Preface to the article “Cryptographic design flaws of early Enigma.”

The “Enigma” cipher machine and its cryptanalysis form a central piece within the history of cryptology. After its invention by the German Arthur Scherbius (1878–1929) in 1918, it went through an eventful and tortuous development history during the next decade before, on 1st June 1930, the finally revised standard version of Enigma I was officially put into service by the German Army.

This article is about the early years (1918–1930) of the Enigma. It illustrates its development story with a particular focus on design flaws by which its cryptographic strength was significantly weaker than it could have been.

The article was inspired by the occasion of the International Conference on Historical Cryptology (HistoCrypt) held in June 2023 in Munich, Germany. This date coincided with the 100th anniversary of Chiffriermaschinen Aktiengesellschaft (ChiMaAG)—“Cipher machines joint-stock company,” founded on 9th July 1923 in Berlin, Germany, to fabricate the Enigma.

The article was intended as a companion paper to “Scherbius and the Enigma” by Claus Taaks. His writing focuses on Enigma's development story's fascinating political, economic, and military aspects during the 1920s. The origins and first years of the invention are described with a focus on the courageous and enterprising inventors, successes, failures, fraud, and embezzlement embedded within the political environment during this remarkable decade in Germany. The technical cryptography of the cipher machine was intentionally left out and should be described in a companion paper.

While the article “Scherbius and the Enigma” has been accepted for presentation at the HistoCrypt 2023, the program committee did not select the companion paper for publication in the proceedings. Hence, it is presented here for all readers interested in some cryptologic details of the early Enigma.

On 24th May 2024 the author was informed through an email sent to Frode Weierud, who forwarded it on the same day, that Suzanne Carter, who is working with Bletchley Park, spotted a flaw in the way the figure of unique rotor start positions was previously calculated. According to her analysis only 650 have to be subtracted from the 17,576 possible ones, 26 fewer than the previously calculated 676, amending the formerly stated 16,900 to 16,926.

Cryptographic design flaws of early Enigma

Olaf Ostwald

5 April 2023 (revised 7 June 2024)

Abstract

The principal topic is the early glow lamp Enigma machine and its cryptographic weaknesses. Development started with a few first prototypes in 1918, mainly driven by the German businessman and engineer Arthur Scherbius. It was continued after the foundation of *Chiffriermaschinen Aktiengesellschaft (ChiMaAG)*—"Cipher machines joint-stock company" on 9th July 1923 with the aid of chief engineer Willi Korn in the 1920s and resulted in the German Army Enigma machine.

In this paper some design flaws are illustrated, and the reasons why they occurred are explained. Possible alternatives which could have avoided or at least reduced such flaws are described.

On 1st June 1930, the finally revised standard version of Enigma I was officially put into service by the German Army.

1 Introduction

The focus here is on the cryptographic methods on which Scherbius' rotor machine was based, and how they evolved and were implemented.

A short chronological overview of Enigma's early design story is given in section 3. Several important events will be briefly considered, for instance, patents that influenced its cryptographic design. In section 5, several options are described on how an alternative Enigma could have been designed cryptographically stronger. The suggestions are not speculations or ideas of the author but are based on contemporary ideas of German cryptographers or Allied codebreakers.

The focus will not be on technical differences between models, such as Enigma A, B, C, D, G, H, or K, or their individual histories. These have been described in detail e.g., by Hamer et al. (1998), by Kruh and Deavours (2002) (with erroneous assignments for Enigma A and B), by Wik (2018), and by Kenyon and Weierud (2020).

2 Procedural Errors

Moreover, the focus is not on espionage, treason, and human blunders. A good cipher system should be robust against it. It is also not on the encipherment procedures or procedural mistakes. Many of those occurred. To mention just a few:

(1) Quarterly change of rotor orders: The very rare exchange of rotors and rotor orders, which happened just once within three months until 1st February 1936.

(2) Non-clashing rule: The creation of a rule that a certain rotor should never be used at the same position within the scrambler on two consecutive days. By this, the number of available rotor orders was drastically reduced. This helped to save precious *Bombe* time at Bletchley Park (B.P.).

(3) Six plugs only: The use of only six plugs until 1st October 1936 was a mistake that could very easily have been avoided. Through this error, the cryptographic potential of the reciprocal, and thus already weakened, plugboard was further reduced. Most of the 26 letters remained "unsteckered," by that enabling the early cryptanalytic attacks with the aid of the Polish *grill method*, which relied on unplugged letters. This attack would not have succeeded if at least ten plugs had been used from the beginning.

Also, later, the Polish *Bomba* was based on the fact that the plug connections did not change all the letters. Hence, for Enigma, avoiding any unplugged letters would have been better.

A codebreaker is hindered not by a high number of plugging possibilities, but by the maximum number of swapped letters. With only a few exceptions, 13 plugs were never used, possibly because of space restrictions: It was not easy to arrange the cords between the plugs to be able to close the front lid.

Despite all this, the attack through the Polish *Cyclometer* as well as the British *Bombe* would not have been affected even by 13 plugs.

(4) Doubling the message key: This was a gross error which allowed Marian Rejewski (1940) to break into Enigma as early as 1932. The erroneous procedure was finally abandoned by the German Army as late as 1st May 1940.

Such procedural mistakes may certainly not be denoted design flaws of the machine. They could have happened also if Enigma had been designed cryptographically much stronger. And this would have been possible: Gordon Welchman (1982), one of the leading figures at B.P., wrote in his book *The Hut Six Story*: "modifications in the design of the Enigma could have defeated us completely in spite of the procedural mistakes."

But how could such a modified Enigma have looked like possibly from the beginning? It's easy to be wise after the event. Today we are in a comfortable position: It is known that Enigma could be broken and indeed had been broken, and one knows, how this was done. From that it is possible to give specific suggestions for improvements to strengthen Enigma against the now-known cryptanalytic attacks. In principle, such improvements could have been implemented already during the 1920s.

