ENIGMA VARIATIONS: AN EXTENDED FAMILY OF MACHINES

David H. Hamer,[1] Geoff Sullivan[2] and Frode Weierud[3]

ADDRESS: (1) 66 Academy Court, Bedminster, NJ 07921, U.S.A. Email: dhamer@eclipse.net, URL: http://www.eclipse.net/∼dhamer/; (2) 64 Tennyson Road, Headless Cross, Redditch, Worcs. B97 5BJ, United Kingdom. Email: geoff@blueangel.demon.co.uk, URL: http://www.blueangel.demon.co.uk/crypto/; (3) Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens, France. Email: Frode.Weierud@cern.ch, URL: http://wwwcn.cern.ch/∼frode/crypto/

ABSTRACT: Several previously unknown models of the Enigma machine have recently been discovered through archive research and inspection of machines in museum collections. The present knowledge about these machines, including both use and technical details, is presented. The paper shows that the Enigma was not one machine, but rather a family of machines built upon the principle of wired rotors with a fixed or rotatable reflector. It also describes simulations in software for some of these machines.

KEYWORDS: Enigma, Railway Enigma, rotor wiring, multi-notch machines, rotor classes, computer simulations.

INTRODUCTION

The Enigma machine is probably the most widely known cipher machine ever made. It now has a firm place in history and has played an important part in both a theatre play and in a best selling novel.[1] Few other cipher machines can claim such a level of popularity.

Unfortunately the story surrounding the Enigma is often very muddled and many completely wrong accounts have been published. One recurring mistake is the alleged link between Enigma and Colossus: the unfounded claim that Colossus was used to break the Enigma.[2]

Enigma is too often considered to be a single machine notwithstanding the existence of both commercial and military models. We show that it was in fact a relatively

[1] Hugh Whitemore's play *Breaking the Code* and Robert Harris' novel *Enigma*, (New York: Random House, 1995).

[2] A classic example of this is in Dr. A.W.M. Coombs' contribution "Building the machine: Design and construction of Colossus" in "Discussion on: The code-breaking computers of 1944." The discussion took place at the IEE, Savoy Place, London on 26 March 1987 and appeared in the *IEE Proceedings-A*, Vol. 140, No. 3, May 1993.

large family of machines built around the same principle, wired wheels (rotors) with a fixed or rotatable *Umkehrwalze* (reflector).[3]

We will not deal with all of these machines in detail. The *Wehrmacht* Enigma,[4] the three-wheel machine used by the German Army and Air Force, and the Naval Enigma machines, both the three and four-wheel models, have been covered extensively elsewhere. [3, 4] We should like to introduce several three-wheel Enigma machines without *Steckers* (plugboard) derived from the commercial Enigma models D and K, as well as touch briefly on the 11-15-17 machine, also known as *Abwehr* Enigma, which will be covered extensively in a future paper.

The main machines, being based on the commercial models, have three wired wheels and a settable *Umkehrwalze* (UKW). It should be stressed that there is a significant difference between a **settable** UKW and a **moving** one. They are both rotatable, but while the settable UKW stays put during the whole ciphering/deciphering process, a moving one may be stepped forward by its neighbouring wheel while the process is going on. The 11-15-17 machine had a moving UKW. It is the only machine of the Enigma family known to have one.

Due to the lack of *Steckers*, these machines are significantly less secure than the *Wehrmacht* Enigma and the Naval Enigma machines, but some are equipped with multiple turnover wheels. This results in a much more frequent turnover of all wheels – something the normal three and four-wheel Bombes were ill-equipped to handle.

THE RAILWAY ENIGMA

From 7 February 1941 the Government Code and Cipher School (GC&CS) decrypted what they believed to be a new variant of the Enigma traffic, introduced by the Germans on 23 January.[5] The traffic consisted of serial numbers and esoteric references and abbreviations referring to the movement of railway stock. Hence the machine got the name, Railway Enigma. BP would later name this key Rocket.[6] However, this was not the first encounter with the Railway Enigma. In a letter of 17 August

[3] To stay in the historical context we will adopt many of the original Bletchley Park (BP) terms. Hence we will use the terms wired wheels and *Umkehrwalze* instead of the more common American terms rotor and reflector.

[4] At BP these machines were covered by the term the service machine or Service Enigma, referring to the three services: Army, Navy and Air Force.

[5] F.H. Hinsley et al., *British Intelligence in the Second World War*, (London: Her Majesty's Stationery Office (HMSO), 1979), Vol. 1, p. 357.

[6] Hinsley et al. seem to err in their claim that this key was named Rocket from September 1943. See F.H. Hinsley et al., *British Intelligence in the Second World War*, (London: HMSO, 1981), Vol. 2, p. 668. W.F. Friedman's report on his visit to GC&CS in the period 25 April - 13 June 1943, refers on p. 66 to "E" messages of the German Railways as "Rocket" traffic. See "Report on E Operations of the GC&CS at Bletchley Park" of 12 Aug. 1943, National Archives and Records Administration (NARA), RG 457, NSA Historical Collection, Box 1126, Nr. 3620. Furthermore, Hinsley et al. mention June 1940 as the date the Railway key was identified. This contradicts what they say in Vol. 1, see note 5.

1940, an unknown writer referred to the railway decrypts and said that Colonel Tiltman had recently broken their method of encipherment.[7] Joan Murray's account of this break gives Colonel Tiltman the credit of getting the first wedge into the cipher by finding messages in "depth" which then enabled him to recover their plaintext.[8] The wiring of the wheels was subsequently recovered by the people in Hut 8 using the then well known principle of "boxing," the forming of chains. BP's annual report for 1940 mentions that the railway signals were first intercepted on 25 July 1940 and that all messages were decrypted until the traffic ceased on 27 August. Hence, the details of the machine and its wiring had already been deduced by BP in August 1940.[9] The machine was basically the commercial model with three rewired wheels, a settable UKW, and without *Steckers*. It is described in Alan Turing's "Treatise on the Enigma," where the machine is used to explain various cryptanalytical methods.[10] W.F. Friedman stated that the Railway UKW was of the moving type, but we are inclined to believe that he errs.[11] In a machine with wheels that each have a single turnover the UKW will rarely, if ever, move within a message, even if it is capable of doing so, and no other sources support his statement.

