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

ENIGMA BEFORE ULTRA POLISH WORK AND THE FRENCH CONTRIBUTION

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 POLISH WORK AND THE FRENCH CONTRIBUTION, Cryptologia, 11:3, 142-155

To link to this article: http://dx.doi.org/10.1080/0161-118791861947

ENIGMA BEFORE ULTRA
POLISH WORK AND
THE FRENCH CONTRIBUTION

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.

INTRODUCTION FROM THE TRANSLATOR

The Enigma story seems to be an unending series of revelations and corrections to previous revelations. It is then with genuine happiness that *Cryptologia* begins, in the current issue, to publish a series of chapters from the French work *Enigma Avant Ultra (Enigma Before Ultra).* The author of this work, M. Gilbert Bloch, has done a real service to those of us interested in this subject. Mr. Bloch has examined all of the publicly available documents and put together what is the most comprehensive documentation on the subject of Enigma which has yet to appear. He has been able, in many cases, to clarify and correct dates and to establish the sequence of events. Where there are discrepancies and mysteries remaining, this too has been pointed out for the reader's benefit. In particular, the crucial period between May and September 1940 has received the author's attention. It now seems likely that the explanation of how the British *got by* may yet prove more interesting than the story told by the late Gordon Welchman in his remarkable book, *The Hut Six Story.*

I am not a professional translator as will, no doubt, be evident. Although Mr. Bloch will examine every bit of material published before its appearance, the final guilt for any mistranslations or missed meanings is with me. In making the translation, I have tried to stay somewhere between the *just give me the facts* school of translation where the author's personality and style disappears and is replaced by that of the translator, and the *don't change a comma* school, which, in this case, would mean quarter of a page sentences with accompanying clauses and parenthetical remarks. As the old maxim goes "What is not clear is not French" — but, then again, it's not English either. *Au boulot!...*

Avis à Nos Lecteurs Francophones

Il y a disponible, en quantité strictemente limitée, des exemplaires de cette oeuvre en version originale. On peut en obtenir une copie (gratuite) du traducteur (ne pas la demander de l'auteur, svp).

CRYPTOLOGIA July 1987 Volume XI Number 3

PRESENTING "ENIGMA BEFORE ULTRA"

Books and articles on what could be called *The Enigma Saga* are many; it is even tempting to say, taking into account the irrelevance of part of these publications, *too many* ... The production of a new study and its partial reproduction (not contemplated initially!) in *Cryptologia* necessitate therefore some explanation, if not an excuse.

The fact that the author of this new study is a Frenchman (and consequently, the original text written in French) does not constitute a recommendation. Rather on the contrary ... French literature on Enigma has until recently been coarse and poor [1]. One could therefore expect that the main purpose of a French study would be the filling, in French knowledge, of gaps that do not exist anymore in Anglo-Saxon minds; but, on some important points, new documentation, explanations and interpretations are brought to light.

It is only fair, before listing the areas where the reader can expect to find new developments, to warn on the *limitations* of the study.

1. *Enigma before Ultra* (*Enigma avant Ultra*), as indicated by its title, embraces only the 1930-1940 period.
2. The study is not a technical one.
3. The extraordinary spying process through which the French obtained secret German documents is not examined in detail [2].

Turning now to the more positive aspects, *Enigma before Ultra* will, among other things, provide the reader with improved views in the following fields:

1. For the first time, a precise and comprehensive time-table of the events is given, particularly for the 1931-1933 period, where the real course had been until now difficult to retrace. The interrelations between France and Poland are shown and dated: a coherent picture emerges from this process.
2. The knowledge of the exact time-table of events shows clearly how the Polish mathematician M. Rejewski was able to organize his work during the 4 decisive ending months of 1932.
3. As could be expected from a French study, particular attention has been given to the French contribution to the Polish success. One could have feared at that stage a burst of French *chauvinisme*. This is not the case, and it is made perfectly clear that the French contribution was limited to obtaining secret German documents and transmitting them to the Poles, who receive full credit for their work. But, what is shown beyond any doubt is that
   a) The documents transmitted by the French *conditioned* the Polish success (and not only facilitated it, as it has till now been widely believed).
   b) Besides the four documents (explicitly identified, and with their dates of transmission duly indicated) that were put at Rejewski's disposal, the Poles received, from 1931 till the end of 1938, a lot of other Enigma documents. These were not transmitted to the Polish mathematicians by their superiors, but were used for monitoring the quality of their work, and perhaps warned the Poles of procedural changes.

4. Hypotheses liable to explain how the British re-entered the 22nd May 1940 Enigma Luftwaffe net (after having lost all their prior means of access with the dropping, the 1st May, of the duplication of the message key by the Germans) are examined in detail.

