= Marian Rejewski =

Marian Adam Rejewski [?marjan re?jefski] (16 August 1905 ? 13 February 1980) was a Polish mathematician and cryptologist who reconstructed the Nazi German military Enigma cipher machine sight @-@ unseen in 1932 . The cryptologic achievements of Rejewski and colleagues Jerzy Ró?ycki and Henryk Zygalski enabled the British to begin reading German Enigma @-@ encrypted messages at the start of World War II , seven years after Rejewski 's original reconstruction of the machine . The intelligence that was gained by the British from Enigma decrypts formed part of what was code @-@ named Ultra and contributed ? perhaps decisively ? to the defeat of Germany .

In 1929 , while studying mathematics at Pozna? University , Rejewski attended a secret cryptology course conducted by the Polish General Staff 's Cipher Bureau (Biuro Szyfrów) , which he joined in September 1932 . The Bureau had had no success in reading Enigma @-@ enciphered messages and set Rejewski to work on the problem in late 1932 ; he deduced the machine 's secret internal wiring after only a few weeks . Rejewski and his two colleagues then developed successive techniques for the regular decryption of Enigma messages . His contributions included the cryptologic card catalog , derived using the cyclometer that he had invented , and the cryptologic bomb .

Five weeks before the German invasion of Poland in 1939 , Rejewski and colleagues presented their achievements to French and British intelligence representatives summoned to Warsaw . Shortly after the outbreak of war , the Polish cryptologists were evacuated to France , where they continued breaking Enigma @-@ enciphered messages . They and their support staff were again compelled to evacuate after the fall of France in June 1940 , and they resumed work undercover a few months later in Vichy France . After the French " Free Zone " was occupied by Germany in November 1942 , Rejewski and Zygalski fled via Spain , Portugal , and Gibraltar to Britain . There they enlisted in the Polish Armed Forces and were put to work solving low @-@ grade German ciphers .

After the war , Rejewski reunited with his family in Poland and worked as an accountant . For two decades , he remained silent about his prewar and wartime cryptologic work to avoid adverse attention from the country 's Soviet @-@ dominated government ; he broke his silence in 1967 when he provided to the Polish Military Historical Institute his memoirs of his work in the Cipher Bureau . He died at age 74 of a heart attack and was interred with military honors at Warsaw 's Pow?zki Military Cemetery .

= = Early life = =

Marian Rejewski was born 16 August 1905 in Bromberg in the Prussian Province of Posen (now Bydgoszcz , Poland) to Józef and Matylda , née Thoms . After completing secondary school , he studied mathematics at Pozna? University 's Mathematics Institute , housed in Pozna? Castle .

In 1929 , shortly before graduating from university , Rejewski began attending a secret cryptology course which opened on 15 January , organized for select German @-@ speaking mathematics students by the Polish General Staff 's Cipher Bureau with the help of the Mathematics Institute 's Professor Zdzis?aw Krygowski . The course was conducted off @-@ campus at a military facility and , as Rejewski would discover in France in 1939 , " was entirely and literally based " on French General Marcel Givièrge 's 1925 book , Cours de cryptographie (Cryptography Course) . Rejewski and fellow students Henryk Zygalski and Jerzy Ró?ycki were among the few who could keep up with the course while balancing the demands of their normal studies .

On 1 March 1929 Rejewski graduated with a Master of Philosophy degree in mathematics . A few weeks after graduating , and without having completed the Cipher Bureau 's cryptology course , he began the first year of a two @-@ year actuarial statistics course at Göttingen , Germany . He did not complete the statistics course , because while home for the summer of 1930 , he accepted an offer , from Professor Krygowski , of a mathematics teaching assistantship at Pozna? University . He also began working part @-@ time for the Cipher Bureau , which by then had set up an outpost at Pozna? to decrypt intercepted German radio messages . Rejewski worked some twelve hours a

week near the Mathematics Institute in an underground vault referred to puckishly as the " Black Chamber " .

