Facts and myths of Enigma: breaking stereotypes

Kris Gaj[1] and Arkadiusz Orlowski[2]

[1] George Mason University, Electrical and Computer Engineering
4400 University Drive, Fairfax, VA 22030, U.S.A.
kgaj@gmu.edu
[2] Institute of Physics, Polish Academy of Sciences
Aleja Lotników 32/46, 02-668 Warszawa, Poland
orlow@ifpan.edu.pl

Abstract. In spite of a relatively large number of publications about breaking Enigma by the Allies before and during the World War II, this subject remains relatively unknown not only to the general public, but also to people professionally involved in cryptological research. For example, the story of Enigma is rarely a part of a modern textbook on cryptology or a modern course on cryptography and network security. There exist multiple reasons for this situation. First, there are still a few unresolved issues, resulting from conflicting reports, the lack of reliable sources, and a long period required for declassifying documents related to any cryptological activity during the World War II. Secondly, the issue is highly political, and there is little consensus in weighing the contribution of all involved countries. Thirdly, many contemporary cryptologists honestly believe that there is little to learn from the analysis of old cryptosystems, because of the tremendous progress in theory and practice of cryptography and a little similarity between old and modern ciphers. In this paper we confront these opinions by presenting a look at the current state of knowledge about cryptological methods and devices used to break Enigma. We introduce all major players involved in these activities, and we make an effort to weigh their original contributions. Finally, we show that the story of Enigma can still provide contemporary cryptographers with many useful lessons regarding the way of organizing and building any large-scale security system.

Keywords. Enigma, cipher machine, rotor, cryptanalytical bombe, codebreaking.

1 Beginnings of Enigma

Enigma belongs to a group of rotor-based crypto machines. The first such machines were developed and patented independently by several inventors from different countries in the period from 1917 to 1921. The first designers included American Edward Hugh Hebern, German Arthur Scherbius, Dutchman Hugo Alexander Koch, and the Swede Arvid Gerhard Damm [1]. Arthur Scherbius bought Koch's patent, and improved his design. He hoped to sell his machine, named Enigma, to the world's business community, but appeared to be much more successful in a different market. In 1926 German Navy, and in 1928 German Army introduced Scherbius cipher machines that were simple modifications of the commercial version of Enigma. In

1930, a military version of Enigma was developed. The most important innovation was an introduction of the plugboard, a component that significantly increased the number of possible settings of the machine, and thus also a total number of cipher keys. Since mid 1930's, Enigma became universally used in all German armed forces. It is estimated that a total number of Enigma machines used in the period 1935-1945 exceeded 100,000 [13].

2 Machine construction

Enigma was a small portable electromechanical machine equipped with a battery. It had dimensions and looks of a typical typewriter. Its major components and the way of connecting them together are shown schematically in Fig. 1. A keyboard of Enigma included 26 characters of the Latin alphabet. There were no digits, no punctuation characters, no function keys. Instead of type, Enigma had a panel with 26 bulbs of the type used in flashlights. Small windows of the panel were marked with 26 Latin letters, the same as the keys in the keyboard.

When a key of the keyboard was pressed, a bulb associated with a different letter of the alphabet lit. When the pressed key corresponded to a letter of the plaintext, the highlighted letter represented the corresponding character of the ciphertext. Similarly, when a key representing a ciphertext letter was pressed, the corresponding letter of the plaintext lit.

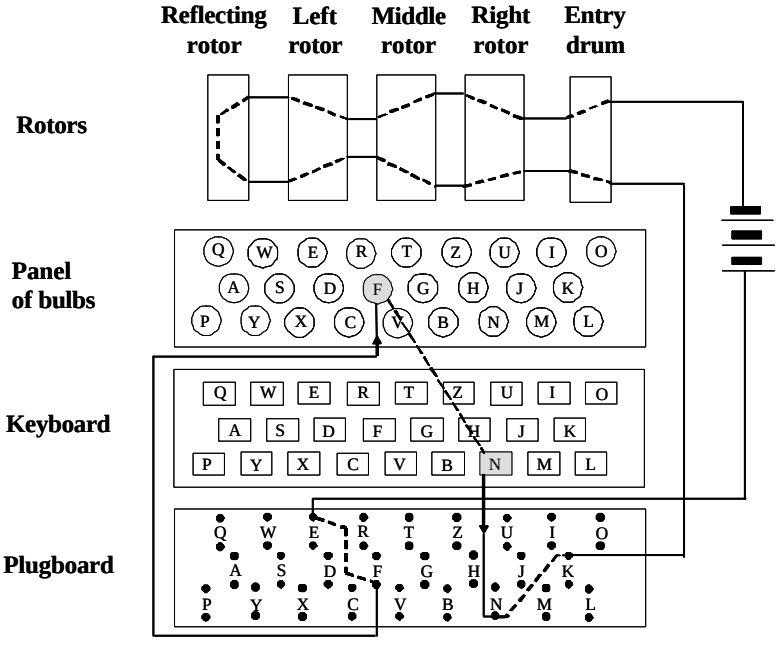

Fig. 1. Functional diagram and the dataflow of the military Enigma.