In such a field as the Enigma story, nothing will every be considered as *final*; but, on many aspects, the new study hopes to clarify things, and to allow future research to make further advances.

Cryptologia will not furnish a *complete* translation of *Enigma avant Ultra.* The introduction and the two first chapters (devoted respectively to the description of the Enigma machine, to a review of its procedures of use — and the evolution through time of these procedures) are omitted, as *Cryptologia* readers should be familiar with such aspects. Also omitted will be an Annex 1, devoted to the problem of Marine Enigma: more specialized studies on this subject already exist, and better ones are in preparation.

The introduction of *Enigma avant Ultra* includes acknowledgments that it would be unfair to omit. The author owes large debts of gratitude to Sir F. H. Hinsley (Cambridge), Colonel T. Lisicki (London), J. Garlinski (London), P. Calvocoressi (Bath), R. Erskine (Belfast), and on *the other side of the hill*, to Pr. J. Rohwer (Stuttgart). Enigma instructions have been obligingly furnished by the *Militärgeschichtliches Forschungsamt* (Freiburg in Breisgau) and other German archives.

The study would never have been written without the constant encouragement of Colonel P. Paillole.

NOTES

1. It must nevertheless be remembered that the book that started the unveiling of the Enigma mystery was published in France in 1973. *Enigma, ou la plus grande énigme de la guerre 1939-45* by General Gustave Bertrand (Plon ed.) was not the first publication on Enigma: a Polish book on the subject *Bitwa o tajemnice* (*Battle for Secrets*) was issued as early as 1967, under the signature of Colonel W. Kozaczuk, but went practically unnoticed... Without Bertrand's book, it seems doubtful that Group Captain F. W. Winterbotham would have been granted the authorisation to publish in 1974 *The Ultra Secret.* Bertrand's book, despite the crucial role played by the author in the first phase of the Enigma story, is unfortunately, both from the historical and technical points of view, not very satisfactory: it is furthermore marred by errors on dates (some of these errors are simply misprints!) that have prevented many historians (Garlinski and Stengers are notable exceptions!) to draw a correct time-table of the events. Winterbotham simply did not take notice of Bertrand's book, and what he wrote in his second chapter on *the Birth of Ultra* for the period 1930-39 was nonsensical.

2. These aspects of the story are fully covered in the recent book of Colonel Paillole, *Notre espion chez Hitler*, (Laffont ed. 1986.) An English translation is due to appear shortly.

CHAPTER III

POLISH WORK AND THE FRENCH CONTRIBUTION

A. THE POLES AND THE INTRODUCTION OF THE ENIGMA

The reconstituted Polish State of 1919, sandwiched between two equally hostile neighbors, thought cryptology could bring some factor of security to its precarious existence. The Polish cipher bureau, always very active, included excellent specialists. Initially, the decryption of the radio messages of the Reichwehr and Kriegsmarine was accomplished without great difficulty.

This favorable state of affairs was not to last. The naval messages became unreadable beginning in February 1926. The same thing occurred with the army traffic in July 1928.

The German ciphered messages, which were still being intercepted by listening stations, resisted all the established methods of cryptanalysis.

The Poles rapidly arrived at the conclusion that the German armed forces were using a new method of encipherment *by machine*. This presented the Poles with a triple problem, or rather, three problems whose solutions depended upon one another.

1. To determine the type of machine being used
2. To obtain or reconstruct the machine
3. To develop methods of decipherment.

The study of these problems fell, logically, in the *Services*, i.e., the Second Department of the General Staff of the Army at Warsaw.

This Army Department, as well as its directors, had undergone changes during the period under review. For our purposes, it is sufficient to note that the division charged with interception, radio intelligence, and cryptology directed until January 15, 1930 by Major Pokorny was led thereafter by Major (later Lieutenant Colonel) Gwido Langer. In the middle of 1931, this division became the *Biuro Szyfrow* (Cipher Bureau) which was in turn divided into sections covering each geographic zone. The most important of the sections was BS4 which was responsible for Germany. This section was placed under the direction of Captain (later Major) Maksymilian Ciezki.

From 1928, the work on the Enigma was confined to a team of three officers: Ciezki, Michalowski, and Czajsner.

B. DETERMINATION OF THE MACHINE TYPE

The attention of the Poles seems to have been drawn to the commercial Enigma machine and its possible use by the German Army during 1927-28. A curious story about the interception by customs officials at the railroad station in Warsaw of a package containing an Enigma and its subsequent examination over the weekend by Polish technicians is found, in several versions and with conflicting dates, in the works of Lewin, Garlinski, and Rejewski [1]. At the indicated dates, the machine examined could only have been a commercial model of the Enigma. Our interest in this incident is only to indicate at what time the Poles became interested in the Enigma. The result was a purchase (perfectly legal but done under a cover address) of an Enigma machine by the Poles.