3 Timeline (1918–1930)

3.1 The Year 1918

On 23rd February 1918, Arthur Scherbius (1878–1929) applied for German patent DE416219 *Chiffrierapparat*—"Cipher apparatus." The name "Enigma" was not yet chosen in 1918. The first prototypes had a keyboard and lamp board with 25 letters each, omitting the letter J. The lamps and the keys were both arranged in a 5×5 matrix. One of the prototypes, intended for demonstration, had two rotors. Back then, the rotors were called "rolls," and later then, "wheels." Another prototype had seven rotors. Arthur Scherbius relied on the concept:

security through a high number of rotors.

Already in his fundamental patent, Scherbius had calculated the key space for different numbers of wheels: "with ten wheels, one gets more than 95 trillion." In fact 25 to 10th power yields 95,367,431,640,625, an impressive number. Two demonstrations of the prototype with two rotors took place still during WWI. One at the Grand Headquarters in Spa shortly after the 15th of April, and another around 10th May 1918 at the *Reichsmarineamt*—"German Imperial Naval Office" in Berlin (BArch MA, RM 5/3566).

During the meeting in the Naval Office, Scherbius and his companion Richard Ritter (1882–1936) explained that the number of available permuted cryptographic alphabets corresponds with the number of rotors used within the machine. They gave the following examples:

2 rotors yield 25^2 or 625 alphabets,

7 rotors yield 25^7 or $6.10 \cdot 10^9$ alphabets,

10 rotors yield 25^{10} or $9.53 \cdot 10^{13}$ alphabets,

12 rotors yield 25^{12} or $5.96 \cdot 10^{16}$ alphabets.

On request of the Naval Office, a short time later, they produced four ciphertext samples from a plaintext containing nothing else but 625 times the letter N. This time they utilised one of the other glow lamp machine prototypes, which had seven rotors. As requested by the Navy, the keys for the four ciphertexts were only slightly different, such as TFLXHKL and TFLXIKL. The Naval Office inspected the ciphertext samples, which apparently were completely different, and was highly satisfied.

Shortly after this episode, Scherbius unexpectedly experienced practical problems caused by the oxidation of the wheel contacts. This effect was especially dramatic when using as many wheels as seven. It turned out that a machine, when using such high numbers of rotors, was not reliable. On 2nd June 1918, patent DE416833 was claimed as an addendum to DE416219, describing the oxidation as a technical disadvantage, and suggesting a pneumatic or hydraulic solution.

Another problem he probably observed, is the mechanical friction between the many rotor contacts. A machine with many rotors would be heavy and hard to operate by hand. This urged him to limit the number of rotors to three or four at the most. Reluctantly Scherbius had to drop his original concept idea of s*ecurity through a high number of rotors*. Hence other measures had to be found to strengthen the machine.

3.2 The Year 1920

During the year 1920, one idea was to implement something in addition to the permutation caused by the rotors, thus producing another level of complexity. A device named *Umwürfelung*—"reshuffling" was invented, which was intended for the printing cipher machines, not for the glow lamp machines. As described in patent DE 425147, it generated a transposition of the letters within a line, and even between adjacent lines.

3.3 The Year 1923

On 9th July 1923 *Chiffriermaschinen Aktiengesellschaft (ChiMaAG)*—"Cipher machines joint-stock company" was founded in Berlin to fabricate cipher machines.

Figure 1. The logo was created ca. 1924–5, after the name "Enigma" had been given in 1923.

Shortly afterwards, on 1st September 1923, an article entitled *Die Chiffriermaschine*—"The cipher machine," written by the journalist Fritz Hansen (1923a), was published in a weekly popular science magazine *Die Umschau*—"The look around." The commercial version *Handelsmaschine* of Enigma utilizing a typewriter as a printing device, and no glow lamps, was presented. In this article, the name "Enigma" can be seen, possibly for the first time. The article was reprinted in November of the same year in the monthly magazine *Der Radio-Amateur* (1923b).

On 29th November, Scherbius' article entitled *"Enigma" Chiffriermaschine* was published in *Elektrotechnische Zeitschrift*—"Electrotechnical journal." Again, the commercial printing Enigma, utilizing an irregular stepping controlled by gears, was presented.

3.4 The Year 1924

Finally, in 1924 the serial production of glow lamp machines started. The first model, called "Enigma A," was intended for military use, or perhaps dual use, and was also called *Die kleine Militärmaschine*—"The little military machine." In contrast to the big and heavy commercial writing Enigmas, this lightweight (5 kg) portable model provided no irregular stepping, but a simple odometer fashion. Furthermore, for the first time, a reflector was introduced, but patented by Korn only two years later.

3.5 The Year 1925

On 26th August 1925, the German Navy, *Reichsmarine*, secretly ordered 50 *Funkschlüssel C*—"Radio cipher C" machines, a special version of glow lamp Enigma C, including the umlauts Ä, Ö, and Ü, with 28 letter contacts on each rotor.

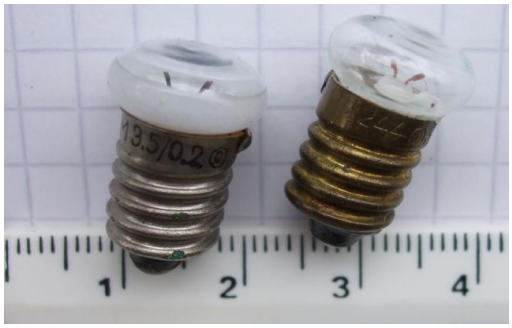


Figure 2. Glow lamps with flat tops, which were common back then, were used for Enigma.

3.6 The Year 1926

On 11th and 21st March 1926, Korn applied for German patents DE460457 and DE452194, describing his inventions of a reflector and an exchange of the rotors as well as their permutation within the scrambler. The latter two are splendid ideas, because both the combinatorial complexity of the machine and its key space were significantly enhanced. The reflector makes the Enigma cipher reciprocal. This eased the construction and operation of the machine as intended. Moreover, Korn also suggested it "so that the electric current arriving through the rotors returns again through the same rotors." By this, Korn hoped for increased cryptographic strength. After all, the current is now flowing through each rotor twice.

