Enigma G: The Counter Enigma

David Kenyon and Frode Weierud

Bletchley Park Trust and Crypto Cellar Research

5 May 2019

Abstract The development history of Enigma G, the counter Enigma, is presented and traced from the very beginning of the development of the small, glow-lamp Enigma machine in early 1923 until the end of the Second World War. The commercial customers and governmental users of the machines are introduced and covered in considerable details. The Hungarian machine, G 110, recently found buried in Poland and its subsequent conservation by the Bletchley Park Trust is then analysed and explained.

Keywords *Abwehr*, *Abwehr* Enigma, Bletchley Park (BP), Counter Enigma, *Deutsches Stickstoff-Syndikat*, Dutch Navy, Enigma, Enigma G, G31, G 110, German Armistice Commission, Hungarian Army, *I.G. Farben*, KK-machine, *Zählwerksmaschine*

Contact Dr. David Kenyon, Research Historian, Bletchley Park Trust. Email: dkenyon@bletchleypark.org.uk Address: The Mansion, Bletchley Park, Milton Keynes, MK3 6EB, United Kingdom.

Introduction

Enigma G, also called Enigma G31, was normally referred to as *Die Zählwerksmaschine*, the counter Enigma, by the Germans, however, after the war this special version of the Enigma was often called the *Abwehr* Enigma. It is understandable that it was so-called, because most of the messages enciphered on this machine during the war were traffic from the German military intelligence service the *Abwehr*. Nevertheless, that name is a misnomer, because even if the *Abwehr* perhaps was the biggest user of the machine it was not the only user of the machine and neither was it the first user. Enigma G was the final development in a series of Enigma machines equipped with a counter and where the rotors could be moved backwards and forwards in synchronism to allow for the correction of errors. The idea for a commercial machine equipped with a counter was born as early as 1926. The new *Zählwerksmaschine* or as the Germans expressed it: "*Glühlampen Chiffriermaschine mit Zählwerk und zwangsläufiger Walzen-Kupplung*" — Glow-lamp cipher machine with counter and forced rotor coupling, went through at least three major design revisions before the Enigma G finally was launched in 1931. (Chiffriermaschinen AG 1928)

The Enigma G was produced in relatively small numbers. The estimate today is that less than 350 machines were produced. Compared with the large number of plugboard Enigma machines produced for the German army and navy, it is perhaps even strange that the Enigma G is publicly known at all. However, the Enigma G received its share of fame because of the fact that it was the machine used by the 'sinister' *Abwehr* and whose communications BP unravelled thanks, first of all to the eccentric codebreaker Dilly Knox, but also to his brilliant staff, Mavis Batey (née Lever) and Margaret Rock. The intelligence obtained through breaking the *Abwehr* ciphers, both machine and hand ciphers, played an important part in the double-cross system of rounding up and turning the *Abwehr's* agents in Britain and keeping a watchful eye on their agent's activities in Spain and Portugal. And then suddenly the machine became front-line news on 1 April 2000, when Bletchley Park's then only Enigma G machine, G 312, was stolen. The puzzling theft, a cavalcade running over several months, until the machine suddenly turned up in a parcel addressed to the BBC television presenter Jeremy Paxman on 17 October 2000, has never really been solved. That is was much more than an April-fool joke gone bad is nevertheless clear,

however, it rekindled people's interest in the Enigma and made many curious to know more. Seen in this light and also due to the positive outcome, the return of the machine, the theft was not altogether a negative affair.

Figure 1. Enigma G 312, the machine stolen from the Bletchley Park Trust (BPT) in April 2000. Photo © 2019 courtesy of BPT.

Below the authors will have a look beyond the headlines and stories about the *Abwehr* Enigma and try to give a better understanding of the Enigma G, its developments from a mere idea to an operational machine. Furthermore, we will try to follow the history of one of the earliest Enigma G machines, G 110, a machine sold to the Hungarians in 1931. The machine, an archaeological relic that has been restored by the Bletchley Park Trust and now is a part of their cryptological exhibits, shows what most likely happened to thousands of Enigma machines in the final days of the Second World War.

The First Glow-Lamp Machines

The first idea for a less complex cipher machine using glow lamps instead of a printer seems to have come early in 1923. Until then the Enigma cipher machine made by *Gewerkschaft Securitas*, Berlin, as the Enigma company was then called, had been a big and heavy machine equipped with a printer. A blueprint dated 31 May 1923, shows the electrical and mechanical principles of a new machine with glow lamps and perhaps more astonishingly a reflector or as the Germans called it, an *Umkehrwalze* or UKW.[1] All the Enigma machines until then had been straight through machines where the cleartext characters entered on one side of a bank of electrical rotors or wired wheels[2] and the ciphertext characters exited at the other side. The system was not symmetrical such that to decipher a message the keyboard input and the printer output had to change places. To achieve this a rather large cipher/decipher switch with at least 26 contact points had to be used. The reflector did away with this switch. The machine became symmetrical such that when entering plaintext at a given setting ciphertext would be produced, and if at the same setting the ciphertext was entered the original plaintext would reappear. This innovation had two great advantages. The big switch, with its increased risk of contact failures, was no longer needed and possible operator errors by using the machine in the wrong mode were removed. However, the reflector had one big disadvantage a character could no longer encipher to itself; plaintext letter A could not become ciphertext letter A. At first sight this looks like a small sacrifice to pay for such big advantages, however it hides a cryptanalytical wedge, a tool for the codebreaker to master the machine. That a letter cannot encipher to itself means that the process of placing a crib, a possible word or a part of guessed plaintext, in a given ciphertext is greatly simplified. Any position of the crib where a letter is found to be at the same position in the crib as in the ciphertext is known to be a non-valid position and can therefore be discarded. The longer the crib the easier it is to find the correct matching.

---

1. The documents referred to in this section are part of the TICOM (Target Intelligence Committee) collections T 1715, T1716, T1717, and T1718 containing original documents from *Chiffriermaschinen-Aktiengesellschaft* (ChiMaAG) and *Chiffriermaschinen-Gesellschaft Heimsoeth und Rinke* (H&R). The collections are in the *Politisches Archiv des Auswärtigen Amts* (PAAA), Berlin. (TICOM 1945b)
2. The more common usage is the term wheels instead of rotors, however here rotors is used to distinguish them from the simple gear wheels used in the counter Enigma.

For some unknown reason the reflector idea was not immediately adopted. On 18 January 1924, the engineer Paul Bernstein (1891–1976)[3] applied for a patent, DE407804 in the name of *Chiffriermaschinen-Aktiengesellschaft* (ChiMaAG)[4], for a small two rotor cipher machine with glow lamps, but the machine was not equipped with a reflector. Instead the keyboard was connected to the fixed righthand entry rotor and the glow lamps connected to the fixed left-hand exit rotor, however as the machine did not have a cipher/decipher switch two such machines had to be used, one configured for ciphering and the other for deciphering.

At the exhibition that was part of the 8th Congress of the Universal Postal Union in Stockholm and which ran from 4 July to 28 August 1924, ChiMaAG exhibited two cipher machines. One machine was their big printing Enigma *"Die Handelsmaschine"* (the commercial machine) while the second was a new development called the *Glühlampenchiffriermaschine "Enigma A"* (glow lamp cipher machine "Enigma A") but also going under the name *"Die kleine Militärmaschine"* (the small military machine). (Wik 2018)

The machine was indeed small measuring only 23 x 27 x 13 cm and with a weight of only 5 kg. It was equipped with two 26-point rotors carrying the numbers 01 to 26 on their circumference and a settable reflector with the 26 letters A to Z.[5] This meant the machine had 17576 start positions or message settings but only a period of 676. Another speciality with this machine was that all the lamps and all the keys carried removable labels allowing the lamps and keys to have 26 different letters, numbers or symbols. It was also physically unlike any later Enigma machines because the keyboard and the lamps were laid out in two double rows of each 13 lamps and keys, such that the keys and lamps were in alternating rows. And finally, to move the rotors for each new letter to be enciphered it was necessary to press a separate transport lever (*Antriebstaste*). To avoid two or more letters being enciphered on the same

3. Engineer Paul Alfred Bernstein was born on 14 December 1891, in Debschwitz, Gera, Thuringia. He died in 1976 in Esslingen in Neckar. Information provided by Claus Taaks.
4. ChiMaAG was founded on 9 July 1923, and all the patents and equipment were transferred from *Gewerkschaft Securitas* to the new company.
5. It appears that the machine that was displayed in Stockholm must have been a prototype of "Enigma A" because it was apparently not equipped with a settable reflector.

machine setting all the other keys were physically locked until the transport lever had been pressed and the rotors had moved to a new position. Nevertheless, this was operationally a drawback of this machine.

As Anders Wik explains in his article the Swedish military was very interested in the two Enigma machines. They even borrowed the machines for a month for further tests and investigations and when they returned the machines in September 1924, they expressed an interest in buying fifteen of the small glow lamp machines of type "Enigma A" if ChiMaAG was willing to make several modifications. The company was very receptive to the proposed changes and already on 13 November 1924, they offered an improved version of the "Enigma A" and a new model "Enigma B" that had the 28-point rotors and other changes that the Swedish military had proposed and wished for. "Enigma B" now had a third rotor in the place of the settable reflector of the "Enigma A" and a fixed reflector. With three 28-point rotors the machine period of "Enigma B" was 21168 steps, a big improvement compared with the rather short period of 676 steps for the "Enigma A."[6] Another big improvement was that the movement of the rotors now was done automatically when pressing any of the keys on the keyboard; the transport lever of the "Enigma A" was no longer needed. While the "Enigma A" could be delivered immediately, ChiMaAG had ten machines in stock, the delivery time was two months for two "Enigma B" machines.

After considerable deliberations the Swedish General Staff decided to order two of the new "Enigma B" machines for further tests and an order was placed on 13 January 1925. However, ChiMaAG had some problems with the construction of the new "Enigma B" and the two machines, A 133 and A 134, were first delivered on 8 April 1925. The General Staff was also interested in the printing Enigma machines and through the Swedish military attaché in Berlin they continued technical discussions with ChiMaAG in the months and years to follow. Their correspondence gives many clues about the company's ideas and plans in these important years. (Swedish General Staff 1924)

6. The glow lamp Enigma models "Enigma A" and "Enigma B" are the correct machine names. The previously erroneous usage of Enigma A and B for the two models of the big printing Enigma machines is unfortunately due to misunderstandings made by early Enigma researchers and collectors. In reality there were altogether four different models of the early printing Enigma machines.