It was logical for the Poles to believe that there was some connection between the commercial Enigma which they had just acquired and the new model of the machine used by the German Army. They began by checking, with the aid of their commercial model, whether or not the undecipherable messages *could have* been generated by a similar machine. The answer to this question was in the affirmative.

The Poles were not devoid of sources of information. Their intelligence service soon began investigations in Germany, and the Poles rapidly acquired confirmation that the machine introduced into the German armed forces was a modified Enigma (in fact, significantly modified with the introduction of the Type I model on June 1, 1930).

C. RECONSTRUCTION OF THE MACHINE

1. Differences Between the Commercial Enigma and the Military Model

The commercial Enigma was a machine having 3 movable rotors and a *reversing drum* but it did not have a *plugboard* (*steckerverbindung*).

The military Type I Enigma model of 1930 differed from the commercial model in 4 ways:

a. The three movable rotors had completely different wirings from those of the commercial machine;

b. The reversing drum (*Umkehrwalze*) was of a new type and not settable;

c. A plugboard with changeable connecting plugs (the steckers) was added to the machine;

d. The wiring connecting the keyboard to the entry/exit drum (via the plugboard) was different from the corresponding wiring on the commercial machine which connected the keyboard directly with the entry text drum.

2. 1928-1931. The Initial Deceptive Attempt.

The first task of the Polish team was to identify with precision the differences between the commercial Enigma and the military version. Up to the end of 1931, only slight progress was made in this direction.

It is certain that the Poles, who had at their disposal at least one copy of the commercial Enigma, received from their intelligence service some information about the military Enigma [2]. It was thus that the *Stöpstellstellung*, the early version of the *steckers* was identified and described. But, the information remained imprecise and fragmentary. At the end of 1931, the Poles were still very far from having a clear and precise notion of the general structure of the machine and, therefore, could not envision that they might ever be able to reconstruct the internal wirings. In fact, research on the machine was abandoned.

One all important point had, however, been noted. Systematic studies of the encrypted German messages had shown that the first 6 letters of these texts had some particular significance. Very probably, these first 6 letters formed some sort of *key*.

3. The French Contribution (1931-1932)

In October 1931 [3], an employee of the *Chiffrierstelle* of the *Reichswehrministerium* (Cipher Bureau of the German Ministry of Defense) [4] proposed to deliver documents to the agents of the French *Service de Renseignement*, (S.R.F.).

Since October 30, 1930, the S.R.F. included a *Service Crypto* (called *Section D*) whose role was to obtain information concerning foreign codes and ciphers. (Section D had no decrypting or analytic functions and was limited to transmitting any information gained to the experts of the *Service de Chiffre*). Captain (later General) Bertrand, head of the crypto service of the S.R.F. (and at this date about the only person in its service), was put in charge as *case officer* of individual contacts with new agents.

It was thus that Captain Bertrand received from *Asche* or H.E. (the pseudonyms of Hans Thilo Schmidt) [5], on the 8th of November 1931, the first set of secret documents of which the most important were:

a. *Gebrauchsanleitung für die Chiffriermaschine Enigma*
(Instructions for Using the Enigma Cryptograph). Document H.Dv. g 13 of the Army (H=Heer) and L.Dv g 13 of the Luftwaffe.

b. *Schlüsselanleitung zur Chiffriermaschine Enigma*
(Instructions for Ciphering on the Enigma Cryptograph). Document H.Dv g 14 of the Army and L.Dv g 14 of the Luftwaffe.

These two documents, in fact, the instructions given to machine operators, furnished a detailed description (with photos) and the operating instructions for the military Enigma I (Eins), put into service in 1930. Nevertheless, nothing about the internal wirings of the machine was included [6].

Bertrand transmitted his acquisitions to the S.C.F. which declared immediately that the Enigma was impossible to solve, the documents useless, and removed itself from further discussion of the question. This unfortunate state resulted, perhaps, from the character of Bertrand himself – a character which hardly facilitated relations with the other services.

Bertrand, to his credit, was not convinced by these peremptory affirmations, but he was practically alone and his limited cryptologic competence prevented him from personally attacking the problem. He then had the idea, and was able to obtain from his superiors the necessary authorization, to transmit the documents to the *services* of France's allies and to suggest to them a common attack on the problem.

London was contacted first: the Government Code and Cypher School – the modest name of the British cryptologic service, better known later under the name of *Bletchley Park* – received the documents, carefully filed them, and gave no follow up offer of cooperation [7].

