The Swiss NEMA Cipher Machine

Geoff Sullivan[1] and Frode Weierud[2]

ADDRESS: (1) 64 Tennyson Road, Headless Cross, Redditch, Worcs. B97 5BJ UNITED KINGDOM. Email: geoff@blueangel.demon.co.uk, URL: http://www.blueangel.demon.co.uk; (2) Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens FRANCE. Email: Frode.Weierud@cern.ch, URL: http://home.cern.ch/~frode/crypto/

ABSTRACT: The Enigma is probably the most well known wired wheel cipher machine. The NEMA is a cipher machine developed during World War II by the Swiss Army. It is designed on the same principle as the Enigma but with particular emphasis on overcoming some of its weak features. It was declassified by the Swiss Authorities in 1992. This paper describes its mechanism and the way in which it operates, so that it may be more widely known to cryptology researchers.

KEYWORDS: cipher machine, Enigma, NEMA, rotor wiring, computer simulations.

Historical Overview

Between 1941 and 1943 the Swiss Army's Cipher Bureau[1] which was created in 1939 under the command of Captain Arthur Alder, professor of mathematics at the University of Bern, began the design of a new cipher machine[2]. The machine was colloquially called *NEue MAschine*, NEMA, to distinguish it from the commercial Enigma machine already in use with the Swiss Army. It also went under the name T-D or *Tasten-Drücker-Maschine* which perhaps best can be translated as the Key-Stroke-Machine.

This article represents the views of the authors but not necessarily those of their employers or any third party.

[1] The swiss Army Cipher Bereau existed as a temporary organisation during the "active service" periods 1914-19 and 1939-45. A permanently staffed Cipher Bureau was first created in late 1946. In 1951 it became part of the Federal Signals Office (*Abteilung für Übermittlungstruppen*), headed by Paul Glur until autumn 1982.

[2] Unpublished notes, Dipl. Ing. Rudolf J. Ritter, "Notes on Early Use of Machine Cypher in Switzerland." 16 Jan. 1996.

The design team consisted of Professor Hugo Hadwiger (1908-1981), professor of analytical mathematics at the University of Bern, Dipl. Ing. Heinrich Emil Weber (1908-1997), later professor at ETH[3] in Zurich, and Dipl. Math. Paul Glur (1917-), also of the University of Bern and later chief of the Cipher Bureau.

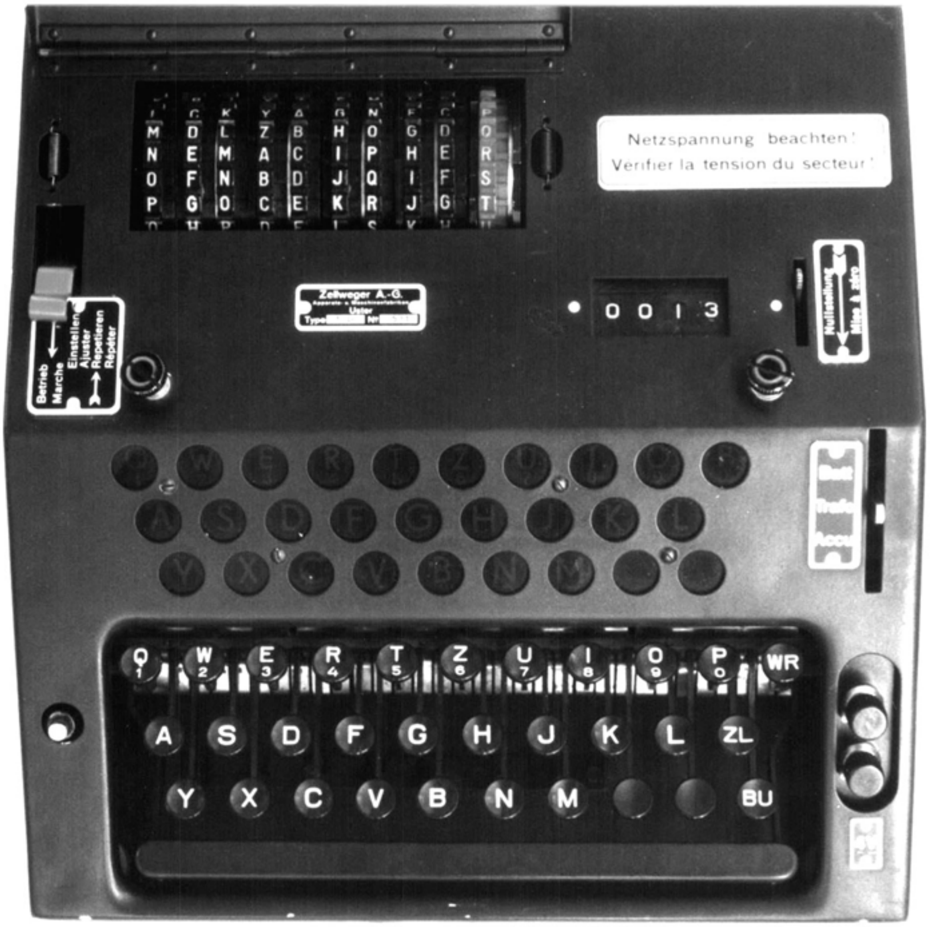


Figure 1. The NEMA cipher machine.

As we have shown previously the Swiss K machine[4], which was based on the commercial Enigma, was broken by both the Allied and German cryptographic services. This slowly became known to the Swiss. Few details are available about the breaks into the Swiss Army Enigma, however, the Swiss Foreign Office’s use of

[3] ETH = *Eidgenössische Technische Hochschule*, Zürich.

[4] David H. Hamer, Geoff Sullivan, and Frode Weierud, “Enigma Variations: An Extended Family of Machines,” *Cryptologia*, 22(3): 211–229.

the same machine appear to have been lax. In an interrogation of Dr. Rudolf Schauffler[5] the mathematician in charge of the theoretical research section of *Pers. Z*[6], he states: "The commercial Enigma used by the Swiss was sometimes solved because of stereotype beginnings and known settings. The Swiss used to include in their messages the machine setting for the next message."