It is instructive to look closely at the Railway Enigma keys and how BP dealt with this problem. Rocket, or Rocket I as it was later called, was used by the German *Reichsbahn* in Eastern Europe, Russia and the Balkans. There does not appear to have been a similar key for Western Europe before September 1942, when another railway key was discovered.[12] This new key was named Rocket II and the first and only break occurred during this month when the traffic was encrypted for a short period using the Rocket I (Railway) Enigma. The traffic consisted of practice messages with feminine signatures like *Olga, Berta*, etc.[13] The transmission of practice messages appears to have continued until May 1944. Apart from the initial break, the key remained unbroken, but a study of discriminants and other external characteristics suggested a circuit where the majority of the messages were of a practice nature. In May a new key started up, using a different set of discriminants. This key was named Rocket III and appeared to be carrying normal traffic as it contained multi-part messages and occasional KRs,

[7] Colonel (later Brigadier) John H. Tiltman was one of BP's foremost cryptanalysts. After his retirement from Government Communications Headquarters (GCHQ) in 1964 he worked at the US National Security Agency (NSA).

[8] Joan Murray, "Hut 8 and naval Enigma, Part I." Chapter 14 in *Codebreakers*, [5] p. 116

[9] This appears to contradict Hinsley et al.'s account above. However, they write specifically about the situation in the Balkans in 1941 and we believe their use of "new variant of Enigma traffic" should be seen in the context of the Balkan situation.

[10] Turing's "Treatise on the Enigma," NARA RG 457, NSA Hist. Col., Box 201, Nr. 964. The treatise was most likely written in 1940, which correlates with Tiltman's break in August the same year.

[11] Friedman's "Report on E Operations of GC&CS," pp. 39, 67. See note 6. Strong evidence to the contrary appears in a table giving an overview of several rotor machines, where the UKW for the Railway Enigma is marked as settable by hand. See "Tentative List of Enigma and Other Machine Usages," NARA RG 457, NSA Hist. Col., Box 580, Nr. 1417.

[12] This can be explained by better and more secure land-line communications in the west.

[13] See Hut 6 Report, Part III, 26 Aug. 1944 addendum to Captain Walter J. Fried's report No. 88 of 6 Sept. 1944. NARA RG 457, NSA Hist. Col., Box 880, Nr. 2612. Henceforth called Fried reports.

Kriegsnotmeldungen.[14]

BP regarded the solution of Rocket I traffic as relatively simple and broke it in Hut 6 using cribs and hand methods. In the occasional difficult case a Bombe would be used to facilitate the solution. However, we will see that the traffic could occasionally pose serious problems. Rocket I provided good intelligence; according to Friedman: "The intelligence obtained from "Rocket" traffic is of first-grade importance since it gives long-term information as to production and movement of supplies."[15]

The problem posed by Rocket II and III was baffling and BP was unable to determine if these keys used the same machine as Rocket I or a different, perhaps steckered, machine. To try to come to grips with this problem it was decided on 20 June 1944 to ask OP-20-G to run statistical tests on three long messages using Hypo, the US Navy's Dudbuster.[16] A negative outcome would have been seen as strong evidence against the use of the Rocket I machine. The Hypo run had low priority and it was not until 23 July that it was reported that the first message was "down."[17] It had taken 90 hours to run. The final two messages were also reported as negative on 19 August and it became clear that OP-20-G was not anxious to run other Rocket I problems on Hypo.[18]

In the last week of August things suddenly changed. In the Hut 6 report of 26 August, Major Dennis Babbage, under the heading of "Unsolved Problems" sets out in detail what was known about the Rocket II/III traffic and where Hut 6 stood with this problem at that moment.[19] He states grimly: "We are not likely to get into it except by a re-encodement." He also mentions that the Germans had declared the key compromised on 9 August.

The report was hardly out of the door, when news arrived from London that a deserter had brought a long-hand copy of the Rocket II key for August. This allowed BP to solve a number of messages. Unfortunately it is nowhere clearly stated which machine was used. In the Hut 6 report of 2 September 1944, Stuart Milner-Barry says: "The result of Major Babbage's note on unsolved problems last week was to produce a captured key sheet for the August Rocket II keys, which proves that the Enigma machine was in use.[20] From what has been seen of the decrypted traffic, it

[14] War emergency signals; also used as high priority message indicator.

[15] Friedman's "Report on E Operations of GC&CS" p. 66, see note 6.

[16] See U.D. Committee, 14th Meeting - 20 June 1944, NARA RG 457, NSA Hist. Col., Box 200, Nr. 962. Hypo was one of the rapid, optical film type comparators developed by the US Navy. The U.D. Committee, which presumably stands for "*Umkehrwalze* D Committee," was created to deal with the *Umkehrwalze* D and related problems and had its first meeting on 3 Apr. 1944.

[17] "Up" and "down" are BP expressions for a positive and negative outcome of a hypothesis test.

[18] See U.D. Committee, 23rd Meeting - 19 Aug. 1944, NARA RG 457, NSA Hist. Col., Box 200, Nr. 962.

[19] Rocket II/III, which contained stations in Paris, Rouen, Bordeaux, Toulouse, Lyons, Liege and Brussels, were given serial M22. A new serial M24 had recently appeared. Stations on this network were DF'd to Stuttgart, Strasbourg, Rheims, Vitry and the Calais area. See note 13.

[20] The Hut 6 report talks about a captured key sheet, but Captain Fried made it clear that the key sheet originated with a German deserter. He wrote: "The August keys were not actually captured – a long-hand copy was brought in by a prisoner who had deserted and was evidently trying to ingratiate

looks singularly unpromising cryptographically.” Milner-Barry was probably thinking in terms of “his” Enigma, the service machine, and as the Hypo runs had shown Rocket II not to be the Railway Enigma, we conclude that it must indeed have been using the service machine.