Korn's main intention was to avoid the encipher/decipher switch and thus simplify both construction and operation of the machine. Additionally, he wanted to virtually double the number of wheels, as the current is now flowing through each wheel twice, first on its way towards the reflector and afterwards back. By this, the reflector should also help to reduce the contact problems, that had been experienced when using seven wheels. The reflector should allow to half the number of wheels by using each wheel twice. Korn wrote:

"By this return of the current through the cipher wheel set, a further scrambling is produced. Because of this set-up, it is possible to use a relatively low number of cipher wheels and, despite it, maintain high cipher security."

This, however, is a fatal miscalculation. In fact, the reflector caused a significant weakening of Enigma's encryption. One result is that from now on, no letter could be enciphered as itself. Another is that by the reflector Enigma's encryption became reciprocal. What might be indeed

comfortable for the operator is, however, fatal for encryption security. Enigma without the reflector would have been harder to break.

From the cryptanalyst's point of view the seemingly complex flow of the current is not a decisive obstacle. Generally, in each position of the scrambler, it produces a single permuted alphabet. As an example of an arbitrary position of the wheel set, the constatations between the 26 plaintext letters A to Z (upper row) at the input of the scrambler and the corresponding ciphertext letters (lower row) at the output are shown in the table, here for wheel order B123 and wheel setting AAA:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
UEJOBTPZWCNSRKDGVMLFAQIYXH
```

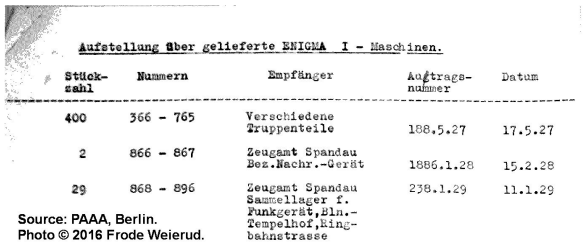
Table 1. Enigma's reciprocal cipher alphabet for wheel order B123 and wheel setting AAA.

As can be seen, this alphabet is reciprocal, which is true also for all the other Enigma alphabets. Here the letter A, for instance, is enciphered as U, and U is enciphered as A. This is what the scrambler produces, regardless of how complex the current flow may be, and regardless of how many wheels would be used. Of course, one gets different reciprocal alphabets at every single position of the rotors.

What indeed is an obstacle for a codebreaker, is the number of positions the wheels can assume, meaning the number of different alphabets of the scrambler. For three wheels with 26 letter contacts each, this number remains 26^3 or 17,576. This is precisely the same number with and without a reflector. Thus, contrary to Korn's opinion, "further scrambling" has no effect on increased cipher security, in contrast to what he had hoped for.

3.7 The Year 1927

The first 400 Enigma I series machines were ordered by the *Reichswehrministerium (RWM)*—"Reich Ministry of Defence" on 17th May 1927. ChiMaAG delivered the first 20 machines in August, the bulk of 300 during December, and the last 80 the month after, on the 6th. They were distributed to different units of the German Army. These machines had a *Schaltbrett*—"switch board." As investigated by Paul Reuvers and Marc Simons from Crypto Museum, this board consisted of 26 single pole sockets arranged in two adjacent circles with 13 sockets each.



Aufstellung über gelieferte ENIGMA I - Maschinen.

Stück-zahl	Nummern	Empfänger	Auftrags-nummer	Datum
400	366 - 765	Verschiedene Truppenteile	188.5.27	17.5.27
2	866 - 867	Zeugamt Spandau Bez.Nachr.-Gerät	1886.1.28	15.2.28
29	868 - 896	Zeugamt Spandau Sammellager f. Funkgerät,Bln.-Tempelhof,Ring-bahnstrasse	238.1.29	11.1.29

Source: PAAA, Berlin.
Photo © 2016 Frode Weierud.

Figure 3. First delivered Enigma I machines.

3.8 The Year 1928

The month of February 1928 turned out to be a pivotal one within the history of early Enigma. Three meetings took place in the *Chiffrierstelle*—"Cipher Office" of the RWM in Berlin on Tuesday 7th and 14th, and on Friday 17th of February. Besides practical aspects, such as where to store the leads within Enigma's wooden case, the principal topic was the design of the plugboard.

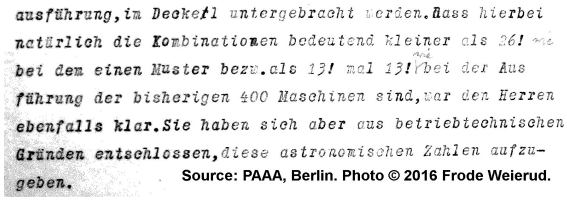
The original variant utilizing the said two-part circular arrangement (A to M and N to Z) with single-ended leads, with which the first 400 machines had been equipped, was discarded during the first meeting, and replaced by a second version with two times 26 sockets (A to Z). During the second meeting, this, however, was assessed as too complicated and error-prone.

The crucial meeting concerning Enigma's plugboard was the third one, on 17th February 1928. As before, five persons were present: Two officers from RWM, Major Georg Schröder and First Lieutenant Walther Seifert (1896–1982). (Five years later, both became leading figures in the *Forschungsamt*—"Research bureau.") They were accompanied by cryptologist *Regierungsrat*—"senior civil servant" Wilhelm Fenner (1891–1961). Elsbeth Rinke (1879–1960) and Willi Korn (1893–1972) represented the ChiMaAG.

The RWM people proposed a third version for plug connections, declared it their own invention, and decided to equip all future versions of Enigma I, intended for military use, exclusively with this new and secret device. This was the day when Enigma's famous plugboard was born.

