Stijn Maatje
*Korteweg-de Vries Instituut voor Wiskunde*
*Universiteit van Amsterdam*
*stijnmaatje@gmail.com*

**History**

# Secret Communications: Enigma, Fialka and Rubicon

**In October 2023, Raf Bocklandt and Stijn Maatje organized a visit to the Secret Communications exhibition of the Cryptomuseum for a visiting German school class. The Cryptomuseum is an online museum which provides information about everything to do with cryptography and espionage. While the museum itself is online, they do have a physical collection which they exhibit every few years. In this article Stijn Maatje will explore some personal highlights from the exhibition and tell the stories associated with these items.**

## Enigma

When talking about cryptographic equipment, we cannot omit the Enigma machine, which is arguably the most important cryptographic device from the 20th century. It was by used by Nazi Germany in the 1930s and 1940s to encrypt almost all military communication. If the Allies were to break this encryption, they would have access to incredibly valuable information which could help them in the war effort.

To understand the story of Enigma, we have to go back to the First World War. The Netherlands were neutral and wanted to remain neutral in this war. Belgian and German ships entering Dutch waters were closely watched to prevent smuggling. The tension between the countries was high.

Meanwhile, on the other side of the globe, maintaining neutrality in the Dutch East Indies proved to be difficult. The navy squadron there was small (only about ten ships) and would be obliterated if it were to engage in battle. The Dutch East Indies was an archipelago consisting of thousands of islands which were difficult to monitor with such a small fleet. Germany took advantage of this by building illegal refueling stations on some islands. This, in turn, provoked British, French and Japanese warships to patrol the surrounding area. This was a violation of Dutch neutrality, but the Dutch squadron present could not withstand the power of the larger fleets in the area, so declaring war was not really an option unless the situation escalated even more. It also wasn't always clear how to react to certain circumstances, since it may not be the smartest decision to start a war by following orders too strictly. To prevent this, the commander of the squadron was only allowed to act with permission from the Commander of the Navy in Batavia, the capital of the Dutch East Indies at the time.

The need of a secure communications link between the squadron and Batavia was very much needed. Back in the Netherlands, at the Navy Academy in Willemsoord, Den Helder, two sea lieutenants working at the naval base, Theo van Hengel and Rudolf Spengler, were tasked with creating a cipher machine to be used in the Dutch East Indies. Unfortunately, the drawings of their design have been lost to time and no machine was saved either. A description of the machine survives:

> "The machine is quite heavy and bulky, bearing a standard typewriter keyboard for input. It consisted of four rotors which were driven by four geared wheels. The four drive wheels each drove one rotor and were grapped in their number of teeth [...]. The rotor movement was quite irregular looking because rotors paused whenever they encountered a gapped sector of their drive wheel [...] ." [8]

The machine was never patented by Spengler and van Hengel, since they couldn't agree with the Navy Minister, Hendrik Bijleveld, about who owned the patent: Spengler and van Hengel or the Dutch Navy [14].

One country over, in Germany, an engineer called Arthur Scherbius also invented a cipher machine based on rotors, similar to the machine invented by Spengler and Van Hengel. He filed for a patent for this machine in 1918, and called his machine *Enigma*, Greek for 'riddle'. The machine itself resembled a typewriter, but with some notable differences. A keyboard was present to type a plaintext messages, the *Tastatur*. When a letter on this keyboard was pressed, a mechanical system of rotors was then set in motion and an electrical signal could flow through the machine, ultimately lighting up a light bulb on the *Lampenfeld*, corresponding to another letter. This is how messages were encryp-

An Enigma I machine. The plugboard can be seen on the front of the machine. The keyboard and lampboard are located on top of the machine. Above the lampboard are three little windows, through which one can see the current configuration of the rotors.

ted on the Enigma machine, and this is how the machine works and looks to the layman's eye. However, a deeper dive into the inner workings of the machine reveals some interesting mathematics.

Internally, the Enigma machine consists of turning rotors. A single rotor on the Enigma machine has 26 inputs contacts which are connected internally with 26 output contacts. Mathematically speaking, a rotor is just an element of the symmetric group on 26 letters, $S_{26}$. Only using this permutation as encryption is not very safe: it is a mono-alphabetic substitution, which can be cracked very easily using frequency analysis, a method devised by polymath Al-Kindi in the 9th century. Instead, we can turn the rotor after each letter we encrypt, changing the nature of the monoalphabetic substitution, and turning it into a polyalphabetic substitution of period 26 [11].

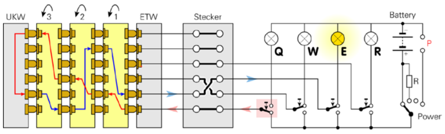
For example, let's imagine we are using an alphabet consisting of 6 letters. The wiring of the rotor inside is an element of the symmetric group on 6 letters, $S_6$, for example $\sigma = (aeb)(d)(cf)$. If we want to encrypt the word *cafe* we determine $\sigma(c) = f$, after which the rotor turns one sixth of a full revolution. Mathematically, we can simulate this by including an extra permutation $\rho = (abcdef)$. To encrypt the second letter we determine $\rho\sigma\rho^{-1}(a) = f$. In general, to encrypt the $i$-th letter we determine its image under $\rho^{i-1}\sigma\rho^{-(i-1)}$. So in our simple one-rotor system *cafe* gets encrypted as *ffed*. This is slightly different from the Enigma machine, where the internal mechanism already turns the rotor while pressing a button, so the encryption of the $i$-th letter is actually its image under $\rho^i\sigma\rho^{-i}$ [7].