The main encryption portion of Enigma used in the German army consisted of three variable-position rotors (drums), one fixed reflecting rotor, and one fixed entry drum. Each of the three variable-position rotors had 26 fixed contacts on one side, and 26 spring-loaded contacts on the other side. Internally, contacts of one side were connected in the irregular fashion with the contacts of the other side. The reflecting rotor, placed to the left of the variable-position rotors was fixed, and had 26 spring-loaded contacts located on one side of the rotor. These contacts were connected among themselves in pairs. The entry drum, located to the right of the variable-position rotors, had 26 fixed contacts connected to the sockets of the plugboard.

Whenever a key was pressed, the right rotor made a $1/26^{th}$ of the full revolution. When the right rotor reached a certain position, referred to as a turnover position, the middle rotor turned by $1/26^{th}$ of the full angle. Finally, when the middle rotor reached the turnover position, then both the middle and the left rotors turned by $1/26^{th}$ of the full revolution. This way, each subsequent letter was encrypted using a different setting of rotors, and Enigma implemented a polyalphabetic cipher with a very large period. As a result, a frequency distribution of letters in the ciphertext was almost perfectly uniform, and no attacks based on the classical frequency analysis applied to Enigma.

Each of the three variable-position rotors was equipped with a ring with 26 letters of the alphabet engraved on its circumference. This ring could change its position with respect to the rest of the rotor. A notch on this ring determined the turnover position of the given rotor. The letters of the rings found at the top of the three variable-position rotors were visible through small windows located in a metal lid of the machine. These letters were used to describe the current positions of rotors.

The last component of the military Enigma, not used in the commercial Enigma, was a plugboard (also known as a switchboard). Each letter of the alphabet was represented on the plugboard using a pair of sockets. Connecting two pairs of sockets together had an effect of swapping two letters of the alphabet at the input of the enciphering transformation, and at the output of the enciphering transformation.

Certain components of Enigma were different in the naval version of the machine. For, example a number of main rotors used in the German Navy Enigma was four compared to three in the German Army Enigma.

3 Three secrets of Enigma

3.1 Internal connections of the machine

As in case of majority of military systems, the Enigma machine encryption algorithm itself was secret. The number of possible internal connections of Enigma has been estimated to be approximately $3 \cdot 10^{114}$, compared to the estimated number of 10^{80} atoms in the entire observable universe [6, 15]. Therefore, the internal connections of Enigma clearly could not be guessed, and the only way of discovering them was either through the mathematical analysis or by capturing a copy of the machine.

3.2 Daily keys

The majority of settings of the machine were determined based on the tables of daily keys, which were distributed by couriers to all military units using Enigma. Initially, all units used exactly the same machine and the same daily keys. In 1936, there were already six networks using different sets of daily keys [13].

In the period, 1930-1938, a daily key of Enigma used by German Army consisted of the following settings:

a. order of three rotors inside of the machine – 6 combinations,

b. plugboard connections – about $0.5 \cdot 10^{15}$ combinations,

c. initial positions of rotors – $26^3 = 17{,}576$ combinations,

d. positions of rings that determined reflecting positions of two rotors – $26^2 = 676$ combinations.

Thus, the total number of possible combinations of daily keys was about $3.6 \cdot 10^{22}$ or 2^{75} [6, 15]. This number might look very impressive, one need however remember that the largest contribution came from the plugboard connections that affected only limited number of letters, and that many different keys resulted in very similar encryption transformations. As a result, different components of the daily keys could be reconstructed one by one independently of each other.

3.2 Message keys

If all messages on a given day had been encrypted using the same initial setting of Enigma machines determined by the daily key, the cryptanalysts could have simply applied the frequency analysis to all first letters of the ciphertexts encrypted on a given day, then to all second letters, and so on. To prevent this kind of analysis, a message key, equivalent to a modern day initialization vector (IV), was needed.

In the period, 1930-1938, a message key was composed of three letters that determined the initial settings of three rotors at the moment when the given message started to be encrypted. It is fascinating to see that, similarly to modern day initialization vectors, message key could have been transmitted to the other side in clear. Instead, German cryptographers, striving to accomplish the ultimate security, decided to encrypt message keys using machines set to the positions determined by the daily keys. To make matters worse, to detect possible transmission errors, each message key was encrypted twice, and the obtained six letters were placed in the header of the message. The situation was made even worse, by the fact that message keys were chosen by individual operators themselves, who tended to select simple, predictable patterns, such as three identical letters, or letters corresponding to three neighboring keys on the keyboard.

As a result, this message key distribution procedure appeared to be the weakest link of the Enigma cryptosystem and a source of multiple attacks, including the attack that led to the reconstruction of the internal connections of the machine itself.

The procedure for transferring message keys was changed by Germans in 1938, and then again in 1940, but by then, the internal connections of the machine had already been reconstructed, and the alternative methods of recovering daily keys were developed by Polish and then British cryptologists shortly after each change.

4 Reconstruction of the internal connections of Enigma by a Polish mathematician Marian Rejewski

Poland was the first country that recognized the adoption of the machine-based cipher by Germans. The first sign of this recognition was a purchase of a copy of the commercial version of Enigma. Since the military version of Enigma had been substantially modified compared to its commercial counterpart, little knowledge was gained regarding the actual machine used by the German armed forces. In 1929, Polish Cipher Bureau organized a cryptology course for over 20 students of mathematics at the University of Poznan. Three of the most talented students were later hired to work on breaking Enigma. The most advanced of these students, Marian Rejewski, was the first to be assigned to investigate the strength of the new German cipher.