All participants of the meeting were fully aware of the fact that this final version of the plugboard was weaker than the earlier versions; it also offered much fewer plugging possibilities (approx. 10^{14}) than the previous two. The first version allowed for $13!\cdot 13!$ (approx. 10^{19}) possibilities and the second one has even 26! (approx. 10^{26}) different plug connections. As stated in the memo from that day, written and signed by Korn and Rinke (1928):

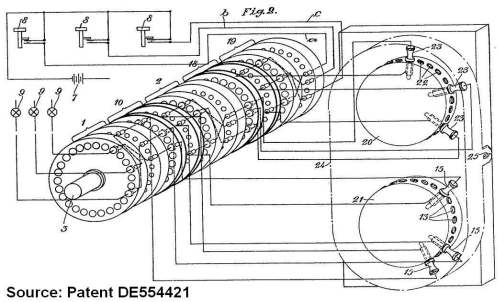
The representatives of the RWM, “for operational reasons,” however, decided “to abandon these astronomical numbers.”


ausführung, im Deckel untergebracht werden. Dass hierbei natürlich die Kombinationen bedeutend kleiner als 26! bei dem einen Muster bezw. als 13! mal 13! bei der Ausführung der bisherigen 400 Maschinen sind, war den Herren ebenfalls klar. Sie haben sich aber aus betriebtechnischen Gründen entschlossen, diese astronomischen Zahlen aufzugeben.

Source: PAAA, Berlin. Photo © 2016 Frode Weierud.

Figure 4. Abandoning “astronomical numbers.”

Shortly before, on 31st January, ChiMaAG had applied for patent DE554421 entitled *Elektrische Chiffriervorrichtung*—“Electrical cipher device.” The principal claim regards one or two pluggable stators newly inserted in between the rotors. Each stator would allow any arbitrary connection by means of pluggable leads, thus forming a non-rotating, however fully arbitrary, wired wheel.



Source: Patent DE554421

Figure 5. Pluggable stators between the rotors.

In July of the same year, for the first time, German Army radio messages utilizing Enigma were perceived by *Biuro Szyfrów*, the Polish Cipher Office. Since the Polish codebreakers could at first not achieve any significant progress, the work was abandoned for a while.

3.9 The Year 1929

In May 1929, Arthur Scherbius suffered a severe accident while manoeuvering with a horse-drawn carriage and was fatally injured. He died on 13th May. From now on, Willi Korn continued to drive Enigma's development forward.

3.10 The Year 1930

On 31st May 1930, Enigma with switchboard was put out of service, and the next day, 1st June 1930, the finally revised standard version of plugboard Enigma I was officially put into service by the German Army.

4 Enigma's Key Space

The number of different keys for Enigma I can be calculated as the product of four factors:

wheel orders × wheel settings × ring settings × plugboard settings

From a codebreaker's point of view, not all of the four factors are equally important. Generally, not the magnitude of a number is decisive, but how difficult it is to overcome it. In the case of Enigma I, only the first two are cryptographically strong. These are the number of wheel orders and the number of start positions of the wheels, called the wheel settings. Their product gives the number of available Enigma alphabets, and it poses a major obstacle when trying to break a ciphertext since no cryptanalytic shortcuts are known. Hence, if no additional information is available, all combinations of wheel orders and wheel settings must be exhaustively tested when trying to break a secret message.

The other two factors, given by the number of ring settings and plugboard setting, are weak. In fact, they are only slightly more than illusory complications. The codebreakers at B.P. knew about this fact. Without a doubt, Alan Turing and Gordon Welchman did know it. That's why the *Bombes* could be designed such as to completely overcome the plugboard settings and the ring settings. What remained to do at B.P. was an exhaustive key search for all 17,576 wheel settings for not more than 60 wheel orders. Several wheel orders could be filtered out with the aid of the non-clashing rule or by other means.

The precise number of how many different Enigma keys that can be chosen is not really important in order to assess Enigma's cryptographic strength. Nevertheless, one should know the correct number. For Enigma I, with ten plugs and three wheels being chosen out of a set of five, it is (Suzanne Carter, 2024):

$$5\cdot4\cdot3\times16{,}926\times26\cdot26\times150{,}738{,}274{,}937{,}250$$
$$= 103{,}484{,}623{,}446{,}804{,}960{,}360{,}000$$

If we look back at Enigma I as it was used before 1st October 1936, then only six plugs and just 3·2·1 or 6 different wheel orders were available. Enigma's key space thus, until this date, was much smaller and given by:

$$3\cdot2\cdot1\times16{,}926\times26\cdot26\times100{,}391{,}791{,}500$$
$$= 6{,}892{,}082{,}813{,}640{,}024{,}000$$

The by far greatest contribution to the above numbers comes from the plugboard. This, however, is a cryptographically weak component, and no major obstacle for a smart codebreaker. The first half of the plugboard, on the way from the keyboard to the scrambler, just produces an additional involutory monoalphabetic encryption of the plaintext. This is one of the weakest methods ever. Though even a general monoalphabetic substitution alone allows for 26! keys and cipher alphabets, much more than the number of Enigma keys, it can be easily broken.

Hence, from a codebreaker's point of view, the high number of different key possibilities produced by the plugboard can be seen as an illusory complication. In B.P. the plugboard connections were completely overcome through the clever invention of the Turing-Welchman-Bombe.

Even though the plugboard is indeed an improvement of Enigma's cryptographic strength, the improvement is much weaker than the large number indicates. That is why for a worst-case approximation, the cryptographer should neglect the factor produced by the plugboard when calculating the total key space.

