From Poznań to Bletchley Park : the history of cracking the ENIGMA machine:

Marie-José Durand-Richard[1]
Philippe Guillot[2]

INTRODUCTION

During World War II, the Allies could read many of the German ciphered messages they intercepted in plain text almost immediately, providing them with an advantage that had a significant impact on the course of the conflict. Movies such as *Enigma* (1999) and *The Imitation Game* (2015), highlight the success of the work of the British at Bletchley Park, and particularly the work of the mathematician Alan Madison Turing (1912-1954). But Turing did not work alone on breaking the Enigma code at Bletchley Park, and it is much less well-known that during the 1930s, the Poles had already accomplished the feat of making transparent the enciphered communications between the German army and its General Staff. So, the history of breaking the Enigma code is rather more complicated than is shown in such hagiographic movies.

In this perspective, this paper focuses on the various skills at work in cracking the Enigma machine. In the period from 1932 to 1942, both the French and the British considered military intelligence would be more essential than mathematical cryptanalysis in overcoming the problem. However, their political and geographical situation stimulated the Poles to coordinate their technical, mathematical and political capabilities. Cyclometers, *Bombas* and perforated sheets were produced to help them overcome complications gradually introduced by the German armies in their Enigma ciphering methods.

As early as 1936, the British codebreaker A. Dillwyn (Dilly) Knox (1884-1943) started a manual cryptanalysis of the commercial Enigma code at the Government Code and Cipher School (GC&CS) and succeeded in breaking the code of its Spanish and Italian versions in 1937. The threat of invasion by the Germans led the Poles to communicate their Enigma codebreaking achievements to their French and British Allies. When the GC&CS moved to Bletchley Park at the outbreak of the war, it

[1] Honorary Lecturer, University Paris 8 Vincennes-Saint-Denis. Associate Researcher SPHERE Laboratory, UMR 7219 CNRS – Université Paris Diderot. marie-jo.durand-richard@orange.fr.

[2] Assistant Professor, University Paris 8 Vincennes-Saint-Denis. Mathematics and History of Science Department. philippe.guillot@univ-paris8.fr.

underwent a radical change of scale, enforcing deploying enormous efforts to face the huge quantity of communications traffic generated by the German military in their newly adopted art of war, the *Blitzkrieg.* Bletchley Park became a real cryptanalysis factory, where research work was carried out collectively, and developed continuously throughout the war. Analysis of all this traffic and the enumerable trials required to achieve the deciphering process would have been impossible to complete without the help of machines such as British and US *Bombes.* However, even these machines would have been useless, or at any rate inefficient, without preliminary human work and military operations.

The design and manufacture of another machine, Colossus, took place in the final years of the war. This electronic machine, the first in the world, was designed to work against the Lorenz machine which enciphered infrastructure communications, and not against the Enigma machine which was devoted to tactical communications. Colossus was produced mainly by a team led by Maxwell Hermann Alexander – Max – Newman (1897-1984),with the help of the Post Office Research Station at Dollis Hill. Over this period, after his stay in the United States between November 1942 and March 1943, Turing was more interested in research on an advanced speech security system, for the Radio Security Service of the Secret Services, located at Hanslope Park near London, outside Bletchley Park. All this work was very influential on the course and the duration of the war, and fundamentally marked the future of cryptology.

ENIGMA: A NEW CIPHERING MACHINE

1. First rotor machines

The Enigma machine used by the Germans belongs to the family of rotor ciphering machines. These machines appeared after the First World War, during the return to business at the end of the hostilities, taking advantage of the development of wireless telegraphy. Several inventors filed patents almost simultaneously for similar machines.

In 1915, the American Hebern Edward (1869-1952) linked two electric typewriters with irregular wiring so that a key pressed on the first machine would print a different letter on the second. This process of simple substitution reproduces the regularities of natural language and is known to be easy to decipher with a little training. Hebern corrected this weakness by inserting a rotating drum, which turns for each key pressed, and thereby varies the ciphering alphabet. He filed his patent in 1918.

The history of Enigma machines is worthy of the best espionage novels. In 1915, during World War I, and in the greatest secrecy, two engineers from the Dutch navy, Theo van Hengel (1875-1939) and Rudolf Pieter Cornelis Spengler (1875-1955) developed a rotor ciphering machine. After the Armistice, they sought to patent their invention and addressed an agency that asked them to wait for approval from the Dutch navy. Before they received it, Hugo Alexander Koch (1870-1928), the brother-in-law of a certain Huybrecht Verhagen, an employee of the agency, filed a patent on October 7, 1919 for a "secret writing machine". In 1922, the company *Naamlooze Venootschap Ingenieursbureau* "Securitas", was founded to exploit this patent, and was finally absorbed in 1927 by the Gewerkshaft Securitas, the company owned by German engineer Arthur Scherbius (1878-1929), who had previously filed similar patents

[BAU]. Scherbius called his machines "Enigma" [DEL]. Models A and B – model A was surprisingly similar to Hengel and Spengler's machine – had four rotors[3] and were launched commercially, but without success due to their high price. Model C was a cheaper, portable model, with only three rotors and with an array of bulbs replacing the printing system. The third wheel was connected to a drum provided with contacts connected one to another on the same side and known as the reflector (*umkerhwalze*). An electrical impulse that arrived on the drum was then reflected towards the rotor from where that impulse came.

2. Adoption by the German army

In 1923, the book *The World Crisis* by Winston Churchill (1874-1965) provided evidence that the German code book, the *Signalbuch Kaiserlichen der Marine*, had been compromised in 1914. Consequently the *Reichsmarine* sought a safer ciphering method and adopted Enigma in 1926. The *Reichswehr* followed in 1928. In March 1935, violating the Treaty of Versailles, Adolf Hitler (1889-1945) announced the restoration of compulsory military service and decided to increase the size of the German army from 100 000 to 500 000 men. The *Reichswehr* became the *Wehrmacht,* the *Reichsmarine* became the *Kriegsmarine*, the *Luftwaffe*'s air power was restored and they in turn adopted Enigma. The rearmament of Germany had begun.

The portable, easy- to-use Enigma machine could be used at the battlefront and was at the heart of the *Blitzkrieg*. The army would manufacture tens of thousands of the machines in five factories spread throughout the territory to diversify sources. When World War II started, all German radio communications were enciphered on various models of Enigma machines having varying levels of sophistication. Thousands of enciphered messages were sent every day, from orders signed by Hitler and troop movements to weather reports and inventories for supplies of troops and boats. By the end of the war, between 50 000 and 120 000 Enigma machines had been manufactured, according to various estimates [KAH2, pp. 45-54].

3. Description and operation of the Enigma machine

An Enigma machine has a keyboard of 26 keys that can write 26 letters, with no digits or punctuation symbols. The space between words is represented by X, and the separation of sentences by Y. Above the keyboard is a bulb board that shows the enciphered letter for each key typed. Above the bulb board, are the three wheels, each one having a movable ring (*Ringstellung*) which clicks into a wedge in one of twenty six positions. On the front of the machine is a plug board.

The action of a key closes an electrical circuit in which the current flows through the plugboard, the three wheels and the reflector, which then returns the current to the three wheels in reverse order, and then back through the plugboard to finally light a bulb. At the same time, pressing the key rotates the right wheel a twenty-sixth of a turn. Once the wheel has completed a full rotation, a pin rotates the middle wheel a twenty-sixth of a turn and similarly for the left wheel when the middle wheel has itself completed a full rotation. So, the Enigma machine carries out a polyalphabetic

[3] Bletchley Park Cryptanalysts called them 'wheels'. Today, these wheels are called rotors.

substitution whose period is 26 x 26 x 25 = 16 900 (not 26 x 26 x 26 due to a double stepping mechanism that sometimes moves the middle and left wheels simultaneously).

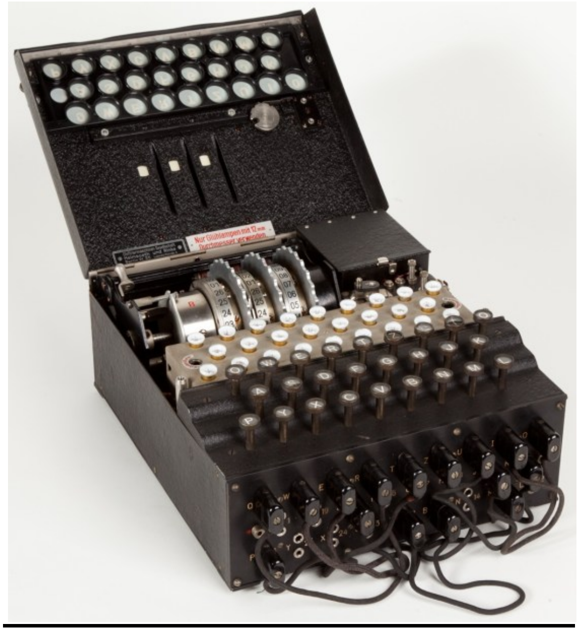


Fig.1. The Enigma machine.Wikimedia Commons. Public domain.
Museo scienza e technologi. Milano.

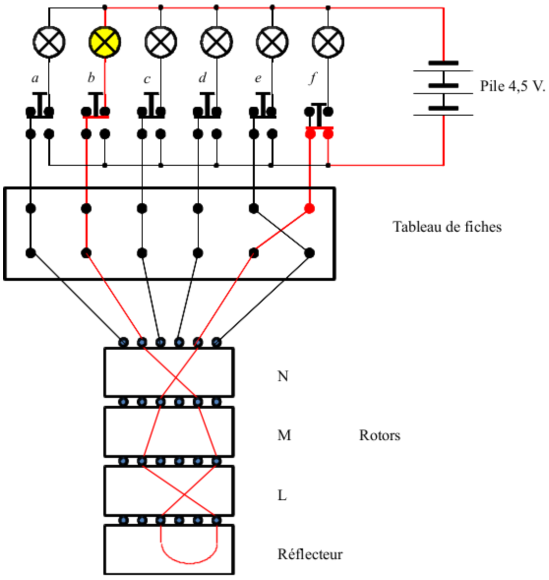


Fig. 2. Diagram of the course of the ciphering of a letter on Enigma, by the authors.

The activation of a key opens the circuit that supplies its own bulb. Thus, a letter cannot be encrypted by itself. This is called the *exclusivity principle.* When a key is pressed, say the *f* key it lights a bulb, say *b*. The activation of the *b* key has the effect of making the current flow in the opposite direction to light the *f* bulb. This is the *reciprocity principle*. Encryption exchanges letters in pairs. So, retrieving the plain text from the enciphered message is performed with exactly the same operation. This process allows the same machine to have the same positioning for enciphering and deciphering. This is a great operational convenience, but is also a serious weakness that the cryptanalysts would not fail to exploit.

Each day, the operator had to set up the machine according to details given in a printed key table. Here is a sample for May 4, 1937:

Datum [Date]	*Walzenlage* [Rotor order]	*Ringstellung* [Ring settings]	*Grunfstellung* [Initial rotor settings]	*Steckerverbindungen* [Plugboard settings]
4 May	III-I-II	16-11-13	01-12-22	*CO DI FR HU JW LS TX*

On this particular day, the operator had to place the wheels in the cage in the following order: wheel III on the left, wheel I in the middle and wheel II on the right. The rings on the three wheels would have been set in the position shown: 16 for the left wheel, 11 for the middle one and 13 for the right wheel. The wheels would then have been rotated to reveal the number indicated by the fourth column: 1 for the left wheel, 12 for the middle one and 22 for the right wheel. The letters indicate the plugs to be connected together on the plug board: the *O* with *C*, the *D* with *I*, the *F* with *R*, and so on.

Then, before enciphering a message, a specific protocol had to be obeyed so as to avoid all the messages on a given day being enciphered with the same sequence of substitutions. The operator chose three letters, for example *X F R* that were enciphered twice with the daily key. The six letters so obtained are placed as the message header, and constitute the message key, for instance *h u i l k b*. The operator then positions the wheels according to the three letters *XFR* he has chosen, and then ciphers the sequel of the message.

In deciphering, the operator processes in the inverse way. He deciphers the header *h u i l k b*. If everything ran correctly, twice XFR XFR would be found. Then, the operator would position the wheels according to these three letters, and decipher the rest of the message.

THE POLISH CIPHER BUREAU

1. Setting up of the cryptology team

The Treaty of Versailles restored Poland to its "Prussian Partition". Germany did not hide its ambition to recover these territories at the first opportunity, prompting the Poles to distrust their ambitious neighbor. A radiocommunications interception center was located in the city of Poznań near the German border. The intelligence services were organized around an "Intelligence Transmissions Bureau" directed by Guido Langer (1894-1948) and a "Cipher Bureau" led by Franciszek Pokorny, a cousin of the cryptologist Hermann Pokorny (1882-1960), who ran the Austro-Hungarian General Staff's Russian-Cipher Bureau during World War I. In the Cipher Bureau, a German section called *BS4* was headed by Maksymilian Ciężki (1899-1951). This section managed, more or less, to solve the rudimentary ciphering code of intercepted German messages.

But from 1926, the adoption of Enigma changed the ciphering methods and defeated the BS4. The traffic continued to be analyzed systematically, but without success.

One Friday early in the year 1929, an incident occurred at the Warsaw Customs Office where a package from Germany was due to be transported to a German company in Warsaw. An employee from this company insisted that the package, which he said contained radio equipment, should be returned to the sender as soon as possible. The Customs Office replied that this would be done on the following Monday, as the office was closed for the weekend. But the insistence of the employee awoke the customs officer's curiosity. Their suspicions were heightened when the German consulate itself intervened to make the same request. Customs then appealed to BS4 to clarify the matter. Ciężki was called in as an expert and requested the help of two old friends that he had known during the Greater Poland Uprising (19189-1919). two engineers from the Radio AVA factory, who were also shortwave radio enthusiasts: Ludomir Danilewicz (-1971) and Antoni Palluth (1900-1944). This event would seal the beginning of cooperation that would last until 1942. The two engineers examined the package and discovered that, rather than the stated radio equipment, it contained a ciphering machine, the Enigma machine that was sold on the civilian market. Thinking it would be the solution to their problem, Ciężki procured a similar machine. But they were still unable to decipher the messages.

The cryptography office then became aware of the inadequacy of its resources. The method of ciphering had changed in nature. There were no longer substitutions or transpositions, but a more sophisticated process that required new skills. Ciężki first called for the help of Stefan Ossowiecki, an engineer and psychic who, at the time, managed to guess the content of a message in a sealed envelope, but who failed of course to give a sense to the German cryptograms. After this stinging failure, Ciężki had the bright idea would overcome the problem.

