The First Classical Enigmas
Swedish Views on Enigma Development 1924-1930

Anders Wik
S Catalinagr 9
S-18368 Täby, Sweden
anders.h.wik@gmail.com

Abstract

This paper concerns the very first "classical" Enigma from 1924, with rotors, reflector and lamp display. A description is given of the Enigma machines bought by the Swedish General Staff in early 1925, of the competition regarding the first standard crypto machine for the Swedish armed forces, and of some later developments.

1 Introduction

The Enigma cipher machine which had such importance in the Second World War has its roots in a machine that was first shown publicly at the Universal Postal Union Congress in Stockholm 1924. In Sweden it generated a strong interest which lasted for about five years during a time when the Enigma machine was developed through a number of models. This paper is mainly based on some 80 pages of correspondence between the Swedish General Staff (SGS) and Chiffriermaschinen AG (ChiMaAG) in Berlin and documents in connection with that. That material is used in a multitude of places throughout this paper and is not specifically referenced. It comes from the archive of FRA, the National Defence Radio Establishment, Stockholm, Sweden (FRA 1924-1930). Communication and cooperation was handled through the Swedish military attaché in Berlin. Much of the correspondence is in Swedish, whereas letters and documentation from ChiMaAG are in German.

2 Crypto use in Sweden 1924

The main players regarding ciphers were the General Staff and the Ministry for Foreign Affairs. Codes and simple lookup-tables were used, sometimes with a superencipherment, e.g. by the Köhl cipher ruler which was the Ministry for Foreign Affairs "System 1920" (Faurholt, 2006). Systems of the Wheatstone clock type were in use in the Military since 1907. Captain de Champs had developed a revolving cylinder cipher for the Navy in 1920 but it was just a prototype until 1926. A.G. Damm at AB Cryptograph had developed an impressive number of different crypto devices since the mid 1910s but at the time the only system Cryptograph could offer to the General Staff was the handheld model A22.

Looking at the available options it is easy to understand that the Enigmas on show at the exhibition in 1924 seemed very attractive.

3 The Stockholm machine

At the exhibition during the Congress of the Universal Postal Union in Stockholm in the summer of 1924 ChiMaAG demonstrated two crypto machines, an Enigma "Handelsmaschine" and a small "Militärmaschine". The Handelsmaschine was big machine (about 65 x 45 x 38 cm) and was quite heavy (about 50 kg). It had earlier been shown at exhibitions in Leipzig and Bern in 1923. It could print the output using a type wheel. The "Glühlampenmaschine" was a new model, probably made in just a few copies. It was the first model in a development, which was to last for more than 20 years. No such original machine or parts of it have been found. Since SGS had a strong interest in both machines the company left them in Stockholm for trials by the prospective customer. Also supplied was a one page typewritten description entitled "Glühlampenmaschine Enigma A" as well as a 16 page printed booklet describing the Handelsmaschine (ENIGMA Chiffriermaschinen, 1924).

Proceedings of the 1st Conference on Historical Cryptology, pages 83– 88,
Uppsala, Sweden, 18-20 June, 2018

It should be noted that ChiMaAG uses the name Enigma A and later Enigma B for the early "Glühlampenmaschine". The Enigma A is also called "die kleine Militärmaschine" and in this paper, for clarity, "the Stockholm machine". This is contrary to what has earlier been assumed, i.e. that A and B were the printing Enigma models. This paper will use the notations A and B as ChiMaAG used them in the correspondence.

Some details about the Stockholm machine can be gathered from the letters and the short description:

1. It measured 23 x 27 x 13 cm with a weight of about 5 kilograms.
2. It had 26 keys and 26 lamps arranged in two rows each, alternating lamp rows and key rows.
3. The keys and the lamp covers were unmarked and left for the user to mark (with characters or symbols).
4. There was an "Antriebstaste", a key that advances the rotors and that must be pressed each time before ciphering a character.
5. There were three rotors, one marked with letters and two with numbers. It had a period length of 676 and "more than 17000" (presumably 26^3) different settings.
6. Ciphering and deciphering were the same.
7. A reasonable conclusion is that it had two rotors and in addition an important novelty, a settable reflector (Umkehrwalze).