The Pozna? branch of the Cipher Bureau was disbanded in the summer of 1932 . On 1 September 1932 , Rejewski , Zygalski , and Ró?ycki joined the Cipher Bureau as civilian employees working at the General Staff building (the Saxon Palace) in Warsaw . Their first assignment was to solve a four @-@ letter code used by the Kriegsmarine (German Navy) . Progress was initially slow , but sped up after a test exchange ? consisting of a six @-@ group signal , followed by a four @-@ group response ? was intercepted . The cryptologists guessed correctly that the first signal was the question , " When was Frederick the Great born ? " followed by the response , " 1712 . "

On 20 June 1934 Rejewski married Irena Maria Lewandowska , daughter of a prosperous dentist . The couple eventually had two children : a son , Andrzej (Andrew) , born in 1936 ; and a daughter , Janina (Joan) , born in 1939 . Janina would later become a mathematician like her father .

= = Enigma machine = =

The Enigma machine was an electromechanical device , equipped with a 26 @-@ letter keyboard and 26 lamps , corresponding to the letters of the alphabet . Inside was a set of wired drums (rotors and a reflector) that scrambled the input . The machine used a plugboard to swap pairs of letters , and the encipherment varied from one key press to the next . For two operators to communicate , both Enigma machines had to be set up in the same way . The large number of possibilities for setting the rotors and the plugboard combined to form an astronomical number of configurations , and the settings were changed daily , so the machine code had to be " broken " anew each day .

Before 1932 , the Cipher Bureau had succeeded in solving an earlier Enigma machine that functioned without a plugboard , but had been unsuccessful with the Enigma I , a new standard German cipher machine that was coming into widespread use . In late October or early November 1932 , the head of the Cipher Bureau 's German section , Captain Maksymilian Ci??ki , tasked Rejewski to work alone on the German Enigma I machine for a couple of hours per day ; Rejewski was not to tell his colleagues what he was doing .

= = Solving the wiring = =

To decrypt Enigma messages , three pieces of information were needed : (1) a general understanding of how Enigma functioned ; (2) the wiring of the rotors ; and (3) the daily settings (the sequence and orientations of the rotors , and the plug connections on the plugboard) . Rejewski had only the first at his disposal , based on information already acquired by the Cipher Bureau .

First Rejewski tackled the problem of discovering the wiring of the rotors . To do this , according to historian David Kahn , he pioneered the use of pure mathematics in cryptanalysis . Previous methods had largely exploited linguistic patterns and the statistics of natural @-@ language texts ? letter @-@ frequency analysis . Rejewski applied techniques from group theory ? theorems about permutations ? in his attack on Enigma . These mathematical techniques , combined with material supplied by Gustave Bertrand , chief of French radio intelligence , enabled him to reconstruct the internal wirings of the machine 's rotors and nonrotating reflector . " The solution " , writes Kahn , " was Rejewski 's own stunning achievement , one that elevates him to the pantheon of the greatest cryptanalysts of all time . " Rejewski used a mathematical theorem ? that two permutations are conjugate if and only if they have the same cycle structure ? that mathematics professor and Cryptologia co @-@ editor Cipher A. Deavours describes as " the theorem that won World War II " .

Before receiving the French intelligence material , Rejewski had made a careful study of Enigma messages , particularly of the first six letters of messages intercepted on a single day . For security , each message was encrypted using different starting positions of the rotors , as selected by the operator . This message setting was three letters long . To convey it to the receiving operator , the sending operator began the message by sending the message setting in a disguised form ? a six @-@ letter indicator . The indicator was formed using the Enigma with its rotors set to a common global setting for that day , termed the ground setting , which was shared by all operators . The

particular way that the indicator was constructed introduced a weakness into the cipher .

For example , suppose the operator chose the message setting KYG for a message . The operator would first set the Enigma 's rotors to the ground setting , which might be GBL on that particular day , and then encrypt the message setting on the Enigma twice ; that is , the operator would enter KYGKYG (which might come out to something like QZKBLX) . The operator would then reposition the rotors at KYG , and encrypt the actual message . A receiving operator could reverse the process to recover first the message setting , then the message itself . The repetition of the message setting was apparently meant as an error check to detect garbles , but it had the unforeseen effect of greatly weakening the cipher . Due to the indicator 's repetition of the message setting , Rejewski knew that , in the plaintext of the indicator , the first and fourth letters were the same , the second and fifth were the same , and the third and sixth were the same . These relations could be exploited to break into the cipher .