In 1929, a cryptography course was organized at the University of Poznań, open to students in mathematics. These courses were taught by Franciszek Pokorny, based on the 1925 cryptography handbook by Colonel Marcel Givierge (1871-1931)[4], and by Maksymilian Ciężki who taught the resolution of classic German cryptograms, and finally by Antoni Palluth, from Radio AVA. At the end of this course, three of the best students were recruited from the class of twenty ones: Marian Rejewski (1905-1980), Jerzy Różycki (1909-1942) and Henryk Zygalski (1906-1978). The cryptography office had its three new recruits. The following year, the cryptography course was no longer offered [KAH2, pp. 60-63].

2. French intelligence's contribution

Meanwhile the French intelligence services had confirmed to the Polish that the German army actually used the Enigma machine.

French cryptologists had been very successful during the First World War in particular with the resolution of the so-called "Radiogram of Victory" which helped to

[4] Colonel Marcel Givierge was the head of the French Cipher Bureau from 1914 to 1917. His handbook *Cours de Cryptographie* was widely distributed, including in the United States, where it was read in particular by Claude Shannon (1916-2001).

inform the French General Staff of a major German offensive around Compiègne in June 1918, and allowed them to take measures to make it fail. But after the war, the French Cipher Bureau declined and in 1923 it had no more than eight employees. It became accepted that the cryptograms produced by the new machines could no longer be solved mathematically, but only by espionage. Marcel Givierge himself admitted: "Such machines provide cryptograms that can be considered theoretically as indecipherable" [GIV, p. 228].

The French Ministry of War therefore created a D section in 1930, which was tasked with obtaining, by any means possible, information on the ciphering methods used by foreign countries. At its head stood the Captain Gustave Bertrand (1896-1976). At the beginning of July 1931, he received a letter from Rodolphe Lemoine (1871-1946), a recruiting agent in Berlin whose real name was Rudolf Stahlmann, alias Rex, a double agent. This letter, signed by a certain Hans-Thilo Schmidt (1888-1943), offered him the chance to "negotiate documents of the highest importance". The signatory was a civilian employee at the *Chiffrierstelle* or Chistelle – the German cryptographic service –, and brother of Rudolf Schmidt (1886-1957), a Lieutenant Colonel in the German army who had obtained this position for him after a failure in business [KAH2, pp. 66-69].

A meeting took place on November 8, 1931 in Vervier, Belgium where Hans-Thilo Schmidt showed the Frenchman several documents including the manual for the Enigma machine and its operator user manual. These documents were estimated to be of great value by Bertrand, who photographed them in exchange for the sum of 10,000 marks, or about 22,000 dollars at today's value. Bertrand forwarded the documents to his colleagues in the cipher service but received a very cool response: "This is a machine against which we can do nothing, even with your documents" [KAH2**,** pp. 70]. On November 23, the documents were forwarded to the Parisian representative of the British Secret Intelligence Service (SIS), who sent them to London[5]. The same answer came from the Government Code and Cipher School, GC& CS: "These documents do not have sufficient value for the GC&CS to help share the costs" [KAH2**,** pp. 70].

Bertrand then turned to his Polish contacts, Langer and Ciężki, and there, the welcome was more enthusiastic. The Poles recognized in these documents a solution to fulfill their mission. This marked the beginning of a long period of cooperation between Bertrand, Schmidt, Langer and Ciężki. Schmidt would now be known by the code name Asche (HE). He would provide the daily keys for the different departments that used Enigma. The cooperation would last until September 1938, the date on which Asche was transferred to the *Forschungsamt* (FA), the Research Department where he would no longer have access to Enigma documents [KAH2**,** pp. 71-72].

Although the British had also received the documents, it seems that they did not exploit them until 1938. In the early 1930s, a large part of the British Establishment did not perceive Germany as a threat, but rather as a bulwark against the Bolsheviks.

The recruiting agent Lemoine was later questioned by the *Abwehr (*the *Wehrmacht*'s military intelligence service) in February 1943. To save his skin, he

[5] Wilfred B. Dunderdale, the SIS station chief in Paris, likely photographed the documents, allowing Knox to analyse them only later. But the refusal to pay cut the British off from all future Asche documents [BAT, p. 65].

confessed that Schmidt betrayed the Germans. Schmidt was later found dead in a street in September 1943. Despite a brilliant service record, his brother Rudolf, who had become a General, was removed from his functions and dismissed from the Army [KAH2, pp. 135].

MATHEMATICS AND MACHINES IN POLISH CRYPTANALYSIS

Following the recruitment of Rejewski, Zygalski and Różycki by the *Biuro Szyfrów,* the Polish group succeeded in breaking the German Enigma codes throughout the pre-war period. This work was supported through close collaboration between mathematics, engineering and military intelligence. Their hard work had to overcome numerous difficulties, particularly the changes in the mode of operation periodically carried out by the Germans.

1. The permutation theory for recovering *Wehrmart* Enigma wiring

The Polish mathematicians' first task was to recover the internal wiring of the machine used by the German army. Indeed, it differed from the wiring of the commercial machine. In order to accomplish this task, they used the permutation theory, with the help of the first documents provided by Asche.

As mentioned above, the operator chose three letters a, b and c. These three letters were repeated and underwent the first six substitutions of the Enigma machine. Let us denote these six substitutions by A, B, C, D, E and F respectively. The message key consisted of the six resulting letters $x = A\ (a)$, $y = B(b)$, $z = C(c)$, $t = D(a)$, $u = E(b)$ and $v = F(c)$. But the ciphering was reciprocal, which meant that the substitution A maps a onto x, but also x onto a. Therefore, the product of composition of A and D maps x onto t. Here**,** x and t are known by the interceptor, as these letters are part of the message key, transmitted in clear in the preamble of the cryptogram. Similarly, the composition of B and E maps b onto u, and the composition of C and F maps c onto v. By accumulating a sufficient number of messages, the cryptanalyst could discover the composition of AD, BE and CF. The solution to "the coupon collector's problem" tells us that an average of 74 messages have to be collected to retrieve the complete collection of the 26 values of substitutions AD, BE and CF. [WEL2, p. 208-211]

Knowing the composition of the products resulted in knowing the permutations A, B, C, D, E and F themselves. One of the three mathematicians, Marian Rejewski, would use a theorem that he established for the occasion on the length of transposition cycles:

> "If two permutations of the same degree consist only of disjoint transpositions, then their product contains an even number of disjoint cycles of the same length…… The reverse theorem is particularly important. if in any permutation of even degree there appears an even number of cycles of the same length, then the permutation can be regarded as a product of two permutations, each of which consists only of disjoint transpositions" [REJ1, p. 8-9].

But this factorization is not unique. Therefore, the choice of an element and its image in two cycles of the same length imposes other transpositions. The number of options are quite limited and equal the product of the lengths of the product cycles [CAR1, pp. 5-7].

Here our mathematicians made an assumption, based on the laziness of German radio operators working under severe pressure: for convenience, the operators often chose identical letters for the message key, for example *j j j*, or consecutive letters such as *a b c*, or keys that were close on the keyboard such as *q w e*. This hypothesis was tested frequently enough to allow the reconstruction of the first six substitutions *A*, *B*, *C*, *D*, *E* and *F*. Mathematical insight would not be the cryptanalyst's only quality. Rejewski wrote "... that the cryptanalyst generally does not know the preferences [of the operators], but he tries to compensate his ignorance with long tests, imagination, and sometimes with an ounce of luck" [REJ1, p. 9]

Now our team was able to reconstruct the internal wiring of the right wheel. They had to assume that it was the only wheel to move during the enciphering of the message key. This hypothesis was very plausible, as the turnover of the following rotor depended on the position of the ring, and proved correct in 20 cases out of 26. There were still unknowns to express substitutions performed by the right wheel. This had been solved thanks to the daily keys provided by Asche via the French. The internal wiring of the other wheels could be determined when other keys were placed in the correct position. Once the positions of the three wheels were known, rebuilding the wiring of the reflector was a mere formality.

In January 1933, the plans of the machine were provided to the Radio AVA factory and a "made in Poland" replica of the *Wehrmacht* Enigma machine was now available for the Cipher Bureau. Thanks again to the daily keys provided by the French, intercepted messages were now regularly deciphered. But the results were still insufficient. The Poles needed to be able to carry out this deciphering without French assistance and to find a way to reconstruct the daily key without external help.

2. First manual method

Initially and for a period of three years, from 1933 to 1936, the Polish team used manual methods applied from classic cryptanalysis. Let us quote one of them. "The count of the letters which coincide when two cryptograms are superimposed, can decide whether or not they are from the same sequence of substitutions" [KAH1, p. 378]. Indeed, if two German texts were superimposed one over another, one identical letter among 13 letters[6] was observed on average. The same frequency occurred when the two texts had undergone the same substitutions, whereas if the texts were random sequences of letters, or had undergone various substitutions, only one coincidence among 26 was observed on average. Counting the coincidences on different cryptograms could determine when the middle wheel had rotated. Let us suppose that the position of the ring on the right wheel rotates the middle wheel during the passage from *j* to *k*. The following positions of the wheel will be *c l i*, *c l j*, *c m k*, *c m l*, and so on. This hypothesis can be validated by superimposing a message for which the initial position of the wheels is *c m k* and counting the coincidences. This method, discovered by Zygalski, is called the "Clock Method" after the big clock in the room where it was discovered.

[6] The Index of Coincidence of the German language is 0.0762 which corresponds to one coincidence every 13 1234 letters [KAH1, p.378].

However, manual methods were slow, and gave partial and uncertain results, which did not always lead to the real key.

3. The cyclometer

A breakthrough was achieved in 1936. The mathematicians noticed that the cycle structure of the *AD*, *BE* and *CF* substitutions could characterize the order and the initial position of the wheels. There are six ways to arrange three wheels, and 26 possible starting positions for each wheel, and so, there are 6 x 26 x 26 x 26 = 105 456 possible combinations. If a catalog could be drawn up that, from the number and size of the cycles of the *AD*, *BE* and *CF* permutations, could give the orders and starting positions of the wheels, it would suffice simply to refer to this catalog to derive a majority of the daily key. To establish this catalog of more than one hundred thousand entries would be a colossal piece of work. A machine would make it possible to determine the cycles of *AD*, *BE* and *CF* substitutions more quickly. Such a device was in fact invented, and called a cyclometer. It included two sets of wheels and a reflector, together with a switchboard for the twenty-six letters. Its circuit diagram was remarkably simple. The action of one of the twenty-six switches closed the electrical circuit. The current then passed back-and-forth between the two sets of wheels, moving alternately in one direction and then the other to light bulbs in a cycle in a series circuit. Simply counting the number of lamps lit gave information on the size of the cycle. Activating the switch of the bulb that had not yet turned on made it possible to then know the size of another cycle, and so on to discover the whole cycle structure. A few seconds were enough for each combination. Once the catalog had been established, the daily key was found in a few minutes.

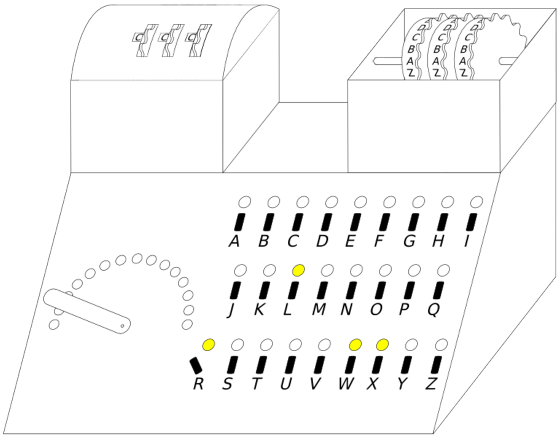


Fig. 3. Diagram of the Marian Rejewski cyclometer, by Math Crypto. Wikimedia Commons. Public domain.

In November 1937, the internal wiring of the reflector was changed. As a result a new catalog had to be established, which was finished with much hard work before the end of the same year. In early 1938, the Poles were able to decrypt the daily *Wehrmacht* and *Luftwaffe* messages.

4. Zygalski's perforated sheets

But on September 15, 1938, the messages became incomprehensible once again. After the annexation of Austria on March 13, 1938, Hitler continued his expansionist policy and called for the annexation of the Sudetenland, the German-speaking region of Czechoslovakia. With the mounting tension, the Enigma procedures changed. The Germans wanted to avoid enciphering all the messages with the unique position of the wheels of the daily key. The operator now selected the position of the wheels that he transmitted in clear for enciphering the message key. He then twice enciphered the three letters he had chosen as an initial position of the wheels for the rest of the message. A message header could be, for example:

gkd wav wha.

The first three letters indicate the positions of the wheels for enciphering the message key and the following six are the results of twice enciphering the positions of the wheels for the rest of the cryptogram [WEL1, p. 36]. The actual position of the wheels remained unknown to the cryptanalysts because it also depended on the secret placement of the rings, but the information transmitted in clear provides information on the relative positions of the wheels to each other. The permutations *AD*, *BE* and *CF* are no longer accessible in their entirety, and the catalog of cycles becomes useless.

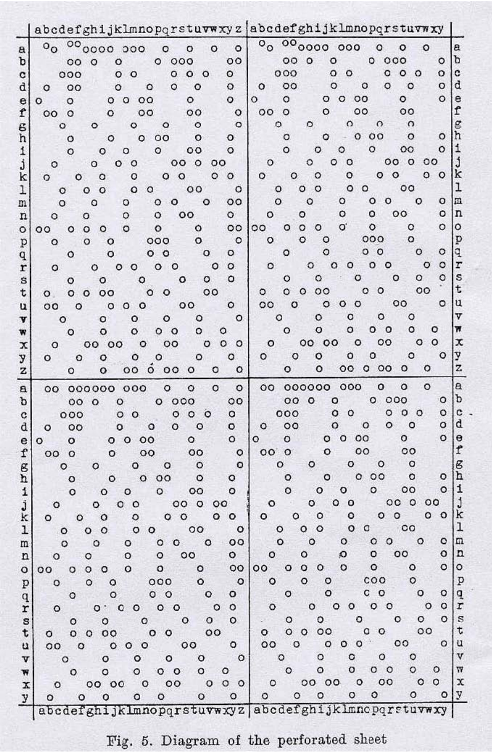

abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxy
Fig. 5. Diagram of the perforated sheet

Fig. 4. A Zygalski sheet. from Płachta Zygalskiego - decrypting Enigma.jpg
Wikimedia Commons. Public domain.

The Poles did not give up and pursued the approach that had previously led to their success. In the above example, we observe that the image of *w* substituted by *AD* is the letter *w* itself. This is a fixed point; in fact a cycle of length one[7]. The mathematicians were satisfied. A probabilistic calculation showed that about one message key in nine had a fixed point in one of three possible positions. On the other hand, the cycle catalog showed that a fixed point can eliminate 40% of the keys. By intercepting about 180 messages, it could be hoped to get enough information to restore the order and the starting position of the wheels. It was necessary to establish something like a catalog of fixed points. This was produced in the form of perforated sheets based on an idea from Zygalski [KAH2, pp. 84-85].

