= Biuro Szyfrów =

The Biuro Szyfrów ([?b?ur? ???fruf] , Polish for " Cipher Bureau ") was the interwar Polish General Staff 's Second Department 's organizational unit charged with SIGINT and both cryptography (the use of ciphers and codes) and cryptanalysis (the study of ciphers and codes , particularly for the purpose of " breaking " them) .

The precursor of the agency that would become the Cipher Bureau was created in May 1919 , during the Polish @-@ Soviet War (1919 ? 21) , and played a vital role in securing Poland 's survival in that war .

In mid @-@ 1931 , the Cipher Bureau was formed by the merger of pre @-@ existing agencies . In December 1932 , the Bureau began breaking Germany 's Enigma ciphers . Over the next seven years , Polish cryptologists overcame the growing structural and operating complexities of the plugboard @-@ equipped Enigma . The Bureau also broke Soviet cryptography .

Five weeks before the outbreak of World War II , on 25 July 1939 , in Warsaw , the Polish Cipher Bureau revealed its Enigma @-@ decryption techniques and equipment to representatives of French and British military intelligence , which had been unable to make any headway against Enigma . This Polish intelligence @-@ and @-@ technology transfer would give the Allies an unprecedented advantage (Ultra) in their ultimately victorious prosecution of World War II .

= = Precursor = =

On 8 May 1919 , a Polish Army " Cipher Section " (Sekcja Szyfrów) , precursor to the " Cipher Bureau " (Biuro Szyfrów) , was created by Lt. Józef Serafin Stanslicki . The Cipher Section reported to the Polish General Staff and contributed substantially to Poland 's defense by Józef Pi?sudski 's forces during the Polish @-@ Soviet War of 1919 ? 21 , thereby helping preserve Poland 's independence , recently regained in the wake of World War I. The Cipher Section 's purview included both ciphers and codes . In loose Polish parlance , the term " cipher " (" szyfr ") refers to both these two principal categories of cryptography . (The opposite is the practice in English , which loosely refers to both codes and ciphers as " codes . ")

During the Polish ? Soviet War (1919 ? 1921) , some one hundred Russian ciphers were broken by a sizable cadre of Polish cryptologists who included army Lieutenant Jan Kowalewski and three world @-@ famous professors of mathematics ? Stefan Mazurkiewicz , Wac?aw Sierpi?ski and Stanis?aw Le?niewski . Russian army staffs were still following the same disastrously ill @-@ disciplined signals @-@ security procedures as had Tsarist army staffs during World War I , to the decisive advantage of their German enemy . As a result , during the Polish @-@ Soviet War the Polish military were regularly kept informed by Russian signals stations about the movements of Russian armies and their intentions and operational orders .

The Russian staffs , according to Polish Colonel Mieczys?aw ?cie?y?ski , " had not the slightest hesitation about sending any and all messages of an operational nature by means of radiotelegraphy ; there were periods during the war when , for purposes of operational communications and for purposes of command by higher staffs , no other means of communication whatever were used , messages being transmitted either entirely (" in clear , " or plaintext) or encrypted by means of such an incredibly uncomplicated system that for our trained specialists reading the messages was child 's play . The same held for the chitchat of personnel at radiotelegraphic stations , where discipline was disastrously lax . "

In the crucial month of August 1920 alone , Polish cryptologists decrypted 410 signals : from Soviet General Mikhail Tukhachevsky , commander of the northern front ; from Leon Trotsky , Soviet commissar of war ; from commanders of armies , e.g. the commander of the IV Army , Sergieyev ; the commander of the Horse Army , Semyon Budionny ; the commander of the 3 Cavalry Corps , Gaya ; from the staffs of the XII , XV and XVI Armies ; from the staffs of the Mozyr Group (named after the Belarusian city) ; the Zolochiv Group (after the Ukrainian town) ; the Yakir Group [after General Iona Emmanuilovich Yakir] ; from the 2 , 4 , 7 , 10 , 11 , 12 , 16 , 17 , 18 , 24 , 27 , 41 , 44 , 45 , 53 , 54 , 58 and 60 Infantry Divisions ; from the 8 Cavalry Division , etc .

