Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

ENIGMA BEFORE ULTRA THE POLISH SUCCESS AND CHECK (1933-1939)

Gilbert Bloch [a] & C. A. Deavours [b]

[a] 7 Rue du Cher, 75029 Paris FRANCE

[b] Department of Mathematics, Kean College of New Jersey, Union NJ 07083 USA.

Available online: 04 Jun 2010

To cite this article: Gilbert Bloch & C. A. Deavours (1987): ENIGMA BEFORE ULTRA THE POLISH SUCCESS AND CHECK (1933-1939), Cryptologia, 11:4, 227-234

To link to this article: http://dx.doi.org/10.1080/0161-118791862054

CRYPTOLOGIA October 1987 Volume XI Number 4

ENIGMA BEFORE ULTRA
THE POLISH SUCCESS AND CHECK
(1933-1939)

Gilbert Bloch[1]
Translated by C. A. Deavours[2]

ADDRESS: (1) 7 Rue du Cher, 75029 Paris FRANCE and (2) Department of Mathematics, Kean College of New Jersey, Union NJ 07083 USA.

We continue the translation of selected sections of Gilbert Bloch's book, *Enigma Avant Ultra (Enigma Before Ultra)*. See the previous issue of this journal for the first part of the publication, Chapter III — Polish Work and the French Contribution

CHAPTER IV

A. OVERVIEW

At the beginning of 1933, the Poles had attained their objectives:

a. They had completely reconstructed the German military Enigma. By this time, they possessed a replica of the machine — a prototype, of course, but fully operational;

b. They had developed methods which, exploiting the German error of the twice enciphered message key, permitted the determination of the machine settings and the individual message keys, and, therefore, the decipherment of intercepted messages on an Enigma replica with as much ease as that of the German addressees.

From 1933 until the end of 1938, the Poles kept their advantage. The *Biuro Szyfrow* read the majority of German radio Enigma messages transmitted by the Army, the Luftwaffe, and the S.S. [1] All through this period, the Germans changed certain workings of the machine, increased the frequency of key changes, and altered ciphering procedures. The Poles always, and with surprisingly short delays, kept up with these changes and continued their decipherments. To better aid them in their tasks, the Poles — particularly the trio of mathematicians Rejewski, Rozycki, and Zygalski — devised numerous methods, invented hand and mechanical *devices*, and, finally, created electro-mechanical machines which, from characteristic data of the intercepted messages, could find the daily settings used for the encipherment. During all of this period, the Poles alone were able to accomplish these things. [2]

On the 15th of December 1938, following new German modifications, the Polish lost the ability to decipher messages even though they had correctly diagnosed the new changes made,

and reconstructed the new workings. In order to successfully confront these changes, the Poles would have needed to augment considerably (in fact, tenfold) their available materiel. For them, this was impossible.

On the 24th of July 1939 — one month before the beginning of the Second World War — the Poles revealed, during a meeting with French and British experts, their results. They gave to each of their astonished allies a copy of their German Enigma replica (complete with 5 rotors!), a detailed description of all decipherment methods, and schematics of all the devices they had developed to decipher the machine in which the Germans placed — and kept — complete confidence.

Until this date, the Poles had kept absolute secrecy even towards Bertrand who, from 1933 to 1939, continued to make numerous trips to Warsaw (compensated for by an equal number of trips of Langer to Paris) in order to transmit documents. This absence of reciprocity, this lack of *tit for tat*, should not surprise. Examples abound which show that relations between the *Services* are never free of hidden motives and that *an eye for an eye* is not always the rule. [3]

The Polish *gift* of 24 July 1939, which would have never been possible without the French aid received, was to play in its turn an essential role in the future British success.

B. THE CONSTRUCTION OF THE ENIGMA REPLICAS

Possession of only one copy of the Enigma machine was, even in 1933, not sufficient, and it was clear that in the future many more machines would be needed. Consequently, the Poles launched the industrial manufacture of Enigma replicas. This task was the responsibility of A. Palluth, one of the associate directors of the AVA company in Warsaw who specialized in the fabrication of radio equipment. He had been closely connected with the work of the *Biuro Szyfrow* and it was certainly he, following Rejewski's progress in reconstructing the schematics of the Enigma, who translated these schematics into actual pieces of equipment.