From the 7th to the 11th of December 1931 [8] Bertrand himself visited Warsaw and recontacted Major Langer, the very competent head of the *Biuro Szyfrow*, who understood immediately that the documents furnished would allow resumption of the interrupted Enigma studies. Bertrand and Langer, provided with codenames *BOLEK* and *LUC* respectively, promised each other to share all information. This meant that in exchange for these documents (and those to follow), the Poles promised Bertrand to keep him informed of the results which they obtained.

Major Langer, Captain Ciezki, and his team renewed their work with enthusiasm. The documents brought by Bertrand indicated clearly the points where the military Enigma differed

from the commercial models: different wirings, the new type of reversing drum, addition of the plugboard and its plugs. The Poles also learned the frequency and procedures for changing the machine's settings as well as the significance of the first six ciphertext letters of each message. In other words, the Poles knew, from this time, that in each message the first and the fourth letters, the second and fifth letters, and the third and sixth letters resulted from the encipherment of the *same* cleartext letter.

Enthusiasm waned rapidly. All efforts to reconstruct the inner wirings of the machine failed: the magic mountain which had been opened by Bertrand's documents had ended in a blind alley – and this in spite of the receipt of new documents from *Asche*. The visits of Captain Bertrand to Warsaw on 9-11 May and 17-21 September 1932 [8], and, probably, other transmissions of documents through the Polish Services in Paris, placed in Major Langer's hands monthly schedules giving the daily settings of the Enigma. However, in the absence of a complete reconstruction of the machine (the difficulty of which has been discussed in Chapter II), all these documents were, apparently, useless.

4. Mathematicians to the Rescue

Being in despair, Langer and Ciezki decided to seek the intervention of other persons. For a long time, they had had the idea that the level of mathematical competence necessary for cryptanalysis surpassed that of the Army cryptologic personnel available and would require professional mathematicians. Beginning in 1929, they had organized a course of study in cryptology at the University of Poznan [9]. This course was taken by about 20 students already skilled in higher mathematics. The professors were officers in civil guise: Major Pokorny, then responsible for the interception service and cryptology (the predecessor of Langer), Captain Ciezki, future chief of the German section of the Cipher Bureau and a radio specialist, A. Palluth, employed as a high level technician by the Cipher Bureau.

Among the students, three distinguished themselves particularly: Marian Rejewski, Henryk Zygalski and Jerzy Rozycki. Rejewski, who had a degree in Mathematics (1st Class), spent the academic year 1929-30 at the University of Göttingen in Germany in order to pursue a special course of actuarial mathematics and returned in the summer of 1930 to take a post as assistant at the University of Poznan. At Poznan, he recontacted Rozycki and Zygalski who both worked several hours per day in an annex that the Cipher Bureau had set up in the town. They were occupied with the study of cryptologic problems related to the double transposition cipher. Rejewski rejoined his two fellow workers. The problem of Enigma was not considered.

At the beginning of 1932, the three mathematicians were warned of the impending closing of the annex. On the 1st of September 1932, they were officially *enlisted* into the Cipher Bureau at Warsaw. There, for more than a month, they studied the decryption of a German Naval code which they mastered. Suddenly, about the middle of October, Major Ciezki assigned Rejewski to work, alone and in great secrecy, on a new problem.

5. The Extraordinary Success of Mr. Rejewski (October 1932 - January 1933 [10])

What Major Ciezki had asked of Rejewski was to attempt the complete reconstruction of the German military Enigma. Rejewski was very young – born in 1905 he was then 27 years old – and had never even heard mention of the Enigma machine. But proving himself to be a worker of prodigious talent, he succeeded in *10 weeks* (from mid-October to the end of December

1932) in establishing a mathematical theory of the workings of the Enigma, in reconstructing the internal wirings, and in devising the first cryptanalytic methods to decipher the Enigma messages.

a. *The First Phase* (approximately October 15 - November 15, 1932).
Rejewski initially had at his disposal the following information and tools:

i. The two basic German documents on Enigma –
GebrauchsAnleitung and *Schlüsselanleitung* –
obtained from Asche and brought by Bertrand on December 7, 1931;

ii. A brand new model of the commercial Enigma;

iii. The continuous flow of German ciphertext messages captured by the Polish interception stations.

The two Asche documents allowed Rejewski to become rapidly familiar with the structure of the machine and the procedures used to operate it.

In studying the implications of the *repetition of the message key* – the first six letters – Rejewski realized that in 81% of the cases (21 out of 26) the typing of the six letters on the machine's keyboard caused only a movement of the righthand rotor. The rest of the machine could then be considered as a single fixed ensemble. Moreover, the first and the fourth letters, the second and the fifth letters, and the third and the sixth letters each corresponded to the same cleartext letter.