A set of sheets was required for each order of the wheels and for each starting position of the right wheel, that is 6 x 26 = 156 sets. On each sheet, the abscissa represented the position of the middle wheel and the ordinate that of the left wheel. A hole was drilled at this point if there was a fixed point of the *AD* permutation for this position. For the fixed points of the *BE* permutation, it was simply necessary to shift the position of the right wheel by a row. To use these sheets, messages whose preamble had a fixed point – that is the same letter in the first and fourth position, or to the second and fifth position, or the third and sixth position – were superimposed. The perforated sheets were filed on a light table by shifting the plates according to the data given by the letter of the first trigram of the message key. A common perforation for all sheets showed the configuration of the wheels corresponding to all observed fixed points. This configuration of the wheels revealed the daily key. With this method, it could be found in a few hours [CAR1, pp. 17-22].

5. The Polish *Bombas*

At the same time as the perforated sheets technique, Różycki came up with an electromechanical machine: the *Bomba*. This term means 'beautiful', 'superb' in Polish. It was also the name of a vanilla ice cream topped with chocolate that was fashionable in Warsaw at the time. The ticking of the machine while it was in operation is sometimes evoked as the reason for this name, but it could also be because this machine would destroy the German cryptograms [KAH2, pp. 85-86].

For the *Bomba* to work, three messages with the same letter as a fixed point were needed. Whether the fixed point was in the first, second or third position was irrelevant, but it had to be the same letter as a fixed point in the three messages. Suppose, for example, three messages had been intercepted whose headers were:

*cku a**m**t s**m**u, rtz **m**rk **m**pw, uyl **m**ib **m**sr.*

The letter *m* is a fixed point in the second position in the first message and the first position in the other two. The number of messages needed to be intercepted to expect this situation is not so high. It is given by the so-called “birthday paradox”. By intercepting 144 messages, there was a one in two chance of having three suitable messages. On the other hand, very few wheel configurations can lead to this situation, making it a very discriminating criterion. A *Bomba* included six sets of wheels in three pairs which each detect a fixed point at the observed position [CAR1, pp. 14-17]. A motor rotates the wheels at a rate of 2.7 trials per second, so that in 105 minutes, less than two hours, all combinations are explored. The parts required to build these Bombas

[7] It was latter called a “female letter” by the British.

were ordered from Radio AVA in October 1938. They were delivered on November 10. The assembly was carried out in the utmost secrecy at the premises of BS4, and from that moment, the daily keys were routinely recovered in less than two hours!

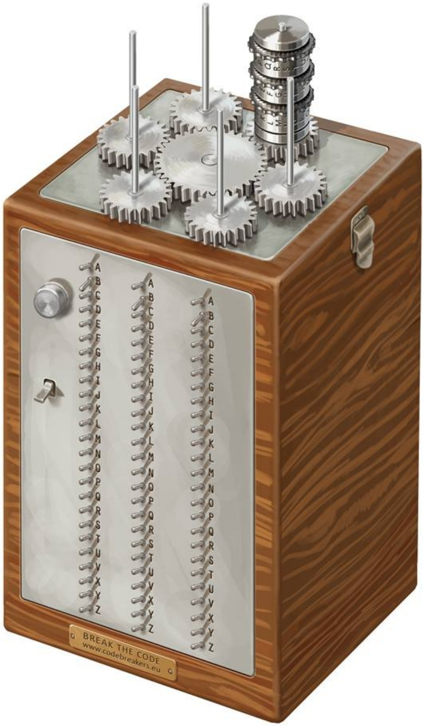


Fig. 5. Image of a Polish Bomba.
With the kind permission of the Crypto Museum, The Netherlands.
https://www.cryptomuseum.com/crypto/bombe/

6. Contacts with the French and British services

Nearly two months later, on December 15, 1938, incomprehensible messages were again intercepted. Polish intelligence had informed the mathematicians about the commissioning of two new wheels. So, the number of combinations of wheels jumped from 6 to 60, ten times more. Contrarily to what was performed in 1932, the new procedures could no longer recover the internal wiring! Fortunately, the *Sicherheitsdienst*, the Nazi party intelligence service, did not change its procedures and the interception of its messages enabled the Poles to recover the internal wiring of the two new wheels [WEL2, p. 216].

The perforated sheets had to be given up. It would now have needed 1560 sets instead of the 156 existing sets! The work of making them was beyond the reach and means of the team. *Bombas* could still operate, but it would have been necessary to build 60 of them, and the finances of the cipher bureau could not run to such an expense. They could still be used one after the other, but the search for a key could take up to 17 hours.

Meanwhile, driven to desperation by the lack of results, Bertrand suggested to Langer the crazy idea of using several clear messages communicated by Asche to persuade the Germans that the Enigma code had been broken and lead them to abandon its use. This idea was of course unbearable for Langer who would have seen the collapse of nearly ten years of work. He managed to persuade Bertrand to consult the British before taking such a drastic step. A meeting at the initiative of the Poles, involving French, British and Polish officials, was held on January 9 and 10, 1939 in Paris, at the premises of the French intelligence service at *Les Invalides*. But the Poles had orders not to reveal anything about their expertise. After this meeting, Dillwyn Knox, the head British cryptologist at the GC&CS, was very disappointed [KAH2, pp. 90-91].

But then the international situation deteriorated more seriously. The Nazis invaded Czechoslovakia on March 14, and in response, the French and British guaranteed Poland their support in case of a German attack. Hitler declared the non-aggression agreement signed in 1934 null and void, and his speeches became increasingly anti-Polish. The decryption of German messages showed the Poles that Wehrmacht divisions were gathering along the borders. So, they organized a second meeting with the French and the British on July, 25 and 26, 1939 at Pyry[8], a suburb of Warsaw where the Polish Cipher Bureau was situated. The French delegation was led by Bertrand. He was accompanied by a cryptologist, Captain Henri Braquenié. The British delegation included Alistair Denniston (1881-1961), head of the GC&CS, Knox and Commander Humphrey Sandwith (1881-?), founder and Chief Executive Officer (CEO) of the Royal Navy Interception stations [BAT, p. 74].

In front of a thunderstruck audience, the Poles finally revealed everything: how they had reconstructed and built a replica of the military Enigma machine, how *Bombas* and perforated sheets were used to reconstruct the daily keys. It was the first feedback Bertrand had received on the use of the many documents he had tirelessly continued to transmit. The British were especially appreciative, as they had recently put a team in place to try to crack Enigma**.**

This Pyry meeting was the "priceless gift" from the Poles to their Allies [KAH2, p. 94]. They offered two replica Enigma machines that traveled to Paris by diplomatic bag. One of them passed across the Channel on August 16, 1939 by the Golden Arrow train from Paris to London. So as not to arouse the suspicions of the German intelligence services, the machine traveled in the suitcases of the playwright Sacha Guitry (1885-1957) and his wife, the singer and actress Yvonne Printemps (1894-1977) [KAH2, p. 94].

Events now rushed on apace. German armored divisions entered Poland on September 1st, with a particular accident of history: the first Armored Division was commanded by General Rudolf Schmidt, brother of Hans-Thilo Schmidt who had provided the French with the Enigma documents. On September 3, France and Great Britain declared war on Germany. The Polish defenses cracked under German superiority. The *Biuro Szyfrów* was evacuated, and all traces of its work destroyed. The Polish team was sent to the safety of a refugee camp in Romania.

The three mathematicians preferred to take a train to Bucharest where they first made contact with the British Embassy. They received a polite refusal, the British

[8] Most of the sources give these dates. Mavis Battey asserts 26 and 27, from Denniston's report written in 1948. According to her, other sources such as Bertrand or Rejewski claimed the dates of 24 and 25, but only by their own memories thirty years later [BAT, p. 74].

having too much to do with their own nationals. So they turned to the French Embassy asking for Bertrand. This name opened doors. The French gave them papers, visas, money and train tickets. They reached Paris on September 25, 1939 after a journey that took them through Belgrade, Zagreb, Trieste and Turin. A little later, the British offered them refuge in London but the French refused, and they declined the British proposal to set up a common cryptologic center in France. Bertrand himself traveled to the refugee camp in Romania to find Langer and Ciężki and brought them back to Paris on October1^{rst} 1939 [KAH2, p. 105-106].

The Polish team was brought together in an undisclosed center known as PC Bruno, located in the Château de Vignolles in Gretz-Armainvilliers in the Paris area. This team became known as Ekipa Z. The center had three replica Enigma machines and began the work of decipherment fueled by messages collected by French interception stations. The former Radio AVA engineer Antoni Palluth, a member of Ekipa Z, dismantled one of the replicas in order to draw up the plans and ordered one from a French company. This machine would only be ready in July 1940.

INTER-WAR BRITISH CRYPTOLOGY

In Great Britain, the British Intelligence and Security organization was the GC&CS, which would become the *Government Communication Headquarters* (GCHQ) in 1946. The GC&CS brought together two signal intelligence agencies in 1919: *Room 40,* founded by the Admiralty in 1914, and its Army counterpart, M.I.1b. Commander Alexander G. – Alistair – Denniston (1881-1961) was its operational head until 1942.

During the inter-war period, the GC&CS was transferred from the Admiralty to the Foreign Office, and headed by the Secret Services. Its public function was to ensure the security of government communications, and its secret one to read messages sent and received by foreign government. Its activity was at such a low level that it was sometimes nicknamed the "Golf Club and Chess Society". In 1935, it was a relatively small department, with 90 employees, 30 of whom were cryptologists, essentially concerned with diplomatic traffic, and using classic crytographic methods [KAH2, pp. 95-96].

Since World War I, the cryptographic methods used in the GC&CS had been more concerned with linguistics than with mathematics. For example, Knox was a Cambridge scholar recruited in 1914. He was involved in breaking the Zimmermann telegram in 1917, which brought the USA into WW1. He was above all a specialist in ancient Greek, and edited papyrus Herodas texts in 1922. He was "neither an organization man, nor a technical man", but "essentially an idea-struck man" [WEL1, p. 34]. In 1927, the CG&CS acquired a commercial Enigma machine, which was evaluated by a Japanese speaking graduate from Cambridge, Hugh Foss (1902-1971, GC&CS 1924). In a Report entitled "The Reciprocal Enigma"[9], Foss established that, in spite of the sales leaflet, an Enigma machine without a plugboard could be broken if a crib – that is a probable piece of plaintext – could be guessed by other means: "If the wiring of the wheels was known, just fifteen letters were all that was needed to find the machine setting – that is the correct initial starting positions of the three wheels – but, if

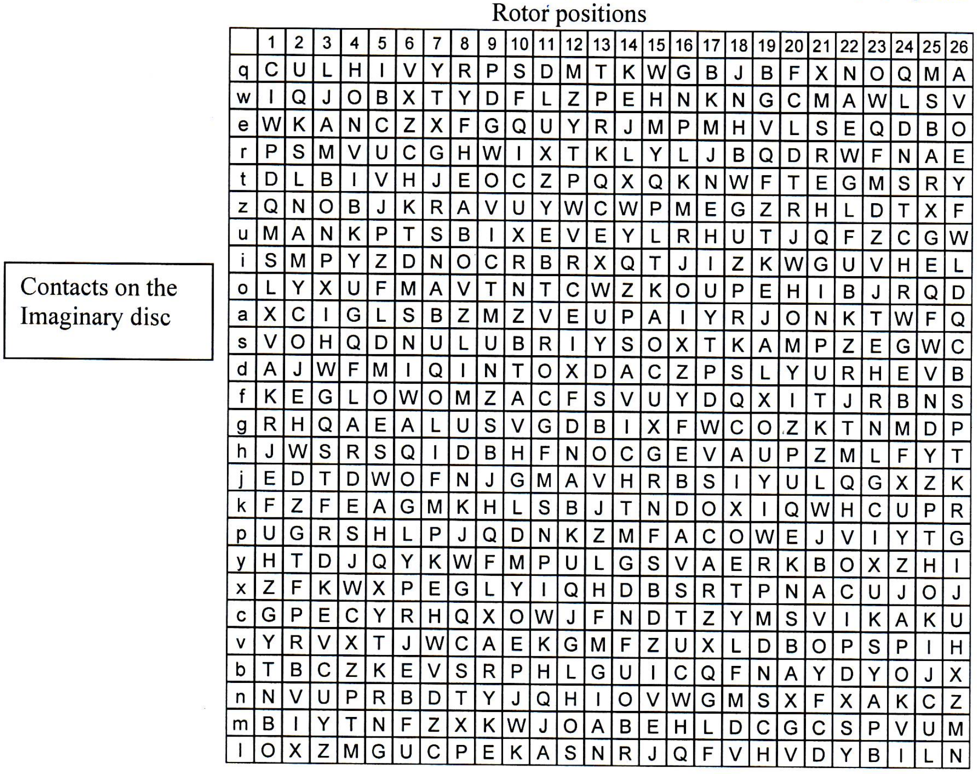
[9] Foss named the machine set up with a reflector (*Urnkehrwalze*) **the** "Reciprocal Enigma"**.**

the wiring of the wheels was unknown, at least 180 letters would be needed" [BAT, p. 58].

By 1936, The Germans had produced the K Model Enigma machine with modified wiring. The K Model was supplied to a variety of customers in Germany and abroad, especially in Italy and in Spain. After his discussions with Foss, Knox invented the so-called 'rodding method' to find the wheel order and positions. By 1937 he could read corresponding messages [BAT, p. 60-61]. This method also required cribs. However, it provided only a fragmentary sequence of characters in plaintext. So, considerable linguistic skill was needed to achieve the discovery of the remaining parts of the plaintext, just like for a German crossword. Fond of the logic of Lewis Caroll's literary nonsense[10], Knox excelled in playing with words, and he always worked as a linguist, looking for messages through their meaning [BAT, p. 31-401]. Let us briefly look at the rodding process in the following example [CAR 2].

1. The rodding method

The name comes from the paper rods on which Knox inscribed letters. The method supposes that the wiring of the wheels is known.


Rotor positions
Contacts on the Imaginary disc

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Rod square for Rotor I

Fig. 6.The Rodding Square. From CAR2, p. 2.

The first step is to analyze the effect of the right wheel on the 26 first letters of the cryptogram. It also considers as a whole the effect of the two other wheels and of the

[10] The former historian Frank Birch – later head of the Naval section – wrote a comic skit on Room 40, *Alice in ID 25*, with poems by Knox. It was performed by the codebreakers at the end of the First World War [BAT p. 31].

reflector. The 26 x 26 rod-square table gives all the possible correspondences between the input and output letters across this rotor, for each initial position.

The right wheel had one notch turn for each input letter. On this example, the table indicates that in position 10, this wheel connects the letter ‘C’ to the letter ‘t’, and in position 15, the letter ‘Z’ to the letter ‘v’. In all the diagonals from top right to bottom left, the letters follow the order of the letters connected to QWERTZU …, the German keyboard for the K-model of the Enigma machine. A set of 26 rods is made up from the 26 rows of this table. In fact, three sets are needed, one for each wheel, with different colors to distinguish them.