The Enigma machine is slightly more complex than the machine described above. In fact, over the years multiple versions of the Enigma machine have been made, so there is no such thing as *the* Enigma machine. For now, we will look at the *Enigma I*, the most common version of the Enigma machine, which was introduced in 1930. More than 20,000 machines of this type were manufactured, and it was used by the *Heer* (Army) and the *Luftwaffe* (Air Force), and later adopted by the *Kriegsmarine* (Navy) as well. We will briefly explore some other types of Enigma machines as well.

In the Enigma I, there are three rotors (*Walzen*) in the machine, working as an odometer in a car, or as hands on a clock. After a button press, only the right-most rotor turns one 26th of a full revolution. The middle rotor only turns once the right-most rotor completed a full revolution, roughly once every 26 letter presses. The left-most rotor only turns once the middle rotor completed a full revolution, roughly once every 676 letter presses.

After a button press, an electric signal travels through these rotors, arriving at an essential part of the Enigma machine: the reflector (*Umkehrwalze*). When a signal enters the reflector, it sends an output signal through another letter, which is then sent through the rotors once more, essentially acting a sort of mirror.

The reflector is essential to the practicality of sending and receiving messages on the Enigma machine. As a permutation, the reflector is a product of 13 transpositions. Since the signal of a button press travels through the exact same rotors on the way to the reflector, as the way out of the reflector, a single setting of the Enigma machine can be viewed as a conjugation of the reflector. Since conjugation doesn't change the type of permutation, a single setting of the Enigma machine is also a product of 13 transpositions. This makes it easy to encrypt and decrypt: whenever a message is encrypted, the machine is set using the daily key and the message is typed in. To decrypt, the encrypted message can be typed in on the Enigma machine using the exact same setting that was used to encrypt the message. Since the rotors of the machine will turn in exactly the same manner in decrypting as in encrypting, and since every setting of the Enigma machine consists of only transpositions, the original message will appear. An important side effect of the reflector is that a letter can never be encrypted to itself, a fact that will become important later.



A simplified schematic of the Enigma machine.

The Enigma machine as described above is how Scherbius sold the machine for commercial use. Banks, police and companies all have interest in being able to communicate sensitive information securely. For the military version, the *Wehrmacht* added something extra: before the signal of a button press travels through the rotors, it enters the plugboard, located at the front of the machine. The plugboard is a board of all 26 letters, where cables can be used to connect two letters. This has the effect of swapping two letters before a signal enters the rotors, or after a signal leaves the rotors. In early procedures (1931-1937) six cables were used, while in later procedures (1940-1945) ten cables were used [11].

The plugboard offers an enormous amount of starting possibilities [16]. This was one of the reasons the Germans thought Enigma to be unbreakable. It is notable that the number of possible plugboard settings is highest using eleven cables, though the Germans never used eleven cables to decrypt messages.

To decrypt an Enigma message, one needs to know the basic setting of the machine. This is the setting of the machine when encryption starts and acts as the key of the message. The key consisted of the order of the rotors (*Walzenlage*), the basic setting of the rotors (*Grundstellung*), the reflector used and the plugboard (*Steckerbrett*) used. Furthermore, the internal wiring of each rotor could be changed with respect to the 26-letter alphabet on the outside of the rotor, this was known as the *Ringstellung*. The exact procedure would change through the years. For example, in the early years there were a total of three rotors used. Later, one had to choose three

A closeup of the rotors of the Enigma machine. Sometimes the numbers 01-26 would be used instead of the letters A-Z.

rotors out of a total of five - and for the Navy even eight - different rotors. Making some assumptions, the total size of the key space is in the order of $10^{20}$. The key would change every day, known to all Enigma operators. Brute forcing the key was an impossible task. Since the contents of the message were highly time sensitive, it was key to obtain the daily key as fast as possible. Clever linguists and mathematicians were needed to exploit structure or mistakes introduced into the encryption process [11].

In later years, many versions of the Enigma machine would arise, some significantly more difficult (but not impossible) to break. The Kriegsmarine would unexpectedly adopt the Enigma M4 in 1942 which used four rotors instead of three, with added complexity by the addition of a rotating reflector. Some versions (Enigma T, Enigma A28, Enigma G) had rotors that stepped more often and more irregularly, making the ciphertext much less predictable [13].

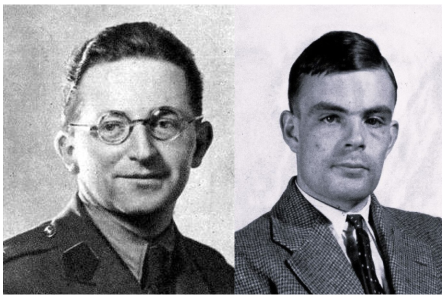
After winning the Polish-Soviet war (1918-1921), the Polish government decided to found a cryptographic bureau in the interwar years, the *Biuro Szyfrów*, in Warsaw. The Polish-Russian war was won, partly because of the codebreaking capabilities of the Polish. The Biuro had two main goals: to determine the internal wiring of the rotors, and to develop a fast, reliable way to decipher Enigma messages. One of the mathematicians employed at the Biuro was Marian Rejewski (1905-1980), who would ultimately be responsible for cracking Enigma.