Perhaps the cipher security was not the best at all levels, but the Swiss cryptographers studying the Enigma had also come to the conclusion that the commercial model was far from secure. As we have explained they modified the wheel stepping and re-wired the wheels frequently, but they knew that only a new design would improve the security of the machine. We will show that NEMA is based on the same principle as the Enigma using an *Umkehrwalze* (UKW) to reflect the electrical current through the wired wheels. However, the designers abandoned the idea of a settable, but static, input wheel as used in their modified Enigma machine or the use of Steckers as in the German Service machines. Instead they opted for a much more irregular motion of the wheels where the fast moving and slow moving wheels are interlaced such as to prevent the isolation of the fast wheel as was done with Enigma.

The new design was adopted by the Swiss Army's Procurement Agency[7] and the construction was entrusted to Zellweger AG in Uster near Zurich. In the spring of 1944 the first functional NEMA model became available. Modifications to the final design were decided in March 1944 and in October two pre-production models were ready for type approval. The formal military approval (*Truppentauglichkeit*) was given in March 1945 and a production order for 640 machines was issued in April 1945. It appears that this is the total number of NEMA machines that were produced. Zellweger AG started the serial numbering at 100 and the last machines are supposed to carry numbers around 740. The first machines went into service in 1947 under the name NEMA Model 45.

The machine and its documentation were declassified on 9 July 1992 and many of the machines were offered for sale to the public for the first time on 4 May 1994, at Meiringen close to Interlaken.

[5] "Security of Allied Communications, May–June, 1945." ZIP/SAC/S.2. Public Record Office (PRO), Kew, Surrey. ADM 223/505.

[6] The cryptographic bureau of the German Foreign Office. For further details see Michael van der Meulen, "The Road to German Diplomatic Ciphers – 1919 to 1945," *Cryptologia*, 22(2): 141–166.

[7] *Kriegstechnische Abteilung* (KTA) which in 1968 was renamed to *Gruppe für Rüstungsdienste* (GRD)

General Construction

The NEMA works on the same principle as Enigma. A bank of wired wheels and drive wheels is arranged on a common axle, with a reflector at the left end of the bank and an entry plate at the right. The entry plate connects to a 26 way lampboard and a keyboard having a QWERTZU layout. All the wheels step during operation but it is the method of stepping, determined by the drive wheels, that makes this machine very different to the Enigma family. Pressing a key causes the wheels to move, at the end of this movement, when the key is fully depressed, current passes from the active key to the entry plate, through the scrambler and is reflected back again and returns to the entry plate to light one of the lampboard letters. The bank of ten wheels appears through an aperture with a small hinged lid to allow manual adjustment of their position, above the lampboard. The keyboard is positioned below the lampboard.

The Scrambler

The NEMA scrambler bank contains four random wired wheels and an *Umkehrwalze*. The connections to the scrambler are by means of an entry plate, also called the input stator, but we will use the German expression *Eintrittwalze* (ETW). Each of the wired wheels and the UKW has a drive wheel positioned to its right. These are known by the German term *Fortschaltwalze* (literally turn away wheel), we will use the term 'drive wheel' here which more accurately describes its action; a drive wheel determines the movement of a wired wheel by means of a notch pattern set into a ring fixed to the left face of the drive wheel. The four wired wheels will be known as 'contact wheels'.

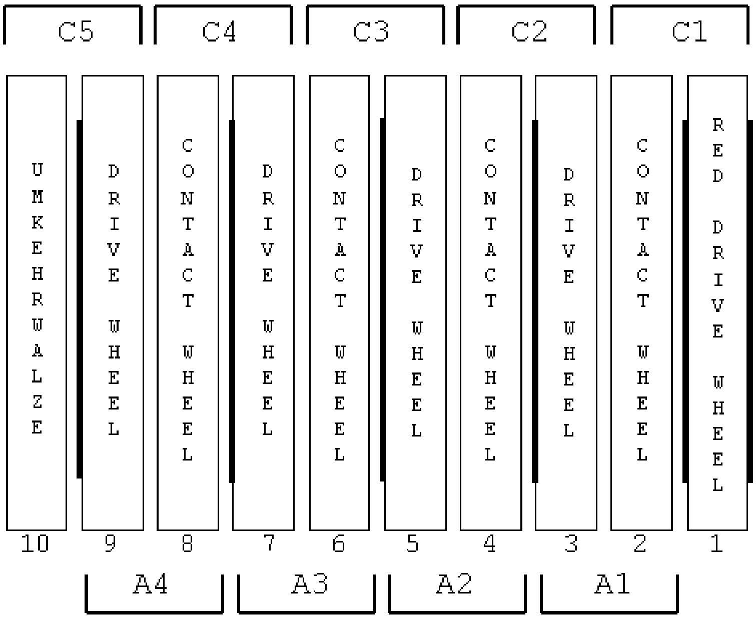


Figure 2. The physical arrangement of the ten wheels in positions numbered 1 to 10. Position 1 is the special red drive wheel fitted with two notch rings and position 10 is the reflector (UKW). A1 to A4 are contact wheel and drive wheel assemblies. The combined positions are numbered C1 to C5.

The machine therefore has a total of ten settable wheels which all step during operation. All wheels step in a counterclockwise direction when viewed from the right hand side of the bank. We will number their positions from 1 to 10 starting from the right as in Figure 2. Positions 2, 4, 6 and 8 are occupied by a contact wheel. Position 10 is the UKW. The drive wheels occupy positions 1, 3, 5, 7 and 9. The drive wheel in position 1 is a special red coloured wheel whose features will be described later. In Figure 2 the positions labelled A1, A2, A3 and A4 each consist of a mechanical assembly of a contact wheel and a drive wheel, which are assembled as a unit and fitted on the axle. Figure 5 shows the components of one such unit. Each section labelled C1, C2, C3, C4 and C5 is a combined position of a contact wheel and its controlling drive wheel. This logical pairing of a wheel and its controlling drive wheel will be referred to later when the stepping is described in detail. The keyboard and lampboard connect to the ETW positioned on the right of the bank. This arrangement, together with the use of a reflector, means that as with Enigma no letter is ever enciphered to itself.