Suppose that the letter *V* from an enciphered message is known to represent the plaintext letter *T,* and that this occurs when the right hand wheel is in its 6th position. Then, from the reciprocal principle, the two terminals *q* and *u* must be electrically connected together through the remaining components of the Enigma machine. And their corresponding rods can be associated.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
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

The letters *q* and *u* are known as the ‘rod coupling’ letters. Associating these two rods gives other corresponding letters between the crib and the enciphered message. For instance, with this enciphered message:
MLXVK SCLDU HOHSV FKXKU SDVRP NGCYA T and the starting crib : ‘**CODEX**’
and let us suppose first that the correct right wheel starting position has been determined by testing the 3 x 26 = 78 possible configurations. This is done by checking inconsistencies between their corresponding pairs of rods with the exclusivity principle. Here, for each of the first five letters, the rods which can be associated by pairs are:

- those for *M* and *C* in position 1
- those for *L* and *O* in position 2,
- those for *X* and *D* in position 3,
- those for *V* and *E* in position 4,
- those for *K* and *X* in position 5.

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
			M	**L**	**X**	**V**	**K**	**S**	**C**	**L**	**D**	**U**	**H**	**O**	**H**	**S**	**V**	**F**	**K**	**X**	**K**	**U**	**S**	**D**	**V**	**R**	**P**	**N**	**G**	**C**	**Y**	**A**	**T**
			C	**O**	**D**	**E**	**X**																										
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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					
		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	**O**	**D**	**E**	**X**			**E**			**I**		**G**	**X**				**B**				**C**		**Z**	**A**						

Afterwards, for the following letters of the enciphered message, when a letter corresponds to one of any rod, the corresponding coupled letter gives another possible letter for the crib. So, the crib can be partially completed at the bottom of the page. The resulting fragmentary plaintext can be completed step by step by guessing the missing letters as in a crossword game: here CODEXBREAKING.

In this process, it is supposed that there is no turn-over of the middle rotor for this part of the message. When such a turn-over occurred, the same procedure could be pursued with some more complications.

Knox also invented the so called 'buttoning-up' method, in order to find the wiring of wheels [CAR3]. It permitted the discovery of the first column of the rod square table, and started from two adjacent letters of the enciphered message corresponding to two adjacent letters of the plaintext, which Knox named a 'beetle'[11]. Going down from the beetle along the QWERTZU diagonals... made it possible to discover a pair of 'buttoned-up' letters on the upright column. The procedure made it necessary to discover numerous beetles, and to test a sequence of possible initial assumptions by comparing the various pairs of buttoned-up letters, and to eliminate the assumptions that lead to inconsistent derivations**.** Diagrams helped to analyze these conclusions. Once the first column of the rod square was discovered, the whole table could be obtained, as the order of the letters on each diagonal was that of the keyboard connection.

The rodding method and the buttoning-up method were of course very tedious and lengthy. They were carried out by hand, and only allowed the codes for messages to be broken one by one. Knox presented them as a 'kind of word game which even a beginner could do without knowing how the machine worked' [BAT, p. 113]. Nevertheless, they led to several successes. Knox quickly used them to crack the modified commercial Enigma machine used by volunteers of the *Luftwaffe* 'Condor Legion', which was supporting Franco’s troops during the Spanish Civil War in 1937.

[11] Knox excelled in giving special names to his procedures, for instance, from 'crab' and 'lobster' to similar specific ones used in breaking the code of the *Abwehr* Enigma. As it will be seen later in this paper, the habit would continue in the work of the specialized Huts.

He also helped the Admiralty to break the codes of the four submarines Mussolini sent to Franco [BAT, p. 62-63], but this knowledge was never shared with the Republicans.

After the military Enigma machines were equipped with a plugboard in 1930, Knox considered that his methods could still be used, even if they required many more messages and much more time to be efficient. But the connection between the keyboard and the right wheel had changed on this military model, and as Knox imagined that it was arranged in a random order, he failed to find what it could be.

So, when the British delegation arrived at the Pyry meeting, Knox had already designed manual methods for breaking Enigma codes on machines without a plugboard. But the British had not developed the same levels of coordinated mobilization between intelligence, mathematics and engineering that the Poles had during the 1930s. Nevertheless, Knox's practices were effective enough to be used immediately with the results communicated by the Poles in July 1939.

2. The legacy of Polish codebreaking

British codebreakers had been fully mobilized since Bertrand's invitation to join a council of war in early November 1938 in London, where he brought new documents from Asche. Denniston, Knox, John Tiltman (1894-1882) and Oliver Strachey (1874-1960) attended [BAT, p. 67]. Tiltman was a former army officer who had decoded Russian diplomatic traffic with Afghanistan and Turkestan, and now headed the new military section. Strachey, from the Foreign Office, was chief cryptographer at the GC&CS, and would go on to head the ISOS (Illicit Service Oliver Strachey) department at Bletchley Park, that was part of the Double Cross system – composed of double agents – which Churchill called the 'bodyguard of lies' [BAT, p. 153] – so important in the preparations for D-Day.

In the Paris meeting of January 1939 with the Poles, the British delegation was led by Denniston with three codebreakers: Knox, Foss and Tiltman. Knox, by then the expert in Enigma, was very disappointed as at first Ciężki gave a general presentation of the machine that he already knew inside-out. But Knox went on to present his rodding method, and was to strike up a lasting friendship with Braquenié, Bertrand's chief cryptographer [BAT, p. 70]. Rejewski was impressed by Knox's presentation and insisted he should be present at the Pyry meeting in July 1939. He wrote :

> "Just how much Braquenié understood, I don't know; but there is no question that Knox grasped everything very quickly, almost as quick as a lightning. It was evident that the British really had been working on Enigma. So they didn't require many explanations. They were specialists of a different kind." [WEL2, p. 217].

Knox learned from Rejewski that the connection from the keyboard and the right wheel was not at random as he thought, but was as simple as A to A, B to B and so on. So he turned out to be both disappointed and excited. Disappointed because he had dismissed this idea as being too simple at first– it had already been suggested by one of his young female assistants known as 'Dilly girls' [BAT, p. 76] –, and excited because his methods became usable again. The rodding and the buttoning-up methods allowed the Italian Navy Enigma codes to be broken. This ensured the victory of the Royal Navy at the Battle of Cape Matapan[12] in the Peloponnese on March 1941. And this was also crucial in breaking, in October 1941, the Enigma code used by the *Abwehr* [BAT, p. 118-131].

The Pyry meeting reinforced Knox's confidence in his own 1937 results. But above all, he noticed the recurring difficulties encountered by the Poles at each German decision to change the message-key procedure, because the Poles' methodology was based on the analysis of this indicator. He was quickly convinced that the approach was too hazardous. As a linguistic codebreaker, he considered that it was better to work on the content of the message.

3. The GC&CS recruited mathematicians and settled up at Bletchley Park

Even though the Poles did not reveal anything on the means by which they had broken the Enigma codes, the Paris meeting alerted the GC&CS of the existence of increasingly serious threats to peace. This conviction was reinforced by the *Anschluss,* the Nazis annexation of Austria on March 13, 1938. Consequently, the GC&CS decided to prepare lists of Cambridge and Oxford scholars who could be recruited. Two series of courses in cryptology were organized in London, in September and at Christmas 1938, bringing together about thirty people, essentially mathematicians, linguists, and German speakers. Among the mathematicians involved were Peter Twinn (1916- 2004), from Oxford University, and, from Cambridge, W. Gordon Welchman (1906-1985), a specialist in Algebraic Geometry from Cambridge, John Jeffreys (1916-1941), and Alan Turing (1912-1954), who in July 1938 had just returned from two years spent in the Department of Mathematics at Princeton University (New Jersey). There, Turing had completed his Ph. D thesis with Alonzo Church (1903-1995) as director, both of them working on different approaches of effective computability. Since his return, he was in contact with Denniston and worked regularly with Knox who introduced him to his own methods just after the Pyry meeting at the very beginning of August 1939 [BAT, p. 80]. Turing soon shared Knox's conviction that it would be more secure to work on the content of the enciphered message rather than on their indicators – the message keys –, whose coding methods were always threatened with changes. Their collaboration would be pursued even after the specialization of GC&CS's activities until Knox's death in 1942 [BAT, p. 81, p. 102].

The major new step in the code-breaking enterprise was the secret establishment of the GC&CS at Bletchley Park on August 15, 1939. The park surrounded a large Victorian Tudor-Gothic mansion with an ornamental lake. Station X, as it was known during the war, was ideally situated: 50 miles northwest of London, at the junction of major road, rail, telegraph and teleprinter connections to all parts of the country, especially Oxford and Cambridge. In order to provide more space, wooden huts were rapidly built in the park and later brick-built blocks were constructed for more specialized activities.Twinn had already joined the GC&CS in February 1939, and at the outbreak of the war, and Turing volunteered to join it at Bletchley Park, together with Jeffreys and Welchman.

[12] As secret documents had not been declassified when Winterbotham published his book on Enigma, *The ULTRA Secret* in 1974, he wrongly assigned this success to the *Luftewaffe* break in Hut 6. He was the head of the SIS air intelligence section, which superintended the setting up of Hut 3 in 1939. Because of a severe division of labour at Bletchley Park, he "only knew about the German air force ULTRA intelligence, and nothing about the Italians" [BAT, p. 128].

Thenceforth, mathematicians would play a major role in the organization of Station X. These first recruitments were only the beginning of continuous involvement of mathematicians, essentially from Cambridge. Stuart Milner-Barry (1906-1995) joined in January 1940, and recruited Hugh Alexander (1909-1974). They were famous with Turing and Welchman as the "four uncles", or the "wicked uncles"[13]. John William Jameson Herivel (1918-2011) was also recruited by Welchman in early 1940, as was Dennis Babbage (1909-1991) and Keith Batey (1919-2010), who married Mavis Lever (1921-2013), the former Germanist assistant to Knox, and who played a key role in breaking the code of the *Abwehr*[14] Enigma machine[15]. Jack Good (1916-2009), recruited in 1941, continued working with Turing after the war on the design of computers and Bayesian statistics at the University of Manchester. But linguists were also recruited, including Patrick Mahon (1921-72), who joined in 1941, and was a specialist in modern languages from Cambridge [COP1, p. 265]. He headed Hut 8 from 1944, and wrote its history [MAH] in 1946. William Tutte (1917-2002), was also recruited in 1941, and Max Newman in 1943. Both of them, with the engineer Thomas H. Flowers (1905-1998), ultimately contributed to the design of the Colossus electronic calculator. In the early years, the recruitment of scientists and mathematicians resulted essentially from personal acquaintanceships. From spring 1941, recruitment was entrusted to C. P. Snow, a Cambridge man, who often followed Welchman's suggestions [WEL2, p. 223].

This nascent organization at Bletchley Park inherited the work carried out by the Poles, and it is important to understand the similarities and the differences between the Polish and British approaches to breaking the Enigma code. The importance of their relationship was emphasized by Welchman in 1982 when he asserted: "The Poles had given us the full advantage of their brilliant work on Enigma. When I come to describe what happened at Bletchley Park, it will become apparent that these gifts were of immense importance in getting us started on the road that led to Hut 6 Ultra" [WEL1, p. 13].

4. Cooperation between Bletchley Park, the Poles and PC Bruno

The precious gift from the Poles, including the replica Enigma machine and detailed information on the wiring of wheels and their codebreaking methods, including Rosycki’s *Bomba* and Zygalski’s perforated sheets, reached Victoria Station on August 16, 1939, and was immediately forwarded to Bletchley Park. Knox and Turing set to work straight away on these materials.

Between the outbreak of the war and the invasion of France, Bletchley Park and PC Bruno worked in close cooperation. A GC&CS liaison officer was stationed permanently at PC Bruno, giving Captain Bertrand a direct teleprinter service with Denniston at Bletchley Park, and Braquenié came to work with Knox in September 1939 [BAT, p. 90]. Twelve thousand pounds were immediately allocated to build replica Enigma machines and, thanks to a special machine built for that purpose, the GC&CS

[13] They wrote a letter directly to Churchill on October 21, 1941, asking for more resources for codebreaking. Aware of the importance of ciphering from the First World War, the Prime Minister immediately answered positively. The GC&CS was then reorganized, and Denniston was replaced by his deputy, Commandant Edward Travis (1888-1956), later the head of the GCHQ.

[14] The German military Intelligence organization. Dee p. 8.

[15] She later wrote a lively book on Knox : *Dilly, the Man who broke Enigmas*.

began to manufacture the 1560 perforated sheet set required to find the daily key after the Germans introduced the two additional wheels in December 1938. These sheets would be completed in January 1940 under the supervision of Jeffreys. Turing made the trip to Paris and met the Polish team at the Château de Vignolles on January 17, 1940 to bring them these sheets. Turing transmitted information on the *Reichsmarine* Enigma machine captured by the English from a German U-boat, revealing the existence of a sixth and a seventh wheels on these machines. In his presence, and thanks to Jeffreys sheets, Rejewski decoded a message from October 28, 1939, from the German army's military districts [BAT, p. 99]. Back at the GC&CS, the crucial information Turing had learned at the Château de Vignolles enabled him to crack the *Luftewaffe* practice cipher on January 29, 1940 [BAT, p. 102[16]]. Knox was careful to maintain a fruitful relationship with PC Bruno: whoever was first to have worked out the keys for a given day would immediately pass the information to notify their Allied counterparts [BAT, p. 101]. The proportion of messages decrypted by each of the two teams –17% for PC Bruno and 83% for Bletchley Park – corresponded to their respective resources [KAH2, p. 134]. Welchman repeatedly emphasized that the Polish transmission and cooperation since the Pyry meeting had been essential in giving the initial codebreaking successes, and that this allowed Bletchley Park to convince the British authorities to develop scientific codebreaking, and in doing so, to overcome the May 1940 crisis [WEL1, p. 223].

On May 1, 1940, German messages could no longer be decrypted. The starting position of the wheels was no longer repeated in the message key, making the usual methods based on indicator analysis totally ineffective. On May 10, 1940, the German army launched a major offensive against Holland, Luxembourg, Belgium and France, and the messages remained unreadable during this offensive. A solution was found at Bletchley Park by Herivel, the 'Herivel tip', taking advantage of a blunder by German operators who did not always move the rotors from one day to another. From May 21, it again became possible to read some messages.

The debacle of the French army and the progress of the German offensive led to the signing of an armistice between France and Germany on June 22, 1940. PC Bruno was evacuated to Algiers via Oran on June 26, 1940. The French intelligence services were restored clandestinely by General Weygand (1867-1965), Minister of War for the first Vichy government. The French-Polish team was reconstituted in the unoccupied zone, at the Château des Fouzes near Uzès, under the name PC Cadix. The Poles received the code name *Eksposytura* 300 – position 300 – and lived clandestinely under false names: Marian Rejewski was Pierre Ranaud, a mathematics teacher from a high school in Nantes. This center broke the codes of German messages with keys provided by Bletchley Park. Scientific codebreaking was now going to be fully supported by the British.