Rejewski then deduced the mathematical consequences implied by his two observations. Namely, that it was possible to express the encipherment of these six letters by equations representing the six successive permutations involved. Further, if given a sufficient number of messages from the same day (which would therefore use the same settings of the machine), one could draw out certain characteristics of the permutations of that day. The system of six equations was therefore *theoretically* capable of a solution which would, in turn, yield the wiring of the rightmost rotor.

Since the Germans changed the order of the rotors periodically, each of the three movable rotors would, from time to time, find itself placed on the extreme right. This allowed the three rotor wirings to eventually be reconstructed. In a similar manner, the reversing drum (Umkehrwalze) wirings could also be found.

The method which had just been described was *theoretically* applicable even if the machine settings (order of rotors, *Ringstellung*, *Grundstellung*, and plugboard setting) were completely unknown. Nevertheless, in this case, carrying out the *actual* calculations involved was practically impossible because no powerful calculating devices such as today's computers were available. Theoretically, one could dream of a solution but it implied use of a very large number of messages and a succession of luck too extraordinary to be believable [12].

Once again, the work seemingly landed in a blind alley.

b. *The Second Phase* (approximately November 15 - December 31, 1932).

In October, Major Ciezki had only furnished Rejewski with the two basic documents on Enigma. No doubt he wished to determine the ability of the young mathematician to use them. Experience having decided the question (beyond all possible expectations) Ciezki gave Rejewski, probably around November 15, two new documents also acquired from Asche, and

transmitted by Bertrand. These documents were two monthly schedules giving the daily settings for the Enigma. Rejewski had at his disposal the ciphertexts of the messages intercepted during these two months. He knew from the latest documents the order of the rotors, the setting of the rings, the rotor starting positions (for enciphering the message key), and the plugboard connections. All this information allowed Rejewski to simplify his equations enough to solve them. By luck, the two months covered in the schedules fell in different trimesters of the year [13]. Because the rotor order was altered each trimester, two different rotors occupied the rightmost position. The solution of the wiring of these two rotors allowed the solution of the wiring of the third rotor. With this done, the wirings of the reversing drum (*Umkehrwalze*) could be determined without difficulty.

Rejewski immediately threw himself into his calculations. Initially, no valid results were obtained. In seeking the cause for this failure, Rejewski had the idea that his assumption about the wiring from the plugboard to the entry/exit drum had been wrong. In the commercial Enigma, the wiring was *straight through* from the keyboard to the 26 contacts of the entry/exit drum. This placed the wires in the same order as the letters on the keyboard of the standard German typewriter: the letter Q connected to contact 1, W to contact 2, E to contact 3, etc.

Rejewski had thought initially that the military Enigma was wired similarly. The keys being wired according to a straight alphabetic correspondence (key A joined to plugboard connection A, B to B, etc.) and the plugboard letters joined in the order of the entry keyboard letters with the contacts of the entry/exit drum.

Rejewski told himself that if the order had been modified, the methodical Germans would not have changed to a random wiring. He then tried the wiring where the letters were arranged in regular alphabetic order (A connected to the first contact, B to the second, C to the third, etc.). This inspiration was correct and, as if by a miracle, the internal wirings began to emerge from his calculations.

By the end of 1932, the combination of mathematical genius displayed by Rejewski and the trove of secret Asche documents sent to the Poles by Bertrand, as well as a good dose of luck (Rejewski's *intuition* concerning the entry wiring), had led to the complete reconstruction of the German military Enigma.

This reconstruction was not only carried out *on paper*. An eminent technician, the engineer Antoni Palluth, one of the directors of the AVA radio equipment fabrication factory in Vasovie and also a consultant for the Cipher Bureau had, following Rejewski's progress, modified a commercial Enigma into the military model of the machine. This perfectly operational prototype served first to verify Rejewski's results. Second, this machine was used as an industrial prototype for the AVA manufacture of replicas of the military Enigma destined for the Polish cryptologic services.

D. THE FIRST METHODS OF DECIPHERMENT

The knowledge that the first six letters of each message was the twice enciphered key to that specific message furnished Rejewski with the means of reconstructing the internal wirings of the Enigma. It also led to his decipherment of the messages coming from the machine.

A detailed description of the decrypting methods developed by Rejewski while at the same time reconstructing the Enigma machine will not be attempted here. Suffice it to say that these methods allowed, from some characteristics of the 6 letter groups corresponding to the twice

repeated enciphered *message keys, one to determine* the settings of the machine *compatible* with these characteristics, to test these settings and finally to find out the exact message key used. After this had been done, the decipherment could be carried out under the same conditions as the German clerks to whom the messages were addressed had. In other words, using the same machine settings, each message could be deciphered by typing the ciphertext on the keyboard of the machine.