	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
Wheel	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	05	14	15	19	13	02	22	10	04	18	16	26	24	09	23	25	08	20	06	11	03	01	12	21	07	17
B	04	17	18	09	20	15	08	11	16	01	10	24	19	25	13	22	14	21	03	02	17	06	12	05	23	26
C	18	17	19	26	14	10	15	07	02	11	25	20	09	05	03	21	16	04	08	06	24	13	12	23	22	01
D	05	22	12	19	18	03	16	08	01	09	26	11	14	04	25	07	06	10	15	02	20	23	17	24	13	21
E	06	19	21	24	13	02	23	11	15	04	18	01	25	22	08	07	03	20	26	10	09	12	17	14	16	05
F	15	04	06	11	26	08	07	19	24	17	01	16	03	20	22	10	02	21	18	14	25	23	09	05	13	12
UKW	14	12	19	18	13	22	17	21	16	11	10	02	05	01	20	09	07	04	03	15	08	06	25	26	23	24

Figure 3. Wiring of contact wheels A - F and the UKW for the NEMA cipher machine.

Contact wheels

A set of six contact wheels is labelled A, B, C, D, E and F. Each wheel has a central alphabet ring with protrusions between each letter to allow manual position adjustment when installed in the machine. The alphabet runs counterclockwise when viewed from the right hand side of the wheel. To the right of the alphabet section is a notched region of smaller diameter, the notch protrusions or teeth are positioned between the alphabet notches and are aligned with the letters of the alphabet. These teeth drive the wheel through stepping levers that engage between the teeth. This action will be described in detail later. On the right hand side face of the wheel are the 26 contact blades. These are radially positioned blades which are sprung. They are 6mm long and normally protrude 2.5mm above the wheel body. When compressed they are flush with the wheel body. The contacts on the left hand side of the wheels are V shaped, the V pointing counter clockwise when viewed side on. These V contacts are fixed in the wheel and do not move. The wiping action of the V and blade gives a better contact than the pin and pad system of the Enigma. The wiring for the contact wheels and of the UKW are given in Figure 3. The reference point number 1 contact is on the right hand face and corresponds to the position of the letter I on the letter ring. The ETW connections to the keyboard and lampboard run in a clockwise direction in QWERTZU sequence starting from contact point number 1, when viewed from the right hand side of the bank. The wheel, which has a central plain metal bearing, fits onto the plain axle of 8mm diameter. The left hand side of each contact wheel is reduced in diameter to 50mm and the drive wheel fits over this and is free to rotate on this section.

Drive Wheels (Fortschaltwalzen)

Each drive wheel mounted in positions 3, 5, 7 and 9 comprises an alphabet ring and a toothed region similar in shape to the contact wheels. On the left face of the drive wheel there is a metal notch ring, held in position by 3 screws. The notch patterns of these rings are given in Figure 4, where 0 represents the inactive protrusion of the notch ring and 1 represents the active low region. The notch rings are actually cams that lift the stepping levers away from the teeth of the contact wheel, preventing its movement. The notch ring on a given drive wheel determines the movement of the contact wheel immediately to its left.

The red drive wheel located in position 1 has a second notch ring fixed to its right hand face. This controls the movement of two other drive wheels and two contact wheels by means of a shaft carrying blocking arms, which can be set to prevent the movement of the combined position components when the right hand notch ring of the red drive wheel is in the inactive state. The remaining three drive wheels all advance one step for each letter. A four digit resettable letter counter is driven from a gear meshed with the letter ring of the red drive wheel.

The notch rings, identified by a two digit number, that attach to the drive wheels are marked with their identity number on one face. These rings should be fixed to the drive wheel with the marked number aligned with the letter U on the letter ring with three countersunk screws[8]. It is also possible to fix these notch rings with the number in position Y. In addition to the countersunk mounting holes, there are also three plain holes and three indents on the inner surface of the ring, but these serve no purpose in locating the ring on the drive wheel. The special notch rings numbered 1 and 2 can only be fixed to the right face of the first red drive wheel with the single digit identification number aligned with the letter L.

[8] The NEMA Instruction Manual, see reference [1], stresses that the correct position for the notch rings is with the number aligned to the letter U.

Notch Ring	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Active Notches
1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	5
2	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	5
12	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	1	1	21
13	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	0	1	1	1	1	1	1	0	19
14	0	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	0	1	17
15	1	0	0	1	1	0	1	0	0	0	0	0	1	0	1	1	1	1	1	1	0	1	0	1	1	1	15
16	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	23
17	0	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	0	1	0	1	1	0	1	1	0	11
18	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	0	1	1	23
19	1	1	1	0	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	21
20	1	1	1	1	1	1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	1	0	1	1	1	1	19
21	1	0	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0	1	0	0	17
22	1	1	0	0	1	0	1	1	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	1	0	0	15
23	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	23

Figure 4. Notch Ring patterns for the NEMA cipher machine. The notch protrusions represent the inactive state, indicated by 0 in the figure. The number of active notches is also given.