Rejewski studied these related pairs of letters . For example , if there were four messages that had the following indicators on the same day : BJGTDN , LIFBAB , ETULZR , TFREII , then by looking at the first and fourth letters of each set , he knew that certain pairs of letters were related . B was related to T , L was related to B , E was related to L , and T was related to E : (B , T) , (L , B) , (E , L) , and (T , E) . If he had enough different messages to work with , he could build entire sequences of relationships : the letter B was related to T , which was related to E , which was related to L , which was related to B (see diagram) . This was a " cycle of 4 " , since it took four jumps until it got back to the start letter . Another cycle on the same day might be A <formula> F <formula> W <formula> A , or a " cycle of 3 " . If there were enough messages on a given day , all the letters of the alphabet might be covered by a number of different cycles of various sizes . The cycles would be consistent for one day , and then would change to a different set of cycles the next day . Similar analysis could be done on the 2nd and 5th letters , and the 3rd and 6th , identifying the cycles in each case and the number of steps in each cycle .

Using the data thus gained , combined with Enigma operators ' tendency to choose predictable letter combinations as indicators (such as girlfriends ' initials or a pattern of keys that they saw on the Enigma keyboard < these became known to the allies as " Cillies " (" Sillies " misspelled) >) , Rejewski was able to deduce six permutations corresponding to the encipherment at six consecutive positions of the Enigma machine . These permutations could be described by six equations with various unknowns , representing the wiring within the entry drum , rotors , reflector , and plugboard .

= = = French help = = =

At this point , Rejewski ran into difficulties due to the large number of unknowns in the set of equations that he had developed . He would later comment in 1980 that it was still not known whether such a set of six equations was soluble without further data . But he was assisted by cryptographic documents that Section D of French military intelligence (the Deuxième Bureau) , under future General Gustave Bertrand , had obtained and passed on to the Polish Cipher Bureau . The documents , procured from a spy in the German Cryptographic Service , Hans @-@ Thilo Schmidt , included the Enigma settings for the months of September and October 1932 . About 9 or 10 December 1932 , the documents were given to Rejewski . They enabled him to reduce the number of unknowns and solve the wirings of the rotors and reflector .

There was another obstacle to overcome , however . The military Enigma had been modified from the commercial Enigma , of which Rejewski had had an actual example to study . In the commercial machine , the keys were connected to the entry drum in German keyboard order (" QWERTZU ... ") . However , in the military Enigma , the connections had instead been wired in alphabetical order : " ABCDEF ... " This new wiring sequence foiled British cryptologists working on Enigma , who dismissed the " ABCDEF ... " wiring as too obvious . Rejewski , perhaps guided by an intuition about a German fondness for order , simply guessed that the wiring was the normal alphabetic ordering . He later recalled that , after he had made this assumption , " from my pencil , as by magic , began to issue numbers designating the connections in rotor N. Thus the connections in one rotor , the right @-@ hand rotor , were finally known . "

The settings provided by French Intelligence covered two months that straddled a changeover period for the rotor ordering . A different rotor happened to be in the right @-@ hand position for the second month , and so the wirings of two rotors could be recovered by the same method . Rejewski later recalled : " Finding the [wiring] in the third [rotor] , and especially ... in the [reflector] , now presented no great difficulties . Likewise there were no difficulties with determining the correct torsion of the [rotors '] side walls with respect to each other , or the moments when the left and middle drums turned . " By year 's end 1932 , the wirings of all three rotors and the reflector had been recovered . A sample message in an Enigma instruction manual , providing a plaintext and its corresponding ciphertext produced using a stated daily key and message key , helped clarify some remaining details .

There has been speculation as to whether the rotor wirings could have been solved without the documents supplied by French Intelligence . Rejewski recalled in 1980 that another way had been found that could have been used to solve the wirings , but that the method was " imperfect and tedious " and relied on chance . In 2005 , mathematician John Lawrence claimed that it would have taken four years for this method to have had a reasonable likelihood of success . Rejewski had earlier written that " the conclusion is that the intelligence material furnished to us should be regarded as having been decisive to solution of the machine . "

= = Solving daily settings = =

After Rejewski had determined the wiring in the remaining rotors , he was joined in early 1933 by Ró?ycki and Zygalski in devising methods and equipment to break Enigma ciphers routinely . Rejewski later recalled :

Now we had the machine , but we didn 't have the keys and we couldn 't very well require Bertrand to keep on supplying us with the keys every month ... The situation had reversed itself : before , we 'd had the keys but we hadn 't had the machine ? we solved the machine ; now we had the machine but we didn 't have the keys . We had to work out methods to find the daily keys .