There does not seem to be any other remaining documents elsewhere about the Stockholm machine (Enigma A). It may have been a further development of a German patent application, DE407804, filed on January 18, 1924 by the inventor Paul Bernstein for ChiMaAG (Bernstein 1924). That construction was the first with a lamp field but it had straight ciphering from the keyboard through two rotors to the lamps field without a reflector, i.e. similar but simpler than the Handelsmaschine. It is not known whether any machines were produced on basis of Bernstein´s patent.

The Handelsmaschine and the Enigma A were returned by courier to ChiMaAG in September 1924. Captain Gyllencreutz who handled the matter for SGS asked for changes in the Enigma A they would like to see and test. In October 1924 he wrote that they considered buying 15 such machines. The desired modifications of the machine were:

1. A possibility to turn on all lamps at the same time to check that no lamps are broken.
2. The lamp field should have dark background and the letters lit. *(Apparently this was not the case with the Stockholm machine.)*
3. The lamp field ought to be behind the keyboard and the keys should not be blank but instead marked with letters.
4. The lever to move the wheels (presumably the Antriebstaste) should be on the left side of the machine.

Gyllencreutz added further tentative improvements

5. The machine should have a larger character set, preferably around 40, with digits, comma and period.
6. It would be desirable to have four wheels like in the big machine.

As to the bigger machine, the Handelsmaschine, Gyllencreutz was less certain, but possibly SGS might be interested in buying two or three.

4 Further negotiations

During the rest of 1924 discussions continued between SGS in Stockholm and the company in Berlin through the Swedish military attaché Major Henry Peyron in Berlin. In October the price with the requested modifications and some other improvements was given as 100 dollars each at an order of 15 machines. The technical officer at SGS suggested that the offer should be accepted. The total cost for 15 Enigma A machines with modifications 1-4 above would be 6250 Swedish crowns. The problem was funding. An attempt to influence the Swedish government was made through General von Bender who knew the Grand Duke of Baden, father of the Swedish queen Victoria. This seems to have been unsuccessful.

In November 1924 ChiMaAG offered a new possibility, a model they call "Enigma B". In this machine the third rotor, which in the first model was a settable reflector, would be a true rotor and step in the encipherment process giving it a period length of “about 17500” (*26^3=17576*). The new machine could also be delivered with a 28-character alphabet whereas the Enigma A only could have a 26-character set. The Enigma A was apparently in stock since they stated that up to 10 machines could be sold with immediate delivery. Improvements for the Enigma B compared to the machine shown in Stockholm should be:

1. Different layout: From back to front first two rows of lamps, then the rotors, then two rows of keys.
2. The rotors move automatically when a key is pressed making the Antriebstaste unnecessary.
3. The letters are white on a black background
4. The possibility to check that no lamp is faulty.

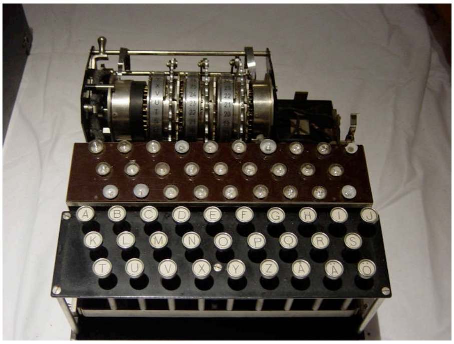

Photo 1: A133 without cover. Source: FRA

5 Swedish Enigmas

On January 13, 1925 SGS places an order for two “Enigma B” with a Swedish 28-character alphabet A…Z ÅÄÖ without W. The price was 650 RM each. The machines were delivered on April 6, 1925. They have serial numbers A133 and A134 and are today part of the FRA Crypto collections. The machines do not seem to be much used, possibly only for evaluation purposes. The weight is 5 kilo (without the wooden box) and the measures WxDxH = 26 x 27,5 x 11 cm, somewhat wider and lower than the Stockholm machine.

