Die Chiffriermaschine Nema

Kryptologische Grundlagen
Entwicklung der Rotormaschine
Brechen der Rotormaschine
Arbeiten mit der Nema
Geschichte der Nema
Technische Details

Walter Schmid

Dritte überarbeitete und erweiterte Auflage
Titelbild: Die Chiffriermaschine Nema [BRS]
Bewilligung Bundesarchiv: 451-11322 vom 2.12.2004
Copyright: Walter Schmid, CH-8634 Hombrechtikon

Vorwort

Die mechanische Chiffriermaschine "Nema" wurde in den 1940er-Jahren in der Schweiz entwickelt und gebaut. Sie stand von 1947 bis etwa 1977 bei der Schweizer Armee und im Verkehr mit den Botschaften im Einsatz. 1992 wurde die Nema aus der Geheimhaltung entlassen. Ein Teil der Maschinen wurde an Sammler verkauft.

Die Nema ist eine Weiterentwicklung der legendären Enigma, jener Chiffriermaschine, die von den Deutschen im Zweiten Weltkrieg eingesetzt wurde, und deren Code zuerst die Polen, später die Alliierten systematisch und mit enormem Aufwand brachen.

Zur Nema ist nur wenig Literatur vorhanden. Die zur Maschine gehörende Instruktion zur Schlüsseleinstellung und die Bedienungsanleitung gehen nicht auf die Grundlagen der Maschine ein, vor allem wird nicht auf systembedingte und sicherheitsrelevante Schwachpunkte hingewiesen, die der Enigma und der Nema anhaften.

Die vorliegende Dokumentation vermittelt im ersten Teil einen Überblick über die verschiedenen Chiffrierverfahren. Ausführlicher wird jenes behandelt, das den Rotormaschinen zu Grunde liegt. Am Beispiel der Enigma zeige ich, wie die theoretischen Überlegungen in einer mechanischen Maschine realisiert werden können. Der Schritt zur Nema ist dann nicht mehr gross.

Aussergewöhnliche Umstände führten zur Entwicklung der Nema. Anhand von Literaturauszügen und Dokumenten aus dem Bundesarchiv ist diese spannende Geschichte ausführlich dargelegt.

Der zweite Teil zeigt, wie mit der Enigma und der Nema gearbeitet wurde und welche Schwächen den beiden Rotormaschinen innewohnen, die letztlich Ansatzpunkte zum Brechen des Enigma-Codes lieferten. Die kleinen, aber entscheidenden Unterschiede bei der Mechanik und der Schlüsselorganisation zwischen Enigma und Nema werden im Detail erklärt.

Der dritte Abschnitt befasst sich ausführlich mit der Bedienung der Nema. Die besonderen Massnahmen werden vorgestellt, die getroffen wurden, um ein Brechen des Codes zu verhindern, oder doch wenigstens zu erschweren. Die Grundlagen dazu stammen aus meinen persönlichen Erfahrungen, die ich beim Arbeiten mit der Nema in verschiedenen militärischen Kursen sowie im Botschaftsfunk gemacht habe. Sicher war der Nema-Code feindlichen Angriffen ausgesetzt; ob solche auch erfolgreich waren, das weiss man nicht. Darüber kann man nur Vermutungen anstellen und spekulieren.

Anhand nachvollziehbarer Beispiele zeige ich, wie die Funktion der Nema berechnet werden kann. Alle dazu notwendigen Informationen sind als Tabellen in dieser Dokumentation enthalten.

Für die Enigma und die Nema wurden Simulationsprogramme geschrieben. Im Anhang werden zwei dieser Simulatoren für die Nema vorgestellt.

Hombrechtikon, Februar 2005/3 Walter Schmid

Inhaltsverzeichnis

Einführung 6
- Was ist Chiffrieren? 6
- Warum wird chiffriert? 7
- Wer chiffriert? 7

Grundlagen 8
- Das Vor-Computer-Zeitalter 8
- Begriffe 8
  - Algorithmus 8
  - Schlüssel 9
  - Telegramm 9
  - Zeichensatz 9
  - Klartext – Geheimtext 9
  - Fünfergruppen 9

Chiffrierverfahren 1 10
- Steganografie 10
- Codierung 10
- Transposition 11
- Substitution 12
- Zufallsverteilung erzeugen 13
- Dechiffrieren 14
- Monoalphabetisch reichte aus 14

Kryptanalyse 1 15
- Cäsar brechen 15
- Die Statistik deckt auf 15
- Mit Intuition und Probieren zum Ziel 16
- Statistiktabellen 17

Chiffrierverfahren 2 18
- Homophone Substitution 18
- Polyalphabetische Substitution 18
- Das Verfahren nach Vigenère 19

Kryptanalyse 2 21
- Vigenère wird gebrochen 21
- Absolute Sicherheit 23
- Erzeugen von echtem Zufall 24
- Die Sicherheit muss umfassend sein 24

Die Rotormaschine 25
- Taster und Lämpchen 25
- Der Rotor 25
- Automatischer Vorschub 26
- Weiterentwicklung 26
- Wie dechiffrieren? 27
- Einführung des Reflektors 27
- Involutorische Permutation 28
- Die Enigma 29
  - Das Steckerbrett 29

Die Nema 33
- Wann und warum wurde sie gebaut? 33
- Verbesserungen gegenüber der Enigma 34
- Wichtige Teile der Maschine 36
  - Reservewalzen 38
  - Originalbatterie 38
- Inbetriebnahme 39
- Schlüssel einstellen 39
- Detailbilder der Nema 41

Schlüsselorganisation 42
Netzarten 42
Chiffrieren mit der Enigma 44
Chiffrieren mit der Nema 45
Grundsätzliche Fragen 46

Brechen der Enigma 48
Schwachpunkte 48
Die Stunde der Genies 48
Bletchley Park 49

Arbeiten mit der Nema 50
Vorsicht: Feind liest mit! 50
Bescheidener Zeichensatz 50
Abmachungen 51
Aus Fehlern lernen 52
Verschiedene Sicherheitsvorkehrungen 52
Wichtige Regeln 53
Falsche Eingaben korrigieren 53

Wurde die Nema gebrochen? 55
Warum wurde die Nema aufgegeben? 57

Mehr Sicherheit 58
Mehrfachverschlüsselung 58
Moderne Algorithmen 59

Geschichte der Nema 61
Zuerst war die Enigma 61
Die Schweizer Enigma wurde gebrochen 61
Soldaten als Erfinder 65
Eine Neue Maschine wird gebaut 65
Die Erfinder wehren sich 73
Weitere Dokumente zur Geschichte 75

Anhang 80
Walzenvorschub der Nema 80
Zur Periodendauer 82
Varianten der Fortschaltmechanik 84
Varianten beim Walzensatz 86
Nummernzuteilung 87
Was geschah mit den Maschinen? 88
Walzensätze der Militärmaschinen 89
Die letzten Geheimnisse der Nema 91
Berechnen des Walzenvorschubs 93
Berechnen der Permutation 95
Elektrische Verdrahtung 100
Simulationsprogramme 101
Programm für die Nema 101
Übungsbeispiele 104
Simulator Sulivan / Weierud 106
Literatur 108
Informationen im Internet 109
Dokumente im Bundesarchiv 109
Bildnachweis 109
Dank 109
Anschrift des Autors 109

Inhaltsverzeichnis

Seit es vernunftbegabte Wesen gibt, besteht der Wunsch, vertrauliche Meldungen an Einzelpersonen oder Mitglieder einer bestimmten Gruppe weiterzuleiten.

Einführung

Was ist Chiffrieren?

Beim Chiffrieren wird ein Text so verändert, dass ein aussenstehender Beobachter den Sinn des Geschriebenen nicht mehr verstehen kann. Er sieht nur noch eine Ansammlung sinnloser Zahlen, Buchstaben und Symbole. Das geheime Verfahren, mit dem dies erreicht wird, kennen nur zwei Stellen: Der Absender, der die Meldung chiffriert hat und der Empfänger der Nachricht. Dieser ist mit dem geheimen Wissen in der Lage, den ursprünglichen Text wieder buchstabengetreu herzustellen. Ein unerwünschter Beobachter oder Horcher wird versuchen, die Mitteilung unerlaubterweise zu entziffern. Das Wissen um den Inhalt der Mitteilung kann ihm Vorteile verschaffen. Mit grossem Aufwand gelingt es ihm vielleicht den Sinn der Meldung aufzudecken. Je grösser der Aufwand ist, den er dafür betreiben muss, desto sicherer wird ein Chiffrierverfahren eingestuft.

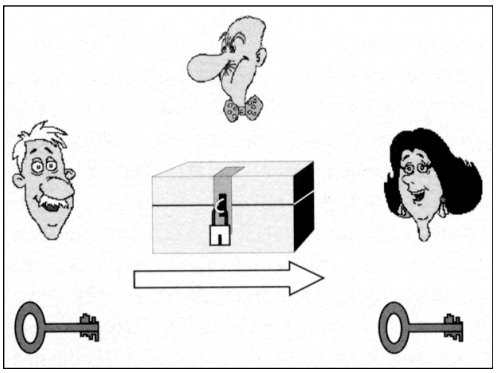


1 Neugier und persönliche Vorteile sind der Antrieb, vom Inhalt vertraulicher Meldungen Kenntnis zu erlangen. [16]

Mit dem Chiffrieren wird der Inhalt einer Mitteilung vor den neugierigen Augen eines unerwünschten Beobachters verborgen.

Abb. 2 zeigt das Verfahren in symbolischer Weise. Der Absender, Herr Weiss, legt die geheim zu haltende Meldung in eine Kiste, die er mit einem Schloss verschliesst. Dieser Vorgang entspricht dem Chiffrieren. Dann übergibt er die Kiste der Post für den Transport. Die Empfängerin, Frau Schwarz, ist im Besitz des passenden Schlüssels. Nur sie kann die Kiste wieder öffnen und die Meldung lesen. Das Öffnen der Kiste entspricht dem Dechiffrieren. Ein neugieriger Beobachter, Herr Kahl, der die Meldung gerne lesen möchte, stellt wohl fest, dass eine Kiste verschickt wird, er weiss aber nicht, was sie enthält. Ohne Schlüssel kann er die Kiste nicht öffnen, selbst dann nicht, wenn er Zeit und Gelegenheit hat, sich mit dem Schloss und der Kiste eingehend zu beschäftigen. Um das Schloss öffnen zu können, müsste er einen passenden Nachschlüssel anfertigen oder sich einen solchen beschaffen.

Abb. 5 zeigt den Vorgang des Chiffrierens etwas theoretischer: Der Klartext des Telegramms wird nach einem oft geheim gehaltenen Verfahren und mit einem streng geheimen individuellen Schlüssel in einen unverständlichen Geheimtext umgesetzt. Ein unerwünschter Beobachter kann den übermittelten Geheimtext wohl mitlesen oder abhören, den Inhalt des Textes jedoch nicht verstehen. Nur der Empfänger, der die Methode und den geheimen Schlüssel kennt, ist in der Lage, den ursprünglichen Klartext wieder herzustellen.



2 Hier wird der Vorgang des Chiffrierens symbolisch dargestellt. [1]

Beim klassischen Chiffrieren wird nicht verheimlicht, dass eine Meldung verschickt wird, es wird jedoch verhindert, dass unberechtigte Personen deren Inhalt vor ihre Augen bekommen.

Warum wird chiffriert?

Geheime oder vertrauliche Mitteilungen reisen auf ihrem

Weg vom Absender zum Empfänger oft durch unsichere Kanäle. Unsicher heisst, dass unbekannte und unberechtigte Personen die Möglichkeit haben, die Meldung in die Hände zu bekommen oder abzuhören. Sehr unsicher ist natürlich die Funkverbindung, sie kann weltweit abgehört werden. Unsicher sind auch Drahtverbindungen, also Telefon und Fernschreiber; staatliche Dienste können diese problemlos anzapfen. Auch die Briefpost ist nicht vor neugierigen Augen sicher. Selbst der einem Kurier mitgegebene Brief kann in falsche Hände geraten.

In den wenigsten Fällen sind es Privatpersonen, die sich für fremde Meldungen interessieren. Meist sind es Geheimdienste, die systematisch fremde Funksprüche, Telefongespräche und Telefaxe abhören und mitschreiben. Selbst die Briefpost wurde – und wird sicher auch noch heute – von den Nachrichtendiensten geöffnet und gelesen, siehe Abb. 6.



3 Die etwas altmodische Zustellung per Brieftaube wird oft belächelt; sie stellt aber einen recht sicheren Übertragungsweg dar, in den nicht so leicht eingedrungen werden kann. [16]

Der Grund des Chiffrierens liegt darin, dass geheime Meldungen durch unsichere Kanäle übermittelt werden müssen, weil keine sicheren Kanäle zur Verfügung stehen.

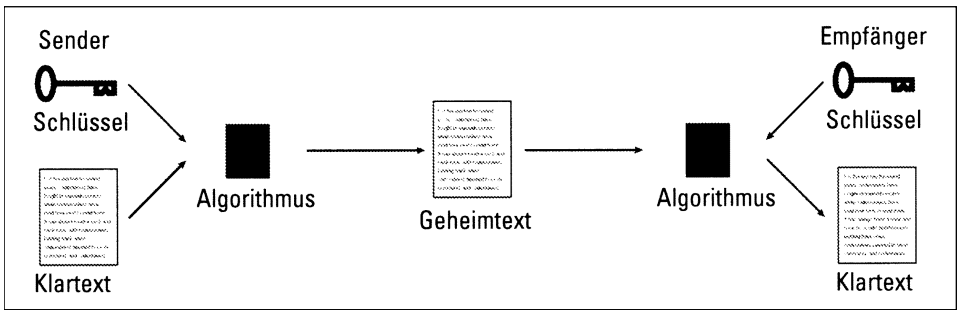
Wer chiffriert?

Es sind vor allem die Militärs, die geheime Mitteilungen über Funkverbindungen austauschen. Ein weiterer Anwenderkreis des Chiffrierens sind Regierungen, die über Funk und Draht mit ihren diplomatischen Vertretungen und Missionen im Ausland in Verbindung stehen. Aber auch die Banken, die Wirtschaft, die Industrie und die Polizei tauschen geheime oder vertrauliche Meldungen aus und verhindern mit dem Chiffrieren, dass von unerwünschter Seite mitgehört wird.

Das Chiffrieren hat übrigens noch einen interessanten Nebeneffekt: Der Empfänger einer chiffrierten Nachricht ist sicher, dass die Meldung unverändert ist und vom "richtigen" Absender stammt. Nur dieser besitzt den gleichen Schlüssel wie der Empfänger. Was der Empfänger dechiffrieren kann, muss vom "richtigen" Absender chiffriert worden sein. Im Verkehr zwischen Banken ist dieser Aspekt, die Authentizität einer Meldung, ebenso wichtig wie das Sichern der Meldung gegen unberechtigtes Mitlesen.

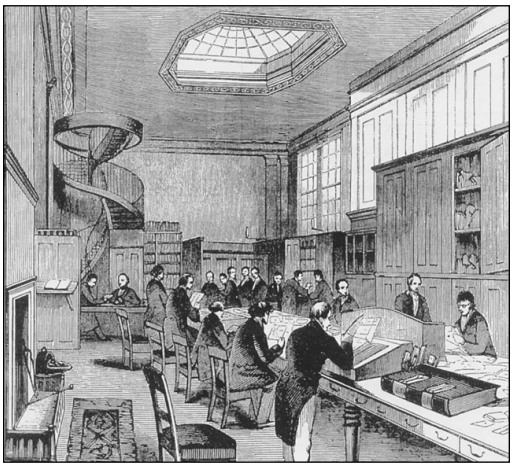


4 Jeder Funker weiss, oder sollte wissen, dass seine Aussendungen abgehört werden. [18]



5 Das Chiffrieren in abstrakter Form dargestellt. [13]

Chiffrieren ist eine exakte Wissenschaft, es ist nichts Geheimnisumwobenes; alles was damit zusammenhängt wird aber oft geheim gehalten.



6 "Handarbeit" in früheren Zeiten. In einem Hinterzimmer des Londoner Oberpostamtes werden Briefe geöffnet und abgeschrieben. [16]

Kryptologie

- Verschlüsseln
- Kryptografie
- Kryptanalyse
- Chiffrieren
- Dechiffrieren
- Codieren
- Schlüssel
- Algorithmus
- Entschlüsseln

Grundlagen

Das Vor-Computer-Zeitalter

Die Betrachtungen in dieser Dokumentation gelten für das "Vor-Computer-Zeitalter", also bis etwa 1960. Damals begann der Siegeszug der elektronischen Rechenmaschine auf breiter Front. Aus heutiger Sicht mögen einige Aussagen veraltet sein, teilweise sind sie nicht mehr zutreffend. Sie waren damals so zu sagen "Stand der Technik". Was heute der Computer in Sekunden berechnet, analysiert und auswertet, bescherte damals Handarbeit über Stunden, Tage, ja Wochen und Monate. Und fehlerfrei wie der Computer war die Handarbeit auch nicht!

Begriffe

Obwohl sehr vieles, das mit dem Chiffrieren zusammenhängt, streng geheim gehalten wird, ist das Chiffrieren nichts Geheimnisvolles. Alles was mit Chiffrieren, Dechiffrieren und Code brechen zu tun hat ist eine exakte Wissenschaft. Es ist ein Zweig der Mathematik, zusammengefasst unter dem Begriff **Kryptologie.** Das eigentliche Chiffrieren oder die Erfindung und Entwicklung neuer Chiffriermethoden wird **Kryptografie** genannt.

In Abb. 2 bedienen sich Herr Weiss und Frau Schwarz der Kryptografie. Herr Kahl dagegen möchte ohne Kenntnis der Methode und des Schlüssels die Nachricht lesen. Er wendet die **Kryptanalyse** an, um die chiffrierte Meldung zu brechen, zu knacken. Dazu muss er nicht unbedingt das Schloss öffnen (den Schlüssel besitzen), es gibt andere Möglichkeiten, ein Schloss oder eine Kiste gewaltsam aufzubrechen.

Die Begriffe "**Chiffrieren**" und "**Verschlüsseln**" sind identisch und bedeuten die Umwandlung von Klar- in Geheimtext. Unter "**Dechiffrieren**" und "**Entschlüsseln**" versteht man das Wiederherstellen des Klartextes.

Die Begriffe "**Codieren**" und "**Decodieren**" werden von Nichtfachleuten oft in der Bedeutung von "Chiffrieren" und "Dechiffrieren" verwendet. Sie haben jedoch eine andere Bedeutung, mehr dazu später.

Algorithmus

Ein Algorithmus ist eine exakte Anweisung, wie etwas (meist mathematisch) zu machen ist, wie man vorzugehen hat. Das Ergebnis muss eindeutig sein; von verschiedenen Personen angewandt, muss ein Algorithmus immer das gleiche Resultat liefern. Die Anweisungen von Algorithmen können auf verschiedene Arten ausgeführt werden: Mit einem Computerprogramm, mit einer mechanischen Maschine, von Hand mit Papier und Bleistift, oder im Kopf. Einen Algorithmus kann man am besten mit einem Computerprogramm vergleichen oder mit einem Rezept. Hingegen ist er keine mathematische Formel. Er ist auch keine Regel, denn diese hat per Definition Ausnahmen, was beim Algorithmus nicht der Fall ist.

Schlüssel

Unter dem Schlüssel versteht man die individuelle Einstellung eines Verfahrens. Im Beispiel nach Abb. 2 verwendet Herr Weiss wohl immer den gleichen Schlosstyp,

ein Vorhängeschloss genau definierter Beschaffenheit. Jedes Schloss hat jedoch seinen individuellen Schlüssel. Die genaue Form des Schlüsselbartes ist die individuelle Einstellung bei diesem Verfahren. Herr Weiss hat eine grosse Auswahl verschiedener Vorhängeschlösser auf Lager. Er wird eines verwenden, zu dem Frau Schwarz den passenden Schlüssel besitzt. Sie wird das Schloss nicht nochmals verwenden. Nachdem sie es geöffnet hat, wirft sie es weg, oder tauscht den Schliesszylinder aus. Man will den gleichen Schlüssel nicht mehrfach einsetzen, denn man kann nie ganz sicher sein, ob es Herr Kahl in der Zwischenzeit nicht doch gelungen ist, den passenden Schlüssel nachzumachen oder durch Verrat zu einer Kopie zu kommen.



7 Der Schlüssel ist der Inbegriff des Individuellen und Geheimen. Nur sein Besitzer kann bestimmte Vorgänge auslösen. [AUT]

Telegramm

Diesen Ausdruck verwende ich im folgenden als Synonym für "Meldung" oder "Mitteilung". Es ist ein kurzer, klarer Text mit einem stark eingeschränkten Zeichensatz. Auf die grafische Gestaltung und die Typografie wird kein besonderer Wert gelegt, wichtig ist lediglich der Inhalt.

Zeichensatz

Der Zeichensatz ist die Gesamtheit aller Zeichen, die von einem Chiffrieralgorithmus verarbeitet werden kann. Er kann aus Klein- und Grossbuchstaben, Zahlen, Interpunktionszeichen und Gestaltungselementen (Absatz, Tabulator, Schrifttyp, Schriftgrösse usw.) bestehen. Für die Übermittlung von Telegrammen reicht in der Regel ein stark eingeschränkter Zeichensatz aus, siehe Abb. 8.

ankunft in zuerich hb am achten mai um zwanzig uhr neunzehn stop bitte abholen stop erkennungszeichen ist gruener hut und zeitung in der linken hand stop stephan stop

8 Ein Telegramm lässt sich mit einem auf die 26 Kleinbuchstaben (und den Wortabstand) reduzierten Zeichensatz abfassen. [AUT]

Klartext – Geheimtext

Unter dem Klartext versteht man den originalen, lesbaren Text, so wie ihn der Absender abgefasst hat. Als Ergebnis des Chiffrierens erhält man den Geheimtext. Dieser muss nicht zwingend den gleichen Zeichensatz umfassen wie der Klartext. Es ist durchaus möglich, dass der Geheimtext nur aus Zahlen besteht. Es mag eigenartig anmuten, dass der Geheimtext überhaupt nicht geheim ist, er kann z. B. im Funkverkehr abgehört werden. Vielleicht sollte man ihn, um Missverständnissen vorzubeugen, als "Chiffrat" bezeichnen. Ein Ausdruck, den man hie und da antrifft, der aber nicht sehr geläufig ist.

Fünfergruppen

Der vom Chiffrieralgorithmus erzeugte Geheimtext ist ein Bandwurm ohne irgend welche Strukturen, Wortzwischenräume sind nicht mehr vorhanden. Für die Übermittlung ist es hilfreich, wenn der Bandwurm in Fünfergruppen aufgeteilt wird. Nach fünf Geheimtextzeichen wird jeweils ein Abstand eingefügt. Die so entstehenden Gruppen werden als Worte bezeichnet. Für den Funker ist die Aufteilung des Geheimtextes in Gruppen oder Worte eine Voraussetzung für die effiziente Übermittlung per Morsecode.

```
ikdlu dlwfr vbleu sqydd tavue aymbf
fbpwz eaexs affdb anwrh beqgd jhijx
nxcjj xdnnm cluub pgcza kpfug qohtw
upuuk mpnwp vuwbg buazc rfkka krfir
taaqt hthxo dlwfr vbleu sqydd tavue
zpulb fbpwz eaexs affdb anwrh beqgd
czpid nxcjj xdnnm cluub pgcza kpfug
cgwqv upuuk mpnwp vuwbg buazc rfkka
bqpyw taaqt ikdlu hthxo taaqt hthxo
tavue aymbf jgjfh inioa zpulb fbpwz
beqgd jhijx brbxw jefud czpid nxcjj
kpfug qohtw weanq lbxgo cgwqv upuuk
rfkka krfir cluub pgcza kpfug qohtw
upuuk mpnwp vuwbg buazc rfkka krfir
```

9 Der besseren Übersicht wegen und als Hilfe für den Funker, wird der Geheimtext in Fünfergruppen aufgeteilt. [AUT]

Ein Chiffrierverfahren muss nicht nur sicher sein, es muss in der Praxis unter erschwerten Bedingungen auch sicher gehandhabt werden können.

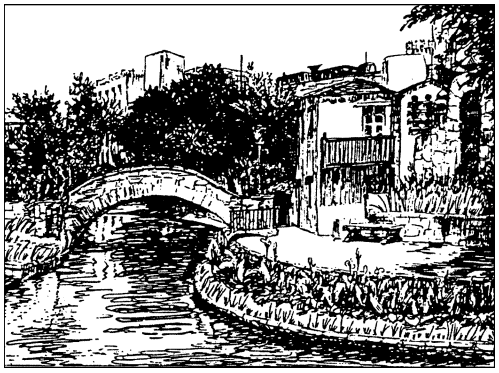
Chiffrierverfahren 1

Für das Chiffrieren kennt man mehrere grundlegend verschiedene Verfahren oder Algorithmen. So wie es die verschiedensten Arten von Schliessmechanismen und Schlüsseln gibt, kennt man beim Chiffrieren verschiedene Wege, um das gewünschte Ziel zu erreichen. Jedes Verfahren hat seine Vor- und Nachteile. Je nach Einsatzgebiet, Umständen und Bedürfnissen ist die eine oder die andere Methode besser geeignet. Wir wollen uns nachfolgend mit den wichtigsten Verfahren kurz vertraut machen. Ausführlicher werden wir auf dasjenige eingehen, das den mechanischen Rotormaschinen (Enigma und Nema) zu Grunde liegt.

Steganografie

Mehr als Erklärungen sagen Beispiele:

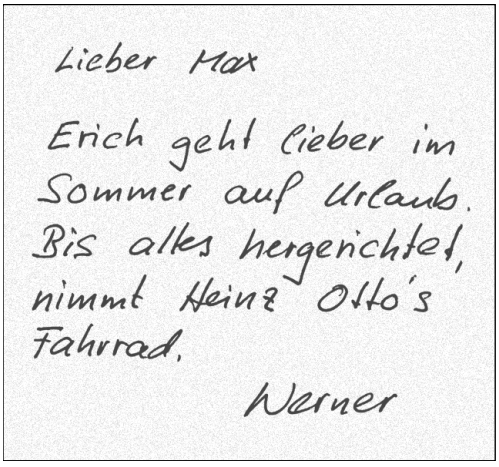
- Geheimtinten und Mikrofilme kennt man als Vertreter der **technischen Steganografie**.
- Verborgene Bilder in komplizierten Strichzeichnungen (Vexierbilder) sind Vertreter der **grafischen Steganografie**, siehe Abb. 10.
- Bei der **linguistischen Steganografie** versteckt man die geheime Botschaft in bestimmten Buchstaben eines harmlosen Textes. So können z. B. die ersten Buchstaben aller Worte, aneinander gereiht, die verborgene Mitteilung bilden, siehe Abb. 11. Man kennt in der linguistischen Steganografie noch verschiedene andere, raffiniertere und weniger leicht durchschaubare Methoden.



10 Grafische Steganografie. Die Information ist in den verschieden langen Grashalmen verborgen, die man entlang des Kanals erkennt. [5]

Bei der Steganografie wird nicht im eigentlichen Sinn unkenntlich gemacht, es wird eher getarnt. Mit Belanglosem wird vom Wesentlichen abgelenkt. Grundsätzlich wird verheimlicht, dass überhaupt eine geheime Meldung vorliegt.

Linguistische Steganografie wird vom geübten Auge rasch als solche erkannt. Der Text wirkt unnatürlich, gestelzt, unzusammenhängend und unlogisch. Sie wurde und wird oft von Kriegsgefangenen verwendet, um unerlaubterweise Mitteilungen an der Zensur vorbei aus dem Lager zu schmuggeln. Sie lässt sich ohne irgendwelche aufwändige Einrichtungen oder Hilfsmittel realisieren.



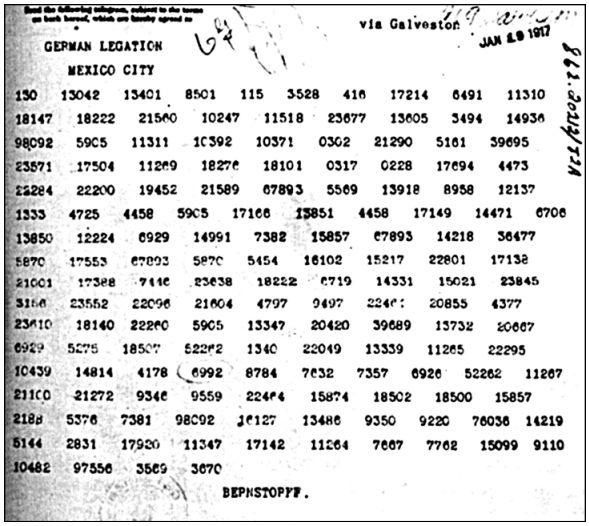
11 Linguistische Steganografie. Die Anfangsbuchstaben des Textes (ohne Anrede und Unterschrift) ergeben den geheimen Text, er lautet hier: "Eglisau Bahnhof". [AUT]

Codierung

Im Ersten Weltkrieg wurde die Methode des Codierens noch oft eingesetzt. In einem Codebuch sind häufig gebrauchte Sätze, Satzteile, Wörter, Silben, einzelne Buchstaben, Ziffern oder andere Zeichen in geeigneter Reihenfolge aufgeführt, entweder alphabetisch oder nach Sachgebiet geordnet. Hinter jedem Begriff steht eine zwei- bis vierstellige Nummer. Beim Codieren wird der Klartext mit Hilfe des Codebuches in eine Folge von Nummern umgesetzt. Der Empfänger besitzt eine Liste, die nach Nummern geordnet ist. Mit dieser stellt er den ursprünglichen Klartext wieder her. Ein Telefonbuch kann als Codebuch angesehen werden, es setzt Namen und Adressen in Nummern um. Auch das Gegenstück existiert, ein Verzeichnis, nach Telefonnummern geordnet, dahinter der zugehörende Name mit Adresse. Einen individuellen

Schlüssel kennt man beim Codieren nicht. Identische Meldungen werden in identische Nummernfolgen des Geheimtextes umgesetzt. Das Fehlen eines indiviuellen Schlüssels ist grundsätzlich eine Schwäche eines jeden Codier- und Chiffrierverfahrens. Man kann diesen Mangel dadurch etwas abschwächen, dass man oft verwendeten Begriffen verschiedene Nummern zuordnet. Der Chiffreur muss dann zufällig zwischen den Möglichkeiten abwechseln. Aus Erfahrungen weiss man, dass er das in der Hitze des Gefechts oft nicht tut.

Beim Codieren wird auf eine buchstabengetreue Übermittlung kein besonderer Wert gelegt. Wichtig ist vielmehr, dass der Sinn der Meldung nicht verloren geht. Den Begriff "Codieren" sollte man vorsichtig anwenden. Oft sagt man Codieren und meint Chiffrieren. In der Informatik hat der Begriff "Code" noch eine andere Bedeutung: Man verwendet ihn für spezielle Datenformate, wie z.B. Binärcode, Dezimalcode, ASCII-Code, Fernschreiber-Code, Morsecode usw. Entsprechend versteht man dann unter Codieren eine Umwandlung von einem Datenformat in ein anderes.



12 Ein codiertes Telegramm. Die Codenummern haben eine variable Länge von drei bis fünf Stellen. [12]

Transposition

Bei der Transpositions-Methode werden die Buchstaben des Klartextes nach einem geheimen Schema in ihrer Position umgestellt, transponiert. Ein Beispiel soll zeigen, wie das einfach gemacht werden kann: In eine Tabelle mit z. B. 6 Zeilen und 6 Spalten wird der Klartext fortlaufend zeilenweise eingefüllt, Wortzwischenräume müssen weggelassen werden, siehe Abb. 13. Der Geheimtext wird erhalten, indem man die Tabelle spaltenweise ausliesst und Fünfergruppen bildet. Zum Dechiffrieren wird sinngemäss umgekehrt vorgegangen: Spaltenweise den Geheimtext eintragen, zeilenweise den Klartext auslesen. Ist der Klartext länger als 36 (6 x 6) Zeichen, wird das Verfahren mehrmals aufeinander folgend angewandt. Reicht am Schluss der Text nicht aus, um alle Felder zu füllen, wird mit Füllwörtern ergänzt. Man muss zwingend mit sinnvollem Text auffüllen, und nicht stur mit immer dem gleichen Buchstaben!

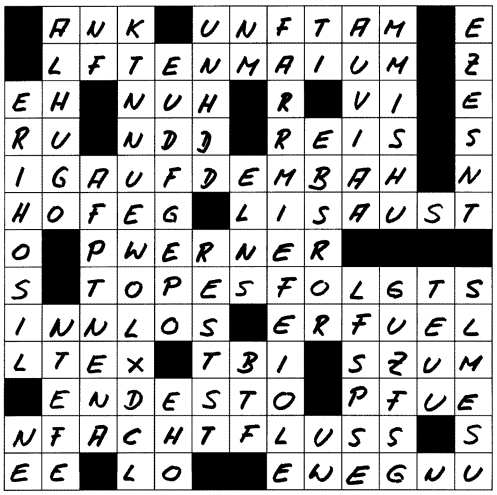
Der Algorithmus lautet hier: zeilenweise einlesen, spaltenweise auslesen. Als individuellen Schlüssel kann man die Anzahl der Zeilen und Spalten absprechen.

Man ahnt es, besonders sicher scheint dieses Verfahren nicht zu sein. Es lässt sich etwas verbessern, indem man auf die Tabelle eine Schablone legt, die ein unregelmässiges Muster von nicht beschreibbaren schwarzen Feldern aufweist. Das Bild erinnert an das Gerüst eines Kreuzworträtsels, siehe Abb. 14. Bei dieser Methode gilt als individueller Schlüssel – neben der Grösse der Tabelle – die Anordnung der schwarzen Felder. Für jedes Telegramm wird eine andere Schablone auf die Tabelle gelegt, so dass jede Meldung individuell chiffriert wird. Die gleiche Schablone kann auf vier verschiedene Arten benutzt werden, indem man sie jeweils um 90° dreht. Selbstverständlich muss man sich mit der Gegenseite absprechen, mit welcher Schablone und in welcher Ausrichtung man arbeiten will. Diese Angaben bilden den individuellen Schlüssel.

Der Algorithmus bei der Transpositionsmethode lautet generell: nach einem vorgegebenen Schema ein- und wieder auslesen. Als individuellen Schlüssel verwendet man verschiedene Tabellenformate und verschiedene Schablonen.

A	N	K	U	N	F
T	A	M	E	L	F
T	E	N	M	A	I
U	M	Z	E	H	N
U	H	R	N	U	L
L	N	E	U	N	A

13 Beispiel einer Transposition mit einer Tabelle 6 x 6. Der Klartext wird "waagrecht" eingetragen, den Geheimtext erhält man durch "senkrechtes" auslesen. Es werden Fünfergruppen gebildet: "ATTUU LNAEM HNKMN ZREUE ... " [AUT]



14 Mit einer Schablone auf der Tabelle wird die Transposition etwas sicherer. Der Geheimtext beginnt mit: ERIHO SILNE ALHUG ONTEF ENFAF ... [AUT]

Man kennt noch viele weitere Variationen bei der Transpositionsmethode. Wortzwischenräume müssen in jedem Fall weggelassen werden. Beim Auslesen würden sie bei der Bildung von Fünfergruppen unweigerlich Probleme verursachen.