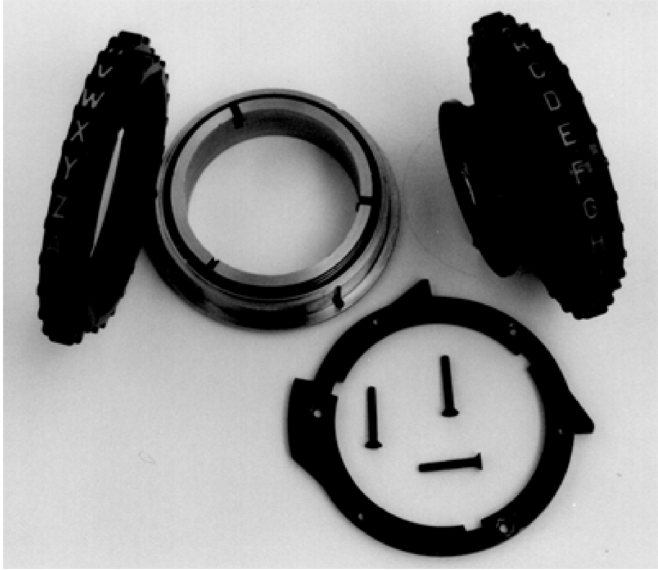


Figure 5. A contact wheel and drive wheel assembly shown disassembled into its component parts. From left to right: drive wheel letter ring, drive wheel body, notch ring (No. 12) with fixing screws and wired contact wheel assembly.

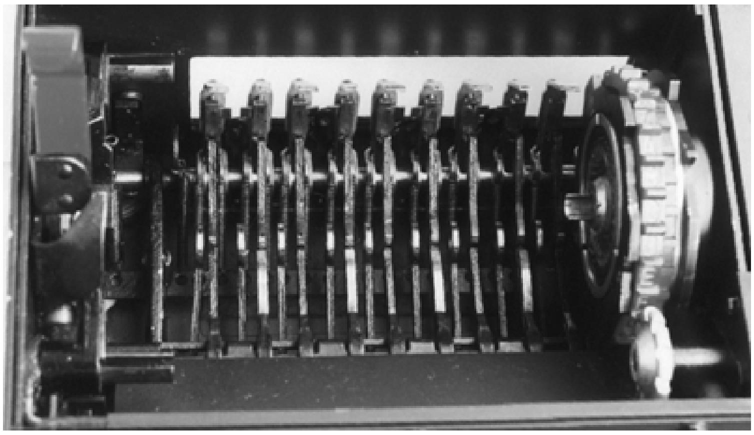


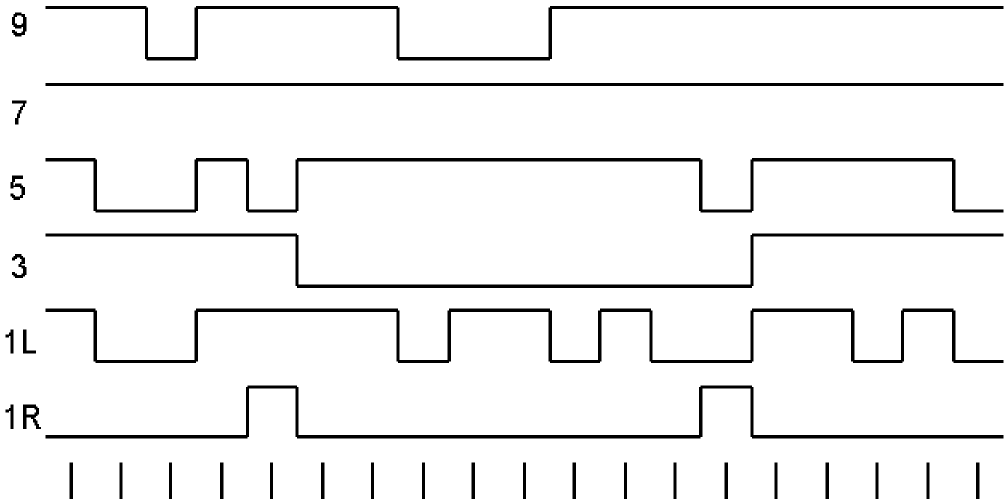
Figure 6. View of the stepping levers with all wheels removed, except the first red drive wheel. This can be removed separately to change its two notch rings. The axle release lever, shown on the left, is raised upwards to release the axle.

Wheel Movements

When a key is depressed on the keyboard, a set of ten stepping levers moves upwards. See Figure 6. The stepping levers associated with the contact wheels are wider than those for the drive wheels, shown in Figure 10. The profile of the notch ring can lift the lever away from the contact wheel drive teeth and prevent its movement. This occurs in the inactive high sections of the notch, designated by 0 in the notch patterns of Figure 4. The three levers positioned over drive wheels 1, 5 and 9 always engage and advance these wheels one step for every keyed letter. The movement of wheels 2, 6 and 10 are thus determined by the notch state at this time. Drive wheels 3 and 7 are programmed by the special notch ring on the right hand face of drive wheel 1. If this notch wheel is in an inactive state, determined by a sensing lever, then drive wheels 3 and 7 and also contact wheels 4 and 8 will not move. In an active state, drive wheels 3 and 7 will advance, while the movement of the wheels in position 4 and 8 will depend on the notch state on their drive wheels. Figure 11 shows the logical arrangement of the contact wheels and their controlling drive wheels. Figure 7 shows a typical stepping sequence of the ten moving wheels. The machine configuration used here is 12A-13B-14C-15D, where the letters designate the contact wheels and the double figures are the drive wheels installed from left to right in the machine. The red drive wheel notch rings being 22/1.