The AVA factory produced the first Enigma copies in 1934. In 1939, the Poles had 17 Enigmas of which two were given to the Allies (one to the French and one to the British). Taking into account the considerable number of Enigma *rotors* used in the mechanical devices invented by the Poles (*cyclometers* and *bombes*) to aid them in the tasks of decipherment, the number of Enigmas (or parts of Enigmas) produced by the factory between 1934 and 1939 was much greater (by at least 4 or 5 times) than one would think from the number existing in 1939.

C. THE POLISH SUCCESS (FROM 1933 TO THE END OF 1938)

To achieve mastery of the Enigma, the Polish aimed at numerous methods "from the simplest to the most complicated, from manual to mechanical, from the cheapest to the most costly." [4]

1. Manual methods

As has already been mentioned (c.f. Chapter III, Polish Work and the French Contribution), the methods used by the Poles consisted, essentially, of listing first characteristics from the first six letters of the encrypted part of the intercepted German messages — the portion corresponding to the encipherment of the *message key* (one group of three letters repeated twice). From these

groups, one could then determine the settings of the machine which were *compatible* with these characteristics and, if the number of messages were sufficient, these *compatible* settings could be reduced to a small enough number that could be *tested* on the Enigma replicas. The tests permitted one to determine *the* actual setting used for the day under consideration (the *daily key*) and, by another process, the specific key for each message. It *sufficed* then to read the messages using the Enigma replicas.

2. The First Mechanical Methods

In order to make their work easier and faster, the Poles invented an apparatus, the *cyclometer* [5] composed of elements (rotors) from two Enigma machines joined together. This instrument allowed one to setup mechanically a catalogue of *compatible settings*, at least as long as the Germans made use of a daily master *Grundstellung*. The cyclometer began service in 1937.

3. The First Enigma Modifications — 1937

From 1930 to 1937, The German military Enigma hardly changed.

Of course, the method of use evolved: increase in the frequency — ending in a daily alteration of all elements of the settings — increase in the number of *steckers* used. [6] This evolution was not of such a nature as to seriously impede the Polish work.

It was the 1st of November 1937 when the Germans brought to their machine the first important modification. The original reversing drum (*Umkehrwalze*) was replaced by a new one (*Umkehrwalze B*). The Polish reconstruction of the wirings of the new reversing drum was very rapid and decipherments continued as in the past.

The facility with which the Poles adapted to this change would seem to pose a problem. It is certain that, once having determined the nature of the modification (the change of the *Umkehrwalze*), the Poles (by their mathematical theory of the machine, by the permutation equations which resulted from this theory, and by their methods of solving these equations) found themselves perfectly well able to determine the wirings of the new drum. [7]

But how was it possible for the Poles to establish an exact *diagnosis*, that is, how could they find the exact nature of the unexpected change? The Polish answer to this question is apparently clear: the Germans, always strongly methodical, sent by Enigma to all users a text reminding them that, beginning a 00:00 hours on 1 November, they must mount in their machines — formerly called the *Wehrmacht Enigma*, the new reversing drum. [8] The Poles, thanks to their decipherments, were therefore forewarned and mastered the new machine as well as the old one.

In January 1938, a *test* of two weeks by the Polish Cipher Bureau, showed that 75% of the intercepted messages had been decrypted. [9]

4. Procedural Modifications from September 1938 and the Polish *Bombe*

The 15th of September 1938, the Germans abandoned the daily master *Grundstellung*, used until then, for the encipherment of the specific message key for *all* messages of that day. From now on, a particular *Grundstellung* for each message had to be randomly chosen by the operator (and indicated in the clear in the first part of the message).