ChiMaAG had changed the layout compared to what they had offered, probably after consent from SGS. From the back are now rotors, three rows of lamps and then the keyboard set up in alphabetical order. The rotors have an adjustable ring setting.

The wiring of the rotors is as follows in cyclical notation:

I: (ÖAPRE) (CBSZYLÄKOFXN) (DGQTVI) (JH) (MUÅ)

II: (7, 1, 3, 14, 23, 21, 11, 20, 5, 24, 16, 27, 22, 17, 9, 13, 25, 6, 28, 10, 15, 2, 8, 4, 19, 26, 12, 18)

III: (5, 1, 26, 11, 28, 12, 25) (10, 2, 22, 4, 9) (15, 3, 17, 24, 13, 19, 14, 16, 6, 27, 7, 23) (8, 18, 21) (20)

The reflector is fixed in one position and has the following connections:

(1,12) (2,4) (3,7) (5, 27) (6, 14) (8,16) (9,19) (10,11) (13, 22) (15,25) (17,23) (18,21) (20,26) (24,28)

In theory it would be possible to change the wiring. The following picture shows that this would be a tricky procedure with clear risks to damage the function.

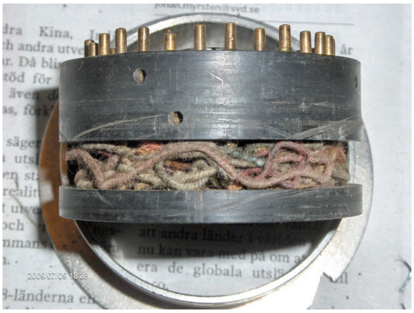

Photo 2: Opened rotor A133. Source: FRA

6 Funkschlüssel C

ChiMaAG was also negotiating with the Reichsmarine which in December 1924 ordered 10 prototype machines. That model was called “Funkschlüssel C” and had rotors with 28 contacts. This fits very well with what was offered to Sweden and the two machines that were ordered in January 1925. The

“Funkschlüssel C” had 29 keys and 29 lamps where the letter X went straight to the lamps without being enciphered. The wiring of the rotors was most likely different. The Swedish machine had a reflector which was fixed in one position whereas the Funkschlüssel C had a possibility to fix the reflector in four different positions. Apart from that the two machine types would very likely have been the same.

A delivery of 50 machines to the Reichsmarine took place in January 1926 (Weierud 2014). These machines were supplied with two extra rotors. This was mentioned in a report from the Swedish military attaché in October 1925, which said that a customer had ordered two extra rotors which gives 60 different rotor combinations instead of 6. ChiMaAG suggested that SGS should do the same.

7 Swedish competition

Boris Hagelin, who was now in charge of AB Cryptograph, heard about the strong interest from SGS for the new Enigma machines. Cryptograph had good contacts with the Swedish military, but their only viable product was the A22, which was far less attractive than the Enigma.

Nevertheless, the two machines were tested against each other in May 1925. Captain Backlund limited his comparison to practical matters such as encryption speed where he stated that encrypting a 100 character message would take 6 1/2, 4 and 3 minutes respectively for 1, 2 or 3 persons whereas for the A22 it would take around 4 minutes independently of the number of people involved. Backlund noted that the Enigma machines had a stepping error. This is the double stepping effect described by Hamer (1997).

Lt Samsioe gave a preliminary assessment of the security in November 1925. He wrote that the A22 seems to give a fairly low security, which possibly could be improved. His study of Enigma B was not concluded. He notes that the period is 28^3 but that there are subperiods of 28 which it might be possible to isolate. (*Actually the period is 28 x 27 x 28 because of the double stepping.)* A22 and Enigma B share the problem that a change of message keys does not change the character of the cipher enough. A new key is just a new starting position in the same crypto period. Since the order of the three rotors could be changed there could be six different key series.