Moreover, also the rings are a rather weak element. As known, all three wheels have a ring each, and the ring settings of the three wheels were part of the daily key. As also known, the ring setting of the left-hand wheel has no cryptographic effect at all, as there is no rotating wheel on its left-hand side which could be controlled. The left-hand wheel itself, because of the well-known and well-described “double stepping” of the middle rotor (Hamer, 1997), steps only every 25·26 or 650 letters. This is controlled by the ring setting of the middle wheel.

A typical ciphertext had 80 to 125 letters (250 was the ordered maximum). Hence a stepping of the left-hand wheel occurred with a probability of 80/650 to 125/650 or roughly 12 % to 19 % for ciphertexts with the said lengths. In other words: Only one out of five to eight typical Enigma messages experienced a stepping of the left-hand wheel. That means, the ring setting of the middle wheel had, in most cases, no effect and did not contribute to the key space. Thus, mostly the corresponding factor 26, as given by the middle ring, may be completely neglected.

And lastly, also the ring setting of the right-hand wheel is of minor importance. When all the other key parts are correct (meaning, in the case of the right-hand wheel, a correct offset between the wheel setting and the ring setting), then also with a slightly wrong adjusted right-hand ring, plaintext passages will appear. To summarise: the rings do not really obstruct codebreaking.

In conclusion, the ring settings, as well as the plugboard connections, can be assessed as cryptographically rather weak elements. When now, as a cryptographer's worst-case approximation, neglecting their contributions to Enigma's key space, then not much remains from the previously seemingly gigantic key space:

$$3 \cdot 2 \cdot 1 \times 26 \cdot 26 \cdot 26 \times 1 \times 1 = 105{,}456$$

This number represents the cryptographically strong part of Enigma's key space. (With unknown rings, all 26·26·26 wheel settings must be taken into consideration, and not only 16,926 as before.) And this is what the codebreakers were principally faced with until 1938.

This obviously far too small number ($6 \cdot 26^3$) also indicates, how Enigma could have been designed stronger. Possible solutions could increase either the first factor (3·2·1) or the second one (26·26·26), or both, or introduce new factors.

5 A Possible Stronger Enigma

5.1 Basics

Enigma's decisive cryptographic component is the scrambler with its rotating wheels. Without this rotation, Enigma produces just a simple monoalphabetic encryption. A cryptographically significantly stronger Enigma could benefit from one or more of the following improvements.

(1) A basic measure to increase Enigma's combinatorial complexity is to use more wheels, like what was done later for the British Typex.

(a) Rotors within the scrambler,
(b) settable stators,
(c) extra rotors (in a separate wheel box),
(d) extra reflectors for swapping (ditto).

(2) A more frequent wheel stepping of the “inner” (i.e., left-hand and middle) rotors was needed. This could be achieved by driving the left-hand rotor instead of the right-hand one, alternatively with the aid of gears, or very easily by using some more notches,

(a) say at least three notches, or even better,
(b) variable notches controlled by the key.

(3) Wheels with variable wiring, e.g., by using removable wiring cores, controlled by the key, would be an ultimate refinement,

(a) for the rotors themselves,
(b) through pluggable stators,
(c) through a pluggable reflector.

(4) A differently designed plugboard.

Enigma's plugboard, as implemented, was a cryptographically weak solution. It produced an additional simple monoalphabetic encryption of the plaintext and an identical one for the ciphertext. Instead of using it as it was implemented, it could e.g., have been utilised for altering the wirings of the reflector through 13 single-ended connections. The latter was proposed one more time by Rinke and Korn (1929); however, explicitly rejected by Fenner and Seifert.

In addition to the cryptographic characteristics, also several practical aspects of a cipher machine are important. It must be handy, reliable, portable, and easy to operate. Some of these demands stand in contrast to high cryptographic strength. For instance, the splendid idea of achieving security through many wheels within the scrambler is disadvantageous with respect to reliability and ease of operation. Moreover, a plugboard with two times 26 sockets connected by 26 single-ended leads yields 26! possible permutations might be a cryptographer's dream, but it would be a nightmare for the operator.

5.2 More Wheels

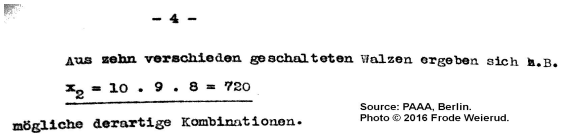
The first factor from above (3·2·1) was increased to 5·4·3, thus by a factor of ten, when wheels IV and V were put into service by the German Army on 15th December 1938. Here the question arises: Why so late and why so few?

Scherbius and Korn knew about this option to increase Enigma's strength. After Scherbius had learned that his original idea of *security through a high number of rotors* could not be realised through many adjacent wheels *in* the Enigma itself, he concluded that it was mandatory to use more than a mere three wheels to choose from *outside* the Enigma.