= = = Early methods = = =

A number of methods and devices had to be invented in response to continual improvements in German operating procedure and to the Enigma machine itself . The earliest method for reconstructing daily keys was the " grill " , based on the fact that the plugboard 's connections exchanged only six pairs of letters , leaving fourteen letters unchanged . Next was Ró?ycki 's " clock " method , which sometimes made it possible to determine which rotor was at the right @-@ hand side of the Enigma machine on a given day .

After 1 October 1936 , German procedure changed , and the number of plugboard connections became variable , ranging between five and eight . As a result , the grill method became considerably less effective . However , a method using a card catalog had been devised around 1934 or 1935 , and was independent of the number of plug connections . The catalog was constructed using Rejewski 's " cyclometer " , a special @-@ purpose device for creating a catalog of permutations . Once the catalog was complete , the permutation could be looked up in the catalog , yielding the Enigma rotor settings for that day .

The cyclometer comprised two sets of Enigma rotors , and was used to determine the length and number of cycles of the permutations that could be generated by the Enigma machine . Even with the cyclometer , preparing the catalog was a long and difficult task . Each position of the Enigma machine (there were 17 @,@ 576 positions) had to be examined for each possible sequence of rotors (there were 6 possible sequences) ; therefore , the catalog comprised 105 @,@ 456 entries . Preparation of the catalog took over a year , but when it was ready about 1935 , it made obtaining daily keys a matter of 12 ? 20 minutes . However , on 1 or 2 November 1937 , the Germans replaced the reflector in their Enigma machines , which meant that the entire catalog had to be recalculated from scratch . Nonetheless , by January 1938 the Cipher Bureau 's German section was reading a remarkable 75 % of Enigma intercepts , and according to Rejewski , with a minimal

increase in personnel this could have been increased to 90 % .

= = = Bomba and sheets = = =

In 1937 Rejewski , along with the German section of the Cipher Bureau , transferred to a secret facility near Pyry in the Kabaty Woods south of Warsaw . On 15 September 1938 , the Germans introduced new rules for enciphering message keys (a new " indicator procedure ") , making the Poles ' earlier techniques obsolete . The Polish cryptanalysts rapidly responded with new techniques . One was Rejewski 's bomba , an electrically powered aggregate of six Enigmas , which solved the daily keys within about two hours . Six bombas were built and were ready for use by mid @-@ November 1938 . The bomba exploited the fact that the plugboard connections did not affect all the letters ; therefore , when another change to German operating procedure occurred on 1 January 1939 , increasing the number of plugboard connections , the usefulness of the bombas was greatly reduced . The British bombe , the main tool that would be used to break Enigma messages during World War II , would be named after , and likely inspired by , the Polish bomba , though the cryptologic methods embodied in the two machines were different .

Around the same time as Rejewski 's bomba , a manual method was invented by Henryk Zygalski , that of " perforated sheets " (" Zygalski sheets ") , which was independent of the number of plugboard connections . Rejewski describes the construction of the Zygalski mechanism and its manipulation :

Fairly thick paper sheets , lettered " a " through " z " , were prepared for all twenty @-@ six possible positions of rotor L [the left @-@ hand Enigma rotor] and a square was drawn on each sheet , divided into 51 by 51 smaller squares . The sides , top , and bottom of each large square (it could as well be a rectangle) were lettered " a " through " z " and then again " a " through " y " . This was , as it were , a system of coordinates in which the abscissas and ordinates marked successive possible positions of rotors M [the middle Enigma rotor] and N [the right @-@ hand Enigma rotor] , and each little square marked permutations , with or without constant points , corresponding to those positions . Cases with constant points were perforated .