Rejewski started his work by first analyzing the beginnings of the intercepted German cipher messages. In 1932, those beginnings were composed of a special group of six letters that resulted from two successive encryptions of three letters of the message keys. The keys were different for each message but they were encrypted with the same setting (daily key) of the Enigma machine. This observation led to a given below set of equations, in which permutations played a part of unknowns:

$$
\begin{aligned}
A &= S H \quad R' \quad T' \quad R'^{-1} \quad H^{-1} S^{-1} \\
B &= S H Q \quad R' Q^{-1} \quad T' \quad Q R'^{-1} Q^{-1} \quad H^{-1} S^{-1} \\
C &= S H Q^2 \quad R' Q^{-2} \quad T' \quad Q^2 R'^{-1} Q^{-2} \quad H^{-1} S^{-1} \\
D &= S H Q^3 \quad R' Q^{-3} \quad T' \quad Q^3 R'^{-1} Q^{-3} \quad H^{-1} S^{-1} \\
E &= S H Q^4 \quad R' Q^{-4} \quad T' \quad Q^4 R'^{-1} Q^{-4} \quad H^{-1} S^{-1} \\
F &= S H Q^5 \quad R' Q^{-5} \quad T' \quad Q^5 R'^{-1} Q^{-5} \quad H^{-1} S^{-1}
\end{aligned}
$$

This set of equations consists of six equations with four unknown permutations: S, H, R', T'. These unknown permutations represent respectively:

S – permutation determined by the plugboard connections,

H – fixed permutation determined by the connections between the sockets of the plugboard and connectors of the fixed entry drum,

R' – permutation determined by the internal connections of the right rotor,

T' – the combined permutation determined by the internal connections of the middle, left, and fixed reflecting rotor.

Out of the remaining seven permutations:

Q is a simple permutation that changes each letter into the letter immediately following it in the alphabet, e.g., "a" to "b", "b" to "c", …, "z" to "a".

A-E are known permutations that have been determined by Rejewski based on the analysis of the enciphered message keys, combined with an assumption that a significant percentage of the message keys was chosen by operators to consist of three identical letters of the alphabet.

To this day, it is not known whether this set of equations can be solved at all. Fortunately, by the time Rejewski was trying to solve this intricate problem, he received some unexpected help. Capt. Gustave Bertrand – chief of radio intelligence

section of the French Intelligence Service supplied the Polish Cipher Bureau with information originating from the paid agent, Hans-Thilo Schmidt, pseudonym Asche, who was working in the cryptographic department of the German Army. The material included among other things, tables of daily keys for two consecutive months, September and October 1932 [2, 13, 18]. However, it contained no information about the internal wirings of the Enigma rotors. Nevertheless, the material proved to be very important for Rejewski. The tables of daily keys unmasked his third permutation, S, which represented the plugboard connections of the machine. The second permutation, H, remained a tantalizing secret, but Rejewski was lucky enough to discover it by his imaginative guessing. It appeared that in contrast to the commercial version of Enigma, in the military version of the machine, this transformation was chosen to have a form of identity permutation (e.g., it transformed "a" to "a", "b" to "b", etc.). The obtained set of equations, now with two unknown permutations only, R' and T', was for Rejewski rather easy to solve. The solution of one set of equations divulged the connections of the rotor that was placed, in a given day, as a most right one. The two tables of daily keys for two months belonging to different quarters, supplied by the French, made it possible to find the connections of two rotors. The rest of unknowns was now easier to find, and was reconstructed shortly after with an additional help of a fragment of the German instructions for using Enigma, delivered by Asche, containing an authentic pair plaintext-ciphertext for a sample daily key and a sample message key [18].

In his unpublished manuscript [19], Rejewski has demonstrated, that he could have reconstructed internal connections of Enigma rotors, based on the knowledge of only one daily key and without the need of guessing permutation H. Although this method required access to the radio intercepts (enciphered message keys) over a longer period of time (about a year), and involved more time consuming computations, nevertheless it could have led to reconstructing internal connections of Enigma even if the material provided by the French intelligence was limited to a single table of daily keys [6, 19].

5 Polish methods of recovering cryptographic keys

Mastering the internal connections of the rotors would have remained useless if effective procedure for a systematic reconstruction of daily keys had not been developed. In the period 1932-39, several such methods have been invented by three Polish cryptologists, Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski. The necessity of elaborating so many methods resulted from subsequent changes made in the key distribution procedure and the machine itself by Germans.

The following key recovering methods appeared to be the most effective:

- method of "grill," which was applied together with methods of "distinct letters," "Rozycki's clock," and so called "ANX" method,
- catalog of "characteristics," developed with the help of a special device called "cyclometer",
- Zygalski's perforated sheets,
- Polish cryptological "Bomby".

5.1 Grill method

The grill method, used in the period 1933-36, consisted of a series of paper-and-pencil procedures aimed at reconstructing all components of the daily key, one by one [18].

The first step was to find unencrypted message keys as well as permutations A-F used in the equations (1)-(6). The analysis of the enciphered message keys, belonging to about 70-80 intercepted Enigma ciphertexts was initially revealing only the value of products AD, BE, CF. To obtain separate values of permutations A-F, the Polish cryptologists used the knowledge of habits of Enigma operators regarding the choice of three letters of the message keys. In the period 1931-32, the quite common habit was to choose message keys composed of three identical letters. When this choice was forbidden by German procedures, the operators tended to choose three letters that appeared on three neighboring positions of the Enigma keyboard. When such patterns were forbidden as well, Polish cryptologists came up with the method of "distinct letters". This method was based on the fact that when operators were forbidden to use three identical letters, they also subconsciously avoided any message keys in which only two letters repeated. This small statistical bias, combined with the knowledge of the theory of permutations, appeared to be sufficient to reconstruct permutations A-F, as well as all individual message keys for a given day.