On 20 October 1925, ChiMaAG informed the Swedish military attaché Henry Peyron about some of their new developments. In about fourteen days they would be able to show him a new version of their printing Enigma machine, a machine using type bars instead of the rotating print wheel of *"Die Handelsmaschine."* They further informed Major Peyron that for increased security several of their customers were now ordering five rotors for their machines such that they would have a choice of 60 different machine wirings instead of only 6 when using three rotors. And finally, they now had an improved version of their small glow lamp Enigma. The new model had the keyboard keys laid out in a staircase form, the three rows forming a staircase, a regulator to limit the current in the lamps and the possibility to attach an external battery or power supply. Furthermore, the wooden box now had a proper lock and a carrying handle. The new model was called "Enigma C". A rare photo of this first Enigma C model shows it had serial number A 120. This seems to indicate that while ChiMaAG was preparing the "Enigma B" version with a 28 letters alphabet for the Swedes they were already working on the new and improved model. Like the "Enigma B" the C-model had the keyboard laid out in alphabetic ABCD order and not the QWERTZ order that was first used with the Enigma D. This fits well with what we know about the Enigma model ordered by the *Reichsmarine*; they placed an order for ten prototype machines on 1 December 1924, of what they called *Funkschlüssel C.*

The prototype of *Funkschlüssel C* was very similar to the Enigma B delivered to the Swedes. It had 28-points rotors, but a 29 letters keyboard and lamp display where the 29th letter X did not go through the rotors but was connected directly from the key X to the lamp X. Originally the *Funkschlüssel C* was used to superencipher the 4-letter code groups from the *Allgemeines Funkspruchbuch* (A.F.B.). (Marineleitung 1926a; Marineleitung 1926b) Code groups containing the letter X would then leave this letter unenciphered. However, in the regulations for *Funkschlüssel C* from 1933 the A.F.B. was no longer being used. The message was now composed by normal plaintext and the letter X was used as a random dummy letter that is to be freely added to the plaintext. The 4-letter cipher groups were maintained as was also the case later for all *Kriegsmarine* Enigma traffic.

It turned out that ChiMaAG ran into many problems with the development and production of the new printing Enigma machine, *Die schreibende Chiffriermaschine "Enigma"*, and it was not until 10 March 1926, that Major Peyron was shown the

machine. Sweden was still interested in the printing Enigma machines or in a printing machine that could correspond with the small glow lamp machines. ChiMaAG explained that this was possible, but it would mean a new design of the glow lamp Enigma, which would make this machine both larger and more expensive. The company explained that they had developed such a glow lamp machine but that they had decided to drop the idea because of the large cost, size and weight of such a machine. They further explained that the design ideas for the glow lamp Enigma machines were simplified use, ease of transport, low weight, few error sources and low price; and these were design principles they would like to retain.

In the summer of 1926 Carl Herslow took over as the Swedish military attaché in Berlin. On 21 August 1926, Lt.Col. Herslow made a visit to the offices of ChiMaAG to see their latest model of the glow lamp Enigma, Enigma D[7] also called A26 — the 1926 model of the A-series. Internally at ChiMaAG the machine carried the designation Ch. 11, their 11th cipher device, a name that was also used on all technical drawings. The machine Lt.Col. Herslow was shown was A 325, which now had four rotors or to be more accurate three rotors and a settable reflector. ChiMaAG informed him that the fourth rotor had been added to increase security of the machine due to wishes from certain German authorities and private companies. The machine had already been adopted by the German Foreign Office and was going to be adopted by the *Reichswehrministerium*. The machines A 316 and A 317 had then already been delivered to the *Heereswaffenamt* (Army Ordnance Department) for tests and evaluation. The machines A 320 and A 323 were bought by the United Kingdom, A 320 was the machine analysed by Hugh Foss and A 323 was possibly bought by the Royal Navy[8] for their tests. (Foss 1928) Commercial customers were also interested in the new machine. The Swedish company *Svenska Tändsticksaktiebolaget* (STAB — Swedish Match AB) owned by the financier Ivar Kreuger bought A 324 and A 325 — the same machine shown to Lt.Col. Herslow, and four other machines, A 327, A 328, A 343 and A 344. The price for the Enigma D was 600 RM, equivalent to 143 USD.

On 8 November 1926, Herslow reported that during a new visit to ChiMaAG he was informed about a new development, a device to count cipher- and plaintext letters.

7. There is no doubt that this machine, A26, was called Enigma D, but the name was not used by ChiMaAG after 1926. The new version that arrived in 1927 was always referred to as A27.
8. Private communication with the Historian of GCHQ, UK.

Some customers had expressed an interest in such a counter. Herslow does not give any details about the counter or for which glow lamp Enigma it is available. However, a letter to Lt.Col. Herslow from ChiMaAG dated 18 November 1926, makes clear that machines with a counter is only made on special order. A machine with counter necessitates among other things to make the rotors smaller as well as to make several other internal changes to the machine. To make one such machine would increase the normal price of 600 RM by another 250 RM and the production would take three weeks.

The Counter Enigmas

The counter Enigma (*Zählwerksmaschine*) that Lt.Col. Herslow was told about in November 1926 was later patented by ChiMaAG's chief engineer Willi Korn (1893–?).[9] On 9 November 1928, he applied for a patent for the counter Enigma principle; the patent was published on 6 October 1931, as DE534947. (Korn 1931) Then one week later, on 17 November 1928, he applied for yet another patent for the same principle but with some variations. This patent was published 3 July 1933, as DE579555. (Korn 1933)

The idea behind the counter Enigma was more than to simply keep a tally on the cipher- and plaintext letters. The core idea was to have a machine where the wheels could be moved backwards and forwards in synchronism to allow for easy correction of ciphering errors. With the ratchet and pawl wheel movement, which all the other glow lamp Enigma machines used, it was almost impossible to move back a number of steps to correct an error. In almost all cases it was necessary for the user to start all over again from the beginning. The new idea was to strongly couple the rotors together using pinion and cog wheels instead of the ratchet and pawl arrangement. With the pinion and cog wheel movement the rotors could be moved correctly backwards and forwards any number of steps by using a small crank, the number of steps being shown by the counter. Using gear wheels for the rotor movement was nothing new for ChiMaAG; from the very beginning their big printing Enigma machine, "*Die Handelsmaschine,*" had used such wheels. The periodic movement of the rotors were produced by using notched cog wheels (*Lückenzahnräder*), cog wheels where a number of the teeth were missing producing gaps as explained by C.A. Deavours in his Cryptologia article "Lobsters, Crabs, and The Abwehr Enigma." (Deavours 1997)

The first patent, DE534947, was for a machine with rotors having only one single notch. In reality the cog wheel had only two teeth, that made up the single notch, and the rest of the wheel was one large gap. The notched cog wheel was mounted on the contact pad or left-hand side of the rotor, while on the contact pin or right-hand side there was a normal cog wheel with 52 teeth and without any gaps, the

9. *Oberingenieur* Richard Georg Willi Korn was born on 31 July 1893 in Rogätz, Wolmierstedt. When and where he died is not known.

rotor's drive wheel. A pinion sat between one rotor and its neighbour and when a notch arrived at the pinion it would be engaged by it and be connected to the drive wheel of the neighbouring rotor. Thus, momentarily the two rotors would be firmly coupled together, and the right-hand rotor would drive its left-hand neighbour one step forward. The drive wheel of the right-hand rotor was coupled with a pinion to another 52-teeth cog wheel that was firmly connected to a ratchet wheel. The sandwich of the two wheels was mounted on the circumference of the entry rotor, *Eintrittwalze*, where the two wheels were free to rotate. The ratchet wheel was moved forward with a pawl exactly like in the other Enigma machines each time a key was pressed. Hence the key press was transformed to a smooth movement of the 52-teeth cogwheel that is coupled via the pinion to the drive wheel of the fast, right-hand rotor and steps this rotor forward one position for each key press.

Because all the rotors have only one notch the rotor movement of the first counter Enigma version is cyclometric, however unlike the other glow lamp Enigma models with pawl and ratchet movement it does not have the double stepping anomaly of the middle rotor. Furthermore, like the previous glow lamp Enigma models the notch wheel was connected to the rotor body and not the letter ring. Connecting the notch wheel to the rotor body had the disadvantage that the turnover of the wheels would always take place at the same point in the rotor wiring, something that eased the work of the codebreaker. This problem seems to have been discovered by the *Reichswehr Chiffrierstelle*, cipher office, who on 1 March 1928, asked ChiMaAG to modify the 400 Enigma machines they had bought such that the notch ring would be connected to the letter/number ring and not to the rotor body. Exactly this problem is covered by Willy Korn's second patent, DE579555, that he applied for on 17 November 1928. Who saw this problem first, the *Chiffrierstelle* or ChiMaAG, is difficult to ascertain today, because the patent application dates do not give a proof of when an idea was born. One indication that not all the ideas in this second patent were Willy Korn's is the fact that later his name as the inventor was removed and only the name of the patent assigned owner, ChiMaAG, was retained.

As we shall see Willy Korn's second patent also introduced the idea of having multiple notches on each rotor; their numbers being chosen such as not to divide the alphabet size and therefore ensure that the machine's cycle or cipher period is the maximum. He further promoted the idea of using different number of notches on each rotor, that the number of the notches are relatively prime and again that none of these

numbers can divide the alphabet size. But Willy Korn went even further with his ideas. He also proposed to make the notch rings moveable and exchangeable such that either the position of the notches can be changed relative to the letter ring or that the whole notch ring can be removed and attached to any other rotor at will. This is indeed a very profound idea, which later would lead to the use of exchangeable rotor cores. Rotors with removable cores were made for the Naval Enigma M4 and also the *Lückenfüllerwalze* (variable notch wheel) had a removable core, but it is not known if this element was ever used operationally.

