten. Nachfolgend werden kurz die Leistungen der bedeutendsten Forscher angesprochen:

6.2.1 Thomas (Tommy) Flowers

Bild 42: erster Digitalelektroniker T. Flowers[421]

Thomas FLOWERS (1905-1998) lernte zunächst Mechaniker und studierte dann Elektrotechnik. Nach seiner Graduierung ging er zum britischen *General Post Office* (GPO) und arbeitete in dessen Forschungslabor Dollis Hill bei London an „....*experimental electronic solutions for long-distance telephone systems*“, und zwar bereits ab 1930.[422]

Mit Röhrenschaltungen zur Erzeugung und Speicherung von Impulsen wollte FLOWERS diese elektronischen Telefonvermittlungen bauen, denn er war nicht nur von der weit größeren Schaltgeschwindigkeit der Röhren überzeugt, sondern auch von deren geringer Abnutzung, die einen wirtschaftlichen Betrieb versprachen. [Zu dieser Zeit war er vermutlich der Erste, der die Brauchbarkeit größerer Röhrenschaltungen untersuchte]. Bereits 1934 hatte er eine automatische Telefonverteilung für 1000 Linien aufgebaut, die von 3000 – 4000 Röhren geschaltet wurde. Nach ausführlichen Versuchsprogrammen akzeptierte die Post das System und führte es 1939 in begrenztem Umfang ein. Als fernes Ziel wollte FLOWERS alle relaisbasierten Telefonschaltungen durch Elektronik ersetzen.

---

[421] Bild nach British Telecom (BT): People-Personalities – Tommy Flowers. Von:http://www.btplc.com/Corporateinformation/BTArchives/ImageGallery/People-Personalities/index.htm, am 25.9.03.

[422] BBC-Homepage: Tommy Flowers - Technical Innovator. Von: http://www.bbc.co.uk/dna/h2g2/A1010070, am 21.9.2003.

Nach Kriegsbeginn war er der einzige britische Fachmann – [wenn nicht der weltweit einzige] – , der wußte, wie Röhren in schnellen Digitalschaltungen [betriebssicher] anzuwenden waren.[423]
Diese Erfahrungen ermöglichten ihm 1943 Konstruktion und Bau des weltweit ersten elektronischen Großrechners, des COLOSSUS.[424]

6.2.2 Schreyer/Zuse

Der Computerpionier Konrad ZUSE (1910-1995) hatte bereits als Student 1938 einen mechanischen Rechner mit Elektroantrieb entwickelt, den Z1, den er bald durch das verbesserte und voll betriebsfähige Modell Z2 ersetzte. Doch erst sein relaisbasierter Rechner Z3 (1941) errang den Status des ersten digitalen Großrechners, der mit seinem Dualsystem seiner Zeit weit voraus war. Gegen Kriegsende hatte ZUSE auch eine leistungsstärkere Version Z4 fertiggestellt und die erste Programmiersprache entwickelt („Plankalkül"), die jedoch ein mehr theoretischer Beitrag war. Besonders erwähnenswert ist, daß ZUSE seine Geräte ohne jede öffentliche Unterstützung bauen mußte, die andere Computerpioniere erhielten.
Nach dem Krieg war ZUSES Z4 (in der ETH Zürich) der einzige betriebsfähige Großrechner in Europa und bis 1955 im Einsatz. In einer eigenen Firma entwickelte und produzierte ZUSE dann zahlreiche Rechner für die mittlere Datentechnik.
ZUSE wird gelegentlich genannt im Zusammenhang mit Kryptanalyse, weil er dafür eine elektronische Version seiner Z3 bauen wollte. Doch das war eine Legende: BAUER erläutert, wie diese entstand und in die seriöse Geschichtsschreibung (BURKE, RANDELL) Eingang fand.[425] Auch nach dem Krieg bildeten sich kryptologische Legenden um ZUSE, weil sich Kryptologen für seine Z22 interessiert haben sollen.

Die Erforschung elektronischer Digitalschaltungen in Deutschland begann ebenfalls mit dem Ziel, die Telefonvermittlungstechnik zu beschleunigen, analog zur erwähnten Entwicklung FLOWERS': ZUSE's Freund und gelegentlicher Helfer Helmut SCHREYER (1912-?) befaßte sich bereits während seines Studiums der Nachrichtentechnik mit Möglichkeiten, die Relais durch Vakuumröhren abzulösen. Die Zusammenarbeit mit ZUSE brachte ihn auf den Gedanken, die Relais in ZUSES Rechnern ebenso durch die schnellere Elektronik zu ersetzen. Er entwarf dazu Versuchsschaltungen und untersuchte in seiner Dissertation[426] die Möglichkeiten des Einsatzes in Rechnern: Man benötige dazu Schaltgeschwindigkeiten, die um „Größenordnungen über dem normalen Fernsprechrelais" liegen und die nur mit Elektronenröhren erreichbar sind. Doch

[423] Vgl. Copeland, Computer Age, S. 351-352.
[424] Zu Flowers herausragender Leistung bei Planung und Bau des COLOSSUS s. 6.3.2.
[425] Vgl. Bauer, Friedrich L.: Konrad Zuse – Fakten und Legenden. In: Rojas, R. (Hrsg.): Die Rechenmaschinen von Konrad Zuse, S. 18-19.
[426] Vgl. Schreyer, Helmut: Das Röhrenrelais und seine Schaltungstechnik. Diss. TH Berlin 1941.

diese sind wegen ihrer nicht eindeutigen Schaltzustände nicht ohne weiteres verwendbar. Besonders die immer verbleibenden Restspannungen können zu undefinierten Zuständen führen, wenn mehrere Röhren zusammengeschaltet werden.

SCHREYER diskutierte dann zwei Lösungen:

a) „Glimmrelais“ (nach GEFFKEN und RICHTER): Glimmlampen unterscheiden scharf zwischen leitend und nichtleitend. [Glimmlampen dienten damals als Dioden].

b) Thyratron (nach LANGMUIR und HULL): Ebenfalls scharf trennend, jedoch Nachteil der aktiven Löschung – Lichtbogen bleibt bestehen. [SCHREYER erkannte damals offenbar nicht den Vorteil dieser Eigenschaft, Speicher zu bilden, kam jedoch später in seiner Patentanmeldung darauf zurück – s. u.].

Eine Kombination Elektronenröhre-Glimmlampen, das erwähnte „Glimmrelais“, könnte die gewünschten Schaltvarianten erbringen. Mehrere Varianten prüfte SCHREYER meßtechnisch und diskutierte eine praktische Anwendung, eine „taktgesteuerte Relaiskette“, die heute als „Schieberegister“ zu bezeichnen wäre. Daraufhin sprach er die Verwendung für den Bau in Rechenmaschinen an und betonte, daß die schnelle Verarbeitungszeit nur dann lohnt, wenn von Hand einzustellende Eingangs- und Zwischenwerte nicht erforderlich sind. „Dies bedeuted ein vollautomatisches Rechengerät mit abzutastendem Rechenplan und Speicherwerk, welches bereits mit anderen Schaltmitteln in neuester Zeit entwickelt wurde.“[427]

Damit meinte er sicher ZUSE’S Z3, denn ZUSE berichtete in diesem Zusammenhang nach dem Krieg: „[...] wurden elektronische Bauelemente entwickelt, die von vornherein für Rechenmaschinen zugeschnitten waren.“[428]
SCHREYER entwickelte neben seiner Berufstätigkeit ein Muster in Zusammenarbeit mit ZUSE, der es in seiner Z4 verwenden wollte, und erhielt dafür am 11.6.1943 ein Patent[429] für ein „Elektrisches Kombinations-Speicherwerk“ zuerkannt. Das Versuchsmuster, „ein zehnstelliges duales Rechenwerk mit ca. 100 Röhren“, ging auf der Flucht bei Kriegsende verloren.[430]

ZUSE und SCHREYER versuchten 1942 vom Heeres-Waffenamt Unterstützung für die Entwicklung eines elektronischen Rechners zu erhalten, wurden jedoch von den Militärs abgewiesen, da angeblich dessen Entwicklung zu lange dauern

[427] Vgl. Schreyer, Helmut: Das Röhrenrelais und seine Schaltungstechnik.
[428] Zuse,K.: Entwicklungslinien einer Rechengeräte-Entwicklung von der Mechanik zur Elektronik. Von: Konrad Zuse-Internetarchiv, URL: http://www.zib.de/zuse/index.html, am 25.3.02.
[429] Patentschrift Nr. 937170, Deutsches Patentamt, angemeldet 19.11.1940, patentiert 11. Juni 1943, ausgegeben am 29. Dezember 1955.
[430] Zuse,K.: Entwicklungslinien einer RechengeräteEntwicklung von der Mechanik zur Elektronik. Von: Konrad ZuseInternetarchiv, URL: http://www.zib.de/zuse/index.html, am 25.3.02.

würde. Sie gingen daraufhin zur Deutschen Versuchsanstalt für Luftfahrt (DVL), deren Wissenschaftler die Bedeutung der geplanten Maschine erkannten, jedoch nur eingeschränkt behilflich sein konnten. Immerhin baute SCHREYER mit Hilfe der DVL ein erstes Versuchsmodell, das jedoch Ende 1943 nach einem Bombenschaden nicht mehr verwendungsfähig war. Es wurde zwar noch repariert, zu weiteren Experimenten kam es wegen Verlagerung des Instituts und baldigem Kriegsende nicht mehr.[431]

SCHREYER emigrierte nach dem Krieg, wurde in Brasilien Professor für Fernmeldetechnik und befaßte sich nicht mehr damit. Doch anläßlich eines Besuchs bei ZUSE in 1977 schrieb er darüber einen ausführlichen Bericht, und erwähnte u.a.: „Verwendet wurden sogenannte Thyratron-Speicherelemente, wie sie auch in dem jetzt bekannt gewordenen Colossus-Computer in England während des Krieges angewandt wurden.“ [432]
Weiter schrieb er: „Ich hatte damals keine Möglichkeit, wegen der Kriegsumstände mich über ausländische Entwicklungen zu informieren, und mußte daher zu meinem Erstaunen später feststellen, daß die Schaltungen von Computern mit Röhren meinen Schaltungen doch sehr ähnlich waren. Es ist daher interessant, auch hier festzustellen, daß derartige Entwicklungen mitunter ‚in der Luft liegen', wie es ja bei anderen Erfindungen z.B. von Telefon und Elektronenröhre auch der Fall war.“[433]

6.2.3 Wynn-Williams

Der Physiker WYNN-WILLIAMS hatte erstmals 1932 Thyratronröhren in Zählschaltungen verwendet[434], die er an der Universität Cambridge benötigte für Messungen an schnellen subatomaren Teilchen. Er arbeitete später am geheimen *Telecommunikations Research Establishment* (TRE) in Malvern, entwickelte dort u.a. das HF/DF-Gerät zur automatischen U-Boot-Peilung, bis er nach BP versetzt wurde.

Die von WYNN-WILLIAMS bereits in Cambridge gebauten digitalen Zähleinrichtungen wurden später in der kryptanalytischen Maschine HEATH ROBINSON verwendet, und auch für deren elektronische Variante SUPER ROBINSON (s.u.). Hierzu entwickelte WYNN-WILLIAMS eine elegante Methode, die Boole'sche Logikfunktion XOR durch Phasenwechsel zu realisieren (s. 6.3.1).
WYNN-WILLIAMS zeichnete sich als Forscher und Entwickler aus, hatte aber keinen Bezug zur praktischen Realisierung seiner Ergebnisse in betriebssicheren Maschinen.

---

[431] Vgl. Schreyer, Helmut: Das Röhrenrelais und seine Schaltungstechnik, S. 7.
[432] Vgl. Schreyer, H.: Entwicklung eines Versuchsmodells einer elektronischen Rechenmaschine, S. 8. Bericht vom 1.8.77.
Von: Konrad ZuseInternetarchiv, URL: http://www.zib.de/zuse/index.html, am 25.3.02.
[433] Vgl. Ebd., S. 13-14.
[434] Deutsches Museum München, Abt. Rechentechnik und Informatik, Erläuterungen.

6.2.4 Atanasoff/Berry

Der Mathematiker ATANASOFF (1903-1995) konstruierte an der Universität Iowa einen für die damalige Zeit neuartigen Rechner für die Lösung von Differentialgleichungen, den ab 1940 der technisch begabte Absolvent BERRY baute.[435] Er enthielt u.a. erstmalig einen elektronischen Speicher, und arbeitete digital mit 300 Röhren.
Das Gerät konnte nicht fertiggestellt werden, weil ATANASOFF 1942 für kriegswichtige Entwicklungsarbeiten dienstverpflichtet wurde.

Für den hier betrachteten Zusammenhang ist wesentlich, daß der „Atanasoff-Berry-Computer" (ABC), so dessen Bezeichnung in der Literatur, nur ein Versuchsgerät war, von dem vermutlich einzelne Module kurzzeitig betrieben wurden. In der Literatur wird bezweifelt, ob es überhaupt als Ganzes betriebsfähig war.[436] Festzuhalten bleibt, daß mit diesem Gerät keine Erfahrungen zur Betriebssicherheit elektronischer Logikschaltungen gesammelt wurden.

6.3 Erste betriebssichere Großgeräte

Wie bereits erwähnt, war die Betriebssicherheit elektronischer Digitalschaltungen das entscheidende Kriterium für die Verwendung in elektronischen Logiksystemen. Man konnte sich scheinbar nicht vorstellen, unter realen Betriebsbedingungen einen Dauerbetrieb einzurichten, denn die Erfahrungen aus der Analogtechnik sprachen dagegen.
Eine Ausnahme stellte FLOWERS elektronische Telefonvermittlung dar, welche die britische Post 1939 erstmals einführte (s. 6.2.1), aber nicht publik machte. Die Erfahrungen mit diesem System, wo erstmals Relais durch Röhrengroßschaltungen abgelöst wurden, ermöglichten FLOWERS u. a. den Bau des COLOSSUS.
Die nachfolgend beschriebenen Geräte waren die ersten Exemplare elektronischer bzw. teilelektronischer Maschinen, die sich im Dauerbetrieb bewährten.

6.3.1 SUPER-ROBINSON

Diese teilelektronische kryptanalytische Maschine wird in der Literatur gelegentlich verwechselt mit dem COLOSSUS, dessen Vorläufer sie war. Sie unterschied sich vom elektromechanischen Vorgängergerät HEATH ROBINSON, beschrieben unter 5.3.2 „Robinson-Maschinen", nur durch eine elektronische Logikschaltung, welche die Arbeitsgeschwindigkeit steigern sollte: Nach SALE[437]

[435] Vgl. Gustafson, John: Reconstruktion of the Atanasoff-Berry-Computer. In: Rojas, R./Hashagen, U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA, London, 2000, S. 91-93.
[436] Vgl. Gustafson, John: Reconstruktion of the Atanasoff-Berry-Computer, S. 102. Gustafson bejaht das und nennt einige wahrscheinliche Anwendungen.
[437] Vgl. Sale, Codes and Ciphers: The rebuild of Heath Robinson, page 4.

schlug WYNN-WILLIAMS vor, das XORing – bisher langsame Relaislogik – elektronisch elegant nachzubilden durch den Phasenwechsel einer Generatorschwingung: Logisch 0 entsprach 0°, logisch 1 entsprechend 180°. Bei XOR 1 + 1 = 0 wurde daher 2× die Phase gedreht, also 2 × 180° = 0°, womit man das gewünschte Resultat erzielte.

Damit konnte man zwar die Verarbeitungsgeschwindigkeit steigern, jedoch erbrachten die Geräte dennoch nicht die geforderte Leistung: Es blieben die mechanischen Probleme des HEATH ROBINSON, nämlich Bandrisse und Synchronisationsfehler durch unterschiedliche Bänderdehnung.

6.3.2 COLOSSUS

In London interessierte man sich nicht für diese technischen Probleme, sondern verlangte immer dringlicher SZ42-Entzifferungen wegen der strategischen Bedeutung dieser Informationen. Bei einer Besprechung darüber schlug nun TURING vor, es doch einmal mit Tommy FLOWERS zu versuchen, dessen technische Kompetenz er bei verschiedenen Gelegenheiten kennengelernt hatte. Daraufhin wurde FLOWERS beauftragt, die ROBINSON-Maschinen für eine ausreichende Leistung umzurüsten. Doch FLOWERS erkannte bald die Undurchführbarkeit dieser Vorgabe, weil das Synchronisationsproblem der zwei parallel laufenden Lochbänder unlösbar erschien.
Er schlug stattdessen eine komplett neue Maschine vor, vollelektronisch arbeitend und mit nur einem Band zur Eingabe, um Synchronisationsfehler von vornherein auszuschließen – den später so genannten COLOSSUS. Für dessen Realisierung rechnete er mit ca. 2000 Röhren für die gesamte Elektronik, doch das galt in BP (und sonst überall) wegen der zu erwartenden Unzuverlässigkeit als nicht akzeptabel: Schon der Ausfall einer einzelnen Röhre konnte zu großen Rechenfehlern führen, und überdies würde man das bei digitalen Logikschaltungen kaum sofort bemerken, so der damalige Wissensstand. Doch FLOWERS verwies auf seine elektronischen Telefonzentralen und kommentierte das später: „...ich hatte vor dem Krieg sehr viele Röhren in Telefonschaltungen eingebaut, und ich wußte, daß sie, wenn sie nie bewegt und ausgeschaltet wurden, ewig hielten.“[438]

Doch dieser Hinweis auf seine guten Erfahrungen nützte nichts, die Fachleute lehnten das Projekt ab. FLOWERS konnte als einzigen nur den zuständigen Abteilungsleiter Max NEWMAN überzeugen, der daraufhin entschied, zunächst weiter ROBINSON-Geräte bauen zu lassen, aber FLOWERS die Realisierung seiner Idee zu ermöglichen. FLOWERS konnte dann nicht einmal Testschaltungen aufbauen, um seine Ideen für den geplanten Rechner zu prüfen, denn der kriegsbedingte Zeit- und Erfolgsdruck zwang ihn, sofort mit der Konstruktion zu beginnen. Doch am 8. Dezember 1943, nach nur 9 Monaten Planungs-, Bau- und

[438] Zit. nach Vgl. Smith, Michael: Enigma entschlüsselt, S. 232.

Montagezeit, konnte der Rechner in Betrieb genommen werden und arbeitete zuverlässig. Dieser erste elektronische Großrechner COLOSSUS war nach COPELAND'S Darstellung gänzlich FLOWERS Werk.[439]

Diese in der Literatur übliche Darstellung muß man fairerweise um NEWMAN'S Beitrag ergänzen: Er formulierte nicht nur die Algorithmen, die in die Maschine zu implementieren waren, sondern ohne seine mutige Entscheidung gegen die Experten wäre COLOSSUS nie gebaut worden.

Bild 43: Max Newman[440]

Max NEWMAN (1897-1984) lehrte von 1927-1945 als Professor für Mathematik an der Universität Cambridge, war dort auch TURING'S Lehrer, und wurde 1942 nach BP dienstverpflichtet. Nach dem Krieg leitete er den Fachbereich Mathematik an der Universität Manchester, wo er u.a. ein Computerlabor einrichtete und die Entwicklung des Computers Manchester Mark 1 organisierte (s. dazu 7.3.1).

Für NEWMAN'S Entscheidung, die riskante Entwicklung des COLOSSUS zu unterstützen, wird vermutlich FLOWERS Idee zur Synchronisation ausschlaggebend gewesen sein. Denn die Synchronisationsprobleme zwischen den beiden Lochbändern (für Geheimtext und Schlüsselstrom) machten den Betrieb der ROBINSON-Maschinen ineffektiv, wie unter 5.3.2 „Robinson-Maschinen" dargelegt wurde. Dementsprechend bescheiden waren die SZ42-Entzifferungsergebnisse, und dafür war NEWMAN verantwortlich. Daher mußte für eine leistungsstarke Maschine der Synchronlauf sichergestellt werden, eine Bedingung, deren Einhaltung erst den Bau der Maschine rechtfertigte. Und hierfür fand FLOWERS eine elegante, wenn nicht geniale Lösung: Er ersetzte die Synchronisierung durch eine Taktsteuerung, damals eine völlig neue Idee, die u.a. die elektronische Speicherung des Schlüsselalgorithmus voraussetzte (s.u.). Dazu wurde das Geheimtextband mit 5.000 Ziffern/sec fotoelektrisch gelesen, und dessen Transportlochung steuerte als Taktgeber das gesamte System; die Maschine paßte sich damit automatisch der jeweiligen Bandgeschwindigkeit an.

