The Origins of the Enigma

Dr. Władysław Kozaczuk

September 1996

The inter-allied intelligence operation Enigma — wrote a prominent American historian of cryptography — was "the greatest secret of World War II after the atom bomb" (1) The breaking of the sophisticated German machine cipher was the most spectacular event, in terms of difficulty and far-reaching consequences, in the entire history of cryptography. Operation Enigma was one of powerful weapons of the anti-Nazi war coalition but in contrast of to the atomic energy, which itself had come to light in the terrific holocaust of Hiroshima and Nagasaki in August 1945, the secrets of the Enigma remained hidden and unknown to the public for almost three decades. Its details have been emerging only fragment by fragment from the darkness in which the governments concerned have felt it was better to keep them.

However, the lid of the mysterious Enigma-"box" was first lifted a bit by the present writer as early as 1967. In my book "Struggle for Secrets: Intelligence Services of Poland and the Third Reich 1992–1939" (2) the reader may find documented evidence that the German Enigma had already been solved in Poland in the inter-war period. The book was duly reviewed in a Göttingen scholarly monthly, (3) and in 1970 Heinz Bonatz, formerly head of the navy radio intelligence, in his reminiscence book questioned whether the Poles had in fact broken Enigma. (4)

Three years later, in his "Enigma: the Greatest Puzzle of the War 1939-1945" (5), France's General Gustave Bertrand supplied ample corroboration for the Polish claims and highlighted the French contribution: the provision to the Poles of valuable intelligence collected in Germany through an agent of their Deuxieme Bureau. Meanwhile, Bertrand's book, which ascribes "all the credit and all the glory" for breaking the German machine cipher to the Poles, was totally ignored by the British. But also there, in Great Britain, time had been growing ripe for disclosure.

It finally appeared in 1974, in a book, "The Ultra Secret", written by F.W. Winterbotham (6), a former RAF intelligence officer. But this book virtually begins at the point where Enigma was already broken, and continues with accounts of the dissemination, use, and impact of the Enigma-derived intelligence on the Allies' conduct of the war. It gives a fairly true if, at times, blurred picture of the gigantic "intelligence factory," with its central station at Bletchley, some 70 km north of London. There,

intercepted German and other Axis cipher messages were turned into plain language, translated, re-edited to conceal their source, and then sent to decision-makers, ranging from Winston Churchill and his chiefs of staff to various military commands in Europe and all over the world.

The most serious flaw of the book is a complete elimination from the Enigma picture of what was the prerequisite to its very existence: the mastering by Polish mathematicians of the German secret machine cipher, and passing of the results of this work, along with the Polish-made replicas of the machine (the Enigma-"double") to the French and the British during a tripartite conference in Warsaw as early as in July, 1939. The "Winterbotham story", long since discarded, had it that British Intelligence Service, sometime in 1938, contacted a Polish worker who was employed in a German factory making Enigma machines, and persuaded him to build a big wooden model of the machine. They gave the Poles the necessary money, and the Polish Intelligence "acquired" the machine, by means not specified. Then, in the utmost secrecy, "the complete, new, electrically operated Enigma" was brought back to London. The British set to work, invented a device called the "Bronze Goddess" and were able to read German Enigma ciphers.

The point that Winterbothams's book is completely unreliable as regards the true origins of the Enigma/Ultra would scarcely need to be labored further were not for the fact that the contagion has spread. The circulation of false coin was difficult to prevent, and it was to re-appear many a time.

But also in Great Britain, laudable attempts have been made to make a just and unbiased assessment of Enigma's origins and its influence upon the military operations of 1939 to 1945, as for instance in R. Lewin's "Ultra Goes to War" (1978) (7). A title- page dedication in Lewin's book reads: "To the Poles who sowed the seed and to those who reaped the harvest". Much in the same line of approach was the book of P. Calvocoressi "Top Secret Ultra" (1980) which centers on the organization of Bletchley with its over 9000 cryptologists, intelligence analysts, signal and security officers, technicians, and WREN clerks; and Ralph Bennett's "Ultra in the West: the Normandy Campaign, 1944,45" (1980). However, an unpleasant set-back was the 1st Volume of the official "British Intelligence in the Second World War: Its Influence on Strategy and Operations" (1979), which clearly downgraded the Polish and French contributions, misquoting G. Bertrand's book etc. To be sure, the authors have revised some of their false opinions in Volume 3 (2), which appeared in 1988. (8)