Little was known to the public about German cryptography. The only information available to Rejewski was intercepted messages from Germany, which were still encrypted. At this point in time, Rejewski roughly knew how the Enigma machine worked, but no information about the internal wiring of the rotors or reflectors was known to him. To determine the wiring of the rotors, Rejewski used basic permutation theory, some information from espionage and exploited the laziness of Enigma operators and insecurities of Enigma procedures. After this, he could deduce the internals of the Enigma machine, which could then be used to build replicas of the machine, to be studied further. Since Rejewski only used the ciphertext, he employed a *ciphertext-only attack*.

This technique could then also be used to determine the daily key. To aid them in determining this key, Rejewski and his colleagues invented a machine called the *bomba kryptologiczna* and built one for each possible order of the rotors. Since the Germans used a total of three possible rotors, there were $3! = 6$ possible orders. In 1933, the Bomba was used together with other techniques to find the daily key in ten to twenty minutes. This means that in the year that Hitler came to power, the Polish had already cracked Enigma [1].

To prepare for the War, the Germans changed the procedures of Enigma, which meant the codebreaking techniques employed by the Poles would no longer work. Fearing they might soon be invaded, the Polish met with the French and the British, and gave them all of their code breaking efforts: blueprints, mathematical analyses, etc. The British brought all of this to the intelligence bureau of the United Kingdom, the Government Code and Cipher School (GC&CS). Preparations for an outbreak of war were already underway and GC&CS had recently moved to an estate just an hour north of London, to Bletchley Park. Just far away enough from London to avoid bombings, but strategically located equidistant between Cambridge and Oxford, where much of Bletchley's workforce would be coming from [13].

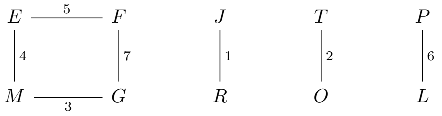
One of the mathematicians working at Bletchley Park was Alan Turing (1912-1954). Turing devised a alternative technique to crack Enigma messages. Turing's technique exploited the biggest weakness of Enigma: humans. In the encryption procedure, Enigma operators often had to use a random string of three letters. Since they would send many messages each day, they usually opted for easy to generate strings, which resulted in predictable strings like `ABC`, `AAA` or `QWE`. The German army also had to report when all was quiet, which resulted in predictable messages like `KEINEXBESONDERENXVORKOMMISSE`. When intercepting a message the exact location could also be determined using triangulation. Combining this with the fact that the first message of the day at 6 a.m. would often be the weather forecast, one could expect to see messages like `WETTERVORHERSAGEXBISKAYA` for the weather forecast of the Bay of Biscay. This (educated) guess of the plaintext is called a *crib*, making this type of attack a *known-plaintext attack*.



Marian Rejewski (1905-1980) (l) and Alan Turing (1912-1954) (r).

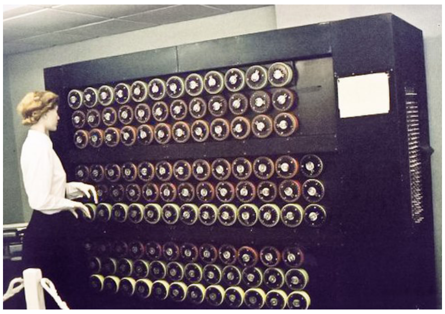
After finding a probable crib, one could use the fact that a letter can never be encrypted to itself to determine where in the ciphertext this crib would occur, known as the *depth* of the crib. This is the guess of what part of the ciphertext corresponds with the plaintext. From this correspondence a special graph called a *menu* was made. The vertices of this graph are the letters in the crib, and we draw lines between the $i$-th letter of the ciphertext and the $i$-th letter of the crib.

For example, we intercepted a message which we think is about general Rommel, and we think that in this message, `JTGEFPG` corresponds with `ROMMELF`. We can then draw the following menu:



A machine called the *Bombe* could then be set according to this menu. The Bombe was an invention by Turing, and it was improved upon by Gordon Welchman. Given a menu, it brute forced possible Enigma setting in a clever manner, essentially doing a proof by contradiction electrically. When the Bombe had found a possible setting, it would stop and the operator would note the position the Bombe stopped at and would then let the machine continue. There might be multiple possible Enigma settings for a given menu, but only one of these would correctly decrypt the original message. One could greatly improve the Bombe's accuracy by choosing a crib that yielded a menu with more cycles. This eliminated an enormous number of possible settings.

The Bombe was used together with countless other techniques (Banburismus, Rodding, etc.) to determine the daily key. The first Bombe prototype *Victory*, cost one hundred thousand pounds to build and took a week to find the right key. After some refining, a proper Bombe, called *Ag-*



The Bombe was set according to a menu, and would stop when it had found a possible solution.

*nus Dei*, was built and took only an hour to find the right key [13].