The intercepts were as a rule decrypted the same day , or at latest the next day , and were immediately sent to the Polish General Staff 's Section II (Intelligence) and operational section . The more important signals were read in their entirety by the Chief of the General Staff , and even by the Commander in Chief , Marshal Józef Pi?sudski . Interception and reading of the signals provided Polish intelligence with entire Russian operational orders . The Poles were able to follow the whole operation of Budionny 's Horse Army in the second half of August 1920 with incredible precision , just by monitoring his radiotelegraphic correspondence with Tukhachevsky , including the famous and historic conflict between the two Russian commanders .

The intercepts even included an order from Trotsky to the revolutionary council of war of the Western Front , confirming Tukhachevsky 's operational orders , thus giving them the authority of the supreme chief of the Soviet armed forces . An entire operational order from Tukhachevsky to Budionny was intercepted on 19 August and read on 20 August , stating the tasks of all of Tukhachevsky 's armies , of which only the essence had previously been known .

?cie?y?ski surmises that the Soviets must likewise have intercepted Polish operational signals ; but he doubts that this would have availed them much since Polish cryptography " stood abreast of modern cryptography " and since only a small number of Polish higher headquarters were equipped with radio stations , of which there was a great shortage ; and finally , Polish headquarters were more cautious than the Russians and almost every Polish division had the use of a land line .

Polish cryptologists enjoyed generous support under the command of Col. Tadeusz Schaetzel , chief of the Polish General Staff 's Section II (Intelligence) . They worked at Warsaw 's radio station WAR , one of two Polish long @-@ range radio transmitters at the time . The Polish cryptologists ' work led , among many other things , to discovery of a large gap on the Red Army 's left flank , which enabled Poland 's Marshal Józef Pi?sudski to drive a war @-@ winning wedge into that gap during the August 1920 Battle of Warsaw .

The discovery of the Cipher Bureau 's archives , decades after the Polish @-@ Soviet War , has borne out ?cie?y?ski 's assertion

that ... radio intelligence ... furnished [the Polish Commander @-@ in @-@ Chief , Józef Pi?sudski] , in the years 1919 ? 1920 ... the most complete and ... current intelligence on all aspects of the functioning of the Red Army , especially of units operating on the anti @-@ Polish front , that it was radio intelligence that to a large degree determined the course of all ... military operations conducted by Poland in 1920 ? from the January fighting at Ovruch , through the March operation against Mozyr and Kiev , the April operation in Ukraine , the battles with Tukhachevsky 's first and second offensives in Belarus , the battles with Budionny 's Cavalry Army , the Battle of Brody , to the Battles of Warsaw , Lwów and the Niemen .

= = Cipher Bureau = =

In mid @-@ 1931 , at the Polish General Staff , a Cipher Bureau was formed by merging the Radio @-@ Intelligence Office (Referat Radiowywiadu) and the Polish @-@ Cryptography Office (Referat Szyfrów W?asnych) . The Bureau was charged with both cryptography ? the generation , and supervision of the use , of ciphers and codes ? and cryptology , the study of ciphers and codes , particularly for the purpose of " breaking " them .

Between 1932 and 1936 , the Cipher Bureau took on additional responsibilities , including radio communications between military @-@ intelligence posts in Poland and abroad , as well as radio counterintelligence ? mobile direction @-@ finding and intercept stations for the locating and traffic @-@ analysis of spy and fifth @-@ column transmitters operating in Poland .