The earliest Polish work on the intercepted German machine ciphers had begun already in 1928, right after the system's introduction by the German Army. However, no progress was made during the next four years. Then the Polish Cipher Bureau — which was part of 2nd Section (Military Intelligence) of the General Staff — decided to recruit three young mathematicians, all of them graduates of the Mathematical Institute at the University in Poznań. To be sure they were first all given, along with twenty-odd their fellow-students, a rudimentary training in codebreaking during a special course, organized by the military. Their real aim was to find cryptological talents, the most promising of which was considered Marian Rejewski. After his graduation, he went for a

one-year period of advanced study in actuarial mathematics to Göttingen and following his return, thought at the Mathematical Institute in Poznań.

On September 1, 1932, Rejewski and his two somewhat younger colleagues, Jerzy Różycki, and Henryk Żygalski began work as regular employees at the Cipher Bureau in Warsaw. During the first few weeks, the young mathematicians worked on relatively simpler German Navy codes. At that time the Kriegsmarine was particularly active on Polish shore, as the German government tried to curtail the Polish rights, stipulated by the Versailles Treaty, in then — Free City of Danzig. In early October 1932, Rejewski was given a separate room and told to take a closer look at a pile of Enigma-research. He was also supplied with an obsolete commercial Enigma machine, of the initial type, which had been bought in Germany. It, however, lacking many essential components of the military-type machine, especially the commutator ("plug board"), and was quite useless. Polish penetration into the secrets of the Enigma — remarks an American cipher expert and historian — began in earnest when Rejewski realized the applicability of some properties of permutations to his analysis of the German machine cipher. (10)

The whole complicated process of mastering the secrets of the German Enigma, that was ultimately achieved in the first days of January, 1933, involved a combination of mathematics, statistics, computational ability and inspired guesswork. An erroneous view has been reiterated in various publications that the breaking of Enigma was a one-time feat. In fact, it involved two distinct matters:

First, the theoretical reconstruction of the cipher device itself. The most important matter was determining Enigma's electric wiring, then the intricate interdependence between different components of the machine: the exchangeable rotors, the so called entry ring, the commutator etc. This knowledge enabled the Poles to build doubles of Enigma that made it possible to read German enciphered radio communication.

Second, the elaboration of methods for recovering the Enigma keys (starting positions) exclusively on the basis of intercepts.

Success could not have been more timely. Just under way in Germany just then was the Nazi campaign that on 30 January 1933 would deliver power into Hitler's hand.

The only British book dealing with cryptological nuts and bolt of the Enigma/Ultra, "The Hut Six Story: Breaking the Enigma Codes," written by Gordon Welshman (9) — a Cambridge mathematician who, along with Alan Turing, was one of the leading lights at Bletchley — could not be published in Great Britain because it was banned by the Official Secrets Act. It eventually appeared, with considerable delay, in USA (Welshman became an American citizen after the war), and is the only publication by a former Bletchley codebreaker who pursues the way of Enigma research already paved by Marian Rejwski. His first comprehensive report on how the Enigma system was broken, including full mathematical proof, Rejewski had completed in 1942 in southern France while working in the clandestine French-Polish center ("Cadix") (10) and its first printed version appeared as Appendix to my book "W kręgu Enigmy" (The Enigma Circle) in 1979. Anyway, in his "The Hut Six Story" Welshman unequivocally states that the

British Ultra "would never have gotten off the ground if we had not learned from the Poles, in the nick of time, the details both of the German military Enigma machine, and of the operating procedures that were in use." (11)

Welshman's appreciative words find also a strong corroboration in a comment, written by an American cryptology expert to Rejewski's article, which in 1981 appeared in USA in the "Annals of the History of Computing" (Volume 3, n.3, July 1981) and reads as follows: "No doubt practitioners of group theory should introduce this property of permutations (which had been applied by Rejewski — W.K.) to students as"the theorem that won World War II". Of course, actually solving the Enigma traffic via statistical analysis, table look-up or mechanical computation (the Poles used all these methods) was an immense undertaking — one that no other county was up to at the time. While Rejewski and his compatriots were cracking Enigma traffic on a ongoing basis, the only cryptanalytic technique available to the British was a method known as "cliques on the rods" to the British or the "baton" method to the French.