The next step was to determine which of the three rotors was placed on a given day on the right-most position. Rozycki's "clock method" relied on the property of Enigma that the position of the right-most rotor at which the middle rotor moved was different for each of the three rotors used by the German Army. By statistical analysis of two ciphertexts encrypted using similar message keys (and thus also similar machine settings), it was possible to determine at which position of the right-most rotor, the middle rotor moved, and thus to determine the choice of the right rotor [6, 18].

The main part of the grill method was devoted to the reconstruction of the connections of the plugboard. This method was based on the fact that the plugboard did not change all letters. The entire procedure has been automated by shifting a sheet of paper with permutations A-F over a sheet of paper with transformations of the form $Q^{-x}RQ^{x}$, for x=0..25 (where R represents the transformation of the right rotor), and looking for a value of x for which appropriate correlations exist between related permutations obtained in six subsequent rows. This procedure was revealing both the plugboard connections, and the position of the right rotor [6, 18].

Next, the order and positions of the middle and left rotor were found using an exhaustive search involving 2x26x26=1352 trials based on the encrypted and unencrypted message keys. Finally, the location of the rotor rings was determined using another search based on the fact that majority of German messages started from the letters "an" (German for "to") followed by "x" (used instead of space) [6, 18].

5.2 Catalog of "characteristics"

A method of the catalog of characteristics, used in the period 1936-1938, was based on the fact that a format of the products of permutations AD, BE, and CF depended on the order and the exact settings of rotors, and did not depend on the plugboard

connections [18]. By a format of a permutation, we mean the length of cycles in the representation of a permutation in the form of a product of disjunctive cycles. For example, a permutation of 26 letters can have a form of anything between:

$(a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}\ a_{12}\ a_{13})\ (b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13})$,

where a_1 is transformed to a_2, a_2 to a_3, …, and a_{13} back to a_1, as well as, b_1 is transformed to b_2, b_2 to b_3, …, and b_{13} back to b_1,

up to

$$(a_1)\ (a_2)\ (a_3)\ (a_4)\ (a_5)\ (a_6)\ (a_7)\ (a_8)\ (a_9)\ (a_{10})\ (a_{11})\ (a_{12})\ (a_{13})$$
$$(b_1)\ (b_2)\ (b_3)\ (b_4)\ (b_5)\ (b_6)\ (b_7)\ (b_8)\ (b_9)\ (b_{10})\ (b_{11})\ (b_{12})\ (b_{13}),$$

where each letter is transformed to itself.

This pattern of cycle lengths was extremely characteristic for each daily key, and therefore was named by Rejewski a “characteristic of a day”. Based on the individual properties of permutations A-F, the products AD, BE, and CF can have 101 different cycle length patterns each, or 101^3 = 1,030,301 different cycle patterns (“characteristics”) as a total. On the other hand, there are only $3! \cdot 26^3$ possible arrangements (orders and settings) of three rotors. That meant that it was quite likely that a given “characteristic” corresponded either to a unique arrangement of rotors or at least to a small number of arrangements that could be easily tested.

To make this method practical, it was necessary to create a catalog of “characteristics” for all $6 \cdot 26^3$ = 105,456 rotor orders and settings. Given a cycle pattern for permutations AD, BE, and CF, this catalog returned the corresponding order and setting of rotors. With known positions of rotors, the plugboard connections could be determined relatively easily, and the ANX known-plaintext method was still used to determine the ring settings. To create a catalog of characteristics, Rejewski designed, and Polish engineers implemented an electromechanical device called cyclometer, a predecessor of Polish “Bomba” and British “Bombe” [6, 13, 18].

5.3 Polish “Bomba”

As a result of the major change introduced in the Enigma key distribution procedure on September 15, 1938, all previously developed methods of recovering daily keys lost their significance. Starting from this date, each Enigma operator was choosing by himself the initial settings of rotors used to encrypt message keys. These positions were then transmitted in clear in the header of the ciphertext, and were not any longer identical for all operators.

Polish “Bomba”, developed in November 1938 by AVA Radio Manufacturing Company, based on the design of Marian Rejewski, was a Polish response to this change. Polish “Bomba” consisted of an aggregate of six Enigma machines, operating in concert, starting from some initial settings determined based on the analysis of the encrypted message keys. With an appropriate input, Polish “Bomba” was able to determine the correct positions of rotors within two hours. The plugboard connections, and the ring settings were determined similarly as before [6, 13, 18].

5.4 Zygalski's perforated sheets

Zygalski's method, developed at the end of 1938, required the application of special paper sheets. Many computations and manual trials were necessary to produce such sheets, as it was a complicated and time-consuming task [6, 13, 18].

The key recovering method was based on the fact that out of 26^3 possible rotor settings, only 40% led to the AD permutation that included at least one pair of one-letter cycles (a_1) (a_2). A separate sheet was created for each position of a left rotor. Each sheet contained a square matrix corresponding to all positions of the right and middle rotors. Fields of the matrix corresponding to the positions of rotors with single-letter cycles were perforated [18].