BLETCHLEY PARK AS A FACTORY FOR INDUSTRIAL-SCALE CODEBREAKING

From the outbreak of the war, the GC&CS experienced a radical change of scale. Initially a small structure, it became a very large-scale organization combining manual and mechanical methods. Bletchley Park was divided into different sections and units.

[16] See p. 26.

between which a strict division of labour was established to preserve secrecy. Even though mathematicians, as individuals, often considered their work at Bletchley Park as a personal game, and did not really want "to know anything about what was going on outside [their] own bailiwick" [WEL1 p. 58], their research was part of a collective enterprise supported by a vast framework, which grew continuously in both manpower and influence throughout the war.

1. Bletchley Park's answer to the *Blitzkrieg*

In his *Hut Six Story*, Welchman characterized Hitler's *Blitzkrieg* as "speed of attack through speed of communications, [achieving] one of the greatest revolutionary changes in military history" [WEL1 p.19]. The speed of attacks by *Panzer* divisions and *Stukas* was supported by very well-coordinated cooperation between all the fast-moving German forces, ensured by the speed of their communications. Enigma played a major role in this secure coordination of information flow, particularly between the air force and the ground forces, and between the front lines and the rear, where command vehicles were equipped with portable battery-operated Enigma machines. This new situation "was not a revolution in technology", Welchman insisted:

> "Rather, it was a revolutionary attitude to what existing communications and crytpographic technology could contribute to the combined operation of fast-moving ground forces and their air support. It was a matter of organization, training and scale of effort. Above all, it was a matter of thinking out what problems had to be solved. Because the Germans had done such a good job, the problems with which we were faced were unprecedented. Never before had radio signaling and cryptography been employed on such a large scale to provide battlefield communications" [WEL1 p. 20].

The cryptanalysis work of the Polish Cypher Bureau had already born witness to the importance of close cooperation between intelligence services, mathematicians, engineers and operators responsible for implementing the procedures accompanying the use of the equipment. This cooperation took place through personal acquaintance in a small department, the *Biuro Szyfrów.* What was new in the organization of cryptanalysis at Bletchley Park was the construction of a systematic, and even a systemic view of its organization, which is clearly embodied in its material structure.

The mansion was dedicated to the supervisory staff. For the first weeks at Bletchley Park, the Research Section, Knox's team, was located in the Cottage –part of the stables on the side of the mansion –, with Twinn, Turing, Jeffreys, and Welchman. And very quickly, all through the grounds, around twenty much less comfortable wooden *Huts,* were built, hosting both cryptanalysts and the more and more numerous staff needed to prepare their work. Each of these Huts was dedicated to a specific activity, largely to the breaking of specific Enigma ciphers, but also to the reception of messages from interception stations, to the translation of decoded messages, and to their transmission to intelligence services or government authorities.

The first group of mathematicians recruited were gradually dispersed around the site as they headed up research in different Huts. For instance:

- Hut 7 dealt with the Japanese naval section. It was headed by Foss before he went to the USA in 1944. The unit later expanded and moved to Block B.

- Hut 6 was initially dedicated to the *Wehrmacht* and the *Luftwaffe* Enigma ciphers. At its head, Welchman organized his original views on traffic analysis (TA), before he became Assistant Director of Mechanization in the fall of 1943.
- Hut 8 was dedicated to the German Naval Enigma machine. It was headed by Turing, then Alexander (1942), and later Mahon (1944). Its name was retained when Huts 3, 6 and 8 moved to Block D in February 1943.
- Hut 3 dealt with messages sent by the German Army and German Air Force. It prepared the messages for the Hut 6 production line, and, when messages had been decoded, it ensured their translation, their interpretation and their delivery to various intelligence departments in London. Peter Calvocoressi (1912-2010), the author of *Top Secret Ultra* (1980), headed the *Luftewaffe* section in Hut 3. In 1939, it was supervised by Frederick Winterbotham (1897-1990), the author of *The Ultra Secret* (1974), who organized the Special Liaison Units (SLU), who ensured that the rigorous security procedures were correctly followed [WEL1, p. 160].
- Hut 4 had the same role for the messages of Hut 8.
- Several of the Huts, like Hut 1 and Hut 11, would host the British bombes.

The specialization of work in Huts and Blocks was the essential character of the new organization of Bletchley Park, which Knox for instance was particularly reluctant to follow. He repeatedly threatened Denniston that he would resign because he would no longer be able to keep an eye on the whole process of codebreaking, until transmission to the Intelligence Service. This new structure did not fit well with his own linguistic approach [BAT, pp. 133-134], Welchman was very influential in setting up this new organizational plan of work. Before the Huts were built, he proposed a whole organizational plan to Denniston and his deputy, Commandant Edward Travis (1888-1956), covering all Bletchley Park's activities. He considered it necessary to work 24 hours a day, with five closely coordinated departments:

> "a Registration Room, to perform a continuous traffic analysis of Enigma messages, based on traffic registers received by teleprinters from the interception stations; an Intercept Control Room, which would …. [help] them concentrate on the most valuable traffic; a Machine Room handling the cryptanalytic aspects in close collaboration with [these two Rooms]; a Sheet-Stacking Room, which would be called into action by the Machine Room whenever the traffic of a particular day on a particular key merited an attempt at a break; and finally a Decoding Room to handle the messages on any key that might be broken" [WEL1, p. 76]

Denniston and Travis gave their full support to the plan, as did the heads of the Army and Air Force sections, and official agreement was obtained to implement it. This organization would be generalized to all the Huts, even after Jeffreys' perforated sheets were no longer the main codebreaking tool. Welchman considered this to be his "biggest single contribution to the war effort" [WEL1, p. 77]. He was also conscious that a considerable staff was needed to execute this huge number of distinct tasks, from the stacking routine of Jeffreys' sheets to the work of Enigma experts [WEL1, p. 75]. The whole staff of Bletchley Park numbered several hundred people in 1940. This would increase to about 10 000 in 1945, with each swearing an oath of absolute secrecy as to their activities. Young women were also needed more and more to staff these Rooms [WEL 1, p. 86]. Responsibility and trust were the hallmarks of the work of all participants regardless of their role, rather than the usual respect of hierarchical positions. And so, even though Turing is often considered as a very eccentric man, he could very well adapt to this type of organization**.** The work was very intense, and from March 1940, was carried out 24 hours a day, in three watches [MAH, p. 27]. Irene

Young, one of the operators from Edinburgh University, would testify that in the Decoding Room, operators often had to go outside because of the terrible noise and the pace of work [YOU, p. 74].

In fact, this division of labour was suited to the profusion of messages to be cracked, the necessity of speed, and the security requirements. For instance, when Welchman was instructed by Knox to analyse intercepted traffic in the first months of his recruitment, he did not know anything of the contents of the Poles' gift [WEL2, p. 196-198], and he reinvented Jeffreys' sheets, which irritated Knox because Welchman had strayed outside what he was supposed to do. In fact, until the preparations of D-day, it was "most extraordinary … how little everyone knew about the whole picture", having only "tunnel vision" [WEL2, p. 223].

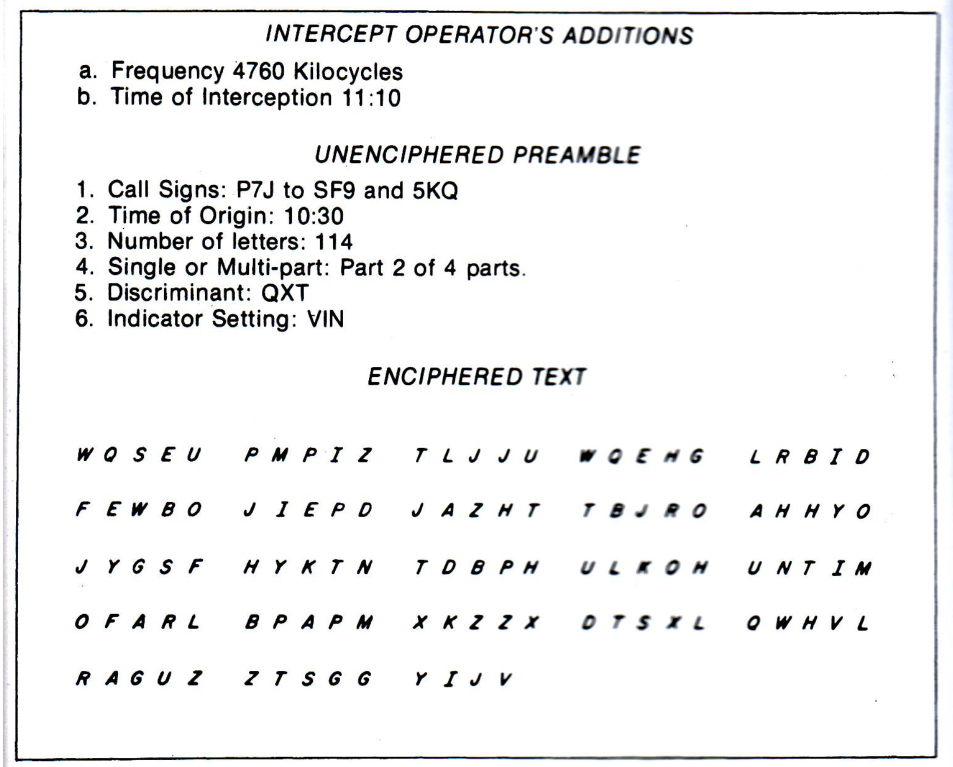
2. The organisation of work at Bletchley Park

The level of research was changing radically. In the first months at Bletchley Park, the Enigma traffic was analyzed in a very "methodical manner". And Welchman underlines how he began to think of its characteristics with the same state of mind as in algebraic geometry research, when he had first to find a method, when faced "with the problem of thinking of something to think about" [WEL1 p. 37].

Before the setting up of Hut 6, Welchman left the Cottage for the neighboring Elmer's School, and "began to analyze intercepted Enigma traffic simply as traffic – worrying about the structure of the communications system rather than the unknown content of the messages that it carried" [WEL1 p. 58]. As soon as he received the first collection of decoded Enigma messages – without knowing their origin – he began to understand that cryptology was no longer a question of dealing with inextricable puzzles in individual messages, but that Bletchley Park had to deal with something very different. So he developed what he called 'traffic analysis', today described as metadata analysis. He echoed Auguste Kerckhoffs' claim (1835-1903) – whom he referred to – when he considered cryptographic systems where armies communicated by telegraph.

As it is common in scientific research in general, he began to classify different pieces of information, drawing up lists and charts in order to sort out the different sources of German messages. Many useful elements came from the Army radio interception radio station at Chatham. Close collaboration between Welchman and Commander M. J. N. Ellingworth, head of the Chatham station, led to their joint decision that a daily register of intercepted teletype traffic would be sent from Chatham to Bletchley. By analysing the un-ciphered preamble to the German messages he received, Welchman was able to obtain various valuable indications such as:

- the callsigns of the radio stations sending and receiving the messages, because a same station often sent messages to several groups,
- the discriminants, which distinguish different types of Enigma traffic, because communications were also partitioned between German army corps,
- the indicator setting, which gave the receiving operator the starting position for the three wheels, – here VIN – from which the wheel setting – here RCM – was encoded twice, giving the six first letters of the message, this is the indicator, or the message setting – here WQSEUP.



INTERCEPT OPERATOR'S ADDITIONS

a. Frequency 4760 Kilocycles
b. Time of Interception 11:10

UNENCIPHERED PREAMBLE

1. Call Signs: P7J to SF9 and 5KQ
2. Time of Origin: 10:30
3. Number of letters: 114
4. Single or Multi-part: Part 2 of 4 parts.
5. Discriminant: QXT
6. Indicator Setting: VIN

ENCIPHERED TEXT

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

Figure 3.2 Composition of a Typical Enigma Message

By permission of the publishers M & M Baldwin

Classifying messages from these preambles gave the structure of the German system of ciphering on different Enigma machines. Moreover, an indexing system was established, by cross-referencing, from each decoded message every correspondent, every ship, every unit, every weapon, every technical term, and every stereotyped locution such as form of address and any other piece of German military jargon, and by recording this information on cards to help the interpretation of later messages [WEL, p. 160]. It was essential in order to allocate messages to the different Huts where they were to be analyzed and broken. Welchman considered that:

> "We were dealing with an entire communications system that would serve the needs of the German ground and air forces. The callsigns came alive as representing elements of those forces, whose commanders at various echelons would have to send messages to each other. The use of different keys for different purposes, which was known to be the reason for the discriminants, suggested different command structures for the various aspects of military operations" [WEL1, p. 38].

So, Welchman's traffic analysis resulted from a conscious and systematic approach to how to respond to the new German organization for secret communications. For each message, his data recorded; the German network identifier, the time the message was sent, the indicative of the transmitting and receiving stations, the discriminant and the indicator. He came up with the idea of using colors to distinguish the different networks: Red for the main *Luftwaffe* cipher, used for operational purposes; Green for the cipher used by the German army's military districts and Blue for the *Luftwaffe* practice cipher. And the corresponding messages could therefore be allocated to the corresponding Huts and Blocks, so that specific methods could be applied to decode them [WEL1, p. 54].

Cipher breaking did not consist solely in recovering the Enigma machine's cryptographic system. Once cryptanalysts obtained a consistent and readable sequence of German words, the work went on to the decoders, who extended the reading thanks to the key; translators and consultants then had to interpret abbreviations and military jargon. So, the success of cipher breaking required delicate coordination between all these activities, and it was not always very easy. In Bletchley Park as in Poland, the process was not always smooth, and enciphered messages were often broken weeks or even months after they were received. But even in these cases, they still provided useful information about the enemy.

MANUAL METHODS
PREPARING THE WORK FOR THE MACHINES

When Turing arrived at Bletchley Park in September 1939, he joined the research section and studied the Polish documents they had received on August 16, 1939. Although he started designing the British Bombes in the fall of 1939, the first prototypes were not built until March 1940, and there would not be enough machines to keep up with the German traffic before mid-1941. So manual methods and much manpower were necessary from the outset to break the codes and to deal with the traffic. This continued even when the Bombes were fully operational, and would remain necessary to deal with the Bombes and to shorten their running time.

1. Specific methods from encoding weaknesses

To explore cribs, whether manually or mechanically, the crucial point was to reduce the huge number of possible rotor positions and their initial positions. To this end, vulnerabilities in the cryptographic system, such as the clumsiness of German radio operators, were systematically analyzed, giving rise to specific methods for working on indicators.