**The people of Bletchley Park**

Nowadays, everybody rightfully celebrates Alan Turing as one the most important mathematicians at Bletchley Park. It is however also important to note that cracking Enigma was far from an individual achievement. In fact, on the height of its success, around ten thousand people were employed at Bletchley Park, with around three quarters of them being women [15]. I want to highlight two people who worked at Bletchley Park, who, in my view, embody the spirit of codebreakers at Bletchley Park: Dillwyn (Dilly) Knox (1884-1943) and Mavis Batey, née Lever (1921-2013). To get an idea of the type of people working at Bletchley Park, this excerpt from the biography of senior codebreaker Emily Anderson gives an idea:

> “A lifelong proponent of teamwork and synergy, Denniston [Commander Alastair Denniston (1881 - 1961), head of GC&CS] had, from the outset, provided an environment that encouraged individuality and harnessed it to enable a disparate team of often quirky individuals to work successfully towards a common goal. [...] Denniston recruited prospective cryptographers and cryptanalysts irrespective of their age, gender or background, valuing talent and potential above all else. Experience had shown that codebreakers had to be able to think laterally. Dilly Knox, for example, brilliant but a noted eccentric, had been known for doing most of his thinking sitting in the bathtub installed in his office in MI1(b) [the army’s intelligence division during the First World War].” [2]

During the First World War, Knox helped decrypt the famous Zimmerman Telegram which resulted in the involvement of the United States in the War. During the Second World War, Knox founded his own department: *Intelligence Services Knox* (ISK). Everybody at Bletchley Park referred to the unit as *Dilly’s Fillies*, since Knox only wanted to employ female codebreakers. Mavis Batey, who would later write Knox’s biography, explained:

> “Dilly chose people who were language orientated. There was an actress, and some girls who’d been at drama school and they were quite glamorous, but they also understood rhythms and patterns of speech. Dilly was always looking for rhythms and patterns. There were linguists like me, and one girl was a speech therapist. We were always referred to as ‘Dilly’s Girls’ or ‘Dilly’s Fillies’, even in places like Whitehall, but he chose us because he liked the fact we were intelligent, made good coffee, and we could pick up his ideas and work on them while he came up with more. It was no use asking the mathematicians because they were too busy with their own ideas. But we could give him the attention he needed and try to pin down his ideas and try them. Some worked, some didn’t, but he was never short of them. He was an extraordinary man.” [2]

Knox’s unit focused on cracking the versions of Enigma which could not be cracked using techniques developed by other departments such as Hut 8, which was Alan Turing’s unit.

Mavis Batey arrived at Bletchley Park when she was just 19 years old. When she arrived at the ISK unit, Knox said to her: ‘*Oh, hello, we’re breaking machines, have you got a pencil?*’ [12]. She was then thrown in the deep end and had to figure out herself what to do. Her first result came very quickly. Knox himself had previously cracked the version of Enigma used by the Italian Navy, which was notoriously difficult to crack. This version had since become unreadable by some procedural changes from the Italians. In the new procedure messages had to be of a certain length. When reading the ciphertext of an intercepted message, Batey noticed that the second part of the message didn’t contain any L’s. Knowing that on an Enigma machine a letter cannot be encrypted to itself, she suspected that the sender of the message had repeatedly pressed the L to pad the original messages. Sure enough the key could be recovered and the plaintext could be read: *Today’s the day minus three*. After waiting three days, a very long message came in, detailing a planned attack on a Royal Navy convoy carrying supplies from Cairo to Greece. An attack was planned by the British and thanks to the information supplied by Batey; it was a landslide victory. After that, the Italians never attacked the Royal Navy in the Mediterranean again. Following this victory, Knox wrote the following ‘epitaph to Mussolini’:

> “These have knelled your fall and ruin, but your ears were far away. English lassies rustling papers through the sodden Bletchley day.” [2]

Batey’s biggest contribution was a collaboration with Knox and Marget Rock, another leading female codebreaker. The Enigma G was a version of Enigma mainly used by the German intelligence Agency (Abwehr). In the ‘normal’ version of Enigma, a notch was present on each rotor so the rotor to the left of it would advance by one position every revolution. Enigma G had rotors with 11, 15 and 17 notches (all coprime), making rotor movements much more unpredictable. In addition to this, the reflector which is stationary in Enigma I also turns in the Enigma G. The department tasked with cracking Army and Air Force Enigma machines, Hut 6, lead by Gordon Welchman, could not crack this version of Enigma and deemed it unbreakable. At this point, the problem was forwarded to ISK where, on 8 December 1941, Mavis Batey broke a message intercepted from Belgrade. This allowed them to reconstruct part of the machine and break Enigma G.

Breaking Enigma G was an important step in the way the war would progress. The British now knew exactly how to decrypt Enigma G messages, but also how to encrypt messages. The British security services MI5 and MI6 came up with a plan to feed false information to the German intelligence agency by encrypting it using Enigma and sending it as if it came from a German source, essentially creating fake news. This scheme was known as the Double-Cross System (XX System), which would play a hugely important role in Operation Fortitude. The Germans were fed information that the Normandy landings of 1944 (D-Day) would take place in

Calais, where the Channel is at its narrowest, when in fact they would take place in Normandy, hundreds of kilometers to the south. This meant that a significant portion of the German Army was stationed at Calais. Since the British could now read Enigma G messages, they knew for a fact the Germans believed the deception and that the Normandy landings could take place as planned, without much resistance.