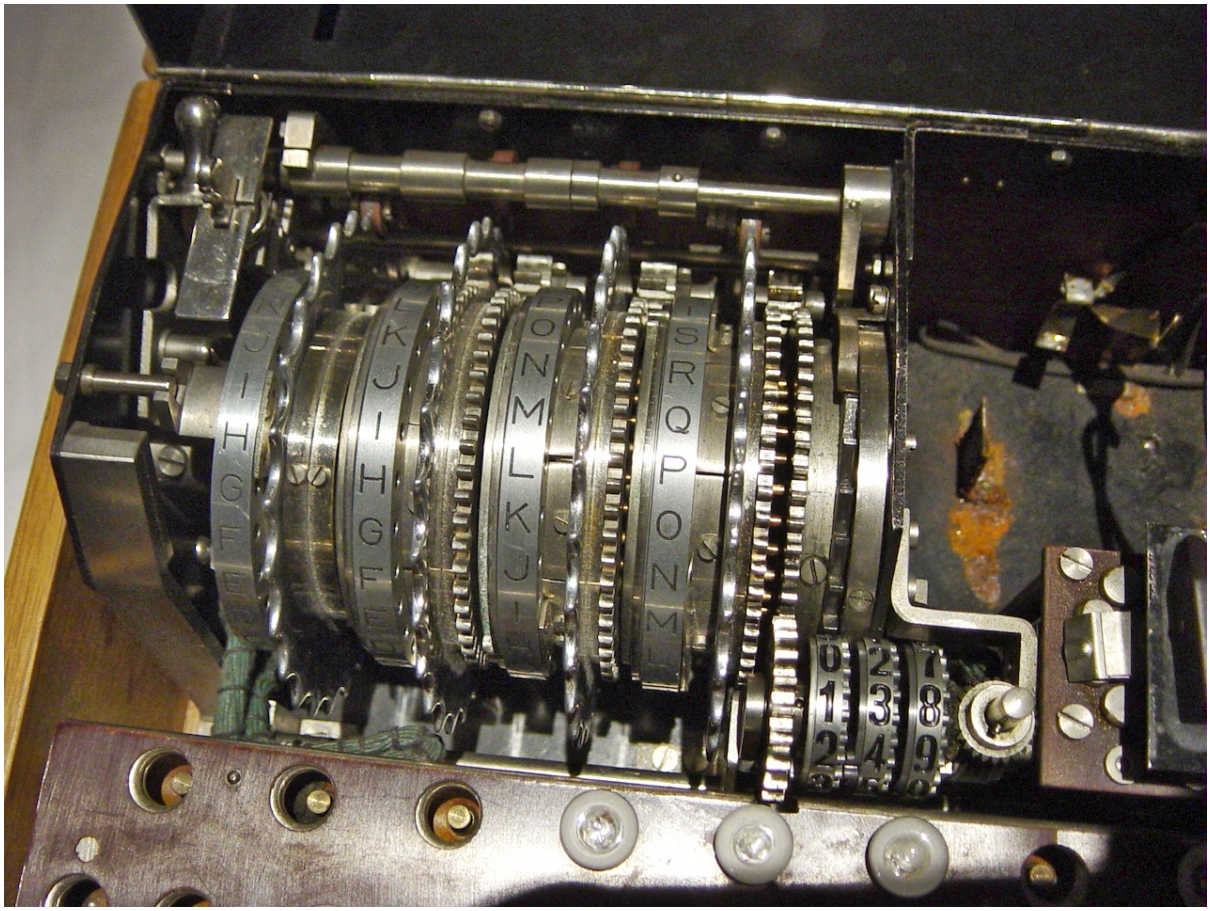


Figure 2. Interior view of *Zählwerks* Enigma A 351 bought by the Swedish Army in February 1927. From the collection of Försvarets Radioanstalt (FRA). Photo © 2007 Ingvar Eriksson, courtesy of FRA.

However, at the same time as the *Chiffrierstelle* discovered the notch ring problem they introduced another error. They asked for the notches to be at different positions for the three rotors. Rotor I should have its notch at Y, rotor II at M and rotor III at D,

while earlier all the rotors had their notches at the same position, namely at G.[10] With rotors having different notch positions it is easy for the codebreaker to identify the rotors and their position in the machine from the turnover patterns.

Like all the early glow lamp Enigma machines the first counter Enigma had only one notch on each rotor and all the notches were at position G. It is likely that the very first machines that Lt.Col. Herslow heard about in November 1926 also their notches at G. However, it seems this machine only had a counter and that the function of moving the rotors forwards and backwards had not yet been implemented in this version. In their letter of 18 November 1926, ChiMaAG says clearly that the counter only has a control function, e.g. checking the number of enciphered letters at the end of a message to ensure that the correct number has been enciphered. Nevertheless, this situation would quickly change. Already on 25 January 1927, Lt.Col. Herslow was able to inform the Swedish General Staff that ChiMaAG had now improved the counter Enigma. The rotors could now be moved backwards and forwards in complete synchronism to allow for correcting ciphering errors etc. The Swedes decided to buy two of the new counter Enigma machines and an order was placed on 17 February with expected delivery at the end of March. However, yet again ChiMaAG experienced unforeseen problems and the two machines A 350 and A 351 were not delivered before on 12 May 1927.

Everything indicates that these were the very first real counter Enigma machines that were delivered by ChiMaAG. The machines were equipped with the standard 26-point rotors and looked very similar to the Enigma D delivered in that period. The only external difference was a 3-digit counter and the shaft for a crank that was placed to the right of the four rotor windows and next to the switch controlling the lamp currents and the external power supply attachment. Opening the top cover on the other hand revealed that both the rotors and the drive arrangement were very different from the ratchet and pawl movement of the Enigma D.

On 10 December 1927, after testing the machines for 6 months the Swedes asked for a quote for 40 – 60 machines of two types, one with and one without counter, both equipped with 28-point rotors. Four days later ChiMaAG replied with an extensive quotation for machines with 26- and 28-point rotors and both with and without

10. The notch ring is fixed to the rotor body, so the position G only makes sense when the letter ring is in the neutral position A.

counter. The price for the normal glow lamp Enigma without counter, A27, with 26-point rotors and for a quantity of 40 machines was 600 RM, while the cost of a counter Enigma for the same quantity was 700 RM. Having machines with 28-point rotors increased the cost of both type of machines by 30 RM, while increasing the number of machines to 60 made all types 20 RM cheaper. Additional 26-point rotors for machines with and without counter were respectively 25 and 27 RM per piece, while 28-point rotors for both types of machines were 1 RM more expensive. ChiMaAG was clearly very eager to have this contract and it ended the offer with the words: It would be a great honour for us if we could deliver our machines for Swedish requirements.

Unfortunately, ChiMaAG never experienced that honour because the Swedish Army decided to spend their money in Sweden. Instead of the Enigma the Army ordered the B21 machine, designed by Boris Hagelin, from the Swedish company AB Cryptograph. As Anders Wik says it is not clear why the B21 was chosen instead of the Enigma, whether the reason was technical, financial or patriotic is not known.

The Swedish Navy, also looking for a modern cipher machine but operating quite independent from the Army, took delivery in April 1929 of three counter Enigma machines of the latest model with the serial numbers A 853, A 854, and A 855. Unfortunately, yet again the available documents do not tell us what the navy did with these machines and what final decision was reached about them. What we know for sure is that no other Enigma machines were bought by the Swedish authorities.

The machines bought by the Swedish Navy were ChiMaAG's latest counter Enigma model called A28. Externally the most obvious change is that the counter now has four digits instead of three and that it is placed on the left-hand side of the machine in the space between the rotors and the lamp field. The coupling for the crank is still on the right-hand side next to the fast rotor. However, internally the changes are greater. Now all the rotors have multiple notches as patented in the second patent, DE579555. Rotor I, II and III have respectively 17, 15 and 11 notches. The number of notches is relatively prime, and no factor can divide the alphabet size of 26. The number of notches is the same as are used in ChiMaAG's printing Enigma machines.

A problem for the Enigma historian is that since the very first glow lamp Enigma was produced all the machines have serial numbers in what we might call the A-series. Regardless of it being a model A, B, C or D or for that matter a *Zählwerksmaschine*, the serial number was always A-something. It is therefore often difficult to know if a

machine is a counter Enigma or not, however in some cases it is nevertheless possible to identify the machine and sometimes also the user.

The Chileans and the Dutch

There was no queue at the door of ChiMaAG of customers that wanted the new *Zählwerksmaschine* A28, but it is worth looking closer at a few of the customers. Chile seems to have been one of the first with an order for the two machines A 826 and A 829, probably ordered in early 1928. And later in the year they ordered four more machines A 842, A 843, A 859 and A 860. However, Chile had also ordered 16 of the A27 machines so in total they had at least 22 Enigma machines. Who exactly in Chile bought these machines we don't know, but it is likely it was governmental and most likely either the Chilean army or navy. Chile also bought an unknown number of the number cipher machine, *Die Zahlenmaschine*, Enigma Z also called Z30 and internally known as Ch. 16.

Other Latin American countries also bought Enigma machines. Argentina bought a total of ten machines, Brazil bought an unknown number of machines and Mexico bought two, all were of the type A27.

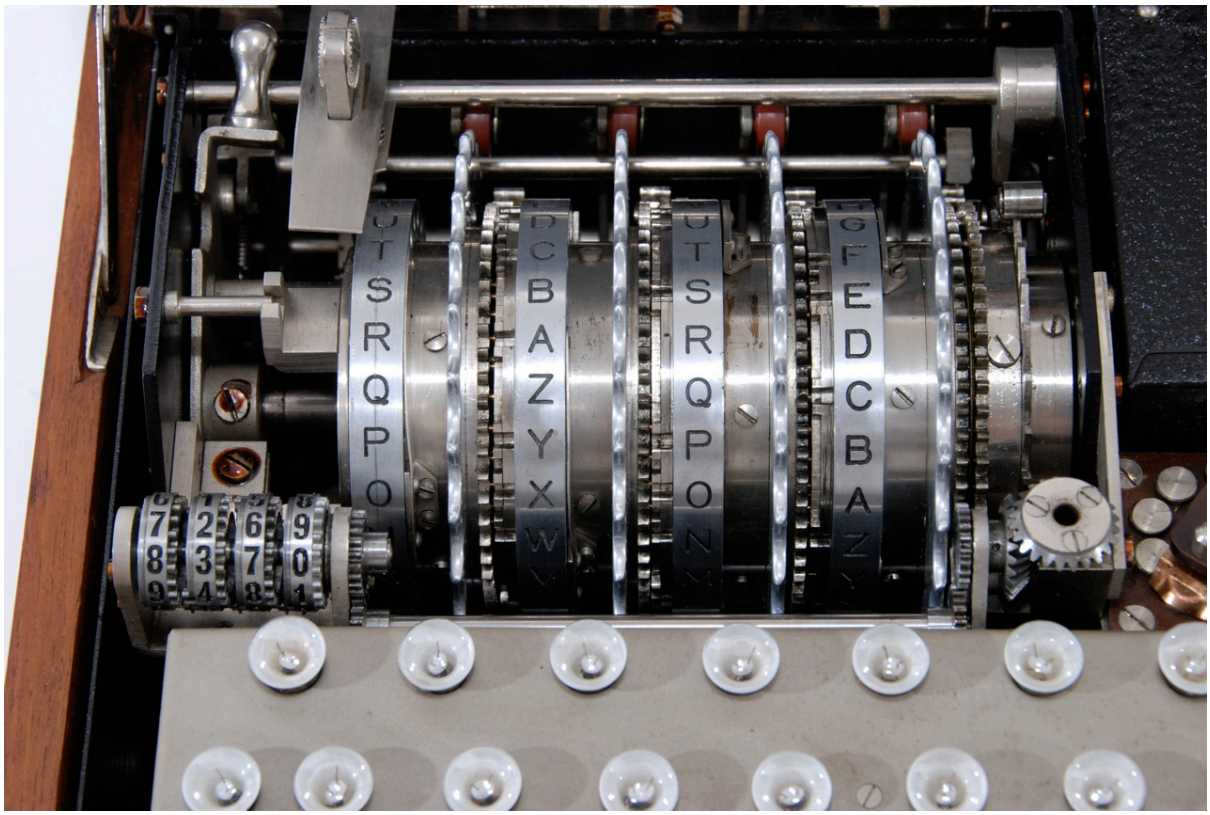


Figure 3. Interior view of *Zählwerks* Enigma A 865 bought by the Dutch Navy in 1928.
Photo © 2019 Paul Reuvers, courtesy of Crypto Museum, The Netherlands.