During his work in establishing the first methods of decipherment, Rejewski could exploit certain errors committed by the German operators. In particular, the use of particular groupings of letters such as AAA, BBB, SSS, etc. as message keys. The use of such letter groups was forbidden to the operators at the end of 1932, which was, of course, too late.

From the beginning of 1933, the decipherment methods perfected by Rejewski showed themselves to be entirely adequate.

The Polish success was complete.

E. THE ROLE AND IMPORTANCE OF THE FRENCH CONTRIBUTION

The Poles and *only* the Poles attempted the reconstruction and cryptanalysis of the German military Enigma. Alone, they carried out the totality of intellectual, cryptologic, and mathematical investments necessary. And they alone arrived at the solution. Chapter IV will show that they were the only ones, between 1933 and the beginning of 1939, to retain mastery over the Enigma and its decipherment. For these extraordinary exploits, the Poles must receive all of the credit and retain all of the glory.

It does not diminish the value of their accomplishment to recall that there was a French contribution and to try to evaluate its importance.

The French contribution to the Polish success was *both* mediocre and fundamental:

a. *Mediocre*, because that contribution was limited to the transmission by Bertrand of the documents obtained from Asche;

b. *Fundamental*, because the documents supplied by Bertrand played a decisive role. The writings of Rejewski and a careful study of the timetable of events leads to the following inescapable conclusions: the first two documents, *Gebrauchsanleitung* and *Schlüsselanleitung*, constituted the indispensable base upon which Rejewski's genius built his reasoning and equations; the two monthly schedules of daily machine settings allowed the theory thus established to be actually carried out. Without these four documents, success could not have been attained.

It would not be necessary to emphasize the role of the French contribution had that role been correctly described and appreciated in the available documentation. But, if the existence of a French contribution is acknowledged at all, most works on the Enigma appear to agree that the documents furnished by the French intelligence service merely *facilitated* the tasks of the Polish mathematicians and, that, in their absence, the same result would have been obtained with only an additional delay. These affirmations do not correspond to reality. The documents furnished by Bertrand not only *facilitated* the Polish success – they made it possible. One may consider that the methodical and obstinate efforts of the Poles have a *value* superior to the *stroke of luck* which was offered to the S.R.F by Hans Thilo Schmidt. But, without the Asche documents furnished to the Poles, it is nearly certain that the Enigma would have kept its secrets a lot longer [14].

There remains a secondary problem to discuss in regard to the French contribution. At first glance, this problem may appear quite strange. Rejewski has stated publicly, and there is every reason to believe him, that he only received four secret German documents (the two basic ones and the two monthly sets of machine settings). Bertrand has indicated that, thanks to Asche, a very large number of documents (notably, the monthly machine setting schedules from December 1931 to December 1932) were obtained, and it would seem implicit that this bulk of information was immediately repeated to the Poles, i.e., Langer and Ciezki. (However, there do not exist accompanying letters or memoranda explicitly proving that this transmission took place.)

Could this situation be explained by the fact that Rejewski was only allowed to see a fraction of the material received by his superiors? On second thought, such a situation would not appear surprising. The *need to know* principle is the rule in intelligence work. Rejewski, a completely new employee of the *Biuro Szyfrow*, had proved his worth when confronted with two documents (*GebrauchsAnleitung* and *Schlüsselanleitung*) which were, in turn, followed by two other documents (the two monthly schedules of machine settings). Those documents were sufficient to lead to the success of his enterprise and there was no cause to reveal the existence of the other *papers* (which were no longer indispensable to his work but would serve to verify it). Finally, it is worth noting that, up to 1939, Rejewski ignored that the base of his work had been furnished by the S.R.F. Only Langer and Ciezki knew of the liaison with Bertrand.

NOTES FOR CHAPTER III

1. R. Lewin – *Ultra Goes To War*. See note on page 30, paperback edition. J. Garlinski – *Intercept*: p 2-3. M. Rejewski – *How the Polish Mathematicians Broke Enigma* – English translation of an article which appeared in 1980 (posthumously) in a Polish mathematical magazine; this translation is to be found in the appendix of the book *Enigma*, by W. Kozaczuk, p. 246.

2. T. Lisicki *Die Funkaufklärung und Ihre Rolle im zweiten Weltkrieg*, p. 67.

3. And not 1932 as indicated by Bertrand (*Enigma*, 23). The mixture of dates in Bertrand's book which sometimes place the events of 1931 in 1932 did not help the Enigma historians. The chronology now established beyond any doubt.