The intelligence gathered at Bletchley Park was codenamed *ULTRA* and was instrumental in the victory of the Allies in the War. At the start of the war Churchill was sure he could win the battle on land and in the air, but he feared the Battle of the Atlantic, since German U-boats employed very sophisticated attack tactics which were difficult to predict. Churchill credits the Ultra intelligence gathered at Bletchley Park as the reason the Allies won on sea. Even early on in the war Churchill recognized the importance of the codebreakers at Bletchley, calling them *the geese who laid golden eggs and never cackled*. When the codebreakers at Bletchley felt they were understaffed in important sections, they asked Churchill for more personnel, to which he replied with a now famous memo:

> "ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done." [3]

## Fialka

During and after the Second World War, the USSR gathered intelligence from espionage about Enigma and started development on their own cryptographic machine. After two years of development, this resulted in the introduction of a new machine in 1956 based on the Enigma machine: the M-125, codenamed FIALKA (ФИАЛКА)[17]. The Soviets noted all flaws present in the Enigma machine and improved every single one of them. Fialka was used by the Soviets well into the 1990s.

Mavis Batey (1921-2013) (l) and Dilly Knox (1884-1943) (r). Batey would later write Knox's biography 'Dilly, the man who broke Enigma'.

The Enigma keyboard used the Latin alphabet which consists of twenty-six letters. The Cyrillic alphabet used in the Russian language has thirty-three letters, but only thirty are present on the Fialka, where some less frequently used letters have been omitted. On a later version of Fialka a button was present where one could switch between the Latin and Cyrillic alphabet.

Broadly speaking, the working of the mechanism on the Fialka machine is similar to that of the Enigma machine.  Once a letter on the keyboard has been pressed a signal is sent through some rotors, reflected in the reflector and sent back through the rotors. The lamps of the Enigma have been replaced by a printhead. Instead of having to write down each encrypted letter manually, each letter is automatically encoded using a Cyrillic version of the Baudot code. Every letter is encoded using five bits, and is punched on a standard teleprinter tape, which could then easily be transmitted by telegram. This way of encoding was much faster and less prone to human error than manually writing down letters and sending them with Morse code, as was done with Enigma.

The most obvious difference between the Enigma machine and the Fialka machine is the number of rotors: ten instead of three. Furthermore, adjacent rotors rotated in opposite direction. On every rotor of the Enigma machine, a notch was present so that a rotor could turn the rotor to the left of it after a full revolution. In practice, this meant that the left most rotor almost never turned during encryption, rendering it (almost) useless.

The turning mechanism on the Fialka machine worked slightly differently. One rotor didn't influence the movement of the rotor next to it, but was instead connected to the rotor next to that one. On the Enigma a single pin on a rotor controlled the stepping of the rotor next to it. On the Fialka numerous pins were present on a rotor, controlling the stepping of the rotor next to the rotors neighbor.

The M-125 Fialka

This increased size of the keyspace considerably and made the turning of the rotors highly irregular. The pins were present on the outer part of a rotor, while the inner part contained the actual wiring of the rotor. In 1978 new rotors were introduced where the inner wiring and outer pins could be separated and interchanged with other rotors, increasing the size of the keyspace once again.

One flaw of the Enigma machine was that a letter could never be encrypted to itself, which turned out to be an enormous vulnerability, exploited by the cryptanalysts at Bletchley Park. The Soviets solved this problem by slightly modifying the reflector. In the Enigma machine, the reflector is a product of thirteen transpositions. The Fialka utilized a thirty letter alphabet, so the naive equivalent of the Enigma reflector would be a product of fifteen transpositions. The Soviets, however, made a reflector which was a product of thirteen transpositions, one 3-cycle and one 1-cycle:

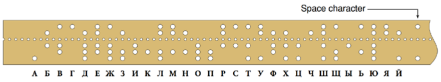
$$\rho = (\text{А}, \text{Б})\ (\text{Э}, \text{Г})\ \dots\ (\text{Ж}, \text{В}, \text{Ц})\ (\text{Й}).$$

Note that this 1-cycle makes it possible for a letter to encrypt to itself. Having a 3-cycle in the reflector meant that the encryption and decryption process became slightly more complicated. If the reflector above was used during encryption, the machine now has to make sure to invert this 3-cycle during decryption:

$$\rho^{-1} = (\text{А}, \text{Б})\ (\text{Э}, \text{Г})\ \dots\ (\text{Ж}, \text{Ц}, \text{В})\ (\text{Й}),$$

which could be easily done using a small electronic circuit.

The addition of the plugboard in the Enigma machine provided a lot of possible starting settings, increasing security. It was very tedious for an operator to use the plugboard, so for the Fialka, the Soviets thought of an easier equivalent, which was also more secure. Instead of physically connecting letters on a plugboard, a punchcard was used which could slide into the side of the machine. This punch-

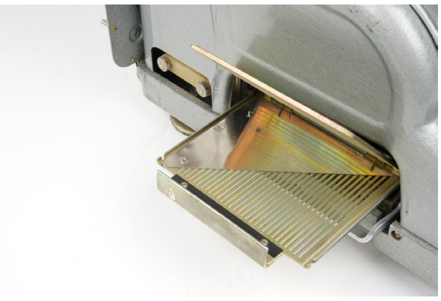


The Fialka standard for 5-bit encoding of the Cyrillic alphabet.

card consisted of a $30 \times 30$ matrix, indexed by the letters of the alphabet. The operator received this punchcard in a sealed bag from the Soviet High Command with holes pre-punched. The punchcards were changed daily. A punched hole in this matrix represented a 1, signifying a swap of two letters. A 1 at position $(i,j)$ lets the machine know to send input $i$ to letter $j$. Every column and every row would have exactly one non-zero entry, which makes the punchcard a permutation matrix. Essentially, the punchcard is an additional (static) rotor with completely random wiring. Compare the $2.0 \cdot 10^{14}$ possible settings of the plugboard on the Enigma machine (with 11 cables) to the $30! \approx 2.7 \cdot 10^{32}$ possible settings of the punchcard, and you can understand why the Soviets opted for the latter option. When the punchcard was not in use, a metal triangle would be inserted into the machine: a physical identity matrix!