[E] ach constant point had to be perforated as many as four times . [...] When the sheets were superposed and moved in the proper sequence and the proper manner with respect to each other , in accordance with a [precisely] defined program , the number of visible apertures gradually decreased . And , if a sufficient quantity of data was available , there finally remained a single aperture , probably corresponding to the right case , that is , to the solution . From the position of the aperture one could calculate the order of the rotors , the setting of their rings , and , by comparing the letters of the cipher keys with the letters in the machine , likewise permutation S ; in other words , the entire cipher key .

However , application of both the bomba and Zygalski sheets was complicated by yet another change to the Enigma machine on 15 December 1938 . The Germans had supplied Enigma operators with an additional two rotors to supplement the original three , and this increased the complexity of decryption tenfold . Building ten times as many bombas (60 would now be needed) was beyond the Cipher Bureau 's ability ? that many bombas would have cost fifteen times its entire annual equipment budget .

Two and a half weeks later , effective 1 January 1939 , the Germans increased the number of plug connections to 7 ? 10 , which , writes Rejewski , " to a great degree , decreased the usefulness of the bombs . " Zygalski 's perforated (" Zygalski ") sheets , writes Rejewski , " like the card @-@ catalog method , was independent of the number of plug connections . But the manufacture of these sheets , [...] in our [...] circumstances , was very time @-@ consuming , so that by 15 December 1938 , only one @-@ third of the whole job had been done . [T] he Germans ' [introduction of rotors] IV and V [...] increased the labor of making the sheets tenfold [since 60 , or ten times as many , sets of sheets were now needed] , considerably exceeding our [...] capacities . "

= = = Allies informed = = =

As it became clear that war was imminent and that Polish financial resources were insufficient to keep pace with the evolution of Enigma encryption (e.g. , due to the prohibitive expense of an additional 54 bombas and due to the Poles ' difficulty in producing in timely fashion the full 60 series of 26 " Zygalski sheets ") , the Polish General Staff and government decided to initiate their Western allies into the secrets of Enigma decryption . The Polish methods were revealed to French and British intelligence representatives in a meeting at Pyry , south of Warsaw , on 25 July 1939 . France was represented by Gustave Bertrand and Air Force cryptologist Captain Henri Braquenié ; Britain , by Government Code and Cypher School chief Alastair Denniston , veteran cryptologist Alfred Dillwyn Knox , and Commander Humphrey Sandwith , head of the section that had developed and controlled the Royal Navy 's intercept and direction @-@ finding stations . The Polish hosts included Cipher Bureau chief Gwido Langer , the Bureau 's German @-@ Section chief Maksymilian Ci??ki , the Bureau 's General @-@ Staff @-@ Intelligence supervisor Stefan Mayer , and the three cryptologists Rejewski , Ró?ycki and Zygalski .

The Poles ' gift of Enigma decryption to their Western allies , five weeks before the outbreak of World War II , came not a moment too soon . Knowledge that the cipher was crackable was a morale boost to Allied cryptologists . The British were able to manufacture at least two complete sets of perforated sheets ? they sent one to PC Bruno , outside Paris , in mid @-@ December 1939 ? and began reading Enigma within months of the outbreak of war .

Without the Polish assistance , British cryptologists would , at the very least , have been considerably delayed in reading Enigma . Hugh Sebag @-@ Montefiore concludes that substantial breaks into German Army and Air Force Enigma ciphers by the British would have occurred only after November 1941 at the earliest , after an Enigma machine and key lists had been captured , and similarly into Naval Enigma only after late 1942 .

Intelligence gained from solving high @-@ level German ciphers ? intelligence codenamed Ultra by the British and Americans ? came chiefly from Enigma decrypts . While the exact contribution of Ultra intelligence to Allied victory is disputed , Kozaczuk and Straszak note that " it is widely believed that Ultra saved the world at least two years of war and possibly prevented Hitler from winning . " The English historian Sir Harry Hinsley , who worked at Bletchley Park , similarly assessed it as having " shortened the war by not less than two years and probably by four years " . The availability of Ultra was due to the earlier Polish breaking of Enigma ; Gordon Welchman , head of Bletchley Park 's Hut 6 (which solved German Army and Air Force Enigma ciphers) , writes : " Hut 6 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 version of the commercial Enigma machine , and of the operating procedures that were in use . "