The Navy people came to the same conclusion. The secret order from 26th August 1925 of 50 *Funkschlüssel C*, signed by *Korvettenkapitän* Günther Guse (1886–1953), later Admiral of the *Kriegsmarine*, included five rotors, thus two extra rotors, for each machine. These Enigmas were delivered in the first weeks of 1926.

A short time later, in March, Korn (1926) wrote a four-page description on behalf of ChiMaAG entitled "Theory of the cipher system of the glow lamp machine 'Enigma' for the Naval Command." Korn explained the cryptographic fundamentals of *Funkschlüssel C*, including its period and the key space. Also, the double stepping of the middle rotor was described, as well as a settable reflector with four positions.

Concerning the number of wheel orders, he wrote: "From ten differently wired wheels e.g., $x_2 = 10 \cdot 9 \cdot 8 = 720$ possible such combinations result."


- 4 -

Aus zehn verschieden geschalteten Walzen ergeben sich z.B.

$x_2 = 10 \cdot 9 \cdot 8 = 720$

mögliche derartige Kombinationen.

Source: PAAA, Berlin.
Photo © 2016 Frode Weierud.

Figure 6. Statement by Korn (1926)

After rotors I to III had been constructed in July 1927 for Enigma I, rotors IV and V were designed in June 1932; however, brought into service by the German Army as late as December 1938. A little later, the German Navy used eight wheels (I to VIII) together with Enigma-M3.

Figure 7. Extra rotor box for up to seven wheels.

The Polish cryptanalysts were unable to proceed with their successful codebreaking after the German Army had increased the number of possible wheel orders from 6 to 60 in 1938. That's why the Poles asked their French and British Allies for help during the meeting at Pyry in July 1939. One could now ask: What if Enigma had had, say, seven different wheels to choose from already in the 1920s, resulting in 7·6·5 or 210 different wheel orders? Consequently, the Polish codebreakers would then have had to fabricate much more Zygalski sheets and later *Bomby* instead of the only six being used. Possibly the first break in 1932 had then never happened.

A few years later, in the case of the British Typex, this is actually how it was done: Five rotor inserts could be selected from a set of 14·2, with dozens of different sets, resulting in hundreds of wirings. Ralph Erskine (1997) made this comment: "Even Marian Rejewski or Alan Turing might have blanched at that Herculean task."

An explanation for why not many more wheel wirings were used for the early Enigma could be that one wanted to keep it cheap and simple.

5.3 Pluggable Stators

ChiMaAG invented the concept of pluggable variations to the Enigma as early as 1926 and, on 9th August 1926, applied for a patent. The idea was to introduce variable components either inside or outside the scrambler that could easily be changed by plug connections. This was to make Enigma more variable and secure, designated "neutrality of the machine," so that knowing the wirings of the rotating wheels would not suffice to break messages. This patent covered all future developments, such as the plugboard from 1928 and the pluggable reflector introduced in 1944.

The original patent application from 1926 is lost. It was intentionally destroyed together with many other secret patents: Due to the growing threat of Allied bombing attacks in Berlin in 1944, the German patent library had been evacuated from the German capital to Heringen in eastern Hesse. This included the secret patent documents, which were then safely stored in a deep potash mine several hundred meters underground. It has been reported (Wilder, 1958) that on 30th March 1945, *Regierungsrat* Franke, who referred to a secret order from the Reich Defence Commissioner, destroyed the documents by means of five litres of liquid air.

The original idea of the invention from 1926 is nevertheless known. It is mentioned in a memo and explained in German patent DE554421, both from 1928. The latter describes one or two fixed stators situated in between the rotors. A stator would allow any arbitrary connection by means of pluggable short leads, thus forming a non-rotating but fully arbitrary wired wheel.

This cryptographically strong solution was never implemented. The reason for this may again have been contact problems, or possibly rooted in the already mentioned crucial meeting concerning Enigma's plugboard on 17th February 1928 at the RWM in Berlin.

5.4 Pluggable Reflector

An alternative option for a pluggable device, which was also covered by the said patents from 1926 and 1928, was a pluggable reflector. Invented as early as 1926, it had, in fact, an extremely long development history and was only introduced as late as 1944. The *Umkehrwalze Dora (UKWD)*, as it was called by the Germans, or nicknamed "Uncle Dick" by the British, enhanced both the key space and the cryptographic security of Enigma.

Once again, fatal procedural errors happened: The new UKWD was not introduced universally and in one fell swoop, but piecemeal and just for certain nets of the German Air Force. Moreover, it was only used for very important messages, while the bulk of the other messages continued to be enciphered with the long-serving and non-pluggable UKWB reflector.

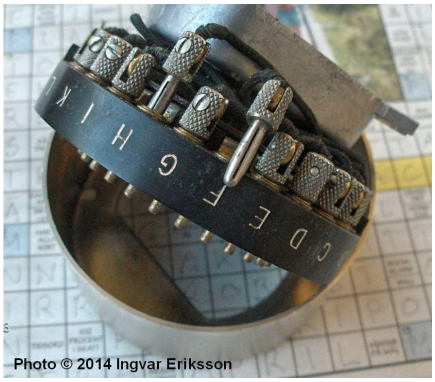
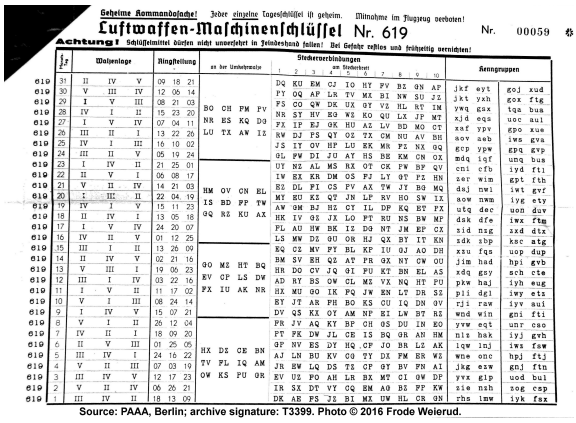


Figure 8. Pluggable UKWD reflector.

Even worse, to ease operation, identical daily keys were used for messages sent with the common UKWB reflector and with UKWD. This procedural mistake allowed the codebreakers to recover "Uncle Dick's" wirings regularly and read the corresponding messages.