[439] Vgl. Copeland, Computer Age, S. 360-361.
[440] Bild nach Sale, Tony: Codes and Ciphers in the Second World War.

Die Verarbeitung von binären Schlüsselströmen setzte freilich ein binäres System voraus. Das war damals ebenfalls nicht selbstverständlich, obwohl es bereits Versuchsschaltungen gab, von denen FLOWERS jedoch nichts wissen konnte, ebenso nicht von ZUSE'S binären elektromechanischen Rechenschaltungen.

Den Speicher für die fünf Kanäle des Baudot-Codes entwarf FLOWERS als fünffaches Schieberegister mit Thyratronröhren, es war also kein RAM nach heutigen Begriffen und auch kein Programmspeicher, wie verschiedentlich behauptet wird. Er war speziell für den kryptanalytischen Vergleichsprozeß optimiert, denn mit ihm erzeugte die Maschine einen Schlüsselstrom entsprechend dem SZ42-Algorithmus. Diese Bitfolge verglich die Maschine per Boole'scher Logik mit dem im Gleichtakt eingelesenen Geheimtext nach kryptanalytischen Kriterien. Dabei gefundene Übereinstimmungen wurden gezählt und die Ergebnisse zwischengespeichert. Diese Speicher und die Vergleicher- und Zählerlogik konnten bei Bedarf schnell umprogrammiert werden, wofür ein Steckerfeld und zahlreiche Schalter vorgesehen waren.[441]

Eine weitere, damals ebenso neue Entwicklung bleibt noch zu erwähnen: Die fünf Baudot-Kanäle verarbeitete die Maschine parallel, im Gegensatz bspw. zur von Kollegen gebauten Tunny-Maschine, die nur langsamen seriellen Betrieb gestattete.

Schließlich löste FLOWERS ein letztes und wohl entscheidendes Problem: Den *störungsfreien* Betrieb einer Anlage mit 1500 Röhren (später 2500 bei COLOSSUS II) zu gewährleisten, was damals als unrealisierbar galt. Er erreichte das durch Herabsetzung der Röhrenleistung auf ca. 30% (für Logikschaltungen völlig ausreichend) und Dauerbetrieb bei konstanten Temperaturverhältnissen. So konnten auch handelsübliche Röhren verwendet werden.

[441] Vgl. General Report on Tunny, 53L (b).

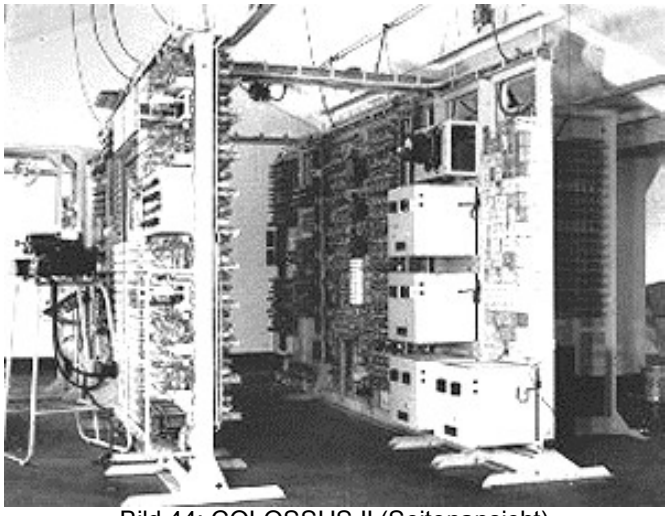


Bild 44: COLOSSUS II (Seitenansicht)

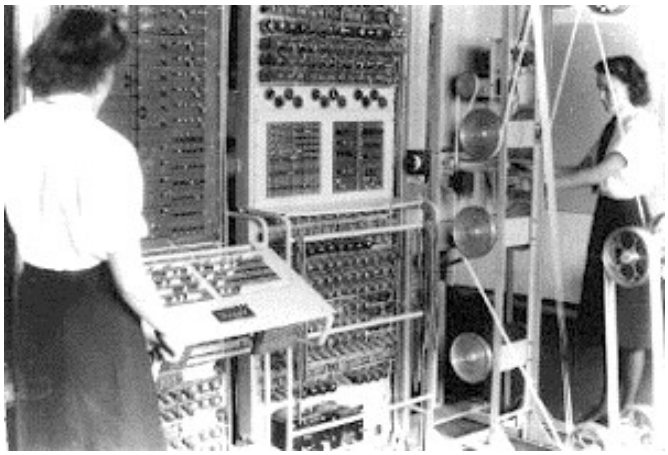


Bild 45: COLOSSUS II im Einsatz[442]

Leistung und Betriebssicherheit des COLOSSUS übertrafen die Erwartungen. In der Weiterentwicklung COLOSSUS II konnten zusätzlich bedingte Sprungbefehle und Verzweigungen geschaltet werden, weil manche Verbesserungen der SZ42 (Klartextfunktionen, s. 4.4 – "Varianten") das erforderten. Mit den nach und nach installierten zehn COLOSSI II konnte BP die Schlüsseleinstellungen (*wheel setting*) der SZ42-Maschinen meist innerhalb weniger Stunden ermitteln. Diese Ergebnisse verwertete man anschließend zur Programmierung der *TUNNY-machine*, die den Klartext erzeugte – überwiegend längere Texte der Kommunikation der obersten Führungsebene der Wehrmacht.
Ob COLOSSUS auch für andere Aufgaben eingesetzt wurde, ist nicht bekannt.
Die Verdienste FLOWERS und seines kleinen Teams werden in der Literatur immer noch unterbewertet, manchmal überhaupt nicht erwähnt. Der Grund dafür: COLOSSUS stand – wie alle ULTRA-Informationen – unter striktem Geheimschutz bis 1974, sogar die bloße Existenz der Maschine wurde geleugnet. Auch danach wurden nur allmählich technische Einzelheiten bekannt. Das aber

[442] Bilder nach Imperial War Museum London, Online Exhibition: ENIGMA and the codebreakers,COLOSSUS.

ermöglichte den US-Amerikanern, den Beginn des Informatikzeitalters (*birth of information age*) der erst 1946 erfolgten offiziellen Inbetriebnahme des Großrechners ENIAC zuzuschreiben, obwohl die Maschine damals schon veraltet war (s. 7.2.1).
FLOWERS hingegen baute, beginnend mit der Idee, über die Konstruktion bis zur erfolgreichen Inbetriebnahme 1943 in nur 9 Monaten eine damals völlig neuartige Maschine, was allein schon eine hervorragende Ingenieurleistung war. Überdies gab es für deren wesentlichen Elemente keine Vorbilder oder Erfahrungen, und deren Architektur umfaßte bereits Binärsystem und Parallelbetrieb. Vor allem bewies er damit bereits 1943 die Machbarkeit einer großen vollelektronischen Rechenmaschine, *die im Dauerbetrieb zuverlässig arbeitete.*

6.3.3 Teilelektronische US-BOMBE

Die Leitung des US-Navy-Dienstes war frustriert, weil die Briten bisher nur die nötigsten Informationen aus der ENIGMA-Entzifferung mitteilten, [obwohl US-Schiffe die Hauptlast der alliierten Konvoisicherung im Atlantik zu tragen hatten]. Nach der Einführung der ENIGMA M4 gelang es den Briten zudem nicht, rechtzeitig genügend leistungsfähige BOMBE-Maschinen zu bauen. Man beschloß daher eigene 4-Rotoren-Maschinen zu entwickeln, die besonders schnell arbeiten und daher mit Elektronik ausgerüstet werden sollten.[443]
Gleichwohl war man mangels eigener Erfahrung auf umfassende britische Hilfe angewiesen, die man nach dem Travis-Wenger-Abkommen (s. 7.1) auch erhielt, denn im Atlantikkrieg war Großbritannien auf US-Unterstützung angewiesen.
Im September 1942 übernahm Joseph DESCH (1907-1987) von der Firma NCR diese Aufgabe; er wurde dazu berufen, weil er Erfahrungen in der Entwicklung von schnellen elektronischen Zählschaltungen gesammelt hatte, die für das Projekt vorgesehen waren. Die ursprüngliche Navy-Vorgabe einer vollelektronischen Maschine verwarf DESCH, da er dazu ca. 20.000 Röhren für erforderlich hielt, was damals als unmöglich zu betreiben galt. Er plante die Übernahme der britischen Rotoren-Mechanik zu kombinieren mit schnellen elektronischen Zählern und Vergleichern, aufgebaut aus ca. 1500 Thyratrons und Vakuum-Röhren.[444]
Folgt man einem Interview[445] mit DESCH'S Freund und Kollegen MUMMA, war TURING in die Konstruktion der Maschine wesentlich mehr eingebunden, als bisher bekannt. So berichtet MUMMA u.a. über die lange Zusammenarbeit mit TURING, der wie kein anderer bereits in der Planungsphase das Projekt kontrollierte und entsprechende Vorgaben machte. TURING wußte immer genau,

---

[443] Vgl. Lee/Burke/Anderson: The US Bombes. NCR, Joseph Desch, and 600 WAVES. In: IEEE Annals of the History of Computing, July–September 2000, S. 56.
Von: http://frode.home.cern.ch/frode/crypto/USBombe/index.html, am 28.04.02.

[444] Vgl. Ebd., S. 5.

[445] Mumma, Robert: Oral history, conducted in 15.9.1995 by Frederik Nebeker. In: IEEE History Center, Rutgers University, New Brunswick, NJ/USA. Von: www.ieee.org/organizations/history_center/oral_histories/transcripts/mumma.html, am 9.11.02.

was zu tun war, und alle anderen waren nicht in der Lage, mit ihm ernsthaft darüber zu diskutieren.
Das widerspricht der offiziösen Darstellung, wonach TURING nur den Entwurf geprüft habe, und dessen negatives Ergebnis DESCH nicht mitgeteilt wurde.[446]
Es ist jedoch sehr unwahrscheinlich, daß der Amerikaner MUMMA die intensive Mitarbeit TURINGS an diesem Projekt „erfunden" hat – womöglich wollte man TURINGS maßgebliche Leistung aus „patriotischen" Gründen minimieren?

TURING hatte in seinem Bericht besonders Bedenken gegen Teile der Mechanik geäußert. Zu Recht, wie sich zeigte, als diese Schwierigkeiten eine mehrmonatliche Verzögerung des Projekts bewirkten und es fast zum Scheitern brachten. DESCH gab aber nicht auf, und ab Dezember 1943 überzeugten die Maschinen durch Leistung.[447]

Einen wesentlichen Unterschied zur britischen BOMBE-Konstruktion gab es: Eine elektronische Steuer- und Speicherschaltung mit ca. 1500 Thyratrons hielt die Stellungen der Rotoren dann fest, wenn die gemäß *crib*-Vorgabe richtige Rotorstellung durchgeschaltet hatte, d.h. die zum jeweiligen *crib* passende ENIGMA-Einstellung gefunden war. So konnte die Maschine allmählich auslaufen und wurde dadurch weit weniger mechanisch belastet als die speicherlose britische Version: Denn diese mußte beim Durchschalten sofort gestoppt werden, um die gefundene Einstellung ablesen zu können. Das erforderte aus mechanischen Gründen einen wesentlich langsameren Lauf.
Die zur Entzifferung unentbehrlichen *cribs* lieferte im Übrigen BP über eine sichere Fernschreiber-Übertragung [vermutlich ROCKEX].[448]

[446] Vgl. Erskine/Marks/Weierud (Ed.): Turing's Report on His Visit to NCR. (Die Navy befürchtete, daß Desch das Projekt niederlegt und soll ihm Turings Bericht vorenthalten haben).
[447] Vgl. Erskine, Ralph: Breaking German Naval Enigma. In: Erskine/Smith, Action, S. 190-192.
[448] Vgl. Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", Aug. 1943.

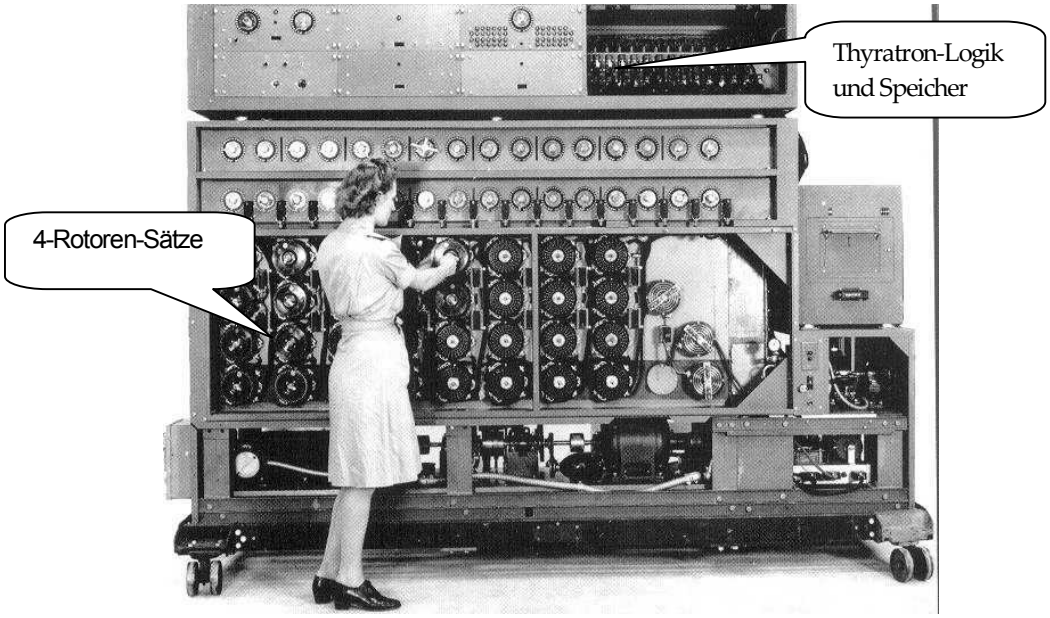


Bild 46: Desch-US-BOMBE[449]

In der Spätphase des Krieges konnte überraschend nicht mehr entziffert werden: Die deutsche Marine hatte zum November 1944 für jedes U-Boot individuelle Schlüssel („Sonderschlüssel“) befohlen, und die nun fehlenden *cribs* machten die BOMBE-Maschinen unbrauchbar. Aber nur vorübergehend, denn diese scheinbar besonders raffinierte Erschwernis erwies sich bald als Illusion: Die nun zahlreichen Schlüsselkreise hatten zur Folge, daß Sammelinformationen entsprechend mehrfach gesendet werden mußten, wortgleich natürlich, und so BP per Geheimtext-Geheimtext-Kompromittierungen wieder *cribs* erarbeiten konnte. Das aber hätten individuelle bzw. jeweils abgeänderte Texte verhindert, doch diese Einsicht war von den Nachrichtenoffizieren mangels kryptologischer Kompetenz nicht zu erwarten.

Gleichwohl konnten die Alliierten nicht mehr regelmäßig entziffern, bspw. bei Mangel an Sammelsendungen. Dieses Problem konnte überwunden werden, als eine neue kryptanalytische Maschine mit der Tarnbezeichnung FILIBUSTER zur Verfügung stand, deren Aufbau und Funktion bis heute geheim gehalten wird.[450]

6.3.4 COBRA-Bombe in Bletchley Park

Die parallel zur US-BOMBE entwickelte britische 4-Rotor-Maschine, genannt COBRA, leistete bedeutend weniger als diese. Zwar wurden 25 Maschinen gebaut und installiert, jedoch wegen ungenügender Leistungen wenig genutzt, und überdies scheiterten geplante konstruktive Verbesserungen an der fehlenden

[449] Bild nach: Crypto Machine Menu Page, BOMBE (NCR).
[450] Vgl. Erskine, Ralph: Breaking German Naval Enigma. In: Erskine/Smith, Action , S. 195-196.

Realisierbarkeit. Dementsprechend übertrug man die Entzifferungsarbeit für die U-Boot-Schlüsselnetze Ende 1943 dem OP-20-G, nachdem dort bereits 75 leistungsstarke Desch-BOMBS installiert waren.[451]

Die Ursachen für die mangelhaften Leistungen dieser Maschine sind nicht bekannt. Sie sind auch nicht verständlich, da ja der gleiche Wissensstand beiderseits des Atlantiks eine annähernd gleiche Konstruktion vermuten läßt, ausgenommen die Steuer- und Speicherelektronik. Allerdings war TURING nicht an der COBRA-Konstruktion beteiligt, da er sich zu dieser Zeit in den USA aufhielt.

6.3.5 SUPERSCRITCHER

Die unter 5.2.4 beschriebenen AUTOSCRITCHER waren Relaismaschinen, die systembedingt langsam arbeiteten, und daher Anfang 1946 durch funktionsgleiche, aber schnellere elektronische SUPERSCRITCHER abgelöst wurden. Diese Maschinen arbeiteten vollständig digital und waren dazu mit ca. 3500 Röhren ausgerüstet. Nach CRAWFORD wurden sie gegen „*enigma-type machines*“ zur Entzifferung eingesetzt, sollten aber auch den Nutzen der elektronischen Digitaltechnik demonstrieren. Es stellte sich jedoch heraus, daß dazu flexiblere Architekturen nötig wären, um mehr als dieses spezielle Problem [ENIGMA-Entzifferungen nach dem Krieg] lösen zu können.[452]

Immer noch geheim bleiben Informationen über die installierten elektronischen Logikschaltungen und deren Architektur.

[451] Vgl. Erskine, Ralph: Breaking German Naval Enigma. In: Erskine/Smith, Action. S. 190-192.

[452] Vgl. Crawford, David J.: The Autoscritcher and the Superscritcher, in: IEEE Annals of the History of Computing, July-September 1992, Vol. 14, No. 3, pp. 922.

6.4 Elektronische Sprachtarnung (Kryptophonie)

Schon bald nach der Einführung des Telefons verspürte man wohl das Bedürfnis, Gespräche vertraulich führen und heimliche Mithörer aussperren zu können. Dementsprechend machten sich Erfinder Gedanken und bereits im Dezember 1881 gab es das erste Patent für eine solche Vorrichtung.[453] Doch erst ab den 20er Jahren des vergangenen Jahrhunderts konnten man dafür brauchbare Schaltungen entwickeln, mit den inzwischen verfügbaren Elektronenröhren. Und es gab nun auch einen „Markt" und zahlungskräftige Interessenten dafür: Die Fortschritte der Funktechnik ermöglichten inzwischen transatlantische Funktelefongespräche, die aber jedermann abhören konnte. Gleichwohl war das Interesse dafür groß, denn Überseegespräche konnten nur per Funk geführt werden, weil die technischen Parameter der damaligen Seekabel (zu starke Dämpfung im Bereich der Sprachfrequenzen) Telefonie nicht zuließen. Allerdings begrenzte die Mithörbarkeit das Geschäft der privaten US-Telefongesellschaften, und daher suchten sie nach Möglichkeiten, das Mithören zu unterbinden. Freilich hatten ebenso Diplomaten und Militärs großes Interesse für solche Verfahren, für die heute die Bezeichnung Kryptophonie bzw. *cyphony* gebräuchlich ist. Deren Entwicklung führte zu Sprachcodierungen, die zur Grundlage des heutigen digitalen Telefonnetzes und des Mobilfunks wurden.

6.4.1 Analoge Verfahren

Die ersten funktionsfähigen Anlagen arbeitete mit der damals verfügbaren analogen Technik, und verschleierten die Sprachinformation mit Röhren-schaltungen der Radiotechnik. Doch die ersten unausgereiften Geräte erschwerten wohl eher die Verständigung der Anrufer, als unbefugte Lauscher auszuschließen. Gleichwohl setzten sich diese Verfahren durch, die Illusion der Abhörsicherheit scheint damals schon sehr verbreitet gewesen zu sein, denn die Telefongesellschaften warben damit. Diese als *scrambler* bezeichneten Geräte tarnten das Gesprochene mit zwei Varianten: Im ersten Fall zerteilte das Gerät die Sprachinformation in zeitgleiche Blöcke und veränderte deren Reihenfolge. In der Gegenstelle setzte ein Gerät nach dem gleichen Schema diese Sprachblöcke wieder zusammen. Im anderen Fall veränderten die Geräte die Sprachfrequenzen durch Invertierung, die in der Gegenstelle wieder aufgehoben wurde.
Doch beide Verfahren wurden sehr bald durch Amateurfunker kompromittiert, die passende Gegengeräte bastelten, sog. *de-scrambler,* und an Interessierte verkauften, die mithören wollten. Um dennoch ihr Geschäft zu sichern, ließen die Telefon-Gesellschaften verbesserte Geräte entwickeln, die beide Varianten kombinierten.[454]

[453] Vgl. Kahn, Codebreakers, S. 551.
[454] Ebd. , S. 554.