The decrypts did not inspire optimism because addresses and signatures were buried in the text and the cribs did not look promising. On 19 September 1944 the U.D. Committee reported problems with Rocket I. No messages had been broken for more than a week. On 14 October 1944 the Rocket I situation was still unresolved. A Hut 6 report states: “There are now many weeks since a day came out. Either the cribs have suddenly gone wrong, or it has gone over to a new machine. There is very little traffic, and on the whole the former seems the more likely hypothesis.” However, there was some consolation in the fact that the Rocket II key had again been broken on a re-encodement from Bantam, the Army key for France. The message content also gave some hope for the future. Also during this period a new key appeared which was christened Stephenson.[21] The key used the Service Enigma with only wheels I, II and III and the traffic had remarkably good cribs.[22]

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	JGDQOXUSCAMIFRVTPNEWKBLZYH	V	N
II	NTZPSFBOKMWRCJDIVLAEYUXHGQ	M	E
III	JVIUBHTCDYAKEQZPOSGXNRMWFL	G	Y
UKW	QYHOGNECVPUZTFDJAXWMKISRBL		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Notes: 1: The Notch column gives the location of the notch on the alphabet ring while the Window column gives the letter appearing in the window when the notch is engaged in its turnover position.

2: Alphabets progress clockwise as viewed along the wheel axis from the ETW. All wheels are in their neutral position, *Ringstellung* A.

3: UKW = *Umkehrwalze* (Reflector); ETW = *Eintrittwalze* (Stator)

Figure 1: Wiring of the Wheels, Umkehrwalze and Eintrittwalze for the Railway Enigma.[23]

However, in the end Rocket I inevitably gave in to the sustained effort to break it. On 28 October 1944 Stuart Milner-Barry reports in his usual style: “Rocket I, an ancient day has been broken by the determination of Miss Esperson, and discloses grave eccentricities in the cribs which may account for our repeated failure, though later

himself.”

[21] Both Stephenson and Stevenson appear in several places. The former is believed to be the correct spelling, since it is reasonable to suppose that BP’s use of the codewords Rocket and Stephenson for Railway traffic is derived from George Stephenson (1781-1848) and his locomotive, Rocket, which won the speed competition on the Liverpool-Manchester railway line in 1829.

[22] Hut 6 Report, 14 Oct. 1944, addendum to Fried report No. 103 of 19 Oct. 1944.

[23] The wiring has been recovered from various tables and figures in Turing’s “Treatise on the Enigma.”

breaks looked normal. Rocket II (now Blunderbuss), interesting and not unhopeful; Stevenson (now Culverin), most messages are cribs."[24]

Rocket I now seemed to peter out completely and Hut 6 reports on 4 November that nothing has been heard from the Rocket I front. The report adds: "Culverin, which does not encode its callsigns, is healthy; Blunderbuss is not, though much is tried." On 18 November Blunderbuss had changed for the better and Hut 6 reports: "Among keys broken in quantity were Blunderbuss (not at all easy), Culverin, Pigeon and Albatross."[25] Culverin appears to have ceased operations in December 1944 while Blunderbuss continued until some time in spring 1945. Apart from describing in detail some of the more obscure Enigma keys, this history of BP's fight against the Railway keys illustrates several interesting facts. First, that even a rewired, commercial Enigma could create severe problems for BP if the message content was of a sufficiently obscure nature. Second, without cribs the Bombes were virtually useless, and third, without cribs or re-encodements BP was not always able to break into a new key.

THE MULTIPLE TURNOVER MACHINES

When introducing the subject of turnovers (notches) it is important to stress the type of wheel stepping motion involved. One of the authors has already dealt with this issue in some detail.[26] There are two main stepping motions, Enigma stepping and cyclometric stepping. In the case of single-notch wheels, cyclometric stepping means that a wheel will step forward one position each time its right-hand neighbour has made a complete cycle. Enigma stepping on the other hand will move the middle wheel an extra step each time its left-hand neighbour is stepped, due to the mechanical construction of the notches and stepping pawls. Machines with multi-notch wheels can have either cyclometric or Enigma stepping. The only difference from the single-notch case is a more frequent turnover of the wheels. Therefore with cyclometric stepping a single-notched, three-wheel machine has a period of 17576, while with Enigma stepping the period is 16900.

The Naval Enigma had three special wheels with two notches diametrically opposite in positions H and U. This shows that the Naval cryptographers had seen at least two problems with the *Wehrmacht* Enigma, the too infrequent turnover of the wheels and the risk of identifying a wheel by its turnover characteristics. Theoretically, the choice of the relative location of the two notches is not a very good one: 2 and 13 being the prime factors of 26. The outcome is a reduction in the total period of the machine. However, due to the operational use of the Enigma machine this is much less of a problem than it might appear to be.

[24] Hut 6 Report, 28 Oct. 1944, addendum to Fried report No. 109 of 2 Nov. 1944.

[25] Hut 6 Report, 29 Nov. 1944, addendum to Fried report No. 121 of 29 Nov. 1944. Albatross was the key for the 10th Army in Italy, while Pigeon was one of the keys passing Y (Sigint) traffic in the West.

[26] David H. Hamer, "Enigma: Actions Involved in the "Double Stepping" of the Middle Rotor," *Cryptologia*, 21(1): 47-50.

The real multiple turnover machines went much further by using wheels having from five to 17 notches. Among these were the 11-15-17, the K.D., and the Enigma T machines. The 11-15-17 models do not have the same wheel movement mechanism as the other Enigmas. Instead of notches and pawls, their movement is based on coupled gears as explained by Deavours. [2]

The T Machine

In the summer of 1944, probably in the beginning of August, several so-called *Tirpitz* machines or Enigma model T's were captured in a warehouse, in the vicinity of Lorient. The exact location is not known and one US naval document even mentions a warehouse in Normandy.[27] There are also conflicting claims as to how many machines were captured. The US Army's liaison officer at Bletchley Park at the time, Captain Walter J. Fried, mentions 15 to 20 machines.[28] However, six weeks later the inventory of Gordon Welchman's store of captured machines in Block H at BP shows a total of 62. As it is known that a number of machines were sent to the USA for further study it is likely that the catch was more like 70 machines.