In each day, several encrypted message keys led to the permutations AD with a one letter-cycle. Based on the rotor settings used to encrypt message keys, which were sent in clear in the header of the ciphertext, cryptanalists were able to determine the relative positions of rotors leading to single-letter cycles.

During the analysis, the Zygalski's sheets were superimposed, and displaced in the proper way in respect to each other. The number of apertures that shone through gradually decreased, and finally only one, or at most a few fields remained with apertures that shone through all the sheets. The corresponding positions of rotors remained as potential suspects for further testing.

With three rotors to choose from, there were 3!=6 possible combinations of rotors. A set of 26 perforated sheets had to be fabricated for each such combination. Unfortunately, because of the limited resources of the Polish Cipher Bureau, from the end of 1938 till September 1, 1939, only two sets of perforated sheets had been fabricated. To make things worse, on December 15, 1938, Germans introduced two additional rotors. Although the machine itself did not change, and only three rotors were used at a time, these three rotors were now chosen from a set of five rotors available with each Enigma machine. This change increased the number of possible combinations of rotors to 60. As a result, Polish capabilities for recovering Enigma keys substantially decreased in the months immediately proceeding the World War II.

6 Passing a copy of the reconstructed Enigma machine to the representatives of the French and British intelligence

On July 24-26, 1939, in Pyry in the Kabackie Woods outside Warsaw a historic meeting took place. The Polish side was represented by three cryptologists (Rejewski, Rozycki, Zygalski) and two officers of the Polish Cipher Bureau (Langer, Ciezki). The French side was represented by Gustave Bertrand and Henri Braquenie, and the British side by Alastair Denniston, Alfred D. Knox, and one more officer (most likely Humprey Sandwith). During this meeting, Polish passed two copies of the reconstructed Enigma machine to French and British respectively. Similarly, the detailed documentation of Zygalski's sheets and Polish "Bomby" and other Polish methods was discussed and passed to the representatives of both countries. The meeting came as a big surprise for French and British intelligence, as by that time

they were completely unaware of the Polish progress with breaking Enigma, and did not make any substantial progress with breaking Enigma cipher by themselves.

7 Operation of the Bletchley Park center and British methods of reconstructing Enigma keys

In the Summer of 1939, Britain's Government Code and Cypher School (GC&CS) moved from London to a Victorian manor in Bletchley, north-west of London, called Bletchley Park. Initially, the entire center counted no more than thirty persons, but it continuously grew, up to the level of about 10,000 employees.

Britain, like Poland, began hiring mathematicians to work on codebreaking, and two of them, Alan Turing and Gordon Welchman, became instrumental to the center success with breaking Enigma [8, 9, 23, 25, 26]. Both of them came from Cambridge University.

Initially, British adapted Polish methods. For example, by the end of 1939 they managed to fabricate all 60 sets of Zygalski's sheets and used this method under the name "Jeffrey's apparatus" till May 1940. On May 10th, 1940, the day of attack at France, Germans changed again their key distribution procedure. The change was to encrypt each message key only once, except of twice. This seemingly minor change made all previous methods of reconstructing keys obsolete.

Fortunately, shortly after, British cryptologists managed to come up with some impromptu methods. First of them relied, similarly to early Polish methods, on exploiting bad habits of a few Enigma operators, and included so called Herivel tips and "sillies". For example, a lot of operators, after inserting rotors to the machine, did not change their locations before starting working on the first message. Since the rotors were typically inserted into the machine using a specific orientation, the analysis of several ciphertext headers for the first messages of the day often revealed a significant portion of a daily key. The other common error was to use the same triple of letters for both: an initial position of rotors (sent in clear), and for a message key (sent in an encrypted form) [25].

Nevertheless, the major breakthrough was the invention and development of the British "Bombe". Unlike Polish "Bomba", British "Bombe" was based not on the key distribution procedure, but on the known-plaintext attack [8, 25, 26].

British "Bombe" exploited stereotype forms of many messages enciphered using Enigma which were transmitted within the German armed forces networks during the World War II. These stereotype wordings were responsible for so called "cribs" – fragments of plaintext that cryptologists were able to guess.

In Bletchley Park, a special division, called Crib Room, was responsible for finding new cribs on a regular basis [25]. The sources of these cribs were numerous. For example, German messages typically contained full data about senders and receivers, including full titles and affiliations, as well as stereotypical greetings. These data were easy to guess based on the knowledge of the interception station the encrypted messages came from, as well as control information included in the unencrypted headers of the ciphertexts. Other sources included stereotypical reports (such as having nothing to report), easily predictable weather forecasts, or messages

retransmitted between networks using different daily keys (in which case it was sufficient to break a key of one network to obtain a significant crib for another network).

The idea of the British "Bombe" came from Alan Turing, and a significant improvement, so called "diagonal board" was proposed by Gordon Welchman. The technical realization was a responsibility of Harold "Doc" Keen, an engineer at British Tabulating Machines (BTM) [8, 25, 27].

From the cryptological point of view British "Bombes" were very different from Polish "Bomby," nevertheless the goal of operation was the same: find positions of rotors that could not be excluded as possibly being used at the start of encryption. The big advantage of British "Bombes" was that they did not rely on the key distribution procedure, which had constantly evolved and made previous methods obsolete. The certain disadvantage was the reliance on cribs, which might have been guessed incorrectly.