Manchmal wird die Transpositionsmethode zweimal hintereinander mit verschieden grossen Schablonen ausgeführt. Das geschieht mit der Absicht, es dem Gegner möglichst schwer zu machen, wenn er den Inhalt der Meldung aufdecken, die Meldung brechen will. Mehr dazu im Abschnitt "Mehrfachverschlüsselung".

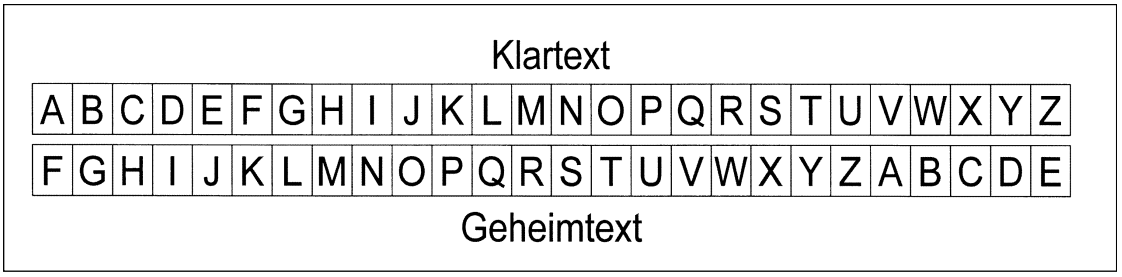
Für uns ist die Transpositionsmethode weiter nicht von Wichtigkeit, sie hat bei den mechanischen Chiffriermaschinen kaum Bedeutung. Der Grund liegt vor allem darin, dass dieses Verfahren ein Speichermedium benötigt, das den eingelesenen Text bis zum Auslesen zwischenspeichert. In unserem Beispiel ist der Speicher lediglich ein Stück Papier, das hier aber seinen Zweck erfüllt. Auf rein mechanischer Basis kann ein Speicher nicht so einfach realisiert werden. Bei modernen Computerverfahren kommt der Transpositionsmethode wieder mehr Bedeutung zu, denn hier lässt sich die Zwischenspeicherung einfach realisieren.

Man spricht bei der Transpositionsmethode auch von einer Blockchiffrierung. Der Klar- und der Geheimtext werden Block für Block verarbeitet.

Substitution

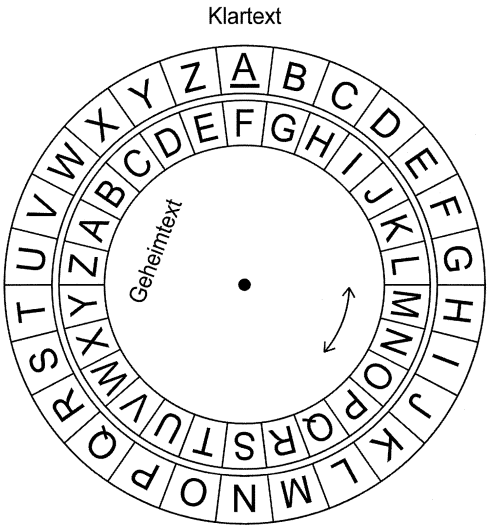
Aus der Geschichtsschreibung weiss man, dass Julius Cäsar ein Chiffrierverfahren einsetzte, das noch heute nach ihm benannt wird. Cäsar ist jedoch nicht der Erfinder dieser Methode; sie war schon vor seiner Zeit bekannt. In Abb. 15 erkennt man, worauf sie beruht. Zwei Alphabete sind übereinander angeordnet, das untere ist um fünf Positionen nach links verschoben. Die Verschlüsselung geht so vor sich, dass man den Klartext Buchstabe für Buchstabe in der oberen Zeile einstellt oder markiert und darunter die zugehörenden Geheimtextbuchstaben abliest. Dieses Verfahren funktioniert auch dann, wenn die Wortzwischenräume als solche beibehalten werden. Aus Sicher-heitsgründen lässt man sie aber meist weg. Die Buchstaben des Klartextes werden hier durch andere ersetzt, substitu-iert, daher die Bezeichnung "Substitutionsmethode". Es gibt 26 Möglichkeiten, die Buchstaben in der unteren Reihe geordnet einzutragen, aber nur deren 25 sind sinn-voll, die 26. bewirkt nichts. Das Schema nach Abb. 15 kann jederzeit und ohne weitere Anweisungen erstellt werden. Es lässt sich auch kreisförmig anordnen, siehe Abb. 16, so entsteht die "Chiffrierscheibe". Man muss lediglich wissen, um wie viele Positionen die beiden Rei-hen gegeneinander

15 Zwei geordnete, gegeneinander verschobene Alphabete, sie sind die Grundlage der Substitutionsmethode nach Cäsar. [AUT]



verschoben sind. Diese Zahl (oder der Buchstabe) bildet den individuellen Schlüssel.

Die Zahl der verschiedenen Anordnungen auf dem inneren Kreis erhöht sich enorm, wenn die Buchstaben nicht geordnet, sondern in beliebiger Reihenfolge eingetragen werden. Es gibt 26! (26 Fakultät) Möglichkeiten, Permutationen, das zu tun. Das entspricht einer Anzahl von etwa 4×10^{26}. Eine dieser Permutationen, willkürlich ausgewählt, zeigt Abb. 17, ebenfalls in der Form einer Chiffrierscheibe dargestellt. Das Vorgehen beim Chiffrieren ist immer noch gleich wie bei einem "Cäsar". Die Zahl der individuellen Schlüssel ist aber ins Unvorstellbare gestiegen. Der Schlüssel ist jetzt nicht mehr eine einfache Zahl, sondern die Reihenfolge von 26 Buchstaben. Da man sich diese nicht so ohne weiteres auswendig merken kann, entwickelte man Verfahren, um aus einem Schlüsselwort eine zufällig wirkende Anordnung der 26 Buchstaben zu erzeugen. Eines dieser Verfahren wollen wir uns an einem Beispiel kurz ansehen.



16 Die Tabelle nach Abb. 15 ist hier kreisförmig auf einer Scheibe dargestellt. Der innere Ring lässt sich drehen, so dass sich alle 26 Schlüssel einstellen lassen. Hier ist der Schlüssel 'F' oder 5 eingestellt. [AUT]

Zufallsverteilung erzeugen

Wir gehen von einem individuellen Schlüsselwort aus, es sollte nicht zu kurz sein, je länger, desto besser. Es darf auch aus einem ganzen Satz bestehen und Buchstaben dürfen mehrfach vorkommen. In unserem Beispiel verwenden wir den Begriff: ***Zar und Zimmermann***. Diesen schreiben wir in Grossbuchstaben auf, wobei wir mehrfach vorkommende Buchstaben nur bei ihrem ersten Auftreten notieren, sonst überspringen wir sie. Nur die 26 Buchstaben des Alphabets werden beachtet, alle übrigen Zeichen lassen wir weg. Unsere Reihe beginnt demnach mit:

Anschliessend tragen wir die übrig gebliebenen Buchstaben des Alphabets in geordneter Folge hinter dem bereits Niedergeschriebenen ein, wobei wir beim letzten eingetragenen Buchstaben (in unserem Beispiel bei 'E') die Reihe alphabetisch aufsteigend weiterführen. Ist man am Ende des Alphabets angelangt, folgen die noch übriggebliebenen Buchstaben ('B' und 'C'), wieder in alphabetischer Folge. Die komplette Reihe lautet:

Dechiffrieren

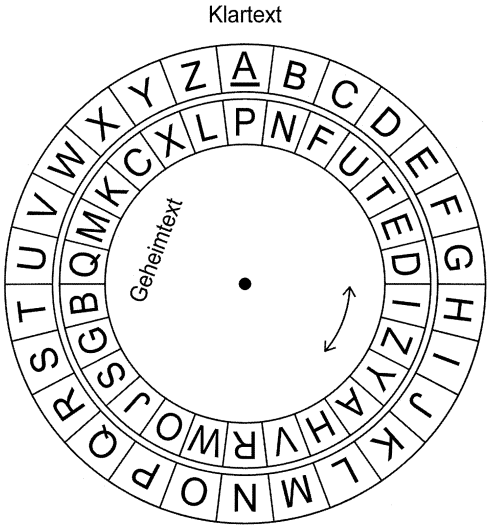
Zum Dechiffrieren wird der Geheimtext auf der unteren Reihe (Abb. 15) oder auf dem inneren Ring (Abb. 16 und 17) markiert, den zugehörenden Klartextbuchstaben liest man auf der oberen Reihe, resp. auf dem äusseren Ring ab. Es leuchtet sofort ein, dass das Dechiffrieren mit der Scheibe nach Abb. 16 wesentlich schneller geht als bei

```
Z A R U N D I M E . . . . . .
```

jener nach Abb. 17, wo die hilfreiche und gewohnte Ordnung des Alphabets fehlt. Auch wenn uns das klassische Verfahren nach Cäsar nicht so sicher vorkommen mag wie die "allgemeine Substitution" nach Abb. 17, so ist es dafür in der Anwendung einfacher. Zum Dechiffrieren einer "allgemeinen Substitution" könnte man eine Scheibe herstellen, bei der die innere Reihenfolge alphabetisch geordnet ist, dafür würde dann die Folge auf dem äusseren Ring chaotisch erscheinen.

Alle Chiffrierverfahren, die mit immer der gleichen Um-

```
Z A R U N D I M E F G H J K L O P Q S T V W X Y B C
```



17 Die Substitutionsscheibe mit ungeordnetem Alphabet im inneren Kreis. [AUT]



18 Leon Battista Alberti, 1404 in Venedig geboren. Er soll die Chiffrierscheibe erfunden haben. [16]

setztabelle arbeiten, haben die Eigenschaft, dass gleiche Buchstaben des Klartextes im Geheimtext wohl andere, aber ebenfalls gleiche Buchstaben erzeugen. Bei der Tabelle nach Abb. 15 wird aus einem 'E' immer ein 'J', aus dem 'N' immer ein 'S' usw. Man bezeichnet dieses Verfahren deshalb als monoalphabetisch, einalphabetisch, nur mit einem Alphabet arbeitend.

Für die Substitutionsmethode kennt man auch den Ausdruck "Stromchiffrierung". Man will damit ausdrücken, dass der Text Buchstabe um Buchstabe in einem stetig fliessenden Strom verarbeitet wird.

Monoalphabetisch reichte aus

Die monoalphabetische Substitution war über lange Zeit im Einsatz, mindestens seit dem Anfang unserer Zeitrechnung bis ins 16. Jahrhundert. Man ahnte oder wusste zwar schon lange, dass diese Chiffriermethode unsicher war und mit geringem Aufwand gebrochen werden konnte. Es wurde deshalb versucht, mit verschiedenen Komplikationen allfällige Code-Brecher zu verwirren. So wurde der Klartext z. B. in eine Folge von Phantasiezeichen umgesetzt. Viel hat das natürlich nicht gebracht, das Verfahren war und blieb trotzdem eine monoalphabetische Substitution.

Bei der Beurteilung der eher bescheidenen Sicherheit, die man durch eine monoalphabetische Substitution erhält, muss man berücksichtigen, dass die Verhältnisse damals anders waren als heute. Funk, Telefon, Telex gab es nicht, auch kaum einen öffentlichen Postdienst. Vieles wurde mit eigenen Boten transportiert. Die Mehrheit dieser Boten dürfte des Lesens nicht mächtig gewesen sein. Mit Geschriebenem konnten sie nicht viel anfangen, bestenfalls konnten sie es abzeichnen.

Das Chiffrieren hatte zu jener Zeit wohl eher die Aufgabe des Verschleierns. Man wollte verhindern, dass ein Text sofort, innerhalb eines Augenblicks, gelesen und verstanden werden konnte. Ernsthafte Angriffe auf einen Geheimtext waren wohl kaum an der Tagesordnung. Im Gegensatz zu heute war es schwierig, an den Geheimtext heran zu kommen. Denn wenn überhaupt, wurde er von zuverlässigen Boten befördert.

Kryptanalyse 1

Die Kryptanalyse ist das Vorhaben, eine chiffrierte Meldung ohne Kenntnis des Schlüssels lesbar zu machen.

Cäsar brechen

Eine Verschlüsselung nach Cäsar lässt sich brechen, indem man im ungünstigsten Fall die 25 verschiedenen Umsetztabellen durchprobiert. Natürlich dechiffriert man jeweils nicht den ganzen Geheimtext, nach einigen Buchstaben merkt man bald, ob sinnvoller Text erscheint oder nicht. Wenn dann noch die Wortabstände erhalten sind, liest ein geübtes Auge eine "Cäsar-Verschlüsselung" wie Klartext. Bei einer allgemeinen monoalphabetischen Verschlüsselung ist das nicht mehr so einfach, aber auch hier sind dem Kryptanalysten die Wortabstände eine wertvolle Hilfe. Darum galt in der professionellen Kryptographie:

> Wortzwischenräume lässt man beim Chiffrieren generell weg.

Die Statistik deckt auf

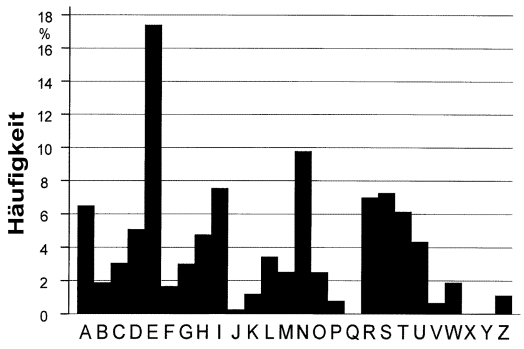
Irgendwann um 1500 kam jemand auf die Idee, geschriebene Sprache auf die Häufigkeit der vorkommenden Buchstaben zu untersuchen. Vielleicht geschah dies im Zusammenhang mit dem Buchdruck. Der Drucker wollte wissen, wie viele der einzelnen Lettern er braucht, um eine Seite Standardtext zu setzen.

Man stellte Erstaunliches fest: Für jede Sprache ist die statistische Häufigkeit der vorkommenden Buchstaben ziemlich konstant. Zwischen den verschiedenen Sprachen bestehen dagegen markante Unterschiede, siehe Abb. 19. Für die deutsche Sprache zeigt die Abb. 20 die Verteilung als Balkengrafik. Besonders auffallend ist die E-Spitze, die gut 17 % erreicht. Am zweithäufigsten kommt der Buchstabe 'N' vor. In den Händen des Kryptanalysten ist dieses Wissen ein sehr starkes Werkzeug. Wird ihm ein Geheimtext zum Brechen vorgelegt, stellt er zuerst die Buchstabenhäufigkeit fest. Mit dieser zeichnet er eine Grafik gemäss dem Muster in Abb. 20. Es ist eine minimale Menge Text erforderlich, um eine einigermassen zuverlässige Aussage machen zu können. Je mehr Text vorliegt, um so aussagekräftiger ist die Analyse. Es ist auch wichtig, zu wissen, in welcher Sprache der Klartext abgefasst wurde, da die typische Verteilung sprachabhängig ist.

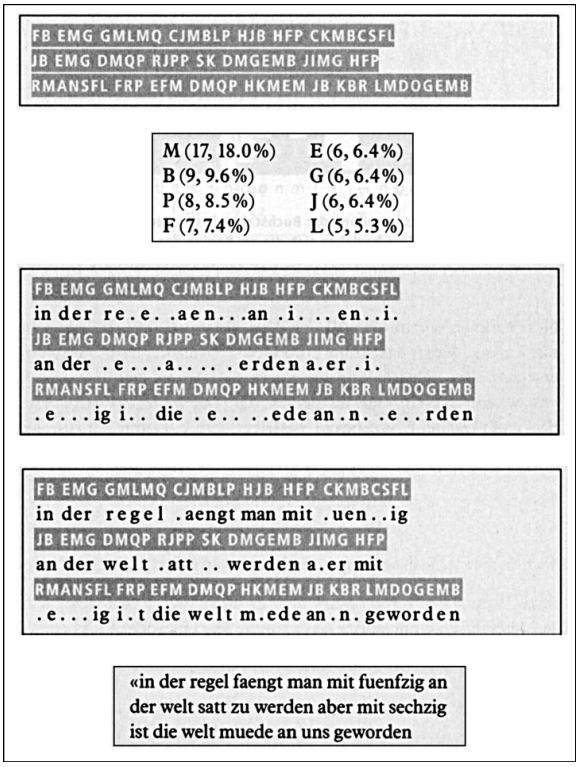
Bei der Analyse einer "Cäsar-Verschlüsselung" wird man eine Grafik nach der Normalverteilung gemäss Abb. 20 erhalten, nur dass alles um einen bestimmten Betrag verschoben ist. Aus dem Betrag der Verschiebung lässt sich die Verschlüsselungstabelle sofort rekonstruieren und damit ist der Geheimtext gebrochen. Bei einer allgemeinen monoalphabetischen Substitution ist es nicht mehr so einfach. Die E-Spitze wird man noch relativ schnell finden. Damit sind immerhin schon 17 % des Textes bekannt! Ab jetzt muss man systematisch probieren. Eine zusätzliche Hilfe ist das Wissen um die Häufigkeit der Bigramme, der Kombination von zwei Buchstaben. 'ER' und 'EN' kommen besonders häufig vor, 'EA' dagegen eher seltener. Einem 'C' folgt in der deutschen Sprache fast immer ein 'H', wenn nicht, ist es in der Regel ein 'K'. Von allen Bigrammen und den häufigsten Trigrammen (Folgen von drei Buchstaben) kennt man deren statistische Häufigkeit. Siehe dazu die Tabellen

Zeichen	englisch	deutsch	Zeichen	englisch	deutsch
a	8.04%	6.47%	n	7.09%	9.84%
b	1.54%	1.93%	o	7.60%	2.98%
c	3.06%	2.68%	p	2.00%	0.96%
d	3.99%	4.83%	q	0.11%	0.02%
e	12.51%	17.48%	r	6.12%	7.54%
f	2.30%	1.65%	s	6.54%	6.83%
g	1.96%	3.06%	t	9.25%	6.13%
h	5.49%	4.23%	u	2.71%	4.17%
i	7.26%	7.73%	v	0.99%	0.94%
j	0.16%	0.27%	w	1.92%	1.48%
k	0.67%	1.46%	x	0.19%	0.04%
l	4.14%	3.49%	y	1.73%	0.08%
m	2.53%	2.58%	z	0.09%	1.14%

19 Statistische Buchstabenhäufigkeit bei englisch- und deutschsprachigem Text. [5]



20 Grafische Darstellung der Buchstabenhäufigkeit bei der deutschen Sprache. [AUT]



21 Schrittweises Brechen eines monoalphabetisch chiffrierten Textes. Die beibehaltenen Wortzwischenräume erleichtern die Arbeit wesentlich. [1] [AUT]

22 und 23. Daneben sind noch verschiedene andere, statistisch signifikante Eigenschaften der geschriebenen Sprache bekannt, die dem Kryptanalysten bei seiner Arbeit eine wertvolle Hilfe sind, z. B.:

- Wortlängen
- Häufigkeit der Worte
- Position der Buchstaben innerhalb eines Wortes
- Verteilung der Konsonanten
- Häufigkeit einzelner Wörter
- Buchstabenfolgen (Bi- und Trigramme)

Mit Intuition und Probieren zum Ziel

Da es sich bei der Buchstabenverteilung um eine statistische, also eine "im Durchschnitt zutreffende" Verteilung handelt, ist die Länge des zu untersuchenden Textes für die Zuverlässigkeit entscheidend. Natürlich muss sich der Kryptanalyst mit dem zufrieden geben, was vorliegt. Aber vielleicht sind mehrere Meldungen nach dem gleichen Alphabet verschlüsselt. In diesem Fall kann er für die statistische Auswertung die Texte aller Meldungen zusammenlegen. Die E-Spitze wird man in der Regel schon mit 100 Buchstaben feststellen. Ab etwa 500 Buchstaben wird das 'N' erkennbar. Auch 'A', 'I', 'R', 'S' und 'T' treten hervor, bei diesen fünf wird eine zuverlässige Zuordnung noch kaum möglich sein. Doch auch seltene Buchstaben werden erkennbar durch ihr geringes Vorkommen. Aus der Höhe der E-Spitze kann bei genügend Text auf die Sprache des Klartextes geschlossen werden.

Abb. 21 zeigt als Beispiel, wie eine monoalphabetische Substitution Schritt für Schritt gebrochen wird: Nach einer statistischen Auswertung sind die häufigsten Buchstaben bald bekannt oder sie lassen sich erraten; Bi- und Trigramme helfen weiter. Oft weiss man, wovon der Klartext handelt oder man hat Vermutungen, dann hilft systematisches Probieren weiter, bis der ganze Geheimtext klar vorliegt.

Wurde nach der Transpositionsmethode chiffriert, zeigt die Analyse eine Grafik, die identisch ist mit jener in Abb. 20. Damit weiss der Kryptanalyst, dass eine Transposition vorliegen muss.

Der geübte Fachmann wird auch bei relativ kurzen Texten schnell zum Ziel gelangen. Neben dem mathematischen Wissen und Können ist auch Intuition und Hartnäckigkeit gefragt. Es ist dem Kryptanalysten eine grosse Hilfe, wenn er weiss, aus welchem Umfeld der Geheimtext stammt, dann kann er gezielt nach vermuteten Wörtern suchen. Die Informationen des Nachrichtendienstes können dem Code-Brecher entscheidende Hinweise geben.

Früher war das Brechen eines Geheimtextes das Metier der Sprachwissenschafter, später kamen Mathematiker dazu. Einem erfolgreichen Team gehören heute auch Fachleute an, denen die Materie, um die es sich im Geheimtext handelt, geläufig ist. Sie sind in der Lage, in einem halbwegs entschlüsselten Text typische Fachwörter zu erraten.

Statistiktabellen

	.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
a.	8	31	27	11	64	15	30	20	5	1	7	59	28	102		4		51	53	46	75	2	3		1	2
b.	16	1		1	101		3	1	12		1	9		1	8			9	6	4	14		1		1	1
c.	2			2	1			242	1		14	1			2				1							
d.	54	3	1	13	227	3	4	2	93	1	3	5	4	6	9	3		10	11	6	16	3	4			3
e.	26	45	25	51	23	26	50	57	193	3	19	63	55	400	6	13	1	409	140	55	36	14	23	2	1	11
f.	19	2		9	25	12	3	1	7		1	5	1	2	9	1		18	4	20	24	1	1			1
g.	20	3		12	147	2	3	3	19	1	3	9	3	5	6	1		14	18	18	11	4	3			3
h.	70	4	1	14	102	2	4	3	23	1	3	25	11	19	18	1		37	11	47	11	4	9			3
i.	7	7	76	20	163	5	38	12	1	1	12	25	27	168	20	2		17	79	78	3	5	1			5
j.	9				9										2						5					
k.	26	1		2	26	1	1	1	7		1	10	1	1	24	1		13	5	14	9	1	1			1
l.	45	7	2	14	65	5	6	2	61	1	7	42	3	4	14	2		2	22	27	13	3	2			3
m.	40	6	1	8	50	4	4	3	44	2	3	4	23	3	15	7		2	10	8	14	4	3			2
n.	68	23	5	187	122	19	94	17	65	5	25	10	23	43	18	10		10	74	59	33	18	29			25
o.	3	8	15	7	25	6	5	9	1	1	3	31	17	64	1	6		50	19	9	3	3	7		1	6
p.	16			3	10	6		2	4			4			11	5		23	1	3	4					
q.																					2					
r.	80	25	9	67	112	18	27	19	52	4	23	18	20	31	30	9		15	54	49	48	12	17			14
s.	36	10	89	20	99	7	13	9	65	2	11	9	12	7	28	22		8	76	116	15	9	10		2	7
t.	57	8	1	35	185	5	10	14	59	2	4	11	9	9	15	3		31	50	23	26	8	21		1	26
u.	3	8	16	5	78	27	8	4	2		3	7	21	119		5		33	48	23	1	3	2			1
v.	3				37				9						43											
w.	34				48				36	1				1	17				1		9					
x.									1						1					1						
y.					1							1	1						1							
z.	4	1		1	28		1		11		1	2	1		2				1	7	43	1	9			1

22 Häufigkeit des Vorkommens aller Bigramme in deutsprachigem Text. Zahlen in %% (pro 10'000). [5]

23 Die wichtigsten Trigramme in deutschsprachigem Text, ebenfalls in %%. [5]

ein	122	das	47	erd	33	ese	27	eni	23	ner	20	hei	18
ich	111	hen	47	enu	33	auf	26	ige	23	nds	20	lei	18
nde	89	ind	46	nen	32	ben	26	aen	22	nst	20	nei	18
die	87	enw	45	rau	32	ber	26	era	22	run	20	nau	18
und	87	ens	44	ist	31	eit	26	ern	22	sic	20	sge	18
der	86	ies	44	nic	31	ent	26	rde	22	enn	19	tte	18
che	75	ste	44	sen	31	est	26	ren	22	ins	19	wei	18
end	75	ten	44	ene	30	sei	26	tun	22	mer	19	abe	17
gen	71	ere	43	nda	30	and	25	ing	21	rei	19	chd	17
sch	66	lic	42	ter	30	ess	25	sta	21	eig	18	des	17
cht	61	ach	41	ass	29	ann	24	sie	21	eng	18	nte	17
den	57	ndi	41	ena	29	esi	24	uer	21	erg	18	rge	17
ine	53	sse	39	ver	29	ges	24	ege	20	ert	18	tes	17
nge	52	aus	36	wir	29	nsc	24	eck	20	erz	18	uns	17
nun	48	ers	36	wie	28	nwi	24	eru	20	fra	18	vor	17
ung	48	ebe	35	ede	27	tei	24	mme	20	hre	18	dem	17

Auch bei einem absolut sicheren Chiffrierverfahren sind mehr oder weniger zuverlässige Menschen involviert.

Chiffrierverfahren 2

Homophone Substitution

Die Schwächen der monoalphabetischen Verschlüsselung waren bekannt, man suchte deshalb nach besseren Methoden. Eine Möglichkeit sah man darin, häufig verwendete Buchstaben des Klartextes abwechslungsweise in verschiedene Geheimtextzeichen umzusetzen. Das wechselnde Auswählen der verschiedenen Zeichen erfolgte zufällig. Eine solche Verschlüsselung nennt man homophon. Abb. 24 zeigt eine Tabelle, mit der eine homophone Chiffrierung möglich ist. Sie setzt jeden Buchstaben des Klartextes in eine zweistellige Zahl um. Häufig vorkommende Buchstaben sind mehrfach vorhanden, 'E' etwa 17 mal, das 'N' 10 mal usw. Damit wird erreicht, dass im Geheimtext die zweistelligen Zahlen alle etwa gleich oft vorkommen. Der Chiffreur wählt bei jedem Buchstaben nach einem zufälligen Muster eine der möglichen Substitutionen aus. Ein Nachteil ist der, dass für jeden Buchstaben im Klartext eine zweistellige Zahl erhalten wird; der Geheimtext wird doppelt so lang wie der Klartext. Die zweistelligen Zahlen könnten durch 100 verschiedene Buchstaben, Symbole und Ziffern ersetzt werden, so liesse sich der Umfang des Geheimtextes wieder auf die Länge des Klartextes reduzieren. Beispiele aus dieser Tabelle sind:

e = 02, 05, 09, 10, 15, 23, 27, 31 usw.
a = 22, 30, 79, 88, 94
x = 86
y = 75

Den Kryptanalysten bereitete die homophone Verschlüsselung keine grossen Probleme. Wohl half ihnen die Häufigkeitsanalyse der Zahlen nicht weiter. Sie stützten sich bei ihren Angriffen vor allem auf das Vorkommen der Bi- und Trigramme. Auch wenn häufig vorkommende Zeichen in verschiedene Zahlen oder Symbole umgesetzt werden, sind seltene Buchstaben noch immer monoalphabetisch umgesetzt. Die Struktur der Sprache wird nur oberflächlich und teilweise zerstört; einem Angriff bot die homophone Verschlüsselung kaum Widerstand.

	0	1	2	3	4	5	6	7	8	9
0	n	h	e	d	n	e	r	o	i	e
1	e	m	c	s	o	e	b	s	g	n
2	t	r	a	e	t	h	i	e	s	t
3	a	e	g	d	w	r	n	d	n	v
4	i	u	i	k	e	d	c	z	m	s
5	n	s	d	n	t	l	j	l	q	n
6	r	e	b	p	i	n	o	l	i	u
7	e	g	s	e	h	y	e	f	s	a
8	i	n	f	r	u	r	x	r	a	h
9	t	e	c	m	a	e	e	t	e	i

24 Tabelle zur Durchführung einer homophonen Substitution. [AUT]

Polyalphabetische Substitution

Bis ins 16. Jahrhundert wurde – neben verschiedenen anderen Verfahren – monoalphabetisch substituiert. Wir haben gesehen, dass es Fachleuten, ja selbst einem Laien, kaum Probleme bereitet, diese Geheimtexte zu brechen. Man wusste um die Schwächen und suchte nach Abhilfe. Im Jahre 1586 veröffentlichte der französische Diplomat Blaise de Vigenère eine revolutionäre Erfindung. Er verschlüsselte nicht mehr den ganzen Text nach ein und derselben Tabelle, eben monoalphabetisch, sondern wechselte zwischen verschiedenen Umsetztabellen ab. Mit dieser Idee hatte er die polyalphabetische Substitution erfunden! Dabei wird das typische Muster gemäss Abb. 20 zerstört. Die Analyse, die auf der Häufigkeitsverteilung der Buchstaben im Geheimtext und dem Muster der häufigen Bi- und Trigrammen beruht, läuft unweigerlich ins Leere.

Das Verfahren nach Vigenère

Vigenère brauchte für seine Erfindung ein Schema nach Abb. 26. Dieses kann jederzeit und ohne zusätzliche Angaben oder Vorlagen erstellt werden.

Das Verschlüsselungsverfahren nach Vigenère benötigt ein geheimes, individuelles Schlüsselwort. Es kann beliebig lang sein. Andere Zeichen als die 26 Buchstaben des Alphabets müssen weglassen werden, Buchstaben dürfen mehrfach vorkommen.

Wir wollen an einem Beispiel die Verschlüsselung nach Vigenère kennen lernen. Neben dem Schema nach Abb. 26 brauchen wir eine leere Tabelle gemäss Abb. 27. Sie besteht aus drei Zeilen, beschriftet mit "Klar", "Schlüssel" und "Geheim". Als individuelles Schlüsselwort verwenden wir "D I S T E L F I N K". Zuerst tragen wir unseren Klartext als Bandwurm, also ohne Wortzwischenräume, in der ersten Zeile ein, es dürfen nur die 26 Buchstaben vorkommen. Die Schlüsselzeile füllen wir fortlaufend mit dem Schlüsselwort auf. Zu jedem Buchstaben des Klartextes gehört jetzt ein Buchstabe des Schlüsselwortes. Nach dieser Vorbereitung können wir mit dem Chiffrieren beginnen. Den ersten Buchstaben des Klartextes (A) markieren wir in der Tabelle 26 auf der Klartextzeile. Der zugehörende Schlüsselbuchstabe (D) legt eine der 26 Umsetzzeilen (Schlüssel) fest. In der Geheimtexttabelle finden wird im Schnittpunkt Klartextspalte / Schlüsselzeile den Geheimtextbuchstaben. In unserem Beispiel steht in der Kreuzung der Klartextspalte (A) und Schlüsselwortzeile (D) der Geheimtextbuchstaben D; N und I ergeben V usw. Für das Chiffrieren könnte man auch die Chiffrierscheibe nach Abb. 16 einsetzen, die man für jeden Buchstaben entsprechend neu einstellt.

Beim Entschlüsseln wird sinngemäss umgekehrt vorgegangen. Im dreizeiligen Schema füllen wir den erhaltenen Geheimtext in der unteren Zeile ein, darüber fortlaufend das Schlüsselwort. Beim ersten Buchstaben suchen wir in der Schlüsselzeile 'D' den Geheimtextbuchstaben 'D' und finden am Spaltenkopf den zugehörigen Klartextbuchstaben 'A'. 'I' und 'V' ergeben 'N', genau so wie wir es erwartet haben. Zweifellos ist die polyalphabetische Methode in der Anwendung komplizierter und aufwändiger als ein "Cäsar", dafür erhalten wir eine viel grössere Sicherheit.

Während langer Zeit galt die polyalphabetische Verschlüsselung nach Vigenère als absolut sicher. Man mag sich daran stören, dass die 26 Zeilen im Geheimtextblock des Schemas – gleich wie bei einem "Cäsar" – geordnet aufgeführt sind. Würde etwas Unordnung die Sicherheit nicht noch weiter erhöhen? Nun – man war überzeugt, ein absolut sicheres Verfahren zur Verfügung zu haben, was wollte man da noch verbessern? Man muss auch immer daran denken, dass der Geheimtext wieder von Hand entschlüsselt werden muss! Probieren Sie das einmal aus, wenn die Geheimtextzeilen nicht die gewohnte Ordnung aufweisen. Es ist sehr anstrengend und zeitraubend! Ein Problem wäre in diesem Fall auch das Aufsetzen des Schemas mit den 26 chaotisch wirkenden Schlüsselzeilen. Es müssten 26 verschiedene Schlüsselwörter verwendet werden, die man irgendwo aufschreiben müsste. Genau das will man in Geheimdienstkreisen aber unter allen Umständen vermeiden; das Schema muss sich jederzeit und ohne Hilfsmittel auswendig aufsetzen lassen.



25 Blaise de Vigenère, der Erfinder der polyalphabetischen Substitution. [13]

Klartext

Schlüssel	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	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
I	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
J	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	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Geheimtext

26 Tabelle für die Verschlüsselung nach Vigenère. Man kann sie als Erweiterung der Tabelle nach Abb. 15 sehen; es sind hier alle 26 möglichen "Cäsar-Schlüssel" aufgeführt. [AUT]

Klar:	**A**	**N**	**K**	**U**	**N**	**F**	**T**	**A**	**M**	**E**	**L**	**F**	**T**	**E**	**N**	**M**	**A**	**I**	**U**	**M**	**E**	**L**	**F**	**.**	**.**
Schlüssel:	**D**	**I**	**S**	**T**	**E**	**L**	**F**	**I**	**N**	**K**	**D**	**I**	**S**	**T**	**E**	**L**	**F**	**I**	**N**	**K**	**D**	**I**	**S**	**.**	**.**
Geheim:	**D**	**V**	**C**	**N**	**R**	**Q**	**Y**	**I**	**Z**	**O**	**O**	**N**	**L**	**X**	**R**	**X**	**F**	**Q**	**H**	**W**	**H**	**T**	**X**	**.**	**.**

27 Beispiel einer Vigenère-Verschlüsselung. [AUT]

Kryptanalyse 2

Jeder nicht zufälligen Struktur wohnt eine Gesetzmässigkeit inne, die sich mit mehr oder weniger Aufwand aufdecken lässt.

Vigenère wird gebrochen

Etwa 300 Jahre lang galt das Verfahren nach Vigenère als sicher. Dem Briten Charles Babbage gelang vermutlich 1854 als erstem das Brechen einer Vigenère-Verschlüsselung. Doch seine Entdeckung fand keinerlei Anerkennung – er hatte sie nie veröffentlicht!