Another customer that knocked on ChiMaAG's door in those days was the Dutch Navy. They bought the machines A 823, A 825, A 845, A 856, A 858, and A 865. Looking at the serial numbers it seems that they bought two machines early in 1928 with another four later in the year. The Dutch Navy would turn out to be the user with the largest number of counter Enigma machines outside Germany, only the German *Abwehr* perhaps had more machines. Altogether they seem to have had at least 93 of these machines. The majority of the Dutch machines were of a new type called Enigma G31 and that was introduced in 1931. We will look at this machine in more detail in a moment.

The first of the Enigma G machines the Dutch Navy bought was G 128, probably bought in 1931. The next big order was for 44 machines, G 145 – G 188, that was delivered to the Dutch naval base in Den Helder in March 1938. However, we also know that G 138 and G 141 are Dutch naval machines so another order for at least four machines must have been made in the period from October 1935 to March 1938. It is also possible that this order was bigger than for only four machines. In September 1939 they ordered another six Enigma G machines for delivery in February 1940, but the delivery was delayed. It apparently took place on 9 May 1940, one day before the German invasion of the Netherlands, when *Heimsoeth und Rinke* (H&R, as the Enigma company now was called)[11] informed OKH/In 7/IV that they had delivered the machines G 298 – G 303 to the *Departement van Defensie, IVde Afdeeling A*, Den Haag (Dutch Department of Defence). In the period from March 1938 to September 1939 the Dutch must also have had another order for machines. All the Dutch machines were delivered with the commercial wiring.

Scattered information in the Dutch archives refers to twelve machines in the range G 195 – G 220. The distribution is such that it is most like all that the machines in this range, a total of 26 units, were Dutch naval machines.[12]

The six machines delivered in May 1940 were most likely recovered by the Germans when they attacked the Netherlands on 10 May 1940. On 28 May 1941, H&R received

11. *Chiffriermaschinen-Gesellschaft Heimsoeth & Rinke oHG* was officially founded on 1 July 1935.
12. The information and documents from the Dutch Naval Archives have generously been provided by Andreas Willemsen. Personal communications in 2018—2019.

an order from OKW/WFSt/Stb WNV/Fu II[13] to rewire the two machines G 298 and G 299 to the wiring Ch. 15 Tz 136 a – c for the three rotors I, II and III and to Ch. 15 Tz 126 for the UKW. In May 1940 the Germans also found rotor II from G 208 in the debris of the radio station of the bombed out *Alexanderkazerne* in Den Haag. The rotor was sent to OKH/In 7/IV for inspection where it was found that the rotor belonged to a machine sold legally to the Dutch and that the rotor had the original commercial wiring. (TICOM 1950b) It is possible that this rotor belonged to the set of spare rotors for G 208, because some of the machines were ordered with a set of three spare rotors. It has long been suspected that the Dutch rewired the rotors of these machines. While the special wiring is not known attempt to break two messages enciphered with one of the Dutch machines has failed to break on the normal commercial wiring.

The machines being used by the Dutch Navy in their home waters were ordered by *Departement van Defensie, Afdeeling Materieel Zeemacht* (Department for Naval Equipment), while those ordered by *Ministerie van Koloniën* (Ministry of Colonies) were destined for service by naval units and naval command posts in the Netherlands' East Indies. These machines were ordered specially for tropical climates (*Tropenausführung*). The home waters Enigmas were also used onboard the Dutch submarines that operated under British command after Germany attacked the Netherlands. But after they lost two submarines, O-13 and O-22, respectively in June and November 1940 it was decided to remove the Enigma machines from all the submarines and redistribute them to other Dutch Naval units operating in British waters. All the submarines had a three-man Royal Navy liaison team onboard that handled operational traffic using Royal Navy cyphers.[14] It is not known which Enigma was onboard O-13, but O-22 carried the machine G 197.[15]

All the Dutch Enigma machines were ordered through N.V. voorheen Ruhaak & Co., Den Haag, that was the representative of ChiMaAG and later H&R in the

13. WFSt/Stb WNV/Fu II (*Wehrmacht Führungsstab/Stab Wehrmacht Nachrichten Verbindungen/Funk II*) was the department responsible for supplying OKW and government agencies, including the *Abwehr*, with communication equipment.
14. Royal Navy cyphers were in reality superenciphered codes.
15. The loss of these two submarines is still somewhat of a mystery. It is suspected they might have hit mines.

Netherlands.[16] The Enigma orders seems to have been handled by the former artillery officer Jhr.[17] Frederik Henri Gerrold van Benthem van den Berg (1895 – 1958). He started his work in Ruhaak & Co in 1929 seemingly after he married the daughter of the director, Reinier Ernest van Eibergen Santhagens (1877 – ?).

16. Personal communications with Andreas Willemsen in 2019.
17. Jhr. stands for *Jonkheer* an honorific used by the untitled nobility.

The Hungarians

The Hungarians took an early interest in Enigma machines. Exactly when they made contact with ChiMaAG is not known but in August 1929 ChiMaAG refers to specific offers made to Hungary. In a meeting on 6 August 1929, between *Regierungsrat* (senior civil servant) Wilhelm Fenner (1891 – 1961) and First Lieutenant Walther Seifert (1896 – 1982) from the *Chiffrierstelle* and Frau Elsbeth Rinke (1879 – 1960)[18] and Willy Korn from ChiMaAG to discuss technical details about the *Steckerbrett* production, ChiMaAG mentions its intention to use pluggable UKWs on its commercial machines. It explains that the pluggable UKW is both cryptographically and operationally a good solution and that it has already offered such an implementation to Hungary.

However, it seems this solution was not adopted by the Hungarians or for that matter any other commercial customer of the Enigma. The pluggable UKW was adopted and first used operationally by the Luftwaffe in 1944 under the name UKW D. (Ostwald and Weierud 2016)

On 18 February 1930, Frau Rinke and Willy Korn had another meeting with First Lieutenant Walther Seifert. During the meeting they asked Seifert if he thought it would be possible to use the plugboard (*Steckerbrett*) on the commercial counter Enigma, *Die Zählwerksmaschine*. That they even asked this question is somewhat astonishing because the plugboard was a secret item and ChiMaAG had signed an agreement with the *Reichswehrministerium* (RWM) that this idea should only be used on the Enigma machines sold to the *Reichswehr*. On 16 May 1929, they had even transferred the rights of their plugboard patent to the RWM and the patent was classified as secret. (Chiffriermaschinen AG 1929) Of course First Lieutenant Seifert's answer was clear: In his view also for the counter Enigma they would not be allowed to use the plugboard.

Was this idea to use the plugboard on the counter Enigma yet another attempt to find an acceptable solution for their Hungarian customer? We will probably never get an answer to this question. The documentary evidence is very thin on the sale of

18. ChiMaAG's Director in those days, Mrs. Rinke, was born Sophie Conradine Elsbeth Schwarz on 21 October 1879, in Sprottau then part of the Prussian Province of Lower Silesia. In July 1904 she married the artillery officer *Oberleutnant*, later Major, Eberhard Rinke.

machines to Hungary. We do not even know who the customer was; however, it seems most likely that it was the Royal Hungarian Army.

What we know is that Hungary bought an unknown number of the large printing Enigma, called Enigma H and Ch. 14 internally. Other customers of this machine were Argentina, *Deutsche Stickstoff-Syndikat* (German Nitrogen Syndicate) and the *Reichswehr* that called this machine Enigma II. The Enigma H machines bought by the *Reichswehr* had the serial numbers H 201 – H 210, and H 216 – H 219 a total of fourteen machines. They were modified to allow the machines to work as a printer for the glow lamp machine, Enigma I, that was similarly modified. The modified Enigma I machines had the serial numbers A 897 – A 906 and A 932 – A 935. The first ten Enigma H machines were ordered on 9 October 1928, with delivery in March 1929, while the four last were ordered on 4 April 1930, and delivered in August 1930. Who bought the five machines H 211 – H 215 is not known, but they are not likely to have been sold to Hungary. The reason is that one Enigma H, H 221, was discovered in 2005 at the Hungarian Museum for Military History (*Hadtörténeti Múzeum*) in Budapest. (Crypto Museum 2019b) It is therefore more likely that at least the machines H 220 and H 221 were sold to Hungary some time in 1931.

This also fits with what we know about the sale of the Enigma G machines to Hungary, who seems to have ordered the very first Enigma G machines in the new series G31. They ordered 24 machines with the serial numbers G 101 – G 124 probably very early in 1931. All these machines were modified to be connected to the printing Enigma H; the machines being described as "*Zählwerk und Kupplung*" (counter and connection) and given the internal description Ch. 15 b. Ch.15 a was the designation for the normal Enigma G machine. That the machines were indeed modified this way has recently been verified through the discovery of two of the Hungarian machines, G 110 and G 111. (Crypto Museum 2019a) G 111 was put up for sale at a German auction house in 2009 while G 110 was bought as an archaeological relic in Poland in 2017. G 110 was originally in a very poor state without rotors while G 111 is in a rather good condition and equipped with the rotors I, II and V.

When inspecting the rotors of G 111 one finds that the wirings are different from the normal commercial wiring, only the UKW has the normal commercial wiring. Either the machines were delivered with special wirings or the Hungarians changed the wiring later. However, most interesting is the discovery that rotor V has seven notches

while rotor I and II has the normal numbers 17 and 15. The question that then immediately comes to mind is what is the number of notches on the unknown rotor IV? Is the number nine?

Another question is how many Enigma H machines the Hungarians bought. It is unlikely that they bought as many as the Enigma G machines for two reasons. The Enigma H with is size and weight is not a machine for use in the field and also with a cost of 13,000 RM per unit it unlikely the Hungarians bought more than ten. The Museum for Military History mentions that they once had three such large machines of which now only H 221 remains.

It is in June 1936 that we again hear something about the Hungarian Enigma machines. On 3 June 1936, the *Oberkommando des Heeres* (OKH) replied to a letter from H&R sent on 28 May concerning the visit of two Hungarian officers to the Enigma production firm *Konski & Krüger* (K&K). On 6 June lieutenant Colonel Karl Kelenfy and Captain Tibor Csegezy from the Royal Hungarian Defence Ministry (*Honved-Ministerium*) were to visit K&K to fetch parts for their commercial Enigma machines. It does not explicitly say Enigma G, but there is no reason to believe it was anything else. The OKH had nothing against this visit, however they stress that the Hungarians are not to be shown work rooms that are subject to secrecy.

During the war Hungary was one of the very few countries outside Germany that would get a few of the *Heeres* Enigma machines with plugboard. The other countries were Bulgaria, Italy, Slovakia and Romania. The number of machines and their actual use is not known; however, it is believed they were used for Wehrmacht communications with these countries.

In a listing of commercial Enigma machines sold to foreign users dated 9 August 1943, Hungary is also listed as having bought machines with the identifier A, most likely A27 the predecessor of Enigma K. Strange enough these machines are not included in a similar listing from October 1935 even if the sale must have taken place before Hungary bought their Enigma G machines. Nothing else is known about these machines.

The Enigma G

Enigma G was probably introduced in 1931, because the machine was also simply called G31, but no document has been found to put an accurate date on its introduction. It seems that the first machine in the G-series carried the serial number G 101, which was one of the machines sold to Hungary.