From the engineering point of view, British devices resembled Polish "Bomby". Each "Bombe" contained 12 sets of three rotors each, and was working synchronously through all possible rotor positions. Each "Bombe" weighed one ton, and was 6.5 feet high, 7 feet long, 2 feet wide. "Bombes" were operated by members of the Women's Royal Naval Service, "Wrens", who were responsible for initializing machines, writing down rotor combinations found by the machine, and restarting machines after each potentially correct combination was discovered. A single run for a given combination of rotors lasted about 15 minutes. To test all 60 possible combinations of rotors, 15 hours were needed.

The first Bombes were put in use in October 1941. They had their names, such as Agnew, Warspite, Victorious, or Tiger. Approximately 210 Bombes were built and used in England throughout the war.

8 Participation of United States in the production of cryptological "Bombes"

Representatives of both U.S. Army and Navy visited Bletchley Park as early as 1941, and they became aware of the British success with Enigma [23, 27]. Nevertheless, initially GC&CS was not very forthcoming with the details of the British methods. The situation changed in summer 1942, when it became apparent that due to limited resources British had to delay their plans for building a new high-speed four-rotor "Bombe" capable of breaking naval Enigma. U.S. Navy assigned the design to Joseph Desch, the research director of the National Cash Register Company (NCR) based in Dayton, Ohio [27]. The American design was based on the same cryptological principles as the British "Bombe", but it was improved from the engineering point of view. In particular, less human intervention was necessary, and the machine was capable of printing all rotor settings that could not be eliminated based on the crib used for the machine initialization. Like the British version, the American Bombes usually found two or three possible correct solutions. A single run for one combination of rotors lasted about 20 minutes. In May 1943, the first two American "Bombes", Adam and Eve, were successfully tested. In summer 1943, "Bombes"

started to be transferred from Dayton, Ohio to Washington, D.C. They were operated by women in the U.S. Navy, so called “Waves” (Women Accepted for Volunteer Emergency Service). Approximately 120 Bombes were built and put into operation before the end of the World War II.

9 Lessons from breaking Enigma

Breaking Enigma offers clear lessons to future designers of cryptographic algorithms, protocols, and systems. First keeping machine, and thus a cipher, secret did not help. Army Enigma was ingeniously reconstructed by Polish Marian Rejewski, based on his mathematical analysis supported by tables of daily keys for the period of two months obtained by French intelligence. Naval Enigma was captured by British navy from the sinking German U-boats. Large number of keys, comparable to that used in modern ciphers, did not help, because the best methods developed by Polish and British cryptologists did not involve exhaustive key search. Instead, these methods allowed codebreakers to reconstruct various components of the daily key one by one. Additional help came from applying electromechanical machines for cryptanalysis, which allowed to speed up the most time-consuming and repetitive phases of the cryptological analysis. In this respect, Polish “Bomby” and British and American “Bombes” were precursors of the modern-day specialized hardware. Similarly, Zygalski’s perforated sheets might be considered as a first application of the optical methods in cryptanalysis.

Known-plaintext attack was easy to mount, because of the stereotypical structure of many messages, easy to predict standard reports, and retransmission of messages between multiple networks using different daily keys. The first known-plaintext attacks against Enigma came from Polish in the form of the ANX method, and were perfected by British with their Crib Room, and the Cryptological “Bombe”.

Key management, in the form of an encrypted exchange of message keys, was the weakest link of the Enigma protocol, as it allowed not only to develop multiple methods of reconstructing daily keys, but also endangered the secrecy of the cipher machine itself. Interestingly, key management remains the weakest link of multiple modern day systems and protocols.

Additionally, multiple methods developed by the Polish and British cryptologists relied on bad habits or unconscious decisions of Enigma operators related to the choice of message keys. The clear conclusion from this lesson is to not let people generate cryptographic keys.

In other respects, people were also the weakest link of the system. German Hans-Thilo Schmidt offered his services to the French intelligence in exchange for money. German cryptologists overestimated the strength of the Enigma cipher. The crews of German U-boats failed to destroy all machines and secret documentation, when their submarines were sunk by British forces.

Finally, the ultimate lesson is to never underestimate the amount of money, time, people, attention, and risk the opponent can use. The operation of breaking German messages by British cryptological center in Bletchley Park required the involvement of thousands of people, perfect organization, attention to details, and grand vision.

Based on their own attempts to break Enigma and experiences with breaking ciphers of other countries, German cryptologists never believed that Enigma could have been broken either before or during World War II. This story demonstrates that authors of a cryptosystem can rarely correctly evaluate its true security.

10 Summary and open problems

Many aspects of the Enigma story still enjoy a splendid obscurity. Some well-established facts are not widely known, some strange artifacts are still deeply believed in, and some facts-to-be are just still hidden from the public. In our lecture we will try to give a complete, detailed, and possibly impartial presentation of the Enigma story. It is not an easy task. Despite the fact that more than 50 years elapsed from the end of the WWII some archives are still kept classified. For example, only recently the British authorities decided to reveal parts of the materials from Bletchley Park, including some details of the Turing inventions [24].