1863 stellte der preussische Infanteriemajor Friedrich Wilhelm Kasiski die gleiche Entdeckung erstmals der Öffentlichkeit vor. Er hatte festgestellt, dass in einem Geheimtext nach Vigenère gleiche Buchstabenfolgen in bestimmten Abständen gehäuft auftreten. Immer dann, wenn identische Passagen im Klartext mit dem gleichen Abschnitt der Schlüsselzeile chiffriert werden, ergeben sich identische Abschnitte im Geheimtext, siehe Abb. 30. Das trifft natürlich nicht sehr oft zu, aber je kürzer das Schlüsselwort und je länger der Text ist, um so öfter. Wird die Distanz zwischen identischen Folgen im Geheimtext bestimmt, so stellt man fest, dass sie ausgeprägt häufig ein Vielfaches der Länge des Schlüsselwortes ist. Bei unserem Beispiel haben wir ein Schlüsselwort der Länge 10 verwendet, wir würden demnach identische Geheimtextfragmente finden, die untereinander einen Abstand aufweisen, der 10 Stellen oder ein Vielfaches davon beträgt.

Was bringt das Wissen um die Länge des Schlüsselwortes? Sehr viel! Wenn man weiss, dass das Schlüsselwort die Länge 10 hat, so ist der 1., der 11., der 21. usw. Buchstabe mit der selben Schlüsselzeile chiffriert, also monoalphabetisch, sogar nach "Cäsar". Mit einer genügenden Menge an Geheimtextmaterial lässt sich dann der zugehörige Schlüsselbuchstabe nach den bekannten statistischen Methoden feststellen. Auf die gleiche Weise findet man die weiteren Stellen des Schlüsselwortes, bis man es bestimmen oder erraten kann.

Das tönt alles sehr einfach, aber nach welchen Mustern soll man suchen, und wie soll man vorgehen? Dazu braucht es ein geschultes Auge und eine Beziehung zu Buchstaben und zur Schrift. Abb. 31 zeigt dazu ein Beispiel. Identische Folgen sind unterstrichen. Sie sollten mehr als zwei Buchstaben umfassen, je länger eine Folge ist, um so mehr Gewicht wird man ihr beimessen. In Abb. 32 ist die zugehörende Auswertung aufgezeichnet. Man kann mit Sicherheit davon ausgehen, dass in diesem Fall das Schlüsselwort die Länge fünf hat.

Viel einfacher scheint es zu sein, systematisch alle möglichen Schlüssellängen auszuprobieren. Das wäre natürlich mit sehr viel Arbeit verbunden. Man würde vermutlich mit der Länge vier beginnen. Wenn das verwendete Schlüsselwort auch die Länge vier hat, ist der 1., 5., 9., 13. usw. Buchstabe monoalphabetisch chiffriert. Eine Häufigkeitsanalyse müsste dann die E-Spitze nach Abb. 20 zeigen. Wenn sich kein Erfolg einstellt, probiert man mit der Länge fünf usw., bis die Analyse das erwartete Muster zeigt.

Das hört sich verlockend an, es ist aber mit sehr viel Handarbeit verbunden! Da man vor einer Analyse zwingend die



28 Charles Babbage. Ihm gelang das Brechen eines nach Vigenère chiffrierten Textes. [13]



29 William Friedman entwickelte ein mathematisches Verfahren zum Brechen der polyalphabetischen Verschlüsselung. [UNB]

Länge des Schlüsselwortes kennen muss, führt kein Weg an Kasiskis Methode vorbei, das zeitaufwändige Durchprobieren war damals praktisch nicht machbar.

Eine Entdeckung des 1891 geborenen Colonels William Friedman brachte den Kryptanalysten eine enorme Hilfe. Friedman gilt in Fachkreisen als der grösste Kryptologe aller Zeiten. Er erfand ein Verfahren zur Ermittlung der Schlüsselwort-Länge, das auf rein mathematischer Basis beruht. Wir wollen hier nicht auf die Details eingehen. Nur soviel: Es ist ein statistisches Verfahren, das die Buchstabenhäufigkeit im Geheimtext mit jener im Klartext in Beziehung setzt. In der Literatur [7] findet man eine ausführliche Beschreibung mit einem Beispiel. Das Verfahren nach Friedman liefert direkt die (ungefähre) Länge des Schlüsselwortes. Für aussagekräftige Resultate ist auch hier – wie bei jedem statistischen Verfahren – genügend Geheimtextmaterial erforderlich. Zudem muss man wissen, in welcher Sprache der Klartext vorliegt. Als Resultat kann man einen Wert von z. B. 6,55 erhalten. In diesem Fall wird man zuerst mit der Länge 7 probieren, und wenn das zu keinem Ergebnis führt, mit der Länge 6. Vielleicht liegt auch der Kasiski-Test vor, der die Längen 6, 9 oder 12 nahe legt. Dann ist es offensichtlich, dass die Länge des Schlüsselwortes 6 sein muss. Je mehr Geheimtext man vorliegen hat, um so zuverlässiger wird eine Aussage zur Länge des Schlüsselwortes ausfallen.

Man muss sich bewusst sein, dass die Verfahren nach Kasiski und Friedman zu einer Zeit entwickelt und angewandt wurden, als man noch keine Rechenmaschinen und Computer kannte. Man arbeitete nur mit Papier und Bleistift! Und trotzdem: Die Vigenère-Verschlüsselung wurde systematisch gebrochen. Wir verstehen jetzt auch die Gründe dafür: Ein relativ kurzer Schlüssel hinterlässt im Geheimtext ein periodisches Muster, das die Länge des Schlüsselwortes verrät. Eigentlich braucht der Kryptanalyst das Schlüsselwort gar nicht zu kennen, er benötigt nur dessen Länge. Im Grunde genommen ist die Sicherheit nicht besser als bei einem "Cäsar", nur ist das Brechen eines "Vigenère" viel arbeitsintensiver. Zudem muss ziemlich viel Geheimtext vorliegen. Wenn wir bei einer monoalphabetischen Substitution mit einigen hundert Zeichen schon gut dran sind, benötigen wir für eine polyalphabetische Substitution mit einem zehnstelligen Schlüsselwort etwa zehn mal mehr Text, also einige tausend Zeichen. Je länger bei einem "Vigenère" das Schlüsselwort ist, um so schwerer haben es die gegnerischen Kryptanalysten.

Klartext:	A	U	S	K	L	A	R	T	E	X	T	W	I	R	D	G	E	H	E	I	M	T	E	X	T	.	.
Schlüssel:	D	R	O	S	S	E	L	D	R	O	S	S	E	L	D	R	O	S	S	E	L	D	R	O	S	.	.
Geheimtext:	D	L	G	C	D	E	C	W	V	L	L	O	M	C	G	X	S	Z	W	M	X	W	V	L	L	.	.

30 Hier erkennt man, wie in speziellen Situationen gleiche Klartextpassagen identische Geheimtextmuster geben. [AUT].

Absolute Sicherheit

Wir haben erkannt, dass bei der polyalphabetischen Substitution die Sicherheit mit zunehmender Länge des Schlüsselwortes grösser wird. Der Grund liegt darin, dass die Anzahl der Schlüsselperioden abnimmt, damit wird die Basis für eine statistische Auswertung immer dürftiger. Im Extremfall ist das Schlüsselwort ein Schlüsselwurm, der so lange ist wie der Klartext selbst und dann ist eine statistische Auswertung nicht mehr möglich.

Wie kommt man zu einem solchen Wurm? Da sind verschiedene Möglichkeiten denkbar, etwa die Verwendung des Textes aus einem zuvor abgesprochenen Buch. Als Schlüsselangabe würde man Seite und Zeile angeben und schon hätte man den Anfang des Wurms. Leider führt diese Idee nicht zum gewünschten Ziel. Der Schlüssel ist wohl nicht mehr periodisch, dafür haften ihm die statistischen Eigenheiten der Sprache an. Sie enthält ein schwer ausrottbares inneres Gerüst an Gesetzmässigkeiten. Denken wir nur an die Buchstabenverteilung und die typischen Bi- und Trigramme. So käme der Buchstabe 'E' und das Bigramm 'EN' im Klartext sowie im Schlüsselwurm besonders häufig vor. Wenn im Klartext und im Schlüssel solche Sequenzen übereinander zu liegen kommen, schlägt sich das im Geheimtext nieder. Dieser wird ebenfalls ein charakteristisches Muster zeigen. Und genau hier setzen die Kryptanalysten erfolgreich ihre mathematischen Werkzeuge ein.

Unter den folgenden Bedingungen ist eine Verschlüsselung nach der polyalphabetischen Substitution absolut sicher, das

U E Q P F V C K Λ H V N R Z U R N L Λ O K I R V G
J T D V R V R I C V I D L M Y I Y S B C C O J Q S
Z N Y M B V D L O K F S L M W E F R Z Λ V I Q M F
J T D I H C I F P S E B X M F F T D M H Z G N M W
K Λ X Λ U V U H J H N U U L S V S J I P J C K T I
V S V M Z J E N Z S K Λ H Z S U I H Q V I B X M F
F I P L C X E Q X O C Λ V B V R T W M B L N G N I
V R L P F V T D M H Z G N M W K R X V R Q E K V R
L K D B S E I P U C E Λ W J S B Λ P M B V S Z C F
U E G I T L E U O S J O U O H U Λ V Λ G Z E Z I S
Y R H V R Z H U M F R R E M W K U L K V K G H Λ H
F E U B K L R G M B J I H L I I F W M B Z H U M P
L E U W G R B H Z O L C K C W T H W D S I L D Λ G
V N E M J F R V Q S V I Q M U V S W M Z C T H I I
W G D J S X E O W S J T K I H K E Q

31 Dieser Geheimtext entstand durch eine polyalphabetische Substitution. Für die Kryptanalyse werden identische Folgen gesucht, die eine minimale Länge aufweisen sollten. [7]

Folge	Abstand	Primfaktorzerlegung des Abstands
JTD	50	2·5·5
VIQM	265	5·53
TDMHZGNMWK	90	2·3·3·5
MWK	75	3·5·5

32 Die Analyse des obigen Beispiels. Die Länge des Schlüsselwortes wird mit grosser Wahrscheinlichkeit den Wert 5 haben. [7]

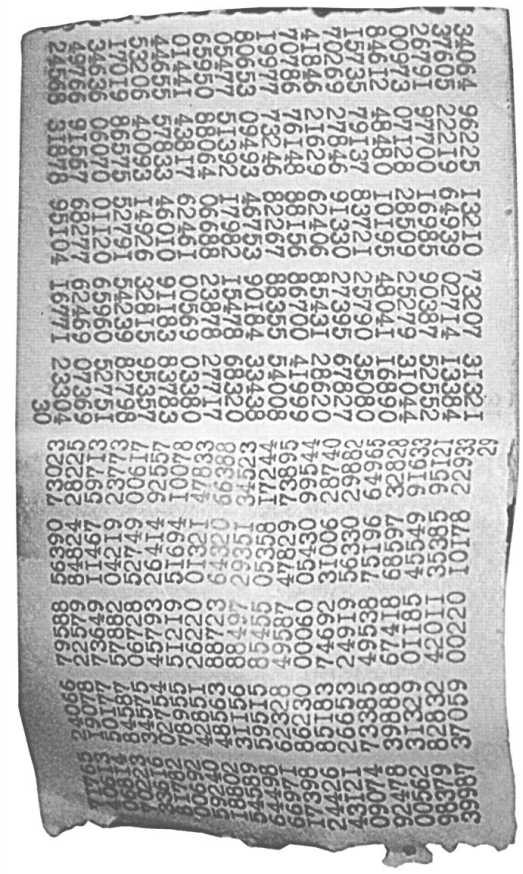
können die Mathematiker sogar beweisen:
Die Befolgung dieser kryptologischen Forderungen führt zu einem polyalphabetischen Substitutionsverfahren, das als "Vernam-Chiffrierung" bekannt ist.

- Der Schlüssel ist so lang wie das Telegramm
- Er weist eine echte Zufallsverteilung auf
- Der Schlüssel wird nur einmal verwendet

Erzeugen von echtem Zufall

Wie wird ein zufälliger Schlüsselwurm erzeugt und wie kommt er auf sicherem Weg zum Empfänger? Dazu als Gedankenanregung kurz folgendes: Zufallsreihen können nicht mit einem Computer erzeugt werden. Dieser kann wohl Zahlen- oder Buchstabenreihen erzeugen, die Eigenschaften aufweisen, wie sie für eine Zufallsverteilung charakteristisch sind. Aber diese Reihen sind vom Computer reproduzierbar, echter Zufall ist nicht reproduzierbar! Zur Erzeugung von echtem Zufall werden Vorgänge herangezogen, die nicht wiederholbar sind und als chaotisch gelten. Beispiele solcher Vorgänge sind: Natürliches oder elektronisch erzeugtes Rauschen. Die Zeit, die zwischen Atomteilungen in einer radioaktiven Substanz verstreicht, ist nicht voraussehbar und deshalb zufällig. Die Zeitspanne, die beim Arbeiten an einer Tastatur zwischen den einzelnen Anschlägen gemessen wird, ist ebenfalls zur Erzeugung von echtem Zufall verwendbar.

Die gemessenen Zufallszeiten setzt man in die erforderlichen Buchstaben oder Zahlen um. Das Ergebnis kann direkt auf ein vorbereitetes Chiffrierformular gedruckt und der Gegenstation per Kurier zugestellt werden. Ein solches Formular sieht ähnlich aus wie jenes nach Abb. 27, ist aber wesentlich länger. Die obere Zeile für den Klartext und die untere für den Geheimtext sind anfänglich unbeschrieben. Der Anwender trägt oben den Klartext ein und ermittelt mit der Vigenère-Tabelle nach Abb. 26, oder der Scheibe nach Abb. 16, den Geheimtext. Nur der Geheimtext wird übermittelt oder verschickt, nicht das ganze Formular! Die Gegenstation muss eine Kopie des Zufallswurms besitzen, damit sie das Telegramm entschlüsseln kann.



33 Zufallszahlen für eine Vernam-Verschlüsselung. Zwei Seiten mit den Schlüsseln 29 und 30 zu je 100 Fünfergruppen wurden gedruckt. [5]

Die Sicherheit muss umfassend sein

Wenn man von absoluter Sicherheit spricht, meint man die theoretische Sicherheit der verwendeten Methode. Den Kryptologen kümmert es nicht, was vor dem Chiffrieren und nach dem Dechiffrieren passiert. Wenn dort Verrat stattfindet, kann man das nicht seinem Chiffrierverfahren anlasteten. Gerade beim eben genannten Vernam-Verfahren mit echten Zufallswürmern nützt es nichts, eine absolut sichere Methode zu haben, wenn jemand den Klartext dem Gegner zusteckt. Aus diesem Grunde sollte man die Sicherheit eines Chiffrierverfahrens nie isoliert betrachten; man muss immer auch berücksichtigen, wie in der Praxis damit umgegangen wird.

Die Rotormaschine

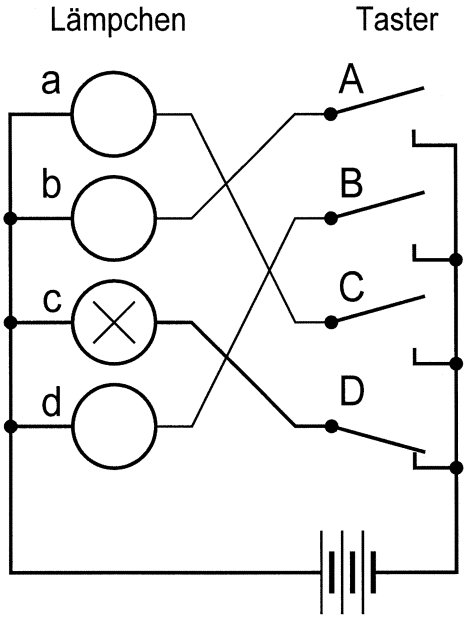
Nichts kann auf die Dauer geheim gehalten werden, es ist eine Frage der Zeit bis ein Verrat erfolgt.

Es ist unser Ziel, eine mechanische Maschine zu bauen, mit der wir chiffrieren und dechiffrieren können. Was wir bis jetzt kennen gelernt haben, sind theoretische Modelle, realisiert mit Papier und Bleistift. In der Praxis lassen sie sich jedoch nur schwer einsetzen.

Taster und Lämpchen

Abb. 34 zeigt eine vereinfachte Anordnung für eine Verschlüsselung nach der Substitutionsmethode. Wir sehen vier Taster, vier Lämpchen und eine Spannungsquelle. In der Realität benötigen wir jedoch je 26 Taster und 26 Lämpchen, das Prinzip erkennen wir aber auch in dieser vereinfachten Darstellung. Wird ein Taster betätigt, leuchtet ein Lämpchen und ein aufgemalter Buchstabe wird sichtbar. Wie aus der Theorie bereits bekannt ist, gibt man den Klartext Buchstabe für Buchstabe an den Tastern ein und liest den Geheimtext an den aufleuchtenden Lämpchen ab. Bei dieser Anordnung erhalten wir eine monoalphabetische Substitution. Einen individuellen Schlüssel kann man nicht einstellen. Die Taster werden über ein Hebelgestänge von einer Tastatur betätigt.

Den gleichen Effekt könnten wir mit einer umgebauten Schreibmaschine erreichen, bei der die Typen vertauscht sind. So müssten wir in diesem Beispiel auf dem Typenhebel 'D' den Buchstaben 'c' montieren usw.



34 Eine monoalphabetische Verschlüsselung, realisiert mit Tastern und Lämpchen. Es sind nur 4 Einheiten gezeichnet, tatsächlich sind es deren 26. [AUT]

Der Rotor

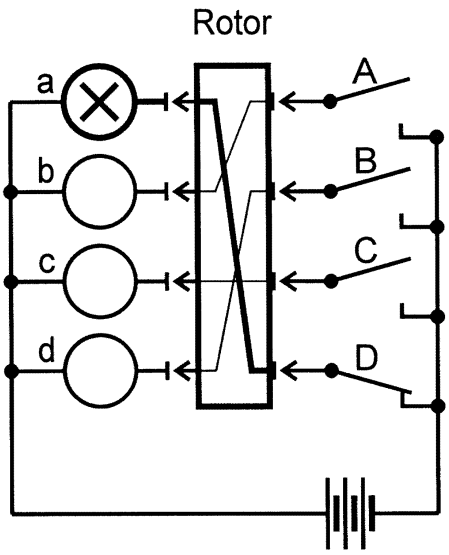
Der Rotor ist ein zentrales Bauteil, dem wir noch oft begegnen werden. Abb. 35 zeigt zwei reale Rotoren aus einer Chiffriermaschine, ihr Durchmesser beträgt ca. 7 cm. Im Prinzip besteht dieses Bauteil aus einer Kunststoffscheibe, die auf beiden Stirnseiten je 26 Kontakte trägt. Im Innern der Scheibe ist je ein Kontakt der einen Seite mit einem auf der Gegenseite verbunden. Diese Verbindungen sind nach einem zufälligen und geheim gehaltenen Schema ausgeführt. Der Rotor ist mit einer zentralen Bohrung versehen, er lässt sich auf eine Achse stecken und kann darauf gedreht werden. Am Umfang ist er mit einer 26er-Rasterung versehen und mit den 26 Buchstaben des Alphabets beschriftet. Abb. 36 zeigt, wie der Rotor an Stelle der festen Verdrahtung zwischen Tastern und Lämpchen eingesetzt wird, auch hier ist natürlich alles 26fach vorhanden. Die Kontakte, die mit den Tastern und den Lämpchen in Verbindung stehen, sind ebenfalls kreisförmig angeordnet, so dass sie mit denen des Rotors übereinstimmen. Der Rotor lässt sich in jede der 26 möglichen Stellungen drehen, so dass jedes Mal eine neue Zuordnung zwischen Tastern und Lämpchen entsteht. Wir haben eine "Maschine" vor uns, mit der wir monoalphabetisch substituieren können. Mit dem Drehen des Rotors lassen sich 26 unterschiedliche Schlüssel einstellen, die wir mit den Buchstaben A ... Z bezeichnen. Durch Auswechseln des Rotors gegen einen andern mit einer anderen Verdrahtung, kann man die Zahl der Schlüssel beliebig erweitern.



35 Zwei reale Rotoren aus der Chiffriermaschine Nema. [AUT]

Automatischer Vorschub

Jetzt versehen wir unsere Einrichtung nach Abb. 36 mit einer Vorschubmechanik. Bei jeder Tasterbetätigung soll der Rotor mit einer Antriebsklinke um eine Position weiter



36 Der Rotor wird eingesetzt. [AUT]

37 Die Anordnung mit drei Rotoren. [AUT]

gedreht werden. Es ist nicht wichtig, welcher Taster betätigt wird, der Rotor wird in jedem Fall um eine Position weiter gedreht. Eine vergleichbare Mechanik kennt man bei der Schreibmaschine; dort wird der Wagen mit dem eingespannten Papier nach jedem Anschlag um eine Position nach links transportiert.

In jeder Position des Rotors entsteht eine andere Zuordnung Taster – Lämpchen. Es darf nicht verschwiegen werden, dass die 26 möglichen Zuordnungstabellen nicht von einander unabhängig sind, denn die innere Verdrahtung des Rotors bleibt natürlich immer dieselbe, eine bestimmte Systematik zwischen den einzelnen Tabellen kann nachgewiesen werden.

Mit diesem Vorschubsystem erhalten wir eine Chiffrierung nach dem Prinzip der polyalphabetischen Substitution. Jeder Buchstabe den wir eingeben wird nach einer anderen Zuordnungstabelle umgesetzt. Nach jeweils 26 Schritten hat der Rotor eine volle Umdrehung ausgeführt und die Umsetzung vollzieht sich wieder nach der ersten Tabelle. Die Periodenlänge, oder die Länge des Schlüsselwortes, ist demnach 26. Die Startposition des Rotors, mit welcher wir beim Chiffrieren beginnen, kann beliebig gewählt werden. Sie stellt einen von 26 individuellen Schlüsseln dar. Wenn mehrere verschiedene Rotoren vorrätig sind, lässt sich die Zahl der Schlüssel beliebig erweitern.

Weiterentwicklung

Der Deutsche Arthur Scherbius erkannte, dass sich das vorgestellte Prinzip weiter entwickeln liess. Im Jahr 1918 meldete er seine Erfindung beim deutschen Patentamt an; er hatte folgende Idee:

Er führte zwei weitere Rotoren ein, jeder mit einer anderen Verdrahtung versehen, siehe Abb. 37. Total stehen drei Rotoren nebeneinander, für den elektrischen Strom sind sie in Serie geschaltet. Der Rotor 1 wird, wie wir das schon aus der Abb. 36 kennen, bei jeder Tasterbetätigung um eine Position weitergedreht. Der Rotor 2 wird vom Rotor 1 um eine Position weiterbewegt, wenn dieser eine volle Umdrehung ausgeführt hat. Der Rotor 3 seinerseits bewegt sich um eine Position weiter, wenn der Rotor 2 eine volle Umdrehung gemacht hat. Die Anordnung funktioniert gleich wie sie uns vom mechanischen Kilometerzähler bestens vertraut ist. Die drei Walzen lassen sich auf $26^3 = 17'576$ verschiedene Positionen einstellen, also erhalten wir 17'576 verschiedene Schlüssel und ebenso viele unterschiedliche Umsetztabellen.

Die "Maschine" nach Abb. 37 bewirkt eine polyalphabetische Substitution mit einer Periodenlänge von 17'576. Das ist lange genug, um auch bei sehr langen Telegrammen keine Wiederholung des Schlüssels zu erhalten. Mit dieser Anordnung haben wir eine der wichtigsten Forderungen erfüllt, die von den Kryptologen an einen sicheren Chiffrieralgorithmus gestellt wird, nämlich die, dass der Schlüssel bei der polyalphabetischen Substitution keine Periode aufweisen darf.

Wie dechiffrieren?

Wir können mit der Maschine nach Abb. 37 sehr einfach chiffrieren, aber wie wird dechiffriert? Im gezeichneten Beispiel ist der Taster 'D' gedrückt und das Lämpchen 'a' leuchtet. Zum Dechiffrieren würden wir den Taster 'A' betätigen, dann sollte 'd' leuchten. Das trifft leider nicht zu, es würde 'c' aufleuchten, es erfolgte keine Dechiffrierung! Wir kennen diese Eigenheit bereits von der Chiffrier-

scheibe nach Abb. 16. Dort mussten wir zum Chiffrieren den Klartext auf dem äusseren Ring eingeben und den Geheimtext innen ablesen. Zum Dechiffrieren gingen wir umgekehrt vor: Innen den Geheimtext eingeben und aussen den Klartext ablesen. Das Dechiffrieren wurde als Chiffrieren in umgekehrter Richtung ausgeführt.

Um das Problem bei der realen Maschine zu lösen, müssten wir zum Dechiffrieren die 26 Anschlüsse der Tastatur und des Lampenfeldes mit einem Umschalter oder Stecker miteinander vertauschen. Die Taster wären dann auf der linken Seite angeschlossen und die Lämpchen auf der rechten, siehe Abb. 39. Dann würde der Strom in umgekehrter Richtung durch die Kontaktwalzen fliessen, vom gedrückten Taster 'A' nach dem Lämpchen 'd'. Jetzt würde die erwünschte Dechiffrierung stattfinden. Besonders elegant scheint diese Lösung mit dem Umschalten nicht zu sein, auch die Zeitgenossen von Scherbius konnten sich nicht dafür begeistern; sie suchten und fanden Besseres.



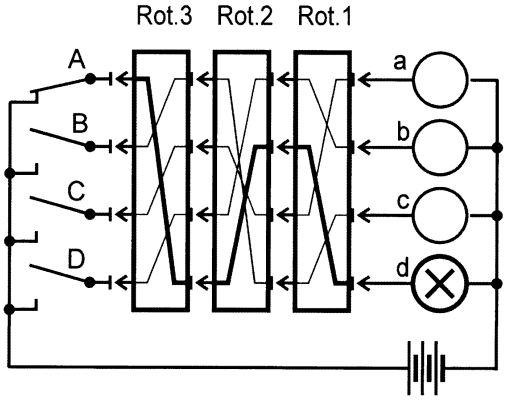
38 Arthur Scherbius, der Urvater der Enigma. [13]

Einführung des Reflektors

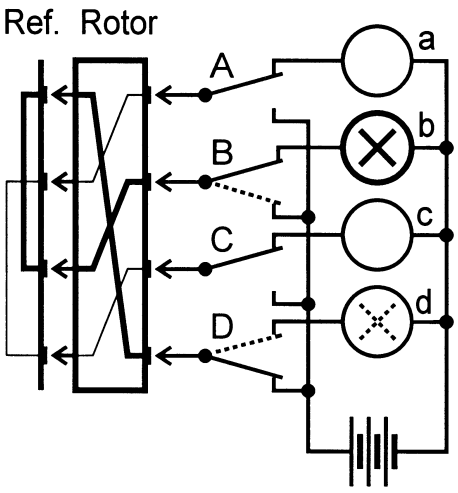
1926/27 löste der Deutsche Willi Korn das Problem mit einer genialen Erfindung. Abb. 40 zeigt in vereinfachter Darstellung, was er im Prinzip gemacht hat. Auf der linken Seite der Schaltung entfernte er die Lämpchen und baute Drahtverbindungen ein. Jeweils zwei Kontakte verband er nach einem unregelmässigen Muster miteinander. Bei der realen Maschine mit 26 Kontakten entstehen so 13 Verbindungen. Diese befinden sich auf einer feststehenden Kontaktplatte. Die Arbeitskontakte an den Tastaturhebeln sind durch Umschalter ersetzt. Die Lämpchen befinden sich auf der Seite der Taster.

Betätigt man zum Chiffrieren den Taster 'D', so leuchtet das Lämpchen 'b'. Zum Dechiffrieren drückt man 'B', und nun leuchtet das Lämpchen 'd'; es findet eine Dechiffrierung statt ohne dass etwas umgeschaltet werden muss! In der Zeichnung sind die Verbindungen beim Dechiffrieren durch gestrichelte Linien gezeichnet. Entsprechendes gilt für alle 26 Taster und Lämpchen. Der Strom fliesst zuerst vom Taster durch den Rotor, wird dort reflektiert (daher der Name "Reflektor"), dann wieder durch den Rotor zurück zu einem Lämpchen. Man kann mit der gleichen Maschine chiffrieren und dechiffrieren. Bei genauem Hinsehen fällt auf, dass der Reflektor etwas ganz besonderes bewirkt: Ein Buchstabe wird niemals in sich selbst überführt. Ganz gleich, welche Stellung der Rotor auch einnimmt, wenn der Taster 'D' betätigt wird, kann das Lämpchen 'd' nie leuchten. Spontan würde man meinen, dass das eine gute Eigenschaft sei, bleibt doch so vom Klartext kein Stein auf dem andern! Tatsächlich aber hat diese Eigenschaft verheerende Folgen auf die Sicherheit dieses Typs von Chiffriermaschine. Die wichtigste Auswirkung lernen wir noch später kennen, eine andere ist das Folgende:

Aus kryptologischer Sicht muss der Geheimtext eine zufällige Verteilung aller Buchstaben aufweisen. Bei einer Maschine mit einem Reflektor ist das nicht der Fall. Wenn wir fortlau-fend den Buchstaben 'A' eintasten würden, käme im erzeugten Geheimtext das 'A' nie vor! Solche Extremfälle gibt es in realen Telegrammen natürlich nicht. Aber denken wir an die Statistik: Im Klartext kommt der Buchstabe 'E' besonders häufig vor, das hat zur Folge, dass bei einer Analyse eines Geheimtextes das 'E' signifikant untervertreten sein wird. Da haken die Kryptanalysten ein, das sind Ansatzpunkte zum Brechen einer Chiffrierung!



39 Zum Dechiffrieren könnte man Tastatur und Lampenfeld miteinander vertauschen. [AUT]



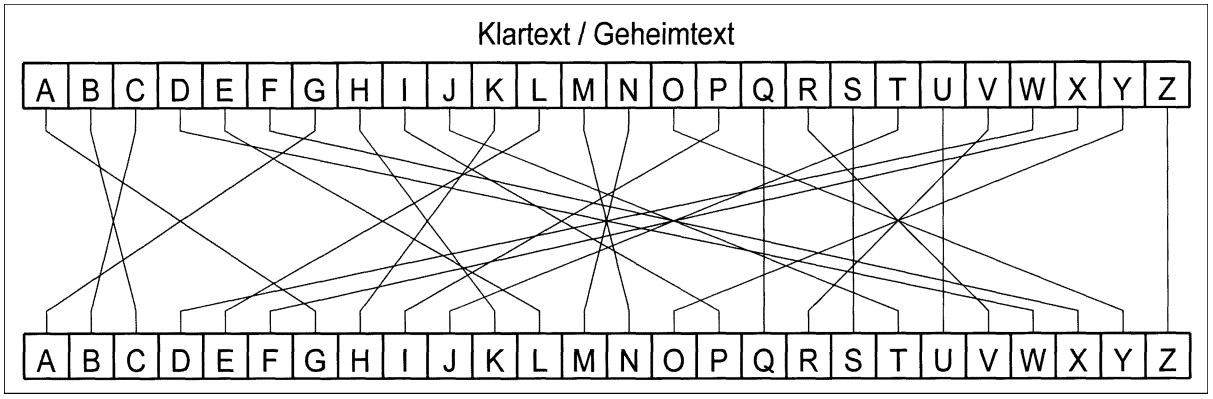
40 Der Reflektor des Deutschen Willi Korn. Die gestrichelten Linien zeigen die Verhältnisse beim Dechiffrieren. [AUT]

Involutorische Permutation

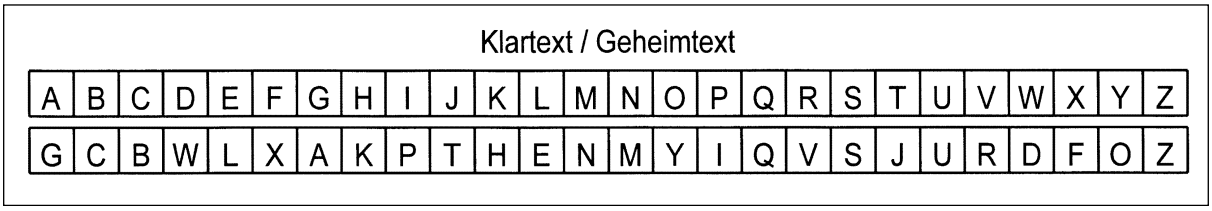
Die Einführung des Reflektors bewirkt eine sogenannte involutorische oder reziproke Permutation. Abb. 41 zeigt eine Tabelle, die nach diesem Prinzip aufgebaut ist. 'A' wird umgesetzt in 'G', dann ist zwingend vorgegeben, dass 'G' in 'A' überführt werden muss. Die Verbindungen oder Zuordnungen erfolgen "übers Kreuz". Zulässig sind auch "gerade" Verbindung, also z.B. 'Q' zu 'Q' und 'S' zu 'S'. Bei der Rotormaschine mit dem Reflektor sind solche "geraden" Verbindungen dagegen nicht realisierbar, das haben wir in der Abb. 40 festgestellt. Man hat bei der involutorischen Permutation bedeutend weniger Möglichkeiten als z.B. bei der Tabelle nach Abb. 17, wo wir keinerlei Einschränkungen und Vorgaben hinzunehmen hatten. Der Vorteil, den wir dafür erhalten ist der, dass man den Klartext beim Chiffrieren und den Geheimtext beim Dechiffrieren auf der gleichen Seite eingeben kann. Was die Tabelle beim ersten mal bewirkt, macht sie beim zweiten Mal wieder zunichte, d. h., aus dem Geheimtext entsteht wieder der Klartext. In Abb. 42 ist die umgezeichnete Abb. 41 zu erkennen, die Zuordnungen von der oberen zur unteren Reihe verlaufen "gradlinig".

Die Enigma

Wenn wir in der Anordnung mit den drei Rotoren (Abb. 37) den Reflektor von Willi Korn einführen, erhalten wir im Wesentlichen die berühmte Chiffriermaschine "Enigma", die von den Deutschen im Zweiten Weltkrieg eingesetzt wurde. In Abb. 43 ist das Prinzip dargestellt. Zusätzlich ist ein Steckerbrett vorhanden, mehr dazu später. Um 1942 wurde bei den Marine-Maschinen noch ein vierter Rotor eingebaut, man wollte die Sicherheit erhöhen. Aus Platz-gründen war dieser schmaler als die übrigen. Man beschrif-tete ihn mit einem griechischen Buchstaben, deshalb die Bezeichnung "Griechenwalze", siehe Abb. 45. Viel brachte dieser vierte Rotor nicht; er bewegte sich während des Chiffrierens höchstens einmal, man denke an die Verhält-nisse beim Kilometerzähler.