Bell-A3-Verfahren

Das am weitesten fortgeschrittene System dieser Bauart, der *Bell-A3-inverter* der American Telegraph & Telefon Company (AT&T), entwickelten die Bell-Laboratorien (*Bell labs*), der Forschungsbetrieb von AT&T. („A3" ist die international übliche Bezeichnung für tonmodulierte Sendeverfahren, mit denen diese Geräte arbeiten).

Mit diesem analogen Verfahren wurde die Tonfrequenz in 6 Bereiche zerlegt, dann verwürfelt und in der Frequenz invertiert, mit jeweils wechselnden Einstellungen während des Gesprächs. In der Gegenstelle wurde dieses rückgängig gemacht:

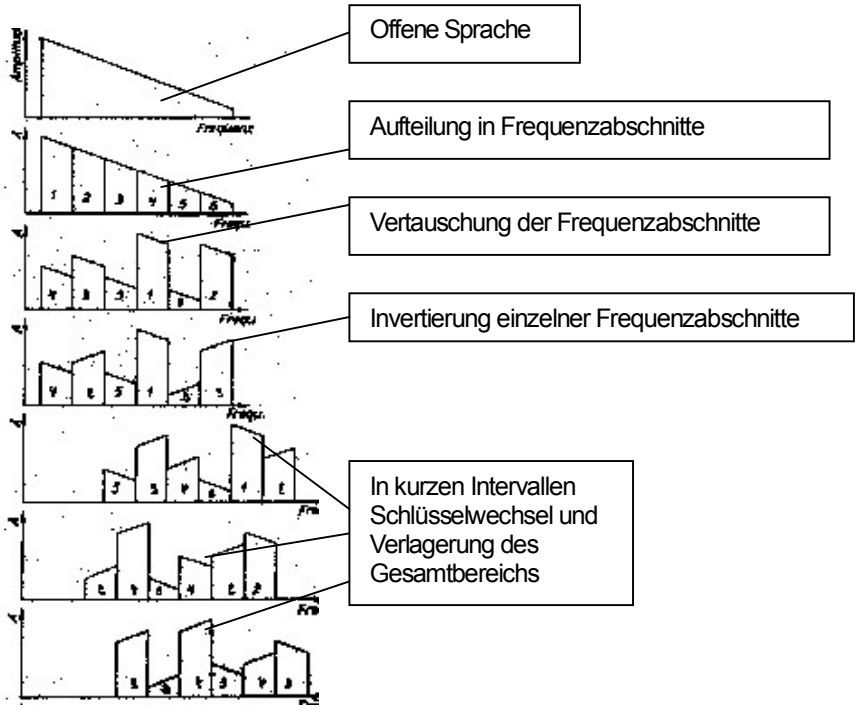


Bild 47: Verschlüsselungsphasen des Bell-A3-scramblers[455]

Mit dem Bell-A3-System sicherte die US-Diplomatie erstmals eine Telefonverbindung, und zwar ab Dezember 1937 die Linie San Francisco-Honolulu, der bald weitere folgten. Sie wurden besonders gern von US-Präsident ROOSEVELT genutzt, der sehr häufig mit diplomatischen Dienststellen telefonierte, weil er Schriftwechsel nicht schätzte. Das galt erst recht für seine intensive Kommunikation mit CHURCHILL nach Kriegsbeginn, die durch ein Bell-A3-System mit zusätzlichen, d.h. häufigeren Frequenzwechseln besser gesichert war. [456]

[455] Bild nach Gellermann, ... und lauschten für Hitler, S. 286.
[456] Vgl. Kahn, Codebreakers, S. 555.

Gleichwohl gelang es dieses System zu brechen: Kurt VETTERLEIN von der „Forschungsstelle“ der Reichspost-Forschungsanstalt[457] entwickelte nach Stimm- und Frequenzanalysen Geräte, die eine direkte Rückgewinnung der Sprachsignale ab September 1941 ermöglichten. In einer eigens dafür errichteten Abhör- und Auswertestation wurden viele Bell-A3-Funkgespräche rekonstruiert und aufgezeichnet. Die Abhörprotokolle gingen dann über das SS-Reichssicherheitshauptamt direkt an HITLER.[458]

Versuche in den *Bell labs* zeigten nach KAHN eine Schwäche des analogen Verfahrens, wonach man nach mehrfachen wiederholten Hören angeblich fast die Hälfte der gescrambelten Konversation dennoch verstehen konnte; trainierte Versuchshörer sollen sogar noch mehr verstanden haben. Daraufhin untersuchte man die Fähigkeiten des menschlichen Gehörs und kam zum Ergebnis, daß jedwede analogen Verfahren nach intensiven Hörtraining mindestens teilweise abhörbar sind.[459]
Dagegen wäre einzuwenden, daß die Abhörbarkeit begrenzt wird von Art und Häufigkeit der jeweiligen Wechsel, d.h. ab einem bestimmten Wert kann auch das beste Gehör nicht mehr folgen bzw. akustische Informationen rekonstruieren. Insoweit muß man die Angaben KAHN'S zumindest für das Bell-A3-Verfahren in Frage stellen und annehmen, daß es nur durch geeignete Geräte abhörbar war.

Deutsche Geräte zur Sprachtarnung

Das Gerät „Kleiner Leitungsverzerrer GK III“ von Siemens & Halske, ein Gerät auf dem technischen Stand der 20er Jahre, scheint häufig verwendet worden zu sein, vermutlich weil es ein besseres nicht gab: Nicht nur militärische Stellen setzten es ein, auch „allgemeine Verwendung“ in Dienststellen der Polizei, der NSdAP und des Staates werden genannt.[460] Es wurde in die Leitung des Telefons eingeschleift und invertierte nur die Sprachfrequenzen, die Trägerfrequenz wechselte jedoch nicht. Man glaubte, das Gerät könne auch eine Verzerrung zusätzlich erzeugen, was sich aber nicht bestätigte. Die erzielte Sprachveränderung hielt sich in Grenzen, so daß nach einiger Übung ein Lauscher dennoch das Gespräch verstehen konnte.[461]
Die Wehrmacht setzte dann verbesserte Inverter mit zwei bzw. fünf Frequenzbändern ein, die allerdings mit fest eingestellter Frequenzband-verwürfelung arbeiteten, und demzufolge einfach zu brechen waren. Diese problematische Sicherheit veranlaßte daher die Verantwortlichen, nach besseren Verfahren zu suchen, die man mit Kombinationen verschiedener Veränderungen zu erreichen hoffte: 18 Verfahren enthält die Aufstellung des Berichtes, doch nur

[457] Offizielle Bezeichnung für eine Einrichtung, die militärisch-technische Forschungen betrieb. Nicht zu verwechseln mit dem „Forschungsamt“ des Reichsluftfahrtministeriums, Tarnbezeichnung für Görings Zentrale für Spionage, Sabotage, Funkaufkklärung etc.
[458] Vgl. Gellermann, Günther: ... und lauschten für Hitler, S. 157.
[459] Vgl. Kahn, Codebreakers, S. 558-560.
[460] Bericht über das Chiffrierwesen in OKW/Chi.
[461] Vgl. Ibing, Hans K.: Blick in das Fernmeldewesen. Köln/Krefeld 1949, S. 239-241.

vier verbesserte Inverter wurden noch eingesetzt.[462]
Nach IBING sollen Trägerfrequenzverfahren mit 8-15 Kanälen versuchsweise eingesetzt worden sein, auf denen jeweils ein schmales invertiertes Frequenzband der Sprache übertragen wurde. Die Kanäle wechselten [pseudozufällig] synchron in beiden Stationen; das Abhören soll dadurch unmöglich gewesen sein.[463]
Ein später verfaßter Bericht[464] kam zum realistischen Ergebnis: „Ein sicheres Sprachverschlüsselungsgerät existiert nicht"; die Inverter „sind nur als Erschwernisgeräte" geeignet. Ein sicheres Sprachverschlüsselungsgerät würde daher auf der „Grundlage der künstlichen Sprache" entwickelt.

Der Nachfolger FELLGIEBELS als Chef des OKW/Chi, General PRAUN, bestätigte diese Angaben nach dem Krieg: „Die Sprachverschlüsselung war zum Kriegsende im Prinzip gelöst, nachdem alle bis dahin beobachteten Systeme des Feindes entziffert worden waren."[465] Mithin entging das nachfolgend beschriebene SIGSALY-System den Abhörexperten, denn vermutlich konnten sie dieses digitale Verfahren nicht einmal abhören, weil digitale Empfangsgeräte fehlten.

6.4.2 Digitale Sprachverschlüsselung SIGSALY

In der erwähnten Forschungsarbeit GELLERMANNS unterstellt der Autor, daß das Fehlen wichtiger Abhörprotokolle auf alliierte Suchaktionen nach dem Kriege zurückzuführen sei, bei denen „peinliche" Protokolle entfernt wurden.[466] Aber: Womöglich gab es diese Protokolle überhaupt nicht, denn die wichtigsten Gespräche wurden ab Herbst 1943 nicht mehr per Bell-A3 geführt, was GELLERMANN vermutlich entgangen ist. Der US-Dienst hatte inzwischen wegen Sicherheitsbedenken das Bell-A3-Verfahren ersetzt durch das neue digitale SIGSALY-System.[467] Allerdings waren, außer CHURCHILL, nur 12 Spitzenbeamte/-militärs SIGSALY-berechtigt; das Bell-A3-System mußte für weniger anspruchsvolle Gespräche im Einsatz bleiben. Gleichwohl verminderte sich der Verkehr darüber, was auch die deutschen Abhörspezialisten bemerkten und daraufhin meldeten, es müßte nun noch eine andere Telephonverbindung geben, nach der sie suchten.[468] Freilich konnten sie diese nicht finden, denn verschlüsselte digitale Übertragung – nur als Summen zu hören – war damals unbekannt, und das System unterlag der höchsten Geheimhaltungsstufe.

---

[462] Bericht über das Chiffrierwesen in OKW/Chi.
[463] Vgl. Ibing, Hans K.: Blick in das Fernmeldewesen.
[464] Vgl. OKW/Chi: Chiffrierwesen Wehrmacht.
[465] Praun, Albert: Das Nachrichtenwesen als Führungsmittel der obersten Heeresführung im Zweiten Weltkrieg. S. 34. BA-MA, ZA 1/1916.
[466] Vgl. Gellermann, S. 154.
[467] Damals „X-System" genannt. Kahn berichtet, daß noch am 29.7.1943 ein wichtiges Gespräch Roosevelt-Churchill über den Sturz Mussolinis aufgenommen und an Hitler geleitet wurde, der daraufhin die Entwaffnung der Italiener beschloß. Vgl. Kahn, Codebreakers, S. 556.
[468] Vgl. Weadon, Patrick D.: The SIGSALY Story.

SIGSALY-System

Sichere geheime Sprachkommunikation erfordert eine Chiffrierung mit einem Schlüssel, was nur mit Digitalisierung der Sprache möglich ist: Die Sprachbits werden dann per XOR-Operation mit einem Schlüsselstrom verknüpft, eine Methode also, die bereits für die unter 4.2 beschriebene Fernschreiber-Chiffrierung verwendet wurde. Die Sicherheit der digitalen Sprachverschlüsselung hängt daher ebenso von der Pseudo-Zufälligkeit der Bitfolgen des Schlüssels ab, es sei denn, man setzt ein aufwendiges OTP-Verfahren ein. Doch das ist schwierig zu realisieren, denn nicht nur Erzeugung und Logistik der Schlüsselsequenzen erfordern großen Aufwand. Darüber hinaus muß die Synchronisation der beiden Sprechstellen sichergestellt werden, da ja in Echtzeit übertragen wird.

Das SIGSALY-System war ein Produkt der Forschungen der *Bell labs*. Dort begann man in den 30er Jahren Sprache in digitale Form zu transformieren und nutzte dazu das Prinzip des VOCODERS (*Voice Coder*), 1935 vom Bell-Ingenieur DUDLEY patentiert, der mit 11 codierten Frequenzproben + Kanal für Zusatzinformationen die zu übertragende Frequenzbandbreite drastisch verkleinerte.
Während seines US-Aufenthaltes November 1942 bis März 1943 war an diesen Arbeiten („Projekt X") in den *Bell labs* auch TURING beteiligt, der weitere Verbesserungen vorschlug. Er prüfte dann im Auftrag der britischen Regierung die fertiggestellte Anlage und war mit dem System insgesamt einverstanden.[469]

SIGSALY arbeitete zwar mit einigen (Hilfs-) Analogkomponenten (z.B. Schallplatten zur Schlüsselspeicherung, analoge Schwundregelung), gleichwohl muß man es als digitales Verfahren bezeichnen, da es digitale Abtastung und Übertragung nutzt, und ebenso digital verschlüsselt.
Das System sollte absolut abhörsicher sein und wurde daher als OTP-Verfahren konzipiert. Dazu wurden zehn Frequenzbänder jede 20 msec abgetastet und das Ergebnis mit einer echt zufälligen akustischen Schlüsselsequenz bitweise addiert. Die resultierende geheime Sprachinformation modulierte dann den Sender; diese Übertragung war nach heutigen Begriffen eine Puls-Code-Modulation (PCM).[470]
Es war das erste betriebssichere digitale Sprachdaten-Übertragungsverfahren.

Wie bei allen OTP-Verfahren, erwies sich die echt zufällige Schlüsselgenerierung als Hauptproblem. Es konnte jedoch mit einer neu entwickelten Methode gelöst werden: An einem Quecksilberdampf-Gleichrichter tastete man dessen thermisches Rauschen ebenfalls alle 20 msec ab, quantisierte es in sechs Stufen gleicher Wahrscheinlichkeit (*equal probability*), und wandelte es anschließend in

[469] Vgl. Hodges, Turing. S. 247-250.
[470] Diesen Begriff verwendet auch Hodges, Turing, S. 247. Das PCM-Verfahren wurde bereits 1914 theoretisch diskutiert und 1926 patentiert, jedoch nicht praxisreif entwickelt.

kanalgetrennte, digitalisierte Audiosequenzen. Diese wurden auf Schallplatten übertragen und mußten jeweils paarweise auf beiden Stationen vorhanden sein. Nach einmaligen Gebrauch vernichtete man sie.

Ebenso erforderte die Synchronisation der beiden Stationen großen Aufwand, besonders für den Gleichlauf der beiden Plattenspieler, welche die Schlüsselsequenzen einwandfrei synchron abtasten mußten. Dazu entwickelte man spezielle Hochfrequenz-Synchron-Antriebsmotoren, und stabilisierte deren Drehzahl durch Quarzoszillatoren und weitere Hilfsgeräte.[471]
Das nachstehende, vereinfachte Schema illustriert die Verwandtschaft mit dem OTP-Verfahren zur Chiffrierung:

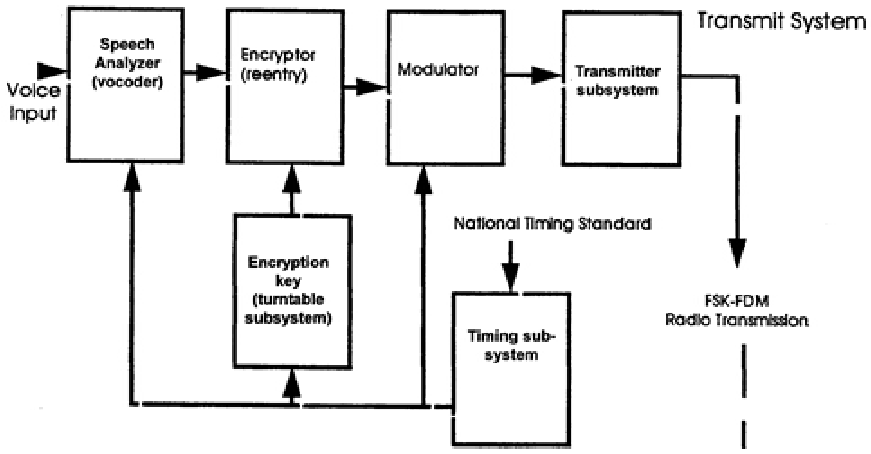


Bild 48: Schema des SIGSALY-Verfahrens[472]
(Empfangsstation reziprok)

Im *Encryptor* erfolgte die Chiffrierung des im *Vocoder* digitalisierten Signals per XOR mit Zufallssequenzen, die auf Schallplatten (*turntable subsystem*) gespeichert waren. In der Gegenstelle erfolgte diese Prozedur reziprok; den Gleichlauf sicherte als System-Taktgeber das per Funk übertragene Zeitzeichen des (US-)*National Timing Standard.*

Wegen des enormen Aufwandes – es waren 50 t Anlagen je Station erforderlich – wurden zunächst nur Terminals in Washington und London installiert, später auf einem Kriegsschiff im Pazifik für die dortige militärische Kommunikation mit Washington.

[471] Vgl. Boone, J. V. and Peterson, R. R.: The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II. Revised October 13, 2000, National Security Agency. Von: http://www.nsa.gov/wwii/papers/sigsaly.htm, am 29.01.03.

[472] Bild nach Boone, J. V. and Peterson, R. R.: The Start of the Digital Revolution.

Bild 49: SIGSALY-Kontrollraum[473]

Diese sehr aufwendige Entwicklung und Realisierung konnte wohl nur unter Kriegsbedingungen erfolgen, und sicherte auch auf diesem Gebiet den USA einen weiten Vorsprung, der später kommerziell ausgewertet wurde.
SIGSALY wurde zunächst nur für geheime militärische Zwecke eingesetzt, und ab 1951 für zivile Anwendungen weiterentwickelt. In den 50er Jahren verwendeten kommerzielle Nutzer noch das analoge System *LYNCH AZ-31 Speech Scrambler*, dessen Sicherheit kaum höher als das des Bell-A3-*Scramblers* gewesen sein wird.
Folgt man einem Firmenbericht, entwickelten die *Bell labs* nach den Erfahrungen mit SIGSALY ab 1946 den Mobilfunk, der per Vermittlung über einen Operator betrieben wurde.[474] Das große Interesse daran veranlaßte die Weiterentwicklung zu einem zellularen Verfahren, das jedoch erst mit Halbleitertechnik zu realisieren war. Die ersten Zellen wurden bereits 1973 errichtet, ein Entwicklungsvorsprung dank SIGSALY, wie ein Vergleich zeigt: Die Deutsche Bundespost nahm erst 1985 das erste zellulare Netz probeweise in Betrieb.[475]
Demnach ist auch der Mobilfunk ein indirektes Ergebnis der Kryptologie, abgesehen davon, daß zu dessen Betrieb – Benutzeridentifikation und Sprachverschlüsselung – heute ohnehin Kryptologie unentbehrlich ist.

[473] Bild nach Boone, J. V. and Peterson, R. R.: The Start of the Digital Revolution.
[474] Vgl. Zysman, G. I. et al.: Technology Evolution for Mobile and Personal Communications, S. 109.
[475] Stichwort „Funktelefonnetz C“ in: Mache, W. (Hrsg.): Lexikon der Text und Daten-Kommunikation. S. 177.

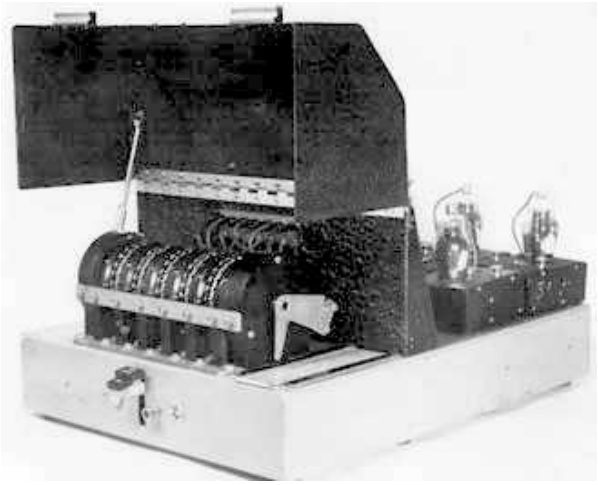
6.4.3 Turings digitales DELILAH-System

TURING arbeitete ab April 1943 – wieder zurück in England – u.a. an einer britischen Version der Sprachverschlüsselung, mit der er sich gedanklich schon länger beschäftigt hatte, vermutlich vom SIGSALY-System inspiriert. Gelegenheit zur Realisierung erhielt er ab Herbst 1943 beim Geheimdienst MI6, der in seiner Funkstation Hanslope Park ein Forschungszentrum für geheime Nachrichtenübertragungsverfahren unterhielt, darunter für ROCKEX (S. 4.5.1). Dort entwickelte er sein Projekt unter einfachsten Bedingungen – es erhielt keine Priorität – unter dem Namen DELILAH. Es mußte mit weit geringerem Aufwand auskommen als das SIGSALY-System, nur die Fernübertragung über Kurzwelle (Probleme das Schwundausgleichs usw.) war nicht vorgesehen, aber dennoch sehr sicher sein. Daher verzichtete er auf den aufwendigen VOCODER und die jeweils auszutauschenden akustischen OTP-Sequenzen, die in Schallplatten beim SIGSALY-System gespeichert waren.[476] Letzteres erforderte jedoch eine maschinelle Schlüsselerzeugung, gegen Kryptanalyse entsprechend zu sichern, worüber TURING durch seine Arbeit in BP freilich bestens informiert war.