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	KPTYUELOCVGRFQDANJMBSWHZXI	EHMSY	WZEKQ
II	UPHZLWEQMTDJXCAKSOIGVBYFNR	EHNTZ	WZFLR
III	QUDLYRFEKONVZAXWHMGPJBSICT	EHMSY	WZEKQ
IV	CIWTBKXNRESPFLYDAGVHQUOJZM	EHNTZ	WZFLR
V	UAXGISNJBVERDYLFZWTPCKOHMQ	GKNSZ	YCFKR
VI	XFUZGALVHCNYSEWQTDMRBKPIOJ	FMQUY	XEIMQ
VII	BJVFTXPLNAYOZIKWGDQERUCHSM	GKNSZ	YCFKR
VIII	YMTPNZHWKODAJXELUQVGCBISFR	FMQUY	XEIMQ
UKW	GEKPBTAUMOCNILJDXZYFHWVQSR		
ETW	KZROUQHYAIGBLWVSTDXFPNMCJE		

Notes: Same as for Fig. 1.

Figure 2: Wiring of the Wheels, Umkehrwalze and Eintrittwalze for the Enigma T (Tirpitz).[29]

The machines had been built for the Japanese, probably the Japanese Navy, and

[27] The information about the capture near Lorient appears in Fried report No. 78 of 19 Aug. 1944. The American forces were at the outskirts of Brest, Lorient and St. Nazaire on 16 August. Lorient itself was not captured until September.

[28] Fried report No. 78 of 19 Aug. 1944 mentions that several T machines were being prepared for shipment to the U.S. Arlington Hall would get at least two machines, with serial numbers around T250 or T260.

[29] We are indebted to Mr. Tony Sale, Director of the Bletchley Park Museum Trust, for the wiring of wheels V, VII, VIII and for verifying the UKW and ETW wiring. The wiring of the other wheels has been measured on three different machines at the NSA's National Cryptologic Museum.

were sitting in the warehouse awaiting shipment to Japan. Prior intelligence on these machines must have been available at BP since Intelligence Memo No. 60 prepared by the Naval Section on 3 July 1944, has the title “The Purchase of German Enigma Machines by the Japanese Navy.”

The T machine is a three-wheel machine with a settable UKW. The machine has no *Steckers* and is clearly based on the commercial Enigma. However, the *Eintrittwalze* or stator does not have the usual QWERTZU diagonal or the ABCD diagonal of the *Wehrmacht* Enigma.[30] Instead it is equipped with a random permutation which is given here together with the wiring of seven of the eight rotors.

It appears that the machine was never used in an operational context. In early 1945 the US Navy performed exhaustive runs with two cribs placed at the beginning of two messages suspected of having been enciphered on the T machine. However, the runs were negative. Due to the multiple turnovers, for a four letter crib alone, eight (out of a theoretical maximum of 64) grenade runs had to be made to cover all stepping possibilities.[31]

We should like to draw attention to Louis Kruh’s 1994 *Cryptologia* article which carries a very good photo of an Enigma T machine.[32] It is marked T179 and a multi-notched wheel is clearly visible. Our present knowledge about the Enigma T shows that the US Postal Service had some grounds for their claim about the origin of the machine. Their caption “Captured Japanese code device” is not the most apt, but it is reasonably accurate.

The Abwehr Machines

The *Abwehr* used a multitude of hand and machine ciphers including the Lorenz SZ42. However, we will here only look at the Enigma machines and particularly the multi-turnover machine which is usually called the *Abwehr* machine or the 11-15-17 machine.[33] We will follow the latter usage.

Of the more normal Enigma machines, the *Abwehr* is known to have used three distinct types usually called GGG, 4J and 4I by BP and the US agencies. It is not entirely clear where these names originate, although GGG probably was an *Abwehr* message indicator. It is therefore possible that 4J and 4I could be the indicators JJJJ and IIII, but this is not known at present. The GGG and 4J machines were commercial Enigma machines possibly of type K.[34] They each had differently wired wheels. On

[30] The name is derived from tables called rod and inverse rod squares. In these tables the input sequence will appear as the top right to bottom left diagonal. See the section on Wheel Identification.

[31] Grenades were attachments to the US Navy Bombes of type N-530 or N-1530 used to solve specific cryptanalytic problems. One exception was the “Cilly Grenade” which was a special usage of the Bombes and not an attachment.

[32] Louis Kruh, “The Postal Service Fails to Deliver the Goods,” *Cryptologia*, 18(3): 250-252.

[33] Deavours [2] gives the turnovers as 11-15-19, based on Peter Twinn’s [6] account in *Codebreakers* [5], which has this printing mistake.

[34] This is a conjecture based on information that the production of the D machine had stopped in 1939.

the other hand, the 4I machine was a three-wheel steckered service machine that used the first three service wheels (I, II and III). All these machines were first detected by the allied services in the beginning or middle of 1941.

However, the 11-15-17 machines pre-dated the others as the first one, labelled Group II by BP, was detected in December 1939. The other two machines of the 11-15-17 type were called 3K and 3N by the US Coast Guard. One of these machines was called ROT Enigma by the Germans.[35] The first break into these machines was by Dillwyn Knox and his team in October 1941. The machines were equipped with a set of three wheels and a moving UKW and the wheels had cyclometric movement. As the machines were not steckered they were conceptually weaker than the service machines, but the very high turnover rate was a serious complication. Nevertheless, the frequent turnovers gave Knox the entry points he needed and his discovery of lobsters and crabs was the breakthrough that unravelled the secrets of the machine.[36] The 11-15-17 machines were broken both at BP and by the US Coast Guard throughout the war. The *Abwehr* traffic was normally broken by hand methods, but in extremely difficult cases machines would be employed. At BP two special Bombes (*Fünf*) were used for this purpose, while the US Coast Guard used Hypo and special Grenades such as the Multiple Notch Grenade.[37] The 11-15-17 machines were not used exclusively by the *Abwehr*. The German Armistice Commission in Vichy France, both in France and the French territories in North Africa, used such a machine. In early 1945, the new Dutch Navy started to use a machine which was suspected to be the 11-15-17.