Enigma G is a further development of the *Zählwerksmaschine* A28. Cryptographically the machines are the same, but the Enigma G is a physically smaller and more refined machine. While the A28 in its wooden box measures 28 x 30 x 15.5 cm with a total weight of about 11 kg the Enigma G measures 27 x 25 x 16.5 cm and weighs only 9.4 kg. The weight of the bare machine without the case is 7.2 kg.

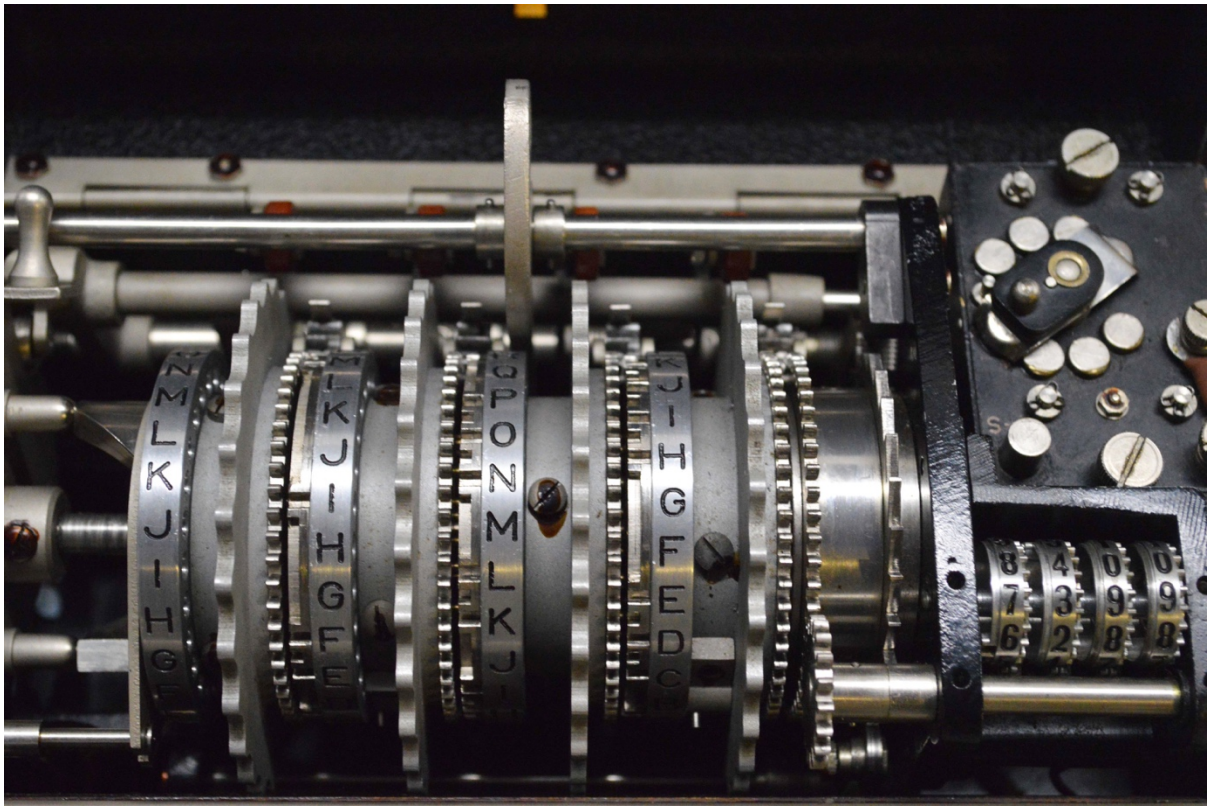


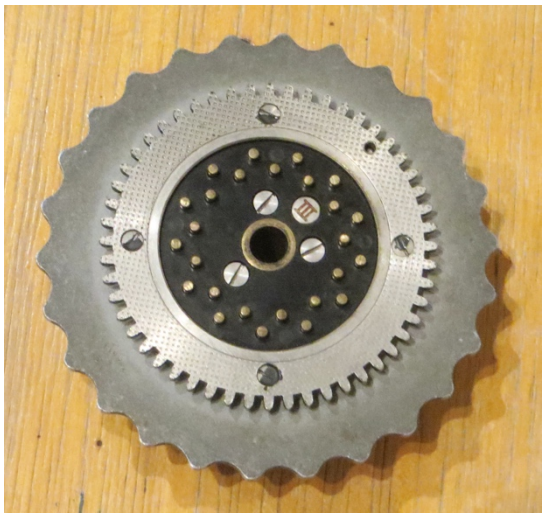
Figure 4. Interior view of Enigma G 312 in the collection of the Bletchley Park Trust. Photo © 2019 courtesy of BPT.

The three fundamental principles of the A28:

1. A high cipher security
2. An easy and also easily learned operating principle
3. A high reliability

were also carried forward into the design of the Enigma G. The machine still has a 4-digit counter like on the A28 machine, but its position is now on the right-hand side next to the right-hand rotor. The crank is now connected to a shaft in the right sidewall next to where the counter sits instead of being connected to a coupling in the lid of the machine as it is done on the A28. This means the cranking is now done horizontally instead of vertically, something that increases the ease and comfort in using the machine.

To make the machine smaller and lighter several design parameters were changed but the most striking is the new design of the rotors. The diameter of the Enigma G rotors is approximately 85 mm while the normal Enigma rotors are 100 mm in diameter. The letter ring on the Enigma G rotors is about 62 mm in diameter while on the normal Enigma rotors the ring is 75 mm. To accommodate the 26 spring loaded contact pins they are not all placed on the same circle. Every second pin is placed on a slightly smaller circle inside the larger circle such that the pins appear to be in a kind of zig-zag pattern. However, due to this layout the shape of the contact pads must also be changed to make contact with the offset pins on the two circles. Instead of being round like on the normal Enigma rotors the pads on the Enigma G rotors are elongated or pear shaped such as to make good contact with all the pins.



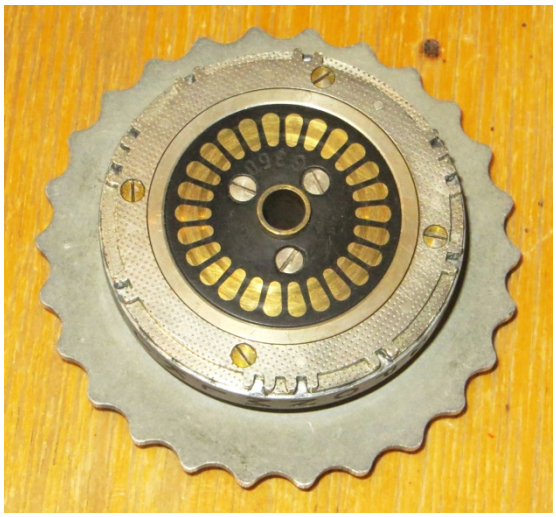


Figure 5 and 6. Side views of rotor III from Enigma G 350 in the collection of Försvarets Radioanstalt. Photo © 2019 Anders Wik, courtesy of FRA.

So far, no documents have been found that indicate clearly why this new version of the counter Enigma was made. Because the machine does not change the

cryptographic principle of the A28 machine, nor increase its security it seems likely that it must have been the weight and size of the old machine that was the reason for the new design. Was this a wish or a demand from one of the customers? If this is the case it is most likely it was the Hungarians who were looking for a smaller and lighter machine for their Army. They were nevertheless a large customer in those days and they also bought the first 28 machines that were delivered. Of course, the Dutch were also interested in the counter Enigma and it is quite possible they also were in favour of a smaller and a lighter machine for their ships and stations overseas. However, in the minds of ChiMaAG it was first of all a commercial machine and it is possible it was their attempt to position themselves in the competition with another maker of such machines, Alexander von Kryha and his Kryha machines. Kryha's two main models were a commercial version ("*Typ Commerce"*) and a diplomatic version ("*Typ Diplomat"*). Their dimensions are respectively 25 x 20 x 10 cm and 30 x 30 x 14 cm, with a weight of 4.5 kg for the commercial model and 6 kg for the diplomatic machine. Documents from H&R shows that they were interested in Alexander von Kryha; two memoranda from 1934 addressed to the *Reichswehr Chiffrierstelle* contain information about von Kryha and his machines. (Marks 2011; Schmeh 2010)

With Enigma G ChiMaAG now had a product that in size and weight could compete with Alexander von Kryha's machines and that cryptologically was greatly superior to his machines. However, they also made modified versions of the Enigma G. On 9 July 1936, the chief engineer of H&R, Willi Korn, prepared a note for Captain Kopp of OKH/In7 that he presented to him the next day. The note covered a variety of subjects concerning the counter Enigma, the new UKW B, Enigma operating instructions, delivery of Enigma M to the navy, questions about a device for Fritz Menzer (Mowry 1983) and concerns about requests from representatives from the Japanese Navy in Berlin for information about cryptography. The first point concerning the Enigma G (*Zählwerksmaschine Ch. 15*) gives an interesting glimpse of H&R's development of this machine. Willi Korn mentions that they have three special versions of this machine in their offices.

a) 1 pc. of Ch. 15 a, the normal model with a driven UKW but with special wirings of the rotors and the UKW.
b) 2 pc. of Ch. 15 b, with a driven UKW but in addition equipped with a printer connection.
c) 2 pc. of Ch. 15 c, equipped with a fixed UKW and a plugboard.

Point a) and b) refer to the normal Enigma G and the special version with a printer connection that was delivered to the Hungarians but point c) is somewhat astonishing. Because the plugboard (*Steckerbrett*) was a secret invention and which ChiMaAG had agreed to only use on machines delivered to the *Reichswehr* this machine must have been developed with this in mind. A question is then: Was this only a prototype development or did they deliver a small series of such machines to a *Reichswehr* office? That the plugboard was added is understandable if they wanted to increase the security of the machine, but why did they equip the machine with a fixed UKW. However, there is another explanation that perhaps is more likely. Perhaps the plugboard was connected to the UKW and not to the entry wheel (*Eintrittwalze*). This explains why the UKW is fixed and how such a machine could be equipped with a plugboard without violating the agreement with the *Reichswehr* about the secret *Steckerbrett*. This fits very well with what we have already seen about ChiMaAG offering a pluggable UKW to the Hungarians already in August 1929. It also means that the two versions mentioned in point b) and c) above both probably are prototypes prepared for being presented to the Hungarians.

The note for Captain Kopp about the Enigma G versions is in reality an unofficial offer for having the five machines serviced and modified such that they can communicate together. It seems that Captain Kopp was looking for a quick delivery of some Enigma G machines for some unknown purpose. Willi Korn explains that the machines can be made ready in about eight weeks and that they will be offered cheaply, however this is an exceptional offer without any precedent for the future. This statement shows clearly that in July 1936 H&R did not expect to sell any more special versions of the Enigma G machines to Hungary or for that matter to anybody else. The models Ch. 15 b and Ch. 15 c had come to the end of their life; any future machine would only be of the normal version of the Enigma G31, model Ch. 15 a.