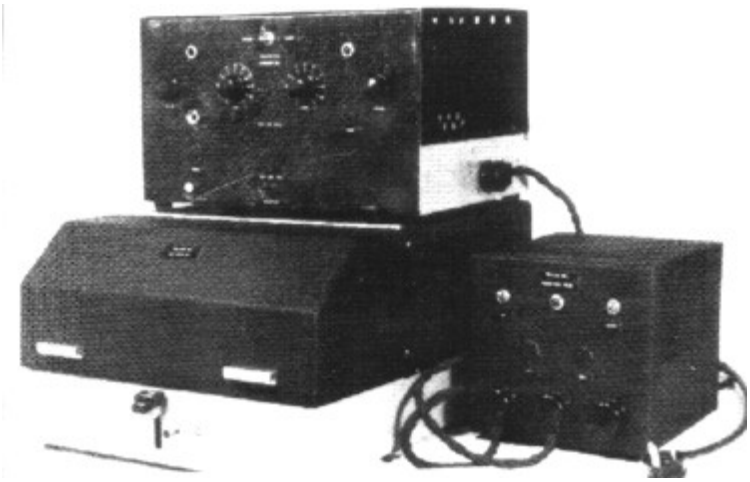
Der Schlüsselgenerator bestand aus acht Schwingkreisen mit unterschiedlicher Frequenz, deren Ausgangsleistung nach der Fourier-Theorie gleichmäßig über den Frequenzbereich verteilt wurde, um Häufigkeitsanalysen der Frequenzen zu verhindern. Die dazu erforderliche genaue Messung und Übertragung der Amplituden war eine analoge Komponente, so daß ein digital-analoges System entstand. Für jede Sendung sollten unterschiedliche Einstellungen gewählt werden, was ein Verfahren mit Spruchschlüssel erforderte. TURING orientierte sich dazu an der ihm bestens bekannten ENIGMA und installierte entsprechend Rotoren und ein Steckerfeld.[477]
Schließlich war noch das schwierige Synchronisationsproblem zu lösen, wozu TURING viel Zeit benötigte, weil einige Meßgeräte fehlten und er diese erst anfertigen mußte. So wurde das System erst zum Kriegsende betriebsfertig und kam daher nicht mehr zum Einsatz.

Für eine zivile Verwendung untersuchte es dann das Post Office, unter Tommy FLOWERS Leitung, der – kaum überraschend – keine kryptologische Schwäche fand.
Doch die Post lehnte das System ab, denn die Sprachqualität war noch zu schlecht. Es hätte dazu weiter entwickelt werden müssen, doch TURING versuchte vergebens, den skeptischen T. FLOWERS vom Potential des DELILAH –Systems zu überzeugen.[478]

[476] Vgl. Hodges, Turing. S. 284.
[477] Ebd. S. 285-286.
[478] Vgl. Hodges, Turing, S. 290.



Haupteinheit mit aufgeklappten Deckel



vollständige Station

Bild 50: TURINGS Sprachverschlüsselungsgerät DELILAH[479]

Anfang 1946 wurden die Geräte zum *Cypher Policy Board* gebracht und installiert. Der zuständige Beamte war sehr interessiert und schlug vor, die Entwicklung von DELILAH fortzusetzen. Das wurde abgelehnt und später gerieten die kleinen Geräte in Vergessenheit.[480] Erst 15 Jahre später soll eine geheime Weiterentwicklung erfolgt sein, über deren Ergebnis und/oder Verwendung nichts bekannt ist.

[479] Bilder nach Hodges, Turing, Tafel nach S. 268.
[480] Ebd. S. 346.

7 Frühe Computer und Kryptanalyse

In der Standardliteratur zu frühen Computern findet man inzwischen fast immer auch einen Bericht über den Rechner COLOSSUS, doch die meisten Autoren unterschätzen dessen wahre Bedeutung, indem sie nach Kriterien urteilen, die für einen „normalen" frühen Computer angezeigt sind. Das überrascht nicht, denn die Literatur scheint fokussiert zu sein auf die Maschine ENIAC und v. NEUMANN, dessen Schrift *First Draft of a Report on the EDVAC* den Beginn der Entwicklung von Computern markieren soll. Die danach so benannte „von Neumann-Architektur" dominierte die nachfolgende Computergeneration, und diese Maschinen scheinen keinen Bezug zur Kryptologie zu haben. Die Autoren beurteilen dabei die Entwicklung aus der Perspektive der Computer-Architektur, doch woher die zugrundeliegende Technik stammt, nämlich die Digitalelektronik, interessiert offenbar weniger.
Hatte diese womöglich einen kryptologischen Hintergrund und beeinflußte damit Entwicklungen von Rechnern/Computern?

7.1 Wissenstransfer GB-USA

Diese nicht nur informatikhistorisch bedeutsame Zusammenarbeit begann inoffiziell bereits im Dezember 1940, also lange vor dem Kriegseintritt der USA. Eine US-Delegation besuchte damals BP und wurde dort umfassend informiert.[481]
(Ob CHURCHILL damit den Kriegseintritt der USA begünstigen wollte?).
Doch erst nach einigen Streitereien kam eine Zusammenarbeit zustande, nachdem sich die unmittelbar Verantwortlichen verständigt hatten: Im Oktober 1942 trafen sich E. TRAVIS (BP-Direktor) und J. WENGER (Chef US-Navy-Dienst OP-20-G), und unterzeichneten eine inoffizielle Vereinbarung, das *Travis-Wenger-Agreement*, in der Literatur auch als *Holden-Agreement* bezeichnet, zur Zusammenarbeit bei der Brechung deutscher Marine-Chiffrierungen. Als ersten Schritt vereinbarte man britische Hilfe zum Bau einer US-BOMBE und die Lieferung aller dazu erforderlichen Unterlagen, dazu ein Papier von TURING, wie dieses Gerät effizient zu betreiben ist.[482]

Diese aus britischer Sicht „sehr einseitige" Vereinbarung bereitete immerhin den Weg zum im Mai 1943 geschlossenen offiziellen BRUSA-Pakt, der eine intensive kryptologische Zusammenarbeit und den Austausch aller Erkenntnisse ermöglichte, die nach dem Krieg fortgesetzt und mit dem *UKUSA-Agreement* 1946 bekräftigt wurde.[483]

---

[481] Vgl. Smith, Michael: Enigma entschlüsselt, S. 198-200.
[482] Vgl. Bletchley Park Museum: "Historical information gathered from the Bletchley Park archives", Aug. 1943.
[483] Vgl. Ebd., Sept. 1942.

Gemäß diesem Abkommen arbeitete eine ständige US-Delegation von 20 (später 45) Experten in BP, hatte dort überall Zutritt und konnte alles Wichtige notierten. Deren Leiter W. BUNDY beschrieb die Zusammenarbeit als „einzigartiges Experiment im gemeinsamen Denken, mit dem größten Erfolg bei der praktischen Realisierung." Den britischen Kollegen bescheinigte er eine „außerordentliche intellektuelle Leistung", die wissenschaftlich-technischen Grundlagen erarbeitet zu haben, und bestätigte eine intensive und vollständige Zusammenarbeit „ohne Geheimnisse" voreinander.[484]

Neben der erarbeiteten *intelligence* wollte man auch alle technischen Informationen austauschen: Auf diesem Weg gelangten dann u.a. die britischen Erfahrungen mit digitalelektronischen Schaltungen in die USA, beispielsweise die von FLOWERS entwickelten Module und deren Betriebsweise. Ein Indiz hierfür ist die Sorgfalt, mit der die US-Delegierten in BP beobachteten und berichteten: Beispielsweise konnte nach SALE das *Colossus-Rebuild-Projekt* des Museums Bletchley Park erst dann realisiert werden, als die detaillierten Aufzeichnungen des US-Delegierten A. SMALL über COLOSSUS freigegeben wurden.[485] [Britische Unterlagen fehlten].

Man kann demnach für beide Seiten des Atlantiks, ungefähr ab der Mitte des Krieges, etwa den gleichen Wissensstand annehmen, denn die technischen Erfahrungen verbreiteten sich vermutlich bald innerhalb der *scientific community* der wenigen Fachleute, die sich untereinander meist schon aus der Vorkriegszeit kannten. Ferner mußte man die Herstellerfirmen der Geräte bzw. Zulieferfirmen über bestimmte technische Zusammenhänge informieren, so daß technisches Wissen wohl auch über diesen Weg ausgetauscht wurde – und deren starke Marktstellung nach dem Krieg förderte. Dokumente hierüber existieren freilich nicht.

7.2 COLOSSUS und Informatikgeschichte

7.2.1 ENIAC - birth of information age?

Das 50jährige Jubiläum des ENIAC wurde 1996 von den USA bombastisch gefeiert; der US-Vizepräsident lobte die amerikanischen Wissenschaftler, sie hätten das Computerzeitalter eröffnet mit dem Begriff „*birth of information age*". Kein Wort fiel freilich über den Beitrag, den Computerpioniere in anderen Ländern leisteten, besonders nicht über den erwähnten Wissenstransfer während des Krieges, wovon auch die US-Computerbauer profitierten. Zwar war dieser

[484] Vgl. Bundy, W.: Some of my Wartime Experiences. In: Deavours, Cipher A. et al. (Eds.): Cryptology – machines, history and methods. Artech House, Norwood MA/USA, 1989, S. 121.

[485] Vgl. Sale, Tony: The Colossus of Bletchley Park. In: Rojas, R./Hashagen,U. (Eds.): The First Computers: History and Architectures, MIT Press, Cambridge MA/USA und London, 2000, S. 363.

nicht allgemein bekannt, aber bspw. die Fachleute der angesehenen IEEE-Annals hätten es wissen müssen, doch auch sie ließen sich von der patriotischen Begeisterung anstecken.[486]

In relevanten Publikationen, auch aktuellen, bezeichnen deren Autoren die US-Maschine ENIAC als „*the world's first large-scale electronic digital computer*".[487] Diese verbreitete Ansicht wird verständlich, wenn man berücksichtigt, daß ENIAC 1946 öffentlich präsentiert wurde, COLOSSUS hingegen unbekannt war und blieb – eine Folge der überzogenen Geheimhaltungspolitik der britischen Behörden: Bis 1974 leugneten sie sogar die bloße Existenz des COLOSSUS, die erst durch WINTERBOTHAM'S Buch[488] bekannt wurde, und erst dann gab man 1975 Photos frei. In 1983 durfte der Erbauer FLOWERS über einige wenige technische Daten der Hardware berichten und erst 1996 erfuhr man Genaueres durch Dokumentfreigaben des US-*Opendoor-Programs*. Das wichtigste Dokument, der „*General Report On Tunny*", wurde gar erst im Jahr 2000 deklassifiziert, nach intensiver Kampagne des BP-Mitarbeiters und Mitverfassers Don MITCHIE.[489] Seither sind fast alle Einzelheiten des kryptanalytischen Rechners COLOSSUS bekannt, freilich nicht dessen weiterhin geheimen kryptanalytischen Algorithmen.

7.2.2 COLOSSUS vs. ENIAC

Um zu einer informatikhistorisch richtigen Einschätzung zu gelangen, ist es erforderlich, den technischen Stand beider Maschinen zu vergleichen. In diesem Zusammenhang sollte ferner einer interessanten Frage nachgegangen werden: Beeinflußte der erwähnte Erfahrungsaustausch das ENIAC-Projekt, d.h. berücksichtigten dessen Konstrukteure direkt oder indirekt technische Erkenntnisse der elektronischen Kryptologie? Diese Fragestellung ist auch deshalb relevant, weil durch ein erbittert geführtes Patentgerichtsverfahren bekannt wurde, daß die ENIAC-Konstrukteure dazu neigten, fremdes geistiges Eigentum ohne Namensnennung zu übernehmen. Demnach wäre es nicht unwahrscheinlich, wenn sie ebenso technische Erkenntnisse der elektronischen Kryptologie übernommen hätten, zumal diese nicht patentiert waren. Welche Innovationen man nun den ENIAC-Konstrukteuren ECKERT und MAUCHLY zuschreiben kann, welche aber nicht, zeigt am besten der nachstehende Vergleich zum Rechner COLOSSUS, der schon zwei Jahre früher im ständigen Einsatz war.

---

[486] Vgl. Winegrad, Dilys : Celebrating The Birth Of Modern Computing. In: IEEEAnnals, Spring 1996, Vol. 18, No. 1, pp. 59. Von: http://www.computer.org/annals/an1996/a1005abs.htm, am 7.1.03.

[487] Bspw. aktuell in: Goldschmidt, Asaf and Atsushi, Akera John: W. Mauchly and the Development of the ENIAC Computer. In: Exhibition in the Department of History and Sociology of Science, University of Pennsylvania. Last update: 03-Feb-2003. Von: http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html, am 3.3.03.

[488] Winterbotham, F.W.: The Ultra Secret, New York, Harper, 1974.

[489] Good/Michie/Timms: General Report On Tunny: With Emphasis on Statistical Methods (1945).

Zunächst ist zu fragen, ob der in der Literatur vertretene Anspruch „ENIAC war der erste vollkommen elektronisch arbeitende Großrechner“ berechtigt ist. Dagegen wäre als erstes einzuwenden, daß COLOSSUS bereits Ende 1943 in Betrieb ging und ebenfalls vollkommen elektronisch arbeitete. Der Begriff „Großrechner“ ist jedoch nicht definiert; doch nach damaligen Maßstäben müßte man COLOSSUS II mit 2.500 Röhren diesen Status zuerkennen. Abgesehen davon unterscheidet sich dessen Betriebsweise nur unwesentlich von der einer Maschine mit der ca. siebenfachen Anzahl Röhren (ENIAC), lediglich der Kühlaufwand steigt entsprechend. Dabei kommt es nur darauf an, die Betriebstemperatur der Röhren zu stabilisieren, wozu beim ENIAC eine aufwendige Ventilation erforderlich war, COLOSSUS hingegen durch seine offene Bauweise ohne Ventilation auskam. Dieser unwesentliche Unterschied im Aufbau begründet sicher nicht eine andere Größenordnung.

Ebenfalls sind kaum Unterschiede zu erkennen hinsichtlich einer universellen Programmierbarkeit, denn beide Geräte konnte man nur mit externen Methoden – Steckverbindungen, Schalter etc. – programmieren, weil Speicher mit freiem Zugriff fehlten. Der elektronische Speicher des COLOSSUS generierte per fest verdrahtetem Schlüsselalgorithmus einen synchronen Schlüsselstrom für Vergleichsoperationen – eine Novität, über die ENIAC nicht verfügte, allerdings auch nicht verfügen mußte.

Sehr unterschiedlich verarbeiteten die Rechner Zahlen: COLOSSUS verfügte über ein leistungsfähiges Binärsystem, das jedoch auch für dezimale Rechnungen programmiert werden konnte, wie Experimente nach dem Krieg zeigten. ENIAC hingegen mußte mit einer aufwendigen Dezimalstruktur auskommen, und jede Dekade benötigte nicht weniger als 24 Röhren.

Wegen seiner Architektur muß man ENIAC bei seiner Inbetriebnahme 1945/46 als technisch veraltetes System bezeichnen, wenn nicht gar als „..*completely obsolete*“ (HODGES).[490] Denn nur die schiere Größe der Maschine ermöglichte die geforderten Leistungen, was auch die Konstrukteure erkannten.[491] Dementsprechend rüstete man bald nach Inbetriebnahme die Maschine in mehreren Stufen auf und strukturierte sie teilweise neu, sobald geeignete Komponenten verfügbar waren. Der so verbesserte ENIAC arbeitete dann bis 1955 zufriedenstellend im *Army Ballistics Laboratory*.

Die veraltete Konstruktion wird verständlich, wenn man den historischen Hintergrund einbezieht: Die US-Artillerie benötigte ballistische Tabellen, die sie

---

[490] Der Turing-Biograph A. Hodges konstatierte „… ENIAC calculator, fully working in 1946, by which time its design was completely obsolete“. Vgl. Hodges, Alan Turing Scrapbook: Who invented the Computer? S. 3.

[491] Eckert und Mauchly wollten bspw. in der Bauphase eine modernere Programmsteuerung entwickeln, und schlugen dazu im Januar 1944 einen rotierenden Magnetspeicher vor. (Vgl. Naumann, Informatik, S. 207). Sie wurden jedoch vom Auftraggeber aus Termingründen daran gehindert. (Vgl. Copeland, Computer Age, S. 367).

seit 1934 mit Hilfe des von V. BUSH gebauten, mechanisch-analogen *differential analyzers* berechnen ließ. Mit Kriegsbeginn stieg der Bedarf drastisch, doch die langsame und systembedingt nicht sehr genaue Maschine genügte nicht mehr. Man requirierte ein zweites Exemplar, das in der *Moore School of Electrical Engineering*[492] installiert war, doch auch das reichte nicht. Daher beauftragte die Army die *Moore School*, dringend ein schnelleres und genaueres System zu entwickeln. Im Juni 1943 begann dort ein Team unter ECKERT und MAUCHLY an der Entwicklung des ENIAC zu arbeiten, unter Aufsicht von H. GOLDSTINE vom *Army Ballistics Laboratory*.[493]
Die fertige Maschine leistete dann genau das, was die Auftraggeber gefordert hatten, nämlich schnelle und genaue ballistische Berechnungen, die allerdings nach Kriegsende nicht mehr benötigt wurden. Es war quasi die leistungsstärkere elektronische Version des *differential analyzers*.

Inzwischen äußern sich sogar amerikanische Autoren differenzierter über ENIAC, bspw. der Professor an der ENIAC-„Mutter"universität Pennsylvania, J. van der SPIEGEL: Er räumte ein, daß bei ENIAC's Konstruktion man auf beträchtliche Forschungsergebnisse aufbauen konnte, die mit Zählschaltungen [=> J. DESCH] und Experimentalschaltungen [=>ATANASOFF-BERRY] gemacht wurden, ebenso von Röhrenherstellern und Forschungseinrichtungen.[494]
Und nach WILLIAMS bestanden ENIAC's Systemkomponenten aus bereits bekannten Konstruktionen, im Wesentlichen aus Teilen des Relaisrechners Harvard Mark 1 [=>AIKEN], die nun elektronisch aufgebaut wurden.[495]

Bei diesen späten Eingeständnissen fehlt aber ein Hinweis, woher man wußte, wie der sichere Betrieb der ca. 17.000 Röhren zu gewährleisten sei. Zwar hatte sich der Wissenschaftler MAUCHLY bereits 1942 mit Möglichkeiten beschäftigt, Elektronenröhren für Rechnersysteme[496] zu verwenden, jedoch nicht mit *technischen* Lösungen für deren Realisierung und Betrieb. Es wird aber auch nirgends behauptet, ECKERT und MAUCHLY hätten die erforderliche Betriebsweise erfunden, nämlich die bereits von FLOWERS in seiner elektronischen Telefonvermittlung realisierte Reduzierung der Röhrenleistung auf 30%, und Dauerbetrieb bei konstanten Bedingungen, die er ab 1943 auch beim COLOSSUS verwendete.

---

[492] Heutige offizielle Bezeichnung: University of Pennsylvania, School of Engineering & Applied Science.

[493] Vgl. Willams, Michael R.: A History of Computing Technology, 2nd ed. IEEE Computer Society Press, Los Alamitos CA/USA, 1997, S. 267-271.

[494] Vgl. Spiegel, Jan van der, et al.: The ENIAC: History, Operation and Recontruction in VLSI. In: Rojas, R./Hashagen, U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA und London, 2000, S.125-126.

[495] Vgl. Willams, Michael R.: A History of Computing Technology, 2nd ed. IEEE Computer Society Press, Los Alamitos CA/USA, 1997, S. 273.