The K.D. Machine

The K.D. machine appeared for the first time on 3 December 1944 and continued to be used until the end of the war.[38] We do not have details of this machine's wiring, but it was a three-wheel machine with a pluggable *Umkehrwalze*. The machine was equipped with a set of six wheels, each with nine turnovers. Like the commercial Enigma, the K.D. machine had no *Steckers* and its diagonal or input permutation was the normal QWERTZU sequence. Like most of the other Enigma machines, it used Enigma stepping.

The machine was used by the German secret intelligence service's *Militärisches Amt (Mil Amt)*, the successor of *Abwehr*, on the Berlin - Madrid - Lisbon link. There was a daily change of wheels and *Ringstellung*, while the station *Grundstellung* changed every three weeks.

[35] These three machines were also labelled GISK 1, GISK 5 and GISK 9 by the allied services. GISK 1 was the Group II machine, GISK 5 was called the S.A. machine (possibly standing for South America), while GISK 9 was the ROT Enigma.

[36] See references [2] and [6].

[37] Multiple Notch Grenade, NARA RG 457, NSA Hist. Col., Box 1119, Nr. 3599.

[38] The origin of the name is unknown, but it may have come from the new abbreviation of the *Abwehrstellen (Ast)*. On 1 June 1944 the *Abwehr* was fully incorporated in the *Reichssicherheitshauptamt (RSHA)* and the *Asts* were renamed *Kommandos des Meldegebietes (KDM)*.

THE SWISS K MACHINE

On 1 July 1938 Switzerland received 14 commercial Enigma D machines together with a shipment of mobile radio stations that they had ordered from C. Lorenz AG, Berlin. This signalled the beginning of the use of cipher machines in Switzerland. In February 1939 they ordered another 65 machines from *Chiffriermaschinen AG*, Berlin, which were delivered on 1 July 1939. Finally in 1940, they received a total of 186 Enigmas in two batches on 5 May and 10 July. These were procured for the Swiss Army and Air Force, who got 102 and 163 machines respectively. A number were also ordered by the Foreign Ministry for use in the Diplomatic Service.[39]

The later delivery consisted of the Enigma model K, but apart from a few manufacturing modifications the D and K machines are identical and were delivered with the normal set of commercial wheel wirings. The machines were rewired by the Swiss. In the surviving machines, however, the UKW wiring is identical with that of the commercial models.

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch[40]	Window
I	PEZUOHXSCVFMTBGLRINQJWAYDK	G	Y
II	ZOUESYDKFWPCIQXHMVBLGNJRAT	M	E
III	EHRVXGAOBQUSIMZFLYNWKTPDJC	V	N
UKW	IMETCGFRAYSQBZXWLHKDVUPOJN		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Notes: Same as for Fig. 1.

Figure 3: Wiring of the Wheels, Umkehrwalze and Eintrittwalze for the Swiss Enigma K.[41]

In 1941 it became known to the Swiss that some of their Enigma traffic was being read in France and they took appropriate steps.[42] One of the modifications consisted of modifying the wheel stepping on the Swiss Army machine. The fast, right-hand wheel was made stationary during operation while the middle wheel stepped with every key stroke.[43] The slow, left-hand wheel and the UKW would step in the normal fashion with Enigma stepping for the slow wheel. The stationary but rotatable right-hand wheel

[39] Unpublished notes, Dipl. Ing. Rudolf J. Ritter, "Notes on Early Use of Machine Cypher in Switzerland," 16 Jan. 1996. We will only deal with the Swiss Enigma machines. NEMA (*NEue MAschine*) and other Swiss post-war machines are outside the scope of this paper.

[40] Observe that the turnover positions on the Railway Enigma and the Swiss K machine are the same except that wheel I on the Railway machine corresponds to wheel III on the Swiss machine.

[41] We are indebted to Mr. Alan Stripp and Professor Edward T. Hall for help with technical details. The wirings given are from machines that are believed to have been used by the Swiss Air Force. The wirings of the Air Force's reserve set of wheels are also known. Turnover positions and UKW wiring are the same as shown here.

[42] See Wladyslaw Kozaczuk, *Enigma* (London: Arms and Armour Press, 1984), p. 125.

[43] Private communication from Lieut. Col. Paul Glur, former chief of the Swiss Army's Cipher Bureau.

was meant to make up for the missing *Stecker* connections on the commercial machine. However, this appears to have been done only on the Army machines. Surviving Air Force machines do not have this modification, nor were these changes made to the machines used by the diplomatic service.

Another modification was a frequent re-wiring of the three wheels. The diplomatic service machines are reported to have been re-wired every two years. It is not known if any of the Swiss Army traffic was broken after the modification of their machine. However, the Swiss diplomatic Enigma traffic continued to be decrypted by both the allied and German cryptographic organisations throughout the war. At BP the Swiss Enigma was broken by Colonel Tiltman some time prior to September 1939.[44] The Americans got the wheel wiring from the British and started to break Swiss diplomatic traffic in their geographical region. Also the Germans broke into the Swiss Enigma traffic in 1939 and appear to have continued to break the traffic during the rest of the war.