= = Stalking Enigma = =

In late 1927 or early 1928 , there arrived at the Warsaw Customs Office from Germany a package that , according to the accompanying declaration , was supposed to contain radio equipment . The German firm 's representative strenuously demanded that the package be returned to Germany even before going through customs , as it had been shipped with other equipment by mistake . His

insistent demands alerted the customs officials , who notified the Polish General Staff 's Cipher Bureau , which took a keen interest in new developments in radio technology . And since it happened to be a Saturday afternoon , the Bureau 's experts had ample time to look into the matter . They carefully opened the box and found that it did not , in fact , contain radio equipment but a cipher machine . They examined the machine minutely , then put it back into the box .

The Bureau 's leading Enigma cryptanalyst Marian Rejewski commented that the cipher machine may be surmised to have been a commercial @-@ model Enigma , since at that time the military model had not yet been devised . " Hence this trivial episode was of no practical importance , though it does fix the date at which the Cipher Bureau 's interest in the Enigma machine began " ? manifested , initially , in the entirely legal acquisition of a single commercial @-@ model Enigma .

On 15 July 1928 the first German machine @-@ enciphered messages were broadcast by German military radio stations . Polish monitoring stations began intercepting them , and cryptologists in the Polish Cipher Bureau 's German section were instructed to try to read them . The effort was fruitless , however , and was eventually abandoned . There remained very slight evidence of the effort , in the form of a few densely written @-@ over sheets of paper and the commercial @-@ model Enigma machine . On 15 January 1929 Major Gwido Langer , after a tour of duty as chief of staff of the 1st Legion Infantry Division , became chief of the Radio @-@ Intelligence Office , and subsequently of the Cipher Bureau . The Bureau 's deputy chief , and the chief of its German section (BS @-@ 4) , was Captain Maksymilian Ci??ki .

In 1929 , while the Cipher Bureau 's predecessor agency was still headed by Major Franciszek Pokorny (a relative of the outstanding World War I Austro @-@ Hungarian Army cryptologist , Captain Herman Pokorny) , Ci??ki , Franciszek Pokorny and a civilian Bureau employee , Antoni Palluth , taught a secret cryptology course at Pozna? University for selected mathematics students . Over ten years later , during World War II while in France , one of the students , Marian Rejewski , would discover that the entire course had been taught from French General Marcel Givièrge 's book , Cours de cryptographie (Course of Cryptography) , published in 1925 .

In September 1932 , Maksymilian Ci??ki hired three young graduates of the Pozna? course to be Bureau staff members : Marian Rejewski , Jerzy Ró?ycki and Henryk Zygalski .

= = Successes and setbacks = =

In 1926 the German Navy adopted , as its top cryptographic device , a modified civilian Enigma machine ; in 1928 the German Army followed suit . The complexity of the system was much increased in 1930 by the introduction of a plugboard (Steckerbrett) , albeit with only six connecting leads in use . In December 1932 , Marian Rejewski made what historian David Kahn describes as one of the greatest advances in cryptologic history , by applying pure mathematics ? the theory of permutations and groups ? to breaking the German armed forces ' Enigma machine ciphers . Rejewski had worked out the precise interconnections of the Enigma rotors and reflector , after the Bureau had received , from French Military Intelligence Captain Gustave Bertrand , two German documents and two pages of Enigma daily keys (for September and October of that year) . These had been obtained by a French military intelligence agent , a German codenamed Rex , from an agent who worked at Germany 's Cipher Office in Berlin , Hans @-@ Thilo Schmidt , whom the French codenamed Asché .

After Rejewski had worked out the military Enigma 's logical structure , the Polish Cipher Bureau commissioned the AVA Radio Company , co @-@ owned by Antoni Palluth , to build replicas (" doubles ") of the Enigma to Rejewski 's specifications . His method of decrypting Enigma messages exploited two weaknesses of the German operating procedures . It used what Rejewski called " characteristics " that were independent of the plugboard connections . This involved compiling a card catalog of certain features of the set of indicator settings .