[496] Vgl. Mauchly, J.W.: The Use of high speed vacuum tube devices for calculating, Moore School of El. Eng., University of Pennsylvania, 1942. (Privately circulated Memorandum).

Diese und andere *technische*[497] Informationen waren über Berichte der US-Delegation in BP den zuständigen Stellen in den USA bekannt. Wahrscheinlich gehörte dazu auch das *Advisory Committee of the Ballistics Research Laboratories*, dessen Mitglieder u.a. GOLDSTINE und V. NEUMANN waren.[498] Sie könnten von dort an die ENIAC-Konstrukteure gelangt sein, etwa über den ENIAC-Projektbetreuer GOLDSTINE, der am Erfolg des Projekts unmittelbar interessiert sein mußte, denn erst seine Empfehlung überzeugte die skeptischen Army-Auftraggeber zur Bewilligung des Projektes.[499]
Ein anderer Weg über die *scientific community* ist ebenfalls denkbar, ebenso wie über die Röhrenhersteller, die ja mindestens teilweise informiert werden mußten.

Freilich werden diese Möglichkeiten nicht durch Dokumente belegt werden können, aber woher sonst kamen die Empfehlungen zur Betriebsweise des ENIAC?
Anders formuliert: Hätten US-Forscher diese Betriebsweise entwickelt, wäre das wohl sicher US-typisch propagiert worden. Und vermutlich hätten sie es sich patentieren lassen, woran der bescheidene FLOWERS nie dachte.

Festzuhalten bleibt: Zu diesem Zeitpunkt – 1943 – hatte nachweisbar nur FLOWERS elektronische Großschaltungen gebaut, die sich im Dauerbetrieb erfolgreich bewährten. Diese Erfahrungen wurden den US-Diensten offenbart, so daß sie während des Krieges in den Wissenspool auf beiden Seiten des Atlantiks eingingen. Es ist daher sehr wahrscheinlich, ja fast sicher, daß über diesen Weg FLOWERS Erkenntnisse auch den Konstrukteuren des ENIAC bekannt wurden. Ebenso wahrscheinlich hätten sich Bau und Inbetriebnahme des ENIAC wohl erheblich verzögert, wenn dessen Konstrukteure diese Betriebsweise hätten erst herausfinden müssen.
Mithin erbrachten britische Forscher, allen voran FLOWERS, damit einen wichtigen Beitrag zur frühen Computerentwicklung.

7.2.3 COLOSSUS in Manchester

Kritiker könnten einwenden, COLOSSUS habe schon deshalb keine informatikhistorische Bedeutung gehabt, weil es keine Weiterentwicklung gab, und erst ab 1974 seine technischen Daten allmählich zu erfahren waren. Mithin könne der Maschine eine Bedeutung für die Computerentwicklung nicht zuerkannt werden. Dagegen wäre jedoch anzuführen: COLOSSUS und dessen

[497] Alle kryptologischen Erkenntnisse unterlagen strenger Geheimhaltung nach dem "need-to-know"-Prinzip.
[498] Vgl. Lee, J.A.N.: International Biographical Dictionary of Computer Pioneers. Fitzroy Dearborn Publishers, Chicago, London, 1995, S. 326.
[499] Vgl. Goldschmidt, Asaf and Atsushi, Akera John: W. Mauchly and the Development of the ENIAC Computer. In: Exhibition in the Department of History and Sociology of Science, University of Pennsylvania, Last update: Monday, 03-Feb-2003. Von: http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html, am 3.3.03.

Vorgängergeräte vermittelten den Beteiligten wertvolle, z.T. völlig neue Erkenntnisse und Erfahrungen, die einmal über die US-Delegation in BP auch in den USA bekannt wurden, und dort die Rechnerentwicklung beeinflußten. Zum anderen konnten die britischen Experten ihre Kenntnisse nach dem Krieg in zivilen Stellungen unmittelbar verwerten; die wichtigsten Projekte sind unter 7.3 erläutert.

Wie sehr die Erfahrungen mit COLOSSUS nachwirkten, zeigt bspw. die Vorgeschichte des Computers *Manchester Mark 1*: Der sehr erfolgreiche Einsatz der COLOSSUS-Maschinen und deren Vorgänger in BP überzeugte den dort zuständigen Abteilungsleiter Max NEWMAN vom Potential elektronischer Rechenmaschinen, und regte ihn zu Gedanken über TURINGS Universalmaschine an. Dessen Schrift „*On Computable Numbers*" war ihm – TURINGS Hochschullehrer in Cambridge – bestens bekannt, und NEWMAN dachte bereits 1944 daran, eine elektronische Turing-Maschine zu bauen. Das geht aus seiner Korrespondenz mit V. NEUMANN hervor, nachdem er im Sommer 1945 einen Lehrstuhl für Mathematik an der Universität Manchester übernommen hatte. In diesem Zusammenhang schrieb er: „*I am hoping to embark on a computing machine section here, having got very interested in electronic devices of this kind.[…] I am of course in close touch with TURING.*"[500]

Die erwähnte *computing machine section* errichtete NEWMAN dann 1946: Es gelang ihm, dank seiner Mitgliedschaft in der *Royal Society*, die Förderung eines *Computer Laboratory* in Manchester[501] zu erreichen mit dem Ziel, einen elektronischen Digitalcomputer zu konstruieren. Er „besorgte" dafür auch geeignete Hardware als Grundausstattung: Einige Zeit nach Kriegsende wurden die COLOSSI in BP demontiert und NEWMAN ließ die Komponenten, nach Entfernung von Hinweisen auf ihre originale Verwendung, in das neue *Computer Laboratory* überführen. Sie wurden also nicht zerstört, wie man bis zur US-Dokumentenfreigabe 1996 glaubte [und wohl glauben sollte]. Und weitere zwei intakte Geräte installierte der Geheimdienst in der BP-Außenstelle Cheltenham und betrieb sie dort bis nach 1960, zuletzt angeblich für „Trainingszwecke".[502]

Das Endprodukt der Entwicklungen in diesem Labor war der Computer *Manchester Mark 1* und dessen kommerzielle Version *Ferranti Mark 1*, wie nachstehend dargelegt ist.

---

[500] Zit. nach Copeland, Computer Age, S. 362.

[501] Das Labor gehörte nicht zur Universität, sondern der Royal Society. Staatliche Förderung erhielt es deshalb nicht.

[502] Vgl. Copeland, Computer Age, S. 344-345.

7.3 Computerentwicklung in England

Die Briten besaßen als Erste einen im Dauerbetrieb bewährten elektronischen Großrechner. Doch dessen Geheimstatus wurde aufrecht erhalten; die Erfahrungen der beteiligten Wissenschaftler und Ingenieure konnten nur indirekt genutzt werden, ebenso – wie bereits erwähnt – dessen Hardware.
Die gemachten Erfahrungen veranlaßten das Verteidigungsministerium, zusammen mit der Abteilung Wissenschaftliche und Industrielle Forschung (DSIR) nationale Computerprojekte zu initiieren.[503] Allerdings, im Gegensatz zu den USA, förderten sie diese nicht genügend, so daß die Projekte von privaten Einrichtungen wie dem erwähnten *Computer Laboratory* NEWMANS getragen werden mußten.

7.3.1 Manchester Mark 1

NEWMANS Mitarbeiter I.J. GOOD , der an elektronischen Entwicklungen in BP beteiligt und mit COLOSSUS vertraut war, kam ebenfalls mit nach Manchester. Später, 1948, übernahm TURING als *Deputy Director* Aufgaben im Computerlabor, nachdem organisatorische Mängel am *National Physical Laboratory* (NPL) sein dort ausgearbeitetes ACE-Projekt verzögert und er daher dort den Dienst quittiert hatte.

NEWMAN wußte, vermutlich aus Diskussionen mit TURING in BP, von der Bedeutung eines Speichers für Programme und Daten, was bereits BABBAGE eingehend diskutiert hatte. Daher beantragte er bald nach seiner Berufung nach Manchester (September 1945) Mittel für die Entwicklung eines *electronic stored-program computer*. Und nach deren Bewilligung erläuterte er dem ebenfalls nach Manchester berufenen Radar- und Elektronikexperten F.C. WILLIAMS und dessen Mitarbeiter Tom KILBURN dieses Projekt – sie hatten bis dahin noch nichts von elektronischen Rechnern gehört – besaßen jedoch nach ihrer Arbeit für die Radarentwicklung Erfahrungen mit der Speicherung von Impulsen. Dafür hatten sie eine Kathodenstrahlröhre patentieren lassen, auf deren Oberfläche die Impulsmuster gespeichert wurden, die sog. *Williams tube*.
Um zu testen, ob diese Röhre sich als Datenspeicher eignet, entwickelte die Gruppe das erste Projekt, den Experimentiercomputer SSEM bzw. *Manchester Baby*. Das Gerät ging im Juni 1948 in Betrieb und, nach einigen Anlaufschwierigkeiten, funktionierte der Speicher wie erwartet, er eignete sich sogar als RAM mit seinen unmittelbaren Zugriffsmöglichkeiten. Damit war das *Baby* der weltweit erste funktionsfähige [Versuchs-]Digitalrechner mit Programmspeicherung.[504]

---

[503] Vgl. Naumann, Informatik, S. 162.
[504] Vgl. Copeland, Computer Age, S. 365.

Nach den erfolgreichen Tests des *Babys* plante man nun eine größere und vielseitigere Maschine, für die der inzwischen nach Manchester gekommene TURING das Programm geschrieben und einige technische Verbesserungen entworfen hatte.[505]
Mit geringen Modifikationen baute das örtliche Unternehmen Ferranti Ltd. nach diesen Vorgaben den Computer *Manchester Mark 1*, den weltweit ersten kommerziell verfügbaren Universalcomputer ab Februar 1951.
Eine verbesserte Version lieferte Ferranti Ltd. ab 1952, die als *Ferranti Mark 1* bekannt wurde.[506]
Ferranti Ltd. setzte die enge Zusammenarbeit mit dem *Computer Laboratory* fort; diese Kombination von universitärer Forschung und produktionstechnischen Möglichkeiten begünstigte verschiedene Innovationen, darunter die Konstruktion des Hochgeschwindigkeits-Computers ATLAS.[507]

7.3.2 Turings ACE-Projekt

Obwohl Turing nicht direkt an Entwicklung und Bau von COLOSSUS mitarbeitete, nahm er teil an den häufigen Diskussionen in NEWMANS Abteilung, zu denen er als *senior consultant* Zutritt hatte. Es war quasi eine Fortsetzung seiner langjährigen Korrespondenz mit seinem akademischen Lehrer über mathematische Logik, bis dieser 1942 nach BP verpflichtet wurde. NEWMAN bemerkte später in diesem Zusammenhang, daß TURING *„… was always full of ideas and he liked to talk about other people's problems."*[508] So konnte sich TURING über die Möglichkeiten der elektronischen Schaltlogik informieren und darüber, wie ein elektronisch gespeicherter Algorithmus die Verarbeitungsgeschwindigkeit der Maschine drastisch steigern konnte.
Folgt man COPELANDS vorgenannten Bericht, diskutierte man bei diesen Gelegenheiten sehr wahrscheinlich auch über TURINGS hypothetische universelle Maschine. Indirekt bestätigte das FLOWERS, da nach seinen Angaben TURING nur auf eine Gelegenheit wartete, nach COLOSSUS' Erfolg seine Turing-Maschine elektronisch zu verwirklichen. Diese Chance bot sich im Sommer 1945, als TURING vom National Physical Laboratory (NPL) eingeladen wurde, einen elektronischen Rechner für wissenschaftliche Aufgaben zu entwickeln, die sog. *Automatic Computing Engine* (ACE). Er nahm diesen Auftrag an, entwarf bis Ende 1945 einen kompletten Rechner mit Programmspeicher und schrieb darüber den detaillierten Bericht „*Proposed Electronic Calculator*". Nach COPELAND war das die erste komplette Spezifikation eines Computers mit Programmspeicher: TURINGS wenig bekannter Bericht enthalte weitaus mehr Substanz, besonders in Bezug auf Programmierung und Hardware, als v. NEUMANNS berühmter, jedoch sehr

[505] Vgl. Willams, Michael R.: A History of Computing Technology, 2nd ed. IEEE Computer Society Press, Los Alamitos CA/USA, 1997, S. 325. (Zuk. zit.: "Williams, History of Computing").
[506] Ebd., S. 325-326.
[507] Vgl. Willams, Michael R.: A History of Computing Technology, S. 397-398.
Diese Maschine ist leicht zu verwechseln mit dem gleichnamigen US-Computer ATLAS I/II, s. 7.5.3.
[508] Copeland, Computer Age, S. 355.

theoretischer „*First Draft of a Report on the EDVAC*".
Diesen Entwurf akzeptierten die Verantwortlichen des NPL, wußten jedoch um die wenig erfahrenen Elektroniker ihres Instituts. Sie beauftragen daher das Postforschungszentrum in Dollis Hill mit der Realisierung, und dort sollte eine Gruppe unter der Leitung von Tommy FLOWERS die Maschine bauen, vermutlich auf TURINGS Empfehlung, der ja über FLOWERS Fähigkeiten bestens informiert war. Leider kam die Zusammenarbeit nicht zustande, da FLOWERS intensiv an neuen Telefon-Vermittlungen arbeiten mußte, die dringend benötigt wurden.
Eine Zusammenarbeit TURINGS mit FLOWERS hätte sehr wahrscheinlich zum schnellen Bau eines herausragenden Computers geführt, und FLOWERS glaubte einen „*minimal ACE*" bereits bis Mitte 1946 bauen zu können. Das hätte der britischen Computerszene einen großen Vorsprung gesichert, und man kann bezweifeln, ob die nachstehend beschriebene dominierende Stellung v. NEUMANNS und der *Moore-School* sich dann herausgebildet hätte.
Nach dieser Absage schlug nun TURING vor, eine eigene Elektronikabteilung am NPL zu etablieren, die auch eingerichtet wurde, jedoch alsbald in interne Rivalitäten mit anderen Abteilungen geriet. Der NPL-Führung gelang es nicht, diese Probleme zu lösen und so kam es immer wieder zu Verzögerungen bei der Realisierung des Projekts – ohne TURINGS Verschulden. Eine verunglückte Personalentscheidung[509] veranlaßte dann TURING in 1948, das NPL zu verlassen und zu NEWMAN nach Manchester zu gehen.[510]
Das ACE-Team konnte nach diesen [vermeidbaren] Verzögerungen TURINGS Entwurf erst 1950 fertigstellen, der als Versuchsmuster „*Pilot ACE*" bekannt wurde und sich durch ungewöhnlich hohe Arbeitsgeschwindigkeit[511] auszeichnete, obwohl nur ein bescheidener Arbeitsspeicher zur Verfügung stand. Auf dieser Grundlage baute die Firma English Electric Co. den kommerziell erfolgreichen Computer DEUCE, der ab 1954 geliefert wurde.[512]

Festzuhalten bleibt, daß TURINGS hypothetische Universalmaschine im Prinzip durch die Fortschritte der Elektronik in ihren Grundzügen verwirklicht werden konnte. Die Erfahrungen und Diskussionen in BP überzeugten TURING wohl von der Realisierbarkeit einer Universalmaschine – letztlich war auch das ein Ergebnis der durch die maschinelle Kryptologie gesammelten Erfahrungen.

7.3.3 EDSAC

An der Universität Cambridge übernahm nach dem Krieg der Mathematiker M. WILKES die Leitung des *University Mathematical Laboratory* (UML) und

[509] Das NPL engagierte den Elektroniker Huskey für den Bau der Hardware, der Erfahrungen bei Arbeiten am ENIAC gesammelt hatte, sich jedoch mit Turing nicht vertrug – oder auch umgekehrt.
[510] Vgl. Copeland, Computer Age, S. 364.
[511] Ebd., Taktfrequenz 1 MHz, damals der weltweit schnellste Computer.
Zum Vergleich: Die EDSAC-Maschine arbeitete nur mit 500 KHz, bei etwa gleicher Speichergröße.
[512] Vgl. Williams, History of Computing, S. 339-341.

besuchte im Sommer 1946 das nachstehend angesprochene Computerseminar an der *Moore School*. Dort konnte er sich über den damaligen Stand der Technik informieren und sich mit v. NEUMANNS Gedanken beschäftigen, dessen Schrift „*First Draft of a Report on the EDVAC*" ihm dort zugänglich war. Diese beeindruckten ihn und er beschloß in Cambridge – trotz begrenzter Mittel – nach diesen Prinzipien einen speicherprogrammierbaren Rechner zu bauen. Da für dessen Entwicklung kaum Mittel zur Verfügung standen, mußte auf vorhandene Komponenten zurückgegriffen werden. So plante er bspw. statt der noch in der Entwicklung befindlichen *Williams tube* einen vorhandenen Quecksilber-Laufzeitspeicher einzusetzen. Er fand dazu in T. GOLD einen versierten Mitarbeiter, der im Krieg in der Radarforschung Erfahrungen mit Quecksilber-Laufzeitröhren gesammelt hatte.

Überdies gewann er sogar einen „Sponsor": Die Großfirma Lyons and Co. Ltd., stellte genügend Mittel zur Verfügung, denn sie versprach sich vom geplanten Computer eine Verbesserung ihres Abrechnungs- und Vertriebssystems. Das gelang ihr später mit der nach Lyons' Vorstellungen weiterentwickelten EDSAC-Maschine namens LEO. Unter diesen günstigen Bedingungen konnte das Projekt EDSAC bis 1949 rasch und erfolgreich realisiert werden.[513]

Zu dieser Zeit war EDSAC der erste betriebsfähige speicherprogrammierbare Großrechner; die beiden britischen Konkurrenzgeräte wurden erst später fertig, ebenso die US-Konkurrenten EDVAC und IAS.

7.4 Kryptanalyse und die Computerseminare 1946

In den USA trafen sich im Sommer 1946 an der *Moore School* der Universität Pennsylvania die meisten Computerforscher und Interessierte in Seminaren, nachdem die Präsentation des ENIAC das Interesse an der Computertechnik geweckt hatte. Diese berühmte und scheinbar rein wissenschaftliche Veranstaltung, wie man lange glaubte und wohl glauben sollte, wurde nach BAMFORD „... vom Marine-Forschungsamt und dem Waffenamt der Armee gemeinsam finanziert."[514] Und sehr wahrscheinlich sollten die beiden genannten „harmlosen" Behörden deren jeweilige kryptologischen Dienste – OP-20-G und SIS – tarnen, die freilich starkes Interesse an leistungsfähigen Elektronik- und Computerentwicklungen hatten und sich auf diese Weise eingehend informieren konnten (s. dazu 7.5.2). Mithin muß man sogar diesen Meilenstein der frühen Computergeschichte indirekt der maschinellen Kryptologie zuordnen, weil die Geheimdienste an leistungsfähigeren elektronischen Geräten arbeiteten oder dieses planten.

---

[513] Vgl. Willams, Michael R.: A History of Computing Technology, 2nd ed. IEEE Computer Society Press, Los Alamitos CA/USA, 1997, S. 329-330.

[514] Bamford, NSA, S. 730.

Gegenüber ihren britischen Kollegen konnten die US-Computerforscher mit massiver staatlicher Unterstützung rechnen, denn die Regierung hatte das strategische Potential erkannt, sie war von den Erfolgen beeindruckt, die man mit kryptanalytischen Maschinen im Krieg erzielt hatte. Die Inbetriebnahme des ENIAC sorgte überdies für Begeisterung, und Herbst 1946 begannen die Forscher intensiv an einigen Projekten zu arbeiten, nachdem sie in den Sommerseminaren der *Moore School* viel Neues erfahren hatten. Die dort diskutierten Rechnerprojekte lösten eine intensive Forschung aus, mit massiver Unterstützung der Geheimdienste, die letztlich zur Dominanz der US-Computerindustrie führte, wie unter 7.5 näher ausgeführt ist. Das ist erst seit wenigen Jahren bekannt und dementsprechend in der Standardliteratur zur frühen Computerentwicklung kaum zu finden.
Ob darüber hinaus die nachstehenden nicht geheimen Projekte indirekt gefördert wurden, ist unbekannt.

7.4.1 EDVAC und IAS

Die erwähnten Sommerseminare 1946 dominierte v. NEUMANN mit seinen Vorstellungen von einem Universalcomputer, die er indirekt als seine Ideen ausgab. Folgt man BAUER, erfuhr v. NEUMANN seit seiner Beratertätigkeit an der *Moore School* (ab 1944) von den ENIAC-Konstrukteuren deren Gedanken zum Bau eines speicherprogrammierbaren Rechners, weit flexibler und leistungsfähiger als der ENIAC, wofür ECKERT die Idee gehabt haben soll.[515] ECKERT wird auch ein entscheidendender Vorschlag zur Realisierung zugeschrieben: Die für Radargeräte zur Impulsspeicherung entwickelte Quecksilber-Laufzeitröhre als Speicher für einen programmierbaren Universalcomputer zu verwenden.