It is not entirely clear who broke the Swiss Enigma traffic in Germany, but surviving documents indicate an involvement by both the *Forschungsamt* and the Foreign Office's cryptological office, *Pers. Z*.[45] One report on breaking the Enigma K surfaced in Switzerland after the war and is supposed to have been written by a member of the *Forschungsamt*.[46] In addition an interrogation report of a Mr. Zastrow of *Pers. Z* contains the following statement: "He had assisted Dr. Kunze with investigations of the Enigma machine, and the Swiss Enigma was successfully solved."[47]

WHEEL IDENTIFICATION

During the process of recovery of the wheel wiring it is extremely helpful to establish immediately whether the new wheel is the same as one already used in another machine. As the *Ringstellung* is frequently unknown at this stage it is necessary to have a method which is invariant to the circular transformation given by the *Ringstellung*. One such method was developed at BP, probably by Turing, and is usually named the "class" of a wheel.[48] A basic tool when working with wheel wiring is the "rod square" which is a table giving the effect of a wheel in its different positions. The "rod square"

[44] Letter of 29 April 1940 from A.G. Denniston, head of BP, to Brigadier Stewart Menzies, Director of BP and head of MI6. Public Record Office, HW 14/47.

[45] *Forschungsamt des Reichs-Luftfahrtsministeriums* reported directly to *Reichsmarschall* Hermann Göring.

[46] A slightly different version of the "Swiss report" has been found: "Analyse der Chiffriermaschine Enigma Type K," NARA RG 457, NSA Hist. Col., Box 1112, Nr. 3448.

[47] NARA RG 457, NSA Hist. Col., Box 1006, Nr. 3142. Mr. Zastrow asked for permission to have Professor Hans Rohrbach present during his interview, which was granted. Professor Rohrbach refers to the breaking of the commercial Enigma in his paper "Maschinelle Methoden bei Chiffrieren und Dechiffrieren," *FIAT Review of German Science*, Applied Mathematics, Part I, pp. 233-257, Wiesbaden, 1948. English translation published in *Cryptologia*, 2(1): 20-37; 2(2): 101-121.

[48] Turing's "Treatise on the Enigma," see note 10.

table is a 26 by 26 square where the columns are labelled with the numbers 1, . . . , 26 (or A,B,C,. . .) and the rows labelled with the letters of the diagonal, e.g. QWERTZU. . . The rods are the rows of the table which for a given rod point will give the output letters for that wheel in the different wheel positions.[49] The columns which will give the complete output alphabet of the wheel in a given position are called "uprights" after their vertical nature. We can also construct the inverse rod square, where the rows are named after the output letters and the elements are the rod points.

ETW	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	C	U	L	H	I	V	Y	R	P	S	D	M	T	K	W	G	B	J	B	F	X	N	O	Q	M	A
W	I	Q	J	O	B	X	T	Y	D	F	L	Z	P	E	H	N	K	N	G	C	M	A	W	L	S	V
E	W	K	A	N	C	Z	X	F	G	Q	U	Y	R	J	M	P	M	H	V	L	S	E	Q	D	B	O
R	P	S	M	V	U	C	G	H	W	I	X	T	K	L	Y	L	J	B	Q	D	R	W	F	N	A	E
T	D	L	B	I	V	H	J	E	O	C	Z	P	Q	X	Q	K	N	W	F	T	E	G	M	S	R	Y
Z	Q	N	O	B	J	K	R	A	V	U	Y	W	C	W	P	M	E	G	Z	R	H	L	D	T	X	F
U	M	A	N	K	P	T	S	B	I	X	E	V	E	Y	L	R	H	U	T	J	Q	F	Z	C	G	W
I	S	M	P	Y	Z	D	N	O	C	R	B	R	X	Q	T	J	I	Z	K	W	G	U	V	H	E	L
O	L	Y	X	U	F	M	A	V	T	N	T	C	W	Z	K	O	U	P	E	H	I	B	J	R	Q	D
A	X	C	I	G	L	S	B	Z	M	Z	V	E	U	P	A	I	Y	R	J	O	N	K	T	W	F	Q
S	V	O	H	Q	D	N	U	L	U	B	R	I	Y	S	O	X	T	K	A	M	P	Z	E	G	W	C
D	A	J	W	F	M	I	Q	I	N	T	O	X	D	A	C	Z	P	S	L	Y	U	R	H	E	V	B
F	K	E	G	L	O	W	O	M	Z	A	C	F	S	V	U	Y	D	Q	X	I	T	J	R	B	N	S
G	R	H	Q	A	E	A	L	U	S	V	G	D	B	I	X	F	W	C	O	Z	K	T	N	M	D	P
H	J	W	S	R	S	Q	I	D	B	H	F	N	O	C	G	E	V	A	U	P	Z	M	L	F	Y	T
J	E	D	T	D	W	O	F	N	J	G	M	A	V	H	R	B	S	I	Y	U	L	Q	G	X	Z	K
K	F	Z	F	E	A	G	M	K	H	L	S	B	J	T	N	D	O	X	I	Q	W	H	C	U	P	R
P	U	G	R	S	H	L	P	J	Q	D	N	K	Z	M	F	A	C	O	W	E	J	V	I	Y	T	G
Y	H	T	D	J	Q	Y	K	W	F	M	P	U	L	G	S	V	A	E	R	K	B	O	X	Z	H	I
X	Z	F	K	W	X	P	E	G	L	Y	I	Q	H	D	B	S	R	T	P	N	A	C	U	J	O	J
C	G	P	E	C	Y	R	H	Q	X	O	W	J	F	N	D	T	Z	Y	M	S	V	I	K	A	K	U
V	Y	R	V	X	T	J	W	C	A	E	K	G	M	F	Z	U	X	L	D	B	O	P	S	P	I	H
B	T	B	C	Z	K	E	V	S	R	P	H	L	G	U	I	C	Q	F	N	A	Y	D	Y	O	J	X
N	N	V	U	P	R	B	D	T	Y	J	Q	H	I	O	V	W	G	M	S	X	F	X	A	K	C	Z
M	B	I	Y	T	N	F	Z	X	K	W	J	O	A	B	E	H	L	D	C	G	C	S	P	V	U	M
L	O	X	Z	M	G	U	C	P	E	K	A	S	N	R	J	Q	F	V	H	V	D	Y	B	I	L	N

Figure 4: Rod Square for Wheel I of the Railway Enigma.