The Germans increased the difficulty of decrypting Enigma messages by decreasing the interval between changes in the order of the rotors from quarterly , initially , to monthly in February 1936 , then daily in October of that year , when they also increased the number of plugboard leads from six to a number that varied between five and eight . This made the Biuro 's grill method much less easy

, as it relied on unsteckered letter pairs . The German navy was more security @-@ conscious than the army and air force , and in May 1937 it introduced a new , much more secure , indicator procedure that remained unbroken for several years .

The next setback occurred in November 1937 , when the scrambler 's reflector was changed to one with different interconnections (known as Umkehrwalze @-@ B) . Rejewski worked out the wiring in the new reflector , but the catalog of characteristics had to be compiled anew , again using Rejewski 's " cyclometer " , which had been built to his specifications by the AVA Radio Company .

In January 1938 , Colonel Stefan Mayer directed that statistics be compiled for a two @-@ week period , comparing the numbers of Enigma messages solved , to Enigma intercepts . The ratio came to 75 percent . " Nor , " Marian Rejewski has commented , " were those 75 percent ... the limit of our possibilities . With slightly augmented personnel , we might have attained about 90 percent ... read . But a certain amount of cipher material ... due to faulty transmission or ... reception , or to various other causes , always remains unread ... " Information obtained from Enigma decryption seems to have been directed from B.S.-4 principally to the German Office of the General Staff 's Section II (Intelligence) . There , from fall 1935 to mid @-@ April 1939 , it was worked up by Major Jan Le?niak , who in April 1939 would turn the German Office over to another officer and himself form a Situation Office intended for wartime service . He would head the Situation Office to and through the September 1939 Campaign .

The system of pre @-@ defining the indicator setting for the day for all Enigma operators on a given network , on which the method of characteristics depended , was changed on 15 September 1938 . The one exception to this was the network used by the Sicherheitsdienst (SD) ? the intelligence agency of the SS and the Nazi Party ? who did not make the change until 1 July 1939 . Operators now chose their own indicator setting . However , the insecure procedure of sending the enciphered message key twice , remained in use , and it was quickly exploited . Henryk Zygalski devised a manual method that used 26 perforated sheets , and Marian Rejewski commissioned the AVA company to produce the bomba kryptologiczna (cryptologic bomb) .

Both the Zygalski @-@ sheet method and each bomba worked for only a single scrambler rotor order , so six sets of Zygalski sheets and six bomby were produced . However , the Germans introduced two new rotors on 15 December 1938 , giving a choice of three out of five to assemble in the machines on a given day . This increased the number of possible rotor orders from 6 to 60 . The Biuro could then only read the small minority of messages that used neither of the two new rotors . They did not have the resources to produce 54 more bomby or 54 sets of Zygalski sheets . Fortunately , however , the fact that the SD network was still using the old method of the same indicator setting for all messages , allowed Rejewski to re @-@ use his previous method of working out the wiring within these rotors . This information was essential for the production of a full set Zygalski sheets which allowed resumption of large @-@ scale decryption in January 1940 . On 1 January 1939 , the Germans made military Enigma even more difficult to break by increasing the number of plugboard connections from between five and eight , to between seven and ten .

When World War II broke out on 1 September 1939 , Le?niak and his colleagues had been working intensively for two or three years to establish the German order of battle and had succeeded in working out nearly 95 percent of it . The German attack on Poland came as no surprise to the Polish General Staff . The results that had been obtained by Polish intelligence , according to Le?niak , " absolutely exceeded what would normally have been possible . "

= = Kabaty Woods = =

Until 1937 the Cipher Bureau 's German section , BS @-@ 4 , had been housed in the Polish General Staff building ? the stately 18th @-@ century " Saxon Palace " ? in Warsaw . That year BS @-@ 4 moved into specially constructed new facilities in the Kabaty Woods near Pyry , south of Warsaw . There , working conditions were incomparably better than in the cramped quarters at the General Staff building .

The move was dictated as well by requirements of security . Germany 's Abwehr was always looking for potential traitors among the military and civilian workers at the General Staff building .