Bereits im Sommer 1945 veröffentlichte v. NEUMANN dann die gemeinsamen Gedanken in der berühmten Schrift „*First Draft of a Report on the EDVAC*" unter seinem Namen, doch die seiner Partner ECKERT und MAUCHLY erwähnte er nicht. Auch verwahrte er sich nicht gegen die weitere Verbreitung dieser Schrift. Daraufhin kam es zum Streit, wobei auch mögliche Patentansprüche eine Rolle spielten.[516]

Danach verfolgten die Parteien getrennte Projekte: Das EDVAC-Projekt der US-Army übernahmen ECKERT und MAUCHLY, während v. NEUMANN zum *Institute for Advanced Study* (IAS) der Princeton University ging.[517]
Dort arbeitete er mit dem bereits als IAS-Mitglied tätigen GOLDSTINE zusammen, den er vom ENIAC-Projekt gut kannte, das dieser im Army-Auftrag geleitet

[515] Bauer, Friedrich L.: Informatik und Informationstechnik – ein Gegensatz?
In: Informatik-Spektrum 21 (1998), S. 85.
Vgl. hingegen Lee (s.u.), wonach Goldstine die Erfindung des „stored program concepts" seinem Freund v. Neumann zuschreibt.
[516] Bauer a.a.O., S. 85-86.
[517] Vgl. Williams, History of Computing, S. 339-341.

hatte. Beide publizierten u.a. eine Anzahl wissenschaftlicher Berichte über den IAS-Computer, der später als Muster einer Serie von Computern diente, der *Princeton Class*.[518]

7.5 US-Geheimdienste und Computerforschung

Die Erfahrungen mit kryptanalytischen (teil-)elektronischen Maschinen beeinflußten direkt oder indirekt die frühe Computerentwicklung, wie die vorangegangen Abschnitte zeigten. Eine womöglich noch größere Bedeutung hatten die geheimen Forschungen der US-Geheimdienste, die erst durch Dokumentefreigaben in den letzten Jahren bekannt wurden und die Nachkriegs-Dominanz der US-Computerindustrie begründeten: Diese Dienste erhielten bald nach Kriegsende große Summen für elektronische Entwicklungen, weil die Erfolge der Kryptanalytiker wesentlich zum Sieg der Alliierten beigetragen hatten. Und um weiter gefördert zu werden, demonstrierten die Dienste bei der Gründung der UNO im Sommer 1945, welche politischen Vorteile durch Kryptanalyse in Friedenszeiten zu erreichen sind – durch die Entzifferung des Nachrichtenaustauschs der Delegationen mit ihren Regierungen.[519]

Die Beschaffung sonstiger militärischer, diplomatischer und zunehmend wirtschaftlicher Informationen wurde nach dem Krieg fortgesetzt und intensiviert, überwiegend durch Entzifferung von Funksendungen. Denn immer mehr konnten erreicht werden: Die im Krieg entwickelte Richtfunktechnik ermöglichte den zügigen Ausbau von überregionalen Telefonnetzen, deren ahnungslose Nutzer im Vertrauen auf das Fernmeldegeheimnis Daten und Sprache offen übertrugen – und abgehört wurden. Die nicht informierten Regierungen verwendeten meist Chiffriermaschinen, darunter geschenkte Rotormaschinen (ENIGMA, TYPEX), deren „Knacken“ für die dazu bestens ausgerüsteten US-Geheimdienste Routine war. Allerdings scheint die zunehmende Masse der abgehörten Sendungen zu Kapazitätsproblemen geführt zu haben: Der Bau immer leistungsstärkerer kryptanalytischer Maschinen nach dem Krieg ist vermutlich die Folge davon.

Die massive Förderung der maschinellen Kryptanalyse ermöglichte Entwicklungen, an die in anderen Ländern mangels staatlicher Unterstützung nicht zu denken war, und im Endergebnis den USA einen uneinholbaren Vorsprung im Bau leistungsstarker Computer sicherte. BAMFORD formuliert das so: „Die Geschichte des modernen Codeknackens und die Geschichte des Computers decken sich zum großen Teil. [Und]: „... in der Entwicklung des

[518] Vgl. Lee, J.A.N.: International Biographical Dictionary of Computer Pioneers. Fitzroy Dearborn Publishers, Chicago, London, 1995, S. 326.
[519] Vgl. Bamford, NSA, S. 727.

Computers war und ist ihre [der NSA und deren Vorgängerdienste] Bedeutung noch immer kaum zu überschätzen."[520]
Diese Geheimdienste interessierten sich freilich nicht für wissenschaftliche Forschungen, sondern verlangten für die bewilligten Summen leistungsfähigere kryptanalytische Maschinen, d.h. zunächst Verbesserungen des vorhandenen Bestandes:

7.5.1 monogram-program

Nach Kriegsende sollten die Geheimdienste die Entzifferungsarbeit mit leistungsstärkeren Maschinen fortsetzen, wofür einflußreiche staatliche Auftraggeber sorgten, und planten deshalb, die im Krieg bewährten elektromechanischen Maschinen mit digitaler Elektronik und Magnetband-speichern aufzurüsten, um deren Arbeit wesentlich zu beschleunigen.

Das erste erfolgreiche Projekt nach diesem *monogram program* (Tarnbezeichnung) war der Bau des COMPARATOR, einer Spezialmaschine für kryptanalytische Zählprozesse („Koinzidenzzählung"). Dieses Projekt hatte bereits vor dem Krieg der Erbauer des *differential analysers* V. BUSH versucht, scheiterte jedoch, auch mangels Unterstützung durch seine Vorgesetzten.[521]
An die Konstruktion einer Super-BOMBE, Gegenstück zum britischen COLOSSUS, dachte man ebenfalls. Diese, und ähnliche andere zweckgebundene Projekte entsprachen den Vorstellungen der Auftraggeber ebenso wie denen der Entwickler, die an einen programmierbaren Computer damals nicht dachten, vermutlich aus Unkenntnis.

7.5.2 Pendergrass-Report

Um sich über den aktuellen Stand zu informieren, entsandte der Cheftechniker des US-Navy-Dienstes OP-20-G, H. ENGSTROM, seinen Mitarbeiter PENDERGRASS zu den Sommerseminaren an der *Moore School*. Überdies war die US-Navy – wie bereits erwähnt – einer der „Sponsoren" dieser Seminare.
PENDERGRASS begeisterte sich dort für V. NEUMANN'S Ideen, und dachte, eine Universalmaschine könnte nahezu alle kryptanalytischen Aufgaben mindestens ebenso gut lösen wie die vorhandenen, nach dem *monogram program* aufzurüstenden Spezialmaschinen. Daher wollte er die Navy überzeugen, dem OP-20G eine eigene Version der geplanten IAS-Maschine V. NEUMANN'S zu bewilligen.
Er verfaßte dazu einen Report[522], in welchem er detailliert ausführte, wie auch die verbesserten kryptanalytischen Verfahren der geplanten *monogram*-Geräte

[520] Vgl. Bamford, NSA, S. 728.
[521] Vgl. Bauer, Geheimnisse, S. 342.
[522] Vgl. Burke, Colin: An Introduction to an Historic Computer Document: The Pendergrass Report – Cryptanalysis and the Digital Computer. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XVII, Nr. 2, April 1993, S. 361-369.
(Der ausführliche Bericht wurde erst vor wenigen Jahren in Teilen freigegeben).

von einer IAS-Maschine effizient ausgeführt werden könnten. Besonders begründete er überzeugend, daß die wichtigsten Kryptanalysen des Weltkriegs funktionieren würden, und wie deren Programmierung zu gestalten sei. Statt wie bisher eine Vielzahl von speziellen kryptanalytischen Geräten einzusetzen, und diese nach dem *monogram program* aufzurüsten, empfahl PENDERGRASS die Entwicklung eines elektronischen Universal-Computers (*general purpose electronic computer*). Er zeigte mit ausführlicher Begründung, daß eine solche Maschine alle wichtigen kryptanalytischen Aufgaben lösen kann. Doch die Navy-Führung ließ sich nur mühsam davon überzeugen, daß eine so aufwendige Entwicklung zweckmäßig wäre, da ja die vorhandenen Geräte im Krieg sich bewährt hatten und aktuell ausreichten. Überdies waren – aus Sicht der Marinebefehlshaber – Versuche der Experten in den frühen 30er Jahren gescheitert, elektronische *rapid analytical machines* zu entwickeln, darunter das erwähnte Projekt BUSH'S. Daß dafür nicht technische Probleme verantwortlich zu machen waren, sondern die halbherzige Unterstützung eben dieser Befehlshaber und bürokratische Schwierigkeiten, das freilich konnte nicht vermittelt werden.

Nach Kriegsbeginn standen endlich genügend Mittel für diese elektronischen *rapid analytical machines* zur Verfügung, jedoch mußten nun schnell Ergebnisse mit speziellen Maschinen erzielt werden, für längerfristige Projekte blieb keine Zeit. Die Forschungsgruppe des OP-20-G unter WENGER und ENGSTROM ging daher den Weg des geringsten Widerstandes und beschränkte sich auf bekannte und erprobte elektromechanische Technik, mit der rasch ausreichend leistungsfähige Maschinen gebaut werden konnten. Auch die nach britischem Vorbild von DESCH konstruierte US-BOMBE folgte diesen Vorgaben, denn deren digitale Zähl- und Speicherelektronik beschleunigte zwar die Maschine, war aber kein Rechnersystem.
Noch strenger verpflichtete die US-Army die Entwicklungsgruppen ihres SIS, und forderte für kryptanalytische Maschinen ausschließlich betriebssichere Relaistechnik.[523]

Die Risiken dieses Weges waren den Verantwortlichen durchaus bekannt: Er erforderte immer kompliziertere und teurere Maschinen, die schon nach relativ geringen Änderungen der Kryptographie des Gegners nutzlos werden konnten. Eine universale Maschine hingegen müßte man dann nur umprogrammieren, was aber erst durch PENDERGRASS' Report bekannt wurde.
Doch die Verantwortlichen sahen vermutlich diese Vorteile zunächst nicht und bestanden auf der Beibehaltung der Relaistechnik, denn diese Maschinen hatten sich im Dauereinsatz bewährt.

[523] SIS entwickelte bspw. in 1943 eine reine Relais-HochleistungsBOMBE X86003, als Gegenstück zur teilelektronischen Desch-BOMBE. Die Maschine war extrem teuer und wurde daher nur einmal gebaut.

7.5.3 ATLAS- und ABNER-Projekt

Nach vielen Bedenken akzeptierte die Navy PENDERGRASS' Vorschläge und unterstützte den Bau eines Universalcomputers, das ATLAS-Projekt.[524] Diese Maschine verfügte über einen Trommelspeicher mit einer für die damalige Zeit enormen Kapazität von 16.384 „*words*", und war als leistungsstarker Parallelrechner konzipiert.[525] Der Entwurf wurde mehrfach geändert und dann in 1950 fertiggestellt durch die *Engineering Research Associates* (ERA), Diese bestand im Kern aus ehemaligen OP-20-G-Mitarbeitern, darunter dem Cheftechniker ENGSTROM, und wurde bereits 1946 gegründet. Sie konstruierte auf privater Basis nicht nur kryptanalytische Computer (ATLAS I und II) sondern auch erste kommerziell nutzbare Maschinen: Die ERA ging später in der Gesellschaft REMINGTON RAND auf, die deren Projekte übernahm.[526]
Zur ERA kam auch der Ingenieur S. CRAY, der sich später (1970) selbstständig machte, und die bei der ERA gesammelten Erfahrungen bei der Entwicklung der CRAY-Hochleistungsrechner verwertete. Die ersten Geräte lieferte er 1976 für die NSA, die damit über die damals leistungsstärksten [kryptanalytischen] Rechner der Welt verfügte.[527]

Der Konstrukteur der US-Bombe J. DESCH trat der ERA nicht bei, sondern nahm nach dem Krieg seine Forschungen wieder auf. Zusammen mit seinem Partner MUMMA meldete er 1946 ein Patent für einen elektronischen Rechner an, wonach der Computers NCR-304 entwickelt wurde.[528]

Der SIS der Army – inzwischen umbenannt in ASA (*Army Security Agency*) – erhielt ebenfalls den PENDERGRASS-Report, und dessen Entwickler äußerten sich in gleicher Weise begeistert. Das Mißtrauen der Army-Führung gegen ein Universalcomputer-Projekt war jedoch immer noch groß, konnte nicht so rasch überwunden werden, und so bewilligte sie, viel später als der OP-20-G, die Entwicklung des Computers ABNER 1, wie das Projekt genannt wurde. Demzufolge ging die Maschine erst 1952 in Betrieb, war aber dann „der technisch ausgereifteste Computer seiner Zeit".[529]

7.5.4 Die Gründung der NSA

Die Erfahrungen des Zweiten Weltkriegs hatten gezeigt, daß die Rivalitäten zwischen den beiden wichtigsten militärischen US-Geheimdiensten, nämlich dem SIS der Army und dem OP-20-G der Navy, zu unnötigen Doppelentwicklungen

[524] Nicht zu verwechseln mit dem späteren (1962) ICL-„Atlas"Computer in GB.
[525] Vgl. Bamford, NSA, S. 730-731.
[526] Vgl. Lee/Burke/Anderson: The US Bombes, S. 8-9
[527] Ebd. S. 741-743.
[528] Vgl. Lee/Burke/Anderson: The US Bombes, S. 14.
[529] Bamford, NSA, S. 732.

und Verzögerungen von Projekten führten. Auch nach dem Krieg konnten diese Rivalitäten nicht abgebaut werden, obwohl man zu deren Überwindung eigens die AFSA gründete, die *Armed Forced Security Agency*, an der alle Teilstreitkräfte beteiligt waren. Diese blieben jedoch in ihrem Bereich souverän und eine zentrale Koordination fehlte. Der Koreakrieg offenbarte dann die gravierenden Mängel dieser Organisation. Hinzu kamen Spionageerfolge der Sowjetunion, die über Agenten in der AFSA verfügte, welche die Entzifferungen sowjetischer Nachrichten nach Moskau meldeten. Daraufhin änderte der sowjetische Geheimdienst die sowjetischen Chiffriersysteme so radikal, daß die AFSA nicht mehr entziffern konnte. Die Lage wurde so schlimm, daß ein Untersuchungsausschuß des US-Senates eingesetzt wurde, der dann die politisch Verantwortlichen ersuchte, die AFSA aufzulösen und eine neue geheime zentrale Organisation zu gründen. Diese NSA, die *National Security Agency*, entstand 1952; deren Etat wurde geheim bewilligt und die Öffentlichkeit nicht informiert.[530]

Die Gründung der NSA ist auch informatikhistorisch bedeutsam, denn sie förderte und fördert weiterhin die Entwicklung kryptologischer Hochleistungscomputer. Mit den dabei gewonnen Erfahrungen bauten und bauen dann die Entwicklerfirmen kommerzielle Computer. Das sicherte und sichert den USA einen uneinholbaren Vorsprung nicht nur auf allen kryptologischen Gebieten, sondern ebenso in der kommerziellen und wissenschaftlichen Computerentwicklung.

[530] Vgl. Burke, Colin: An Introduction to an Historic Computer Document: The Pendergrass Report.

8 Maschinelle Kryptologie und Informatik

In der Literatur zu den Wurzeln der technikwissenschaftlichen Disziplin Informatik findet man viele Beispiele für Entwicklungen, aus denen die Informatik sich schließlich herausbildete. Darunter auch die Digitalelektronik, doch ohne jeden Hinweis darauf, wie aus Experimentierschaltungen betriebsfähige Großsysteme entstanden. Scheinbar betrachtete man das als „normale“ Weiterentwicklung.

8.1 Digitalelektronik als Grundlage

Die in den vorhergehenden Kapiteln geschilderten Erfahrungen aus der maschinellen Kryptologie beeinflußten demnach die Entstehung des Computers, denn dessen technische Grundlage, die Digitalelektronik, wurde dabei erstmals in betriebssicheren Großschaltungen erprobt. Man kann freilich darüber spekulieren, ob ohne diese kriegsbedingt forcierte Entwicklung und Anwendung elektronischer Digitalkomponenten geeignete Hardware erst viele Jahre später zur Verfügung gestanden hätte. Ebenso darüber, ob ohne die geheime Nachkriegsentwicklung kryptanalytischer Computer bald kommerzielle Maschinen lieferbar gewesen wären. Festzuhalten bleibt, daß ohne die Erprobung von elektronischen Digitalsystemen in kryptanalytischen Maschinen der Bau von Computern längere Zeit sich auf die bewährte Relaistechnik hätte stützen müssen, mit dem Ergebnis, daß die elektronische Speichertechnik zunächst nicht anwendbar gewesen wäre. Somit hätte man nur Rechner bauen können, aber keine Computer.

Die Informatik konnte sich aber erst dann herausbilden, als speicherprogrammierbare Rechner zur Verfügung standen, die „richtigen“ Computer: Denn nun trat zur reinen Rechnerfunktion die informationelle Komponente hinzu, nämlich die „Software“: Diese Komponente bot eine neue Qualität der Informationsverarbeitung, denn ein Rechner konnte nur nach einem festen Algorithmus das verarbeiten, was von den Anwendern jeweils eingegeben wurde. Ein digitaler Speicher hingegen ermöglichte die logische Verarbeitung von Programmteilen und Zwischenwerten entsprechend einer Software mit den dazu erforderlichen komplexen Algorithmen.

8.2 wissenschaftliche Kontroversen

In der Literatur findet man kontroverse Meinungen zu theoretischen Grundfragen der Informatik, die auch heute noch nicht ausdiskutiert sind. Das ist vermutlich eine Folge der kurzen Geschichte dieser Disziplin, die überdies geprägt ist durch einen komplexen Aufbau: Sie besteht aus sehr gegensätzlichen Elementen, wie beispielsweise Technik (Hardware) und Nichttechnisches (Software). Das zu integrieren erfordert eine Synthese aus ingenieur- und geisteswissenschaftlichen Denkweisen, die, wie die Wissenschaftsgeschichte zeigt, stets problematisch war und ist. Darüber hinaus wirkten im Verlauf der Genese der Disziplin vielfältige Einflüsse aus anderen Wissensgebieten ein, deren Zuordnung keineswegs immer eindeutig ist, und dementsprechend unterschiedliche Meinungen zur Folge hatten und haben.
Besonders die Definitionsfragen lösten in der einschlägigen Literatur zahlreiche Debatten aus, wobei es vorwiegend um das wissenschaftliche Selbstverständnis der noch jungen Disziplin ging. Namhafte Autoren reklamierten zunächst die Informatik als Geisteswissenschaft, beispielsweise bezeichnete BAUER in 1974 Informatik als „Ingenieur-Geisteswissenschaft“, ebenso ZEMANEK, der sie 1971 eine „Ingenieurwissenschaft für abstrakte Objekte“ nannte. Diese, und ähnliche Meinungen wurden besonders in den 60er/70er Jahren des vergangenen Jahrhunderts vertreten. In den 80er Jahren setzte ein Umdenken ein und es wurde beispielsweise vom erwähnten Autor BAUER dezidiert geäußert: „Die Informatik ist eine Ingenieurwissenschaft.“[531]

Doch die teilweise strittigen Diskussionen setzten sich fort, mitunter ergänzt durch soziologische, gar ideologisch beeinflußte Ansichten. Beispielsweise wurde in den USA in Hinblick auf die Entwicklung großer Systeme der Informationsverarbeitung gefragt, was daran überhaupt wissenschaftlich sei, „...ob es sich dabei nicht vielmehr um ein reines Handwerk handle...“ Die Autoren stellen jedoch dezidiert fest, daß das „... zweifellos eine Ingenieurdisziplin ist...“, verweisen jedoch auf die „... heute noch unzureichende wissenschaftliche Basis ...“ [532]

Möglicherweise sind diese Beiträge inzwischen überholt, doch hier kann und soll diese theoretische Diskussion nicht fortgeführt werden. Vielmehr könnten die geschilderten Erfahrungen der maschinellen Kryptologie und ihrer Folgewirkung mehr zu den wichtigeren praktischen Aspekten dieser Diskussion beitragen. Denn:
Es geht bei diesen Debatten keineswegs nur um akademische Fragen, wie man meinen könnte, denn daraus resultieren durchaus praktische Konsequenzen,

[531] Bauer, Friedrich L.: Informatik und Informationstechnik – ein Gegensatz? Vortrag 1987, in: Informatik-Spektrum (1988) 11, S. 231-232.
[532] Broy, Manfred und Schmidt, Joachim: Informatik: Grundlagenwissenschaft oder Ingenieurdisziplin? In: Informatik-Spektrum 22 (1999), S. 206-207.

etwa wo in der Ausbildung von Informatikern die Schwerpunkte zu setzen sind. Mithin ist es nicht überraschend, daß diese Fragen auch heute noch Gegenstand einer „endlosen Diskussion“ sind.[533]

8.3 Wissenschaft und Ingenieurwesen

Im 19. Jahrhundert behinderte die Dominanz der Geistes- und Naturwissenschaften die Herausbildung der Ingenieurwissenschaften. Man sollte meinen, die seither rasanten Fortschritte der Technik hätten diese Auseinandersetzungen bis heute endgültig beendet. Doch, wie vorstehend erwähnt, veranlaßte die Entwicklung der Informatik manche Wissenschaftler zu einer erneuten Diskussion dieser Fragen. Das scheint entbehrlich zu sein, bietet doch beispielsweise die maschinelle Kryptologie zahlreiche Beispiele für herausragende wissenschaftlich-technische Leistungen, die nur erreicht wurden durch intensive Zusammenarbeit von Wissenschaftlern und Ingenieuren. Aber darin zeigt sich auch die Komplexität der Informatik, nämlich der Dualismus aus Informationellem und Technischem. Die nachstehenden Beispiele zeigen aber auch sehr deutlich, wie nur gemeinsam beide Teile das maximal Mögliche erreichen konnten.