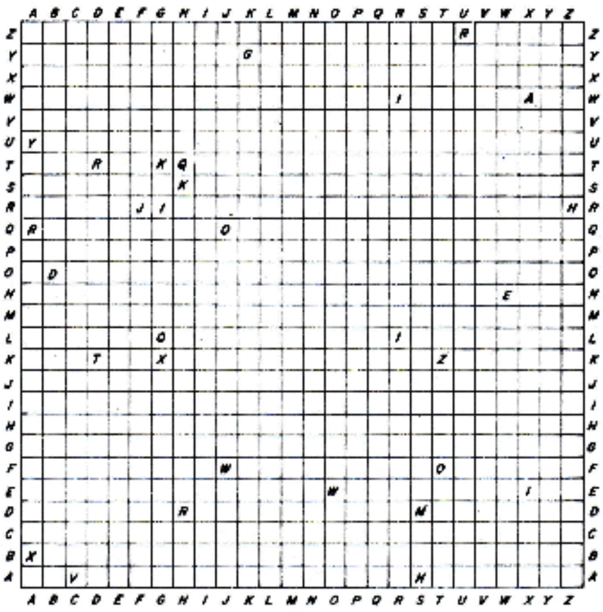
Very often, the lack of time forced German radio operators into making procedural errors such as forgetting to change the daily key or the message key, or sending the same message twice. It was common that naval messages were also sent with the weaker ciphering system installed at the shipyards, which was weaker. British cryptanalysts named called "gardening" the collection of such vulnerabilities. These vulnerabilities often received special names, such as "Cillies", which designated the use of keys easy to guess in the indicator – for example AAA – or adjacent letters on the keyboard – for example QWE or ASD, or frequent swear words [WEL1, p. 97-118].

1.1. The Herivel tip, or 'Herivelius'

In February 1940, the newly recruited[17] Herivel observed that for the first message of the day, German operators sometimes set the ring settings when the rotors were already in the machine, and simply used the letters appearing in the aperture of the machine for the *Grundstellung* – initial rotors position – rather than choosing them at

[17] On January the 20th, 1940.

random. In such conditions, these letters were currently the ring setting itself, or were very close to it. This simple remark became a method, the 'Herivel tip', for which the Herivel square was created in order to narrow down the number of three possible letters of an indicator. The first letter was read horizontally, the second vertically, and the third was written at the intersection of the corresponding line and column. When a cluster of letters close to each other was recognized, the number of ring settings to be tested dropped from 17 576 to between 6 and 30 possibilities. The Herivel tip was then combined with other techniques, such as the ‘Cillies’, to find the order of the rotors and the plugboard settings [WEL1, p. 98-102].



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

HDR TKZ JFW AQR GRI BOD

DKT TFO RLI HTQ WNE ABX

HSK ZRH KYG OEW AUY SAH

JQO GKX GTK GLQ XWA FRJ

XEI CAV DTR RWI SDM UZR

Figure 5.1 A Herivel Square, with Entries Representing 30 Indicator Settings

Fig. 8. The Herivel square [WEL1, p. 100]
By permission of the publishers M & M Baldwin

The Herivel tip was conceived before the Nazis invaded France on May 10, 1940, when the double cipherment of the message keys was interrupted, making the Zygalski sheets unusable. At this very moment, Herivel’s method became very efficient due to the increasing carelessness of German operators under the pressure of the military situation. Welchman noted that Bletchley Park was entirely dependent on the Herivel tip and on the Cillies from May 1940 to the last Eagle Day, on September 15, 1940, which marked the end of the Battle of Britain, when Hitler renounced his invasion plans. "Hut 6 Ultra revealed Goering's plans for that critical day and helped the RAF to make the best use of its remaining capabilities" [WEL1, p. 102]. The first prototypes of the British Bombes arrived at Bletchley Park in August, but were still experimental, and far too few in number to deal with all the Enigma traffic.

1.2. The pinches

Breaking the Naval Enigma code was the key occupation of Hut 8. In May 1937, in order to reinforce communications security between the U-boats and Commander Dönitz, the *Kriegsmarine* had introduced a more hermetic procedure for enciphering the indicator. In fact, the *Grundstellungs* were provided by key lists, and were the same for all the messages sent on a particular day. But the messages were then super-ciphered by using combinations of bigram and trigram substitutions, whose tables were collected in a booklet, the *Kenngruppen Buch*, or K-book in English. Even though Turing discovered the structure of this new Naval Enigma ciphering system shortly after his arrival at Bletchley Park, no work could be undertaken without the K-books, which could only be obtained from the U-boats.

Special operations were organized for the purpose of pinching K-books from the Germans. Documents were finally seized on April, 26, 1940, during the Battle of Narvik in Norway from a German patrol boat disguised as a Dutch trawler, *Polares*: instruction manuals, library card indexes, and a recording of transmissions were collected. These documents allowed a partial reconstruction of the bigram tables and messages could be analyzed for the period between the 22th and the 27th of April, some of them retrospectively, and the last just as the first Bombe "Victory" was installed in March 1940 [COP, p. 259].

Given the crucial necessity of these bigram and trigram tables, numerous plans were then devised in order to retrieve them. The Lofoten pinch on March 3, 1941, gave all the keys for February, and the successful June and July 1941 pinches were a real boon, occurring just at the moment where the bigram tables were changing on the 15th of June [MAH, p. 24-26].

1.3. '*Banburismus'*

Thinking up methods to shorten the breaking of the Engima code also led to the development of a probabilistic approach to the situation. When he discovered the Naval Enigma's system of indicators, Turing both created a method called *Banburismus,* which extended the clock-method invented by Różycki in Poland during the 1930s. Both methods correspond, in being a simpler way to 'attack' a cipher by the index of coincidence, produced in the USA by William Friedman (1891-1969) in 1920. Cases like this, where the same or similar method or theory is produced independently by several scholars at approximately the same time, happens very often in the history of mathematics, and in also cryptography.

As the *Grundstellungs* for the *Kriegsmarine* messages were given for a whole day, it was possible that, for part of a message, the wheel positions became the same as their starting positions for another message. In that case, these parts of the two messages were said to be 'in depth', and the repeat rate of letters between the two messages was 1 / 17 (cf. Paragraph 3.4)[18]. In order to compare two messages in depth, they each one was punched onto a thin card as long as the message, about several meters, and about 25 cm wide. The letters of the alphabet were written in successive columns all along each

[18] This rate is slightly different from the coincidence index of the German language, due probably to the fact that the messages are specific to war time.

card, and a hole perforated for each successive letter of each message. Two message-cards were superimposed over a light, which shone through the cards in the case of repeated letters, called a "fit". The name *Banbarismus* was derived from the place where the cards used in the process were manufactured – Banbury, in the Oxford area. Hugh Alexander, Jack Good and Joan Clarke –Turing’s one-time fiancée – were very efficient Banburists, fond of this "intellectual game" [MAH, p. 20].

Turing described the method in his *Treatise on Enigma*, a manual known as the *Prof's Book*, he wrote in 1940 bringing together the methods used at Bletchley Park for newcomers[19]. While he was a brilliant mathematician, he was too untidy, and devoid of the "determination of practical men", to oversee the establishment of the method [MAH, p. 24]. About 200 messages were needed in order to make it efficient. And an enormous staff had to be recruited, organized and trained. *Banburismus* began to be used in March 1940, and at first, it proved to be more difficult to use than expected. It was first successful on messages from May 8, 1940, finally cracked by Hugo Foss in November. Thereafter May 8 was celebrated as "Foss day" in recognition of this triumph. Autumn 1941 was the beginning of *Banburismus* running at full efficiency, the "operational period", reading 400 daily messages [MAH, p. 31, p. 48]. It was "the fundamental process which Hut 8 performed" [MAH, p. 14] until September 1943, when Bombes were numerous enough to take the place of this vast collective manual endeavor.

2. The crucial role of cribs

Seeing the difficulties encountered by the Poles with the increasing changes in the indicators by the Germans, like Knox, Turing became convinced that it was necessary to tackle codebreaking from the content of the messages. In this approach, as was already the case in the rodding method, cribs gained more and more importance, as they reduced the number of possible wheel positions to test, whether manually or mechanically. Even the British Bombes would have been useless without the cribs [WEL1, p. 120]. They were issued from frequently used stereotypical German sentences or locutions, often located at the head or at the foot of messages, such as hierarchical headers. They also characterized certain types of messages, such as weather reports. But they frequently resulted from the carelessness of the operators caught up in an emergency, what Welchman considered as procedural errors [WEL1, p. 98]. Cribs were recorded in a very systematic way, in order to optimize their use and to ensure maximum continuity in codebreaking.

Polish cryptanalysts had already made use of cribs, particularly the FORTYWEEPYWEEPY. When a message was the continuation of another one, it began by FORT, the abbreviation of the German word *Fortsetzung* – which means 'continuation' – and repeated the time the first message was sent, framed with the letter Y. At this time, digits were represented by letters in the top row on the keyboard. So, the second message sent at 23.30 began by: FORTYWEEPYYWEEPY. This method was particularly efficient when the number of wheels and steckered letters[20] was small,

[19] Turing wrote two main papers on the theory of this probabilistic approach, entitled “The Applications of Probability to Cryptography”[and “Paper on Statistics of Repetitions”. They were released to the UK National Archives only in April 2012.

[20] The steckered letters are the pairs of letters connected by the plugboard. See the indications of the daily key table on p. 5.

as the cryptanalysts could suppose correctly enough that the letters of the crib were not concerned. Anyway, this method became completely useless when it was decided to write numbers in full [MAH, p. 14-16]. Once Turing and his team learned of this change from the interrogation of a German radio operator in early 1940, they could review old messages with this new information on cribs which had previously seemed incorrect[21] from November 1938. They discovered that 70% of them were correct cribs, and continued to gather intelligence from these messages prior to the introduction of the 4th and 5th wheels [MAH, p. 1, p.t 21].

Turing drew up an automatic catalog with all possible ciphers of the word *Eins* – "one" in German, the most common tetragram in all the German messages – for all the possible positions of the wheels, with their orders and possible steckered letters. Short cribs could be used, but their optimal size was about thirty letters. Weather reports were a very valuable source of cribs, particularly from French Channel ports until the spring of 1942, so was the re-encodement of messages from a complicated code to a simpler one. Cribsters had to be open minded to always test new suggestions, have good intuition to recognize similar messages and specific words, and their experience was an irreplaceable quality [MAH, p. 44].

In 1940, cribs were provided to Hut 8 by the Naval Section. This transmission was a waste of time, and tensions existed between the two when the cribs failed. So, Milner-Barry set up a Cribbing Room in Hut 8, with specialized cribsters who knew exactly how Enigma worked, but nevertheless keeping close contact with the Naval Section for good suggestions [MAH, p. 24]. At the same time, the German Security Service kept a close watch for possible weaknesses in these transmission systems, changing them regularly and even sending dummy messages. So, cribs never lasted very long, and it was always necessary not only to find new ones, but also to keep all old or unsuccessful cribs, which might prove efficient later with new combinations and improvements in codebreaking methods [MAH, p. 40].

Beyond all these usual attempts, cribs took a central place as the Bombes could not be used without them. They were presented as diagrams to be established on the machine, before its running detected if it was a correct one or not. Cribbing became the only means of attack after the introduction of the 4-wheel Enigma by the *Kriegsmarine* in February 1942.

THE BRITISH BOMBES

The idea of a machine to help codebreaking had already been considered by Knox, and even more so after he encountered the Polish cryptanalysts. Turing discussed this idea with him [BAT, p. 95], but the Bombe he designed was very different and pioneering compared with the Polish one, as it could be used to determine if a crib was correct or not, from successive assumptions on the steckered letters. Its electrical circuit settings established the relationships between the letters of the ciphered message and the plaintext. So it could be said that the machine automatically carried out logical deductions founded on a *reductio ad absurdum*, as it indicated if a hypothesis was right

[21] The reason for choosing a period so long ago was that the method was no longer efficient with the two new rotors introduced in December 1938.

or wrong. It was designed between late 1939 and early 1940, but initially there were not enough machines to support the analysis of all the traffic.

1. Description of the Bombe

The Bombe was a bit wider than tall and measured about 2 m high and 60 cm deep. It was composed of ranks of twelve sets of three rotating drums. Each triplet of drums was positioned vertically with the fastest drum at the bottom, and represented the three rotors of an Enigma machine. So one Bombe corresponded to twelve Enigma machines. In the refurbished Bombe now at the National Museum of Computing at Bletchley Park, the drums are colored to indicate which of the eight different Enigma rotors they simulate: Red I; Marron II; Green III; Yellow IV; Brown V; Cobalt (blue) VI ; Jet (black) VII; Silver VIII.

The machine had no reflector, and each of the drums carried a double input-output system of 26 letters, that could be connected together in 26 different ways by cables. This is why there are so many cables at the back of the machine. The electric current could browse them in either direction. It took about 20 minutes for the current to flow through all the 17,576 possible rotor order positions.

2. How the Bombe dealt with menus

To form a circuit, the Bombe simulated several Enigma machines, here 36, which ran together in order to test hypotheses on the possible configurations of the Enigma machine that enciphered the message. They are wired together as instructed by a “menu”, which is nothing more than a crib presented as a diagram, and using the principle of reciprocity of the Enigma ciphering process. This menu was prepared by the cryptanalyst, and set on the machine by operators, generally women, to test the consistency of the relationships between the letters in the "crib" and those in the cryptogram.

With a crib such as the one below, presented by Turing in chapter 6 of his *Treatise on Enigma* [TUR3, p. 315]:

1	**2**	3	4	**5**	6	7	8	9	**10**	11	12	13	14	15	16	17	18	19	20	21	22	**23**	24	25
D	**A**	E	D	**A**	Q	O	Z	S	**I**	Q	M	M	K	B	I	I	G	M	P	W	H	**A**	I	V
K	**E**	I	N	**E**	Z	U	S	A	**E**	T	Z	E	Z	U	M	V	O	R	B	E	R	**I**	Q	T

where the plaintext means : "no additions to preliminary report”, there is what was called a loop, or a “closure”:
- between letters *A* and *E*, in positions 2 and 5.
- between letters *A*, *I* and *E*, with positions 5, 10 and 23,

and they have a common letter *A*.

The corresponding menu indicated the position of the links between letters in the enciphered message and the crib, and showed the loops. Turing established that these loops were independent of the stecker values of the input and output letters. That means that, what is seen here between *A* and *E* for example, also happens between the stecker values. So, the process can be used to determine them. If the correct stecker value of A is supposed, the Bombe would show the loop.