41 Eine involutorische Umsetzung. [AUT]

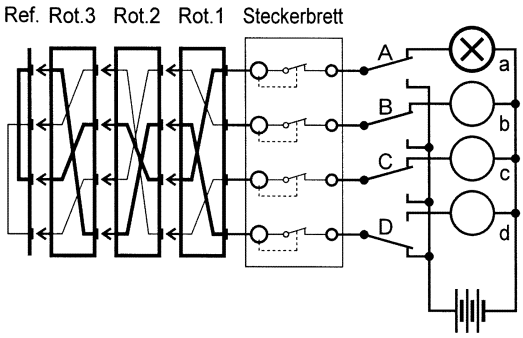


42 Die gleiche Zuordnung wie oben, die untere Zeile ist so geordnet, dass eine "gerade" Zuordnung entsteht zwischen den Zeilen. [AUT]

An den Rotoren lässt sich an einem Ring einstellen, bei welcher Stellung der Nachbarrotor weitergedreht wird. Das ist nicht starr vorgegeben wie beim Kilometerzähler, wo dieser Vorgang logischerweise immer beim Übergang von 9 auf 0 stattfindet.

Jeder der drei Rotoren lässt sich in den Positionen 1, 2 oder 3 einsetzen. Es gibt sechs Möglichkeiten, diese drei Rotoren in verschiedenen Anordnungen zu platzieren, zu permutieren. Selbst wenn die Rotoren in der gleichen Grundstellung stehen (auf den gleichen Schlüssel eingestellt sind) liefert jede der sechs Permutationen eine andere Folge von Umsetztabellen. Tatsächlich stand bei der Enigma ein grösserer Vorrat von Rotoren zur Verfügung. Aus diesem wurden drei ausgewählt und in der Maschine eingesetzt. Bei einem Vorrat von z. B. acht Rotoren liegt die Anzahl der möglichen Permutationen bei: 8! / (8-3)! = 336. Bei der Marinemaschine mit vier Rotoren hatte der vierte, die Griechenwalze, seinen festen Platz, direkt neben dem Reflektor, er konnte nicht permutiert werden.

Bei der realen Maschine sind die Lämpchen hinter einer Kunststoff-Folie angeordnet, auf welcher die Buchstaben aufgedruckt sind. Ein leuchtendes Lämpchen macht den Buchstaben sichtbar.



43 Die Enigma: Drei Rotoren und der Reflektor; zusätzlich ist ein Steckerbrett vorhanden. [AUT]

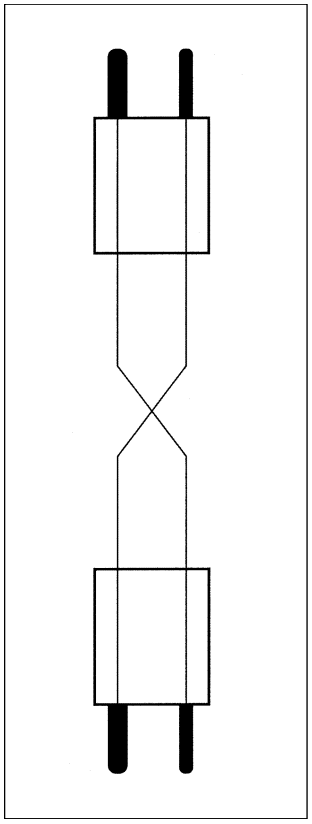
Das Steckerbrett

Die Idee dieser Einrichtung ist die, dass man die festen Verbindungen zwischen den Tastern und dem ersten Rotor untereinander vertauschen kann. Das geschah in der Absicht, die Sicherheit der Enigma zu verbessern. In Abb. 43 ist das Prinzip zu erkennen. Jede der genannten Verbindungen wird auf eine Steckbuchse geführt. Wenn sich kein Stecker in der Buchse befindet, verbindet ein Ruhekontakt die beiden Buchsen miteinander, der Strom fliesst auf direktem Weg "geradeaus" durch das Steckerbrett.

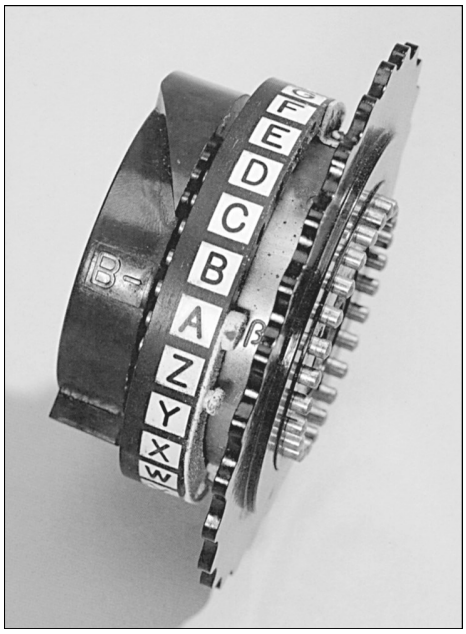
Mit einem Doppelsteckerpaar lassen sich involutorische Vertauschungen vornehmen. Jeder Stecker ist mit zwei Stiften unterschiedlichen Durchmessers versehen, damit er nur in einer Stellung eingesteckt werden kann. Mit dem Einstecken wird die interne Verbindung aufgetrennt. Das andere Kabelende ist mit dem gleichen Stecker versehen, die Verbindungen dazwischen sind "übers Kreuz" geführt, siehe Abb. 44. In Abb. 47 ist das Steckerbrett gut zu erkennen, Abb. 48 zeigt eingesteckte Kabel. Diese werden gemäss den Anweisungen des Schlüsselbefehls in die vorgeschriebenen Buchsen gesteckt. Die Abb. 46 zeigt einen sym -bolischen Ausschnitt des Steckerbretts, zwei Kabelverbindun-gen sind gesteckt. Man erkennt die aus Abb. 40 bekannte involutorische Vertauschung. Es muss unbedingt involuto-risch vertauscht werden, sonst würde die Eigenschaft, dass man mit der gleichen Maschine Chiffrieren und Dechiffrieren kann, verloren gehen. Theoretisch könnte man bei 26 Buch-senpaaren 13 Verbindungen stecken; es standen bei der Enigma aber nur 10 Kabel zur Verfügung. Nicht alle wurden immer gesteckt, mindestens sechs Buchsenpaare blieben in jedem Fall frei.

Elektrisch oder mechanisch?

Bei den vorgestellten Taster-Lämpchen-Schaltungen wird wohl elektrischer Strom benötigt, um die Lämpchen leuchten zu lassen. Trotzdem sprechen wir von einer rein mechani-schen Chiffriermaschine. Der Strom zeigt nur auf elegante Weise an, welche Zuordnung Taster – Lämpchen aktiv ist. Der elektrische Stromfluss hat mit der eigentlichen Krypto-grafie nicht direkt etwas zu tun.

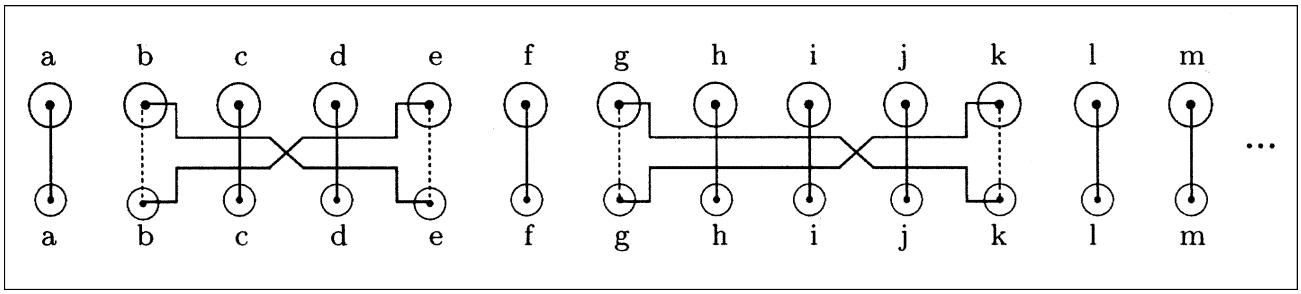


44 Doppelsteckerpaar für die Verbindungen auf dem Steckerbrett. [AUT]



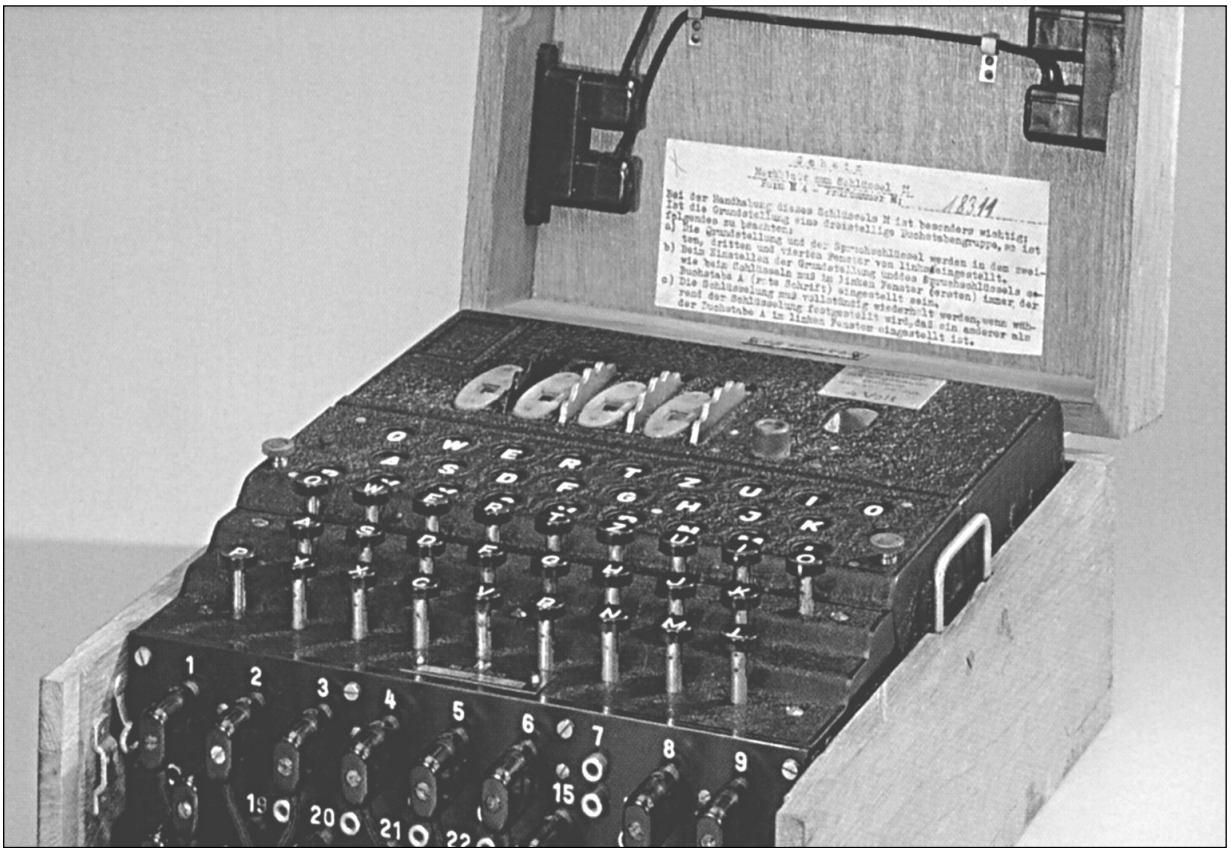
45 Eine "Griechenwalze". Diese vierte Walze bei der Marine-Enigma ist mit einem griechischen Buchstaben beschriftet. Hier die Walze Beta. [16]

46 Das Prinzip des Steckerbretts bei der Enigma. Zwei Doppelsteckerpaare sind verwendet, das erste von 'b' nach 'e', das andere von 'g' nach 'k'. [5]





47 Eine Drei-Rotoren-Enigma im Metallkoffer, die Lampenabdeckung ist hochgeklappt. Es existieren verschiedene Ausführungen, meist jedoch solche mit Holzgehäuse. [16]



48 Eine Marine-Enigma im Holzgehäuse mit vier Rotoren, links die "Griechenwalze" mit schwarzem Einstellrad. [16]



49 Die Enigma im Einsatz bei der deutsche Wehrmacht. [16]

Die Nema

Jeder Entwickler eines Chiffrierverfahrens ist davon überzeugt, dass seine Erfindung absolut sicher sei.

Wann und warum wurde sie gebaut?

Während des Zweiten Weltkrieges verfügte die Schweizer Armee nicht über eine eigene, leistungsfähige Chiffriermaschine. Vor dem Zweiten Weltkrieg war die kommerzielle Enigma im Handel frei erhältlich, siehe Abb. 102. Auch die Schweizer Armee wurde mit dieser Maschine ausgerüstet. Besondere Umstände zwangen die Verantwortlichen in der Schweiz um 1943 zur Entwicklung und Fabrikation einer eigenen Chiffriermaschine. Als Vorbild diente die Enigma, ihre Arbeitsweise und die theoretischen Grundlagen waren allgemein bekannt. Über die Umstände, die zur Entwicklung der Nema führten, sind im Kapitel "Geschichte der Nema" Details und Dokumente zu finden.

Die Entwickler in der Schweiz konnten damals nicht wissen, dass die Enigma während des Krieges von den Briten systematisch gebrochen wurde. Man wusste oder ahnte zwar, dass die Enigma bei nicht sachgemässem Einsatz unsicher sein konnte, siehe Entwicklungsgeschichte. Aber die Enigma galt allgemein als sicher, auch die deutschen Militärs waren von der Sicherheit der Enigma überzeugt.

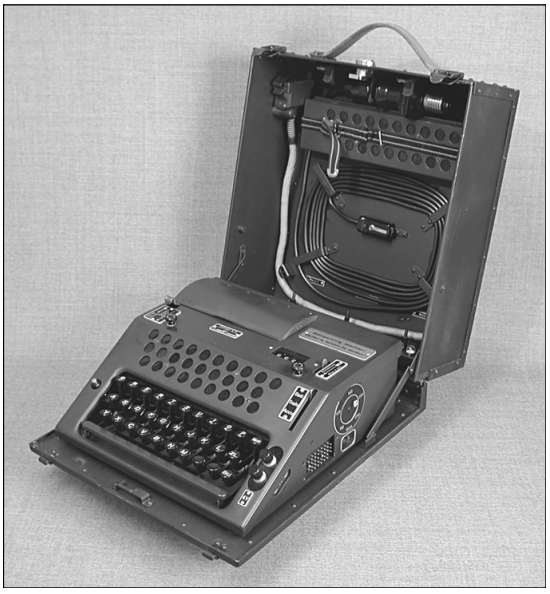
Die Briten hielten ihre Erfolge beim Brechen der Enigma geheim; selbst in den eigenen Reihen wusste man bis hinauf zu höchsten Stellen nicht, woher die wertvollen Informationen stammten. Noch lange Zeit über den Zweiten Weltkrieg hinaus blieben die entsprechenden Akten über die Aktivität des britischen Geheimdienstes unter Verschluss. In seinem 1974 erschienenen Buch "The Ultra Secret" [15] schreibt Frederick W. Winterbotham erstmals umfassend über die Erfolge der polnischen und britischen Kryptanalytiker.

Bei der Schweizer Eigenentwicklung wollte man die Sicherheit der Maschine auf jeden Fall erhöhen. Darum wurde die Anzahl der Rotoren auf fünf erhöht und deren Vorschubsystem grundlegend geändert. Der entscheidende Schwachpunkt der Enigma, der Reflektor, wurde aber auch bei der Nema eingesetzt, es gab keine Alternative dafür, wenn man die elegante involutorische Eigenschaft beibehalten wollte. Daraus muss man schliessen, dass die Mathematiker und Konstrukteure im Chiffrebureau der Armee nichts wussten von den polnisch/britischen Erfolgen beim Brechen der Enigma, die hauptsächlich auf den nachteiligen Eigenschaften des Reflektors beruhten. Sie konnten es zur damaligen Zeit auch nicht wissen!

Unter grösster Geheimhaltung wurden bei der Apparate- und Maschinenfabrik Zellweger in Uster 640 Maschinen gebaut, siehe Abb. 108. Die Geheimhaltung ging so weit, dass aus deren Bezeichnung nicht hervorgehen durfte, wozu sie Verwendung fand. Offiziell hiess sie "Nema", die Abkürzung für Neue Maschine. In der Bedienungsanleitung, siehe Abb. 56, ist auch die Benennung oder Typenbezeichnung "T-D", "Tasten-Drücker-Maschine" erwähnt. Im Frühjahr 1947 wurden erste Exemplare an die Truppen ausgeliefert. Bei den "Fliegern" wollte man nach einem Erprobungsversuch jedoch bei der vermeintlich sicheren Enigma bleiben. Bei dieser Einheit blieb die Enigma offiziell bis in die 1970er-Jahre im Einsatz. Die anderen Armee-Einheiten und das "Eidgenössische Politische Departement" (EPD), das heutige Departement für Äusseres, übernahmen die Nema. Sie galt als sicherer als die Enigma. Beim EPD fand sie Verwendung im Verkehr mit den Botschaften; bis etwa 1976 stand die Nema dort im Einsatz.



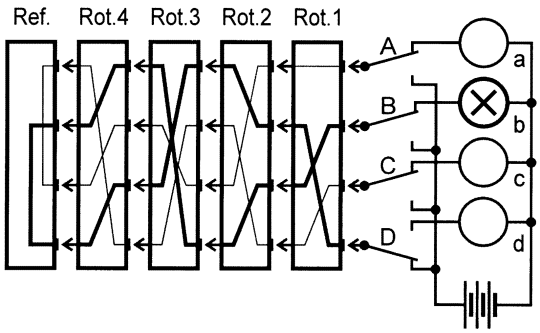
50 Ansicht der geschlossenen Nema, ein schwarzer Koffer mit einem Gewicht von fast 11 kg und den Abmessungen: 33 x 38 x 15 cm. [AUT]



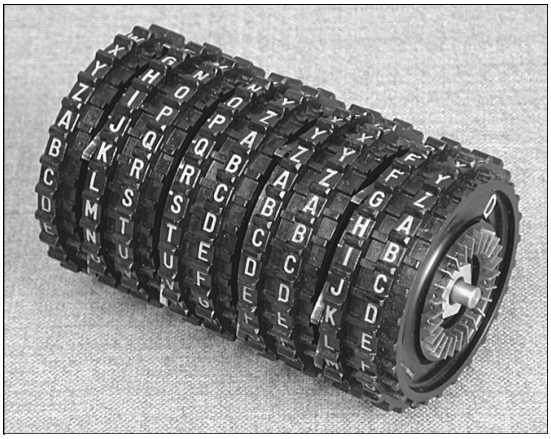
51 Die Nema mit geöffnetem Deckel, einsatzbereiter Zustand. [AUT]



52 Das Typenschild der Nema. Nicht der geringste Hinweis ist zu finden, dass es sich um eine Chiffriermaschine handelt. [AUT]



53 Kryptologisches Schema der Nema. Der drehbare Reflektor bekommt die Eigenschaft eines Rotors, ein Steckerbrett fehlt. Die fünf Fortschaltwalzen sind hier nicht gezeichnet, sie tragen nicht direkt zur Permutierung bei. [AUT]



54 Das Herz der Nema: Das Rotor- oder Walzenpaket. Die rote 10. Walze verbleibt in der Maschine. [AUT]

Verbesserungen gegenüber der Enigma

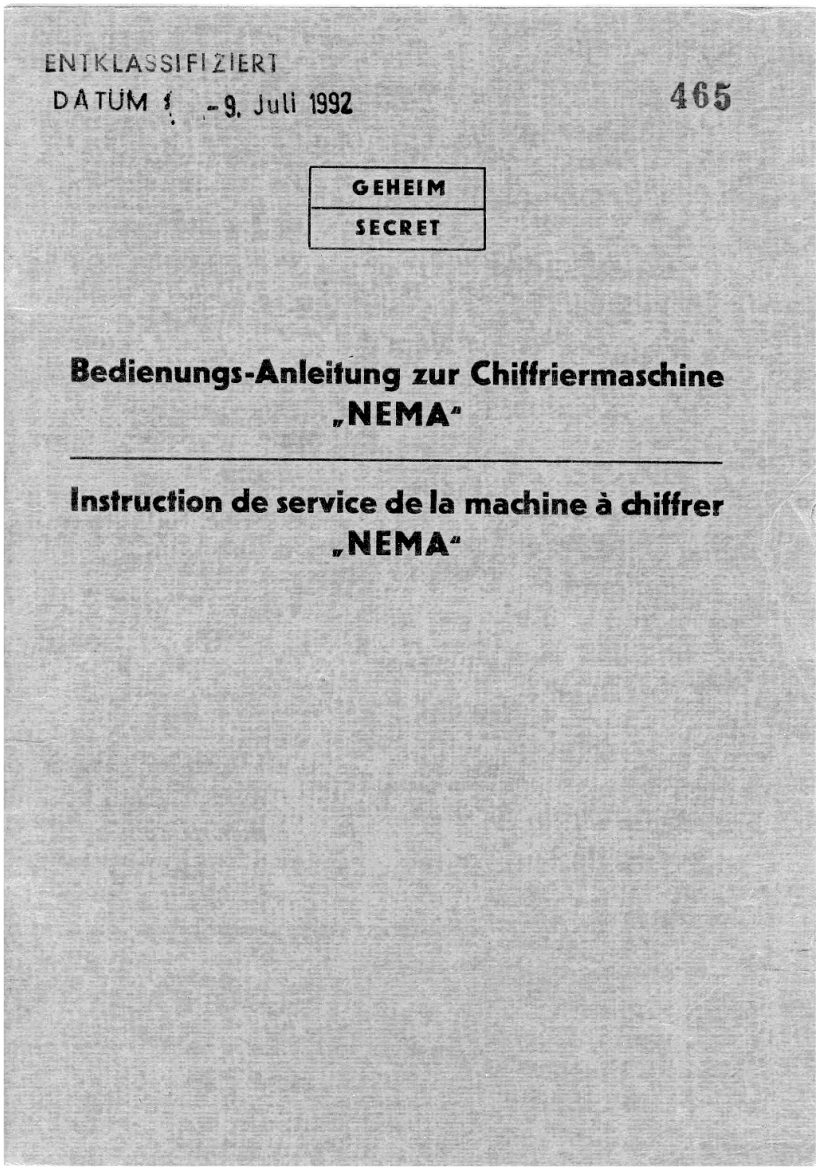
Die erste Änderung betraf die Anzahl der Rotoren. Neben vier "normalen" Rotoren – bei der Nema werden sie Kontaktwalzen, selten auch Permutierwalzen genannt – ist der Reflektor drehbar angeordnet, so dass er die Eigenschaft eines Rotors bekommt, siehe Abb. 53. Der Reflektor wird bei der Nema als Umkehrwalze bezeichnet.

Die entscheidende Verbesserung gegenüber der Enigma liegt beim Vorschubsystem der Walzen. Bei der Enigma geschieht der Vorschub wie bei einem Zähler, regelmässig und einfach durchschaubar. Nur bei jeder 26. Tastenbetätigung drehen sich dort mehrere Rotoren gleichzeitig. Der vierte Rotor bei der Marine-Enigma hat sich höchstens einmal bewegt. Es ist daher einleuchtend, dass zusätzliche Rotoren beim Enigma-Vorschub-System nichts zur Sicherheit beigetragen hätten. Mit zusätzlichen Rotoren wäre nur der Schlüsselraum grösser geworden. Nicht so bei der Nema, bei ihr wird der Vorschub jeder Kontaktwalze (KW) von einer eigenen Fortschaltwalze (FW) gesteuert. Der Vorschub der Walzen wirkt chaotisch, nach einem undurchschaubaren System ablaufend. Man hat den Eindruck, dass sich alle Walzen mehr oder weniger gleich oft, aber ungleichmässig bewegen. Da jeder der fünf Kontaktwalzen eine eigene Fortschaltwalze (Abb. 119) zugeordnet ist, steigt die Anzahl der aktiven Walzen auf zehn. Daraus ergibt sich ein Schlüsselraum von 26^{10}, das entspricht der Zahl von etwa 140 Billionen. Direkt an der Chiffrierung sind nur 5 Walzen beteiligt, es wäre deshalb falsch, zu sagen, die Nema arbeite mit 10 Permutierwalzen und die Enigma nur mit deren drei oder vier, je nach Maschinentyp.

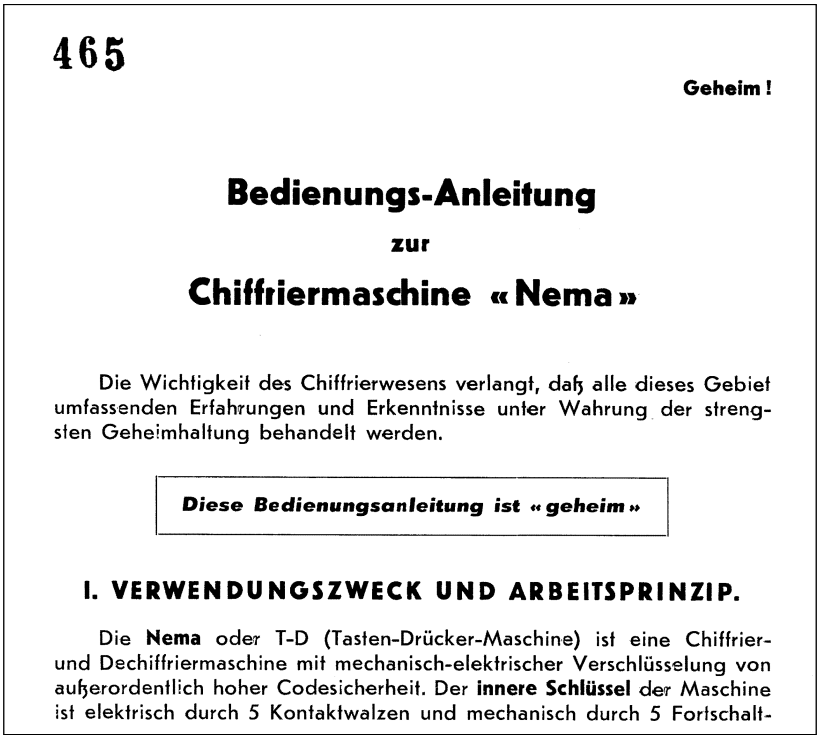
Die Ausgestaltung der Fortschaltwalzen – für jede einzelne gibt es Millionen von Möglichkeiten – ist entscheidend für den Vorschub der Kontaktwalzen. Da ohne Kenntnis des Walzenvorschubs das Brechen einer Rotormaschine nicht möglich ist, tragen die Fortschaltwalzen indirekt wesentlich zur Sicherheit bei.

Das Steckerbrett, das bei der Enigma Verwendung fand, liess man bei der Nema weg. Da diese Einrichtung statisch ist – sich während des Chiffrierens nicht verändert – trägt sie zur Sicherheit nicht viel bei. Zudem wurde die Sicherheit durch die grössere Anzahl an Kontaktwalzen und die Einführung der Fortschaltwalzen so stark verbessert, dass man auf die Verwendung des Steckerbretts mit gutem Gewissen verzichten konnte. Eine potentielle Quelle für fehlerhafte Einstellungen fiel damit weg.

Um die Nema zu verstehen, ist es nicht erforderlich, das Vorschubsystem im Detail zu durchschauen. Man muss nur wissen, dass der Vorschub nach einem unregelmässigen Schema erfolgt. Bei einem Tastendruck bewegen sich immer mindestens drei Walzen, es können aber auch alle zehn weiterschalten. Das ist auch der Grund dafür, dass die Nema schwergängiger ist als die Enigma. Für Interessierte ist im Anhang die Vorschubmechanik der Nema im Detail beschrieben.



55 Die zweisprachige Bedienungsanleitung der Nema in braunem Einband umfasst 32 Seiten. Die Nummern reichen bis über 1000. Ein Teil der Auflage wurde erst mit Datum vom 13. Feb. 1998 entklassifiziert. [AUT]



465

Geheim !

Bedienungs-Anleitung

zur

Chiffriermaschine « Nema »

Die Wichtigkeit des Chiffrierwesens verlangt, daß alle dieses Gebiet umfassenden Erfahrungen und Erkenntnisse unter Wahrung der strengsten Geheimhaltung behandelt werden.

Diese Bedienungsanleitung ist « geheim »

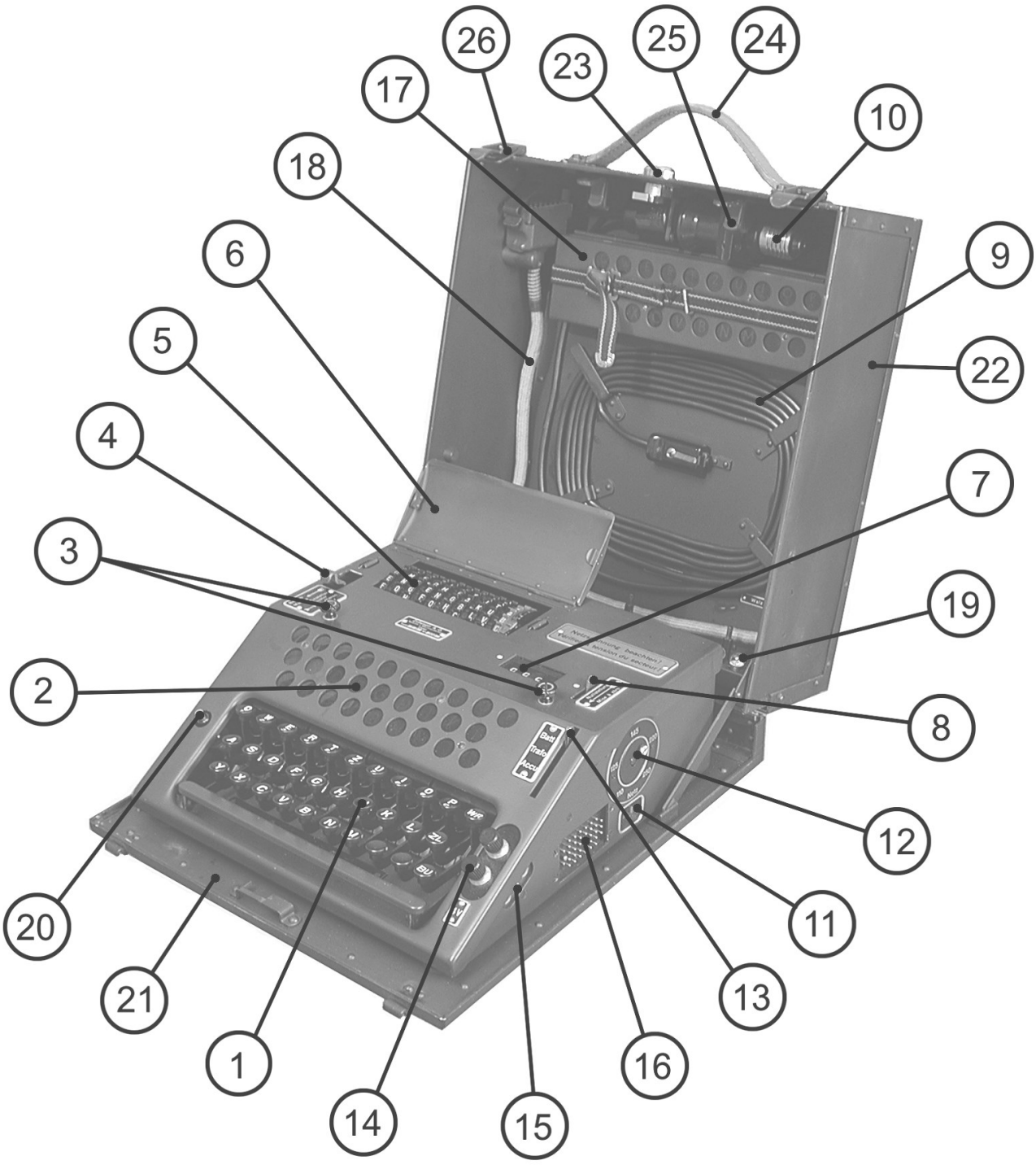
I. VERWENDUNGSZWECK UND ARBEITSPRINZIP.

Die **Nema** oder T-D (Tasten-Drücker-Maschine) ist eine Chiffrier- und Dechiffriermaschine mit mechanisch-elektrischer Verschlüsselung von außerordentlich hoher Codesicherheit. Der **innere Schlüssel** der Maschine ist elektrisch durch 5 Kontaktwalzen und mechanisch durch 5 Fortschalt-

56 Ein Auszug aus der ersten Seite der Bedienungsanleitung. Hier wird die alternative Benennung *"T-D (Tasten-Drücker-Maschine)"* erwähnt. [AUT]

Wichtige Teile der Maschine

Die Maschine ist in einem abschliessbaren Koffer aus Panzerholz (Sandwichmaterial: Alu-Holz-Alu) eingebaut. Er hat die Masse 332 x 384 x 148 mm und wiegt ohne Batterie 10,7 kg. Die eigentliche Maschine ist mit dem Koffer fest verschraubt und wird zum Arbeiten normalerweise nicht herausgenommen. Die Abb. 57 zeigt die einsatzbereite Maschine mit deren wichtigsten Teilen und Bedienelementen.



57 Die Nema mit ihren wichtigsten Bestandteilen. [AUT]

1) Tastatur
Mit 26 aktiven Buchstabentasten A ... Z. Die übrigen Tasten sind entweder blockiert oder für den Chiffriervorgang wirkungslos.

2) Lampenfeld
Unter dem Deckel sind die 26 Glühlämpchen A ... Z angeordnet. In den runden Ausschnitten werden die von den Lämpchen beleuchteten Buchstaben sichtbar.

3) Zwei Rändelschrauben mit rotem Ring
Zwei mit einem roten Ring markierte Schrauben. Sie geben den Maschinendeckel frei und man erhält Zugang zum Walzenpaket, den Lämpchen und zum Batteriefach.

4) Roter Hebel
Er wird betätigt um das Walzenpaket ein- und auszubauen, sowie zur Korrektur bei fehlerhaften Tasteneingaben.

5) Walzenpaket
Bestehend aus der Umkehrwalze mit fest angebauter Achse und vier Walzenpaaren, die je aus einer Kontakt- und einer Fortschaltwalze zusammengesteckt sind, siehe Abb. 54.

6) Abdeckklappe
Schützt das Walzenpaket vor Staub und vor all zu neugierigen Augen.

7) Schrittzähler
Vierstellige Anzeige, sie zählt die ausgeführten Chiffrierschritte, resp. Tastenbetätigungen.

8) Rückstellhebel
Setzt den Zähler auf Null. Eine Voreinstellung auf einen frei wählbaren Wert ist nicht möglich.

9) Netzkabel, 3-polig, 4 m lang

10) Steckdosenfassung "Edison 2P"
Früher sehr verbreitet, heute ist deren Verwendung verboten. Sie wird zwischen Glühlampe und Lampenfassung geschraubt, an zwei Steckdosen kann (bei eingeschalteter Lampe) Netzstrom abgenommen werden, Abb. 60.

11) Apparatedose für den Netzanschluss

12) Spannungswähler für die Netzspannung
Es lassen sich verschiedene Netzspannung zwischen 110 und 250 Volt einstellen.

13) Wahlschalter für die Stromquelle
Batt – interne Batterie, 4,5 Volt
Trafo – Netzspeisung AC
Accu – externe Quelle, 4 Volt AC oder DC

14) Anschlussklemmen
Für eine externe Spannungsquelle von 4 Volt. Hier schliesst man z. B. zwei Zellen eines Bleiakkus an.

15) Anschlussbuchsen
Für die externe Spannungsquelle 4 Volt. Auf die Polarität muss nicht geachtet werden, das gilt auch bei 14).