We will present some new facts, documents and pictures never published before, coming from private files of Marian Rejewski, one of the Polish Enigma busters, as well as other sources. We also hope to shine new light into some historical puzzles about the collaboration between Poland, France and Great Britain. Some essential technical details of the Polish and British methods of breaking the Enigma cipher will be given and some related mathematical questions (concerned with permutations and solving a set of permutation-based equations) will be (re)formulated in the form of the PhD-level "research projects". Also many not so-well-known personal details regarding the later years and ultimate fate of main heroes of the Enigma story will be provided.

Some effort will also be made to explain possible sources of discrepancies between different versions of the Enigma stories scattered trough the literature.

Let us finish with some questions still waiting for unambiguous answers. Why Polish authorities in 1932 provided Rejewski with only two sets of keys gained by espionage (it seems that Asche, working for French intelligence, provided a larger set of keys and that these keys were sent by Bertrand to Poland [21])? Did they want to test Rejewski's ability to work without such an external support in future? Why British authorities decided not to hire Rejewski and Zygalski at Bletchley Park when two Poles (with a well-founded reputation as cryptoanalysts) eventually reached Great Britain (from southern France, through Spain, Portugal, and Gibraltar [13])? The necessity of keeping secret is not totally convincing as both knew the fact that Enigma can be broken and invented themselves a lot of tools for the Enigma cryptanalysis. They even met with Turing in France – in Rejewski's memoirs there is a nice passage about meeting Turing and his sense of humor). Instead Rejewski and Zygalski were engaged in solving other ciphers (mainly double Playfair used by SS) working in a Polish military unit (eventually they were promoted to an officer rank; before landing in England they served as civilians) [13]. Were Germans really completely unaware (say at the end of the WWII) of the fact that Enigma was (or at least could be) broken? Or it was just too late to change anything?

References

1. F. L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, 2nd edition, Springer-Verlag, Berlin 2000.
2. G. Bertrand, *Enigma ou la plus grande enigme de la guerre 1939-1945*, Plon, Paris, 1973.
3. *Bletchley Park*, web page available at http://www.bletchleypark.org.uk/
4. G. Bloch and R. Erskine, "Enigma: The Dropping of the Double Encipherment," Cryptologia, vol. 10, no. 3, Jul. 1986.
5. R. Erskine, Enigma, web page available at http://uboat.net/technical/enigma.htm.
6. K. Gaj, *German Cipher Machine Enigma – Methods of Breaking*, Wydawnictwa Komunikacji i Lacznosci, Warszawa, 1989 (in Polish).
7. F. H. Hinsley, *British Intelligence in the Second World War*, 2 volumes, London: Her Majesty's Stationery Office, 1979, 1981.
8. A. Hodges, *Alan Turing: The Enigma*, London, Burnett Books, 1983.
9. A. Hodges, *The Alan Turing Home Page*, available at http://www.turing.org.uk/turing/
10. D. Kahn, *The Codebreakers*: *The Story of Secret Writing*, 2nd edition, Scribner, New York, 1996.
11. D. Kahn, *Seizing the Enigma*, Houghton Mifflin, Boston, MA, 1991.
12. R. Kippenhahn, *Verschluesselte Botschaften. Geheimschrift, Enigma und Chipkarte*, Rowohlt Verlag, Reinbek bei Hamburg, 1997.
13. W. Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, Edited and Translated by Christopher Kasparek, Frederick, Maryland: University Publications of America, Inc., 1984.
14. L. Maziakowski, *Enigma Cipher Machine – History of Solving*, web page available at http://home.us.net/~encore/Enigma/enigma.html
15. A. R. Miller, The *Cryptographic Mathematics of Enigma*, Center for Cryptologic History, National Security Agency, 1996.
16. W. Momsen, *Codebreaking and Secret Weapons in World War II*, available at http://home.earthlink.net/~nbrass1/enigma.htm
17. A. Orlowski, "The mystery of Enigma," VI National Conference on Applications of Cryptography – Proceedings, Warsaw, Poland, pp. K-103:K-107 (in Polish).
18. M. Rejewski, "An application of the theory of permutations in breaking the Enigma cipher", Applications of Mathematicae, Polish Academy of Sciences, vol. 16, pp. 543-559, 1977.
19. M. Rejewski, *Enigma (1930-40). Method and history of solving the German machine cipher*. Unpublished Manuscript (in Polish).
20. T. Sale, *Codes and Ciphers in the Second World War: The history, science and engineering of cryptanalysis in World War II*, web page available at http://www.codesandciphers.org.uk/
21. H. Sebag-Montefiore, *Enigma: The Battle for the Code*, John Wiley & Sons, New York, 2000.
22. S. Singh, *The CodeBook, The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999.
23. M. Smith, *Station X: Decoding Nazi Secrets*, TVBooks, New York, 1999.
24. A. M. Turing, Turing's *Treatise on Enigma*, Unpublished Manuscript.
25. G. Welchman, *The Hut Six Story*, McGraw Hill, New York, 1982.
26. G. Welchman, "From Polish Bomba to British Bombe. The Birth of Ultra," Intelligence and National Security I, no. 1 (Jan.), pp. 71-110, 1986.
27. J. E. Wilcox, *Solving the Enigma: History of the Cryptanalytic Bombe*, Center for Cryptologic History, National Security Agency, 2001.
28. F. W. Winterbotham, *The Ultra Secret*, Weidenfeld & Nicolson, London, 1974.

Appendix 1

Timetable of events related to the development, use, and breaking of ENIGMA.