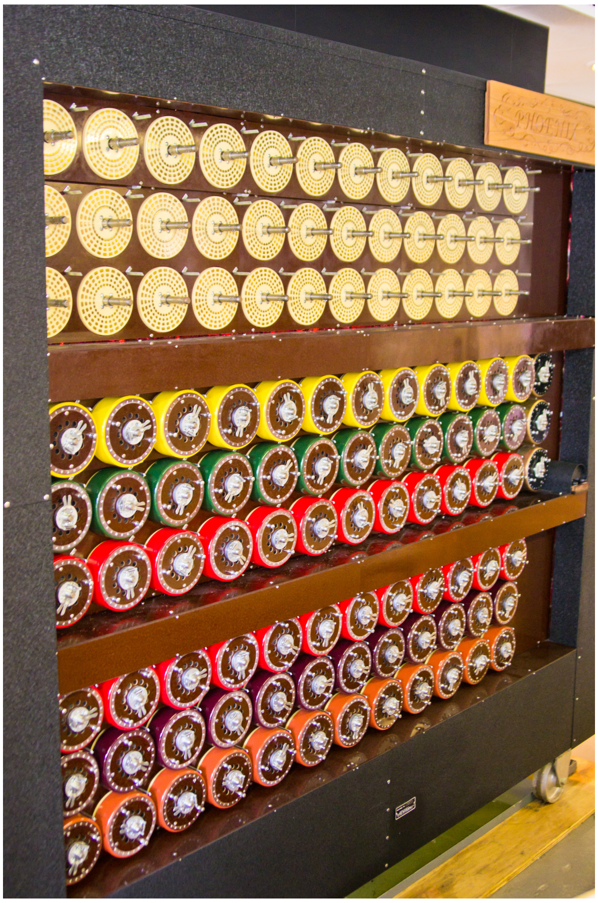


Fig. 9.The British Bombe, as rebuilt now at the National Museum of Computing on Bletchley Park. Wikimedia Commons. Public domain. Author : Alain Taveneaux.

In Appendix I of his *Hut Six Story*, Welchman gave a more detailed example, with a crib in English, where he clearly exemplified the correspondence between the loops and the machine setting. As in examples given for the rodding method, this example assumes there was no turn-over of the middle rotor before the end of the letters in the crib. If this occurred, no correct solution would be found and other positions had to be tested.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
C	O	M	Z	P	V	L	I	L	E	U	I	K	T	E	D	C	G	L	O	V	W	V	G	T	U	F	L	N	Z	P
T	O	T	H	E	P	R	E	S	I	D	E	N	T	O	F	T	H	E	U	N	I	T	E	D	S	T	A	T	E	S

One of the three menus extracted from this crib was as follows :

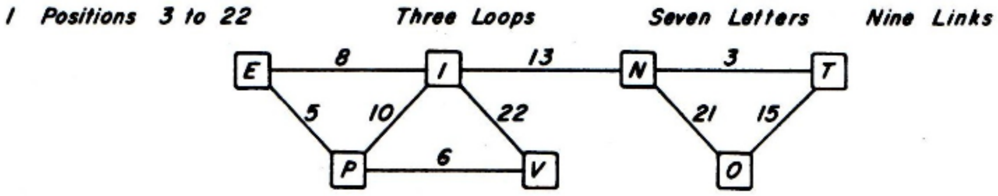


Fig. 9. FromWelchman's diagram of this menu [WEL1, p.240]
By permission of the publishers M & M Baldwin

As seen in fig. 10, the same letter was input as the supposed stecker value of the letter ‘I’ common to the three loops, and each letter of the alphabet would be tested successively. The Bombe would stop whenever the configuration of the drums identified the loop. Then, the positions of the drums and the output letter for each replica were noted.

The number of Enigmas on the Bombe allowed three rotor orders to be tested simultaneously if it was supposed that no more than 12 Enigmas were required for the loops in a crib. Each correct position given by the machine from the crib was then tested in another Hut on an Enigma machine or on the British Type-X enciphering machine to find the entire plaintext.

Turing's idea for the Bombe was improved by the diagonal board, immediately conceived by Welchman during the design period. Welchman would later highlight his own contribution, as well as the collective aspect of the work [WEL1, p. 77-83]. It connected electrically all symmetrical couples on a square panel of 26 by 26 plugs. It made it possible to avoid having to use very long "cribs", and to use fewer loops, or no loop at all. This diagonal board was designed in early 1940, even before the delivery of the first Bombe prototype, and had such a marked effect on operating efficiency that the new Bombe was first called “The Spider” [TUR3, p. 323-331].

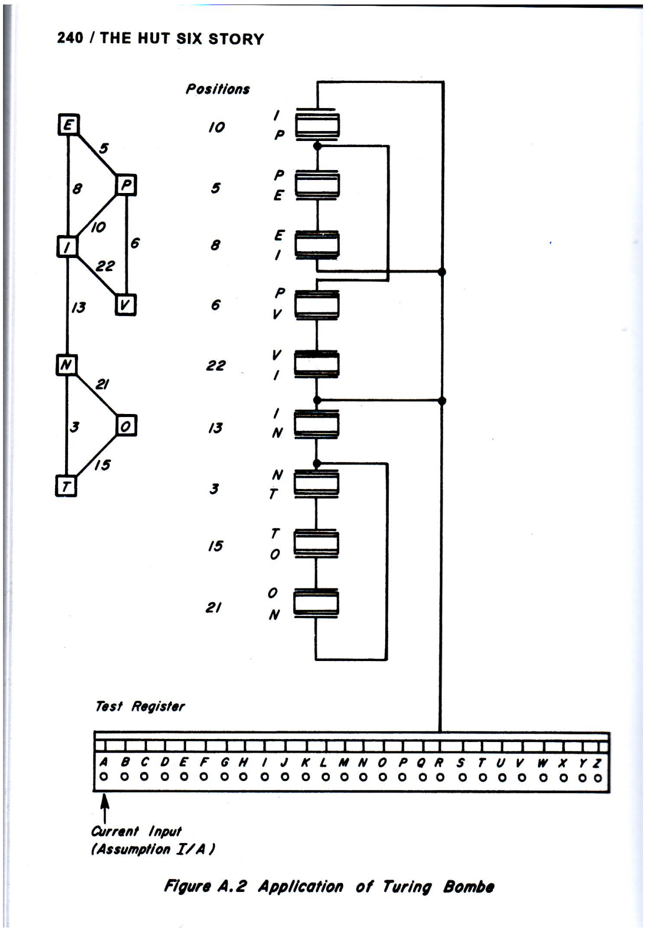

240 / THE HUT SIX STORY

Figure A.2 Application of Turing Bombe

Fig. 10. A menu by Welchman, and the associated Bombe setting [WEL1, p. 240]
By permission of the publishers M & M Baldwin

3. The Construction of the Bombes

A sum of one hundred thousand pounds was allocated to the construction of the Bombes, which was assigned to the British Tabulating Machinery Company (BTM), a subsidiary of IBM directly involved in the mechanization of Ministries and commercial firms from the interwar period. Manufacturing Bombes for Bletchley Park would be its main activity during the war. The construction was briskly managed by Harold Keen, the Head of Design and Development at BTM. He was nicknamed "Doc" because of the doctor's briefcase in which he always carried his documents.

On March 18, 1940, the "Victory" prototype was installed in Hut 1. It would later be equipped with a diagonal board. The complete 'Spider' form of the Bombe was delivered on August 8, 1940, and called "Agnus Dei", later shortened to "Agnes", and then "Aggie". Some described it as a "Bronze Goddess". During the year 1940, 178 messages were read on both machines, almost all successfully. In June 1941, five Bombes were in use. From mid-1941, they would read all the daily Nazi enciphered traffic.

There would be fifteen Bombes in service in November 1941, twenty in September 1942, forty nine in January 1943, and up to 200 at the end of the war. They were much needed during the Battle of the Atlantic, and even more so when the the *Kriegsmarine* introduced a four-rotor Enigma machine. The Bombes were installed at various sites around Bletchley Park for security reasons, and mobilized about 2 000 Operators, essentially women from the Women's Royal Naval Service (WRENS), who worked under the responsibility of an RAF engineer, Sergeant Jones.

By 1942 approximately 39 000 messages were read each month at Bletchley Park and this number increased to approximately 84 000 at the end of 1943.

7.4. Codebreaking was not limited to the Bombes

The work of the Bombes allowed the codebreakers to identify the order of the rotors, their initial positions, and the steckered letters connected by the plug-board. But other methods were still used to complete the codebreaking process, particularly to eliminate wrong stops that could be produced by the menus.

Moreover, there were very few Bombes, especially at the beginning, and their use has to be rationed carefully between the different codebreaking sections. So, to avoid wasting time with an excessive number of wrong stops, Turing carried out a long probabilistic analysis – firstly without electronic aid – to estimate the number of stops for each rotor order. It was adopted as a standard practice to use menus that had been estimated not to produce more than four stops for one rotor order. This led to normalizing the length of the "cribs", according to the number of their loops.

COLLABORATION WITH THE US FROM BOMBES TO ENCODING VOICE

Before the United States entered the war, collaboration was set up with Great Britain on attacking German ciphering. Denniston visited Friedman who held him in high esteem [WEL2, p. 202]. But the British were very cautious because it was crucial for them that the Nazis and their allies did not guess that their Enigma codes had been broken.

US experts were sent to Bletchley Park in February 1941. From December 1941, because of the intensification of the Battle of the Atlantic, and with the adoption of the 4-rotor Enigma machine by the *Kriegsmarine*, the United States and United Kingdom reinforced their relationship, with reciprocal visits, one by Tiltman to the US Navy Cryptanalysis Office (OP-20-G) in April 1942, and another by US Navy lieutenants to Bletchley Park in July 1942. An agreement between the USA and UK was signed on the 2nd of October of that year. The British agreed to provide assistance and information to the United States. The agreement was limited to the construction of 100 Bombes, and the coordination of the work was left to the GC&CS. The Bombes were built by the United States Naval Computing Machine Laboratory of the National Cash Register Corporation (NCR) in Dayton, Ohio [HOD, p. 206].

Turing went to the United States on October 19, 1942, where he stayed until March 1943. He was then attached to the *British Joint Staff Mission* in Washington, because of his expertise in the Bombes and their use. On June the 22nd, 1943, the first two machines, "Adam" and "Eve", broke very difficult messages dated June 9 and 10. In December 1943, 121 machines were finally installed, which were faster than the British ones [WIL, pp. 18-55].

Military coordination between the UK and the USA also required oral communications between political authorities. These transmissions were vulnerable to interception, and research was quickly organized to encode voice. During his six months in the USA, Turing spent much time at the Bell Telephone Laboratories, and was given relatively free access to investigate the security of the speech systems under development at Bell Labs, particularly the SIGSALY machine, and he wrote a report on these devices dated March 4th, 1943 [HOD, p. 215]. They were developed there under a vast modular research system that ensured secrecy.

On his return to Bletchley Park, Turing pursued this research for the Radio Security Service at Hanslope Park, which worked closely with Bletchley Park to develop this new type of equipment. The Delilah machine was a portable digital device for encoding vocal communications, which, like SIGSALY, worked with modular arithmetic and the Vernam ciphering system. It was operational in 1945 and Turing was able to cipher and decipher a speech recorded by Churchill. Nevertheless, this machine lacked the capacity to be used for long distance radio transmissions. It was completed too late to be used during the war and was quickly forgotten.

THE ATTACK ON THE LORENZ MACHINE BY COLOSSUS

Even though the Nazis never suspected that Enigma had been broken, they systematically introduced new methods of ciphering with it throughout the war, such as a new machine for High Security messages. In June 1941, they started ciphering with the Lorenz machine, which was much more sophisticated and faster than Enigma. It was intended solely for the use of the Nazi High Command for military communications at the highest level. The resulting messages intercepted by the British were totally incomprehensible at first, as they bore no resemblance to those enciphered on Enigma. Nevertheless, broken messages enciphered on Enigma revealed that they came from a wireless teleprinter transmission system called *Sägefisch* by the Nazis. So, at Bletchley Park, these communications were referred to as "Fish" and each line of communication was given the name of a fish. For instance the Berlin-Paris line was called "Jelly Fish".

1. Ciphering on the Lorenz machine

The Lorenz code of this teleprinter ciphering machine corresponded to the Vernam system. It was based on the International Baudot Code for teleprinters. In this code, each plaintext character was converted into a group of 5 electrical impulses generated by wheels from which a mark or a space was printed on a paper tape[22]. A mark, that is a hole, in the paper tape, corresponded to a pulse. What is now represented by the symbols 1 and 0 was then denoted by a mark [1] and a space [0] or, at Bletchley Park, as a "cross" [1] and a "point" [0]. Today, these sets of pulses are represented by five binary digit numbers.

The key of the Vernam system automatically ciphered the sequence of pulses produced by the teleprinter. A complex mechanism, based on various arrangements of cams on 10 toothed wheels enabled to it automatically generate the pseudo-random impulses required for the characters of the key[23]. The key was automatically produced as long as the message. The impulse of the key and the message were combined in a way that would be represented today as an addition in scale 2. But this operation was still represented as rules on marks and spaces, or crosses and points [DUR&GUI, p. 14-16][24]. The configuration of the machine was changed for each message, in order to change the key for each message. But the key was no longer transmitted on a paper tape. In fact, a message began with a preamble of 12 letters represented by phonetic names:
A – Anton
B – Berta
C – Caesar
D - Dora etc

It was soon correctly assumed that each set of these 12 names was an indicator that provided the information required by the operators of the receiving station to adjust

[22] See the first part of this publication: Durand-Richard M.-J. & Guillot P., “How mathematics spread and transformed cryptographic activities”, p. 14-16.

[23] The last two wheels were motor wheels.

[24]

their Lorenz machine to the same configuration as that of the machine of the transmitting station [CAR5, pp. 2-9].

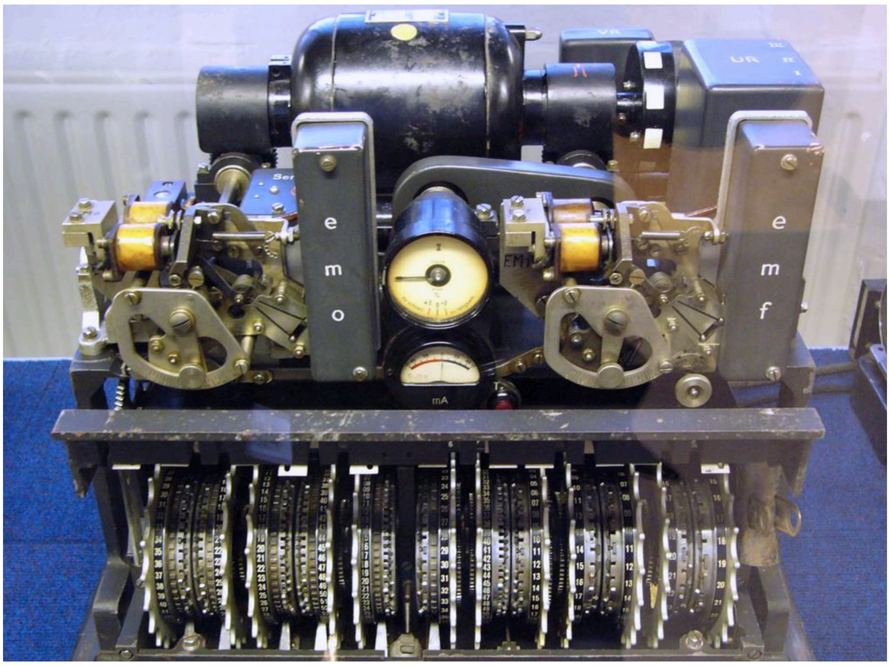


Fig. 11. The Lorenz SZ42 machine with its cover removed. Bletchley Park museum. Author Math Crypto. Wikimedia Commons. Public domain.