16) Steckeranschluss für das externe Lampenfeld
Es war geplant, an Stelle des Lampenfeldes auch ein druckendes Ausgabegerät anschliessen zu können.

17) Externes Lampenfeld
Es ist mit 26 Lämpchen versehen, diese leuchten parallel zu denen im Anzeigefeld. Mit Stoffriemchen befestigt.



58 Eines der 26 Lämpchen, die im Lampenfeld eingebaut sind. [AUT]



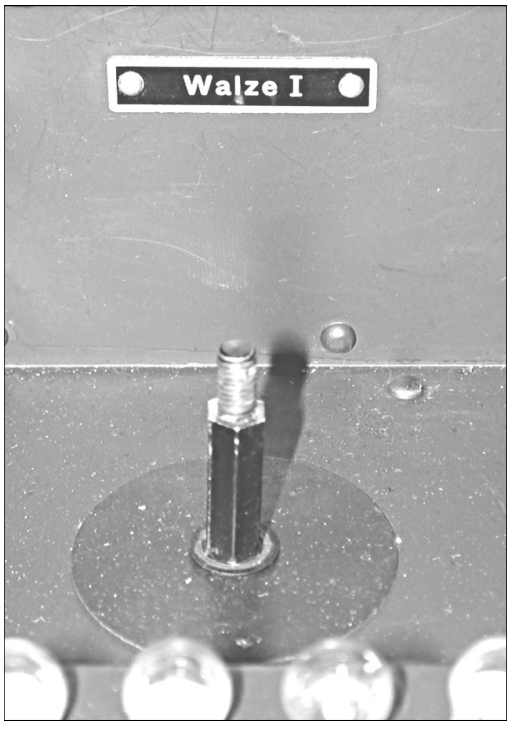
59 Mit diesem Schalter (13) wird die gewünschte Stromquelle eingestellt. [AUT]



60 Steckdosenfassung "Edison 2P" (10) für die Entnahme von Netzstrom aus einer Lampenfassung. [AUT]



61 Der Hauptschalter (Pfeil). Unten links ist eine der drei Schrauben zu sehen, mit welchen die Maschine auf dem Boden befestigt ist. [AUT]



62 Einer der drei Befestigungspfosten zur Aufnahme von Reserve-Walzen. Die zugehörende Abdeckhaube ist auf Abb. 125 zu sehen. [AUT]

18) Verbindungskabel, 90 cm lang
Damit wird das externe Lampenfeld über den Stecker (16) mit der Maschine verbunden.

19) Reservelämpchen
Es sind 16 Stück vorhanden, 3,5 Volt, 0,2 Amp., es handelt sich um handelsübliche Taschenlampen-Birnchen.

20) Hauptschalter
Bei geschlossenem Deckel wird dieser Knopf von einem Steg im Deckel niedergedrückt und schaltet die Stromzufuhr ab. Damit wird ein ungewolltes Entladen der Batterie verhindert, wenn bei geschlossenem Deckel ein eingeklemmter Gegenstand eine Taste niederdrückt, Abb. 61.

21) Kofferboden
Die eigentliche Chiffriermaschine ist mit drei Schrauben auf dem Boden befestigt. Bei geöffnetem Maschinendeckel sieht man zwei Schrauben links und rechts neben der langen Taste, Abb. 61. Die dritte Schraube ist im Batteriefach zugänglich, siehe Abb. 63, rechts neben der Batterie. Diese drei Schrauben sind mit einem roten Ring markiert.

22) Kofferdeckel
Fester Bestandteil der Maschine, er bleibt beim Arbeiten in dieser Position mit der Maschine verbunden.

23) Kofferschloss
Zu jeder Maschine gehören zwei Schlüssel und eine Plakette von 20 mm Durchmesser. Auf diesen drei Teilen ist die Maschinen-Nummer eingeschlagen.

24) Traggriff aus Leder

25) Zwei Manuskripthalter
An diesen zwei Klammern kann der Chiffreur seine Arbeitspapiere gut sichtbar befestigen.

26) Zwei Verschlussbügel
Fixieren den Deckel am Boden. Vorsicht: Wenn das Schloss nicht geöffnet ist, kann der Deckel nicht geschlossen werden, keine Gewalt anwenden!

Reservewalzen

Unten im Deckel sind drei Gewindepfosten angebracht, sie dienen als Halter für plombierbare Abdeckhauben, siehe Abb. 125. Unter diesen waren bei speziellen Maschinen zwei Reserve-Doppelwalzen und ein Satz von acht Zahnscheiben untergebracht. Abb. 62 zeigt einen dieser Pfosten. Sie sind beschriftet mit "Walze I", "Zahnscheiben" und "Walze II".

Originalbatterie

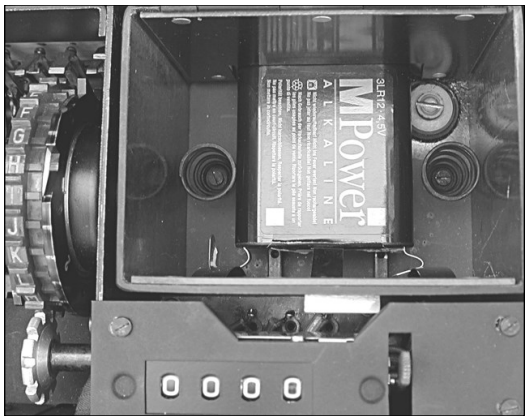
Die Originalbatterie (L. S. A. Nr. 1004,) mit 4,5 Volt Spannung und 6,5 Ah Kapazität (100 x 67 x 76 mm) ist im Handel nicht mehr erhältlich. Das Batteriefach wurde damals aber so konstruiert, dass auch eine handelsübliche Flachbatterie von 4,5 Volt eingesetzt werden kann. Eine Aussparung und eine Feder halten sie fest, Abb. 63.

Inbetriebnahme

Bevor mit der Nema gearbeitet werden kann, sind einige Vorbereitungen auszuführen:

- **Stromversorgung**
  Falls keine Batterie eingebaut ist, schliesst man entweder das 230-Volt-Netz oder eine externe Spannungsquelle an. Der Stromquellen-Schalter wird auf die zutreffende Position gestellt. Ob der Netzspannungs-Wahlschalter auf 220 oder 250 steht ist unkritisch.

- **Externes Lampenfeld**
  Wenn zwei Personen an der Maschine arbeiten, ist es zweckmässig, das externe Lampenfeld anzuschliessen. Die Lämpchen auf den beiden Lampenfeldern sind parallel geschaltet, sie leuchten gleichzeitig.



63 Das Batteriefach. An Stelle der grossen Originalbatterie kann eine 4,5-Volt-Taschenlampen-Batterie eingesetzt werden. Ob "auf dem Bauch" oder "auf dem Rücken" liegend ist nicht von Bedeutung. Eine Aussparung (hinten) und eine Feder (vorn) fixieren die Batterie. [AUT]

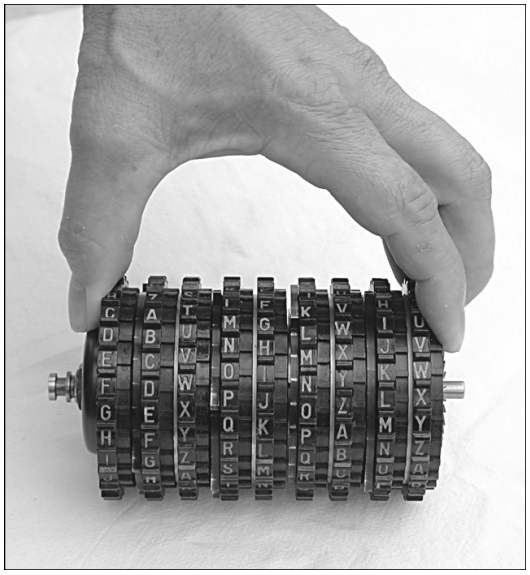
Schlüssel einstellen

Bei der Nema (ebenso bei der Enigma) kennt man zwei verschiedene Schlüssel, den inneren und den äusseren. Im **Schlüsselbefehl** sind sie beschrieben; mit ihm wird die Grundeinstellung der Maschine vorgenommen.

Einstellen des inneren Schlüssels:

Der innere Schlüssel beschreibt, in welcher Reihenfolge die Kontakt- und Fortschaltwalzen in der Maschine einzubauen sind. Die Einstellung des inneren Schlüssel geht bei der Nema wie folgt vor sich:

- Die Abdeckklappe (6) öffnen, den roten Hebel (4) in die Stellung "Einstellen" bringen.
- Die beiden roten Schrauben (3) lösen und den Maschinendeckel hochklappen.
- Den roten Hebel ganz nach hinten drücken, dazu ist etwas Kraft aufzuwenden.
- Mit einer Hand werden die neun schwarzen Walzen gefasst und leicht zusammengedrückt. Jetzt können sie nach oben herausgehoben werden, siehe Abb. 64. Die rote Walze bleibt in der Maschine.
- Die vier Walzenpaare werden von der Achse abgezogen und voneinander getrennt. Dazu fassen die Fingerkuppen jeder Hand eine Walze. Mit einem satten Ruck werden sie auseinander gezogen. Wenn sie wegen langen Nichtgebrauchs festsitzen, greift man mit den Fingerkuppen beider Hände zwischen die Walzen. Die beiden Daumen drücken kräftig auf die Kontakte. Die Walze mit der Zahl muss auf der Daumenseite liegen. Abb. 65 zeigt, wie das gemacht wird.
- Nun liegen die acht Walzen und die Umkehrwalze mit der fest angebauten Achse einzeln vor uns. Die Fortschaltwalzen sind seitlich mit Zahlen bezeichnet, die Kontaktwalzen mit Buchstaben.
- Das Walzenpaket wird nach den Angaben des Schlüsselbefehls neu zusammengesteckt. Dieser kann z.B. lauten:



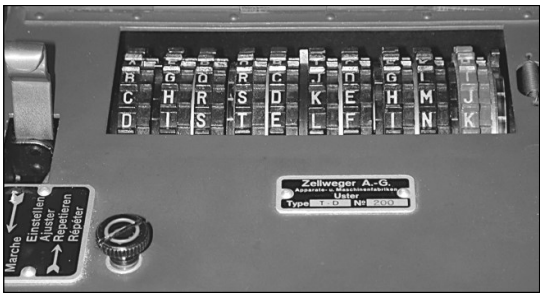
64 Für den Ein- und Ausbau wird das Walzenpaket so gefasst und leicht zusammengepresst. [AUT]

- Zuerst steckt man die vier Walzenpaare zusammen, jedes

20-B / 19-A / 21-C / 16-D



65 Trennen eines Walzenpaares. Die Fingerkuppen greifen zwischen die Walzen, die beiden Daumen drücken auf die Kontakte. Die Zahnscheibe (Zahl) muss auf der Daumenseite liegen. [AUT]



66 Der äussere Schlüssel ist auf "DISTELFINK" eingestellt. [AUT]

besteht aus einer Fortschalt- und Kontaktwalze. In der vorgeschriebenen Reihenfolge schiebt man die Paare auf die Achse, zuerst das Paar "20-B", es kommt direkt an die Umkehrwalze zu liegen. Zum Schluss kontrolliert man, ob keine der Beschriftungen A ... Z am Umfang der Walzen auf dem Kopf steht, sonst wäre ein Paar falsch herum aufgeschoben worden. Jetzt wird das Walzenpaket eingesetzt:

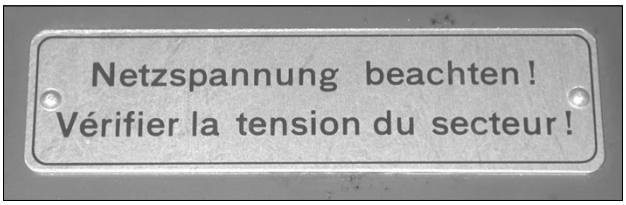
- Der rote Hebel muss ganz nach hinten gedrückt sein. Das Walzenpaket wird mit einer Hand gefasst, etwas zusammengedrückt und in die Maschine eingesetzt. Man achtet darauf, dass die Achse in die dafür vorgesehenen Lagerstellen zu liegen kommt.
- Der rote Hebel wird in die Stellung "Einstellen" gezogen, das geht ziemlich streng! Diese Bewegung drückt das Walzenpaket zusammen, die Kontaktfedern werden gespannt und stellen die Verbindungen zwischen den Walzen her.
- Der Maschinendeckel wird geschlossen und die beiden roten Schrauben leicht festgezogen.
- Der innere Schlüssel ist eingestellt.

Einstellen des äusseren Schlüssels

Unter dem äusseren Schlüssel versteht man die Anfangsstellung der Walzen zu Beginn des Chiffrier- oder des Dechiffriervorgangs. Diese Einstellung wird wie folgt vorgenommen:

- Die Abdeckklappe (6) öffnen und den roten Hebel (4) in die Position "Einstellen" bringen.
- Die einzelnen Walzen werden nach den Angaben des Schlüsselbefehls in die entsprechende Stellung gedreht. Die Walzen dürfen vorwärts und rückwärts bewegt werden. Als Referenz für die Schlüsseleinstellung gilt die noch ganz sichtbare Position an der vorderen Kante der Öffnung. Siehe Abb. 66, dort ist der Schlüssel auf "DISTELFINK" eingestellt.
- Den roten Hebel auf "Betrieb" stellen, und das Zählwerk mit dem Rückstellhebel (8) auf Null setzen.
- Jetzt folgt etwas Wichtiges! Im Reglement wird vorgeschrieben, dass nach jedem Verstellen der Walzen die Taste 'Q' gedrückt werden müsse. Es muss nicht zwingend die Taste 'Q' sein, jede der Tasten A ... Z ist dazu geeignet. Mit diesem "leeren" Tastendruck wird erreicht, dass sich die Vorschubzungen aus ihrer Arretierung lösen und in die Arbeitsposition an den Walzen zurückkehren. Keine der Walzen darf sich bei diesem Vorgang bewegen. Man darf die Walzen jetzt nicht mehr von Hand verstellen, weil die Zungen beschädigt werden könnten.
- Kontrolle: Das Zählwerk steht noch immer auf Null, keine der Walzen hat sich verstellt, der äussere Schlüssel ist unverändert.
- Damit ist der äussere Schlüssel eingestellt, die Maschine ist für das Chiffrieren oder Dechiffrieren einsatzbereit.

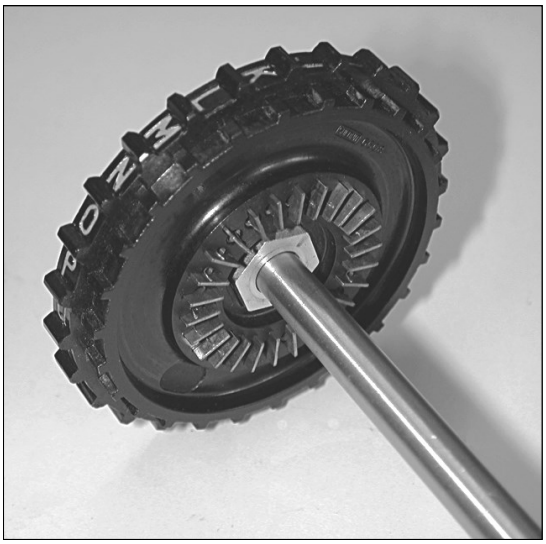
Detailbilder der Nema



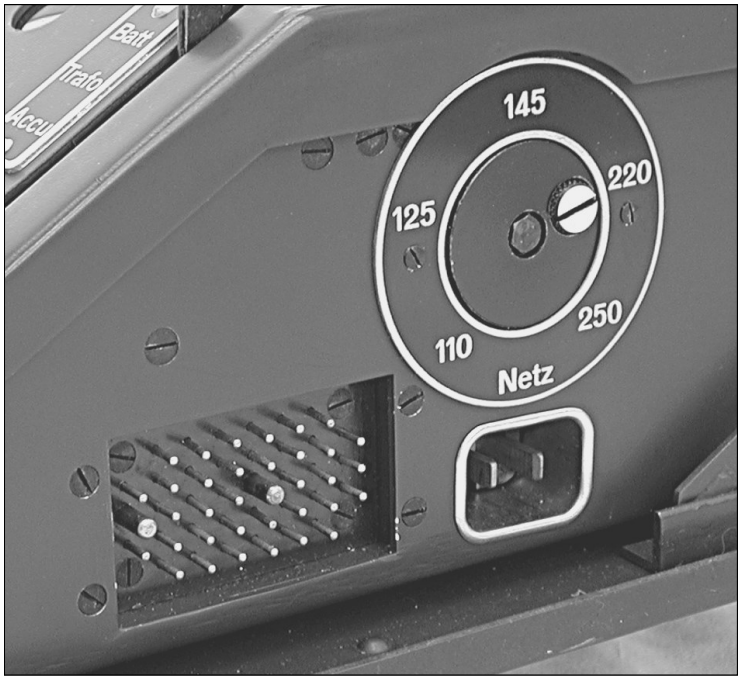
67 Gelbes Hinweisschild. Früher war die Netzspannung nicht einheitlich 230 Volt. [AUT]



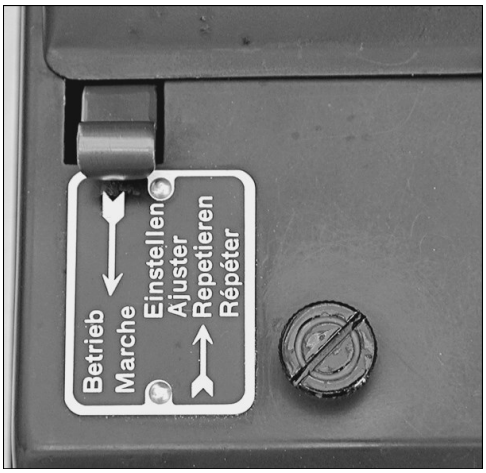
68 Die beiden Schlüssel für den Koffer, mit Plakette und Ring. [AUT]



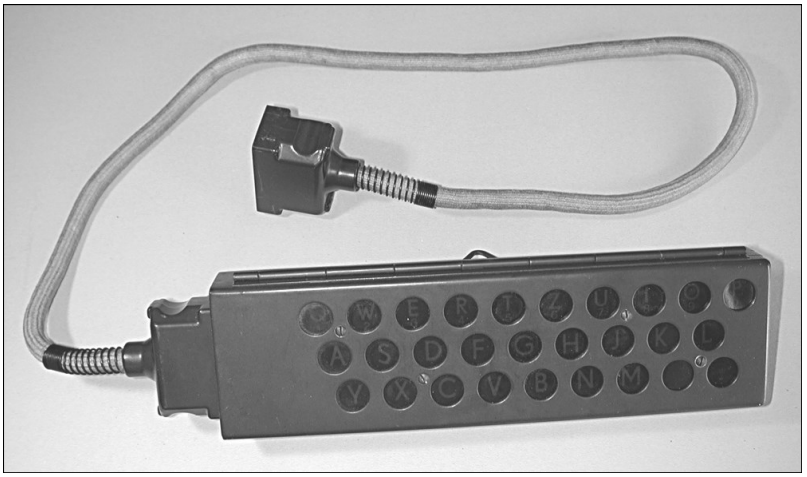
69 Die Umkehrwalze mit fest angebauter Achse. [AUT]



70 Netzspannungs-Wahlschalter, Netzanschluss und Steckdose für das Lampenfeld. [AUT]



71 Der rote Hebel, rechts daneben eine der beiden Schrauben mit dem roten Ring. [AUT]



72 Das Zusatz-Lampenfeld mit angeschlossenem Kabel. [AUT]

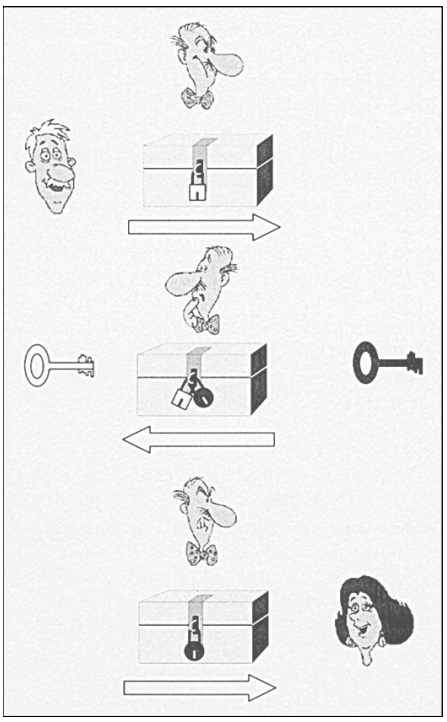
Wichtige Grundsätze der Kryptografie lauten:
- Unterschätze niemals den Gegner.
- Der Gegner weiss mehr als man vermutet.

Schlüsselorganisation

Die Sicherheit beim Chiffrieren steht und fällt mit der Geheimhaltung der Schlüssel. Eine kritische Phase ist das Verteilen der Schlüssel. Wie kommen diese sicher zu den Aussenstationen? Nicht brauchbar ist natürlich jeder unsichere Kanal. Absolut sichere Wege gibt es nicht. Am besten eignet ist noch immer ein zuverlässiger Kurier, der die neuen Schlüssel überbringt.

Im Gegensatz zum Telegramm, das dann abgeschickt werden muss, wenn es aktuell ist, kann die Schlüsselverteilung weit im voraus auf Vorrat erfolgen, der Zeitpunkt ist nicht von Bedeutung. Man wird die Schlüssel bei Gelegenheit einem zuverlässigen Kurier mitgeben.

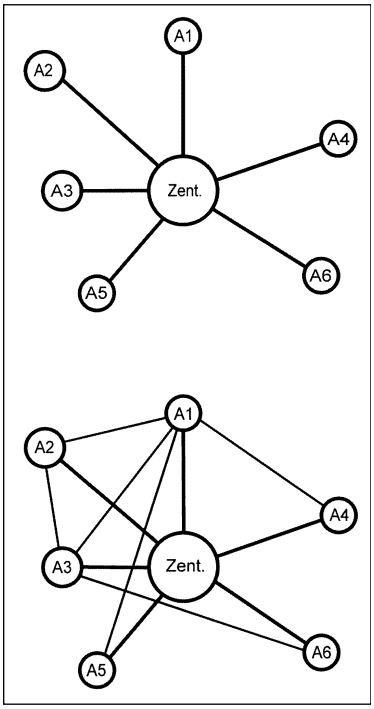
Nur nebenbei: Bei neu entwickelten Chiffrierverfahren kennt man solche, die ohne Schlüsseltausch auskommen. Sehen wir uns dazu nochmals die Abb. 2 an. Herr Weiss schliesst das Schloss mit einem Schlüssel. Frau Schwarz könnte ihm auch ein offenes Schnappschloss geben, das er nur zudrücken müsste. Er könnte dann allerdings die Kiste nicht mehr selber öffnen! Nur Frau Schwarz benötigte in diesem Fall einen Schlüssel, den sie nie aus der Hand geben müsste. Auch die Methode nach Abb. 73 kommt ohne einen Schlüsseltausch aus. Sie erklärt sich von selbst. Solche Verfahren können nur mit Computerprogrammen realisiert werden; mit mechanischen Maschinen geht es nicht.



73 Es geht auch ohne Schlüsseltausch. Niemand muss hier den eigenen Schlüssel aus der Hand geben. [1]

Netzarten

Die geeignete Schlüsselorganisation hängt stark davon ab, wie das Verbindungsnetz aufgebaut ist. Wer muss mit wem und wie oft Telegramme austauschen? Gibt es Meldungen, die von einer Zentrale als Rundschreiben an alle Aussenstationen geschickt werden? Haben die Aussenstationen untereinander Kontakt? Wir sehen uns an, wie zwei typische Netzformen aufgebaut sind und was das für die Schlüsselorganisation für Konsequenzen hat.



74 Oben ein sternförmiges Netz, unten mit zusätzlichen Querverbindungen. [AUT]

Sternförmiges Netz

Die Aussenstationen stehen nur mit der Zentrale in Verbindung, untereinander verkehren sie nicht. Die Zentrale schickt Meldungen nur an einzelne Stationen, also keine "Rundschreiben". Ein typischer Vertreter eines solchen Netzes ist der Botschaftsfunk, siehe Abb. 74 oben. In diesem Fall ist die Schlüsselorganisation einfach. Die Zentrale schickt per Kurier an jeden Posten eine Schlüsselliste, eine Kopie bewahrt sie bei sich auf. Die Schlüssel tragen eine Nummer. Damit es nicht zu Doppelbelegungen kommt, werden zwei Listen benötigt, für jede Verkehrsrichtung eine separate. Abb. 75 zeigt, wie eine solche Liste aussehen kann. Für jedes Telegramm wird ein neuer Schlüssel verwendet. Nach Gebrauch streicht man ihn durch oder schneidet ihn ab, denn ein Schlüssel darf nur einmal eingesetzt werden. Die Schlüsselnummer wird im Telegrammkopf, zusammen mit der Telegrammnummer und andern Dienstvermerken, offen übermittelt, sie ist nicht geheim. Bei dieser Liste sind die zukünftigen Schlüssel einsehbar, ein Spion oder ein ungetreuer Chiffreur könnte sie fotografieren oder abschreiben und weitergeben. Um die Schlüssel vor neugierigen Augen zu verbergen, kam man auf die Idee, zehn Schlüssel auf ein Blatt zu drucken. Die einzelnen Schlüssel auf dem Blatt sind mit einer Perforation versehen, so dass sie einzeln abgetrennt werden können. Eine

grössere Anzahl solcher Schlüsselblätter ist – mit den aufgedruckten Schlüsseln nach unten – zu einem Block zusammengeheftet. Auf der Rückseite tragen die Schlüsselzettel die Schlüsselnummer, nur diese ist sichtbar, nicht jedoch die zehn Buchstaben des Schlüssels. Abb. 76 zeigt wie das im Prinzip aussieht. Der Block ist mit einem Sicherheitspapier eingefasst und auf der Rückseite gestempelt, siehe Abb. 77. Die Heftklammern liegen natürlich unter der Einfassung. Der Block ist "plombiert", er kann nicht ohne Zerstörung der Sicherheitselemente auseinander genommen werden. Die Zettelchen werden erst bei Bedarf aus dem Block herausgetrennt, dann erst wird der Schlüssel sichtbar. Dieses Verfahren wurde beim Botschaftsfunk angewandt.

Der innere Schlüssel wurde nicht für jedes Telegramm neu eingestellt; das wäre zu aufwändig gewesen, und aus kryptologischer Sicht auch nicht notwendig. Er wurde nach einem starren Zeitplan geändert. Beim Botschaftsfunk hatte er meist eine Gültigkeitsdauer, während der etwa hundert Telegramme bearbeitet wurden. Auch die Angaben für den inneren Schlüssel sind in einer Liste aufgeführt, die ähnlich aussah wie der Block nach Abb. 75. Anstelle der Nummer war ein Gültigkeitsdatum oder eine Gültigkeitsperiode angegeben, z. B. 2. APRIL 1972 oder JAN. - MAERZ 73. Wenn man sicher gehen wollte, dass diese Schlüsselangabe nicht eingesehen und verraten werden konnten, wurde auch in diesem Fall das Prinzip des "plombierten Blocks" angewandt. An Stelle der Schlüsselnummer war der Gültigkeits-Zeitraum aufgedruckt, siehe Abb. 79.

00	D	I	I	D	U	Z	D	H	T	H
01	K	D	Z	T	T	U	F	H	J	J
02	V	N	D	Z	D	K	Z	U	F	Z
03	S	O	R	I	J	F	J	J	R	U
04	E	I	D	D	K	E	U	D	J	R
05	E	N	S	H	E	U	D	J	S	D
06	L	L	T	Z	B	U	E	E	F	A
07	E	X	E	R	T	D	U	D	E	L
08	A	N	M	I	U	U	U	B	Q	P
09	T	E	R	L	I	H	H	U	Q	T
10	B	W	V	Y	D	Y	D	A	Z	I
11	C	F	G	I	W	H	Z	W	V	W
12	L	H	B	D	S	M	J	Q	D	H
13	O	K	U	V	L	P	A	G	L	E
14	D	G	H	T	G	F	Q	L	Z	Z
15	C	H	A	L	O	G	I	D	A	N

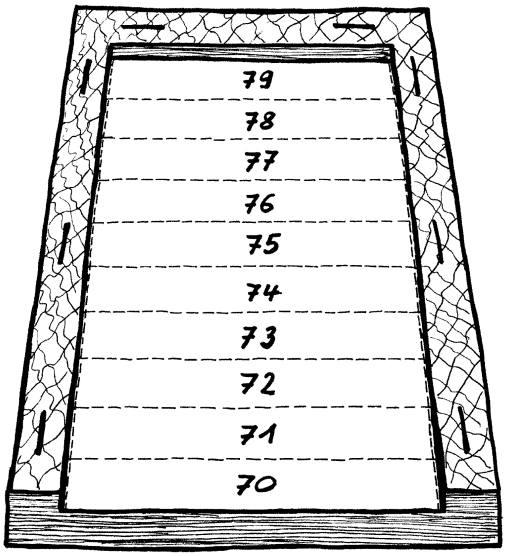
75 So könnte eine Liste mit (äusseren) Schlüsseln aussehen. [AUT]

Maschenförmiges Netz

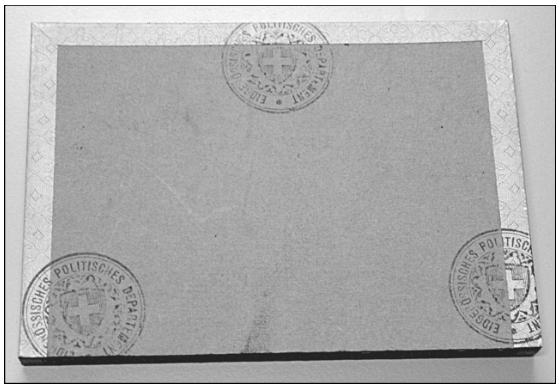
Bei dieser Netzform sind Querverbindungen zwischen den Aussenstationen zulässig. Jetzt funktioniert die Methode mit den Schlüssellisten nicht mehr, es sei denn man hätte für jede mögliche Querverbindung separate Listen. Aber das Problem der Rundschreiben, also das Verschicken der gleiche Meldung an mehrere Stationen, kann auch in diesem Fall nicht mit Schlüssellisten gelöst werden. In einem solchen Fall müsste der gleiche Klartext mit verschiedenen Schlüsseln chiffriert werden. Aus Sicherheitsgründen will man das möglichst vermeiden.

Es gibt eine elegante Methode um dieses Problem zu lösen. Sie erscheint auf den ersten Blick etwas kompliziert und unübersichtlich, dafür ist sie sicher. Es ist das Vorgehen, nach dem auch die Deutschen im Krieg mit der Enigma arbeiteten. Am Beispiel der Enigma und der Nema sehen wir uns an, wie dabei vorgegangen wurde.

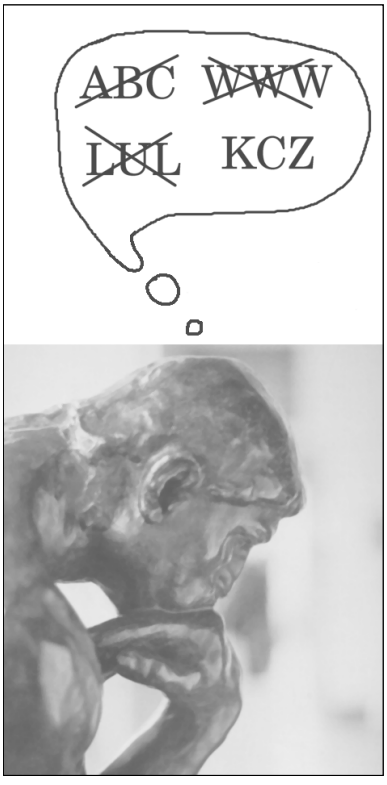
Eine Liste mit individuellen Schlüsseln brauchen wir nicht mehr, dafür einen Tagesschlüssel. Wie schon der Name sagt, handelt es sich um einen Schlüssel, der während eines ganzen Tages für alle Stationen im Netz gültig ist. Er kann aber auch eine Gültigkeitsdauer von mehreren Tagen oder nur von Stunden haben, oder für eine Aktion unbestimmter Dauer gelten; er wird trotzdem Tagesschlüssel genannt. Die Tageschlüssel müssen auf den Stationen für einen längeren Zeitraum vorrätig sein.



76 Aus dem Schlüsselblock werden die einzelnen Schlüsselzettelchen herausgetrennt, sie sind mit einer Perforation versehen. [AUT]



77 Die Rückseite eines Schlüsselblocks. Der Block kann nicht geöffnet werden, ohne das Sicherheitspapier und die Stempel zu zerstören, er ist plombiert. [AUT]



78 Bei der Enigma denkt sich der Chiffreur einen beliebigen dreistelligen Schlüssel aus. [Rodin] [AUT]

Chiffrieren mit der Enigma

- An der Maschine wird der Tagesschlüssel eingestellt. Dieser besteht aus den Angaben für den inneren und den äusseren Schlüssel, sowie den Verbindungen auf dem Steckerbrett.
- Der Chiffreur denkt sich drei beliebige Buchstaben aus, seinen "persönlichen Schlüssel", z. B. KCZ, siehe Abb. 78. Er muss darauf achten, dass er für jedes Telegramm eine andere, wirklich zufällige und sinn-lose Kombination verwendet.
- Diese drei Buchstaben chiffriert er, indem er sie zweimal hintereinander in die auf den Tagesschlüssel eingestellte Maschine eingibt. Er gibt ein: KCZKCZ und erhält als Geheimtext sechs Buchstaben, z. B.: PDFRFC.
- Diese sechs Buchstaben schreibt er als Anfang auf das Geheimtextblatt, das der Funker später der Gegenstation oder den Gegenstationen übermitteln wird.
- Der Chiffreur stellt auf der Maschine "seinen" Schlüssel ein (KCZ), das ist der so genannte Spruchschlüs-sel. Am inneren Schlüssel und an den Verbindungen auf dem Steckerbrett ändert er nichts, es gelten nach wie vor die Angaben des Tagesschlüssels.
- Das Telegramm wird mit dieser neuen Einstellung chiffriert, der erhaltene Geheimtext wird nahtlos an die bereits vorhandenen sechs Buchstaben angefügt, das eigentliche Telegramm beginnt also erst ab dem siebten Zeichen. Der Funker übermittelt das ganze Telegramm ab dem ersten Zeichen.

Das Telegramm besteht demnach aus zwei mit unterschiedlichen Schlüsseln chiffrierten Teilen. Der erste ist sechs Zeichen lang und enthält den verdoppelten und mit dem Tagesschlüssel chiffrierten Spruchschlüssel. Der zweite Teil hat eine variable Länge und enthält den mit dem Spruchschlüssel chiffrierten Klartext. Für den Funker ist alles zusammen ein Telegramm. Es interessiert ihn nicht, dass die ersten sechs Buchstaben etwas mit der Schlüsselübermittlung zu tun haben, das kann er auch nicht erkennen.