Abwehr and Other Users

We have looked in detail on the foreign commercial and government users of the counter Enigma but also the German government and armed forces used this machine. The first known German official use of the machine is dated July 1936 when a new special wiring for the UKW was created with the drawing number Ch. 15 Tz 115. However, it is quite possible that other official German users might have used the machine before then. The drawings for the wiring of the commercial rotors and UKW were labelled respectively Ch. 15 Tz 69 a – c and Ch. 15 Tz 70. Because there is a large gap in the drawing numbers between Tz 70 and Tz 115 this is indeed a probable theory. If the Hungarian machines were, as we believe, delivered with special rotors and UKW wirings these drawing numbers most likely lay in this range.

If we include the wiring of the rotors and UKW for the commercial version of the Enigma G machines, then there is a total of 22 different rotor wirings and five different UKW wirings. Many of these were probably used by the German *Abwehr*, which undoubtedly was the biggest German official user, but several other wirings must have had other users that so far remain unknown. One exception is the machines used by the German commercial firms *Deutsches Stickstoff-Syndikat* (DSS) and *I.G. Farben*. DSS used Enigma G and the large printing Enigma H machines in their communications with Japan and *I.G. Farben* used Enigma G for their communications with Asia and their office in New York. The special wirings for the *I.G. Farben* machines are Ch. 15 Tz 121 a – c for the rotors and Ch. 15 Tz 122 for the UKW, both wirings created on 14 November 1938. Some of the *I.G. Farben* machines are G 222 – G224, G 256, G 257 and G 404 – G 407. However, *I.G. Farben* had bought Enigma machines already in 1930 and 193. In 1930 they took delivery of the machines A 837 and A 838 while in 1931 they received the machines A 839 and A 840. It is most likely that these deliveries were for four machines ordered at the same time, but with two machines delivered in December 1930 and the other two in January 1931. ChiMaAG lists these machines as being of the normal commercial type A27 and it is likely that they were delivered with the normal commercial wiring.

Another known user of Enigma G was the German Armistice Commission (*Waffenstillstandskommission*, DWStK) in France and North Africa. (US Coast Guard 1943) One of these machines, G 292, that the Germans called the KK-machines was captured by American and British commando units during the Operation Torch in

French North Africa at the beginning of November 1942. (Hammarborg 1954; Trevor-Roper 1942) The machine was used to encipher the traffic that passed between Algiers, Casablanca, Oran, Tunis in North Africa and Bourges, Marseilles, Toulon and Wiesbaden. In November 1942 the traffic on this network was about 30 messages daily, but after the fall of North Africa only the French stations remained and then the traffic dwindled to about five or six messages daily. The physical wiring of this machine is known but the drawing designation for the wiring is still unknown even if it is possible to guess at a few likely candidates.

DWStK had close ties to the *Abwehr* and several of their staff in North Africa were in reality *Abwehr* agents reporting back to the *Abwehrstelle* (Ast) in Wiesbaden, where also DWStK had their headquarters in the impressive Hotel Nassauer Hof. This close collaboration between the two organisations might explain why DWStK also used Enigma G. (Kolisch 1946)

Two other special cases of Enigma G machines being used by German signal intelligence agencies are known. The machines G 249 and G 250 were used by OKH/In 7/IV for communications with the General Staff of the Italian Armed Forces. OKW/Chi had also contact with the Italians. They used the machines G 247 and G 275 to communicate with the Italian Military Attaché. (TICOM 1950a)

On 1 August 1946, Dr. Erich Hüttenhain and Dr. Walter Fricke delivered a piece of "homework"(TICOM 1945a) on the *Zählwerk* Enigma that they had been tasked to do while they were kept at CSDIC (UK)[19] for extensive and in-depth interrogations. Drs. Hüttenhain and Fricke were normally good and well-informed witnesses on German cryptology, but their report shows clearly that they had very little knowledge of the Enigma G. They are not quite sure how the machine worked. They cannot remember if the fourth wheel, the reflector, was driven or not and on the number of rotor notches they believed it varied from 7 to 13 instead of the correct numbers, from 11 to 17. Or were they perhaps thinking about the Hungarian Enigma G machines that had five rotors and where the rotor V had seven notches and rotor IV most likely had nine. If so, does this mean that OKW/Chi was working on the Hungarian Enigma G traffic?

19. CSDIC was the "Combined Services Detailed Interrogation Centre", a set of facilities run by the British War Office (specifically MI19) between 1940 and 1948.

They mention that the Enigma G is more secure than the Enigma K, and that the simpler method of breaking Enigma K cannot be used against the counter Enigma. Interestingly enough they mention that when the weaknesses of the *Zählwerk* Enigma became known the idea of adding a plugboard (*Steckerbrett*) to the machine was turned down. To increase the security procedural changes were adopted instead. Hüttenhain and Fricke mention two proposed changes:

a) Double enciphering of each plain text. The basic wheel settings for the second encryption would be kept the same for the complete day.
b) First enciphering the plain text using a simple columnar transposition with a numerical key for selecting the order of the columns.

Here their information is correct, probably because it was a relatively new development, autumn 1944, and something they probably had learned directly from *Regierungs-Oberinspektor* Fritz Menzer (1908–2005), (Mowry 1983) who at this time had become seriously concerned about the security of the G31 machines. BP came across the use of this method on 20 October 1944, on the *Abwehr* link between Berlin and Madrid. BP did not immediately discover what prevented breaking the traffic but on 31 October it was discovered that the messages had first been enciphered on the key of 20 October before it was again enciphered on the key of the 31st. But it was also discovered that before any encipherment on the Enigma G the plaintext was first transposed using a cage or rectangle of four 5-letter groups, a width of 20 letters, that was filled in with the text before the columns were read out and double enciphered on the Enigma G. This would of course remove all word and bigram statistics from the plaintext and prevent using cribs to solve the message. (Batey et al. 1945)

Hüttenhain and Fricke then attempt to give some information about the operational use of the machine, however here their ignorance is again evident. They say only a small number of Enigma G machines were made, approximately 100 units in their estimation, while we shall see that more than 300 machines were produced. Then they mention that two years previously, which would mean some time in 1943, the Enigma G machines used by the German military attachés were withdrawn from use and replaced with *Heeres* Enigma machines with *Stecker*. This is quite possibly true. We know that the military attachés used specially wired *Heeres* Enigma machines for their communications towards the end of the war, but we still know very little about

what cryptological systems they used before and at the beginning of the war. However, Hüttenhain and Fricke then claim that Ag WNV/Fu collected all the machines previously used by the military attachés and gave the machines to the *Abwehr*. They add that they don't know if the *Abwehr* took the machines into operation. It is quite possible that the military attaché machines were offered to the *Abwehr*, but *Abwehr* started to use Enigma G well before 1943.

Dilly Knox made his first break into the Enigma G machines used by the *Abwehr* at the end of October 1941 and the first message was broken and deciphered on 8 December 1941. (Batey et al. 1945; Batey 2009) Internal documents from the Enigma company H&R show that the rotor wirings for the main *Abwehr* machine used in Europe, called Group II by BP, were dated 12 March 1940. However, it is most likely that a previous version of the Group II machine dates from 19 June 1939. This matches well with the knowledge that in July 1941, Dilly Knox took over an accumulation of *Abwehr* traffic dating back to December 1939. (Batey et al. 1945) Other Enigma G machine wirings date from August 1936 and December 1938, but if these were for the *Abwehr* or some other users is not known.

To better understand the *Abwehr's* need for and use of cipher machines it is interesting to take a closer look at their communications. From very early on *Abwehr* had an extensive communication network both inside Germany, in the occupied territories and abroad in the neutral countries. Fritz Staritz, who was a radio operator with *Abwehr* during the war, has estimated that they had 80 officers, 730 non-commissioned officers and 1850 radio operators. (Staritz 2018) Both radio and wire communications for all *Abwehr* departments were managed by Section (*Referat)* Ii under the command of *Oberstleutnant* Rasehorn, who was replaced in March 1944 by his deputy Major Theodor Poretschkin (1913–2006). This move was probably linked with Hitler's order of 12 February 1944, that *Abwehr* should be taken over by the *Reichssicherheitshauptamt* (RSHA) and integrated into their Amt Mil. However, Major Poretschkin did not become the commanding officer of Mil E, the new communication section, as planned; instead *Oberstleutnant* Wilhelm Boening (1897–?) was installed as the combined leader of Mil E, F and G. Major Poretschkin became Boening's deputy and later he received the command of *Nachrichten-Regiment* 506 (NaRgt. 506) when that was created on 15 September 1944. (Kampe 2008) Mil E was the administrative section and can be said to have existed in name only. The real work of running the communications of the Mil Amt (*Abwehr*) was done by NaRgt. 506 with

headquarters at Stahnsdorf in the district of Teltow in Berlin. In March 1945 they moved to Eisenberg in Thuringia before finally ending up at Obing in Bavaria. Altogether *Abwehr* operated close to 40 large radio stations in Germany, the occupied territories and abroad. The principal station for administrative traffic was the station codenamed BURG at Belzig near Dessau, Stahnsdorf had a local station called SCHLOSS, while the other main stations were at Hamburg-Wohldorf (DOMÄNE), Wiesbaden (WILJA), Köln (KONRAD) and Sigmaringen (SONJA). Stations communicating with the *Abwehrstellen* (Asts) of the army groups and armies on the Eastern Front were at Nikolaiken (ATLAS) and at Sulejowek (WALLI) east of Warsaw. Of the stations abroad the most important were Madrid (SABINE), Lisbon (LINA), Rome (TOGO), Merano (JACOB), Paris (PAUL) and Vienna (WERA). In addition to these main stations some of them operated secondary field station working as relays for traffic to more distant regions. Hamburg-Wohldorf (DOMÄNE) had such stations at Arachon, Cherbourg and Libourne in France, while OTTO, the *Abwehr* station in Oslo, controlled five field stations in Norway. The person responsible for issuing callsigns, frequency plans and code and cipher material for all *Abwehr* communications was *Oberleutnant* Alfons Oesterle (1914–?) based at Stahnsdorf. He was working in close collaboration with *Regierungs-Oberinspektor* Fritz Menzer of OKW/Chi on all questions of cryptography and *Oberleutnant* Heine of OKW/WNV/Fu III concerning *Funkabwehr* — radio counter intelligence. (Wenzel 1946)

The communications of the internal *Abwehr* network were enciphered with the use of the Enigma G. At the end of the war they started using the *Schlüsselgerät 41* (SG 41), the KD Enigma, an Enigma K equipped with the pluggable UKW D and specially wired rotors with nine notches, and in a few cases *Heeres* Enigma machines. The stations communicating directly with *Abwehr* agents used a variety of hand ciphers, both substitution and transposition ciphers and in a few cases specially wired Enigma K machines; while for communicating with agents in South America, where controlling stations in Mexico, Chile and Argentina handled the traffic, they used hand ciphers, the Kryha machine and the Enigma G. (Marks 2011)