The use of punched tape on the Fialka made it much easier to work with than the Enigma machine. However, the Soviets noticed some flaws in the machine. When pressing a button, a certain chain of events is set in motion, unique to that button press. This means that every button press produces a different sound and by analyzing the acoustics one could figure out what buttons were pressed in what order. To prevent this, the mechanics of Fialka have been produced in such a way that every button press produces the exact same sound.

Another flaw was present in the way the tape was punched. Whenever a key is pressed, the paper puncher punches a letter on the paper tape. For example, when this letter is A the string 10000 is punched on the strip and when this letter is Д the string 11110 is punched on the strip. In the former case only one puncher is activated, while in the latter case four punchers are activated, drawing four times as much current from the power supply. One can analyze the current drawn by the machine to deduce how many punchers were activated by the keypress, which in turn gives valuable information about the printed letter. To overcome this, the Soviets modified the power supply to produce a stable amount of voltage, while also producing a constant current. In addition, they added a noise generator, which superimposes stochastic noise onto the power line to obfuscate any further hidden signals. This type of attack is called a *side channel attack*, and proves that when analyzing a cryptographic system, one should never only consider the mathematical framework, but also take outside factors into consideration.



The equivalent of the plugboard on the Fialka. Have you ever seen a physical identity matrix?!

The Soviets had a very strict protocol for using Fialka. Only the operator was allowed to use the machine, the sender or recipient were usually not allowed to operate the machine. On big military exercises, the machine was operated in a hut or tent where only a handful of people were allowed inside. The outside area was heavily guarded, everybody who entered the restricted area was in danger of being arrested or being shot on the spot.

The existence of Fialka was kept secret for many years, so little was known about the procedures and the internals of the machine. The first publication about Fialka, including a detailed description of the machine, was published in 2005 by Paul Reuvers and Marc Simons of the Cryptomuseum. To this day, little research has been done about the Fialka and its security, so no successful attack is known, but in 1989 it was believed by Russian cryptologists that Fialka messages could be cracked within 24 hours. This was possible, since Israel captured some Fialka machines during the Six Day War in 1967. Furthermore, the American National Security Agency (NSA) had supercomputers running special Fialka cracking software in the 1970s and there is also proof that the Austrians decrypted a substantial amount of Fialka traffic.

Every country in the Warsaw Pact had their own version of Fialka, with different wired rotors than the other countries. This was because the Soviets didn't want countries to communicate amongst themselves, without informing Moscow first. After the collapse of the Soviet Union all Fialka machines were ordered to be destroyed. The machines were thrown on big piles and would then be set on fire. Most Fialka machines were destroyed in fires or by simply smashing them. There are, however, multiple stories of officers coming to oversee the destruction process, getting intoxicated with alcohol, and not noticing some unburned machines deeper in the stack being sneaked out of the fire. The Cryptomuseum has a fully restored and working Fialka M-125 from Russia, which is (as far as we know) one of only two Fialka machines in the West with Russian wired rotors [10].

### Operation Rubicon

The United States and the Soviet Union were constantly spying on each other during the entire Cold War. This made the use of good encryption more important than ever.

Russian-born Swede Boris Hagelin (1892-1983) founded Crypto AG in 1952 to produce cryptographic and communications equipment. Unlike the Enigma, most of Hagelin's machines were pinwheel machines, where mechanical pins would decide the stepping of the machine, making it purely mechanical and therefore ideal to use in the field. Hagelin based his company in neutral Switzerland and provided cryptographic equipment to more than 120 countries in both the Eastern and Western Bloc.

During World War II, Hagelin sold the rights to his M-209 pinwheel machine to the United States for over eight million dollars [18]. This deal solidified the relationship between Hagelin and the United States.

One of the people who Hagelin had good relations with, was American cryptographer William Friedman (1891-1969) [19], who would later become known as 'the dean of cryptography'. Since Friedman was also born in Russia, the two quickly bonded and became good friends. In 1949 Friedman became head of the cryptographic division of Armed Forces Security Agency (AFSA) until 1952, in which the organization was succeeded by the National Security Agency (NSA), where Friedman also became chief cryptologist.

The United States had released large quantities of the M-209 machines to be sold for as little as fifteen dollars for use in other countries. Many of these machines were bought by South American countries.

Boris Hagelin (1892-1983)

Meanwhile, the NSA started development on a machine (WARLOCK) designed to crack messages encrypted on pinwheel devices.

In 1954 Hagelin was working on a new pinwheel machine called the CX-52 with very unpredictable cryptographic behavior, making it very cryptographically secure. The NSA did not like this. They benefited from other countries using cryptographic equipment which was secure, but not too secure, since that would hinder the breaking of this equipment using their relatively powerful computers, and thus hinder their ability to gather intelligence to use against the Eastern Bloc. Part of Friedman's job was to identify cryptographic developments that would pose risks to the stream of intelligence coming into the NSA and CIA.