Geheime Kommandosache! Jeder einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Luftwaffen-Maschinenschlüssel Nr. 619 Nr. 00059

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen! Bei Gefahr rechtzeitig vernichten!

Tag	Walzenlage			Ringstellung		an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1 2 3 4 5 6 7 8 9 10	Anrufgruppen	
619	31	II	IV	V	00	18	21		DQ KU EM OJ IO HY FV BZ GN AP	jkf eyt	goj xud
619	30	V	III	IV	12	06	14		FY OQ AF LR TV MX BI NW SU JZ	jkt yxh	gox ftg
619	29	I	V	III	08	21	03	BO CH FM FV	FS CO QW DK UX GY VZ HL RT IM	yxq gsx	tqa bus
619	28	IV	I	II	15	23	20	NR ES KQ DJ	NS SY HV EG WZ KO QU LX JP WY	xjd eqs	uoc aul
619	27	I	V	IV	07	04	11	LU TX AW IZ	FX IP EJ GK HU AZ LV BD MO CT	xaf ypv	gpo xue
619	26	III	II	I	13	22	26		NW DJ FS QY GZ TX GM NU AV BH	aov aeb	iws gva
619	25	IV	I	III	16	10	02		JS IT OV HF LU EK MR FZ NX GQ	ecp ypw	gpq gvp
619	24	III	II	V	05	19	24		GL FW DI JU AY HS BE KM CN OX	mdq iqf	unq bus
619	23	I	IV	II	21	25	01		UY NZ AL MS HX OT CK FW BP QV	cnl cfb	iyd ftl
619	22	II	V	I	06	08	17		IW EX KR DM GS PJ LY QT FZ HN	zer wim	gpt fth
619	21	V	II	IV	14	21	03	HM OV CN EL	EZ DL FI CS FV AX TW JY BG MQ	dsj nwl	iwt gvf
619	20	I	III	II	22	04	19	IS BD PP TW	MY EU KZ QT JN LP RV HO SW IX	aow nwm	iyg ety
619	19	IV	I	V	15	11	23	GQ RZ KU AX	AW GM BJ HZ CY IL DF KQ BT PX	utq dac	uon duv
619	18	II	IV	I	13	05	18		HK IV GZ JX LO FT EU NS BW MP	dsk dfe	iwx ftm
619	17	I	V	IV	24	20	07		FL AU HW BK IZ DG NT JM EP CX	sid nsg	xsd dtx
619	16	IV	II	V	01	12	25		LS MW DZ GU OR HJ QX BY IT KN	idk sbp	ksc atg
619	15	III	I	II	13	26	09		EQ CZ MV FY BL KP IU GJ AO DH	xzu fqs	uop dup
619	14	II	IV	V	02	21	15	GO MZ HT BQ	BM SV ER QZ AT FR GX NY GW OU	jim had	hpi gvb
619	13	V	III	I	19	06	23	EV CF LS DW	HR DO CV JQ GI FU KT BN EL AS	xdq gsy	sch cta
619	12	III	I	IV	03	22	16	FX IU AK NR	AD RY BS GW CL MZ VX NQ HT PU	pxw haj	iyh eug
619	11	I	V	II	11	17	02		HX MU GO IK FQ JW EN LT DR SZ	pli dgl	iwy ets
619	10	V	I	III	08	24	14		BY JT AR PH BO KS CU IQ DN GV	rji raw	iyv aul
619	9	I	IV	V	15	07	21		DV QS KX OY AM NP EI LW BT RZ	wnd win	gnl fti
619	8	V	I	II	26	12	04		FR JV AQ KY BF CH GS DU IN EO	yvw eqt	unr cso
619	7	IV	II	I	18	09	20		PT FK DW JL CE IS BQ GR AN HM	nlz hak	iyj gvb
619	6	II	V	III	01	25	05		GP NV ES QY HQ CF JO BR LZ AK	iqw lnj	iws fsw
619	5	III	IV	I	24	16	22	HX DZ CE BN	AJ LN BD XV GQ TY DZ FM ER WZ	wme onc	hpj ftj
619	4	V	II	III	07	03	19	TV FL IQ AM	JR EW LQ DS TZ CF GY BV FN AI	jkg esw	gnj ftn
619	3	III	IV	V	12	17	23	OW KS PU GR	EV UZ FO AH LR BX MT GI GW DP	yvx gip	uod bul
619	2	V	II	IV	06	26	21		IR SX DT VY GQ EM AO BZ FP KW	zls nsh	sog csp
619	1	III	IV	II	18	13	09		DK AE FS JZ BI MZ UW HL GR GN	rhs imw	iyk fsx

Source: PAAA, Berlin; archive signature: T3399. Photo © 2016 Frode Weierud.

Figure 9. Key sheet introducing UKWD.

Shortly after the war, the U.S. Army Security Agency (ASA) stated (1946): "How close the Anglo-Americans came to losing out in their solution of the German Army Enigma is a matter to give cryptanalysts pause. […] Only a trickle of solutions would have resulted if the pluggable reflector had been adopted universally; and this

trickle of solutions would not have contained enough intelligence to furnish the data for cribs needed in subsequent solutions. Thus even the trickle would have eventually vanished."

5.5 Non-reciprocal Plugboard

Gordon Welchman (1982) wrote in his book *The Hut Six Story*: "But the change that fascinates me most is a devasting one that could have been made without too much difficulty during the war [...] Suppose that, at any point during the war, the Germans had simply issued sets of single-ended connectors to replace the sets of double-ended ones [...] the output of Hut 6 Ultra would have been reduced to at best a delayed dribble, as opposed to our up-to-date flood."

Welchman probably did not know that such a plugboard with single-ended connectors did already exist long before the war and that on 17th February 1928, the RWM had decided to abandon it.

5.6 Multiple Notches

A very simple and obvious improvement is the use of wheels with significantly more than just a single notch, thus producing multiple turnovers. By extra notches, a more frequent and less predictable wheel stepping is produced. Curiously, some Enigma models such as G, KD, and T, the ones for the German secret service *Abwehr*, the *Militärisches Amt (Mil Amt)*, and for joint German-Japanese communications, had several notches (Hamer et al., 1998). Enigma T, for instance, was delivered with eight especially wired exclusive wheels with five notches each. However, neither Enigma G nor the KD Enigma or Enigma T took advantage of a plugboard.

Figure 10. Enigma T wheel with five notches.

Welchman (1982) emphasised: "We would have been in grave trouble if each wheel had had two or three turnover positions instead of one." Peter Twinn (1993), another former codebreaker at B.P., wrote, "they [the Germans] certainly missed a trick in not combining multiple-turnover wheels with Steckerverbindungen."

5.7 Variable Notches

A later solution, which never came into service, was a programmable wheel with variable notches called *Lückenfüllerwalze* "gap-filling wheel."

Figure 11. Variable notch rotor.

In case these new wheels had come into service, with the notch settings as a new part of the daily key, then the long-missed irregular stepping of Enigma's rotors would finally have been realised. This could have caused more than quite a headache for the codebreakers.