Abwehr had from early on networks in South America; Brazil, Chile and Argentina were countries with large networks, but which generally were rather unproductive and that also quickly were broken up or greatly reduced by the authorities in the three countries. (Mowry 2011) In Argentina the *Abwehr* and the *Sicherheitsdienst* (SD) ran three joint networks that they called *Grün* (Green), *Rot* (Red) and *Blau* (Blue). The

Enigma G machines used by these networks were therefore called Green, Red and Blue by BP and US Coast Guard Unit 387, that worked on breaking the machines and deciphering the traffic. (Batey et al. 1945; US Coast Guard 1945)

Two of the *Abwehr* machines called Green had the serial numbers G 227 and G 228. These two machines were wired on 10 July 1943, but the rotor wirings Ch. 15 Tz 125 a – c, was most likely created in 1939 while the UKW, Ch. 15 Tz 115, is dated 14 July 1936. This mix of newer rotor wirings with older UKW wirings is typical characteristic for the Enigma G machines. The reason is of course that there seems only to have been five different UKW wirings, the oldest being the commercially wired UKW, Ch. 15 Tz 70, from 1931 and the youngest, Ch. 15 Tz 132, from 14 March 1940. (TICOM 1945b)

The two other G31 machines used in Argentina were called Red and Blue. The wiring of the Blue machine was never recovered by BP or US Coast Guard Unit 387; however, the wiring of the Red machine was recovered cryptanalytically by both BP and Unit 387. Three of the machines are known, G 209, G 260 and G 263, but the drawing IDs for the rotor wirings are still unknown. Curiously enough the Red machines used the commercial UKW, Ch. 15 Tz 70. The first of these machines to be prepared for service was G 209 and this was also the first Red machine to arrive in Argentina. G 209 was a machine with commercial wiring that we believe had previously been sold to the Dutch and then recovered by the Germans when they occupied the Netherlands. The order for the preparation of this machine, dated 4 August 1943, mentions that the machine should be checked out and rewired according to the drawing submitted to chief engineer Willi Korn. The order for the wiring of G 260 and G 263 came one week later on 11 August, with the instructions to have them wired like G 209.

Initially the communications using the new Red machine G 209 could not be deciphered by the agents in Argentina because Berlin made an error and enciphered the messages on a machine with the Red rotors but with a different UKW, Ch. 15 Tz 115 — the Green UKW. Initially BP and Unit 387 thought the Red rotors had been put into a machine with a wrong UKW, but later it would turn out that Berlin had used an altogether existing but wrong machine. This became apparent when it was discovered that the SD in Europe used a machine with the Red rotors and the UKW Ch. 15 Tz 115. The first use of this machine was observed in the summer and autumn of 1944 on a SD link between Berlin and Tirana. In the later part of the war this

machine also occurred in SD traffic between Berlin and Madrid.

The UKW, Ch. 15 Tz 115, was used in many of the specially wired Enigma G machines. It was used in two series of machines with serial numbers G 312 – G 317 and the machines G189 – G 194. These two series have different rotor wirings but share the same UKW. If these machines were used by *Abwehr* or other users is so far not known. In total the UKW, Ch. 15 Tz 115, was used in at least ten different sets of machine wirings.

The Last Days of Enigma G

Enigma G was only made in relatively small numbers; the first machine was G 101 and the machine with the highest serial number that has been found in the available documents is G 426. It is therefore likely that less than 350 machines were produced. The design of this machine with a large number of gear wheels was undoubtedly an expensive machine to produce under war conditions. H&R also expressed this view in a letter to OKW/Chi dated 23 February 1943. The letter presents H&R's latest secret patent, C 58002 IX b/42 — C 8511 Gm 42 n, for their invention of a new and improved pluggable reflector, an improved UKW D, that the authors, for lack of a better name, have decided to call UKW Plus. The new reflector would have the following important advantages:

a. The possibility of connecting freely all available reflector contacts by cables to form 13 reflector pairs.
b. The reflector is settable in all its 26 different position with respect to the other rotors.
c. The reflector is driven during operation exactly like the other rotors.

They stress that their new pluggable reflector has full freedom of connections and it is not limited to only 24 contact points as on UKW D. This means that UKW Plus also can produce the connections of the fixed UKW B and therefore allow machines with the new reflector to be fully compatible with older machines using UKW B. They think their new invention will be of interest for use in the existing *Heeres* and *Marine* Enigma machines as well as in the Enigma K and Enigma T machines already introduced into the Wehrmacht.

They even suggest that for Enigma machines equipped with a plugboard (*Steckerbrett*), rotors with variable notches (*Lückenfüllerwalzen*) and the new driven, settable and fully pluggable reflector the need for the extra rotors IV and V may no longer be present. The basic machine will have sufficient cipher security even without the extra rotors. Furthermore, they pose the question if it now is not advisable to use the same new Enigma model for both the Army and the Navy. They say the advantage of such a standardisation is obvious.

They propose to push the standardisation even further and also to use UKW Plus in the Enigma K machines that are used for Wehrmacht purposes, because apart from

the plugboard these machines are, in most parts and construction, identical to the *Heeres* Enigma. And for the Enigma G, that so far has been used for special purposes and which production in war time with the small quantities needed is now longer profitable, they propose that these machines also can be replaced by the new machines with UKW Plus.

What reaction H&R's proposals got at OKW/Chi is unfortunately not known and their new invention UKW Plus seems not to have been realised, at least not in a Wehrmacht machine. However, H&R's ideas for standardisation was also the wish of OKW/Chi and at the end of the war plans for a new and standard Wehrmacht rotor machine were in various stages of development. Perhaps somebody also noticed H&R's comment about the unprofitable production of Enigma G under war time conditions. Nine months later, on 17 November 1943, H&R and K&K both received a letter from the Plenipotentiary for Technical Communication Equipment (*Der Generalbevollmächtigte für technische Nachrichtenmittel, GBN*) informing them that in a meeting of the users of the Enigma it was decided, as a move towards a unified production of the Enigma cipher machines, to immediately stop the production of the Enigma G and Enigma K machines. The 180 Enigma T machines still in production would be finished and delivered by end of January 1944. Production stopped but existing machines, both Enigma G and K, were repaired, rotors rewired etc. until the end of the war.

Due to the small number of Enigma G machines produced and the very small number of machines that survived the war the machine never had post-war use, with one known exception. The Dutch Naval Enigma G machines continued to be used after the war. It is known that the machines were in use at least until the end of the 1950s. It is reported that most of the Dutch machines were destroyed sometime in the 1970s; today only seven machines are left in Dutch government collections. If the Hungarian machines saw any post-war use is not known.

The History of G 110

Enigma machine G 110 was acquired by the Bletchley Park Trust (BPT) in 2016 from a private individual who had in turn bought it from a source in Poland. The machine was apparently discovered in southern Poland near the Czech border, allegedly dug up in a farmyard. Unfortunately it was not possible for BPT to verify the exact location or circumstances of its discovery, or indeed how many hands it passed through before being acquired by the Trust. However the details of the object itself, and the numbers and markings revealed during the conservation process allow some of the history of the object to be reconstructed.

When G 110 fell into the hands of Bletchley Park it was in rather poor condition. Its provenance suggested that it had been buried in the ground for around 70 years. When it was received at Bletchley it had not been subject to any systematic cleaning or conservation and bore the traces of its sojourn as a buried archaeological object. It was significantly corroded, and still contained areas of compacted mud and organic debris, particularly in its interior. After a short period on display at Bletchley Park in its unrestored condition the decision was made to have the machine professionally cleaned and conserved. This would serve a number of purposes;

- The condition of the machine could be stabilised and further decay prevented as far as possible.
- Detailed examination of the surviving parts of the machine might reveal useful information about its origin and history (which was indeed the case).
- The machine would be more suitable for public display in its conserved state.

The machine was passed to Ian Clark Restoration, a company of specialist conservators with particular expertise in industrial and maritime machinery collections, as well as conservation of decorative metalwork. In total over 100 hours of conservation work was carried out on the machine. Despite its rather unpromising initial appearance the conservator found that the machine was 'surprisingly stable and did not show any immediate signs of structural failure or loss of physical integrity.' Allowing for the time it had spent buried he observed that it had survived 'remarkably well.' (Clark 2018)

However, it did show signs of having been deliberately disabled prior to being disposed of at the end of its working life. In particular the three encryption rotors and

the reflector had been removed from the machine and discarded separately, presumably for reasons of cipher security. It is possible that this had been carried out with some force, as the right-hand pawl and ratchet wheels and the *Eintrittwalze* had become detached from the machine frame and were loose in the body of the machine, retained only by the wiring loom. The counter mechanism on the right-hand side along with the battery and its connecting wires were also absent. The glass from all the bulbs on the lamp board was missing, along with the translucent letter panels, although the aluminium(?) lamp board itself was still in good condition. Most of the keys were in situ, and their labels legible, although the lenses were cracked and discoloured. Only the 'F' and 'H' keys were missing from the central key row. The machine was also lacking its original wooden carrying case.

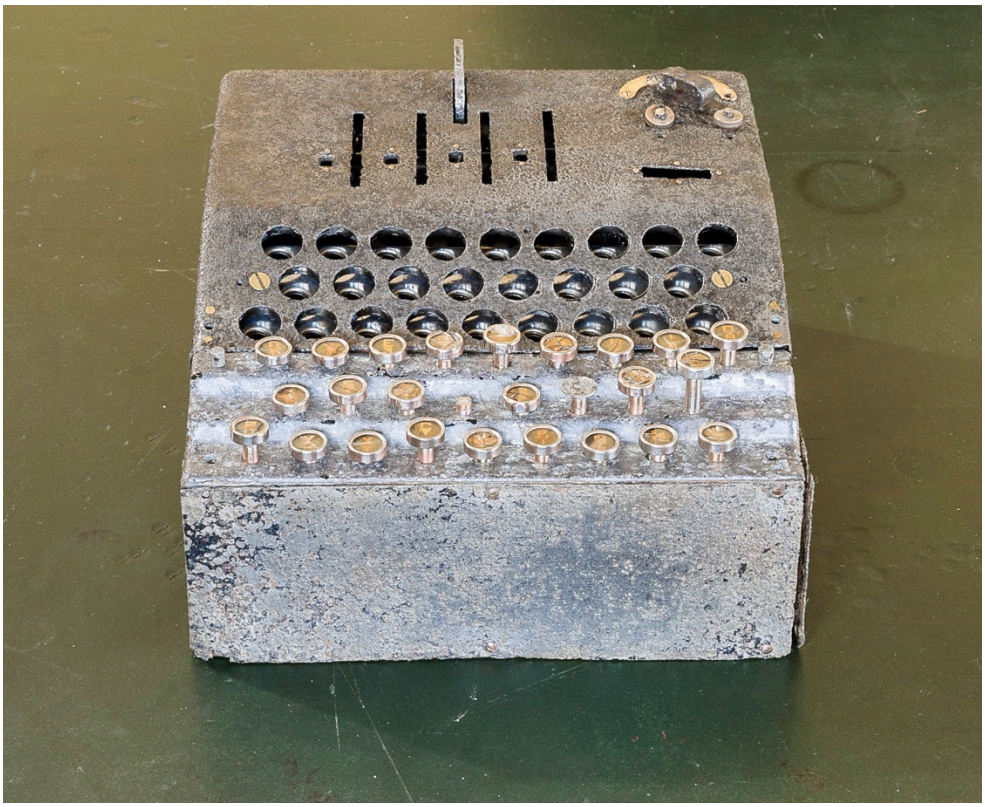


Figure 7. The restored Hungarian machine G 110 in the collection of the Bletchley Park Trust. Photo © 2019 Will Amlot, courtesy of BPT.