8.3.1 Die Bedeutung der Ingenieure

Aufgabe der Ingenieure war es, die meist mathematisch analysierten Algorithmen der Chiffriermaschinen in kryptanalytische Maschinen zu implementieren. Dazu mußten sie unter kriegsbedingtem Zeit- und Erfolgsdruck Geräte konstruieren und bauen, für die es kaum Erfahrungen gab, und auch keine Zeit für Versuche blieb. Darüber hinaus sollten die Maschinen auch noch möglichst schnell arbeiten, einem Dauerbetrieb standhalten, und das bei Bedienung durch angelernte Hilfskräfte. Diese enormen Leistungen findet man in der Literatur traditionell kaum gewürdigt, denn vermutlich kann sich ein Nicht-Ingenieur kaum die Schwierigkeiten vorstellen, die dabei zu überwinden waren. Allerdings muß man hierzu leider ergänzen: Die Ingenieure waren und sind selbst mit schuld an dieser Nichtbeachtung. Denn nahezu alle relevanten Berichte stammen von Historikern oder Wissenschaftsjournalisten, einige auch von Politikern und Militärs, und diesen Autoren kann man mangelndes Verständnis für die Leistungen der Ingenieure kaum vorwerfen. Diese publik zu machen, wäre Aufgabe der Ingenieure selbst, wie es beispielsweise Konrad ZUSE mit seinen ausführlichen und interessanten Berichten erreichte.

[533] Vgl. Endres, Albert: Die Informatik als Ingenieurwissenschaft. In: Informatik Spektrum 22 (1999), Heft 6.

KONRAD ZUSE – die Ausnahme

Obwohl ZUSE keinen Bezug zur Kryptologie hatte, wird sein Name gelegentlich genannt im Zusammenhang mit Kryptanalyse, weil er angeblich dafür eine elektronische Version seiner Z3 bauen wollte. Diese und andere Legenden wurde längst widerlegt.[534]
ZUSE war zwar Ingenieur-Erfinder, aber auch sein eigener wissenschaftlicher Berater. Er studierte dazu beispielsweise mathematische Grundlagen der Rechnerfunktionen, und gelangte so zum damals alles andere als selbstverständlichen Binärsystem mit Gleitkommadarstellung für seine selbstgebauten Rechner. Er verkörperte mithin die Synthese aus Wissenschaft und Technik in seiner Person, und war wohl auch aus diesem Grund sehr erfolgreich, trotz begrenzter Möglichkeiten.

SCHERBIUS und KORN – die andere Ausnahme

Das genaue Gegenteil demonstrierte die Entwicklung der ENIGMA: Die Erfinder hatten die Maschine empirisch entwickelt, doch es fehlten ihnen elementare kryptologische Kenntnisse. Und diese verschafften sie sich auch nicht, vermutlich weil ihnen diese Wissenschaft unbekannt war. Dementsprechend glaubten sie (und ihre Abnehmer wohl ebenso), die theoretisch ermittelte große Zahl der Schlüsseleinstellungen der ENIGMA würde deren Sicherheit ausmachen.

Der promovierte Elektroingenieur SCHERBIUS war zwar wissenschaftlich gebildet, jedoch kryptologischer Laie. So konnte er die Schwächen seiner Maschine nicht erkennen, auch nicht als sein Mitarbeiter, der Entwicklungsingenieur W. KORN, 1926 auf die vermeintlich schlaue Idee kam, mit einer Umkehrwalze die ENIGMA leichter bedienbar und gleichzeitig sicherer zu machen. Ersteres gelang – man konnte nun mit gleicher Walzeneinstellung chiffrieren und dechiffrieren, aber das zweite Ziel verfehlte man völlig: KORN und SCHERBIUS glaubten wohl, ebenso wie die interessierten Militärs, durch den nun zweimaligen Stromdurchgang durch die Walzen die Chiffrierung entsprechend zu verstärken. Aber damit erreichten sie das Gegenteil: Die Maschine wurde infolge der Hin- und Rückleitung des Stromes kryptologisch reziprok, d.h. Chiffrierung und Dechiffrierung erfolgten bei gleicher Einstellung, und das erleichterte später den Kryptanalytikern sehr die Arbeit.

Auch spätere Änderungen der ENIGMA deuten nicht auf kryptologischen Sachverstand, so wurde etwa das Steckerbrett der Wehrmachts-ENIGMA so gestaltet, daß die Reziprozität der Maschine erhalten blieb.
SCHERBIUS und KORN entwickelten und bauten demnach eine zwar elektromechanisch hervorragende Maschine, doch deren problematische Sicherheit erkannten sie nicht. Überdies schwächten sie später sogar deren kryptologische

[534] Vgl. Bauer, Friedrich L.: Konrad Zuse – Fakten und Legenden. In: Rojas, R. (Hrsg.): Die Rechenmaschinen von Konrad Zuse, S. 18-19.

Stärke mangels wissenschaftlicher Beratung. Es war ein Musterbeispiel für fehlende technisch-wissenschaftliche Zusammenarbeit.

Rejewski und Palluth

Dem polnischen Kryptologen REJEWSKI gelang als erstem die mathematische Analyse der ENIGMA, die es ihm ermöglichte, einen Entzifferungs-Algorithmus zu entwickeln und die unbekannte militärische ENIGMA I zu rekonstruieren. Doch diese hervorragende Leistung allein genügte nicht, für Entzifferungen größerer Textmengen benötigte er technische Unterstützung, denn die ermittelten Algorithmen konnten nur mit geeigneten Geräten sinnvoll genutzt werden, wofür er einen versierten Konstrukteur benötigte. Diese Aufgabe übernahm der Ingenieur PALLUTH, Mitarbeiter der AVA-Rundfunkwerke in Warschau, und baute als erstes eine ENIGMA I nach REJEWSKIS Angaben. Dann folgte Konstruktion und Bau des CYCLOMETERS, einer kryptanalytischen Hilfsmaschine. Schließlich gelang ihm sein Meisterstück mit Konstruktion und Bau der BOMBA, der ersten leistungsfähigen kryptanalytischen Maschine, an der besonders der Antrieb der ENIGMA-Rotorsätze durch ein Planetengetriebe beeindruckt.

Diese Leistungen sind bemerkenswert, weil PALLUTH'S Arbeitgeber AVA nur Radios und Funkgeräte herstellte, und er und seine Arbeitsgruppe keine elektromechanischen Erfahrungen besaß. Doch PALLUTH war nicht nur Ingenieur, sondern – eine rare Ausnahme – er verfügte auch über kryptologische Kenntnisse: Er hatte bis ca. 1930 als ziviler Kryptologe für den Geheimdienst BS4 gearbeitet, und gehörte zu den Dozenten, die REJEWSKI und dessen Kollegen bei deren Vorbereitungskurs unterrichtet hatten.

Turing und Keen

Auch ein mathematisches Genie wie TURING benötigte einen Ingenieur, der seine Arbeitsergebnisse in eine leistungsfähige Maschine umsetzen konnte: Den Auftrag zum Bau seiner BOMBE erhielt die *British Tabulating Machine Co*. (BTM), die einschlägige Erfahrung beim Bau von elektromechanischen Geräten besaß, nämlich Lochkarten- und Tabelliermaschinen. Der Leiter der BTM-Entwicklungsabteilung, Harold KEEN, erklärte sich bereit, den schwierigen Entwicklungsauftrag zu übernehmen, obwohl TURING'S BOMBE weit höhere Anforderungen als bisher gewohnt stellte: Beispielsweise waren ca. 100 Rotoren elektrisch unterbrechungsfrei abzutasten, mit je 26 Kontakten, wofür es keine Erfahrungen gab. Deren mechanischer Antrieb über spezielle Getriebe mußte die zykloide Bewegung der ENIGMA-Rotoren nachbilden, und zwar für 36 ENIGMA-Rotorsätze je Maschine. Dazu kamen zahlreiche Relais zur Programmsteuerung und eine umfangreiche Verkabelung. Und, nicht zuletzt, es sollten die Konstruktions- und Bauarbeiten innerhalb kürzester Zeit erfolgreich abgeschlossen sein, denn Zeit für ein eigentlich erforderliches Versuchsprogramm wurde nicht bewilligt.

Welche Meisterleistung KEEN und seine Gruppe erbrachten, und das in knapp fünf Monaten, zeigt sich derzeit bei dem Versuch, für das Museum Bletchley Park eine solche Maschine zu rekonstruieren. Die Probleme konnten bis jetzt – nach über drei Jahren – noch nicht vollständig gelöst werden.

NEWMAN/ TUTTE und FLOWERS

Tommy FLOWERS herausragende Ingenieurleistungen wurden bereits in vorigen Abschnitten dargelegt. Er implementierte nicht einfach nur die Algorithmen, welche die beiden Wissenschaftler NEWMAN und TUTTE erarbeitet hatten – ohnehin eine sehr anspruchsvolle Aufgabe – sondern baute dazu eine völlig neue *vollelektronische* Maschine, den COLOSSUS. Vermutlich war er auch der Einzige, der zu dieser Zeit dazu in der Lage war, denn er hatte als Erster bereits erfolgreich elektronische Großschaltungen mit Röhren gebaut, nämlich Telefonvermittlungen, die sich im Dauerbetrieb bewährt hatten. Dazu hatte er eine neue Betriebsweise der Röhren entwickelt und die damit erreichte Betriebssicherheit elektronischer Digitalschaltungen demonstriert, mithin die Voraussetzung zum Bau elektronischer Rechner geschaffen.
Diese auch informatikhistorisch bedeutsame Leistung fand damals leider nicht die gebührende Anerkennung, und erst im hohen Alter erhielt er wenigstens die Ehrendoktorwürde dafür zuerkannt. Nach dem Krieg setzte er seine Arbeit als Postingenieur fort, ohne auch nur ein Wort über seine Leistungen zu verlieren.
Die beiden Wissenschaftler NEWMAN und TUTTE hingegen wurden ob ihrer Verdienste auf bedeutende Lehrstühle berufen und mit hohe Auszeichnungen dekoriert.

8.3.2 Ingenieure und Informatik

Man kann die vorstehend beschriebenen Beispiele zur Unentbehrlichkeit der Ingenieure freilich nicht ohne weiteres auf die heutigen Verhältnisse übertragen. Gleichwohl stellt sich die Frage, ob ingenieurmäßiges Arbeiten nicht mindestens auf Teilgebieten der Informatik angebracht, ja notwendig ist. So offenbaren beispielsweise die zunehmenden Anwenderprobleme mit immer komplexerer Software einen Mangel an praktischen Fähigkeiten der Entwickler, die sich scheinbar wenig Gedanken über die Probleme der Anwender machen bzw. diese nicht erkennen. Aber genau das waren und sind die Stärken des ingenieurmäßigen Arbeitens, nämlich dem Anwender ein gut und zuverlässig funktionierendes Gerät/System zur Verfügung zu stellen, zu dessen Bedienung nicht immer wieder Expertenwissen benötigt wird. Die beschriebenen Beispiele zeigen eindrücklich, wie selbst unter extremen Bedingungen im Krieg die genannten Ingenieure diese Tugenden demonstrierten.
Die Frage, ob und wie diese Fähigkeiten im Informatikstudium entwickelt werden können und sollen, kann hier freilich nicht diskutiert werden. Sie ist Teil der strittigen, leider sehr theoretischen Auseinandersetzung, die bereits angesprochen wurde.

Festzuhalten bleibt als Ergebnis, daß im Rahmen der maschinellen Kryptologie nur die Synthese aus Wissenschaft und Ingenieurwesen überzeugende Erfolge hervorbrachte, und vermutlich unter den heutigen Verhältnissen ebenso bringen würde.

9 Quellenverzeichnis

9.1 Literatur

BAMFORD, James: *NSA - Die Anatomie des mächtigsten Geheimdienstes der Welt.* Dt. Ausgabe, München 2001. Üb.: Bonn, Dierlamm, Ettinger u. Maass. Orig.: Body of Secrets, New York (NY) 2001.

BARTH, R. und BEDÜRFTIG, F.: Taschenlexikon Zweiter Weltkrieg. München 2000.

BAUER, Friedrich L.: *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie.* Berlin ^{3}2000. Engl. Ausgabe: *Decrypted Secrets: Methods and Maxims of cryptology.* Berlin, Heidelberg, New York (NY) ^{3}2002.

BAUER, Friedrich L.: *Informatik und Informationstechnik – ein Gegensatz?* In: Informatik-Spektrum 21 (1998), S 85.

BAUER, Friedrich L.: *Wer erfand den von-Neumann-Rechner?* Vortrag 1987, in: Informatik-Spektrum (1988) 11.

BAUER, Friedrich L.: *Scherbius und die ENIGMA*. Informatik-Spektrum (1991) 14.

BAUER, Friedrich L.: *Konrad Zuse – Fakten und Legenden.* In: Rojas, R. (Hrsg.): *Die Rechenmaschinen von Konrad Zuse,* Berlin u.a.O. 1998.

BLOCH, Gilbert: *ENIGMA before ULTRA – Polish Work and the French Contribution.* (Transl. by Deavours, C.A.). In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XI, Nr. 3, July 1987, Artech House, Norwood MA/USA, 1998.

BRENNECKE, Jochen: *Die Wende im U-Boot-Krieg*. Ursachen und Folgen 1939-1943, Augsburg 1995.

BROY, Manfred und SCHMIDT, Joachim: *Informatik: Grundlagenwissenschaft oder Ingenieurdisziplin?* In: Informatik-Spektrum 22 (1999), S. 206.

BURKE, Colin: *An Introduction to an Historic Computer Document. The Pendergrass Report – Cryptanalysis and the Digital Computer.* In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XVII, Nr. 2, April 1993, Artech House, Norwood MA/USA, 1998.

COPELAND, Jack B.: *Colossus and the Dawning of the Computer Age*. In: Erskine, Ralph and Smith, Michael (Eds.): *Action this Day*. Bantam Press, London u.a. Orte, 2001.

CRAWFORD, David J.: *The Autoscritcher and the Superscritcher*, in: IEEE Annals of the History of Computing, July-September 1992, Vol. 14, No. 3, pp. 9-22.

DAVIES, Donald: *The Lorenz Cipher Machine SZ42*. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIX, Nr. 1, January 1995, Artech House, Norwood MA/USA, 1998.

DEAVOURS, C.A./KRUH, L.: *The Turing Bombe: Was it enough?* In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIV, Nr. 4, October 1990, Artech House, Norwood MA/USA, 1998.

DEAVOURS, C.A./KRUH, L.: Machine Cryptography and modern Kryptanalysis, Artech House, Norwood MA/USA, 1995.

DONINI, Luigi: *The Cryptographic Services of the Royal (British) and Italian Navies*. Transl. by Buonafalce, A. (Orig. in: Rivista Marittima, Rom, Jan. 1983). In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIV, Nr. 2, April 1990, Artech House, Norwood MA/USA, 1998.

ECKERT, Claudia: *IT-Sicherheit*. München 2003.

ENDRES, Albert: *Die Informatik als Ingenieurwissenschaft*. In: Informatik Spektrum 22, Heft 6, Dez. 1999.

ERSKINE, Ralph: *Enigma's Security: What the Germans Really Knew*. In: Erskine, Ralph and Smith, Michael (Eds.): *Action this Day.* Bantam Press, London u.a.O., 2001.

ERSKINE, Ralph: Der Krieg der Code-Brecher. In: Akademie aktuell Nov. 2002, Zeitschrift der Bayerischen Akademie der Wissenschaften. Übers.: J. Müller. Ergänzt und bearbeitet von F.L. Bauer.

ERSKINE, R. and FREEMAN, P.: *Brigadier John Tiltman: One of Britain's finest Cryptologists*. In: Cryptologia, Vol XXVII (4), Oct 2003.

ERSKINE, Ralph: *The Development of Typex.* In: Kapera, Z.J (Ed.): The Enigma-Bulletin N° 2 - May 1997.

GELLERMANN, Günther: *...und lauschten für Hitler*. Bonn 1991.

GLÜNDER, G.: *Wireless and „Geheimschreiber" Operator in the War 1941-1945*. In: Cryptologia, Vol XXVI (2), April 2002.

GUSTAFSON, John: *Reconstruktion of the Atanasoff-Berry-Computer*. In: Rojas, R./Hashagen, U. (Eds.): *The First Computers: History and Architectures*. MIT Press, Cambridge MA/USA und London, 2000.

HAGELIN, Boris C.W.: *The Story of the Hagelin Cryptos*. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, Artech House, Norwood MA/USA, 1998.

HAMER, D.H.: *G-312: An Abwehr Enigma*. In: Cryptologia; Volume XXIV (1); Jan 2000; pp. 41-54.

HAMER, D.H.: *Enigma: Actions involved in the „double stepping" of the middle rotor*. In: Cryptologia; Volume XXI (1); Jan 1997.

HAMER, D.H., SULLIVAN, G., WEIERUD, F.: *Enigma Variations. An Extended Family of Machines.* In: Cryptologia; Volume XXII (3); July 1998; pp. 211-229.

HINSLEY, F.H., THOMAS, E.E., RANSOM, C.F.G. and KNIGHT, R.C.: *British Intelligence in the Second World War: Its Influence on Strategy and Operations.* 5 vols. London 1991.

HINSLEY, F.H.: *An Introduction to Fish*. In: Hinsley, F.H. and Stripp,A (Eds.):*Codebreakers. The inside story of Bletchley Park*. Oxford (GB) 1993.

HODGES, Andrew: *Alan Turing, The Enigma*. US-Edition by Walker Publishing, New York (NY), [2]2000.

HUSKEY, Harry D.: *Hardware Components and Computer Design*. In: Rojas, R./Hashagen, U. (Eds.): *The First Computers: History and Architectures*. MIT Press, Cambridge MA/USA und London, 2000.

IBING, Hans K.: Blick in das Fernmeldewesen. Köln/Krefeld 1949.

KAHN, David: *The Codebreakers.* The Story of Secret Writing. New York (NY) [2]1996.

KAHN, David: *In Memoriam: G.J. Painvin*. In: Deavours, Cipher A. et al. (Eds.): C*ryptology – machines, history and methods*. Artech House, Norwood MA/USA, 1989.

KAHN, David: *Seizing the Enigma: The Race to Break the German U-Boat-Codes, 1939-1943*. Houghton Mifflin, Boston MA/USA, 1991.

KISTERMANN, F.: *The Dehomag D11 Tabulator.*
In: Rojas, R./Hashagen, U. (Eds.): *The First Computers: History and Architectures*. MIT Press, Cambridge MA/USA und London, 2000.

LEE, J.A.N.: *International Biographical Dictionary of Computer Pioneers*.
Fitzroy Dearborn Publishers, Chicago, London, 1995.

LEEUW, Karl de: *The dutch invention of the rotor machine, 1915 - 1923*.
Cryptologia 27 (2003).