The already mentioned ASA report (1946) stated: "[This] would probably have prevented Anglo-American attempts at reading the Enigma after 1942 if it had been produced in quantity and installed." On the other side, however, nobody knows, what confusion this new element might have created also for the Germans.

6 Conclusion

The breaking of German Enigma messages was an achievement that influenced the course of World War II. It was based on the ingenuity of Allied codebreakers, however, made possible in large part by German procedural errors and design flaws of the Enigma.

The latter could have been significantly reduced through several improvements, such as the use of more cipher wheels, more notches, a pluggable reflector, and a non-reciprocal plugboard. All this could have been easily decided and accomplished already during the 1920's. In this case the Enigma would have initially become cryptographically much stronger and could have been converted into a virtually unbreakable cipher machine.

Acknowledgements

The author is most grateful to Frode Weierud and Claus Taaks for sharing their expertise during many years of fruitful cooperation, for the stimulating discussions on the topic of this paper, for their valuable advice, and for thoroughly proofreading the draft of this article.

Special thanks are directed to Paul Reuvers and Marc Simons for kindly allowing the use of two images from their Crypto Museum website, to Ingvar Eriksson for allowing to use his photo of Enigma's pluggable reflector, and once again to Frode Weierud for allowing the use of several images from his inexhaustible CryptoCellar.

References

Army Security Agency. 1946. *Notes on German High Level Cryptography and Cryptanalysis.* European Axis Signal Intelligence in World War II, Vol. 2, Washington, DC.

BArch MA, RM 5/3566, Bundesarchiv-Militärarchiv, Freiburg, Germany. Az. II 8.–12., Bd. 1.

Mavis Batey. 2009. *Dilly – The Man Who Broke Enigmas*. Biteback Publishing Ltd, London, UK.

Suzanne Carter. 2024. Private Communication. Bletchley Park Trust.

Cryptologia, 2001. *The glow-lamp ciphering and deciphering machine – Enigma.* Reprint of a sales pamphlet. Cryptologia, 25:3, 161–173.

Ralph Erskine, 1997. *The development of Typex.* In Zdzislaw Jan Kapera. *The Enigma Bulletin.* The Enigma press. Krakow, 69–86.

James Gillogly. 1995. *Ciphertext-only cryptanalysis of Enigma.* Cryptologia, 19:4, 321–413.

Daniel J. Girard. 2016. *Breaking "Tirpitz" – Cryptanalysis of the Japanese-German joint naval cipher.* Cryptologia, 40:5, 428–451.

David H. Hamer. 1997. *Enigma – Actions involved in the 'Double Stepping' of the middle rotor.* Cryptologia, 21:1, 47–50.

David H. Hamer, Geoff Sullivan & Frode Weierud. 1998. *Enigma variations – An extended family of machines.* Cryptologia, 22:3, 211–229.

Fritz Hansen. 1923a. *Die Chiffriermaschine.* Die Umschau, 35, 1st Sep. 1923, 552–554.

Fritz Hansen. 1923b. *Die Chiffriermaschine.* Der Radio-Amateur, 23:4, Nov. 1923, 76–78.

David Kahn. 2012. *Seizing the Enigma – The Race to Break the German U-Boat Codes, 1939–1943*. Naval Institute Press, Annapolis, MD, USA.

David Kenyon and Frode Weierud. 2020. *Enigma G – The counter Enigma.* Yale University Press, New Haven and London, Cryptologia, 44:5, 385–420.

Willi Korn. 1926. *Theorie des Chiffriersystems der Glühlampenmaschine "Enigma" für die Marineleitung*. Chiffriermaschinen Aktiengesellschaft, Technische Abteilung, Berlin. Bestand Rückgabe TICOM, Politisches Archiv des Auswärtigen Amts (PAAA), Berlin. Archive signature: T1715 to T1718.

Willi Korn and Elsbeth Rinke. 1928. *Aktennotiz*. Bestand Rückgabe TICOM, PAAA, Berlin. Archive signature: T1715 to T1718.

Willi Korn. 1938. *Theoretisches über die Enigma-Glühlampenchiffriermaschine Ch 11 f (Heeres-Ausführung)*. Chiffriermaschinen Gesellschaft Heimsoeth und Rinke, Berlin. Bestand Rückgabe TICOM, PAAA, Berlin. Archive signature: T1715 to T1718.

Louis Kruh and Cipher Deavours. 2002. *The commercial Enigma – Beginnings of machine cryptography.* Cryptologia, 26:1, 1–16.

Marian Rejewski and Henryk Zygalski. ca. 1940. *Enigma – Kurzgefasste Darstellung der Auflösungsmethoden* "Enigma – brief description of the resolution methods." SHD, DE 2016 ZB 25/6.

Elsbeth Rinke and Willi Korn. 1929. *Aktennotiz über die Besprechung am 6. August 1929*. Bestand Rückgabe TICOM, PAAA, Berlin. Archive signature: T1715 to T1718.

Arthur Scherbius. 1923. *„Enigma" Chiffriermaschine.* Elektrotechnische Zeitschrift, 1035–1036.

Hugh Sebag-Montefiore. 2004. *Enigma – The battle for the code.* Cassell Military Paperbacks, London.

Geoff Sullivan and Frode Weierud. 2005. *Breaking German Army Ciphers.* Cryptologia, 29:3, 193–232.

Dermot Turing. 2018. *X,Y&Z – The Real Story of how Enigma was Broken.* The History Press, Stroud.

Peter Twinn. 1993. *The Abwehr Enigma.* In Francis Harry Hinsley, Alan Stripp. *Codebreakers – The inside story of Bletchley Park.* Oxford University Press, Reading, Berkshire,123–131.

Gordon Welchman. 1982. *The Hut Six Story – Breaking the Enigma Codes.* Allen Lane, London 1982; reprint M&M Baldwin, 2000.

Anders Wik. 2018. *The First Classical Enigmas – Swedish Views on Enigma Development 1924–1930.* Proceedings of the 1st International Conference on Historical Cryptology, 83–88.

Robert Wilder. 1958. *Was wurde aus den deutschen Patenten? – Regierungsrat Frankes Sonderbefehle.* Der Kurier (newspaper), no. 192,West Berlin.