Strolling agents , even if lacking access to the Staff building , could observe personnel entering and leaving , and photograph them with concealed miniature cameras . Annual Abwehr intelligence assignments for German agents in Warsaw placed a priority on securing informants at the Polish General Staff .

= = Gift to allies = =

It was at Pyry , on 25 and 26 July 1939 with war looming that , on instructions from the Polish General Staff , the Cipher Bureau 's chiefs , Lt. Col. Gwido Langer and Major Maksymilian Ci??ki , the three civilian mathematician @-@ cryptologists , and Col. Stefan Mayer , chief of intelligence , revealed Poland 's achievements to cryptanalytical representatives of France and Britain , explaining how they had broken Enigma . They undertook to give each country a Polish @-@ reconstructed Enigma , along with details of their equipment , including Zygalski sheets and Rejewski 's cryptologic bomb . In return , the British pledged to prepare two full sets of Zygalski sheets for all 60 possible wheel orders . The French contingent consisted of Major Gustave Bertrand , the French radio @-@ intelligence and cryptology chief , and Capt. Henri Braquenié of the French Air Force staff . The British sent Commander Alastair Denniston , head of Britain 's Government Code and Cypher School , Dilly Knox , chief British cryptanalyst and Commander Humphrey Sandwith , head of the Royal Navy 's intercept and direction @-@ finding stations .

When Rejewski had been working on reconstructing the German military Enigma machine in late 1932 , he had ultimately solved a crucial element , the wiring of the letters of the alphabet into the entry drum , with the inspired guess that they might be wired in simple alphabetical order . Now , at the trilateral meeting ? Rejewski was later to recount ? " the first question that ... Dillwyn Knox asked was : ' What are the connections in the entry drum ? ' " Knox was mortified to learn how simple the answer was .

The Poles ' gift , to their western Allies , of Enigma decryption , five weeks before the outbreak of World War II , came not a moment too soon . Former Bletchley Park mathematician @-@ cryptologist Gordon Welchman has written : " 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 . " Allied Supreme Commander Dwight D. Eisenhower , at war 's end , described intelligence from Bletchley Park as having been " of priceless value to me . It has simplified my task as a commander enormously . " Eisenhower expressed his thanks for this " decisive contribution to the Allied war effort . "

Churchill 's greatest wartime fear , even after Hitler had suspended Operation Sea Lion and invaded the Soviet Union , was that the German submarine wolfpacks would succeed in strangling sea @-@ locked Britain . A major factor that averted Britain 's defeat in the Battle of the Atlantic was her regained mastery of Naval Enigma decryption ; and while the latter benefited crucially from British seizure of German Enigma @-@ equipped naval vessels , the breaking of German naval signals ultimately relied on techniques that had been pioneered by the Polish Cipher Bureau . Had Britain capitulated to Hitler , the United States would have been deprived of an essential forward base for its subsequent involvement in the European and North African theaters .

A week after the Pyry meeting , Dillwyn Knox , in a letter dated 1 August 1939 , thanked the Poles , in Polish , " for your cooperation and patience . " He enclosed little paper batons and a scarf picturing a Derby horse race ? evidently emblematic of the cryptological race that Knox had hoped to win using the batons , and whose loss he was gallantly acknowledging .

On 5 September 1939 , as it became clear that Poland was unlikely to halt the ongoing German invasion , BS @-@ 4 received orders to destroy part of its files and evacuate essential personnel .

= = Bureau abroad = =

During the German Invasion of Poland in September 1939 , key Cipher Bureau personnel were evacuated southeast and ? after the Soviets invaded eastern Poland on 17 September ? into Romania , on the way destroying their cryptological equipment and documentation . Eventually ,

crossing Yugoslavia and still @-@ neutral Italy , they reached France . Some personnel of the Cipher Bureau 's German section who had worked with Enigma , and most of the workers at the AVA Radio Company that had built Enigma doubles and cryptologic equipment for the German section , remained in Poland . Some were interrogated by the Gestapo , but no one gave away the secret of Polish mastery of Enigma decryption . At PC Bruno , outside Paris , on 20 October 1939 the Poles resumed work on German Enigma ciphers in close collaboration with Britain 's Government Code and Cypher School at Bletchley Park .