= = In France and Britain = =

= = = PC Bruno = = =

On 5 September 1939 the Cipher Bureau began preparations to evacuate key personnel and equipment from Warsaw . Soon a special evacuation train , the Echelon F , transported them eastward , then south . By the time the Cipher Bureau was ordered to cross the border into allied Romania on 17 September , they had destroyed all sensitive documents and equipment and were down to a single very crowded truck . The vehicle was confiscated at the border by a Romanian officer , who separated the military from the civilian personnel . Taking advantage of the confusion , the three mathematicians ignored the Romanian 's instructions . They anticipated that in an internment camp they might be identified by the Romanian security police , in which the German Abwehr and SD had informers . The mathematicians went to the nearest railroad station , exchanged money , bought tickets , and boarded the first train headed south . After a dozen or so hours , they reached Bucharest , at the other end of Romania . There they went to the British embassy . Told by the British to " come back in a few days " , they next tried the French embassy , introducing themselves as " friends of Bolek " (Bertrand 's Polish code name) and asking to speak

with a French military officer . A French Army colonel telephoned Paris and then issued instructions for the three Poles to be assisted in evacuating to Paris .

On 20 October 1939 the three Polish cryptologists resumed work on German ciphers at a joint French ? Polish ? Spanish radio @-@ intelligence unit stationed at Gretz @-@ Armainvilliers , forty kilometers northeast of Paris , and housed in the Château de Vignolles (code @-@ named PC Bruno) .

As late as 3 ? 7 December 1939 , when Lt. Col. Langer and French Air Force Capt. Henri Braquenié visited London and Bletchley Park , the British asked that the Polish cryptologists be made available to them in Britain . Langer , however , took the position that they must remain where the Polish Army in exile was forming ? on French soil .

On 17 January 1940 the Poles found the first Enigma key to be solved in France , one for 28 October 1939 . The PC Bruno staff collaborated by teleprinter with counterparts at Bletchley Park in England . For their mutual communications security , the Polish , French , and British cryptologic agencies used the Enigma machine itself . Bruno closed its Enigma @-@ encrypted messages to Britain with an ironic " Heil Hitler ! "

In the first months of 1940 , Alan Turing ? principal designer of the British cryptological Bombe , elaborated from the Polish bomba ? would visit Bruno to confer about Enigma decryption with the three Polish cryptologists .

On 24 June 1940 , after Germany 's victory in the Battle of France , Gustave Bertrand flew Bruno 's international personnel ? including fifteen Poles , and seven Spaniards who worked on Italian ciphers ? in three planes to Algeria .

= = = Cadix = = =

Some three months later , in September 1940 , they returned to work covertly in unoccupied southern , Vichy France . Rejewski 's cover was as Pierre Ranaud , a lycée professor from Nantes . A radio @-@ intelligence station was set up at the Château des Fouzes , code @-@ named Cadix , near Uzès . Cadix began operations on 1 October . Rejewski and his colleagues solved German telegraph ciphers , and also the Swiss version of the Enigma machine (which had no plugboard) . Rejewski may have had little or no involvement in working on German Enigma at Cadix .

In early July 1941 , Rejewski and Zygalski were asked to try solving messages enciphered on the secret Polish Lacida cipher machine , which was used for secure communications between Cadix and the Polish General Staff in London . Lacida was a rotor machine based on the same cryptographic principle as Enigma , yet had never been subjected to rigorous security analysis . The two cryptologists created consternation by breaking the first message within a couple of hours ; further messages were solved in a similar way .

The youngest of the three Polish mathematicians who had worked together since 1929 ? Jerzy Ró?ycki ? died in the sinking of a French passenger ship on 9 January 1942 , as he was returning to Cadix from a stint in Algeria . By summer 1942 work at Cadix was becoming dangerous , and plans for evacuation were drawn up . Vichy France was liable to be occupied by German troops , and Cadix 's radio transmissions were increasingly at risk of detection by the German Funkabwehr , a unit tasked with locating enemy radio transmitters . Indeed , on 6 November a pickup truck equipped with a circular antenna arrived at the gate of the Château des Fouzes where the cryptologists were operating . The visitors , however , did not enter , and merely investigated nearby farms , badly frightening their occupants . Nonetheless , at Bertrand 's suggestion French intelligence ordered the evacuation of Cadix . The order was carried out on 9 November , the day after the Allied " Operation Torch " landings in North Africa . Three days later , on 12 November , the Germans occupied the chateau .