Dec. 1917	Dutchman Hugo Koch develops a rotor machine, predecessor of Enigma.
Feb. 18, 1918	German Arthur Scherbius files a patent for Enigma Cipher Machine.
Apr. 18, 1918	Arthur Scherbius offers Enigma machine to the German Navy.
Feb. 1926	German Navy begins using Enigma machine.
Jul. 15, 1928	German Army begins using Enigma machine.
1928	Polish Cipher Bureau recognizes the use of machine encryption by Germans.
1928-1929	Polish Cipher Bureau decides to purchase a copy of the commercial version of Enigma.
1929	Polish Cipher Bureau organizes a cryptology course for over 20 students of mathematics at the University of Poznan. Three of the most talented students are later hired to work on breaking Enigma.
Jun 1, 1930	German armed forces start using significantly modified military version of Enigma.
Oct. 1931	Hans-Thilo Schmidt, pseudonym Asche, an employee of the German Cipher Bureau approaches the agents of the French Intelligence Service (S.R.F) and proposes to deliver classified documents.
Nov. 8, 1931	Captain Gustave Bertrand, head of the crypto-service of the S.R.F. receives the first set of documents from Asche.
End of 1931	French Cipher Bureau declares Enigma unbreakable and documents useless. British Cipher Bureau receives the documents, files them, and gives no follow-up offer of collaboration.
Dec. 7-11, 1931	Captain Bertrand visits Warsaw and supplies Polish Cipher Bureau with documents provided by Asche. Two sides agree to share all information.
1932	Based on the analysis of the commercial version of Enigma and intercepted ciphertexts, Polish cryptanalyst Marian Rejewski creates a mathematical model of Enigma in the form of a set of equations with permutations as unknowns. Unfortunately, the number of unknown variables appears to be greater than the number of equations necessary to solve the created set of equations.
End of 1932	Asche delivers to Bertrand a table of daily keys for a number of months. These keys are shared with the Polish Cipher Bureau in December 1932.
Dec. 1932	Tables of keys delivered by Asche enable Rejewski to reduce

	the number of unknowns, solve the equations, and as a result reconstruct the internal wirings of the three Enigma rotors. Poles begin solving German Army messages.
1934	The first replica of the Enigma machine built by AVA Radio Workshops, Polish company based in Warsaw.
1932-39	Three Polish cryptologists: Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki develop sophisticated methods of reconstructing daily keys, including Rozycki's clock method, Rejewski's cyclometer, Zygalski's perforated sheets, and Polish "Bomba".
Dec. 15, 1938	Germans introduce two new extra rotors. Three rotors used on a given day are chosen from a set of five rotors. The number of combinations increases by a factor of 10.
Jul 25-26, 1939	A secret meeting takes place in the Kabackie Woods near the town Pyry (South of Warsaw), where the Poles hand over to the French and British Intelligence Services their complete solution to the German Enigma cipher, and two replicas of the Enigma machine.
Summer, 1939	British Government Code and Cipher School (GC&CS) creates a cryptologic center in Bletchley Park, England. Among British mathematicians hired to work on breaking Enigma are Alan Turing and Gordon Welchman, both mathematicians from Cambridge University.
1939-1940	Alan Turing develops an idea of the British cryptological "Bombe" based on the known-plaintext attack. Gordon Welchman develops an improvement to the Turing's idea called "diagonal board". Harold "Doc" Keen, engineer at British Tabulating Machines (BTM) becomes responsible for implementing British "Bombe".
Jan. 6, 1940	British break into Luftwaffe Enigma.
May, 1940	First British cryptological "Bombe" developed to reconstruct daily keys goes into operation.
1940-1945	Over 210 "Bombes" are used in England throughout the war. Each "Bombe" weighed one ton, and was 6.5 feet high, 7 feet long, 2 feet wide. Machines were operated by members of the Women's Royal Naval Service, "Wrens".
Feb. 12, 1940	British seize two of the three unknown rotors used in the naval Enigma from a crew member of the U-33 captured after the submarine was sunk in Scotland's Firth of Clyde.
Apr. 26, 1940	British seize a canvas bag thrown overboard of the German attack vessel approached by British warships. The bag contained cryptographic documents essential in solving German naval Enigma traffic.
May, 1940	First break into Naval Enigma.
Aug., 1940	The last unknown naval rotor obtained from a naval capture.
Feb.-Mar., 1941	Two US Army and two US Navy cryptanalysts visit

	Bletchley and learn Enigma cryptanalysis.
May, 1941	Britain captures German submarine U-110 with all its encryption equipment and keys intact.
Feb., 1942	German Navy introduces new version of the four-rotor Enigma machines and an additional code referred as “Shark”.
Jul., 1942	U.S. Navy officers visit Bletchley Park and learn the details of the British “Bombe”.
Sep., 1942	The development of the American “Bombe” starts.
Oct., 1942	Important documents retrieved from the sunken German submarine, U-559. Blackout period ends.
Apr., 1943	The production of the American “Bombe” starts in the National Cash Register Company (NCR) in Dayton, Ohio. The engineering design of the “Bombe” comes from Joseph Desch.
1943	77 American Navy “Bombes” constructed and transferred for a continuous operation in Washington D.C. Each “Bombe” was 7 feet high, 10 feet long, 2 feet wide. Machines were operated by women in the U.S. Navy, “Waves” (Women Accepted for Volunteer Emergency Service).
1944	About 44 additional American “Bombes” built and put into action.