Most historians of Enigma (excluding Garlinski and Stengers) have been deceived by the date 1932 which has, in turn, led to inextricable difficulties in reconstructing the correct timetable of events. A more serious fact is that Rejewski himself in his last articles also adopted the date 1932. Existing documents including accounts by Bertrand himself leave no doubt as to the actual date.

4. The *Chiffrierstelle* was not the only German service dealing with cryptology. E. Höttenhain in *Die Funkaufklärung und ihre Rolle im zweiten Weltkrieg*, p. 100 citation 8, shows clearly the waste and disorder resulting from the lack of coordination.

5. The extraordinary story of Hans Thilo Schmidt, whose importance extends beyond Enigma material, is recorded by Paul Paillole in his work *Notre espion chez Hitler*, Editions Laffont, 1985.

6. The wartime destruction in the Polish, French, and German archives was such that no copy of the original 1930 documents exists any longer in continental Europe. The only place where, perhaps, these documents might still be found is in the archives of the British

Government Code and Cypher School (GC&CS), which received copies of them from Bertrand in 1931. These archives are inaccessible.

The original 1930 documents did not carry the reference "L" indicating *Luftwaffe* since this organization did not exist officially until 1935. The documents Dv. g 13 and 14 were the object of numerous editions which incorporated the successive modifications of the Enigma machine and its method of use. These modifications do not seem, at least before May 1940, to have changed any essential aspect or spirit of the documents. Thanks to the amiability of the *Militärgeschichtliches Forschungsamt* (the historical service of the German Army located in Freibourg in Brisgau), the author of this study possesses copies of the following:

a. The *Gebrauchsanleitung* of January 12, 1937 (the edition is of January 1940 but specifies that the text is unchanged); this is a document of 16 pages of which 11 are text and the remaining are photographs of the machine pointing out its different parts.

b. The *Schlüsselanleitung* of January 13, 1940. 14 pages.

7. Cf. Hinsley, *British Intelligence in the Second World War*, Vol. 1, p.488. Bertrand did not go to London on this occasion. The documents were given to the representative of the I.S. in Paris, Commander Wilfred Dunderdale, who carried them to England. (He left on the 23rd of November for England. Source: P. Paillole, *Notre espion chez Hitler*, p. 39).

8. The dates of Bertrand's visits to Warsaw must be connected with those of the Asche meetings, each of which resulted in the transmission of documents. In 1931 and 1932, Bertrand met Asche four times

- November 7-8 1931 at Verviers
- December 19-20 1931 at Verviers
- May 7-8 1932 at Verviers
- October 29-30 at Liège.

Besides this, REX (aka Lemoine), the intermediary of the S.R.F., met Asche in Berlin August 1-2, 1932 and received from him documents which arrived in Paris August 10 by diplomatic pouch.

9. The University of Poznan was excellent. All of the students there spoke both Polish *and* German.

10. Rejewski's complete and detailed explanation of the mathematical theory of the Enigma, the corresponding system of permutations and their solution is beyond the scope of this study. The interested reader can consult the writings of Rejewski himself, writings from (1984) are now available in English. These writings consist of appendices D and E from the book *Enigma*, by W. Kozaczuk. Appendix B of the same book, a liberal transcription of an interview with Rejewski recorded July 24, 1978, furnishes an extraordinarily vivid illustration of Rejewski's career and work.

Another work of Rejewski cited (with numerous extracts) but not furnished *in extenso* in the work of Kozaczuk must be quoted. This article has been, fortunately, fully translated and published in English in *Cryptologia*, 6, No. 1, Jan. 1982, pp. 75-83. The *Remarks on Appendix 1 to "British Intelligence in the Second World War"* consists of Rejewski's comments of the text published in Volume I of Hinsley and furnishes precise corrections.

11. And it appears that the computer time required may, even today, be prohibitive.

12. Cf. Rejewski – *How the Polish Mathematicians Broke Enigma.* Appendix D of the book *Enigma*, W. Kozaczuk, p.258. Rejewski explicitly indicates that, without further information, it was impossible to solve the permutation equations.