Friedman was sent to negotiate with Hagelin, and more than a year later, in February 1955, they agreed on a deal between Hagelin and the NSA. This deal was called 'the Gentleman's agreement'. Hagelin did not want anything to be written down. Still, the agreement had to be authorized by the director of the NSA. This authorization is still classified, but we know the contents of the deal. Although Hagelin would not be paid for this deal, the US Army would be using his cryptographic equipment. Furthermore, we can assume he and his family would receive personal favors from the NSA, like job offers at the NSA or US army. In return, the NSA would provide Hagelin with a list of countries, to which he was not allowed to sell his most sophisticated equipment. The loss of sales would be compensated: Hagelin received seven hundred thousand dollars up front. The countries that Hagelin was allowed to sell to, would receive manuals written by the NSA. NATO countries, however, would receive a different manual, detailing how to 'properly' use the machine. For example, if one were to follow the procedure in the CX-52 manuals provided to non-NATO countries, the cryptographic security would be significantly smaller than if one were to use a NATO manual. [4]

In 1957 Hagelin intended to retire, but the Americans did not want to lose control over Crypto AG. Hagelin discussed this matter with Friedman, saying that the only options he had was to either hand over the management to his son, Bo Hagelin, or to sell his company to Siemens (which Hagelin had considered before). Then Friedman reminded him of a third option: sell his company to the Americans. After exploring several options, the CIA offered a licensing agreement, which essentially formalized the Gentleman's agreement from a few years prior. In addition, Hagelin would receive six hundred thousand dollars, plus an annual bonus of seventy-five thousand dollars. This operation was codenamed SPARTAN.

In the coming years, it became clearer and clearer that mechanical cryptographic equipment would soon be replaced by electronic cryptographic equipment. Instead of mechanical rotors like in the Enigma and Fialka machines, a shift register would be used, which is roughly the electronic equivalent of the rotors from early twentieth century cipher machines and can be used to quickly generate a pseudo random stream of bits.

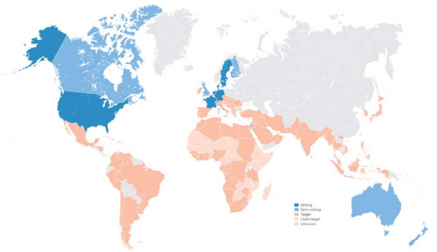
From 1965 onwards Crypto AG focused on electronic cryptographic equipment, since it would otherwise lose business to other manufacturers. Peter Jenks (1924-1989) was cryptanalyst at the NSA and came up with a way to make shift registers which looked pseudo random, but actually inhabited much structure, which could be exploited by NSA cryptographers. These algorithms could then be used in Hagelin's equipment to be sold worldwide. This was the beginning of a closer working relationship between the NSA and Hagelin.

Then, in 1970, using a complex scheme of hard to trace companies and fiduciaries, the German *Bundesnachrichtendienst* (BND) and the American Central Intelligence Agency (CIA) bought Crypto AG in secret from Hagelin, for around seven million dollars. This joint project would be codenamed THESAURUS (treasury) and was changed in 1987 to RUBICON (point of no return). For the purposes of RUBICON, the CIA worked closely together with the NSA to develop algorithms to be put on Crypto AG equipment [6].

Crypto AG controlled 80-90% of all cipher equipment used worldwide, partly because the agreement that no Crypto AG equipment could be used by NATO countries was forfeited. The NSA could read about 57% of all intercepted messages. In comparison: without operation THESAURUS this would be less than 29%. By the 1980s, a mere 10 years after the start of operation THESAURUS, the NSA could read 96% of all messages sent through Crypto AG machines. A CIA report on the evaluation of operation THESAURUS concludes with *'It was the intelligence coup of the century'* [9].

An operation of this scale would surely not go unnoticed, right? Some codebreaking organizations, like the British GCHQ, received intelligence from the United States, but were not aware of operation THESAURUS/RUBICON. Other countries, like Denmark, France, Israel, Sweden and the Netherlands were informed by the NSA and BND how to crack certain Crypto AG equipment, but were not informed about the scale of the operation. In 2020, Bart Jacobs, a Dutch Professor of Security, Privacy and Identity at the Radboud University, revealed that a codebreaking alliance between Denmark, Sweden, Germany, the Netherlands and France, codenamed MAXIMATOR, was established in 1976. Information about operation THESAURUS/RUBICON was presumably also shared amongst the countries in this alliance [5].

In 1992 a sales representative of Crypto AG, Hans Bühler, flew to Iran on a business trip. While in Iran, Bühler was arrested by the Iranian authorities for spying, bribery, illegal contacts and illegal use of alcohol. The CIA didn't know what Bühler knew about operation RUBICON, and they were afraid he would make incriminating statements. The decision was made to pay the full million dollars of bail. Crypto AG itself didn't have the funds to pay this bail, so the BND and CIA had to come up with the money themselves. The BND was prepared to pay half of the money, but the CIA



The witting countries (blue) can be seen, as well as countries which we know for certain were targeted by operation THESAURUS/RUBICON (pink). [4]

was afraid it was illegal. Eventually the CIA agreed to pay their share, but this plan was later rejected by the White House. Months later, the BND paid all the money to the Iranian authorities and Bühler was released. Bühler felt that Crypto AG had not done enough to release him and accused Crypto AG of selling equipment with a weakened algorithm. The German *Bundespolizei* conducted several investigations regarding Crypto AG, but no evidence for Bühler's claims could be found. In the years to come, Bühler would accuse the BND to be the secret owners of Crypto AG.