0	AAAAAAAAAA	7	WTAATTAAVT	14	PMZZOMZZSM	21	JFXWLFXWOF
1	ZZAAZZAAZZ	8	VSAASSAAVS	15	OLZZNLZZSL	22	IEXWKEXWNE
2	YYAAYYAAYY	9	URZZSRZZVR	16	NKZZNKZZRK	23	HDXWKDXWND
3	YXAAXXAAYX	10	TQZZRQZZUQ	17	NJYYNJYYQJ	24	HCXWKCXWNC
4	YWAAWWAAXW	11	SPZZQPZZTP	18	MIYYMIYYQI	25	GBXWJBXWMB
5	YVAAVVAAWV	12	ROZZPOZZTO	19	LHYXMHXXQH	26	FAWVJAWVLA
6	XUAAUUAAWU	13	QNZZONZZSN	20	KGXWLGXWPG		

Figure 7. An example of the stepping sequence for the first 26 steps starting from setting AAAAAAAAAA. The configuration used was 12A-13B-14C-15D-22/1



10	H	G	F	F	E	D	C	B	B	B	B	A	Z	Y	X	W	V	U	T
8	Y	Y	Y	Y	Y	X	X	X	X	X	X	X	X	X	W	W	W	W	W
6	K	J	J	J	I	I	H	G	F	E	D	C	B	A	A	Z	Y	X	W
4	A	A	A	A	A	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
2	M	L	L	L	K	J	I	H	H	G	F	F	E	E	E	D	C	C	B

Figure 8. Timing diagram showing wheel stepping characteristics. The six traces represent the notch states at the stepping lever position. 1L and 1R are the notch rings on left and right sides of drive wheel number 1. The slow wheels 4 and 8 move when the first notch ring, 1R is active at step 5. At step 14, wheel 8 moves once more but wheel 4 is prevented from moving by the inactive state of drive wheel 3. Note that at step 3 no contact wheels move. The notch ring configuration used is that of Figure 7 with the starting position of HFYQKFAQMF.

The stepping levers (Figures 10, 12) engage the wheels at an offset of 10 from the indicating position (i.e. the lower row of letters in the wheel window). When a wheel is set to an indicating position of A then the stepping levers will engage at position Q. The probing lever for the right hand notch ring number 1 is one step ahead, and hence at an offset of 9. The probing lever controls a shaft with four blocking arms located at positions C2, C3, C4 and C5 that can be pushed into an active position and locked by the small screw on the arm. On the machine inspected, two blocking arms were active in the combined positions C2 and C4. When the shaft is moved by the probing lever the drive wheels and contact wheels at the two active combined positions of C2 and C4 are prevented from stepping. The notch rings used on the right face of the red drive wheel rings number 1 and 2 have relatively few active positions. This gives slow stepping of the components at positions C2 and C4. The two wheels at positions 4 and 8 move at the most five steps for each revolution of the red drive wheel as illustrated in Figure 9.

Wheel No.	1 (Red)	2	4	6	8	10(UKW)
Steps	26	15	4	17	4	21

Figure 9. The number of individual wheel steps for the 26 letter sequence of Figure 7 showing
the action of the slow wheels 4 and 8.

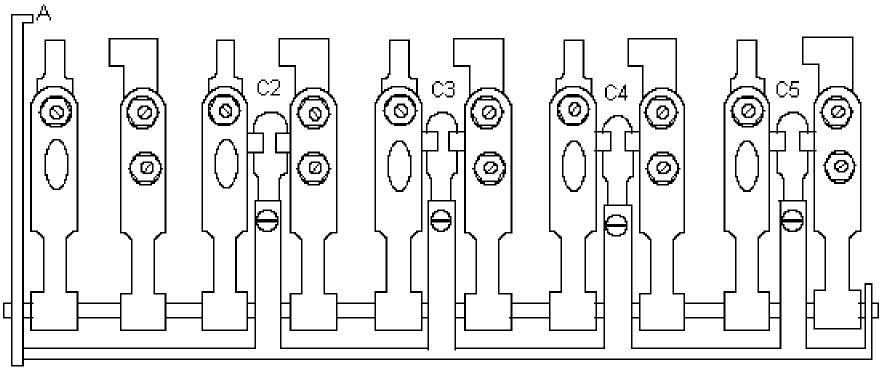


Figure 10. The Stepping lever assembly seen from the rear inspection panel. The contact wheel levers are wider than the drive wheel levers since they are required to sense the notch rings. The sensing lever A operates the shaft carrying the four blocking arms which are located at combined positions C2, C3, C4 and C5. Note there is no blocking arm at combined position C1 since it is not applicable.

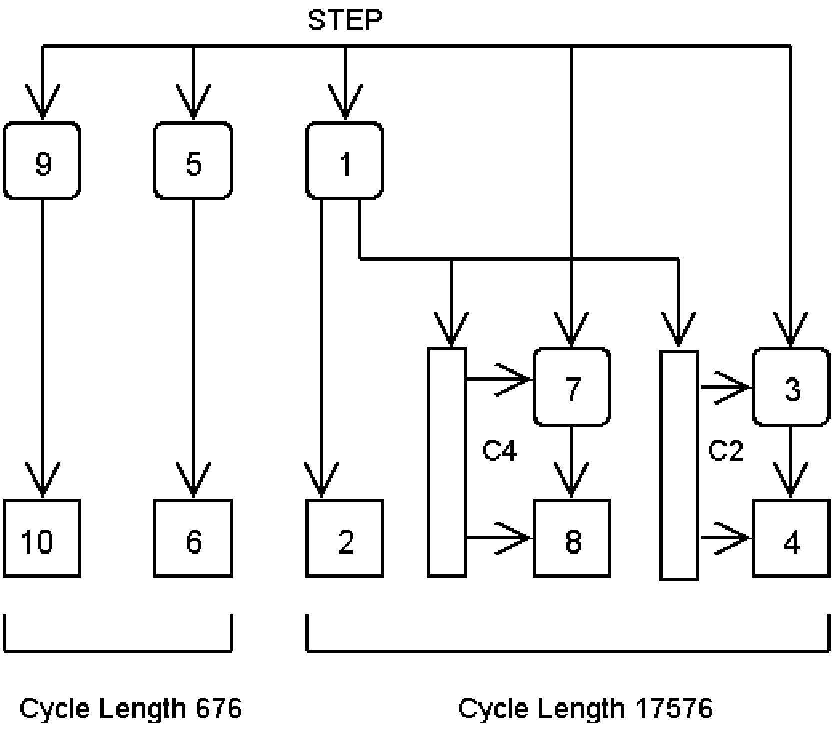


Figure 11. The logical arrangement of contact wheels and their controlling drive wheels, showing the two separate wheel groups with cycle lengths of 676 and 17576. C2 and C4 are the blocking arms controlled by drive wheel number 1.