An inventive way of characterising a wheel is to find the class of the substitution which will transform one "upright" or alphabet into the next one in the rod square.[50] As the class of such a substitution is circularly invariant it is unimportant which "upright" is chosen to generate the class. If the class of two such substitutions for two different wheels is the same, we can extend the approach by finding the class of the substitution

[49] The rod points and rod positions of a wheel are linked with the core of the wheel that contains the wiring. The rod position indicates the absolute position of the wiring in space; it is independent of the *Ringstellung*. The rod points can be seen as connection points lying on a fixed, virtual disk between each wheel. Hence the middle wheel's rod point Q will correspond to the left-hand wheel's output point Q. In BP terminology the right-hand side contact pins were called the "output points" of the wheel while the left-hand side contact pads were called "rod points"

[50] The definition of the class of a substitution will be explained below.

formed by every second “upright” This will become necessary in a few cases. Moreover, the substitution classes will remain invariant even if they are developed from the reverse wiring or the inverse rod square, or if the wheel is used in a machine with a completely different diagonal. The wheel class is therefore an absolute characteristic of the wiring of a wheel.

Service Enigma		Enigma Model T	
I	3,4,6,13; 1,2,9,14	I	2,4,4,4,5,7; 5,21
II	10,16; 5,7,7,7	II	2,5,7,12; 8,18
III	6,6,7,7; 1,1,6,18	III	1,25; 8,18
IV	2,2,11,11; 3,6,8,9	IV	Unknown
V	2,6,9,9; 2,7,8,9	V	7,19; 4,22
VI	2,24; 2,3,5,16	VI	5,21; 3,23
VII	4,5,5,12; 2,24	VII	2,4,6,14; 2,4,8,12
VIII	2,24; 4,22	VIII	2,24; 2,3,4,17
Beta	2,2,3,3,7,9; 1,3,5,17	UKW	1,2,5,18; 1,8,17
Gamma	2,3,8,13; 2,3,9,12	Railway Enigma	
UKW B	1,7,8,10; 1,1,2,2,4,5,11	I	2,24; 1,2,5,18
UKW C	2,2,9,13; 1,2,6,8,9	II	2,4,8,12; 2,2,6,16
Thin B	1,4,5,16; 1,2,2,6,15	III	1,3,8,14; 2,5,7,12
Thin C	1,25; 1,2,3,3,4,8	UKW	2,24; 1,5,20
Swiss Enigma K		Commercial Enigma D	
I	3,7,7,9; 1,2,3,20	I	8,18; 2,24
II	8,18; 1,1,1,2,4,17	II	7,19; 6,20
III	2,2,3,19; 1,1,1,23	III	1,4,9,12; 2,3,5,16
UKW	1,1,2,22; 1,6,19	UKW	1,1,2,22; 1,6,19

Note: The classes are given as type 1 and type 2 in that order separated by a semicolon.

Figure 5: Classes of all known Wheels of the described Enigma machines and the Service Enigma.

We have developed the wheel classes for the machines that have so far been described publicly and we give the results here for easy reference. As the risk of having identical classes increases with the number of wheels we give the two main classes for each wheel.

To illustrate the process of obtaining wheel classes we will use the rod square for wheel I of the Railway Enigma which is given in Fig. 4. This rod square has been reconstructed, but it is identical to the rod square used by Turing in his “Treatise on the Enigma.” This also means that we have maintained the BP convention of using Z as the neutral or “zero” position for the *Ringstellung* for this wheel. It has been known for quite some time that BP considered Z to be the neutral position instead of A which was used by the Germans. This has been a considerable puzzle as there appeared not to be any good reason for this choice. Philip Marks discovered recently that BP used Y as the neutral position for wheel IV of the Service Enigma.[51] This discovery triggered one of the authors to have a closer look at the wiring of the wheels used in the US Navy's test machines. On closer inspection Philip Marks's observation was verified and, at the same time, it was revealed that wheel V had its neutral position at X. All the other wheels, including the three Naval wheels and Beta, had their neutral position at Z.

It has been confirmed that BP knew that wheels IV and V had offsets of two and three, respectively, but apparently this was discovered too late to justify a correction and that throughout the war both Bombes and testing machines used these offsets for these two wheels. It also appears that these mistaken neutral positions originated with the Poles. We will explain the detailed steps involved in obtaining the wheel classes, but the reader who would like a more profound understanding of this and related subjects is advised to consult Professor Bauer's book "Decrypted Secrets." [1] Professor Bauer also gives cycle partitions of the substitutions and their classes as a means of allowing easy identification of the wheels. However, his cycle partitions are different from the Turing cycles given here as he uses the substitutions themselves while Turing uses the transformation from one substitution to the next.

As an example we will use the two substitutions for *Ringstellung* A and B (columns A and B) and write one below the other as shown in Fig. 6. To form the cycles

```
CIWPDQMSLXVAKRJEFUHZGYTNBO
UQKSLNAMYCOJEHWDZGTFPRBVIX
```

Figure 6: Substitutions for Ringstellung A and B.

we can start at any letter in the two rows, but to use a more methodical approach we start at the first letter in row one, C. We write it down as well as its substitute in the second row, U. We now look for U in the first row and write down its substitute letter G, look for G in the upper row and write down its substitute P, etc. until we find a substitute letter which is C. We are then back to the beginning and we have closed the cycle. The result is the following cycle partition which has the class: 2, 24.[52]

```
(CUGPSMAJWKEDLYRHTBIQNVOX)(FZ)
```

This is the class of the transformation between neighbouring substitutions or "uprights" which we have called type one. The class of the transformation between every second substitution, or in Turing's terms: two apart "uprights" and which we call type two, can be developed in the same manner. The cycle partition of such a transformation between the "upright" in column A and that in column C will be the following partition which has the class: 1, 2, 5, 18.

[51] During exploration of test menus for the BP Bombes, one failed to come out as expected. Upon closer investigation Philip Marks discovered that it would work if the neutral position for wheel IV of the Service Enigma was set to Y.