In the interest of security , the allied cryptological services , before sending their messages over a teleprinter line , encrypted them using Enigma doubles . Henri Braquenié often closed messages with an ironic " Heil Hitler ! "

As late as December 1939 , when Lt. Col. Gwido Langer , accompanied by Captain Braquenié , visited London and Bletchley Park , the British asked that the Polish cryptologists be turned over to them . Langer , however , took the position that the Polish team must remain where the Polish Armed Forces were being formed ? on French soil . The mathematicians might actually have reached Britain much earlier ? and much more comfortably ? than they eventually did ; but in September 1939 , when they went to the British embassy in Bucharest , Romania , they were brushed off by a preoccupied British diplomat .

In January 1940 , the British cryptanalyst Alan Turing spent several days at PC Bruno conferring with his Polish colleagues . He had brought the Poles a full set of Zygalski sheets that had been produced at Bletchley Park by John Jeffreys using Polish @-@ supplied information . On 17 January 1940 , the Poles made the first break into wartime Enigma traffic ? that from 28 October 1939 .

During this period , until the collapse of France in June 1940 , ultimately 83 percent of the Enigma keys that were found , were solved at Bletchley Park , the remaining 17 percent at PC Bruno . Rejewski commented :

How could it be otherwise , when there were three of us [Polish cryptologists] and [there were] at least several hundred British cryptologists , since about 10 @,@ 000 people worked in Bletchley ... Besides , recovery of keys also depended on the amount of intercepted cipher material , and that amount was far greater on the British side than on the French side . Finally , in France (by contrast with the work in Poland) we ourselves not only sought for the daily keys , but after finding the key also read the messages .... One can only be surprised that the Poles had as many as 17 percent of the keys to their credit .

The inter @-@ Allied cryptologic collaboration prevented duplication of effort and facilitated discoveries . Before fighting had started in Norway in April 1940 , the Polish @-@ French team solved an uncommonly hard three @-@ letter code used by the Germans to communicate with fighter and bomber squadrons and for exchange of meteorological data between aircraft and land . The code had first appeared in December 1939 , but the Polish cryptologists had been too preoccupied with Enigma to give the code much attention . With the German assault on the west impending , however , the breaking of the Luftwaffe code took on mounting urgency . The trail of the elusive code (whose system of letters changed every 24 hours) led back to Enigma . The first clue came from the British , who had noticed that the code 's letters did not change randomly . If A changed to P , then elsewhere P was replaced by A. The British made no further headway , but the Poles realized that what was manifesting was Enigma 's exclusivity principle that they had discovered in 1932 . The Germans ' carelessness meant that now the Poles , having after midnight solved Enigma 's daily setting , could with no further effort also read the Luftwaffe signals .

The Germans , just before opening their 10 May 1940 offensive in the west that would trample Belgium , Luxembourg and the Netherlands in order to reach the borders of France , once again changed their procedure for enciphering message keys , rendering the Zygalski sheets " completely useless " and temporarily defeating the joint British @-@ Polish cryptologic attacks on Enigma . According to Gustave Bertrand , " It took superhuman day @-@ and @-@ night effort to overcome this new difficulty : on May 20 , decryption resumed . "

Following the capitulation of France in June 1940 , the Poles were evacuated to Algeria . On October 1 , 1940 , they resumed work at " Cadix " , near Uzès in unoccupied southern , Vichy

France , under the sponsorship of Gustave Bertrand .