Der Empfänger des Telegramms führt zum Dechiffrieren folgende Schritte aus:

- Er stellt die Maschine auf den Tagesschlüssel ein.
- Mit dieser Einstellung entschlüsselt er die ersten sechs Buchstaben des Telegramms (PDFRFC).
- Er muss den doppelten Spruchschlüssel erhalten. In unserem Beispiel sind es die beiden identische Dreiergruppen (KCZKCZ). Falls nicht zwei gleiche Grup-pen erhalten werden, liegt ein Übermittlungsfehler vor.
- Den aus der Maschine erhaltenen Spruchschlüssel (KCZ) stellt er auf der Maschine ein.
- Mit dieser Einstellung dechiffriert er das Telegramm, beginnend beim siebten Zeichen, dort beginnt das eigentliche Telegramm.

Chiffrieren mit der Nema

Das Vorgehen bei der Nema ist im Prinzip gleich wie bei der Enigma: Der Spruchschlüssel wird mit dem Tagesschlüssel chiffriert und als Vorspann zum eigentlichen Telegramm übermittelt. Zwischen dem Arbeiten beim Militär und im Botschaftsfunk gab es Unterschiede. Hier zuerst die Version des Militärs:

- An der Maschine wird der Tagesschlüssel eingestellt (innerer und äusserer Schlüssel).
- Der Chiffreur denkt sich einen zufälligen Schlüssel aus, bestehend aus zehn Buchstaben oder zwei Fünfergruppen, beispielsweise: EXTER SNHIK.
- Diese schreibt er in dieser Form, also nicht verschlüsselt, als die beiden ersten Fünfergruppen auf das Geheimtextblatt: EXTER SNHIK.
- Diese zehn Buchstaben chiffriert er mit dem Tagesschlüssel und erhält den Spruchschlüssel, dieser könnte z.B. lauten: KKVTOBUQLE.
- Den Spruchschlüssel stellt er an der Maschine ein. Der innere Schlüssel bleibt so, wie er eingestellt ist. Das Telegramm wird mit dieser neuen Einstellung chiffriert. Der erzeugte Geheimtext wird an die beiden bereits vorhandenen Fünfergruppen angefügt. Am Schluss des Telegramms werden die beiden ausgedachten Gruppen (EXTER SNHIK) nochmals hingesetzt. Auch hier wird alles, ab der ersten Gruppe übermittelt.

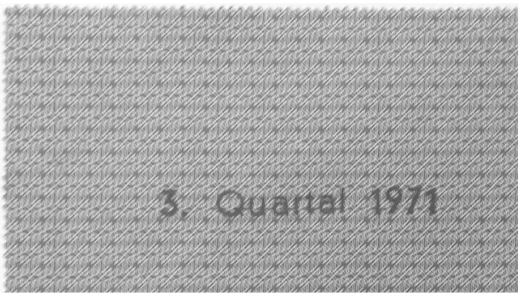
Zum Dechiffrieren führt der Empfänger die folgenden Schritte aus:

- Er stellt die Maschine auf den Tagesschlüssel ein.
- Damit bearbeitet er die ersten zehn Buchstaben des Geheimtextes (EXTER SNHIK) und erhält den Spruchschlüssel, in unserem Beispiel wieder die erwartete Folge: KKVTOBUQLE.
- Damit wird das Telegramm dechiffriert, beginnend ab der dritten Gruppe oder dem elften Zeichen. Die beiden letzten Gruppen werden ignoriert, sie enthalten nur redundante Information.

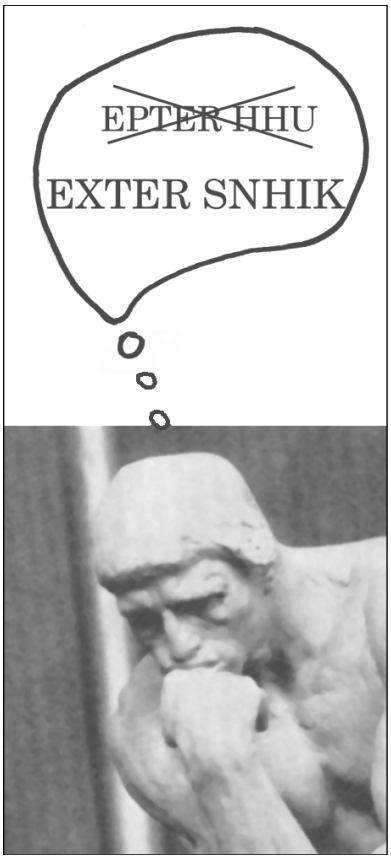
Soweit die Theorie, wie sie in der Schlüsselvorschrift, Abb. 82, beschrieben ist. In Tat und Wahrheit kam im Militär ein "abgekürztes" oder vereinfachtes Verfahren zum Einsatz: Alle Telegramme wurden direkt mit dem Tagesschlüssel chiffriert! Aus kryptologischer Sicht – wohlwollend ausgedrückt – ein zweifelhaftes Vorgehen.

Warum man nach dieser sonderbaren Methode gearbeitet hat und ob das generell bei allen Truppenverbänden der Fall war, ist mir nicht bekannt. Meine persönlichen Erfahrungen dazu: 1964 wurde dieses abgekürzte Verfahren in der Rekrutenschule instruiert. In den folgenden zwanzig Jahren habe ich Kurse bei verschiedenen Übermittlungskompanien absolviert; immer hatte man nach dem abgekürzten Verfahren gearbeitet. Während dieser Zeit wurde die Nema jedoch nur noch von der Funkpolizei im Notfunknetz eingesetzt, der reguläre Telegrammverkehr lief schon seit Jahren über den Krypto-Funk-Fernschreiber (KFF). Vielleicht liegt da die Erklärung: Niemand dachte daran, die Nema bei einem Ernstfall je einzusetzen.

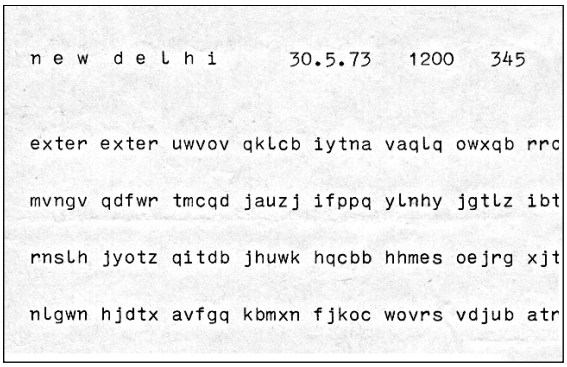
Wenn beim **Botschaftsfunk** in speziellen Fällen nach dem "Tagesschlüsselverfahren" gearbeitet werden musste, geschah das wie folgt:



79 Die inneren Schlüssel sind auf den Blättern eines Blocks aufgedruckt, nur die Rückseite mit der Gültigkeitsangabe ist sichtbar. Das Prinzip ist ähnlich wie bei der Abb. 76 mit dem Block für die äusseren Schlüssel. [AUT]



80 Bei der Nema denkt sich der Chiffreur einen zehnstelligen Schlüssel aus, es soll eine sinnlose Buchstabenkombination sein. [Rodin] [AUT]


n e w d e l h i 30.5.73 1200 345

exter exter uwvov qklcb iytna vaqlq owxqb rrc

mvngv qdfwr tmcqd jauzj ifppq ylnhy jgtlz ibt

rnslh jyotz qitdb jhuwk hqcbb hhmes oejrg xjt

nlgwn hjdtx avfgq kbmxn fjkoc wovrs vdjub atr

81 Der Anfang eines realen Botschafts-Telegramms. Am Anfang die beiden identischen Gruppen. Die eigentliche Meldung beginnt mit "uwvov qklcb iytna ..." Das Telegramm wurde an zwei Stationen abgeschickt, darum musste nach dem Tagesschlüssel-Verfahren gearbeitet werden. Mit Einmalschlüsseln wäre das nicht möglich gewesen. [AUT]

- Der innere und äussere Schlüssel wird gemäss dem Tagesschlüssel eingestellt.
- Der Funker denkt sich eine zufällige Fünfergruppe aus, z.B. EXTER, diese setzt er zweimal hintereinander und erhält einen zehnstelligen Schlüssel.
- Diese zwei Gruppen schreibt er als die beiden ersten Fünfergruppen auf das Geheimtextblatt: EXTER EXTER, siehe Abb. 81.
- Er chiffriert diese zehn Buchstaben und erhält den Spruchschlüssel, z.B. KKVTOCVRMF.
- Diesen stellt er an der Maschine ein, der innere Schlüssel bleibt unverändert. Das Telegramm wird mit dieser Einstellung chiffriert. Der erzeugte Geheimtext wird an die beiden bereits vorhandenen Fünfergruppen angefügt. Am Schluss des Telegramms müssen die beiden ersten Gruppen nicht wiederholt werden, wir werden gleich sehen, warum nicht.

Das Dechiffrieren geschieht auf analoge Weise: Zuerst aus den beiden ersten Gruppen im Telegramm und mit dem Tagesschlüssel den Spruchschlüssel gewinnen und damit das eigentliche Telegramm dechiffrieren.

Grundsätzliche Fragen

Widerspricht es nicht kryptologischen Grundsätzen, wenn die Spruchschlüssel von allen Stationen mit dem gleichen Tagesschlüssel chiffriert werden?

Nein, die Chiffreure haben die strikte Anweisung, als Spruchschlüssel rein zufällige, sinnlose und jedes Mal andere Buchstabenkombinationen zu wählen. Damit können die Kryptanalysten nichts anfangen.

Warum wird der Spruchschlüssel bei der Enigma zweimal chiffriert und bei der Nema zweimal übertragen, theoretisch würde doch einmal genügen?

Zu Zeiten der mechanischen Chiffriermaschinen wurden die Telegramme mit Morsetelegrafie übermittelt, Übermittlungsfehler konnten nie ausgeschlossen und auch nicht erkannt werden. Erhielt der Empfänger beim Dechiffrieren des doppelten Spruchschlüssels (gilt nur bei der Enigma) nicht zwei identische Gruppen, wusste er, dass ein Fehler vorlag. Er hatte dann zwei Möglichkeiten: Er konnte die ersten beiden Wörter (mit den sechs Buchstaben) beim Funkerkollegen nochmals anfordern und viel Zeit verlieren. Oder er probierte die Entschlüsselung mit den beiden unterschiedlichen Spruchschlüsseln aus, einer der beiden wird mit grösster Wahrscheinlichkeit fehlerfrei gewesen sein und sinnvollen Text geliefert haben.

Gleiches galt bei der Nema. Beim Militär wurden die zehn Buchstaben des chiffrierten Spruchschlüssels am Anfang und am Ende des Telegramms übermittelt, beim Botschaftsfunk nur am Anfang, aber hier bestand der Schlüssel aus zwei identischen Gruppen. Schon der Funker konnte eine Kontrolle vornehmen und gegebenenfalls rückfragen.

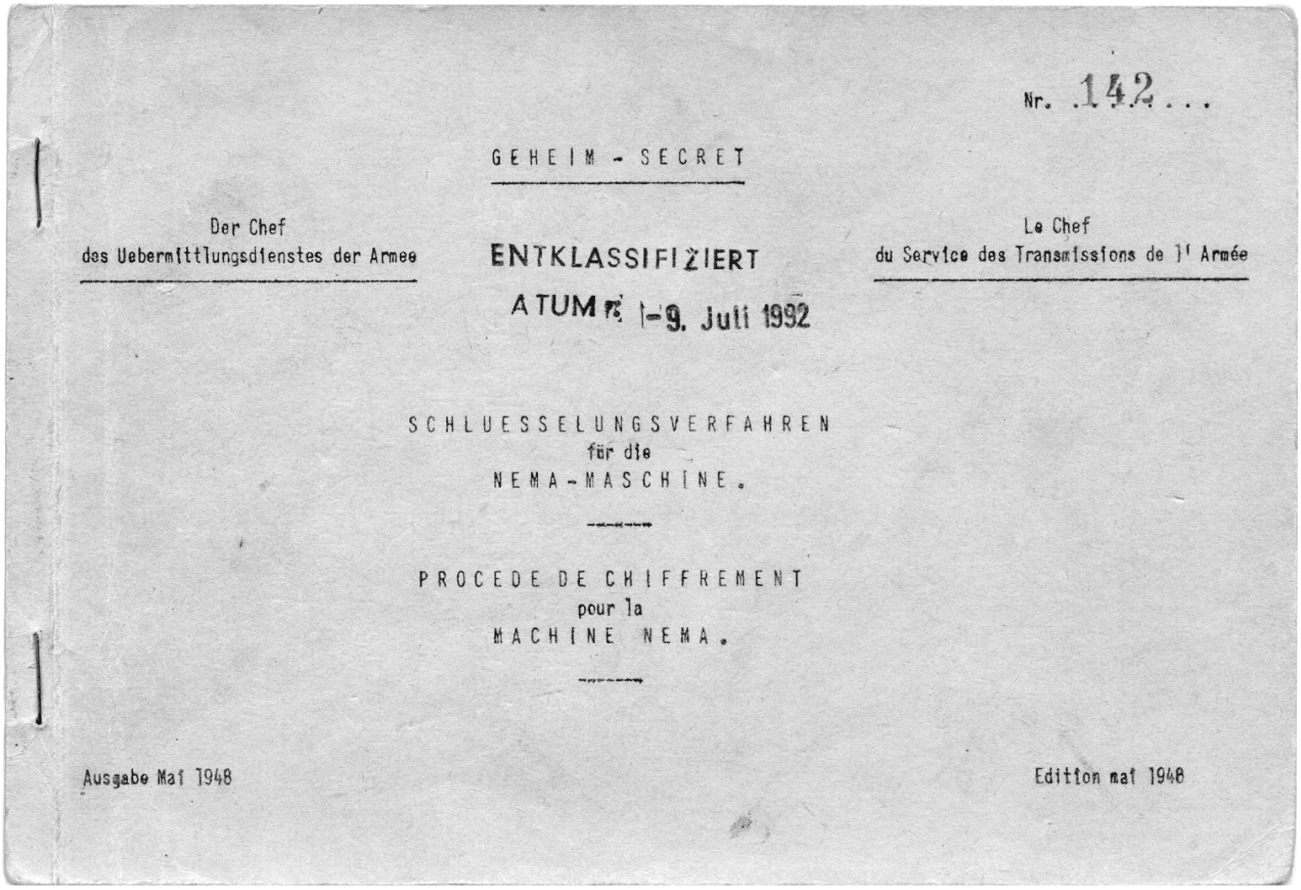
Man darf sich nicht verwirren lassen durch die Tatsache, dass bei der Nema der Schlüssel – wie es scheint – offen über-mittelt wird. Das Prinzip ist bei der Enigma und der Nema gleich. Die ausgedachten Schlüssel werden mit dem Tages-schlüssel bearbeitet. Man erhält zwei Teile, einer ist chiffriert, der andere nicht. Welchen Teil man als Spruchschlüssel ver-wendet und welchen man übermittelt

ist belanglos, es darf nur nicht in beiden Fällen derselbe sein! Man kann es bei der Nema auch so sehen: Der Chiffreur denkt sich einen chiff-rierten Schlüssel aus, den er seinem Kollegen übermittelt. Den Spruchschlüssel erhalten beide durch das Dechiffrieren mit dem Tagesschlüssel.

Die beiden Methoden, bei der Enigma und der Nema, sind von der Idee her gleich, aber doch in einem wesentlichen Punkt verschieden. Die Enigma-Methode hat eine Schwäche, die den Kryptanalysten beim Brechen einen Angriffspunkt bot, mehr dazu später.

Die Nema-Methode des Botschaftsfunks hatte den Vorteil, dass schon der Funker kontrollieren konnte, ob die ersten beiden Gruppen fehlerfrei waren. Wenn sie nicht identisch, waren, forderte er sie bei der Gegenstation sofort nochmals an. Eine zweite Person konnte mit dem Dechiffrieren sogleich beginnen. Bei der Militärmethode stellte sich erst am Schluss des Telegramms heraus, ob die beiden ersten Gruppen fehlerfrei empfangen wurden. Das wird den Chiffreur aber nicht davon abgehalten haben, mit dem Dechiffrieren zu beginnen. Wenn er keinen Erfolg hatte, musste er den Schluss des Telegramms abwarten, dann wurden die beiden Schlüsselgruppen nochmals übermittelt.

82 Die zweisprachige Schlüsselvorschrift für die Nema; sie umfasst 6 Seiten. Die Einstellung des Schlüssels nach den "Tagesschlüssel-Verfahren" wird hier beschrieben. [AUT]



Nr. 142...

GEHEIM - SECRET

Der Chef
des Uebermittlungsdienstes der Armee

ENTKLASSIFIZIERT
ATUM: 1-9. Juli 1992

Le Chef
du Service des Transmissions de l' Armée

SCHLUESSELUNGSVERFAHREN
für die
NEMA-MASCHINE.

PROCEDE DE CHIFFREMENT
pour la
MACHINE NEMA.

Ausgabe Mai 1948

Edition mai 1948

Jeder Text hinterlässt im Geheimtext seine statistischen Spuren, die nur der Zufall verwischen kann.

Brechen der Enigma

Schwachpunkte

Nach Ansicht von Fachleuten wäre die Enigma vom Prinzip her sicher gewesen, zumindest während ihrer Einsatzzeit, während der leistungsfähige Rechenmaschinen noch nicht zur Verfügung standen. Dass der Enigma-Code dennoch gebrochen wurde, hatte mehrere Gründe:

- Der Reflektor ist aus kryptologischer Sicht ein Schwachpunkt, ebenso das einfach durchschaubare Vorschubsystem. Beides geht zu Lasten der Erfinder der Maschine, Scherbius und Korn.
- Die beschriebene Schlüsselübermittlung stellt einen Schwachpunkt dar, sie bot den Kryptanalysten Angriffspunkte: Ein Fehler der Einsatzleitung.
- Bei der Wahl der Spruchschlüssel wurden elementare Regeln und Anweisungen missachtet, das waren Fehler oder Nachlässigkeiten der Chiffreure.



83 Marian Rejewski, ein polnischer Mathematiker, der beim Brechen der Enigma massgeblich beteiligt war. [13]

Die Stunde der Genies

Vor dem Zweiten Weltkrieg war die kommerzielle Enigma im Handel frei erhältlich. Sie war bei zivilen Unternehmen und bei Armeen im Einsatz, auch in der Schweiz wurde sie eingesetzt. Der Aufbau der Maschine war bekannt, ebenso deren Funktionsprinzip. Als die deutschen Militärs sich dazu entschlossen, die Enigma zum Chiffrieren zu verwenden, liessen sie neue Rotoren herstellen, mit anderer, streng geheimer Verdrahtung. Der Verkauf der Enigma an Private und andere Armeen wurde eingestellt. Durch Verrat und Zufall bekamen die Polen, ohne dass die Deutschen davon wussten, Informationen zu den aktuellen Enigma-Rotoren. Die genialen polnischen Mathematiker – zu nennen ist allen voran Marian Rejewski – erarbeiteten mathematische Modelle um die Chiffrierung zu berechnen. Dazu benötigten sie Kenntnisse über die Walzenverdrahtung und eine bestimmte Menge zusammengehörenden Klar- und Geheimtext. Zum Geheimtext kommt man problemlos, indem man den Funkverkehr abhört Aber wie kommt man zum dazu gehörenden Klartext? Hier half der Reflektor. Wir wissen, dass der Reflektor für die Eigenschaft verantwortlich ist, dass ein Buchstabe beim Chiffrieren nie in sich selbst überführt wird. Diese Eigenheit haben die Kryptanalysten ausgenutzt. Vermuteten sie in einem Telegramm eine möglichst lange Buchstabenfolge, so legten sie diese unter den abgefangenen Geheimtext und verschoben sie so lange, bis keine übereinander liegenden Buchstaben im Klar- und Geheimtext gleich waren, siehe Abb. 84. Nur an einer solchen Position konnte der vermutete Klartext im Geheimtext enthalten sein. Da hinterlässt der Reflektor seine Spuren! Auf diese Weise liessen sich Positionen finden, die für eine Geheimtext-Klartext-Kompromittierung in Frage kamen. Am besten gelang das bei kurzen Telegrammen mit langen stereotypen Buchstabenfolgen. Geeignet waren Wettermeldungen mit bekanntem Aufbau. Mit den möglichen Paarungen wurde probiert, bis sich ein Erfolg einstellte.

```
K E N T M B F Z A E T E D B W T S I M E T Z A C F O V Q H
W E T (T) E R B E R I C H T V O M
  W E (T) T E R B E R I C H T V O M
    W E T T E R B (E) R I C H T V O M
      W E T T E R B E R I C H (T) V O (M)
        W E T T E R B (E) R I C H T V O M
          W E T T (E) R B E R I C H T V O M
            W E T T E R B E R I C H T V O M < möglich
              W E T (T) (E) R (B) E R I C H T V O M
                W (E) (T) T E R B E R (I) C H (T) V O M
                  W E T T E R B E R I C H T V O M < möglich
                    W (E) T T E R B E R I C H T V O M
                      W E T T E R B E R I C H T V (O) M
```

84 Der vermutete Klartext wird unter den Geheimtext gelegt und schrittweise nach rechts verschoben. Die Kreise markieren gleiche Buchstaben bei Geheim- und Klartext. Nur bei zwei Positionen ("möglich") gibt es keine Übereinstimung, dort kann der Klartext im Geheimtext enthalten sein. [AUT]

Bletchley Park

Während des Zweiten Weltkriegs wurde die Enigma von den Briten auf der Basis der vorgestellten Methode systematisch gebrochen. Ein Genie, Alain Turing, Abb. 85,

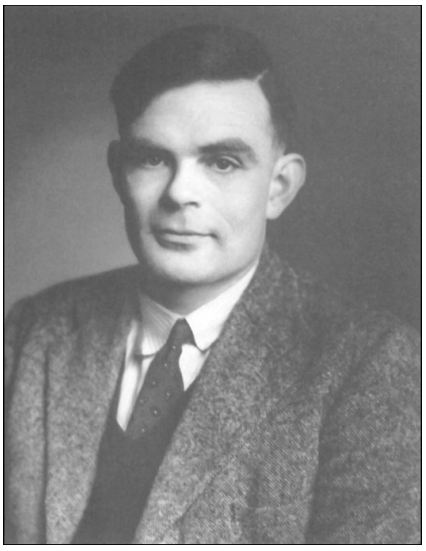
leistete dabei Pionierarbeit. In Bletchley Park, nördlich von London, waren viele tausend Personen damit beschäftigt, die feindlichen Funksprüche abzuhören, zu dechiffrieren und zu übersetzen, Abb. 86. Zuerst musste immer der aktuelle Tagesschlüssel gewonnen werden. Dazu verwendete man spezielle Maschinen, Bombas oder Bomben genannt. Siehe Abb. 87. Diese Bombas waren elektromechanische Ungetüme, bestehend aus Motoren, Kontaktwalzen und Relais, die ein systematisches Probieren erlaubten. Man setzte diese Maschinen meist auf Wettermeldungen an, die trafen früh am Tag ein, waren relativ kurz und, was von grosser Bedeutung war – von bekanntem Aufbau.

Einen weiteren Ansatzpunkt beim Brechen des Enigma-Codes boten die ersten sechs Buchstaben der Telegramme, die den chiffrierten Spruchschlüssel enthielten. Man wusste durch Verrat, dass diese sechs Buchstaben im Klartext zwei identische Gruppen darstellten. Der erste und vierte, der zweite und fünfte, sowie der dritte und sechste Buchstabe im Geheimtext waren beim Klartext identisch. Wegen des Reflektors wusste man, welche Klartext-Buchstaben nicht in Frage kamen. (Erinnern wir uns an die Nema-Methode beim Botschaftsfunk, da wurden die beiden identischen Gruppen offen übertragen, da gab es nichts zu verraten!) Zudem wurde beim Chiffrieren dieser sechs Buchstaben mit einer Wahrscheinlichkeit von 77 % (20/26) nur der erste Rotor bewegt, die beiden andern blieben stehen. Die Bombas wurden mit all diesen Informationen gefüttert. Sie lieferten als Resultat, die Anfangsstellung der Rotoren, die Belegung des Steckerbretts und den inneren Schlüssel. Die Rotorverdrahtungen musste den Bombas bekannt sein. Sobald der Tagesschlüssel gefunden war, konnten die Telegramme ohne Verzug mitgelesen werden. Es war deshalb wichtig, dass der Tagesschlüssel nach einem Wechsel möglichst schnell gebrochen werden konnte.

Der dritte Angriffspunkt lag bei den ausgedachten Spruchschlüsseln. Einzelne Chiffreure benutzten – entgegen der klaren Vorschrift – ständig die gleichen drei Buchstaben. Andere wiederum wandten eine stupide und offensichtliche Systematik an. Beides blieb den gegnerischen Kryptanalysten nicht verborgen und lieferte ihnen wertvolle Angriffspunkte beim Brechen.

Im Nachhinein weiss man, dass die Verwendung des von Willi Korn erfundenen Reflektors in der Maschine von Arthur Scherbius eine wesentliche Reduktion der Sicherheit zur Folge hatte. Der Reflektor ist bei jeder Rotormaschine die entscheidende Schwachstelle.

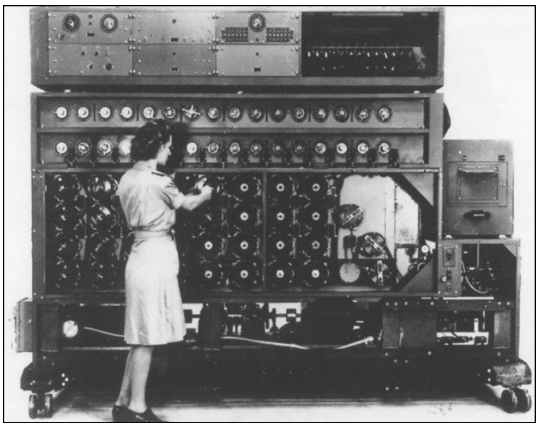
In verschiedenen Quellen äussern Fachleute die Meinung, dass durch das Brechen des Enigma-Codes der Verlauf des Zweiten Weltkriegs entscheidend beeinflusst worden sei. Kritisch war die Situation, als die Enigmas der deutschen U -Boote mit dem vierten Rotor ausgerüstet wurden. Es dauerte Monate, bis man in Bletchley Park die Bombas den neuen Verhältnissen angepasst hatte und wieder Erfolge beim Brechen verbuchen konnte. Im Roman "Enigma" [3] werden die Vorgänge in und um Bletchley Park eindrücklich beschrieben.



85 Alain Turing, englisches Mathematik-Genie und Urvater des modernen Computers. [13]



86 Bletchley Park, ein Landsitz nördlich von London. Er wurde im Laufe der Zeit mit Baracken erweitert. [16]



87 Bombas oder Bomben wurden zum Brechen des Enigma-Codes eingesetzt. [16]

Der gegnerische Kryptanalyst hat viel Geduld, er wartet bis in der Hektik Fehler und Nachlässigkeiten passieren.

Arbeiten mit der Nema

Vorsicht: Feind liest mit!

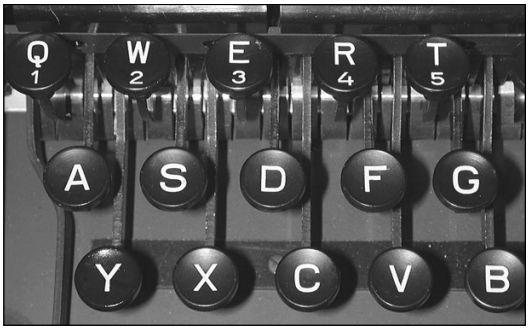
Wir wissen aus dem vorangegangenen Abschnitt, wie ein gegnerischer Kryptanalyst vorgehen wird um die Nema zu brechen: Er wird versuchen, bekannte oder vermutete Klartextpassagen dem Geheimtext zuzuordnen. Er will mit einer Geheimtext-Klartext-Gegenüberstellung in die Nema-Chiffrierung einbrechen. Da auch die Nema mit einem Reflektor ausgerüstet ist, wissen wir, wo dieser seine Spuren hinterlässt, und wie der Kryptanalyst seine Werkzeuge einsetzen wird. Der Gegner hat es nicht einfach, aber er hat Geduld und wartet, bis Fehler oder Nachlässigkeiten passieren, dann schlägt er zu. Die Chiffreure ihrerseits versuchen, diese Angriffe durch geeignete Massnahmen und mit Disziplin zu vereiteln.

Bescheidener Zeichensatz

Sicher ist Ihnen schon aufgefallen, dass wir immer nur von Buchstaben gesprochen haben, die eingestellt und chiffriert werden. Jeder Text enthält aber auch:

- Klein- und Grossbuchstaben
- Umlaute, Spezialzeichen
- Interpunktionszeichen
- Wortzwischenräume
- Ziffern

Es ist tatsächlich so: Wir finden bei der Nema-Tastatur nur die 26 Buchstaben des Alphabets. Eine Unterscheidung zwischen Gross- und Kleinschreibung gibt es nicht. Damit könnte man leben, denn beim Morsecode ist das auch so, ebenfalls beim Fernschreiber. Gleiches zum Thema "Zeichensatz" gilt übrigens auch für die Enigma.



88 Die obere Tastenreihe ist bei der Nema mit Zahlen und Buchstaben beschriftet. [AUT]

Nur die 26 Buchstabentasten sind beim Chiffrieren aktiv und bewirken einen Walzenvorschub und das Aufleuchten eines Lämpchens. Einige der Tasten sind blockiert, andere betätigen lediglich Kontakte, die man für die Steuerung von Zusatzgeräten vorsah. Diese Kontakte sind an den Stecker, Abb. 57 (16) geführt, siehe auch Abb. 152 und 153.

Für das Chiffrieren von Ziffern kennt man bei der Nema ein spezielles Vorgehen: Man kann von der normalen Buchstabenebene in eine virtuelle – also eine gedachte – Ziffernebene umschalten. Befindet man sich in dieser, benutzt man nur die Tasten der oberen Reihe "Q W E ... O P". Diese stehen stellvertretend für die Ziffern "1 2 3 ... 9 0". Aus diesem Grund sind bei der Nema die Tasten in der oberen Reihe sowohl mit Buchstaben als auch mit Ziffern beschriftet, siehe Abb. 88. Wie wird nun umgeschaltet? Es handelt sich nicht um eine mechanische Umschaltung, wie wir sie bei der Schreibmaschine kennen, sondern um eine reine Absprache. Es wird vereinbart, dass mit dem Buchstaben 'Y' in die Ziffernebene geschaltet wird und mit 'X' wieder zurück zu den Buchstaben. Diese Umschalt-Buchstaben werden dem Klartext zugesetzt und mitchiffriert! Bevor der Chiffreur eine oder mehrere Zahlen eingibt, drückt er die Taste 'Y' und dann auf der oberen Tastenreihe die entsprechenden Ziffern. Folgte ein Komma, muss er zuerst die Zahlen-ebene mit 'X‘ verlassen und das Komma als Wort (KOMMA) eingeben. Dann mit 'Y' wieder zurück zur Zahlenebene (Ge-mäss 3.d des Schlüsselungsverfahrens für

die Nema-Maschine, Abb. 82). Es war natürlich erlaubt, die Ziffern als Worte auszu-schreiben. Bei der Enigma wurde das beschriebene Verfahren nicht angewandt, da arbeitete man nur mit Zahlwörtern.

Was passiert, wenn man in der "Ziffernebene" eine Taste der mittleren oder unteren Reihe drücke?

Nichts Besonderes, das ist natürlich möglich. Ein Lämpchen wird aufleuchten und die Walzen schalten weiter. Die Nema "weiss" nicht, dass wir uns in der Ziffernebene befinden, für sie gibt es die gar nicht! Aber der Kollege auf der Gegenstation bekommt Probleme, er kann mit diesem Zeichen nichts anfangen und wird eine Rückfrage machen.

Führen diese eingefügten 'X' und 'Y' nicht zu Missverständnissen, schliesslich kommen 'X' und 'Y' als ganz normale Buchstaben im Text vor?

Nein, Missverständnisse darf es nicht geben, weil jetzt eine wichtige Regel der Chiffreure Anwendung findet:

Ein dechiffrierter Bandwurm könnte so aussehen:

```
Der Chiffreur denkt mit, er vermeidet Missverständnisse, indem er
sich überlegt, wie er den Text dechiffrieren würde.
```

Daraus extrahiert der Chiffreur:

...Besammlung bei Punkt Yvonne 8 exakt um 18 Uhr.

```
...BESAMMLUNGBEIPUNKTYVONNEYIXEXAKTUMYQIXUHRSTOP...
```

gemeint ist. Aber hier hätte der Chiffreur tatsächlich besser "ACHT" geschrieben statt "YIX".

Für den Wortzwischenraum kennt man kein Zeichen, man sollte aus Sicherheitsgründen dafür auch keines verwenden. Notfalls kann man mit YX ein Trennzeichen erzwingen. Bei fremdsprachigen Namen kann das unumgänglich sein. Das Vorgehen muss auf jeden Fall unter den Stationen abgesprochen werden. Das wichtigste Interpunktionszeichen, der Punkt, wird normalerweise als "STOP" ausgeschrieben. Für alle anderen Satzzeichen kennt man keine allgemein gültige Abkürzung. Es steht den Beteiligten jedoch frei, eigene Absprachen zu treffen. Es muss aber sichergestellt sein, dass alle davon Kenntnis haben und damit umzugehen wissen.

Abmachungen

- Der Chiffreur darf am Text des Telegramms nichts ändern. Wichtige Interpunktionszeichen sind als Worte zu chiffrieren, so wie es bei einem Diktat auch gemacht wird, z.B. , QUERSTRICH, ABSATZ, KLAMMERAUF, KLAMMERZU, FRAGEZEICHEN, DOPPELPUNKT, usw. Es hilft dem Kollegen beim Dechiffrieren, wenn er möglichst grosszügig solche Anweisungen erhält. Er wird diese natürlich nicht in ausgeschriebener Form weitergeben, sondern ihrem Sinn entsprechend anwenden. Die Behandlung von Ziffern und Zahlen haben wir schon besprochen.

ANNNKUNFTDERDELEGATIONMITF
LUGYXAIYXDREEEIZWEIFUENFAMD
ONNERSTAGZWEIZWEISSSEPTEMB
ERSTOPABBBHOLENAMFLUGPLAT
ZZZWIEVEREINBARTSTOOOPBALT
ENSWEILERSTOPYREEXSTOPTFM

89 Es braucht etwas Übung um den Klartextwurm zu entziffern. Man erkennt Buchstabenverdreifachungen, am Schluss den Code 433 (YREEX). Mit YX werden Zwischenräume erzwungen. Die Buchstaben "TFM" am Schluss sind Füllbuchstaben, mit ihnen wird erreicht, dass die letzte Fünfergruppe komplett ist. [AUT]

LEONEORIGGGINALBERNKOPIEISL
AMABADSTOPDERPAKISTANISCHE
BOTSCCCHAFTERWIRDERSTAMZW
EIACHTJULIINDERBOTSCHCANEAF
TINNEWDELHHHIEINZUGHALTENST
OPSUTTERYEEWXSTOP

90 Dieser deutschsprachige Text enthält italienische Blender aus der Gruppe "Tiere", in der Realität sind diese natürlich nicht unterstrichen. Daneben findet man noch Buchstabenverdreifachungen und am Ende des Telegramms den Code "332" (YEEWX). [AUT]

- Wenn immer möglich werden Ziffern mit Wörtern ausgeschrieben, statt mit der Ziffernebene zu arbeiten. Ein fehlerhafter Buchstabe kann bei einem Wort in der Regel verkraftet werden, nicht aber in der Ziffernebene. Zeitraubende Rückfragen lassen sich vermeiden.
- Der Geheimtextwurm wird nach dem Chiffrieren in Fünfergruppen aufgeteilt, das ist international so gebräuchlich. Man bezeichnet eine Fünfergruppe als Wort, zehn Wörter bilden eine Zeile, das erleichtert die Übersicht und hilft dem Funker bei der Übermittlung.
- Wenn beim Chiffrieren der Text nicht mit einer vollen Fünfergruppe endet, ergänzt man im Klartext mit beliebigen, sinnlosen Buchstaben. Maximal müssen vier Buchstaben zugesetzt werden. Das eigentliche Ende des Telegramms wird, wenn es nicht offensichtlich ist, am "STOP" erkannt. Das galt beim Botschaftsfunk, beim Militär waren angebrochene Gruppen zulässig.