Here again, the Poles were very quickly informed of the nature of the change, and, equally quickly, found the means of parrying it.

a. A new electro-mechanical machine, the *bomba* incorporating elements (rotors) of six Enigmas was invented. Six such bombes, each corresponding to one possible rotor order of the Enigma, were constructed. These bombes became operational in November 1938.

b. The mathematician H. Zygalski devised a manual system based on the utilization of a series of perforated sheets. Each perforation corresponded to one configuration of the machine compatible with one characteristic of a message key. The juxtaposition, on a light table, of a certain number of sheets corresponding to the characteristics of the keys made apparent the cases in which these characteristics were juxtaposed by permitting light from the table to shine through perforations in the pile of sheets. These perforations corresponded to *compatible settings*. Once the sheets were established (by an initially long process, necessitating complicated calculations and mathematical checks, but done only once), the selections could be rapidly made in *a few minutes*.

D. THE POLISH CHECK (DECEMBER 1938-JULY 1939)

On December 15, 1938, the Germans added to the first set of I, II, and III (which had six possible rotor orders) two more rotors, IV and V. The machine itself was not modified and always used only three rotors, but the number of possible rotor orders was increased from 6 to 60.

This time also, the Poles are said to have had immediate knowledge of the nature of the change: they had known for several months — from intelligence — that in case of extreme international tension, the German operators would receive two new rotors (already stockpiled!) baptized *mobilization rotors* (*Mobilisierungswalzen*), and that the simple ordering of the three existing rotors would become in this case a selection of three rotors out of five, followed by an ordering of the three rotors selected in the machine. Moreover, once again, the Poles are said to have intercepted the Enigma message giving the order to put the new procedure into practice.

The Poles were even able to reconstruct the wirings of the two new rotors thanks to the S.S. During September 1937, a new network of Enigma users appeared transmitting S.S. and *Sicherheitsdienst* messages. Before being enciphered on the Enigma, these messages were enciphered manually using a method that the Poles easily mastered. For some reason, after the 15th of December 1938, the S.S. and the Sicherheitsdienst used, like everyone else, the entire set of five rotors but kept the old keying procedure instead of the *Grundstellung* modification of September 15, 1938. Under these conditions, the experienced Polish mathematicians were able to reconstruct the internal wirings of rotors IV and V, and continued to read the Enigma messages of the S.S. and the Sicherheitsdienst (until July 1939).

On the other hand, the Enigma messages of the other networks had become unreadable to the Poles in spite of the reconstruction of the two new rotors. This occurred because of a *lack of technical resources* and not because of a lack of cryptanalytic mastery. It is easy to see why: in order to read the Enigma using a set of three rotors the Poles had *six Bombes*. The addition of two more rotors multiplied the number of rotor orders by a factor of $\underline{10}$ (i.e., from 6 to 60). In order to expand the number of Bombes (i.e., to build 54 additional Bombes), the Poles would have had to quickly produce $54 \cdot 6 = 324$ more sets of Enigma rotors (since each Bombe used six Enigma rotor sets). (The Poles had only 17 Enigmas in service.) This task largely surpassed the production capacity of the AVA factory. In spite of their intellectual

mastery, the Polish were circumvented by the lack of materiel. Also, the increase in the daily number of plugs (*Steckers*) used (beginning January 1, 1939) limited the effectiveness of the Polish Bombes.

Even if the lack of materiel could have been overcome, the Polish could not have hoped in so short a time to increase their cryptanalytic personnel for dealing with the work which had increased tenfold.

Zygalski's perforated sheets method suffered the same problems. The number of sheets required was also to be increased tenfold. The Poles put themselves to the task, but the magnitude of the necessary calculations made the process very slow, and only very partial results were obtained before the declaration of war.

It is Bletchley Park that, thanks to a prodigious concentration — both quantitative and qualitative — of staff and materiel, mastered the new problems. But the fact of having taken advantage of the Polish experience and having had access to the Polish work represented an enormous advantage for the English.

E. WAS THERE A FRENCH CONTRIBUTION TO THE POLISH SUCCESS OF 1933-38?

The French contribution to the Polish success of 1932 is universally recognized even if its real role may appear misestimated.