= = = Escaping France = = =

The Poles were split into groups of two and three . On 11 November 1942 Rejewski and Zygalski were sent to Nice , in the Italian @-@ occupied zone . After coming under suspicion there , they had

to flee again , moving or hiding constantly . Their trek took them to Cannes , Antibes , back to Nice , then on to Marseilles , Toulouse , Narbonne , Perpignan , and Ax @-@ les @-@ Thermes , near the Spanish border . On 29 January 1943 , accompanied by a local guide , Rejewski , and Zygalski , bound for Spain , began a climb over the Pyrenees , avoiding German and Vichy patrols . Near midnight , close to the Spanish border , the guide pulled out a pistol and demanded that they hand over their remaining money .

After being robbed , Rejewski and Zygalski succeeded in reaching the Spanish side of the border , only to be arrested within hours by security police . They were sent first to a prison in La Seu d 'Urgell , then on 24 March transferred to a prison at Lerida . On 4 May 1943 , after having spent over three months in Spanish prisons , on intervention by the Polish Red Cross the pair were released and sent to Madrid . Leaving there on 21 July , they made it to Portugal ; from there , aboard HMS Scottish , to Gibraltar ; and then by air to RAF Hendon in north London , arriving on 3 August 1943 .

= = = Britain = = =

Rejewski and Zygalski were inducted as privates into the Polish Armed Forces on 16 August 1943 and were posted to a Polish Army facility in Boxmoor , cracking German SS and SD hand ciphers . The ciphers were usually based on the Doppelkassettenverfahren (" double Playfair ") system , which the two cryptologists had already worked on in France . British cryptologist Alan Stripp suggests that " Setting them to work on the Doppelkassetten system was like using racehorses to pull wagons . " On 10 October 1943 , Rejewski and Zygalski were commissioned second lieutenants ; on 1 January 1945 Rejewski , and presumably also Zygalski , were promoted to lieutenant . When Gustave Bertrand fled to England in June 1944 , he and his wife were provided with a house in Boxmoor , a short walk from the Polish radio station and cryptology office , where it seems likely that his collaboration with Rejewski and Zygalski continued .

Enigma decryption , however , had become an exclusively British and American domain ; the Polish mathematicians who had laid the foundations for Allied Enigma decryption were now excluded from making further contributions in this area . By that time , at Bletchley Park , " very few even knew about the Polish contribution " because of the strict secrecy and the " need @-@ to @-@ know " principle .

= = Back in Poland = =

After the Germans suppressed the 1944 Warsaw Uprising , they sent Rejewski 's wife and children west , along with other Warsaw survivors ; the family eventually found refuge with her parents in Bydgoszcz . Rejewski was discharged from the Polish Army in Britain on 15 November 1946 . Six days later , he returned to Poland to be reunited with his wife and family . On his return , he was urged by his old Pozna? University professor , Zdzis?aw Krygowski , to take a university mathematics post at Pozna? or Szczecin , in western Poland . Rejewski could have looked forward to rapid advancement because of personnel shortages as a result of the war . However , he was still recovering from rheumatism , which he had contracted in the dank Spanish prisons . Soon after his return to Poland , in the summer of 1947 , his 11 @-@ year @-@ old son Andrzej died of polio after only five days ' illness . After his son 's death , Rejewski did not want to part , even briefly , with his wife and daughter , so they lived in Bydgoszcz with his in @-@ laws . Rejewski took a position in Bydgoszcz as director of the sales department at a cable @-@ manufacturing company , Kabel Polski (Polish Cable) .

Between 1949 and 1958 Rejewski was repeatedly investigated by the Polish Office of Public Security , who suspected he was a former member of the Polish Armed Forces in the West . He retired in 1967 , and moved with his family back to Warsaw in 1969 , to an apartment he had acquired 30 years earlier with financial help from his father @-@ in @-@ law .