[52] The order of the cycle lengths making up the class is not significant. However, by convention, they are presented in ascending order.

```
(CLXIJSPMNURQOZKGET)(WA)(CBYVH)(F)
```

As the *Umkehrwalze* wiring is reciprocal (involutory), the normal way of finding the substitution from one “upright” to the next will fail. In this case we can form the class of the substitution by going through the UKW wiring and then sliding one position backwards on the diagonal. To illustrate this we will use the Railway Enigma’s UKW substitution in *Ringstellung* A. This is an opportune moment to point out that unlike the Service Enigma, which has a fixed UKW, the machines with a settable or moving UKW have *Ringstellung* for all wheels, including the UKW. The two rows in Fig. 7 are the machine’s diagonal or input sequence together with the UKW substitution. To form the cycle partition we will, as before, progress in a methodical manner

```
QWERTZUIOASDFGHJKPYXCVBNML
NUGZFRWCHXMYTEOLBVDAIPKQSJ
```

Figure 7: The Diagonal and the Substitution for the Umkehrwalze in Ringstellung A.

starting with the first letter in the first row, Q. This is the first letter of the cycle partition. Q’s substitution letter N will not be entered in the cycle but instead we will enter the letter which precedes N on the diagonal, which is B. B’s substitution letter K will not be entered, but K’s preceding neighbour J will be the third letter of the cycle partition, and so on. The resulting partition is given below and is of class: 2, 24.

```
(QBJMAYSNLHIXOGWZEFRTDPCU)(KV)
```

With this method it is also possible to obtain a class of type two for the *Umkehrwalze* substitution. This is developed by sliding two steps back on the diagonal or, in other words, instead of using the directly preceding letter we use the letter which precedes the given letter by two places. For the Railway Enigma’s UKW the cycle partition for a class of type two has the class: 1, 5, 20.

```
(QVJNMOFEDKCZWTSBHULG)(R)(IYAPX)
```

ENIGMA SIMULATORS

This research into the different variants of the Enigma machine was largely initiated by the authors’ desire to create authentic computer simulations of various cipher machines. The aim is to make the simulations as realistic as possible so that they can be used for serious study of the machines themselves as well as being valuable tools for cryptanalytical research. A further aim is to make the machines better known to the wider public, and not just to the few fortunate individuals and organisations that have access to the actual machines.

To make the machines better known to non-experts it was decided very early on to make graphically oriented simulations. Therefore all major moving parts of a machine have been faithfully reproduced in dynamically changing graphic displays. All simulators are designed to run on Intel-based PCs under Windows 3.x and Windows 95/98. At present all the Enigma machines with known wiring have been simulated and most have been certified as accurately reproducing the functions of the real machines.

The Enigma simulators have a normal keyboard entry and the output appears on simulated glow lamps as on the real machine. In addition, both plaintext and ciphertext also appear in two small message windows and can be saved to file for later use and study. The simulators also allow prepared plaintext or ciphertext to be loaded and enciphered or deciphered on the fly. There are various modes for observing the operation of the machine. One is a global view of the scrambler effect which allows the operator to see the complete electrical path for each ciphering step. Other modes give views of all the wheels and plugboard connections.

All the settings of the machine such as wheel selection, wheel order, *Ringstellung* and *Stecker* connections are selectable from within the program. In the case of the service machine the type of machine is also selectable. One can choose between the three-wheel Army/Air Force machine and the three and four-wheel Naval machines. When a machine is selected the simulator will change its appearance and capabilities to that of the selected machine. For example, in the simulation of the Army/Air Force machine only a set of five wheels is available for selection and the rings have numbers instead of letters, etc.

The simulators have not yet been publicly released, but we hope that a suitable distribution policy can be finalised this year. If possible we would like to donate the simulators to institutions with cryptographic collections, such as military and intelligence museums, who would then be responsible for eventual sale and distribution. We also hope to have special versions available for download from the authors' WWW Home Pages. The respective URLs can be found together with the authors' addresses at the head of this paper.

ACKNOWLEDGMENTS

The results presented here are the fruits of archive research and studies of actual machines. However, without the great assistance we have received from many quarters it is doubtful that we would have achieved the results we have. Our helpers are too numerous to thank individually, but we will nevertheless explicitly express our gratitude to Tony Sale, Director of the Bletchley Park Museum Trust, Rudolf Ritter, Jack Ingram and his staff at the National Cryptologic Museum, and the archivists and staff at NARA. We should also like to thank our very good friends and fellow researchers Ralph Erskine and Philip Marks for help with documents, many fruitful discussions, and a thorough review of this paper. The quotations from BP documents, which are Crown copyright, are reproduced with the permission of the Controller of Her Majesty's Stationery Office.

REFERENCES

1. Friedrich L. Bauer. 1997. *Decrypted Secrets, Methods and Maxims of Cryptology*. Berlin: Springer-Verlag.

2. Cipher A. Deavours. 1997. Lobsters, Crabs, and The Abwehr Enigma. *Cryptologia*, 21(3): 193–199.

3. Cipher A. Deavours and Louis Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Norwood, MA: Artech House.

4. Ralph Erskine and Frode Weierud. 1987. Naval Enigma: M4 and Its Rotors. *Cryptologia*, 11(4): 235–244.

5. F.H. Hinsley and Alan Stripp, editors. 1993. *Codebreakers, The Inside Story of Bletchley Park*. Oxford, UK: Oxford University Press.

6. Peter Twinn. 1993. *The Abwehr Enigma*, pp. 123–131. In Hinsley and Stripp [5].

BIOGRAPHICAL SKETCHES

David Hamer has (more or less) retired but retains his interest in things techno-mathematical – in particular: classical cryptology, Enigma and other crypto devices, and computer software applications.

Geoff Sullivan works on the design of scientific instruments, in the areas of software programming and electronic engineering. He has many other varied interests, but is all too easily distracted by cryptography.

Frode Weierud is employed by the European Organization for Particle Physics (CERN) in Geneva. He works as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 30 years. His cryptological research is focused on cipher machines and cryptanalytical techniques.