For the period 1933-38, there is no mention, either in Polish documents or other sources and available references, of a French contribution. Does this silence correspond to reality?

a. The Polish mathematicians, Rejewski, Rozycki, and Zygalski have always said that they had used no secret German documents other than the four used by Rejewski during the last trimester of 1932. There is every reason to believe them. But, this does not imply that their superiors, Langer and Ciezki, did not have possession of other documents which, while not indispensable to the mathematicians' work, which went along magnificently, permitted control of the quality of their results.

b. Bertrand states in his book that Asche delivered during the period 1931-34 a number of important documents relative to Enigma besides the basic ones, the *Gebrauchsanleitung* and the *Schlässelanleitung*. [10] It is practically certain that these documents were transmitted to the Poles.

c. Bertrand mentions (*Enigma*, p. 33) that in 1934 Asche left the *Chiffrierstelle*; the reader is then led to the conclusion that beginning at this date, Asche was no longer in a position to provide cryptologic information on the Enigma.

   The reality is quite different. Use of new — and irrefutable — documents allowed Colonel Paillole, in his book *Notre espion chez Hitler*, to show that Hans Thilo Schmidt alias Asche did not leave the *Chiffrierstelle* in 1934 but only his role there changed. Formerly, he was in charge of the liaison with the *Forschungsamt*, a department reporting to the Air Ministry (i.e., Marshall Goering) and one of the most important German cryptologic agencies. It was not until September 28, 1938 that Asche was administratively attached to the *Forschungsamt* (at an important level since he was director of the Templin station).

Up to this date, at least, he was marvelously placed to secure cryptologic documents and he made considerable use of this advantage.

Hans Thilo Schmidt had, in 1931-32, met six times with the agents of the French *Services*. Bertrand was present at four of these interviews (c.f., note 8, Chapter III and Appendix II of this work).

From 1933 to 1939, the records show 14 meetings between Asche and Bertrand (and there were other meetings at which Bertrand was not present). Each one of these encounters resulted in a transmission of documents.

d. Bertrand went to Poland three times during 1931-32 (c.f., Chapter III). From 1933 to 1939, there were 10 trips to Warsaw (and one to Czechoslovakia), [see Appendix II of this work].

   Langer went to Paris (on dates not precisely known) as many times as Bertrand went to Warsaw. Bertrand never went to Warsaw, and Langer never returned from Paris, empty-handed.

e. One part of the documents delivered by Asche between 1934 and 1940 contained general (but important) information on German armed forces and politics. These documents were *handled* by the German department of the French Services. But the mere fact that Bertrand (whose prerogative was limited to the cryptologic field) had continued to meet Asche between 1934 and 1938 shows unequivocally the duration of the deliveries of the cryptologic information. Bertrand himself gives some examples, not relative to Enigma.

   Colonel Paillole (op. cit.) is able to show that, during the course of this period, Asche continued to deliver Enigma documents and, in particular, a considerable number of monthly key setting schedules (see Appendix II of this work). At each interview, Asche furnished two of these schedules!

   These documents were surely transmitted to the Poles and, beginning in 1937-38, at least partly to the English.

f. It is therefore absolutely *certain* that Enigma documents continued to be transmitted after 1934. What were these documents and what role did they play?

   i. Appendix II gives a list (non-exhaustive) of the monthly key setting schedules furnished by Asche and their date of delivery.

      It seems certain that in the Polish case, no key setting schedules (apart from the two schedules which play a decisive role for Rejewski in the reconstruction of the machine) were ever delivered to the mathematicians who, by their own methods, determined the *daily keys*. Langer and Ciezki would have then used these documents to check on the work of the mathematicians. (Taking into account the *work rules* of a cryptologic service, this hypothesis is not unreasonable. [11])

      In the case of the British, this problem is studied in Chapter V.

ii. Aside from the transmission of the monthly key setting schedules, no explicit mention has been found as to whether or not Asche transmitted information about the procedural and technical modifications made by the Germans to their system between 1934 and 1938. These modifications, which have been detailed in Chapter II, are numerous. It cannot be excluded that such information had indeed been transmitted and would have been of the sort mentioned to the Poles. (The reasons that the Polish have given themselves to explain their knowledge could be *cover stories* — told in all good faith.)

g. There is a possible objection: if Enigma documents were transmitted after 1934, then the absence of mention of this fact, understandable in Polish reports and studies, in Bertrand's book is strange (to say the least).