Aus Fehlern lernen

Ein Gegner sucht im Geheimtext nach vermuteten und möglichst langen Klartextpassagen. Aus der Presse hat er vielleicht erfahren, dass ein HERRBUNDESPRAESIDENT LEUENBERGER nach Delhi reist. Kurz vor dem Reisetermin hört ein gegnerischer Geheimdienst ein Telegramm ab, das von Bern nach Delhi übermittelt wird. Er vermutet, dass darin obige Textpassage ziemlich am Anfang vorkommt; nach dieser wird er suchen. Es ist die Aufgabe des Chiffreurs, dafür zu sorgen, dass Buchstabenfolgen dieser Länge und Einmaligkeit nicht vorkommen. Er sorgt auch dafür, dass der typische Aufbau des Telegramms zerstört wird. Dazu stehen ihm mehrere Mittel zur Verfügung, die er in eigener Kompetenz einsetzt.

Verschiedene Sicherheitsvorkehrungen

Der Einsatz der nachfolgend vorgestellten Massnahmen war beim Botschaftsfunk reglementiert. Nicht alle wurden bei jedem Telegramm gleichzeitig eingesetzt, die Umstände waren Ausschlag gebend, die Entscheidung lag beim Chiffreur. Bei den militärischen Einsätzen der Nema wurden keine dieser Sicherheitsvorkehrungen angewandt.

- Der Chiffreur verdreifacht beliebige Buchstaben, er macht bewusst Fehler, das führt zur Zerstörung des Zusammenhangs Klartext – Geheimtext. Er chiffriert: HHHERRBUNDDDESPRAESIDENTLLLEUENBERGER. Damit bekommt der Gegner schon einige Probleme. Der Funkerkollege auf der Gegenstation wird den Text ohne mit der Wimper zu zucken richtig weitergeben. Weder der Absender noch der Empfänger der Nachricht haben eine Ahnung davon, was sich beim Chiffrieren Eigenartiges zugetragen hat; sie sollen es auch nicht wissen! Selbst der Chiffreur weiss im Nachhinein nicht mehr, wie er chiffriert hat. Die Verdreifachung von Buchstaben nimmt er spontan vor, ohne Notizen zu hinterlassen. Als Regel galt, dass man pro Zeile ein bis zwei Verdreifachungen vornahm.
- Das Telegramm kann mit Wörtern einer textfremden Sprache, mit sog. Blendern, angereichert werden, die natürlich mitchiffriert werden. Auch damit machen wir dem Gegner das Leben schwer. Blender dürfen auch am Anfang des Telegramms stehen! Zulässige Blender sind in einer Auswahlliste aufgeführt und gehörten – damit man sie besser erkennt – einer bestimmten Gruppe an, z. B.: Tiere, Bäume usw., siehe Abb. 90.

- Der Text wird in mehrere beliebig grosse Abschnitte aufgeteilt. Jeder Abschnitt wird am Anfang fortlaufend mit einem sprachfremden Zahlwort versehen. Die Teilstücke werden in ungeordneter Reihenfolge chiffriert, jedes beginnend mit seinem Zahlwort. Das kann dann so aussehen wie Abb. 91 als Beispiel zeigt. Mit diesem Vorgehen wird erreicht, dass der Anfang und das Ende des Telegramms "nach innen geklappt" werden.
- Das typische Aussehen eines Telegramms mit Kopf- und End-Floskeln wird zerstört, indem man häufig vorkommende Passagen wie: "Ihr Telegramm vom ..." oder "Original an ..., Kopie an ..." usw. durch einen Code (dreistellige Zahl) ersetzt, den man an abgesprochener Stelle im Telegramm einfügt.

TWOUNDWIRDBEGEITETVONDENH
ERRENBALTENSWEILERUNDMUELL
ERDERFIRMA...ONEANKUNFTHERR
BUNDESRATAUBERTAUFDENMITT
WOCHVERSCHOBEN...FOURUMGE
HENDIHREANTWORTSTOPHUBERS
TOPYWTRXSTOPDETHREENACHDE
MBESUCHBEIMAUSSENMINISTERIS
TTREFFENGEPLANTMIT...

91 Aufteilung eines Telegramms in Abschnitte, in diesem Beispiel sind es deren vier. Das Telegramm endet vor THREE mit den beiden Füllbuchstaben 'DE'. [AUT]

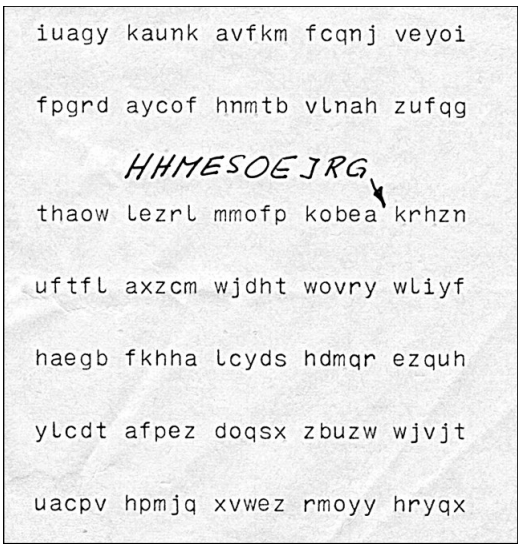
Wichtige Regeln

Das gleiche Telegramm darf niemals eins zu eins mit zwei verschiedenen Schlüsseln chiffriert werden. Muss der gleiche Text an zwei Empfänger geschickt werden, wird das Telegramm, wie zuvor beschrieben, in verschiedene Abschnitte aufgeteilt. Diese sind in unterschiedlicher Reihenfolge zu chiffrieren. Auch die andern beschriebenen Massnahmen sind in diesem Fall grosszügig anzuwenden!

Auf ein Klartexttelegramm wird nie chiffriert geantwortet, auf ein chiffriertes nie klar. Das gilt auch dann, wenn die Antwort nur "ja" oder "nein" lautet, denn oft folgt doch noch ein "aber" oder ein "weil".

Falsche Eingaben korrigieren

Man kann nie ausschliessen, dass beim Chiffrieren oder Dechiffrieren eine falsche Taste gedrückt wird. Im Grunde ist das nicht tragisch. Sofern der Fehler in normalem Text vorkommt, lässt er sich in der Regel erkennen und korrigieren. Auf die Weiterschaltung der Walzen und den nachfolgenden Text hat der Fehler keinen Einfluss. Solange die Taste noch niedergedrückt ist, kann eine Korrektur einfach vorgenommen werden: Man hält die falsche Taste weiterhin gedrückt, betätigt mit einem andern Finger die richtige Taste und lässt erst jetzt die falsche Taste los. Nun leuchtet das richtige Lämpchen. Wurde die Taste bereits losgelassen, kann der Fehler trotzdem noch korrigiert werden: Der rote Hebel an der Nema wird in die Stellung "Repetieren" gebracht und gleich wieder zurück auf "Betrieb" gestellt. Jetzt die richtige Taste drücken und den richtigen Buchstaben ablesen. Dieser zweite Tastendruck bewirkt keinen Vorschub der Walzen, auch das Zählwerk zeigt nach wie vor richtig an. Schwieriger wird es, wenn mehrere falsche Tasten gedrückt wurden, eine Korrektur ist dann nicht möglich. Da gibt es nur einen Weg: Nochmals von vorne beginnen! Die Sache lässt sich etwas vereinfachen, indem man bis zum Beginn der fehlerhaften Stelle immer die gleiche Taste drückt. Für den Walzenvorschub kommt das aufs gleiche heraus, aber es geht schneller. Diese Methode funktioniert beim Dechiffrieren immer, beim Chiffrieren nur dann, wenn keine Buchstaben-Verdreifachun-gen vorgenommen und keine Blender eingesetzt wurden. Der gewiefte Chiffreur setzt bei langen Texten, etwa alle zwei-hundert Wörter, eine Marke und schreibt die zugehörende Walzenstellung auf. Er notiert den aktuellen Schlüssel, siehe Abb. 92. Wenn dann etwas schief läuft, muss er nicht von vorne beginnen: Er stellt die Walzen auf die letzte notierte Position ein, und beginnt die Arbeit ab dort nochmals. Das funktioniert beim Dechiffrieren wie beim Chiffrieren. Der Zähler wird zwar



92 Ausschnitt aus einem sehr langen Telegramm. Der Chiffreur macht sich Schlüsselnotizen. [AUT]

nicht mehr richtig anzeigen, weil er nicht auf einen vorgegebenen Wert eingestellt werden kann, aber das ist weiter nicht so wichtig. Die Notizen mit solchen Schlüsselangaben sind zuverlässig zu vernichten!

Fehlerhaft empfangene Buchstaben bereiten beim Dechiffrieren im Normalfall keine Probleme, es leuchtet lediglich ein falsches Lämpchen auf. Die fehlerhaften Buchstaben sind meist offensichtlich und lassen sich korrigieren. Befindet man sich dagegen in der Ziffernebene, ist es schwieriger. Leuchtet das falsche Lämpchen in der oberen Reihe, kann man den Fehler nicht bemerken, leuchtet eines in der mittleren oder unteren Reihe, wird der Fehler erkannt, lässt sich aber nicht korrigieren. Deshalb nochmals der Rat: Nach Möglichkeit die Ziffern durch Zahlwörter ersetzen und nicht mit der Ziffernebene arbeiten; alles in allem geht das schneller, weil es weniger Rückfragen gibt!

Probleme treten beim Dechiffrieren auf, wenn eine Gruppe aus vier oder sechs Buchstaben besteht. Das sollte eigentlich nicht vorkommen, weil der Geheimtext in Fünfergruppen übermittelt wird. Ein fehlendes oder überzähliges Zeichen müsste dem Funker auffallen. Besteht trotzdem einmal eine Gruppe aus vier oder sechs Buchstaben, drückt man am Ende der Gruppe eine beliebige Taste oder lässt den überzähligen Buchstaben weg. Aus dem erhaltenen Klartext erahnt man, an welcher Position der fehlende oder überflüssige Buchstabe stehen kann. Ein so entstandener Fehler lässt sich in der Regel korrigieren, vorausgesetzt, man befindet sich nicht in der Ziffernebene. Etwas probieren geht in jedem Fall schneller, als eine Rückfrage vorzunehmen.

Fazit

Werden die vorgestellten Vorschriften und Ratschläge konsequent angewandt, kann man mit der Nema zuverlässig und sicher arbeiten. Es ist bekannt, wie die Maschine im Prinzip funktioniert, wo ihre Schwachpunkte liegen und was man gegen feindliche Angriffe vorkehren kann.

Die Geschichte der Enigma zeigt, dass Einbrüche in ein Chiffriersystem sehr oft auf Nachlässigkeiten und weniger auf Verrat beruhen. Aus diesem Grund hält sich der Chiffreur eisern an die Vorschriften, auch dann, wenn es hektisch zugeht. In Ausnahmefällen, z. B. unter aussergewöhnlichem Zeitdruck, ist es besser, ein Telegramm im Klartext zu übermitteln als nachlässig zu chiffrieren. Der Schaden ist im ersten Fall geringer und kann sich nicht fortpflanzen!

Ich möchte nochmals betonen, dass es wichtig ist, sich beim Chiffrieren in die Lage des Kollegen zu versetzen. Versteht er, was ich will, gibt es keine Missverständnisse? Wie würde ich vorgehen, wenn ich dieses Telegramm dechiffrieren müsste? Man sollte ausgeschriebene Anweisungen für den Kollegen grosszügig einsetzen, der Zeitaufwand ist gering, Rückfragen sind wesentlich zeitaufwändiger.

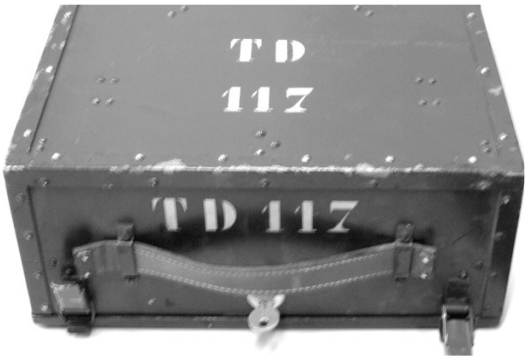
Nema gebrochen?

Nicht jeder Verrat geschieht mit Absicht, meist steckt Nachlässigkeit, Gedankenlosigkeit und Nichtwissen dahinter.

Wie stand es um die Sicherheit der Nema? Wurde sie auch systematisch gebrochen, so wie die Enigma? Wenn ja, von wem und wie? Diese Fragen lassen sich nicht ohne weiteres beantworten. Weder die Benutzer der Nema noch die gegnerischen Kryptanalysten haben ein Interesse daran, Einbrüche in den geheimen Funkverkehr an die grosse Glocke zu hängen. Die Gründe sind offensichtlich: Die Gegner wollen die Informationsquelle nicht versiegen lassen und die Anwender wollen sich nicht blamieren! Ich konnte nicht in Erfahrung bringen, wie es um die Sicherheit der Nema stand, an Hand der folgenden Überlegungen kann man Vermutungen anstellen:

- Wer hatte ein Interesse daran, den Nema-Code zu brechen? Das könnten militärische Stellen gewesen sein, viel lässt sich zwar im Funkverkehr kaum ausspionieren, da die Telegramme meist nur taktische Anweisungen enthalten. Es gibt effizientere Möglichkeiten, militärische Geheimnissen auszuhorchen als das Brechen von Telegrammen. Man kann annehmen, dass der Druck auf den militärischen Nema-Code nicht sehr gross war.
- Bis etwa 1976 wurde die Nema im Botschaftsdienst eingesetzt (Funk, Draht und Post). Wichtige Telegramme wurden mit ihr chiffriert. Die Telegramme des diplomatischen Dienstes haben eine viel länger dauernde Wirkung und eine grössere Brisanz als jene des Militärs. Bei fremden Nachrichtendiensten bestand daher sicher ein Interesse am Brechen des diplomatischen Nema-Codes.
- Dass die Nema im Botschaftsverkehr bis 1976 eingesetzt wurde, kann man als Indiz sehen, dass man keine Kenntnisse oder Vermutungen von Einbrüchen in die Verschlüsselung hatte. Wie die Geschichte zeigt (siehe Dokument Seite 66) tauschen Nachrichtendienste untereinander Informationen aus; in der Schweiz hätte man davon sicher Wind bekommen, wenn Einbrüchen in den Nema-Chiffrierung gelungen wären.
- Die Sicherheit der Nema beruhte auf drei Pfeilern:
  - Der Verdrahtung der Kontaktwalzen.
  - Der Form der Nocken- oder Zahnscheiben.
  - Dem inneren und äusseren Schlüssel.

  Alle drei Elemente ergeben eine extrem grosse Anzahl von Kombinationen. Für einen "brute force"-Angriff, einen Angriff mit roher Gewalt, bei welchem alle möglichen Kombinationen ausprobiert und analysiert werden, fehlten damals, bis in die 1970er-Jahre, die leistungsfähigen Rechner. Die Sicherheit der Maschinen war vermutlich gegeben.
- Im diplomatischen Netz waren knapp 100 Maschinen im Einsatz; sie waren immer in Panzerschränken unter Verschluss. Bedient wurden die Maschinen von einem sehr kleinen und zuverlässig überprüften Personenkreis. Es wurde hauptsächlich mit dem sicheren Einmal-Schlüssel gearbeitet. Für spezielle Zwecke, die das Tagesschlüssel-Verfahren erforderten, stand eine Maschine mit anderen Walzen zur Verfügung, siehe Abb. 94.
- Bei der Armee wurde die Nema von 1948 bis etwa 1959 als Chiffriergerät auf der Stufe Division - Armeecorps - Armeeleitung eingesetzt. Der Kreis der Nema-Chiffreure war bedeutend grösser als beim diplomatischen

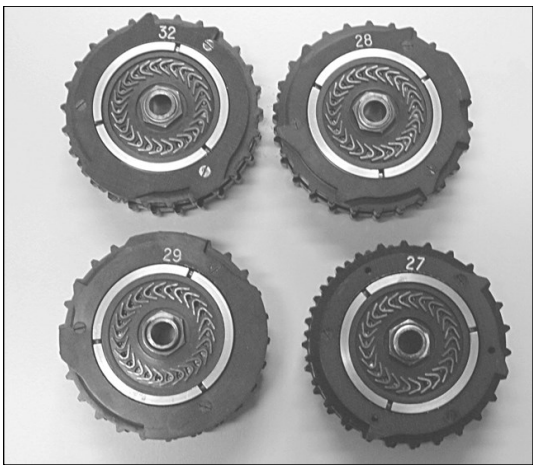


93 Eine der letzten noch erhaltenen Maschinen für den Verkehr mit den Botschaften. [AUT]

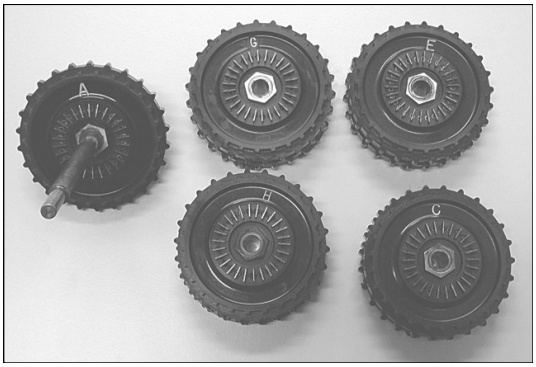
Innere Schlüssel für Nema
(Januar 1971 - Dez. 1980)

1. Quartal	A - 27 C - 28 F - 29 E - 30 D	
	B - 38 J - 44 L - 42 O - 41 N	
	T - 25 U - 26 Y - 33 X - 35 V	
2. Quartal	A - 29 D - 27 H - 28 E - 31 C	
	B - 41 L - 38 N - 44 J - 39 K	
	T - 37 X - 35 Z - 25 U - 33 W	
3. Quartal	A - 31 E - 29 C - 32 H - 28 F	
	B - 43 N - 39 O - 41 K - 38 J	
	T - 33 V - 37 U - 26 Y - 35 Z	

94 Die inneren Schlüssel der Botschaftsmaschinen wurden quartalsweise geändert. Drei verschiedene Walzensätze standen zur Verfügung, für Maschinen mit verschiedenen Einsatzgebieten. Ausschnitt aus einer grösseren Liste. [AUT]



95 Fortschaltwalzen der Botschaftsmaschine TD117 sie sind anders ausgestaltet als diejenigen beim Militär. [AUT]



96 Die Kontaktwalzen und die Umkehrwalze 'A' der selben Maschine 117. [AUT]

Dienst und sicherheitsmässig vermutlich auch nicht so genau überprüfbar. Ende der 1950er-Jahre wurde die Nema durch den Krypto-Fernschreiber abgelöst. Sie stand nur noch im Notfunknetz bei der Funkpolizei im Einsatz. Das Schlüsselverfahren wurde beim Militär aus kryptologischer Sicht nicht immer korrekt gehandhabt, ein Einbruch in diese Maschinen ist deshalb denkbar. In diesem Fall wären die Kontaktwalzen, die Form der Zahnscheiben und das Vorschubsystem verraten gewesen. Bei alle diese Maschinen handelte es sich "nur" um Übungs- oder Schulmaschinen.

- Daneben waren noch die ebenfalls militärischen K-Mob -Maschinen vorhanden. Sie wären im Kriegsfall zum Einsatz gekommen. In einer solchen Situation hätte man die Schulmaschinen durch die K-Mob-Maschinen ersetzt oder sie mit K-Mob-Walzen umgerüstet. Die "Kriegsmaschinen" wurden auf direktem Weg von der Fabrik in die Waffenkammern gebracht und blieben dort bis zur Entklassifizierung unter Verschluss. Diese Maschinen waren mit anderen Zahnscheiben ausgerüstet als die Schulmaschinen. Die Kontaktwalzen waren die gleichen wie bei den Schulmaschinen, zusätzlich noch ergänzt durch die Walzen 'E' und 'F'. Das Vorschubsystem war bei den beiden militärischen Versionen gleich; bei den Botschaftsmaschinen war es davon abweichend eingestellt, siehe dazu auf Seite 84 das Kapitel "Varianten der Fortschaltmechanik".
- Die Geschichte lehrt, dass alles, was verraten werden kann, auch verraten wird. Es ist eine Kleinigkeit, die Form der Zahnscheiben abzuzeichnen oder sich die Stellung der Nocken zu notieren. Die Verdrahtung der Walzen lässt sich mit einem einfachen Messgerät feststellen, wenn es sein musste genügte eine Taschenlampe und zwei Drahtstück. Man darf deshalb annehmen, dass die Verdrahtung der Rotoren und die Form der Zahnscheiben der militärischen Schulmaschinen in unberechtigte Hände kamen. Da die K-Mob-Maschinen nie bei der Truppe im Einsatz standen, konnte hier kein Verrat stattgefunden haben. Natürlich kann man einen Verrat oder ein Ausspionieren der Fabrikationsunterlagen nie ausschliessen.

Auf Grund all dieser Überlegungen möchte ich die unbelegte Behauptung aufstellen, dass die militärischen Schulmaschinen den gegnerischen Seiten bekannt waren, zu sorglos wurde damit umgegangen. Die Kriegsmaschinen waren sicher. Die Maschinen des diplomatischen Netzes hielten vermutlich den starken gegnerischen Angriffen stand. Aber sicher kann man nie sein, das kann man aus den wichtigsten Grundsätzen der Kryptologie ableiten:

Warum wurde die Nema aufgegeben?

Ausschlaggebend waren bestimmt mehrere Gründe. Sicher

> Unterschätze niemals den Gegner, denn:
>
> - Er ist immer aufmerksam, er schläft nie.
> - Er ist ideenreich und anpassungsfähig.
> - Er weiss mehr als man vermutet.

spielten Sicherheitsüberlegungen eine Rolle, aber nicht ausschliesslich.

Wegen des auf 26 Buchstaben beschränkten Zeichensatzes und der relativ langsamen und aufwändigen Arbeitsweise waren den Einsatzmöglichkeiten der Nema Grenzen gesetzt. Für ein effizientes Arbeiten waren zwei Personen erforderlich: Eine tastete den Text ein, die andere notierte die aufleuchtenden Buchstaben. Der Umgang mit der Maschine war nicht einfach. Bei den Anwendern fehlte ein vertieftes Verständnis für die Maschine. Es gab viele Klippen zu umschiffen; selbst kleine Fehler führten dazu, dass sich die beiden Stationen nicht verstehen konnten. Das waren vermutlich starke Argumente, die dazu beitrugen, dass das Militär die Nema grösstenteils schon um 1960 durch den Krypto-Fernschreiber ersetzte. Bis zur ihrer Ausmusterung blieb die Nema bei der Funkpolizei noch halbherzig beim Notfunknetz im Einsatz. Es ist aber kaum anzunehmen, dass jemand ernsthaft daran dachte, sie in einem Kriegsfall auch einzusetzen.

Das Arbeiten mit der Nema nahm sehr viel Zeit in Anspruch, das Dechiffrieren deutlich mehr als das Chiffrieren. Das Entwirren des erhaltenen Klartextwurms, mit all seinen sicherheitsbedingten Komplikationen, war nicht einfach. Wenn der Text dann noch in einer Fremdsprache vorlag erst recht nicht!

Die Maschine liess sich nicht in ein EDV-System einbinden, sie war für den Betrieb unter Morsetelegrafie und für "Handbetrieb" ausgelegt worden.

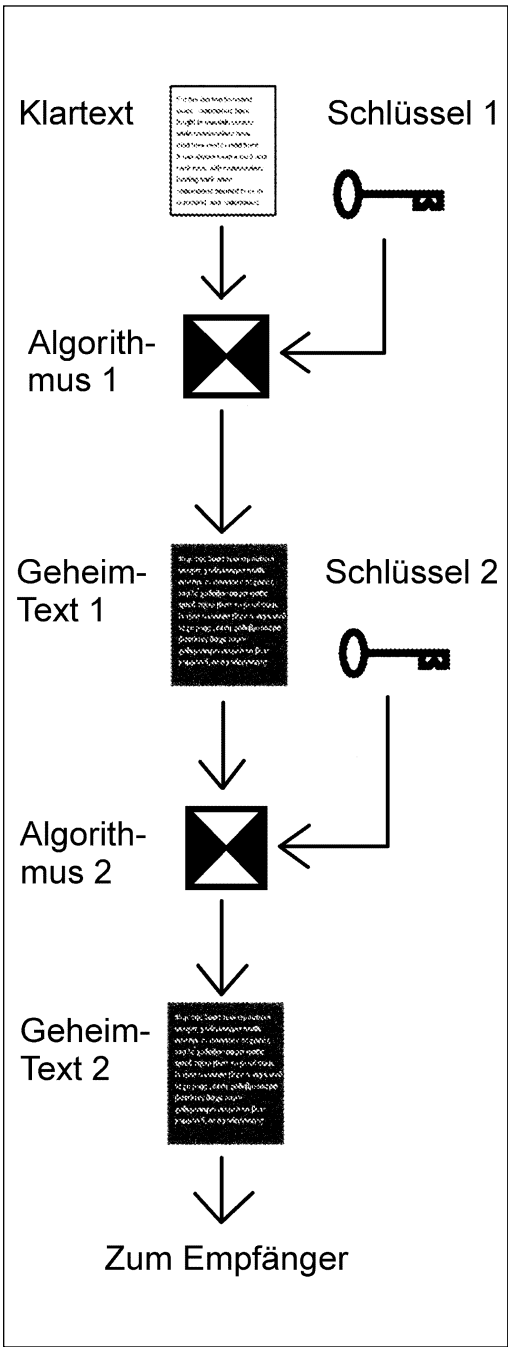
Um 1970 setzte beim professionellen Funkbetrieb allgemein ein technologischer Trend ein: Weg von der Morsetelegrafie, hin zum Fernschreiber. Das galt auch für den Schweizer Botschaftsfunk, wo die Nema noch immer Verwendung fand. Bei der Einführung neuer Techniken erwies sich die Nema als Hemmschuh. Beim Fernschreibbetrieb wurden offene Telegramme einmal auf den Lochstreifen gestanzt, aber dann ging es bis zum Empfänger ohne "Handarbeit". Nicht so bei den chiffrierten Telegrammen. Zuerst musste der Text des Streifens ausgedruckt werden, dann durchlief er in "Handarbeit" die Chiffriermaschine. Anschliessend musste man den erzeugten Geheimtext abschreiben um wieder einen Lochstreifen zu erhalten. Die Prozedur wiederholte sich in umgekehrter Richtung beim Dechiffrieren auf der Gegenstation. Das war alles sehr umständlich, arbeitsintensiv und viele Stolpersteine lauerten darauf, dem Chiffreur das Leben schwer zu machen.

Man wollte den auf Lochstreifen vorliegenden Klartext direkt in eine Chiffriermaschine eingeben und der erzeugte Geheimtext sollte direkt auf einen Lochstreifen gestanzt werden. Mit der Nema liess sich das nicht realisieren. Darum wurden im Botschaftsfunk Mitte der 1970er-Jahre neue Chiffriermaschinen eingeführt, die diese Möglichkeit boten. Daneben verfügten die neuen Maschinen über einen umfangreicheren Zeichensatz, es dürfte der gleiche gewesen sein wie beim Fernschreiber. Probleme wegen Übermittlungsfehlern gingen stark zurück, weil ein fehlerkorrigierendes Übertragungsprotokoll zum Einsatz kam.



97 Nicht nur Sicherheitsbedenken, sondern auch die Forderung nach schnellerem und effizienterem Betrieb verdrängte die Nema. Die Umstellung auf den Funk-Fernschreiber beim Botschaftsfunk verlangte modernere Chiffriergeräte. [AUT]

Fast alle Einbrüche in Chiffrierverfahren basieren auf Fehlern und Nachlässigkeiten seitens der Anwender.



98 Das Prinzip der Mehrfach-verschlüsselung. [16] [AUT]

Mehr Sicherheit

Mehrfachverschlüsselung

Dieses Verfahren ist auch unter dem Begriff "Überschlüsselung" bekannt. Darunter versteht man den Vorgang, bei dem ein Telegramm mehrmals hintereinander chiffriert wird. Entweder geschieht das nach dem gleichen Verfahren, z. B. zweimal mit der Nema – aber natürlich mit verschiedenen Schlüsseln! – oder dann nach verschiedenen Verfahren, z. B. erfolgt zuerst eine Transposition, anschliessend mit der Nema eine Substitution.

Auf Seite 52 haben wir schon einige Sicherheitsvorkehrungen kennen gelernt, die teilweise eine einfache Mehrfachverschlüsselung darstellen. Entweder wurden einzelne Buchstaben (Fehler) oder ganze Wörter (Blender) in den Text eingefügt. Das geschah in der Absicht, dass der ursprüngliche Klartext und der Geheimtext nicht eins zu eins zusammenpassen. Solche Aktionen werden nicht schriftlich festgehalten, der Chiffreur weiss im Nachhinein nicht mehr wo er solche Zusätze eingefügt hat. Das Aufteilen in Blöcke und das "Mischen" entspricht einer Transposition. Der Ersatz der stereotypen Telegrammköpfe durch einen dreistelligen Nummerncode am Ende des Telegramms, ergibt im ersten Schritt eine Codierung, gefolgt von einer Transposition; schliesslich erfolgt mit der Nema eine Substitution.

Wenn die Mehrfachverschlüsselung nicht systematisch angewandt wird und wenn ausser dem Absender und dem Empfänger niemand davon Kenntnis hat, wird es ein gegnerischer Kryptanalyst schwer haben, weil er nicht darauf vorbereitet ist. Früher oder später werden ihm seine Analysen dennoch den richtigen Weg weisen.

Wird die Überschlüsselung hingegen systematisch eingesetzt, wird die gegnerische Seite früher oder später davon Kenntnis bekommen. Es bereitet den Fachleuten dann keine besonderen Probleme, den Klartext stufenweise freizulegen. Ganz allgemein wird von einer Mehrfachverschlüsselung abgeraten, weil:

- Der zeitliche und der personelle Aufwand für das Chiffrieren und Dechiffrieren deutlich zunimmt.
- Die Schlüsselorganisation komplizierter wird, es kommen mehrere Schlüssel zum Einsatz.
- Die Wahrscheinlichkeit, dass Fehler auftreten, grösser wird. Rückfragen werden sich häufen, und die sind immer problematisch. Nach mehreren erfolglosen Versuchen wird das gleiche Telegramm oft nochmals mit einem anderen Schlüssel übermittelt; genau darauf wartet der Gegner!
- Der Gewinn an Sicherheit – wenn überhaupt – eher bescheiden ist. Wenn ein Verfahren die verlangte Sicherheit nicht erbringt, kommt ein stärkeres zum Einsatz.

Wenn die geringsten Anzeichen dafür vorhanden sind, dass ein Chiffriersystem nicht mehr sicher ist, wird man es sofort aufgeben und nicht versuchen, es mit zweifelhaften Massnahmen noch weiter am Leben zu erhalten.

Moderne Algorithmen

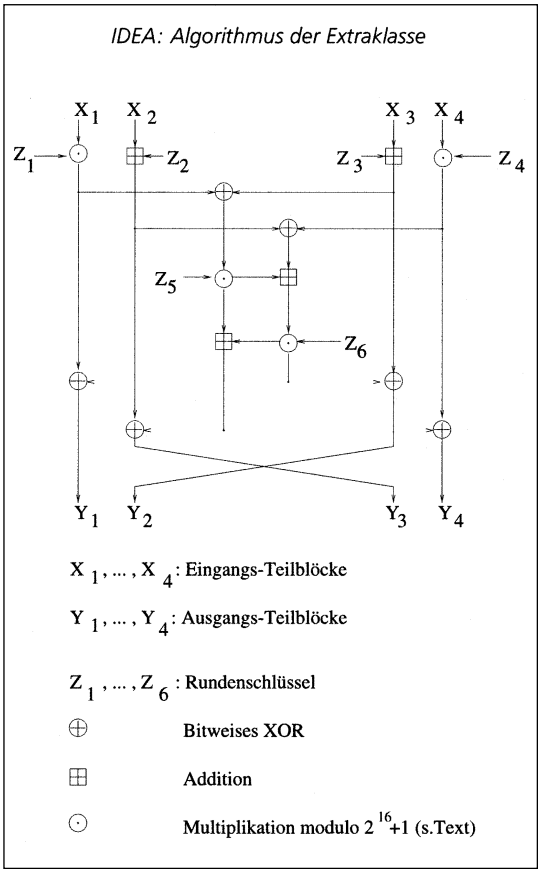
Zu Zeiten der Enigma und der Nema, vor 40 bis 70 Jahren, galt die Devise:

> Alles, was mit Chiffrieren auch nur im Geringsten zu tun hat, ist als "Geheim" zu klassifizieren.

Informationen und Instruktionen wurden nur sehr spär-lich – am liebsten überhaupt nicht – an die Chiffreure abgegeben, wohl in der irrigen Meinung, es könne dann nichts verraten werden. Dass ein unsachgemässes Arbei-ten mit der Maschine viel schlimmere Folgen haben könnte, daran dachte man nicht.

Teilweise war die strikte Geheimhaltung gerechtfertigt. Der Algorithmus bei der Nema, also die Mechanik des Vorschubsystems und die Verdrahtung der Rotoren waren ein wesentlicher Teil der Sicherheit.

Heute denkt man anders. Der Algorithmus ist nicht mehr geheim, er wird von den Entwicklern oder Erfindern in der Fachliteratur publiziert. So kann ein Anwender selbst abschätzen, ob ein neues Verfahren seinen Sicherheits-ansprüchen genügt.



99 Moderne Algorithmen sind Computerprogramme, die bis ins Detail bekannt sind, nur der individuelle Schlüssel muss geheim gehalten werden. [9]

> Die Geheimhaltung oder die Sicherheit ist bei modernen Verfahren ausschliesslich auf den individuellen Schlüssel konzentriert.

Bei der Nema würde diese These bedeuten, dass die Ver-drahtung der Rotoren, die Form der Zahnscheiben und die Mechanik des Vorschubsystems bekannt gegeben würden. Lediglich der innere Schlüssel, also die Reihenfolge der Walzen und der äussere Schlüssel, die Anfangsstellung der Walzen müssten einem feindlichen Angriff standhal-ten. Natürlich wären 10 Walzen nicht mehr ausreichend, vielleicht müssten es dann deren 50 sein. Ob man über-haupt auf der Basis einer Rotormaschine eine minimal geforderte Sicherheit erreichen könnte, das müssten die Mathematiker abklären. Der Vorteil einer konsequenten Offenlegung eines Chiffrieralgorithmus ist aber offen-sichtlich:

> Was öffentlich bekannt ist, kann nicht verraten werden!