NEMA Variations

The NEMA machines appear to have been divided into four distinct user groups, with each group being issued with its own notch rings, although the contact wheels had the same wiring. The contact wheels and the notch rings are the secret parts of the machine. The wheels were wired by the Army and not by Zellweger AG. The notch rings are not mentioned in the list of spare parts[9], which further indicates their secret nature.

A Training model was supplied with contact wheels A, B, C and D and with notch rings 16, 19, 20, 21 and 23/2 for the red drive wheel. An Operational model had the set of contact wheels A, B, C, D, E and F. The notch rings supplied being 12, 13, 14, 15, 17, 18 and 22/1 for the red drive wheel. The UKW wiring given in Figure 3 is common to both models.

The Swiss Foreign Office (FO)[10] also adopted the NEMA and had on average 100 machines in service. No further details are known about the FO machines but it is

[9] "*Ersatzteilkatalog, Chiffriermaschine* NEMA", *Armee Lager Nummer* (ALN) 7610-607-0300, 1972.

[10] *Eidgenössisches Politisches Departement* (EPD), the Swiss Foreign Office, is today named "*Eidgenössisches Departement für auswärtige Angelegenheiten* (EPA)."

suspected that they would have used completely different notch rings from those in use by the Army.

The two types of notch rings, single digit and double digit rings, have been shown to have different uses in the machine. It is clear that there can only exist a total of nine single digit rings. Four of these are known to have been used by the Army while at least one other must have been used by the FO. We are not aware of the total number of double digit notch rings but the NEMA Instruction Manual[11] mentions notch ring no. 10 and the existence of no. 32 has been confirmed. This gives a total of 23 double digit notch rings but the overall total is probably much higher. The list of spare parts for the Army machines shows that there were 12 different contact wheels labelled A–F and J–O. There are some indications that the wheels G and H were in use on the FO machines which would result in a total of 14 contact wheels. It is also possible that wheel I exists but this has not been confirmed.

It is clear from the instructions that the notch rings were intended to be changed in the field. The four blocking arms that determine which of the wheels are slow moving can be set in position with an adjusting screw and a locking nut, this being further locked in place with paint. Clearly this feature was not intended to be changed in the field. However machines can be easily modified for different wheel stepping by adjustment of the blocking arms. The Operational model and the Training model both have the blocking levers active at combined positions C2 and C4.

Machine Configuration

Considering the Operational model, issued with a set of 6 contact wheels, the number of wheel orders available is 360, slightly greater than that of the Naval Enigma[12]. There are furthermore also 360 notch wheel orders, if it is assumed that the two notch rings on the red drive wheel are not changed. The number of possible starting positions for the contact wheels is 26^5 and also for the drive wheels 26^5. The high number of possible machine settings together with the more complex stepping makes this machine reasonably secure for the period. However, it is not without its systematic features, as will be shown later.

[11] See reference [1].

[12] Ralph Erskine and Frode Weierud. “Naval Enigma: M4 and Its Rotors.” *Cryptologia*. 11(4): 235 - 244.

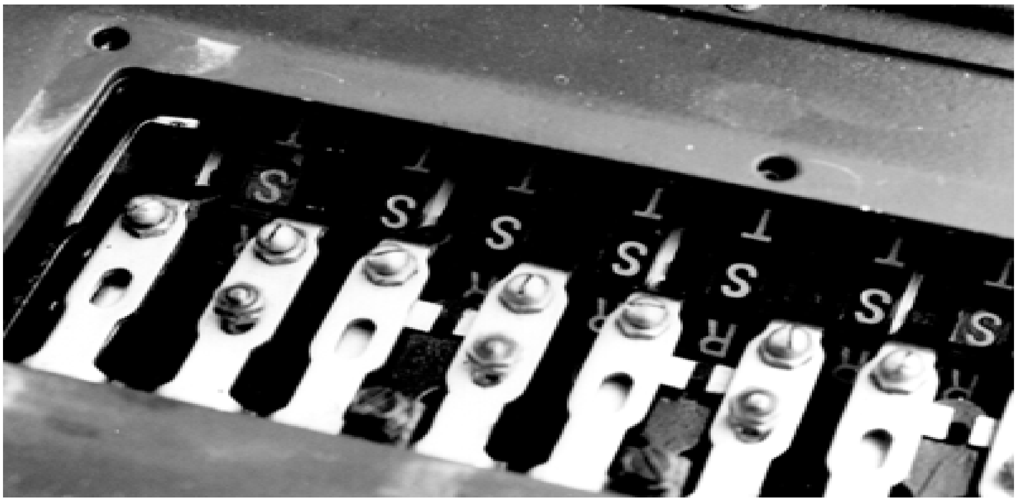


Figure 12. Stepping levers seen from the rear. On the far left is the probing lever of drive wheel 1. The stepping levers are at position S with the alphabet ring letter set to indicating position C. The Blocking arm locations can be seen at combined positions 2, 3 and 4.

Cycle Length

It might be assumed that since the NEMA has 5 wired wheels, which are controlled by notch patterns, the notch counts of which are relatively prime to each other and to the alphabet size, that the cycle length of the machine would be 11,881,376 (26^5). However this is not the position since the wheels do not interact and generate a carry, like for example the family of Enigma machines[13]. The wheels can be considered as two distinct groups. Wheels 10 and 6 are controlled by drive wheels 9 and 5 respectively and both these drive wheels advance for every letter and nothing else influences their motion. Since their notch counts are relatively prime, it follows that wheels 10 and 6 will always return to their starting positions every 676 steps (26 x 26). We now need to consider the three remaining wheels 8, 4 and 2. The maximum possible cycle length these three can have is 17576. This is indeed the case with the notch patterns that are used, all of which are relatively prime. After 17576 steps wheels 10 and 6 will also have returned to their starting position, having themselves completed 26 full cycles. Hence the machine cycle length is 17576. However this unexpected low cycle length is less of a problem than it might appear to be. A drive wheel in position 7, 3 or 1 that has a notch count with a common factor to 26 may reduce the cycle length to 8788. A cycle length as short as 1352 would be possible if two of these drive wheels have a common factor to the alphabet length.