13. The fact that the two monthly schedules belonged to different trimesters is perfectly clear. By contrast, the months covered by the two schedules and the date and circumstances of their possession by the Poles present several problems whose elements are given below:

a. Bertrand (*Enigma*, p. 32) indicates having received from Asche (and then transmitted to the Poles) *les tableau mensuels de configurations (comportant une configuration par jour) pour Décembre 1931, les années 1932, 1933, et 1934 (1er semestre).*

b. Rejewski states in his works, and there is every reason to believe him, that only *two* monthly schedules of machine settings were put at his disposition covering two months belonging to different trimesters. However, he has varied the dates. In his last article (posthumous, 1980) he indicates the months of September and October 1932 which appear not only plausible but probable (see below). But, he has also indicated that these documents were put at his disposal December 9, 1932 (cf. Kozaczuk p.256). This date, apparently based on the erroneous date (December 7, 1932 instead of December 7, 1931) of the first visit of Bertrand to Warsaw, is evidently false. It would have left Rejewski only three weeks to finish all of his calculations before December 31.

In the first paper that Rejewski wrote, in France during 1942 under conditions hardly favorable to composing memoirs, he quotes the months of October and December 1931 – a double impossibility. Bertrand has said that he did not have any table of keys at his disposal until December 1931. The months of October and December belong to the same trimester. (It is strange that, even in the conditions of 1942, Rejewski had forgotten a technical detail of such importance.)

c. The date of the Asche meetings, i.e., the dates of Bertrand's visits to Warsaw, do not allow one to settle, *a priori*, this question.

The monthly schedules could have only been transmitted by Asche during his meetings with Bertrand (or, in one case, with another agent of the S.R.F., Lemoine). These meetings took place November 7-8 and December 19-20 in 1931 and May 7-8 and October 29-30 in 1932. The meeting with Lemoine was on August 1-2, 1932.

Bertrand visited Warsaw from the 7th to the 11th of December 1931, from the 9th to the 11th of May, and from the 17th to the 21st of September 1932. (All of the preceding dates were furnished to the author by Colonel Paillole.)

Assuming, logically, but, as will appear, wrongly, that the monthly schedules of keys were not available in Germany until a few days before the first of the month in which they were to be used, one is led to think that the schedules for September-October 1932 could have been furnished by Asche only during the meeting of October 29-30. This would be too late to have been provided by Bertrand to Warsaw at the time of his visit of September 17-21, 1932. There would nevertheless remain other possibilities: the schedules in question could have been transmitted to Langer by an intermediary representative of the Polish *services* in Paris (the contacts here were constant). It would be equally possible that Langer himself came to Paris at the beginning of November 1932 to take delivery of these documents. Whatever hypothesis is adopted, the schedules provided by Asche to Bertrand during October 29-30 could have found themselves in Warsaw about November 15 without difficulty. This fits perfectly into the timetable of events.

The book of P. Paillole, *Notre espion chez Hitler* (p.53), provides the solution to the prob-

lem. The monthly schedules for September and October 1932 (the October schedule in provisional form) were provided by Asche to Lemoine in Berlin at the beginning of August 1932. This is early enough to have been given to the Poles by Bertrand at the time of his stay in Warsaw, September 17-21.

The date (approximate) of November 15, 1932 when Rejewski received the two monthly schedules of keys suggests they referred to the months September and October 1932. It was logical to furnish Rejewski with the *latest* schedules available since these schedules would correspond to the most recent ciphertexts intercepted by the Polish listening stations and Rejewski already had these ciphertexts.

14. The relative misestimation of the French contribution is understandable. The only French work concerning Enigma was that of Bertrand, published in 1973. This work had the distinction of being the first one to describe what had happened. But, the style of this book, the understandable tendency for the author to discuss more his personal role in the events rather than to provide a complete, clear and technical documentation of the facts, arouses suspicion. Historians can not be blamed for having preferred to utilize two short reports (unpublished but easily accessible) drawn up by Colonel Mayer in London during 1974 in response to the books of Bertrand and Winterbotham. Colonel Mayer was the former head of the Polish Intelligence Services. Mayer has written, "At the stage in which the research of the *Enigma* was at that time in the Polish cryptological section, these documents [those sent by Bertrand] appeared not to be indispensable for the final solution of the problem. But, unquestionably, they facilitated it." In writing this sentence Colonel Mayer was certainly sincere, but, even if he had closely supervised the work of Langer, Ciezki, and Rejewski, this supervision would not entail familiarity with the difficulties encountered, the methods used, nor the solutions found.

The works of Rejewski, partially in English, have been available only a little while. Their interpretation is sometimes made difficult by the fact that Rejewski had ended up being persuaded that the first visit of Bertrand to Warsaw was on December 7, 1932 instead of *1931*.

Of course, recourse to the original documents is impossible since the French and Polish archives were destroyed or lost during the war.

The book of P. Paillole, *Notre espion chez Hitler*, published in September 1985 describes in detail the extraordinary role played by Hans Thilo Schmidt, alias Asche, and, finally, permits one to appreciate exactly the magnitude of the Asche documents and their importance to the Poles.

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.