This argument, while valuable, is not decisive. Bertrand wrote his book in 1973. He knew that from 1933 to 1939, the Poles whom he had pestered with questions about the course of their work had beat around the bush up until July 24, 1939. He could speak of what he had furnished from 1931 to 1934. Psychologically, it was perhaps difficult for him to admit that he had continued to go on helping the Poles for five years without receiving anything in exchange.

NOTES FOR CHAPTER IV

1. Enigma messages sent by the German Navy were decrypted only rarely. The lack of a sufficient number of intercepted messages is the reason.

2. The British seem to have begun study of the Enigma beginning in 1936. During the Spanish Civil War (beginning in 1937) the English deciphered German, Italian, and Spanish Nationalist messages enciphered on commercial models of the Enigma (slightly modified, but without the plugboard). In July 1939, at the moment of the Polish *gift*, the English had not yet reconstructed the German military Enigma.

3. Political factors can explain secrecy observed by the Poles. Political relations between Poland and France from 1933 to 1939 were far from always being excellent and information received from the Poles, partly due to their decryptments, made the Poles doubt the willingness of the French to aid Poland in case of attack, and also of the capacity of the French to keep secret the fact that the Enigma had been decrypted. As for the English, they gave their guarantee to Poland only March 31, 1939.

Besides, Bertrand was not a cryptologist and did not share the *fraternity* which joins specialists. It would not have been easy to explain to him the mathematical and technical complexities of the Polish decipherments.

4. T. Lisicki in *Die Funkaufklärung und ihre Rolle in 2. Weltkrieg*, p. 78.

5. So called because of peculiarities revealed in the encipherment of *message keys* leading to the determination of *cycles* of letters.

6. For this subject, see the part of Chapter II dedicated to setting changes.

7. Welchman (*The Hut Six Story*, p. 113-115) tells that following the interception of a message using a new *trial Umkehrwalze*, Bletchley Park reconstructed the wirings in a few hours (less than one night).

8. Source: interview with Colonel Lisicki.

9. Source: Memoranda of Colonel Mayer.

The percentages refer, without doubt, to messages sent by the Army and the Air Force. The alterations in machines and procedures used by the Navy rendered its messages practically inaccessible.

10. G. Bertrand — *Enigma*, p. 32

> "...the monthly key setting schedules (one key per day): Heeres-M., for December 1931, the years 1932, 1933 and 1934 (1st semester).
>
> ...10 documents concerning the Enigma cipher machine (1930), that became Enigma I in 1931 (when Enigma II was put into service) and, finally, Enigma *type Wehrmacht* (1937), when its use was extended to all of the Wehrmacht, among which two were of decisive value:
>
> ...a piece of information showing, for a given setting of the machine, the ciphered letters obtained by pressing each letter of the keyboard.
>
> ...a ciphertext, in several parts, with the corresponding cleartext and daily key used."

11. The following figures permit one to appreciate the importance that can be assigned to the delivery of the monthly Enigma key setting schedules. The combination of data furnished in the works of Bertrand and Paillole shows that, for the period extending from December 1931 to September 1938 inclusive (a total of 82 months), Hans Thilo Schmidt gave the French Intelligence Service 54 monthly schedules (at least!). Therefore, 66% of the settings of the Enigma used during this time interval were known.

The Poles received the greater part, if not all, of these schedules. In a letter sent to the author on January 15, 1986, Colonel Lisicki admitted the possible existence in the *Biuro Szyfrow* of a Section (whose existence would have been hidden from the Polish mathematicians) which decrypted the Enigma messages using the monthly key settings sent by Bertrand. For its work, such a section, which could not have begun operating until 1934 (the year of the first delivery of the Enigma copies by the AVA factory), would have been able to determine using the methods perfected by the mathematicians the particular key for each message.

BIOGRAPHICAL SKETCHES

Gilbert Bloch is retired and lives in Paris. He is member of the French Military Reserves. His hobbies include cryptology and parachute jumping.

C. A. Deavours teaches a unique sequence of courses in cryptology at Kean College of New Jersey. The courses address both technical and historical issues in cryptology.