It seemed clear that SGS thought highly of the Enigma and were going to buy it. In his memoirs Boris Hagelin wrote that he visited the person in charge at SGS, major Warberg, and asked him to wait six months with their decision. This would allow Cryptograph to make a prototype of a machine of Enigma type – but better. He was granted the time.

A G Damm had in 1919, independently of Scherbius and Koch, patented a form of wired rotors (Damm 1919). This was essential for Hagelin. By using parts of Damm´s B1 and B13 machines he was able to produce a prototype of what was to become the B21 machine. His machine had lamps and rotors, an irregular stepping mechanism for the rotors and a wider variety of operator key settings. Hagelin´s prototype was enough to stall immediate decisions and eventually secure the order from SGS and the Ministry for Foreign Affairs.

Cryptograph had acquired an Enigma (A344), which was sent to Damm in Paris. He sent back a preliminary report in August 1927 (Damm 1927). There he noted that he made a study already in September 1924 based on patent descriptions and other available information. That earlier report has not been found. In the 1927 report he wrote that the security is low if the wirings are known. He claims that he is developing a method to solve Enigma but writes that it would be improper to give details in a letter. Instead he goes into a detailed discussion of the machine.

He concluded his seven-page report with his verdict. *Enigma is a reasonably handy method to encipher…* but … *the security is directly dependent on keeping absolutely secret not only machine details but also texts - even if they are meaningless – that have been enciphered.*

His report might have helped Cryptograph by casting doubt on the Enigma even if his report does not contain arguments to show that the Enigma system is weak.

8 The next generation Enigmas

Contacts between SGS (through the embassy in Berlin) and ChiMaAG continued during 1925 while the two delivered machines were being evaluated in Stockholm. A request from SGS concerned a machine with printer and compatible with the lamp machines. At first the company seemed to be developing such a compatible pair.

However, in April 1926 the company stated that such a solution would not be developed since the printing machine would lose functionality and the lamp machine would be heavier, costlier and less reliable.

In the summer of 1926 LtColonel Carl Herslow succeeded Henry Peyron as military attaché. Herslow had a good knowledge of crypto matters and had worked in the group of officers at SGS which solved Russian diplomatic code traffic during WW1. This work was in cooperation with Germany, which may have benefitted Herslow´s insights into German security matters (Grahn 2017). In August 1926 Herslow visited the company and reported that the new machine was in its final shape. It had been introduced at the Auswärtiges Amt and would soon also be presented to the Reichswehrministerium. The new machine had four rotors (presumably three plus a reflector) and also spare rotors in a separate box. The price was quoted as 600 RM. Warberg at SGS was interested. He would like to test the new machine, preferably with a 28-character alphabet.

In November 1926 Herslow wrote to Warberg to tell him that the Reichswehrministerium had got delivery of a small series of the new machine. With Swedish specifications (28 characters) the new machine would be slightly bigger and could be offered at a price of 600 RM a piece at an order of 30-40 machines. A counter (Zählwerk) was optional and would add 40 RM to the price. A new machine with printer (a development of the Handelsmaschine) was expected to be developed by March 1927. It was aimed for use by higher staffs and had a price of about 2000 RM.

Test machines meeting Swedish requirements would be quite costly. Therefore, in February 1927, Warberg asked Herslow to buy two 26-character Enigmas with Zählwerk (at 700 RM a piece). In March 1927 Warberg reminds him that he should check the machines on delivery so that they do not have the stepping error of the earlier machines (cf section 7 above). The new machines were Zählwerk machines and had a different stepping mechanism. That check should therefore have worked without problem.

Herslow was going to take up a position as military attaché in Moscow. He was instructed to take one machine with him to Moscow. The other one should be delivered to Stockholm so that the pair of machines could be tested in operational use. Herslow was quite familiar with the Enigmas after many discussions at ChiMaAG.

When Herslow left for Moscow in the beginning of April 1927 the new machines were not ready so the company supplied two machines on loan (A361, A362), one for Herslow, one for Stockholm. Warberg provided a 12-page document with detailed instructions for key settings etc. (FRA 1927). The two Zählwerk machines (A350 and A351) were delivered in May 1927 and the machines on loan were sent back.