[13] David H. Hamer "Enigma: Actions Involved in the "Double Stepping" of the Middle Rotor." *Cryptologia*, 21(1): 47-50.

However we have not attempted to fully determine the rules governing the cycle length.

An unexpected phenomenon was discovered during the study of this machine. At certain machine configurations it was noted that none of the five contact wheels moved for one letter and furthermore this event repeated every 26 letters. This produces an identical substitution alphabet for two positions in the message text at 26 letter intervals. An example of this can be seen in Figure 13. Another occurrence of a very much rarer event also happens and in this case the contact wheels do not move for 3 letters, this also repeating at 26 letter intervals. This gives an identical alphabet substitution for 3 consecutive positions in the text.

Position	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
HDXVKDVVMD	Q N J W P T X Y S C L K R B Z E A M I F V U D G H O
GCXVJCVVLC	L H V G X T D B N P Z A W I Q J O Y U F S C M E R K
FFXVJBVVLV	G S M X F E A Y N Q X U C I T R J P B O L W V K H D
FAXVJAVVLA	G S M X F E A Y N Q X U C I T R J P B O L W V K H D
EZXVIZVVKZ	C H A X N T K B J I G O Q E L V M U Y F R P Z D S W

Figure 13. The substitution alphabet map for five consecutive steps. An example of the non-stepping phenomenon. This particular event will repeat at 26 letter intervals.

The non-stepping occurs when the fast drive wheels 9, 5 and 1 have an inactive notch aligned with the wheel stepping levers and the slow wheels are either aligned with an inactive notch on their drive wheels or are prevented from stepping by the blocking arms. Since the three fast drive wheels have a cyclic period of 26 and the right hand notch wheel of the first drive wheel has very few active positions, then periodic non-stepping can occur for many machine configurations. Non-stepping for 3 letter positions can only occur when notch ring number 22 is used on the red drive wheel, since it has several sections of two adjacent inactive positions. Notch ring number 23 in this position only gives non-stepping for 2 letters since it only has single inactive positions, hence the wheel in position 2 would always advance after 2 letters.

For the Operational model, cyclic non-stepping occurs for 16666 out of a possible total of 17576 settings of drive wheels 1, 5 and 9 which is the worst case with notch rings 15 and 17 in positions 5 and 9. The number of settings is configuration dependent and is lowest with notch rings 12 and 18 where the figure is 3458. The maximum cyclic non-stepping for 3 positions is also a maximum for notch rings 15 and 17 at 2236 positions. The Training model shows this cyclic nature much less frequently, and non-stepping for 3 letters is entirely absent. It is interesting to note that the cyclic non-stepping could be eliminated by arranging for the notch patterns on either side of the red drive wheel to be complementary patterns offset by one position. This was not attempted for some reason. Perhaps it was not considered a weakness in view of the limited data processing capacity of the time and the ease at which notch rings could be easily and cheaply distributed.

It should also be noted that the motion of the slow drive wheels 3 and 7 is a repeating cyclic pattern which is determined by the notch pattern of the right hand notch ring on the red drive wheel and this cyclic pattern therefore has a period of 26. It is clear that the NEMA was designed to prevent attacks against the fast wheels that were used so successfully against the Enigma. It is interesting to speculate whether the peculiar stepping features of the NEMA offered a more secure cipher.

Cryptographic Use

The general use of the machine is indicated in the NEMA Instruction Manual while cryptographic usage like setting up of the inner key etc. is given in the small booklet entitled “Cipher Procedure for the NEMA Machine.”[14] The procedure indicates that the secret key will be issued by special key instructions and that the period of validity will depend on the type of traffic and will therefore vary from case to case.

The secret key consists of two parts:

a) The inner key, which gives the order of the contact wheels and the drive wheels and which is given in the following form:

11A – 15F – 12D – 14B

b) A code word, which by the following instructions will give the outer key (message key). The code word must have 10 or more letters, e.g.:

ZAR UND ZIMMERMANN

The cipher procedure states that to maintain the cryptographic security every text must be enciphered using a different message key. The procedure for generating the message key is the following:

a) On the machine where the present valid inner key is in use, the first 10 letters from the secret code word is set up from left to right on the letter rings of the 10 wheels.

[14] “*Schluesselungsverfahren für die* NEMA-*Maschine*”, *Geheim* (Secret), *Ausgabe Mai* 1948. Dual language instructions, German and French.

b) The cipher clerk then selects 10 random letters, divides them into two five letter groups and places the groups as the two first groups of the ciphertext. The two same groups will be added at the end as the two last groups of the ciphertext.

c) With the machine as adjusted under a) the selected 10 random letters are enciphered and noted on a separate piece of paper.

d) The resulting 10 enciphered letters constitute the desired secret message key and the 10 letters are set up on the letter rings from left to right. The letter counter on the machine is set to zero and the message can be enciphered.

Using the secret code word above the first 10 letters adjusted on the letter rings under step a) will be ZARUNDZIMM. If the 10 random letters are QZAFJ TMCAR and the enciphered result is ZOLMKALRQU it is these letters that will make up the message key, while the groups QZAFJ TMCAR will be the two first and the two last groups of the cipher text.

From the information given in the NEMA Cipher Procedure booklet it is possible to derive some additional information about the usage of the machine. First of all the inner key does not give any information about the notch rings on the red drive wheel, something that indicates that the notch rings on this wheel never or rarely changed and then only on special order.