This series of events was later dubbed 'The Hans Bühler Affair', codenamed HYDRA, and permanently damaged the relationship between the CIA and BND. In 1994 the BND backed out of operation RUBICON, making the CIA the sole owners of Crypto AG.

The CIA's ownership continued until 2018, when Crypto AG was bought by Swedish entrepreneur Andreas Linde and split into two companies. The old Crypto AG no longer exists. In February 2020 operation RUBICON was revealed to the public after an extensive two-year investigation of German, Swiss and American journalists [9].

The story of Crypto AG proves the need to do cryptography according to Kerckhoffs's principle: the security of a cryptosystem should never come from the secrecy of the algorithm, only of the secrecy of the key: the algorithm used should always be public knowledge. The Cryptomuseum has a lot of Crypto AG equipment which has been backdoored.

## Closing Remarks

These stories about cryptography are already interesting on their own, but the fact that the Cryptomuseum has so many artifacts which make the stories tangible and come alive, elevates them to another level. The students did not only listen to me talk about Enigma, they actively participated in discussions with me and the people from the Cryptomuseum. They were curious, asked interesting questions and learned about the history of cryptography, and with that, about the importance of cryptography. After the class had sailed back to Germany, Raf received an email from them thanking us for the day we organized, saying that they only talked about cryptography on the journey back home and that *'the highlight of our week was in a basement in Duivendrecht'*, which is the greatest compliment one can get.

## Acknowledgements

The author would like to thank Paul Reuvers and Marc Simons of the Cryptomuseum in Eindhoven. Without them, none of this would have been possible. They opened the exhibition especially for us and answered all the students' questions with great enthusiasm and insight. They also took the time to proofread this article and allowed me to use their photographs of the machines.

Furthermore, my longtime friend Ruud Bos has given me valuable feedback on this article from his persepective as a student of history.

I would also like to express my gratitude to Anette Schröder and her students from the Ubbo-Emmius-Gymnasium in Leer, Germany, for taking an interest in the world of cryptography, asking good questions and being curious, for which I am incredibly grateful.

## References and notes

1 F. L. Bauer, *The History of Information Security: A Comprehensive Handbook*, 381-446, Elsevier, 2007.

2 J. Uí Chionna, *Queen of Codes: The Secret Life of Emily Anderson, Britain's Greatest Female Codebreaker*, Headline, 2023.

3 A. Hodges, *Alan Turing: The Enigma*, Vintage, 2014.

4 Cryptomuseum, *Operation Rubicon: The secret purchase of Crypto AG by BND and CIA*, https://www.cryptomuseum.com/intel/cia/rubicon.htm, 2020.

5 B. Jacobs, European signals intelligence cooperation, from a Dutch perspective, *Intelligence and National Security* 35:5, 659-668, 2020.

6 H. Jaspers, *De cryptoleaks van CIA en BND: 'Dit was de inlichtingen-coup van de eeuw'*

7 R. Klima, N. Sigmon, *Cryptology: Classical and Modern*. Second Edition, CRC Press, 2019, https://www.vpro.nl/argos/lees/onderwerpen/cryptoleaks/2020/decryptoleaks-van-cia-en-bnd.html, Argos, 2020.

8 K. De Leeuw, *Dutch Invention of the Rotor Machine*, 1915-1923, Cryptologia 27:1, 73-94, 2003.

9 G. Miller, The intelligence coup of the century, *The Washington Post*, 2020.

10 P. Reuvers & M. Simons, *Fialka Reference Manual*, Cryptomuseum, 2005.

11 S. Singh, *The Code Book*, Anchor Books, 1999.

12 Mavis Batey Obituary, The Telegraph, 2013.

13 G. Welchman, *The Hut Six Story, M&M Baldwin*, 2023

14 Spengler and van Hengel accused another Dutchman, Hugo Alexander Koch, of stealing their drawings of the rotor machine and applying for a patent with those drawings. Unfortunately for them, Koch's brother-in-law, A.E. Jurriaanse, was partner in N.V. Vereenigde Octrooibureaux, the company responsible for giving out patents. Spengler and van Hengel took this matter to court, but more bad luck would come their way, since the court was presided by none other than former Navy Minister H. Bijleveld.

15 Many codebreakers at Bletchley Park would later become famous mathematicians. J.H.C Whitehead worked at Bletchley Park during the Second World War and would later become one of the founders of homotopy theory. William (Bill) Tutte would be instrumental in cracking the Lorenz cipher, which was used by Hitler and his high command. Tutte would later publish foundational work in matroid theory and algebraic graph theory, in which the Tutte polynomial was named after him.

16 A fun exercise is to calculate the number of possible plugboard settings using k cables, and to prove this is exactly the number of involutions that consist of k 2-cycles in the symmetric group $S_{26}$.

17 Like the Enigma, Fialka is not the name of a machine, but rather of the procedure itself. However, we will use the name Fialka throughout for clarity.

18 Adjusted for inflation, this is around $192 million in 2024.

19 Friedman was a very prolific cryptanalyst. Among other things, he first described the *Index of Coincidence* of a text, a statistic of a piece of text which could determine if a monoalphabetic or polyalphabetic cipher had been used to decrypt a text. Furthermore, if a polyalphabetic cipher had been used, the Index of Coincidence could be used to find the length of the keyword used during the encryption process.