The machine was first mechanically cleaned using brushes, scalpel and bamboo picks, to remove as much as possible of the organic debris. This was followed by careful disassembly of the machine where possible to allow further cleaning and assessment of the individual components. The principal parts of the machine were then subject to repeated sequences of immersion in Biox Liquid for periods of up to 4 hours and

washing with de-ionised water. Biox is a biological oxide corrosion remover, completely harmless to humans and containing no strong acids or alkalis. It is used by conservators for the sympathetic removal of rust, tarnish and Verdigris from iron, copper, brass and aluminium objects. After this process was complete the surfaces were sealed with several coats of micro/crystalline wax. The non-ferrous parts of the machine such as the keys, lamp board, switch labels and internal parts such as the plug socket and drive mechanism were also cleaned and polished using Autosol metal polish before receiving their own coat of wax sealant. The machine was then reassembled, including refitting the *Eintrittwalze* and its drive wheels in their correct position.

The results of this process were readily apparent when the machine was returned to Bletchley Park. What had been a brown rusty box was now clearly a cipher machine. Most of the original lacquer on the exterior of the machine had been lost due to corrosion so the object was now the dark grey colour of the underlying steel, however internally much more lacquer had survived allowing the original black colour to be seen on many of the components. More significantly a number of markings had also been revealed during the cleaning process;

- The interior of the left-hand side of the case, immediately above the printer socket assembly was inscribed "Chiffrier M38".
- The interior floor of the case underneath the lamp board was inscribed "CH M47".
- Externally on the underside, the base was inscribed "110".

Examination of the machine, both before and after conservation, led to the conclusion that it is one of the G31 Series of machines, in addition the presence of the printer socket on the on the left-hand side, strongly suggests that it was one of the "*Zählwerk und Kupplung*" machines within this series. The third inscribed number listed above is of most significance, leading the authors to conclude that this is Machine G 110, one of the series of machines G 101–G 124 delivered to Hungary in 1931 as described earlier. If this is the case it makes this a very rare Enigma. Only one other of this type; G 111 has been identified and this passed into a private collection after auction in 2009, leaving the Bletchley Park example as the only one on public display.

It is difficult to reach any firm conclusions concerning the wartime life of this machine or which part of the Hungarian armed forces or intelligence services used it. All that

is known is that it was sold to Hungary in 1931 and found its way later to a farmyard in southern Poland. If it was in use by the Hungarian army, this location is broadly consistent with the final battlefields of the Hungarian First Army. This force was almost completely destroyed alongside the German First Panzer Army in fighting against the Soviets in January 1945 along the borders of modern Slovakia, the Czech Republic, and Poland. The deliberate disassembly of the machine and its burial are consistent with its disposal by a retreating or surrendering signals unit at that time. At present, however this narrative remains purely speculative.

Acknowledgements

The authors are very grateful to Anders Wik for giving them access to copies of documents related to the early Enigma developments from the Swedish archives. The second author should also like to thank Philip Marks and Ralph Erskine for the many in-depth discussion about Enigma G, *Abwehr* and other Enigma related topics over a great many years. He should also like to thank the Historian of GCHQ for discussion about the Enigma machines bought by the UK in the late 1920s and Andreas Willemsen for information and documents from the Dutch Naval Archives. Furthermore, he is indebted to Claus Taaks for sharing the results of his research on the Enigma companies and their leading personalities and for the many years of discussions about the early Enigma history.

About the Authors

Dr. David Kenyon is the Research historian at Bletchley Park. He is responsible for historical research in support of all content and public output from the site. He worked for a number of years in archaeology before completing his doctorate in military history in 2008 and moving into museums and heritage work. In addition to cryptography and intelligence his interests include 20th and 21st -Century military history, tactics and technology.

Frode Weierud is a retired electronics engineer formerly employed by the European Organization for Particle Physics (CERN) in Geneva. Cryptography has been his main interest for more than 50 years. His cryptological research is focused on cipher machines and cryptanalytical techniques combined with a deep interest in all historical aspects.

References

Batey, J. K., M. L. Batey, M. A. Rock, and P. F. G. Twinn. 1945. GC&CS Secret Service Sigint Volume II: Cryptographic Systems and their Solution. I – Machine Cyphers. HW 43/7. The British National Archives, Kew, London.

Batey, M. 2009. *Dilly: The Man Who Broke Enigmas*. London: Dialogue.

Chiffriermaschinen AG. 1928. Bericht über das sechste Geschäftsjahr der Chiffriermaschinen Aktiengesellschaft, Berlin, 1928. R8127, 6937. Bundesarchiv, Berlin.

Chiffriermaschinen AG. 1929. Schaltungsanordnung für elektrische Leitungen von Chiffriervorrichtungen. Secret German Patent: C 38582 IX/42n, filed August 9, 1928, and issued May 16, 1929.

Clark, I. 2018. Conservation Report, Bletchley Park Trust G31 Enigma Machine. Ian Clark Restoration, Winchester, Hampshire. Unpublished

Crypto Museum. 2019a. Enigma G-111. Accessed February 3, 2019. https://www.cryptomuseum.com/crypto/enigma/g111/index.htm

Crypto Museum. 2019b. Hungarian H-221. Accessed February 3, 2019. https://www.cryptomuseum.com/crypto/enigma/h/index.htm#hungary

Deavours, C. A. 1997. Lobsters, Crabs, and The Abwehr Enigma. *Cryptologia* 21(3): 193–99. doi: 10.1080/0161-119791885904.

Foss, H. 1928. The reciprocal ENIGMA. HW 25/14. The British National Archives, Kew, London.

Hammarborg, A. 1954. Catalog of Enigma Cipher Machine Wirings. Technical Information Division, Bibliographic Research Branch. NSA FOIA Release, Doc ID: 3220592. National Security Agency, Ft. Meade, Maryland.

Kampe, H.-G. 2008. *Das militärische Fernmeldewesen Deutschlands im Zweiten Weltkrieg 1939-1945*. Vol. IV of *Handbuch zur Geschichte des militäriscen Fernmeldewesens*. CDs in PDF format. Berlin: Dr. Erwin Meißler.

Kolisch, J. M. 1946. First Detailed Interrogation Report of Lieutenant Colonel Franz Seubert, Abwehr. RG 263, 640447, Box 36, Folder 2, MIS Austria: SO65/USDIC/DC5. NARA, College Park, MD.

Korn, W. 1933. Chiffriervorrichtung mit Chiffrierwalzen. German Patent: DE579555, filed November 17, 1928, and issued July 3, 1933.

Korn, W. 1931. Elektrische Chiffrier- und Dechiffriervorrichtung. German Patent: DE534947, filed November 9, 1928, and issued October 6, 1931.

Marineleitung. 1926a. M.Dv. Nr. 33 Allgemeines Funkspruchbuch. RM 6/623. Bundesarchiv, Militärarchiv Freiburg.

Marineleitung. 1926b. M.Dv. Nr. 21 Der Funkschlüssel C. RM 6/596. Bundesarchiv, Militärarchiv Freiburg.

Marks, P. 2011. Operational Use and Cryptanalysis of the Kryha Cipher Machine. *Cryptologia* 35(2): 114–55. doi: 10.1080/01611194.2011.558978.

D. P. Mowry. 1983. Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire. *NSA Cryptologic Quarterly* 2(3-4): 21–36. Accessed April 6, 2019. https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/Regierungs_Oberinspektor.pdf

Mowry, D. P. 2011. Cryptologic Aspects of German Intelligence Activities in South America during World War II. Center for Cryptologic History, Series IV, World War II, Volume 11, National Security Agency, Ft. Meade, Maryland. Accessed April 6, 2019. https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/cryptologic_aspects_of_gi.pdf

Ostwald, O., and F. Weierud. 2016. History and Modern Cryptanalysis of Enigma's Pluggable Reflector. *Cryptologia* 40(1): 70–91. doi: 10.1080/01611194.2015.1028682.

Schmeh, K. 2010. Alexander von Kryha and His Encryption Machines. *Cryptologia* 34(4): 291–300. doi: 10.1080/01611194.2010.485440.

Staritz, R. F. 2018. *Abwehrfunk – Funkabwehr: Technik und Verfahren der Spionagefunkdienste*. Bamberg: Unpublished.

Swedish General Staff. 1924. Chifferapparaten Enigma. Bearbetningsbyrån F V:1. FRA Archive, Försvarets Radioanstalt, Bromma, Sweden.

TICOM. 1945a. I-77: Translations of joint report made by Drs. Hüttenhain and Fricke on the "Zaehlwerk" Enigma machine. NSA FOIA Release, S-4577. National Security Agency, Ft. Meade, Maryland.

TICOM. 1945b. ENIGMA Documents from Chiffriermaschinen Gesellschaft Heimsoeth & Rinke. Bestand Rückgabe TICOM: T 1715, T1716, T1717, T1718. Politisches Archiv des Auswärtigen Amts, Berlin.

TICOM. 1950a. DF 190-AM: Enigma Machines in Foreign Countries. RG 457, Series P-4, File 5789, DF 190-AM. NARA, College Park, MD.

TICOM. 1950b. DF 190-Z: Question on Enigma Cipher Wheel II G 208. RG 457, Series P-4, File 5789, DF 190-Z. NARA, College Park, MD.

Trevor-Roper, H. 1942. Letter to Commander Travis and report from Lieutenant Stuart Hampshire. HW 14/62. The British National Archives, Kew, London.

US Coast Guard. 1943. The German Armistice Commission Enigma. NSA MDR Release, S-418, Doc ID: 3597211. National Security Agency, Ft. Meade, Maryland.

US Coast Guard. 1945. History of Coast Guard Unit #387 1940–1945. RG 38, Crane Inactive Stations, Box 57, 5750/2. NARA, College Park, MD.

Wenzel, G. 1946. CI Final Interrogation Report of Oberleutnant Alfons Oesterle, NaRgt. 506. RG 238, 6242123, NM-70 160, MIS, CI-FIR/100. NARA, College Park, MD.

Wik, A. 2018. The First Classical Enigmas: Swedish Views on Enigma Development 1924-1930. In *Proceedings of the 1st Conference on Historical Cryptology*, ed. Megyesi, B., 83–88. Uppsala, Sweden: Linköping University Electronic Press. Accessed April 6, 2019. http://www.ep.liu.se/ecp/contents.asp?issue=149.