2. Breaking the Lorenz system: the principle

British cryptanalysts did not actually see any Lorenz machines until the last days of the war in June 1944. But they succeeded in working out how the machine ran, and in constructing a simulation machine, called "Tunny". As was the case for the Enigma machine, a classic mistake by the operators using the Lorenz machine opened the way for its cipher to be broken. In August 1941, a running error in transmission allowed two long messages to be intercepted, encoded by the Lorenz machine with the same set of letters for the indicator. Once again here, the two messages were said to be "in depth".

It is known that the double of the key is null. This is why the operation of deciphering was the same as the operation of enciphering. When two enciphered characters are obtained with the same character of the key, such that:

$C_1 = P_1 + K$ and $C_2 = P_2 + K$

where P designates a plaintext letter and C the corresponding letter of the cryptogram, the addition of these two equalities in scale 2, gives: $C_1 + C_2 = P_1 + P_2$.

It was still necessary to separate the two messages, butthere was no direct procedure for doing this. However, if one of the plaintexts could be discovered by other means, for instance with a crib, then, the other could be deduced, again by addition. By this method, John Tiltman (1894-1982) succeeded in reading these two messages manually, and the research team, headed by William Tutte, was soon able to deduce the logical structure of the machine. By July 1942, Bletchley Park was regularly able to read messages ciphered on the Lorenz machine. But the pace was too slow [CAR5, pp. 9-17].

3. The Colossus

Looking for a method to break the Lorenz cipher, Turing first worked on the arrangement of the wheels of the machine. He devised a new methodology, an iterative process known as *Turingery,* inspired by *Banburismus.* But it was impossible to use it manually, because of the slowness of its process. It would be used with the Colossus machine when it was built. Other remarks on some regularities of the cryptograms would also be tested. But Turing was not involved with the design and construction of the Colossus, as he was no longer at Bletchley Park.

A first prototype, called the Heath Robinson, operated from April 1943, but it was slow and had many difficulties arising from synchronizing the paper tapes. The Colossus was developed by Newman, who had been recruited in September 1942, and his "Newmanry Section", who worked in Hut 11, investigating ways to improve the initial machine. This group brought together men who would become better known later in mathematics, cryptography, and computer science, such as Shaun Wylie (1913-2009), Jack Good (1916-2009), Donald Michie (1923-2007) and Charles E. Wynn-Williams 1903-1979). Newman was responsible for the research on mechanical methods to counter the Lorenz machine. Tommy Flowers the main engineer and head of the Switching Group at the Post Office Research Station at Dollis Hill, brought together fifty people, including ten engineers. He had worked on automatic switching equipment before the war and was confident in the possibilities offered by electronics. He introduced his expertise into the design of the machine, despite some reluctance at Bletchley Park, particularly from Welchman [RAN, p. 60-65].

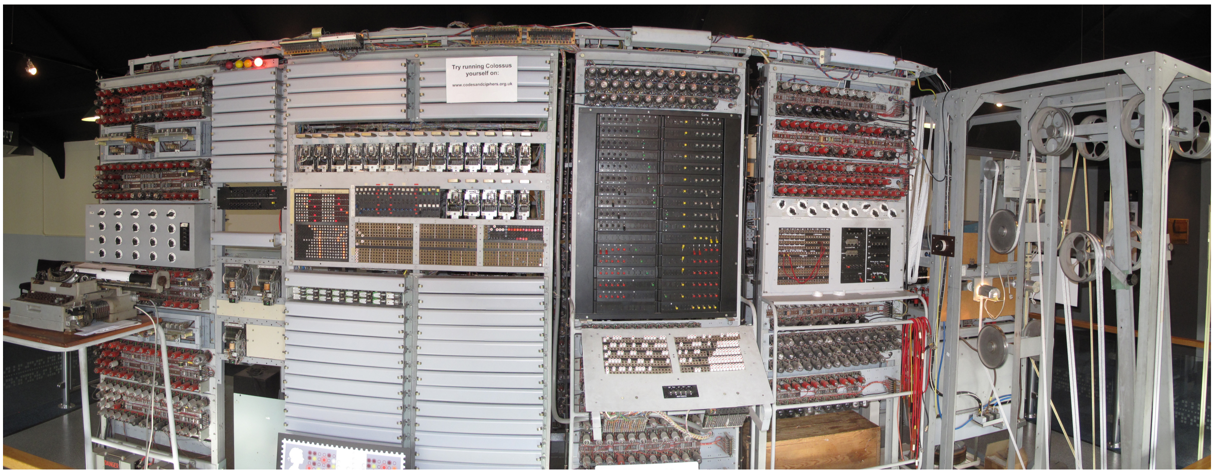


Fig. 12. Frontal view of the reconstructed Colossus; The National Museum of Computing, Bletchley Park
Author Ted Coles. Wikimedia Commons. Public domain.

Colossus was really the world's first major programmable electronic computer, pre-dating ENIAC. Built in London, it was operational in December 1943 and was moved to Bletchley Park in January 1944. It used 1500 to 2400 vacuum tubes, and was programmed using plugs and switches, not yet of course with a recorded program. 5000 operations were run per second [CAR5, pp.]17-24].

At the end of the war, 10 operating models were used to break the Lorenz codes. Each model differed from the previous one, as the design continue to evolve. Its programming was external, but it used conditional switching, and calculus on Boolean functions. The flexibility of the new machine, created by its electronic, soon became clearly apparent to its users. The nature and extent of this machine at Bletchley Park were not revealed until 2000, when the British government declassified 500 pages of a document written in 1945, "General Report on Tunny: With Emphasis on Statistical Methods". Of the ten original Colossus machines, 8 were destroyed with their plans after the war by order of Churchill in order to keep the operation secret. The last two were destroyed in 1960. It was not until 1975 that this secret was partially lifted.

Because of this destruction, the British Colossus machine did not have the same success and renown as the ENIAC in the United States. Some illegally retained plans helped to reconstruct it in 1996, thanks to the memory of the engineers involved in its initial design. And it can be seen today at Bletchley Park.

CONCLUSION

Breaking the Enigma code was a major challenge during World War II. Its success was supported by the efficiency of the work resulting from the involvement of mathematicians and engineers in the practices of military cryptanalysts, strongly endorsed by the political context. Some mechanical processes had already been introduced in cryptology after World War I. These transformations were then pursued at Bletchley Park, and on an industrial scale, which from then on would definitely become one of the characteristic features of cryptology. Cryptanalytic methods had to draw on mathematics and logic to overcome the considerable increase in the number of encryption combinations to consider after the mechanization on Enigma. The success of Bletchley Park continued the first efforts by the Poles on the military Enigma machines, and of Knox's team on the commercial machines. The theory of permutations mobilized by Rejewski, as well as the probabilities and logic mobilized by Turing, could not have been efficient without their respective Bombes. Cryptology is far from being the only field where the relationship between mathematics and technology was efficient during the 20th century. Other talks at *Niš* on analog mathematical machines in 2012 showed this was also the case in the field of physics. But cryptology here is a good example where mathematical treatment could not be carried out without these new and elaborate machines.

It is noteworthy that it was the cracking of another ciphering machine, the Lorenz machine, which led to the design and construction of a first set of electronic computers, the Colossus, which could be programmed externally. These machines were destroyed by political expediency after the War, in order that those successes were not revealed both to Britain's enemies and allies. However, this experience was invested in other British projects on computers. After the war, building computers was undertaken by three different groups: one headed by Maurice V. Wilkes (1913-2010) at the Cambridge Mathematical Laboratory, built the EDSAC, completed in 1949; one headed by Newman in Manchester, the Manchester Mark I, also completed in 1949; and one headed by Turing at the National Physical Laboratory, the ACE (Automatic Computing Engine, of which only a reduced version would be built in 1950. The theoretical Turing machine would gain in importance in this field later, when programs became software, with the development of programming languages.

References

[BAT] Batey, Mavis, 2009, *Dilly, The Man Who Broke Enigmas*, London, Dialogue.

[BAU] Bauer, Friedrich L., 2007, "Rotor Machines and Bombes", in (eds) Karl de Leeuw and Jan Bergstra, The History of Information Security, a comprehensive Handbook, , 2007, London-Amsterdam, Elsevier, pp. 381-446.

[BER] Bertrand Gustave, 1973, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Paris, Plon.

[CAL] Calvocoressi, Peter, 1980, *Top Secret Ultra,* London, Littlehampton Book Service.

[CAR1] Carter, Frank, 1999, "The first Breaking of Enigma, Some of the pioneering techniques developed by the Polish Cipher Bureau", *Report n° 10, Bletchley Park Trust Reports*, Bletchley Park edition, pp. 1-35.

[CAR2] Carter, Frank, 2009, "Rodding", *Bletchley Park Trust Reports*, Bletchley Park edition, pp. in Batey, pp. 174-188.

[CAR3] Carter, Frank, 2009, "Buttoning up, A method for recoveiring the wiring of the rotors used in a un-Steckered Enigma", *Bletchley Park Trust Reports*, in Batey, pp. 189-205.

[CAR4] Carter, Frank, 1999, "The Turing Bombe, An Account of how the machine functioned, together with some illustrative examples ", *Report n° 16, Bletchley Park Trust Reports*, Bletchley Park edition, pp. 1-40.

[CAR5] Carter, Frank, "Codebreaking with the Colossus Computer", *Report n° 1* (2nd edition)*, Bletchley Park Trust Reports*, Bletchley Park edition, pp. 1-34.

[COL] "General Report on Tunny with emphasis on statistical methods"

[COP1] Copeland, B. Jack, *The Essential Turing*, *Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life*, *O*xford, Clarendon Press, 2nd edition, 2013.

[COP2] Copeland, B. Jack, 2006, *Colossus, the Secrets of Bletchley Park's Codebreaking Computers, Oxford University Press.*

[DEL] De Leeuw, Karl, "The Dutch invention of the rotor machine, 1915-1923", *Cryptologia*, 2003, n° 27, pp. 73-934.

[GAJ] Gaj Kris & Orklowski Arkadiusz, *Facts and myths of Enigma: breaking stereotypes*, Eurocrypt 2003 Proceedings, Lecture Notes on Computer Science 2656, pp 106-122.

[GAR] Garliński Józef, *Intercept, The Enigma War*, London, Magnum book, 1979.

[GIV1] Givierge, Marcel , *La cryptographie et les Machines à Cryptographier*, in La Science et la Vie, march 1923, pp. 223-231

[GIV2] Givierge, Marcel, *Cours de cryptographie*, Nancy-Paris-Strasbourg, éditeurs Berger-Levrault, 1925.

[HOD] Hodges, Andrew, 1988, *Alan Turing, ou l'énigme de l'intelligence,* Paris, Payot.

[KAH,1] Kahn David, *The Codebreakers, The comprehensive History of Secret Communications from the Ancient Times to the Internet*, New York, Scribner, 1996.

[KAH2] Kahn, David, *Seizing the Enigma, The Race to Break the German U-boats Codes 1939-1943,* London, Revised edition. Frontline Books, 2012.

[KOZ] Kozacsuk Wladyslaw & Straszak Jersy, *Enigma, How the Poles Broke the Nazi Code*, New York, Hippocrene Books, 2004.

[MAH] Mahon, A. P. *The History of Hut Eight*, http://www.ellsbury.com/hut8/hut8-000.htm, National Archives, Kew, Richmond, Surrey, TW9 4DU. Reference HW 25/2. Its first part is also in Copeland, pp. 267-312.

[MED] Medrala Jean, *Les réseaux de renseignements franco-polonais, 1940-1944,* Paris, L'Harmattan, 2005.

[REJ1] Rejewski Marian, *An application of the Theory of Permutations in Breaking the Enigma Cipher*, Applicationes Mathematicae, 16, n°4, Varsovie, 1980. Typesetted version by Enrico Grigolon (November 2002).
https://www.semanticscholar.org/paper/Marian-Rejewski-An-Application-of-the-Theory-of-in-Mathematicae/3cf1805b074547b88d6d7dfa4c294bfb98911a1e,
site accessed January15, 2018.

[REJ2] Rejewski Marian, *Memories of my work at the Cipher Bureau of the General Staff Second Department, 1930-1945,* Adam Mickiewicz University Press, republished in 2013.

[RAN] Randell, Biran, 1980, "The Colossus", *A History of Computing in the Twentieth Century*, in N. Metropolis, J. Howlett, and Gian Carlo-Rotta, London, Academic Press, pp. 47-92.

[RIB] Ribadeau Dumas Louis, *Les décryptements des machines Enigma allemandes*, Bulletin de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI), Numéro hors-série juillet 2005.*T*

[STE] Stengers Jean, *Enigma, the French, the Poles and the British 1931-1940*, Revue belge de philologie et d'histoire. Tome 82, fasc. 1-2, 2004. Histoire médiévale, moderne et contemporaine, pp 449-466.

[TUR1] Turing, Alan M., n. d., "The Applications of Probability to Cryptography", www.nationalarchives.gov.uk, HW 257.37

[TUR2] Turing, Alan M., n. d., "Paper on Statistics of Repetitions",

[TUR3] Turing, Alan M., 2013, "Bombe and Spider (1940)", in Copeland, pp. 313-335

[WEL1] Welchman, Gordon, 2017 (1982), *The Hut Six Story, Breaking the Enigma Codes,* Kidderinster, M & M Baldwin.

[WEL2] Welchman, Gordon, 1986, "From Polish Bomb to British Bomb : the birth of Ultra", *Intelligence and National Security,* vol. 1, n°. 1, published by Franck Cass & Co, 900 Eastern Avenue, Ilford, Essex, England. Reproduced in *The Hut Six story,* pp. 195-234.

[WIL] Wilcox, Jennifer, 2006, *Solving the Enigma: History of the Cryptanalytic Bombe*, Ft. George G. Meade: Center for Cryptologic History, National Security Agency.

[WIN] Winterbotham, Frederick, 197,4 *The Ultra Secret*, London: Weidenfeld and Nicolson.

[YOU] Young, Irene, 1990, *Enigma Variations: A Memoir of Love and War*, Edinburgh, Mainstream Publishing Winterbotham Frederik, *The Ultra Secret*, London, Weidenfeld & Nicolson,1974.