LEIBERICH, Otto: *Vom diplomatischen Code zur Falltürfunktion.* Hundert Jahre Kryptographie in Deutschland. In: Spektrum der Wissenschaft 4/2001. Verlagsgesellschaft Heidelberg 2001.

MACHE, W. (Hrsg.): *Lexikon der Text und Daten-Kommunikation.*
München, Wien [3]1993.

MACHE, W.: *Der Siemens-Geheimschreiber – ein Beitrag zur Geschichte der Telekommunikation*. Archiv für deutsche Postgeschichte 1991.

MACHE, W.: *The Siemens Cipher Teletype in the History of Telecommunicationes*. In: Deavours, Cipher A. et al. (Eds.), Selections from Cryptologia, Volume XIII, Nr. 2, April 1989, Artech House, Norwood MA/USA, 1998.

MARTIN, Ernst: *Die Schreibmaschine und ihre Entwicklungsgeschichte*.
Aachen [8]1949.

MAUCHLY, J.W.: *The Use of high speed vacuum tube devices for calculating*, Moore School of El. Eng., University of Pennsylvania, 1942. (Privately circulated Memorandum).

MILITÄRGESCHICHTLICHES FORSCHUNGSAMT (Hrsg.): *Das Deutsche Reich und der Zweite Weltkrieg*. 7 Bände, Stuttgart 1993-2001.

MOWRY, David P.: *German Cipher Machines of World War II*,
Center for Cryptologic History, National Security Agency 2003.

MOWRY, David P.: *Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire,* Cryptologic Quarterly, Vol. 2, Nos. 3-4,
Fall/Winter 1983-84, p 21-36.

MÜLLER, Otto: *Telegraphie*. In: Zipp, Die Elektrotechnik, Band 2, Berlin [6]1940.

NAUMANN, F.: *Vom Abakus zum Internet. Die Geschichte der Informatik*.
Darmstadt 2001.

NAUMANN, F.: *Informatik*. In: Buchheim, G. und Sonnemann, R.(Hrsg.): *Geschichte der Technikwissenschaften*. Berlin 1990.

RATCLIFF, R.A.: *Searching for Security: The German Investigations into Enigma's Security.* In: Alvarez, D. (Ed.): Allied and Axis Signals Intelligence in World War II. London, Portland OR 1999.

REJEWSKI, Marian: *Mathematical Solution of the Enigma Cipher*, (Translation by Kasparek, Ch.). In: Deavours, Cipher A. et al. (Eds.): C*ryptology – machines, history and methods*. Artech House, Norwood MA/USA, 1989.

ROHRBACH, Hans*: Chiffrierverfahren der neuesten Zeit*. In: Archiv der elektrischen Übertragung (A.E.Ü.), Heft 9 (1948), S. 362-369.

ROHRBACH, Hans: *Mathematische und Maschinelle Methoden beim Chiffrieren und Dechiffrieren*. In: Angewandte Mathematik I, S. 233-257, Wiesbaden1948. (ursprünglich: FIAT Review of German Science, 1945).

ROHWER, J. und HÜMMELCHEN, G.: *Chronik des Seekrieges 1939-1945*. Oldenburg/Hamburg (1968) [3]1992.

SALE, Tony: *The Colossus of Bletchley Park*. In: Rojas, R./Hashagen,U. (Eds.): The First Computers: History and Architectures. MIT Press, Cambridge MA/USA und London, 2000.

SMITH, Michael: *Enigma entschlüsselt.* München 2000. Übers. H. Dierlamm. Orig.: Station X. The Codebreakers of Bletchley Park. London 1998.

SCHNEIDER, H.J. (Hrsg.): Lexikon der Informatik und Datenverarbeitung. München 1991.

SCHREYER, Helmut: *Das Röhrenrelais und seine Schaltungstechnik*. Diss. TH Berlin 1941.

SELMER, E.S.: *The Norwegian Modification of the Siemens T52e*. In: Cryptologia, Vol XVIII (2), April 1994.

SHANNON, C.E.: *Communication Theory of Secrecy Systems.* In: Bell Systems Technical Journal 28, (1949), S. 656-715.

SHANNON, C. E.: *A symbolic analysis of relay and switching circuits*. In: Trans. AIEE, Vol. 57, 1938, p. 713-723.

SINGH, Simon: *Geheime Botschaften, München* 2000.
Orig.: „The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography", London 1999.

SMITH, B.F.: *New Intelligence Releases: A British Side to the Story*. In: Alvarez, D. (Ed.): Allied and Axis Signals Intelligence in World War II. London, Portland OR 1999.

SMITH, Michael: *Bletchley Park, Double Cross and D-Day*. In: Erskine, Ralph and Smith, Michael (Eds.): Action this Day. Bantam Press, London u.a. 2001.

SPIEGEL, Jan van der, et al.: *The ENIAC: History, Operation and Reconstruction in VLSI)**. In: Rojas, R./Hashagen, U. (Eds.): *The First Computers: History and Architectures*. MIT Press, Cambridge MA/USA und London, 2000.
)* VLSI = eine CMOS-Variante, mit deren Hilfe ENIAC auf einem Chip realisiert wurde.

TELTSCHIK, Walter: *Geschichte der deutschen Großchemie*. Weinheim 1992.

TÜRKEL, Siegfried: *Chiffrieren mit Geräten und Maschinen.* Graz 1927.

ULBRICHT, Heinz: *Uncle Dick and another Horrors of the Enigma*. In: The Journal of Intelligence History, Vol 1 (1), Summer 2001.

ULBRICHT, Heinz: *The Enigma-Uhr*. In: Skillen, Hugh (Ed.): The Enigma Symposium 2000. Bath 2000.

van der MEULEN, M.: *The Road to German Diplomatic Ciphers – 1919 to 1945*. In: Cryptologia, Vol XXII (2), April 1998.

WEGNER, Bernd: *Kriegsgeschichte- Politikgeschichte- Gesellschaftsgeschichte*. In: Rohwer, J. und Müller, H. (Hrsg.): Neue Forschungen zum Zweiten Weltkrieg. Weltkriegsbücherei Stuttgart, Band 28. Koblenz 1990.

WEIERUD, Frode: *Sturgeon, The Fish BP Never Really Caught*. Proceedings on Coding Theory and Cryptography, New York (NY) 2000.

WILLAMS, Michael R.: *A History of Computing Technology*, 2nd ed. IEEE Computer Society Press, Los Alamitos CA/USA, 1997.

WINTERBOTHAM, F.W.: *The Ultra Secret*, New York, Harper, 1974.

WYLIE, Shaun: *Breaking Tunny and the Birth of Colossus*. In: Erskine, Ralph and Smith, Michael (Eds.): *Action this Day.* Bantam Press, London u.a. Orte, 2001.

ZUSE, K.: *Entwicklungslinien einer Rechengeräte-Entwicklung von der Mechanik zur Elektronik*. In: Hoffmann, W. (Hrsg.), *Digitale Informationswandler,* Braunschweig 1962.

9.2 Internet-Quellen

ALEXANDER, C.H.O'D.: *Stecker Knock-Out.* In: Weierud, Frode (Ed.): Frodes Kryptopage, (Orig. internes BP-Dokument o.D., ca. März 1944).
Von: http://mad.home.cern.ch/frode , am 29.11.02.

BBC-Homepage: *Tommy Flowers - Technical Innovator*.
Von: http://www.bbc.co.uk/dna/h2g2/A1010070, am 21.9.2003.

BECKMAN, B.: *Svenska kryptobedrifter*. Kurzfassung in: Teleprinter Ciphers, *The Siemens and Halske Geheimschreiber T52.*

Von: http://hem.passagen.se/tan01/tele.html, am 15.02.02.

BLETCHLEY PARK MUSEUM: "*Historical information gathered from the Bletchley Park archives*".
Von: http://www.bletchleypark.org.uk/dchistory/, am 12.09.03.

BOONE, J. V. and PETERSON, R. R.: *The Start of the Digital Revolution: SIGSALY - Secure Digital Voice Communications in World War II*. Revised October 13, 2000, National Security Agency, Fort George Meade, Maryland.
Von: http://www.nsa.gov/wwii/papers/sigsaly.htm, am 29.01.03.

BRITISH TELECOM (BT): *People-Personalities – Tommy Flowers.*
Von:http://www.btplc.com/Corporateinformation/BTArchives/ImageGallery/People-Personalities/index.htm, am 25.9.03.

BURY, Jan: *The Enigma – A Polish View.*
Von: http://webhome.idirect.com/~jproc/crypto/enigma.html, am 25.03.02.

CARTER, Frank: *The Abwehr Enigma Machine*.
Von: www.bletchleypark.org.uk/abwehr.pdf, am 15.9.03.

GOEBEL, Greg: *Codes, Ciphers, & Codebreaking* .V*2.0.0 / 5 of 12 / 01 mar 02,* [9.1] Telecipher Systems. http://www.vectorsite.net/ttcode.html 25.05.02.

GOLDSCHMIDT, Asaf and ATSUSHI, Akera John: *W. Mauchly and the Development of the ENIAC Computer.* In: Exhibition in the Department of History and Sociology of Science, University of Pennsylvania.
Last update: Monday, 03-Feb-2003.
Von: http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html, am 3.3.03.

HAMER, David H.: *Bombe Rebuild Project, Versions of the Bombe*.
von: http://www.jharper.demon.co.uk/bombe1.htm, am 25.3.02

HINSLEY, Francis Harry: *The Influence of ULTRA in the Second World War.* Vortrag an der University of Cambridge am 19.Okt. 1993.
Von: http://www.cix.co.uk/~klockstone/index.html, am 02.06.02.

HOBBS, Alan G.: *Fiveunit codes*. (NADCOMM-Museum 1999).
Von: http://www.nadcomm.com/fiveunit/fiveunits.htm, am 21.10.01.

HOBBS, Alan G../HALLAS, Sam: *A Short History of Telegraphy* ,1987, Part 2.
Von: www.samhallas.co.uk, am 10.5.03.

HODGES, Andrew: *Alan Turing a short biography*. *Part 4 The Second World War*.
Von: http://www.turing.org.uk/turing/scrapbook/ww2.html, am 02.06.02.

HODGES, Andrew: *Turing's Treatise on the Enigma: a preface* (1998, revised 1999).
In: Mathematical Logic of the Collected Works of A. M. Turing, ed. R. O. Gandy and C. E. M. Yates (2001).
Von: http://www.turing.org.uk/publications/profsbook.html, am 3.10.03.

HODGES, Andrew: The Alan Turing Internet Scrapbook.
-Turing and the Battle of the Atlantic.
-Who invented the Computer?
Von: http://www.turing.org.uk/turing/scrapbook/ww2.html, am 25.10.02.

IMPERIAL WAR MUSEUM, Online Exhibition: *Enigma and the Codebreakers, Colossus*.
Von: http://www.iwm.org.uk/online/enigma/enigma13.htm, am 24.4.02.

KRUH/DEAVOURS: *The Commercial Enigma, Beginnings of Machine Cryptography*.
In: Cryptologia, January 2002, Volume XXVI, Number 1.
Von:http://www.dean.usma.edu/math/pubs/cryptologia/extras/
KruhDeavoursV26N1pp116.PDF,

LANGER, Josef: *SFM T 43*.
Von: http://www.eclipse.net/~dhamer/downloads/SFM T43neu.PDF, am 8.4.03.

LEE/BURKE/ANDERSON: *The US Bombes. NCR, Joseph Desch, and 600 WAVES*.
In: IEEE Annals of the History of Computing, July–September 2000.
Von: http://frode.home.cern.ch/frode/crypto/USBombe/index.html, am 28.04.02.

MAHON, A. P. : *The History of Hut Eight*, a report of 1945 released by the National Security Agency, Washington DC, 1996; reference NR 4685, box 1424, RG 457, National Records and Archives Administration.
Von: http://www.turing.org.uk/publications/profsbook.html, am 3.10.03.

MOMSEN, Bill: Codebreaking and Secret Weapons in World War II, Chapter II.
Von: http://home.earthlink.net/~nbrass1/enigma.htm, 17.02.02.

MUMMA, Robert: *Oral history*, conducted in 15.9.1995 by Frederik Nebeker. In: IEEE History Center, Rutgers University, New Brunswick, NJ/USA. Von: www.ieee.org/organizations/history_center/oral_histories/transcripts/mumma.html, am 9.11.02.

NELSON, A./LOVITT, K.M. (Ed.): *History Of Teletype Development* (Oct. 1963). Von: http://www.thocp.net/hardware/history_of_teletype_development_.htm, am 13.3.02.

LEEUW, Karl de: *The dutch invention of the rotor machine, 1915 - 1923*. Cryptologia 27 (2003). Von: http://www.uni-mainz.de/~pommeren/Kryptologie/Klassisch/4_ZylRot/Hebern.html, 24.2.04.

PROC, Jerry: *Crypto Machine Menu Page*, Alphabetical Listings, Enigma, Feb 25/03. Von: http://webhome.idirect.com/~jproc/crypto/menu.html, am 24.10.03.

SALE, Tony: *Codes and Ciphers in the Second World War.* (Homepage). Von: http://www.codesandciphers.org.uk, am 25./29.10.02.
-*Colossus,* Lecture given at the IEEE, 18th February 1999.
-*The Lorenz Cipher and how Bletchley Park broke it.*
-*The rebuilding of Heath Robinson.*
-*The ENIGMA.*

SAVARD, John J. G.: *The Swedish HC-9 Ciphering Machine.* In: *A Cryptographic Compendium.* Von: http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm, 8.4.03.

SCHMEH, K.: *Als deutscher Code-Knacker im Zweiten Weltkrieg.* Von: http://www.heise.de/tp/r4/artikel/18/18371/1.html, am 23.12.04.

SCHNEIDER, Henner: *Simulation und Animation historischer Geräte*. In: Jahrestagung 1999 Deutscher Museumsbund, HNF Paderborn, 26. bis 28. April 1999, Fachgruppe Technikhistorische Museen. Von: www.fbi.fh-darmstadt.de/, am 6.3.03.

SCHREYER, H.: *Entwicklung eines Versuchsmodells einer elektronischen Rechenmaschine*. in: ZUSE, Konrad: Internetarchiv, Texte chronologisch. Von: www.zib.de/zuse/Inhalt/Texte/Chrono/40er/Html/0534/node3.html – 11k, am 27.10.01

TURING, A.M.: *Treatise on Enigma*. NARA-Document Record Group 457, NSA Coll., Box 201, Nr. 964. Rekonstruiert und editiert von Erskine, R., Marks, P. und Weierud, F., Febr. 1999. Von: http://mad.home.cern.ch/frode/crypto.htm, am 14.01.03.

TUTTE, W.T.: *Fish and I.* University of Waterloo lecture transcript, 1998. von: http://frode.home.cern.ch/frode/crypto/turing/index.html, am 25.03.02

UNIVERSITÄT HAMBURG – Informatik: *Die ENIGMA.* Von: ftp://agnwww.informatik.unihamburg.de/pub/cryptsim/gifs

US-PATENT AND TRADEMARK OFFICE, US-Patentschrift 1,510,441. Von: http://www.uspto.gov/patft/help/.htm, am 16.01.02

WEADON, Patrick D.: *The SIGSALY Story*. Revised October 13, 2000.
Von: http://www.nsa.gov/wwii/papers/sigsaly.htm, 12.3.02

WEIERUD, Frode.: *Frodes Kryptopage, The Siemens and Halske T52d.*
Von: http://mad.home.cern.ch/frode/crypto/simula/t52.htm, am: 9.4.02

WEIERUD, Frode: *TIRPITZ and the Japanese-German Naval War Communikation Agreement*, In: Cryptologia Vol 20, No. 3, Summer 1999, p 610.
Von: http://mad.home.cern.ch/frode/crypto/tirpitz.htm, am 14.01.03.

WINEGRAD, Dilys: *Celebrating The Birth Of Modern Computing*. In: IEEE Annals, Spring 1996, Vol. 18, No. 1, pp. 59.
Von: http://www.computer.org/annals/an1996/a1005abs.htm, am 7.1.03.

W1TP *Telegraph & Scientific Instrument Museums*.
Von: http://www.chss.montclair.edu/~pererat/u_108.jpg, am 10.10.03.

ZENKER, Uwe: Kurzinformation über die wichtigsten Daten der ENIGMA I, Juni 1996.
Von: http://users.informatik.fh-amburg.de/~voeller/krypto/html/enigma/ENIGMA_uwe.htm, am 21.8.99.

ZUSE, Konrad: *Entwicklungslinien einer Rechengeräte-Entwicklung von der Mechanik zur Elektronik*. Von: Konrad Zuse Internetarchiv, http://www.zib.de/zuse/index.html, am 25.3.02.

ZUSE, Konrad: *Elektronenröhre als Relais*. Von: Konrad Zuse Internetarchiv, http://www.zib.de/zuse/index.html, am 25.3.02.

ZYSMAN, George I. et al.*: Technology Evolution for Mobile and Personal Communications.*
In: Bell Labs Technical Journal, January – March 2000, S. 107-130.
Von: http://www.lucent.com/minds/techjournal/pdf/janmar2000/paper07.pdf, am 28. 05.02.

9.3 Ungedruckte bzw. unveröffentlichte Quellen

BUNDESARCHIV – Militärarchiv Freiburg (BArch-MA):
--OKW/Chi: Der Stand des Chiffrierwesens in der Wehrmacht. Interner Bericht (o. N.) vom 15. Febr. 1945, RW 4/920.
--Kriegstagebuch Dönitz vom 5.3.1943. RM 87/26, Bl. 19.
--Praun, Albert: Das Nachrichtenwesen als Führungsmittel der obersten Heeresführung im Zweiten Weltkrieg. ZA 1/1916.
--"Neue Chiffriermaschine für die Marine". Geheime Kommandosache der Marineleitung vom 7.2.1930, dazu Schriftwechsel.

BUNDESARCHIV Berlin (BArch)
--Korrespondenz des Präsidenten der Reichspost-Forschungsanstalt. Signatur R 4701/ 18314.
--Befehl des OKW vom 16.12.1943 zur Freistellung von namentlich genannten 5000 Forschern. Signatur NS 34/8.

DEUTSCHES MUSEUM MÜNCHEN: Abt. Rechentechnik und Informatik – Erläuterungen.

HEINZ NIXDORF MUSEUMS FORUM (HNF), Abteilung Kryptologie.
Ryska, Norbert.: „*Weltgeschichte der Kryptologie*“, Vortrag in Bildern und Texten. Stand 4.12.02.

MACHE, W.: Korrespondenz mit dem Verf. (uv.).
Privates Archiv:
--Viele Angaben zu Schlüsselfernschreibmaschinen.
--HDvg 422 „Schlüsselfernschreibvorschrift“ des OKW, gültig ab 1.12.42.
--Korrespondenz Mache mit Ken Halton über Tunny-Entzifferung.

KOPACZ, K.: Privatarchiv Schlüsselmaschinen
Korrespondenz (uv.)

PUBLIC RECORD OFFICE (PRO), Kew/GB
--Dokumente: ADM 223/464; HW 14/43.
--Good/Michie/Timms: *General Report On Tunny: With Emphasis on Statistical Methods* (HW5/4 u.5).
-- TICOM I- „Neu- und Weiterentwicklung technischer Schlüsselmittel”, Stand Januar 1944.
--TICOM I-38, *Report on Interrogation of Lt. Frowein of OKM/ 4 Skl III*.
--TICOM I-45: *OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cypher Teleprinter Machines.* Written by Huettenhain and Fricke, 1.8.1945.
--TICOM I-77: Homework by Dr. Huettenhain and Dr. Fricke on Zaehlwerk (cyclometer) – Enigma. Ref. G5/80 – 1st Aug. 1945.

SÄCHSISCHES STAATSARCHIV CHEMNITZ (StAC),
Bestand 31030, Wanderer-Werke Chemnitz.

SAMMLUNG R. F. STARITZ, Bamberg:

--STARITZ, R.F.: Korrespondenz mit dem Verf. (u.v.).

--MAAS, F.J.: *Der Stand der Funkfernschreibtechnik in Deutschland 1940 bis 1944.* Laborbericht der Fa. Rohde & Schwarz, München, vom 15.2.1946.

--Bericht über das Chiffrierwesen in OKW/Chi, nach dem Krieg angefertigt. Vertrauliches Dokument der Zentralstelle für das Chiffrierwesen der BRD (--Nur für den Dienstgebrauch--).

--Angebot Chiffriermaschinen AG, Berlin, 16.9.1929, über *„Enigma mit Zählwerk."*

10 Verzeichnis der Abbildungen