Although the opinions or assessments of historical facts and developments made by politicians and statesmen may occasionally be subject to political considerations, they no doubt do reflect the well-balanced and generally accepted views, based on expert investigations. "Before Poland fell — said George Bush while addressing his huge audience in Gdańsk in August 1989, on the eve of the 50th anniversary of the outbreak of World War II — you gave the Allies Enigma the Nazi's secret coding machine. Breaking the unbreakable Axis code saves tens of thousand Allied lives, American lives; and for this, you have the enduring gratitude of the American people. And ultimately, Enigma and freedom fighters played a major role in the winning the Second World War". (12)

Historians will, no doubt, long debate exactly what was the influence upon the course of the Second World War of the Allies' ability to read German machine ciphers. Verdicts will range between a significant speeding up of the ultimate outcome, with the saving of untold thousands of lives, and what some of the highest Allied commanders termed a decisive impact on the results of many campaigns, battles and operations.

NOTES

1. D. Kahn, "Enigma Unwrapped". New York Time Book Review, 29.XII.74
2. W. Kozaczuk, "Bitwa o tajemnice. Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939", Warsaw 1967. A fourth ed. 1977
3. Ostliteratur - Anzeiger, Hrsg. vom Göttinger Arbeitskreis, Holzner Verlag, Wűrzburg, Jahrgang XIII, Heft 3, 3.VI.1967
4. H. Bonatz, "Die deutsche Marine — Funkaufklärung 1914–1945", Darmstadt, 1970
5. G. Bertrand, "Enigma ou la plus grande enigme de la guerre 1939-1945, Paris, 1973
6. F. Winterbotham, "The Ultra Secret", London, 1974
7. R. Lewin, "Ultra Goes to War", London, 1978

8. F.H. Hinsley et al., “British Intelligence in the Second World War: Its Influence on Strategy and Operations”, London, Her Majesty’s Stationary Office, 1, 1979 to 4, 1988
9. G. Welshman, “The Hut Six Story: Breaking the Enigma Codes”, New York 1982
10. Report of Cryptological Work on the German Machine Cipher, Manuscript written in Uzes, France, 1942
11. G. Welshman, ibid
12. “Presidential Documents”, Volume 25 - Number 29, Washington, July 24, 1989

References

- W. Kozaczuk, “Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two”, University Publications of America, 1984; Arms and Armour Press, London, 1984.
- “Geheimoperation Wicher. Polnische Mathematiker knacken den deutschen Funkschlüssel Enigma”, Bernard und Graefe, Koblenz 1989.

This account was originally posted on the server of Poland’s Ministry of Foreign Affairs (http://www.msz.gov.pl/english/iv/past/origins.html)

Transcribed and edited by Frode Weierud, Crypto Cellar Research, January 2025.

Editorial note: The exact date of this document is unknown. The date September 1996 is the date given on the Website https://calculemus.org/aera/kp-uw/96-02/02enig.html that has the article from the publication *Kurier Polityczny*, Nr 2, 30.09.1996. It is therefore likely that September 1996 refers to the date *Kurier Polityczny* published the article and not when it was originally written and posted on the Website of Poland’s Ministry of Foreign Affairs. We only know that is is from the period 1990–1996.

Kurier Polityczny gives the following introduction to Dr. Władysław Kozaczuk’s article: **ENIGMA Operation: the intellectual contribution of Poles to winning the war.**

Looking at September 1939 as the beginning of the road to victory, we remember the scale of the sacrifices and suffering. But since they are given the due respect, and since the contribution of blood in victorious battles is remembered, it is time to recall the intellectual contribution to winning the war: the merits of Polish intelligence and scientists in breaking the German army code; this was a fact with far-reaching consequences for the war. Described concisely in English by Dr. Władysław Kozaczuk, an outstanding expert on the subject, this story also mentions Polish cooperation in the field of cryptography with Alan Turing — the English pioneer of the computer.