There are no warnings in the instructions about how to choose the 10 random letters. This shows the cryptographers assumed it is very unlikely that the same or similar 10 letter sequences will be chosen except by chance. If, however, it would happen that the letters for the contact wheels would be chosen to be exactly the same from one message to another, the irregular motion of the wheels will in most cases prevent encipherment in depths. But real in-depth encipherment will only occur if some of the drive wheel letters are also the same. Even in these extreme cases the in-depth sequences are relatively short (3–8 letters). However, they have a tendency to reoccur at intervals which are sometimes multiples of 26.

That the 10 random letters are given in clear and that it is the resulting 10 enciphered letters that are used as the message key is a much better procedure than that normally used with the Enigma. This way no information about the machine can be given away through the message key. The NEMA Cipher Procedure booklet does not mention anything about a cipher indicator, which probably means that on a given radio/cipher net only one cipher was in use at a given time. The repetition of the two first groups at the end and the use of five letter groups might also have indicated that it was a text enciphered on the NEMA. The hand ciphers in use by the Swiss Army at that time, e.g. SP – *Senkrecht-Playfair* (Vertical Playfair)[15], usually transmitted the ciphertext in groups of four.

The Cipher Procedure also explains how to deal with numbers. The keys on the upper row, QWERTZUIOP, as well as the corresponding lamps, also represented the numbers 1,2,3,4,5,6,7,8,9,0 in that order. When numbers were to be enciphered they would be preceded with Y and they would also be separated by Y. The return to letters would be indicated with an X after the last number. X could also be used as a word separator but only when this was absolutely necessary.

Some Additional Features

The NEMA keyboard consists of 32 keys. In addition to the keys A - Z there are three extra keys labelled WR, ZL and BU and an unmarked Space bar. There are also two unused, unmarked keys. Only the 26 letter keys connect to the scrambler. A 34 pole connector, shown in Figure 14, is provided on the right side panel of the machine for connection to an external teleprinter or lampboard, the latter enabling faster operation. The keys WR, ZL, BU and space connect to four of these contacts with a separate common pin and are intended for use with the teleprinter. The remaining contacts pins are assigned to the 26 lamps, one lamp common pin and two unused. As far as we know the teleprinter connection was not used by the Swiss Army, but the Swiss FO used the machine with an IBM electric typewriter.
The machine may be operated from its internal mains supply, with voltage sources of 110 - 250 volts or by an internal battery or external accumulator.

[15] Gerhard Sulger Büel und Rudolf J. Ritter, "*Das Fernmeldematerial der Schweizerischen Armee seit* 1875, 10. *Folge: Codes und Chiffrierverfahren*". To be published.

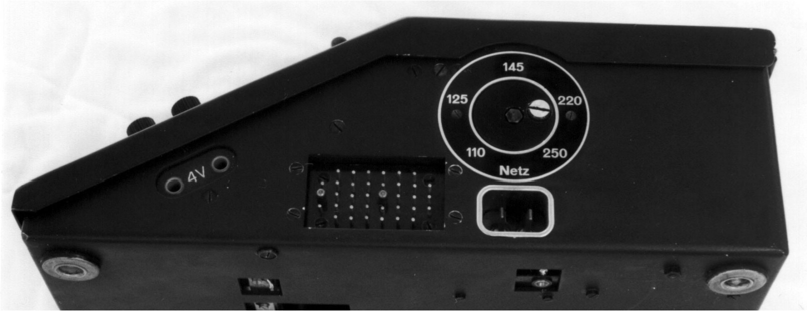


Figure 14 View of right side of machine showing the power connectors and external lampboard and teleprinter connector.

NEMA Simulator

This study of the NEMA was done in conjunction with the development of a computer simulation program. The program was designed to replicate all the feature of the cipher machine in a graphical environment. The simulator was designed to run on Intel based PCs under Windows operating systems. The wheel configurations are available for selection from the program menu. The program can be switched to simulate the Training model or the Operational model. The program accurately reproduces the function of the real machine and also contains some extra functions to allow further investigations of the properties of this cipher machine. Developing a graphical simulation program has proved to be a good method of obtaining a thorough understanding of the machine. It is hoped that a version of the NEMA simulator will be available for download from the authors' WWW Home Pages.

Acknowledgements

The results presented here are based on inspection and studies of NEMA machines that have been on loan to one of the authors over a period of time. For this we should like to specially thank the Swiss Army's Cipher Bureau whose help and encouragement has been of great importance. We should further like to express our very special gratitude to Dipl. Ing. Rudolf J. Ritter and Dipl. Ing. Gerhard E. Sulger Büel who have allowed us to share their immense knowledge about the NEMA's history and use. The authors should also like to thank Dipl. Math. Paul Glur for his help in clarifying several obscure points in the NEMA's history, as well as Dr. David H. Hamer and John Alexander, who in the final phase of our study have helped us a great deal in getting a better understanding of some of the technical details. As always we are indebted to our good friends and fellow researchers Ralph Erskine and Philip Marks for help with documents and for a thorough review of the paper. The quotation from the PRO document, which is Crown Copyright, is reproduced with the permission of the Controller of Her Majesty's Stationery Office.

References

1. Bedienungs-Anleitung zur Chiffriermaschine 'NEMA'.
Zellweger A.-G. No. 117.660-1, 30 April 1947. Dual language instructions, German and French.

2. Schluesselungsverfahren für die NEMA-Maschine. Geheim (Secret), Ausgabe Mai 1948. Dual language instructions, German and French.

Biographical Sketches

Geoff Sullivan works on the design of forensic science instruments as a programmer and electronics engineer. He has many other varied interests, but is all too easily distracted by cryptography.

Frode Weierud is employed by the European Organization for Nuclear Research (CERN) in Geneva. He works as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 30 years. His cryptological research is focussed on cipher machines and cryptanalytical techniques.