A little over two years later , on 8 November 1942 , Bertrand learned from the BBC that the Allies had landed in French North Africa (" Operation Torch ") . Knowing that in such an eventuality the Germans planned to occupy Vichy France , on 9 November he evacuated Cadix . Two days later , on 11 November , the Germans indeed marched into southern France . On the morning of 12 November they occupied Cadix .

Over the two years since its establishment in October 1940 , Cadix had decrypted thousands of Wehrmacht , SS and Gestapo messages , originating not only from French territory but from across Europe , which provided invaluable intelligence to Allied commands and resistance movements . Cadix had also decrypted thousands of Soviet messages .

Having departed Cadix , the Polish personnel evaded the occupying Italian security police and German Gestapo and sought to escape France via Spain . Jerzy Ró?ycki , Jan Grali?ski and Piotr Smole?ski had died in the January 1942 sinking , in the Mediterranean Sea , of a French passenger ship , the Lamoricière , in which they had been returning to southern France from a tour of duty in Algeria .

Marian Rejewski and Henryk Zygalski hiked over the Pyrenees with a guide (who robbed them at gunpoint) to the Spanish border , where they were arrested on January 30 , 1943 . They were incarcerated by the Spaniards for three months before being released , upon Red Cross intervention , on 4 May 1943 . They then managed , by a circuitous land ? sea ? air route , to join the Polish Armed Forces in Britain , Rejewski and Zygalski were inducted into the Polish Army as privates (they would eventually be promoted to lieutenant) and put to work breaking German SS and SD hand ciphers at a Polish signals facility in Boxmoor . Because of their having been in occupied France , the British considered it too risky to invite them to work at Bletchley Park .

Finally , with the end of the two mathematicians ' cryptologic work at the close of World War II , the Cipher Bureau ceased to exist . From nearly its inception in 1931 until war 's end in 1945 , the Bureau , sometimes incorporated into aggregates under cryptonyms (PC Bruno and Cadix) , had been essentially the same agency , with most of the same core personnel , carrying out much the same tasks ; now it was extinguished . Neither Rejewski nor Zygalski would work again as cryptologists . In late 1946 Rejewski returned to his family in a devastated and politically altered Poland , to live there another 33 years until his death in February 1980 . Zygalski would remain in England until his death in August 1978 .

= = Secret preserved = =

Despite their travails , Rejewski and Zygalski had fared better than some of their colleagues . Cadix 's Polish military chiefs , Langer and Ci??ki , had also been captured ? by the Germans , as they tried to escape from France into Spain on the night of March 10 ? 11 , 1943 ? along with three other Poles : Antoni Palluth , Edward Fokczy?ski and Kazimierz Gaca . The first two became prisoners of war ; the other three were sent as slave labourers to Germany , where Palluth and Fokczy?ski perished . Despite the varyingly dire circumstances in which they were held , none of them ? Stefan Mayer emphasizes ? betrayed the secret of Enigma 's decryption , thus making it possible for the Allies to continue exploiting this vital intelligence resource .

Before the war , Palluth , a lecturer in the 1929 secret Pozna? University cryptology course , had been co @-@ owner of AVA , which produced equipment for the Cipher Bureau , and knew many details of the decryption technology . In Warsaw , under German occupation , other Cipher Bureau workers were interrogated by German intelligence commissions , and some AVA workers were approached by German agents , but all kept silent about compromises to Enigma .

= = In popular culture = =

In 1967 the Polish military historian W?adys?aw Kozaczuk , in his book Bitwa o tajemnice (The Battle for Secrets) , first revealed that the German Enigma had been broken by Polish cryptologists before World War II . Kozaczuk 's disclosure came seven years before F.W. Winterbotham 's The

Ultra Secret (1974) changed conventional views of the history of the war .

The 1979 Polish film Sekret Enigmy (The Enigma Secret) is a generally fair , if superficial , account of the Cipher Bureau 's story . Twenty @-@ two years later , the 2001 Hollywood film Enigma was criticized for its many historical inaccuracies , including omission of Poland 's fundamental work in Enigma decryption .