Rejewski had written a " Report of Cryptologic Work on the German Enigma Machine Cipher " in 1942 . Before his 1967 retirement , he began writing his " Memoirs of My Work in the Cipher Bureau of Section II of the [Polish] General Staff " , which were purchased by the Polish Military Historical

Institute , in Warsaw . Rejewski had often wondered what use Alan Turing (who in early 1940 had visited the Polish cryptologists at PC Bruno outside Paris) and the British at Bletchley Park had ultimately made of the Polish discoveries and inventions . For nearly three decades after the war , little was publicly known due to a ban imposed in 1945 by British Prime Minister Winston Churchill . In a 1967 book W?adys?aw Kozaczuk , associated with the Military Historical Institute , disclosed Poland 's breaking of the German Enigma ciphers .

Until 1974 , the scant information published concerning Enigma decryption attracted little attention . Ladislas Farago 's 1971 best @-@ seller The Game of the Foxes presented a garbled account of Ultra 's origins : " Commander Denniston went clandestinely to a secluded Polish castle [sic] on the eve of the war [to pick up an Enigma , ' the Wehrmacht 's top system ' during World War II] . Dilly Knox later solved its keying [sic] ... " Still , this was marginally closer to the truth than many British and American best @-@ seller accounts that would follow after 1974 . Their authors were at a disadvantage : they did not know that the founder of Enigma decryption , Rejewski , was still alive and alert , and that it was reckless to fabricate stories out of whole cloth .

With Gustave Bertrand 's 1973 publication of his Enigma , substantial information about the origins of Ultra began to seep out ; and with F. W. Winterbotham 's 1974 best @-@ seller , The Ultra Secret , the dam began to burst . Still , many aspiring authors were not averse to filling gaps in their information with whole @-@ cloth fabrications . Rejewski fought a gallant (if , into the 21st century , not entirely successful) fight to get the truth before the public . He published a number of papers on his cryptologic work and contributed generously to articles , books , and television programs . He was interviewed by scholars , journalists , and television crews from Poland , East Germany , the United States , Britain , Sweden , Belgium , the Soviet Union , Yugoslavia , and Brazil .

Rejewski maintained a lively correspondence with his wartime French host , General Gustave Bertrand , and at the General 's bidding he began translating Bertrand 's Enigma into Polish . In 1976 , at the request of the Józef Pi?sudski Institute of America , Rejewski broke enciphered correspondence of Józef Pi?sudski and his fellow Polish Socialist conspirators from 1904 . On 12 August 1978 he received from a grateful Polish people the Officer 's Cross of the Order of Polonia Restituta .

Rejewski , who had been suffering from heart disease , died of a heart attack on 13 February 1980 , aged 74 , after returning home from a shopping trip . He was buried with military honors at Warsaw 's Pow?zki Military Cemetery .

= = Recognition = =

On 21 July 2000 , Poland 's President Aleksander Kwa?niewski posthumously awarded Poland 's highest civilian decoration , the Grand Cross of the Order of Polonia Restituta , to Marian Rejewski and Henryk Zygalski . Rejewski 's daughter , Janina Sylwestrzak , also received the War Medal 1939 ? 1945 on his behalf , from the British Chief of the Defence Staff in July 2005 . On 1 August 2012 , Marian Rejewski posthumously received the Knowlton Award of the U.S. Military Intelligence Corps Association ; his daughter Janina accepted the award at his home town , Bydgoszcz , on 4 September 2012 . Rejewski had been nominated for the award by NATO Allied Command Counterintelligence .

On 5 August 2014 , the Institute of Electrical and Electronics Engineers (IEEE) honored Rejewski , Ró?ycki , and Zygalski with its prestigious Milestone award , which recognizes achievements that have changed the world .

A three @-@ sided bronze monument was dedicated in 2007 in front of Pozna? Castle . Each side bears the name of one of the three Polish mathematicians who broke the Enigma cipher .

Rejewski and colleagues were the heroes of Sekret Enigmy (The Enigma Secret) , a thriller movie about the Poles ' solution of the German Enigma cipher . Late 1980 also saw a Polish TV series with a similar theme , Tajemnice Enigmy (" The Secrets of Enigma ") .