9 Enigma or B21

Presumably the Zählwerk Enigma was studied and tested. There is no communication in the file for the coming six months. In December 1927 SGS asked for a quotation for the delivery of 40-60 machines with a 28-character alphabet – with or without Zählwerk. The reply from the company was prompt. They quoted a basic price of 600 RM for a 26-character machine and gave two options. A Zählwerk would add 100RM and 28-character alphabet 30 RM.

Parallel negotiations were going on between SGS and Cryptograph and the decision was made. B21 was chosen as m/29, SGS standard machine model of 1929. No final evaluation has been found in the archives. Therefore one can only speculate about which arguments were the decisive ones. A longer key period? Rotors wired in Sweden? Wider user key space? Support to Swedish industry?

The Navy had some independence from SGS. Their order for three Enigmas was the last sign of interest from the Swedish armed forces. After delivery of A853, A854 and A855 in April 1929 there seems to be no interest in Enigmas from Swedish authorities.

10 Not quite the end

Carl Herslow, mentioned above, was in 1928 recruited by Ivar Kreuger, a Swedish industrialist and entrepreneur known as the “Match King”. By aggressive investments and innovative financial instruments he built a financial empire which in the end controlled between two thirds and three quarters of worldwide match production. His activities needed secure communications and the Swedish match company Svenska Tändsticks AB (S.T.A.B) became one of just a few non-government buyers of Enigma machines.

There is a note that Herslow bought two machines “for Kreuger” in the spring of 1928. Also there is a note from 1935 that two machines (A343 and A344) were presumed to be at S.T.A.B. All in all it seems that Kreuger´s company bought six Enigmas (numbered A327, A328, A343, A344, A801, A802) (Weierud 2014)

Apart from these regular machines S.T.A.B also bought three small Enigmas, model Z30, aimed at enciphering digital codes. No documentation concerning this has been found. The acquisition of these three machines, bought around 1930, concludes all dealings between Sweden and Chiffriermaschinen AG. The three Z30 machines are part of FRA Crypto collections (Wik 2016).

A broader picture of Swedish cryptography and early Swedish Sigint between the world wars is given by McKay and Beckman (2003).

Acknowledgements

The author is most grateful to Frode Weierud for sharing his Enigma expertise and for his valuable advise.

References

Bernstein, Carl. 1924. German patent DE 407 804. http://www.cryptomuseum.com/crypto/enigma/patents/files/DE407804.pdf

Damm, Arvid Gerhard. 1919. Swedish patent SE52 279. Filed Oct 10, 1919. US patent 1 502 376, July 22, 1924.

Damm, Arvid Gerhard. 1927. Preliminärt utlåtande angående “Glühlampen-Chiffriermaschine Enigma”. Krigsarkivet, Stockholm. Boris Hagelins privatarkiv, vol F II:3.

ENIGMA Chiffriermaschinen. 1924. Handelsmaschine. FRA Crypto collections. Booklet.

Faurholt, Niels O. 2006. Alexis Køhl: A Danish Inventor of Cryptosystems. Cryptologia vol 30.

FRA archive. 1924-1930. Bearbetningsbyrån F V:1. “Chifferapparaten Enigma”.

FRA archive. 1927. Bearbetningsbyrån F V:1. Instruktion för användning av Chifferapparat Enigma B /Chiffer EZ/.

Grahn, Jan-Olof. 2017. Om svensk signalspaning - Pionjärerna (“On Swedish SIGINT – The pioneers”). Medströms bokförlag, Stockholm.

Hamer, David. 1997. Enigma: Actions involved in the ‘double stepping’ of the middle rotor. Cryptologia vol 21.

McKay and Beckman. 2003. Swedish signal intelligence 1900-1945. Frank Cass, London.

Weierud, Frode. 2014. Personal communication.

Wik, Anders. 2016. Enigma Z30 retrieved. Cryptologia vol 40.