Bei den heute eingesetzten Chiffrieralgorithmen wird der individuelle Schlüssel meist automatisch zwischen den beiden Stationen ausgetauscht, der Anwender kann darauf keinen Einfluss nehmen. Es sind Verfahren bekannt, um auf einem unsicheren Kanal einen sicheren Schlüsselaus-tausch vorzunehmen. Man erreicht so eine grösstmögliche Sicherheit und Verrat ist praktisch ausgeschlossen. Man denke etwa an die Verschlüsselung bei Banktransaktio-nen über das Internet. Der Anwender erhält mit seinem Passwort den Zugang zu seinem individuellen Konto, den Schlüssel für die chiffrierte Übermittlung dagegen erzeugt das System automatisch.



100 Die kommerzielle Enigma, Modell K. Sie wurde während des Krieges in der Schweizer Armee und im Verkehr mit den Botschaften eingesetzt. Die Maschine ist mit vier Rotoren ausgerüstet und hat kein Steckerbrett. Rechts das Fach für das Zusatzlampenfeld. [GSB]

A. H. Q. 23.11.39

Betrifft Chiffriermaschine "Enigma"

... und Hptm. Alder stattfand wurden von den beiden letztgenannten Herren die Bedenken vorgetragen, die gegen eine Verwendung der unveränderten "Enigma"-Maschine zur Chiffrierung von Meldungen sprechen.

... hat der Unterstabchef Front die Aenderung derjenigen Maschinen verfügt, die für den Verkehr zwischen Armeeleitung und den höheren Stäben bestimmt sind.

... Wir sind überzeugt, dass durch die Verwendung von Chiffriermaschinen, deren Schaltung Dritten bekannt ist, die Sicherheit chiffrierter Meldungen in hohem Mass in Frage gestellt wird. Wir können es daher gestützt auf die von unserem Chiffre-Bureau gemachten Untersuchungen nicht verantworten, dass die ungeänderten "Enigma"-Maschinen zur Chiffrierung von Meldungen in der Armee verwendet werden.

Nachrichtensektion
Der Chef:

101 Der Chef Nachrichtensektion informiert den Chef Flieger und Fliegerabwehr-Truppen über die Sicherheit der Enigma. Zitat aus einem Dokument. [BAR]

Geschichte der Nema

Im Nachhinein scheint jede geniale Erfindung einfach, ja banal zu sein.

Die folgenden Angaben basieren auf Unterlagen des Bundesarchivs und der angegebenen Literatur. Wichtige Dokumente zeige ich hier als Reproduktion. Dort wo eine solche aus technischen Gründen nicht möglich war, begnügte ich mich mit Zitaten.

Zuerst war die Enigma

In den 1930er-Jahren war die kommerzielle Enigma im Handel frei erhältlich, siehe Abb. 102. Auch die Schweizer Armee wurde mit dieser Chiffriermaschine ausgerüstet. Im Dezember 1939 bereitete die K. T. A. (Kriegstechnische Abteilung [des Militärdepartements]) eine Bestellung über 80 zusätzliche Enigmas vor, siehe Abb. 106. Ob die Bestellung auch ausgeführt, und ob die Maschinen dann geliefert wurden ist nicht sicher, siehe Bemerkung in Dokument 109. Beim damaligen EPD, dem heutigen Departement für Äusseres, kam die Enigma für den Verkehr mit den Botschaften zum Einsatz. Total standen im Juli 1942 in der Schweiz 265 Enigmas im Einsatz, 102 beim Heer und 163 bei den Fliegertruppen [19], das EPD lieh seine Maschinen bei der Armee aus.



102 Die kommerzielle Enigma war auf dem Markt frei erhältlich. Verkaufsprospekt. [2]

Die Enigma galt allgemein als absolut sicher. Man war überzeugt, dass es gegnerischen Kryptanalysten nicht gelingen könne, den Code zu brechen, selbst dann nicht, wenn die Rotorverdrahtung verraten würde. Deshalb wurde teilweise mit den nicht geheimen Originalrotoren gearbeitet.

Ganz geheuer war es den Mathematikern im Chiffrebureau (Nachrichtensektion des Armeestabes) nicht. Die Tatsache, dass die Rotorverdrahtung nicht geheim war wurde als kryptologischer Schwachpunkt erachtet. Die Fachleute hatten die Vermutung, dass es mit mathematischen Modellen gelingen könnte, den Code zu brechen, siehe Abb. 101. Dass die Befürchtungen des Chiffrebureau berechtigt waren sollte sich bald sehr eindrücklich herausstellen. Im Verkehr zwischen der Armeeleitung und den höheren Stäben wurden schon früh abgeänderte Rotoren eingesetzt. Bei den Fliegertruppen dagegen blieb man bei den originalen Rotoren, erst auf Befehl von "ganz oben" ging man daran, die Rotoren neu zu verdrahten. Diese Arbeit wurde im Dezember 1942 unter strengsten Sicherheits- und Geheimhaltungsmassnahmen in Angriff genommen, siehe Abb. 111.

Die Schweizer Enigma wurde gebrochen!

Im April 1941, also mitten im Zweiten Weltkrieg, erhielt das Chiffrebureau über verschlungene Pfade die vertrauliche Mitteilung, dass das schweizerische Chiffresystem im Ausland (zum Kauf) angeboten werde, siehe Abb. 107. Als Beweis lagen zwei Telegramme im Klar- und Geheimtext vor, datiert vom 20. 2. 41. Abklärungen ergaben, dass diese Telegramme von den Fliegertruppen stammten. Bei dieser Einheit wurde nicht jedes Telegramm mit einem individuellen Schlüssel bearbeitet, alle Telegramme wurden während einer bestimmten Zeit mit dem gleichen Schlüssel chiffriert. Es kam Hektik auf; ein Befehl für ein sicheres Chiffrieren wurde erlassen: Jedes Telegramm musste mit einem individuellen Schlüs-sel bearbeitet werden und die Rotoren waren neu zu verdrahten. Offen-sichtlich bewirkte der neue Befehl einiges. Wie der Literaturauszug in Abb. 103 zeigt, geriet das Brechen der "Enigma-Chiffren" ins Stocken oder

From the two above documents it is evident that the interception and decryptment of the Swiss radio traffic at Cadix was conducted at least from early-December 1940 to mid-March 1941, and the results obtained were systematically sent to the Polish 2 Bureau Headquarters in London, whence they were passed (rather as a matter of routine) to the British.

103 Zitat aus der Literatur. Der neu angeordnete Schlüsselbefehl zeigte offensichtlich Wirkung: Nach seinem Inkrafttreten hörte das systematische Brechen durch "Cadix" auf. [2]

Schlüsselmaterial war von den 4 eigenen polnischen Funkempfängern, die im Dachboden des Schlosses installiert wurden, abgefangen. Da die polnische »Cadix«-Gruppe über keine Peilstationen verfügte, waren die Standorte der in Frage kommenden Sendestationen mit Hilfe von französischen Peilern festzustellen. Wie sich bald herausstellte, lagen alle eindeutig in der Schweiz. 1

Die Horchstellen, erinnerte sich Marian Rejewski, »hatten uns zwei Kategorien von schweizerischem verschlüsseltem Abhörmaterial geliefert. Die erste war ein Handelscode, den wir ohne größere Mühe gelöst hatten. Die gelesenen Funksprüche betrafen größtenteils verschiedene Wirtschaftsverhandlungen und -abkommen zwischen der Schweiz und den Ländern des Vorderen Orients. Der Inhalt derartiger Funksprüche konnte für die Franzosen recht interessant sein[12].« 2

»Die zweite Kategorie bildeten geheime Funksendungen der schweizerischen Streitkräfte, welche mittels einer Chiffriermaschine verschlüsselt waren. Bereits eine flüchtige Analyse von abgehörtem Material zeigte, daß es sich um eine Art von »Enigma«-Maschine handelte. Doch, im Unterschied zu dem »Enigma«-Verfahren, welches von deutschen Militärstellen angewendet wurde (wo jeder einzelne Spruch seinen eigenen Schlüssel hatte), begannen schweizerische Funker alle an demselben Tag übergebenen Sprüche mit einer und derselben Ausgangsposition. Dieser Sachverhalt, bemerkte Rejewski, »hatte es uns ermöglicht, die derart verschlüsselten Sprüche mitzulesen, sogar ohne wissen zu müssen, was für eine Schlüsselmaschine benutzt wurde. Das war eben schon auf Grund der linguistischen Regelmäßigkeiten möglich, etwa so, wie man einfache Buchstaben-Spaltenchiffren knackt. Der einzige Unterschied bestand darin, daß hier alle ersten Buchstaben eine vereinzelte Spaltenchiffre, alle zweiten Buchstaben die zweite, mit einem anderen Schlüssel verschlüsselte Spaltenchiffre usw. bildeten. Doch die sprachlichen Charakteristika der zu lösenden Schlüsselsprüche waren teilweise verwischt, und es dauerte einige Tage, bis man endlich dahintergekommen war. Es hatte sich herausgestellt, daß nur ein Teil von dem uns gelieferten Abhörmaterial in seinem Klartext in deutscher Sprache verfaßt war. Manche Texte waren in französischer oder auch italienischer Sprache. Dies erschwerte uns die Arbeit ein wenig.« 3

»Parallel aber, als wir schon die ersten Texte angepackt hatten, konnten wir die uns früher bekannte Regelmäßigkeit der ›Enigma‹ herausgreifen, die die Lösung von vereinzelten Spaltenchiffren sehr erleichterte. Das war nämlich die ›Gegenseitigkeitsregel‹, die bei dem ›Enigma‹-Kryptosystem zum Vorschein kommt: so wenn man z. B. die Taste ›X‹ drückt, leuchtet im Glühlampenfeld der Buchstabe ›Y‹ auf und umgekehrt. Diesem Zustand war es zu verdanken, daß bei einem gelungenen Versuch man auf einmal auch den zweiten Buchstaben feststellen konnte. Wir konnten uns jedoch nicht damit begnügen, daß man diesen oder jenen Funkspruch entziffert hatte. Es galt nunmehr, die schweizerische Schlüsselmaschine als System zu lösen.

Die Tatsache, daß die schweizerische Maschine ähnliche Züge wie die deutsche ›Enigma‹ aufwies, hatte es uns nahegelegt, daß die erste auf gleichen oder ähnlichen Regeln basierte. So hatten wir bei unseren Versuchen, sie zu lösen, dieselben Methoden angewendet, welche sich beim Knacken der deutschen ›Enigma‹ bewährt hatten. Die Rolle von Anfängen der deutschen Funksprüche sollten jetzt die ersten Buchstaben der schweizerischen Funksprüche spielen. Den Permutationen A_1, A_2, A_3 ... entsprachen hier die Buchstabenspalten, die man durch das Ablesen von Anfangsabschnitten des Klartextes erhielt. Da wir schon (vgl. Anhang A – Verf.) nachgewiesen hatten, daß zum Auffinden von inneren Verbindungen (der Verdrahtung) der letzten Chiffrierwalze nur vier Gleichungen A_1, A_2, A_3, A_4 genügen, waren auch in diesem Falle nur vier aufeinanderfolgende Buchstabenspalten zum Auffinden dieser Verbindungen nötig. Die Methode erwies sich als durchaus wirksam, und auf diese Weise konnten alle Verdrahtungen der Maschine sukzessiv entdeckt werden[13].« 4

Die schweizerische Schlüsselmaschine war ein früher Typ der »Enigma«, doch natürlich mit anderen Drahtverbindungen als ähnliche deutsche Geräte. »Wir hatten auch keine Sorgen mit den Ringstellungen«, erklärte Rejewski, »weil es in dieser Art von ›Enigma‹ keine Ringe um die Schlüsselwalzen gab. Nichtsdestoweniger, um die Position der letzten Walze festzustellen, gab es für uns keinen anderen Weg als tagtäglich die Anfänge von Klartexten der Funksprüche abzulesen, wozu erst die erwähnte Buchstabenspalten-Methode benutzt werden mußte. Die Lage der anderen zwei Walzen konnte man durch die Versuch-und Irrtum-Methode finden.«

Während diese Darstellung von Rejewski einen kryptologischen Gesichtspunkt repräsentiert, sind die anderen mit der Lösung von schweizerischen Schlüsselverfahren verbundenen Fragen, wie die der Funkhorchtechnik, der inhaltlichen Analyse der mitgelesenen schweizerischen Funkkorrespondenz usw. in einigen anderen erhalten gebliebenen Dokumenten enthalten. Der erste solche Bericht war vom Chef der Expositur 300, Oberstlt. Langer, schon gegen Ende Dezember 1940 zusammengestellt und mit geheimer Kurierpost der Expositur »F« nach London befördert worden[14].

104 Die Schweizer Enigma wurde von "Cadix", einer südfranzösischen Widerstandsbewegung, systematisch gebrochen. [2]

versiegte ganz. Man muss die Sache jedoch realistisch sehen: Das Brechen der Schweizer Enigma wurde von polnischen Mathematikern, der Gruppe um Rejewski, als "Fingerübung" zum "Aufwärmen" betrieben. Die vordringliche und kriegsbeeinflussende Aufgabe des Teams war das Brechen der deutschen Enigma-Chiffren.

Aus der erwähnten Literatur geht eindeutig hervor, dass nicht nur zwei Telegramme gebrochen wurden. Der gesamte Funkverkehr der Fliegertruppen wurde in Südfrankreich von "Cadix" systematisch abgehört und aufgedeckt. Die Sendestationen wurden durch Peilung eindeutig in der Schweiz lokalisiert, Abb. 104 (1). Es gelangen auch Einbrüche in den diplomatischen Verkehr und in codierte Meldungen der Industrie und der Wirtschaft, siehe Abb. 104 (2).

Der Einbruch in den Enigma-Code der Schweiz gelang vor allem deshalb, weil nicht jedes Telegramm mit einem individuellen Schlüssel chiffriert wurde, siehe dazu die Bemerkung in Abb. 104 (3). Jeder Kryptologe weiss, dass man den gleichen Schlüssel unter keinen Umständen systematisch mehrmals verwenden darf! Wenn dieser elementare kryptologische Grundsatz nicht eingehalten wird, kann eine polyalphabetische Substitution nicht sicher sein!

Erstaunlicherweise wurde später beim Arbeiten mit der Nema der gleiche Fehler noch immer gemacht, siehe Seite 45. Die Gründe dafür dürften primär in der ungenügenden Ausbildung der Funker zu suchen sein. Die Bedienung der Nema war nicht einfach, nach dem Tagesschlüssel-Verfahren erst recht nicht. Für eine vertiefte Ausbildung, die das notwendige Verständnis gebracht hätte, fehlte die Zeit und aus Gründen der Geheimhaltung wollte man den Chiffreuren auch nicht zu viel mitteilen. Um das Ausbildungsziel dennoch oberflächlich zu erreichen und die chiffrierten Meldungen in der vorgegebenen Zeit "durchzubringen", wurde von vorgesetzten Stellen das "vereinfachte" Verfahren angeordnet (alle Telegramme mit dem gleichen Schlüssel chiffrieren). Um die Sicherheit trotzdem zu gewährleisten mussten die Funker mit aufgesetztem Stahlhelm arbeiten! Das ist jetzt überspitzt und zynisch formuliert, aber vor Jahrzehnten war es so, dass eine Gefahr erst dann wahrgenommen wurde, wenn sie von etwas "Handfestem" ausging. Das in Abb. 111 gezeigte Dokument vermittelt eine Ahnung vom damaligen Sicherheitsdenken.

»Cadix« solved and read military and diplomatic Swiss ciphers

Rejewski's amazingly exact Memoirs (1967) do include a short note saying that, while in southern France at the clandestine »Cadix« radio intelligence centre, his »Enigma«-cracking team was also able to solve and read some, not clearly specified, Swiss military ciphers. In describing this very briefly, he devotes some words to the method applied for this purpose but does not bother to mention how much and what kind of, Swiss intercepts were actually processed at »Cadix« or what was, eventually, their contents. Seemingly, the Swiss episode did not impress Rejewski too much, having been considered by him a rather marginal venture in comparison with the German »Enigma«.

105 Eine Schlagzeile, wie sie heute in der Boulevard-Presse stehen könnte. Aus jetziger Sicht erstaunt das sorglose Vorgehen beim Chiffrieren. Vielleicht wollten man nicht wahrhaben, dass die Radiowellen die Landesgrenze überquerten. Die Fachleute im Chiffrebureau hatten schon immer grosse Bedenken, aber sie wurden kaum ernst genommen. [2]

Eidg. Militärdepartement
Kriegstechnische Abteilung

Service technique
du Département militaire fédéral

Servizio tecnico
del Dipartimento militare federale

Antwort auf / Réponse à / No. .....
vom — du .....

Ax/Jg

No. 25.160.3/ 26
In der Antwort gefl. obige Nummer angeben
Indiquer ce numéro dans la réponse

Bern, den 2o. Dezember 1939

An das Armee-Kommando

F e l d p o s t

Chiffriermaschinen Enigma

Wir bestätigen die Besprechung vom 18. Dezember 1939 mit Herrn Oberst Mösch und haben von Ihrem Wunsche der Beschaffung von

8o Chiffriermaschinen Enigma
und je 16o Chiffrierwalzen I, II, III

Kenntnis genommen. Die Kosten für das obenerwähnte Material betragen:

8o Chiffriermaschinen	Fr. 112'ooo.-
48o Chiffrierwalzen	" 42'ooo.-
Total	Fr. 154'ooo.-

Wir ersuchen Sie um Bescheid, ob diese Bestellung durchgeführt werden soll und bitten Sie im Bejahungsfalle um Bekanntgabe des Ihnen hierfür zur Verfügung stehenden Kredites.

Kriegstechnische Abteilung
Chef

Fehr

An die Nachrichtensektion.
Von den oben genannten 80 Maschinen müssen 38 Stück an die Fl. + an die Fk. Top. zurückgegeben werden. Ich bitte zu prüfen, ob der verbleibende Rest von 42 Maschinen für den Bedürfnisse ausreicht.

Armeestab - Gruppe Front
Verbindungs-Sektion

23.12.39

Telegramme: Kriegstechnik — Telephon 61
Bitte in einem Brief nur ein Geschäft behandeln — Prière de ne traiter qu'une seule affaire par lettre

23743 -6111

106 Die Armee wurde in mehreren Etappen mit Enigmas ausgerüstet. Hier die Vorbereitung für eine Bestellung über 80 Stück. Es handelt sich um Maschinen mit drei Rotoren und einem drehbaren Reflektor (vierter Rotor). Zur Grundausrüstung wurden zusätzliche Rotoren (Chiffrierwalzen) bestellt. [BAR]

Soldaten als Erfinder

Eine Gruppe von drei Wehrmännern, die im Chiffrebuerau ihren Militärdienst leisteten, machte sich Gedanken über eine neue Chiffriermaschine, die mehr Sicherheit bot als die Enigma. Ohne einen offiziellen Entwicklungsauftrag zu haben, aber mit viel Motivation, entwarf das Trio die Grundzüge einer neuen Maschine. Sie wurden von ihrem militärischen Vorgesetzten, Hptm. Alder, in ihrem Tun unterstützt. Die Gruppe bestand aus einer Idealbesetzung: einem Maschineningenieur und zwei Mathematikern. Man kann davon ausgehen, dass ihre Erfindertätigkeit angespornt und intensiviert wurde, nachdem man von den Einbrüche in den Enigma-Funkverkehr Kenntnis hatte.

Eine neue Maschine wird gebaut

Bei der Armeeleitung dachte man über die Fabrikation einer eigenen Chiffriermaschine nach; es bestand ein grosser Bedarf an zusätzlichen Maschinen. Aus Deutschland waren seit Beginn des Kriegs keine Enigmas mehr erhältlich, siehe Abb. 109. Zudem war der anfängliche Glaube an die absolute Sicherheit der Enigma erschüttert. Die Fachleute drängten zu einer Neuentwicklung. Seitens der KTA glaubte man noch immer an die Sicherheit der Enigma, man dachte eher an einen Nachbau der Enigma. Bei dieser Lösung wären kaum Probleme zu erwarten gewesen, sie wäre vielleicht billiger gekommen und schneller zu realisieren gewesen. Auf der anderen Seite dürfte die Arbeit der Erfinder doch so weit ausgereift gewesen sein, dass man über eine machbare Alternative zum Enigma-Nachbau verfügte.

Die Befürworter einer Neuentwicklung setzten sich durch. Mit Datum vom 5. 5. 43 wurden die Spezifikationen für die neue Maschine formuliert, siehe Abb. 110. Man spürt aus dem Dokument heraus, dass die Zeit drängte. Um schneller zum Ziel zu kommen, wollte man bei der Neuentwicklung auf Bewährtes und Vorhandenes zurückgreifen, so sollte z. B. die Batterie vom gleichen Typ sein wie bei der Enigma.

Für die Detailkonstruktion der Neuen Maschine war sehr wahrscheinlich die KTA federführend, jedoch in enger Zusammenarbeit mit der späteren Herstellerfirma, der Apparate- und Maschinenfabrik Zellweger in Uster (ZAG). Bei der ZAG wurden zwei Prototypen in Auftrag gegeben, die schon anfangs Januar 1944 der KTA abgeliefert wurden.

Es dauerte dann noch etwa ein Jahr, bis alle Mängel behoben und kleine Änderungen ausgeführt waren. Anschliessend erfolgte die Erprobung der Maschine auf ihre Truppentauglichkeit. Am 31. 1. 45 formulierte die KTA eine Bestellung für 640 Nemas, Modell 45, siehe Abb. 108. Der Preis lag mit 2000 Franken nahezu gleich hoch wie für eine Enigma. Um mit heutigen Verhältnissen vergleichen zu können, muss man jenen Betrag etwa mit 20 multiplizieren. Eine Nema hätte in heutigem Geld demnach um 40'000 Franken gekostet!

Die ausgehandelte Lieferfrist betrug für die ersten 100 Maschinen 11 Monate, danach sollten monatlich 100 Maschinen die Fabrik verlassen, Mitte 1946 mussten somit alle Maschinen ausgeliefert sein. Während des gesamten Zweiten Weltkriegs stand die Nema demnach nicht im Einsatz. Die Auslieferung an die Truppen erfolgte 1947 [19]. Die Flieger- und Fliegerabwehrtruppen blieben bei der Enigma, sie hatten die Nema wohl erprobt, sie bemängelten jedoch, dass die Betätigung der Tasten mehr Kraft erfordere als bei der Enigma. Diese Angabe stammt von Paul Glur anlässlich eines Gesprächs.

In den Dokumenten des Bundesarchivs sind keine Hinweise zu finden, wonach zu einem späteren Zeitpunkt nochmals Maschinen gebaut worden wären, weder von der ZAG selbst, noch von der KTA anderswo in Auftrag gegeben. Ins Ausland wurden keine Maschinen verkauft, Lizenzen für einen Nachbau wurden nie vergeben. Man kann mit Sicherheit davon ausgehen, dass total 640 Nemas gebaut wurden.

Feststellungen zur Verwendung der Enigma-Maschine
bei der Fliegertruppe.

Am 21.4.41 machte mir Herr Oberstlt. i.Gst. Cuénoud die vertrauliche Mitteilung, dass er durch Agenten darauf aufmerksam gemacht worden sei, dass das schweizerische Chiffriersystem im Ausland angeboten worden sei. Der Betreffende habe behauptet, das Verfahren zu kennen. Zur Bekräftigung habe er die beiden in der Beilage enthaltenen Kryptogramme vom 20.2.41 vorgewiesen.

Meine Vermutung, es könnte sich um das auch von uns dekryptierte schweizerische System des Politischen Departementes handeln, stellte sich sehr bald als unrichtig heraus. Die den beiden Tg. vorausgehenden Rufzeichen sind, wie ich durch den Fk.Of. beim Tg.Chef der Armee in Erfahrung bringen konnte, Rufzeichen von Funkstationen der schweizerischen Fliegertruppen. Bei den Tg. kann es sich nicht um Tg. nach System F oder GR handeln und nach der Art der Aufmachung ist auch die Chiffrierung mit einer Enigma-Maschine für die höheren Stäbe ausgeschlossen. Es konnte sich daher nur noch um Enigmachiffrate unserer Fl.Trp. handeln. Ich sprach noch am 21.4.41 gegen Abend bei Herrn Oberst i.Gst. Ruedi, Stab Fl. u. Flab. Trp., in Bern vor und der Fk.Of. konnte mir sofort mitteilen, dass die Rufzeichen dem Stab Fl.u.Flab.Trp. und dem Kdo. Fl.Abt. 5 in der fraglichen Zeit zugeteilt waren. Er konnte mir auch ohne weiteres aus der Kenntnis des damals gültigen Schlüssels die beiden Tg. dechiffrieren.

Nachdem ich vorerst an einen Verrat der Schlüsselung der Maschinen der Fl.u.Flab.Trp. geglaubt hatte, erinnerte ich mich der Möglichkeit der Dekryptierung von Enigmachiffraten bei unzweckmässiger Verwendung der Maschine. Ich sprach daher am 22.4.41 nochmals bei Herrn Oberst i.Gst. Ruedi vor und der Fk.Of. bestätigte mir, dass der gesamte Schlüssel bei den Fl. u.Flab.Trp. jeweils während einer unbestimmten Dauer, in der Regel während 14 Tagen, verwendet wird. Gleichzeitig beantwortete er meine Frage nach der Art der Chiffrierung längerer Tg. dahin, dass solche Tg. in Teile von maximal 40 Gruppen aufgeteilt und jeder Teil für sich chiffriert werde. Auf mein Ersuchen stellte er dann an Hand seiner Journale fest, dass

107A Dieses Dokument belegt die Aufdeckung des schweizerischen Enigma-Chiffriersystems durch ausländische Nachrichtendienste, 1. Seite. [BAR]

durchschnittlich 35 Tg. mit durchschnittlich 30 Gruppen mit demselben Schlüssel chiffriert werden. Mit dem am fraglichen 20.2.41 gültigen Schlüssel seien rund 45 Tg. gewechselt worden.

Aus diesen Tatsachen geht hervor, dass die Enigma-Maschine bei der Fl.Trp. in absolut unzweckmässiger Weise verwendet wird. Adj.Uof. Hadwiger hat in seinem Bericht vom 15.6.1940 "Theoretische Studien zur Chiffriermaschine Enigma" unter Zif. 15 auf den Seiten 40 ff. die Möglichkeit der statistischen Enträtselung von Enigmachiffraten studiert. Diese Möglichkeit der Enträtselung war es auch, die das Chiffrebüro im Herbst 1939 veranlasste, die heute gültige Anwendung der Schlüssel vorzuschlagen. Vom Gesamtschlüssel bleibt nur ein Teil geheim, während ein Teil des Schlüssels mit jedem Tg. mitgegeben wird, dadurch wird jede statistische Enträtselung verunmöglicht.

Bei dem starken Chiffrierverkehr der Fl.Trp. (monatlich 50 000 Zeichen) ist es als sozusagen sicher anzunehmen, dass bei ständiger Ueberwachung der Fl. Sender die mit der Maschine chiffrierten Meldungen ohne grosse Mühe dekryptiert werden können. Es besteht sogar die Gefahr, dass durch die unzweckmässige Verwendung der Maschine die Schlüsselungen (Wicklungen) verraten worden sind. Ich beantrage daher, dass

1. Kdo. Fl.u.Flab.Trp. auf die unzweckmässige Verwendung der Maschine aufmerksam gemacht wird.(Herr Oberst Wuhrmann besitzt die Untersuchungen von Hadwiger zum Studium und kann sich dort von der Gefährlichkeit der Verwendung der Maschine im Sinne der Fl.Trp. überzeugen)
2. verlangt wird, dass die Wicklungen der Maschinen bei den Fl. Trp. geändert werden.
3. sofort das Nötige vorgekehrt wird, dass in Zukunft die Schlüsselübermittlung in ähnlicher Weise geschieht wie bei den Maschinen, die im Verkehr zwischen den höheren Stäben eingesetzt sind.

A.H.Q.

Abteilung für Nachrichten- und Sicherheitsdienst.
Chiffrebüro:

Beilage:

2 Kryptogramme und dazugehörige Klartexte.

Hptm. Alder

(Hptm. Alder)

107B Die zweite Seite des nebenstehenden Dokuments. [BAR]

FEB 1945
324

Armeestab
Abteilung für Genie

22/5 000557

31.1.45.

An die Kriegstechnische Abteilung (6 Expl.)

Betr. Chiffriermaschine.

Nachdem die Versuche mit den Prototypen der Chiffriermaschine Nema abgeschlossen sind, beauftragen wir Sie mit der Anordnung der Seriefabrikation. Es sind zu Lasten AL VII

Total 640 Stück Chiffriermaschinen

Nema Modell 1945 Zellweger AG. Uster in Auftrag zu geben.

Bei der Fabrikation müssen folgende Punkte berücksichtigt werden:

1) Die Maschine wird mit der normalen Schreibmaschinen-Tastatur ausgerüstet.

2) Jede Maschine wird mit einem zusätzlichen zweiten Lampenfeld versehen.

3) Zur Erleichterung der Sohlüsselwort-Einstellung werden die Buchstabenwalzen in beiden Richtungen drehbar ausgeführt. Die Rippen auf den Buchstabenwalzen werden "griffiger" ausgeführt als bei den Prototypen.

4) Wie bei den Prototypen kann auch beim Serientyp bei sofort bemerktem Tast-Irrtum ein Buchstabenfehler durch Betätigung des Hebels "Einstellen" korrigiert werden. Mehr als der zuletzt getastete Buchstabe lässt sich nicht korrigieren.

5) Die Maschine wird robuster konstruiert als die Prototypen, der Tastenanschlag wird härter und präziser, die Klinken breiter und solider ausgeführt als bisher.

6) Auf die Herabsetzung des Tastendruckes wird speziell geachtet. Es ist vorgesehen, die Maschinen möglichst ohne gefettete Teile zu bauen. Dies im Hinblick auf das leichte Arbeiten derselben bei tiefen Temperaturen. Voraussichtlich kann eine Tastendruckreduktion gegenüber den Prototypen um ca. 20 % erreicht werden.

7) Die Gleichmässigkeit des Tastendruckes beträgt ca. 1:3. Aus prinzipiellen Gründen kann sie nicht unter diesen Wert gesenkt werden.

8) Das Aufleuchten mehrerer Buchstaben beim Drücken einer einzigen Taste soll durch sorgfältige Einstellung der Maschine vermieden werden.

9) Wie besprochen, wird das Lampenfeld in der Maschine nur "dunkel" aufleuchten, dasjenige im Zusatzlampenfeld jedoch immer "hell". (Vorteil: bei falscher Netzspannungseinstellung können im Maximum nur die Lampen des Zusatzlampenfeldes durchbrennen).

10) Der (ausser der Trockenbatterie) vorgesehene Transformator zum Anschluss der Maschine an die üblichen Wechselstromnetze wird in der Maschine (nicht im zweiten Lampenfeld) montiert.

11) Sämtliche zur Nema gehörenden Teile (zweites Lampenfeld, Kabel, Reserveteile etc.) werden in ein und denselben Kasten untergebracht. Der Panzerholzkasten erhält die

./.

– 2 –

Aussenabmessungen: 330 x 380 x 145 mm. Das komplette Gewicht beträgt voraussichtlich 10, 3 kg.

12) Die Maschine wird derart gebaut, dass später ohne weiteres durch sie gesteuert werden kann:

a) elektrische Schreibmaschine,
b) Fernschreiber,
c) Hellschreiber,
d) Creed-Locher.

Die Lieferung der Maschinen erfolgt entsprechend folgendem Schema:

100 Stück 11 Monate nach Bereinigung des Lieferungs-Vertrages.
hierauf je:

100 Stück pro Monat

Der Waffenchef der Genietruppen:

Gubler.

Kopie an:
Armeestab: Operationssektion (2)
" Chef des Uem. Dienstes (2)
" Materialsektion (2)
Kdo. Fl. und Flab. Trp. (4)

lo/44

108B Die zweite Seite des nebenstehenden Dokuments. [BAR]

108A ◄ Die KTA erhält vom Armeestab den Auftrag zur Bestellung von 640 Nemas. [BAR].

Chiffrier-Maschine "Nema"
Eingabe Chiffer-Bureau.

Durch die Abteilung für Genie wurde uns mit Schreiben vom 24.8.46 Kenntnis gegeben von einer Eingabe der Herren Oblt. Weber, Lt. Hadwiger und Wm. Glur, datiert vom 5.6.46, in welcher dieselben betreffend ihrer an der Chiffrier-Maschine "Nema" geleisteten Mitarbeit Freigabe für Patentverwertung bzw. eine Entschädigung oder Lizenzgebühren beanspruchen. Die Eingabe selbst haben Sie uns mit Schreiben vom 3.September 1946 zugestellt. Wir bemerken zur Angelegenheit wie folgt:

Die Chiffrier-Maschine "Enigma", Vorläufer der "Nema", ist eine deutsche Konstruktion, wurde bis zum Beginn des Weltkrieges von uns aus dem Ausland beschafft und stellte das beste Chiffrier-Gerät, das unsere Armee besass, dar. Diese Maschine wurde während dem Kriege durch das Chiffer-Bureau des Armee-Kommandos inbezug auf Sicherheit eingehend untersucht und als absolut schlüsselfest befunden. Auf Veranlassung des Chiffer-Bureaus wurde lediglich die innere Schaltung der Walzen als zusätzliche Sicherheitsmassnahme umgeändert. Da die Maschine während dem Kriege aus Deutschland wegen grossem Eigenbedarf nicht mehr erhältlich war, und anderseits bei uns noch ein grösserer Bedarf an solchen Geräten vorlag, wurde ein Nachbau der Maschine in der Schweiz ins Auge gefasst. Zu Ihrer Orientierung legen wir eine Kurzbeschreibung der Chiffrier-Maschine "Enigma" bei. Ob dieses Gerät patentrechtlich geschützt ist, geht aus der Beschreibung nicht hervor und ist uns auch sonstwie nicht bekannt.

Die "Nema"-Chiffriermaschine ist eine Weiterentwicklung der "Enigma", in dem Sinne, dass auf Veranlassung des Chiffer-Bureaus die Schlüsselfestigkeit der "Nema" wesentlich höher als bei der "Enigma" getrieben und das Gerät mit zusätzlichen "Schikanen" ausstaffiert wurde. Wir legen auch

109 In einer Stellungnahme vom 23. Sept. 1946 ist die KTA noch immer der Ansicht, dass die Enigma während der Kriegszeit absolut schlüsselfest gewesen sei. Während des Krieges waren keine Maschinen erhältlich. [BAR]

16 A.H.Q., 5.5.43.

7/W

An die Kriegstechnische Abteilung des E.M.D., Bern.

Betr. Chiffriermaschinen.

In Bestätigung der Besprechungen vom 3.5.43 zwischen den Herren Oberstlt. Leutwyler, Hptm. von Arx, Hptm. Alder und Oblt. Weber präzisieren wir die Forderungen und Wünsche, die an eine neue Maschine gestellt werden müssen:

1. Das Prinzip Enigma ist beizubehalten mit Tasterfeld, Lampenfeld und auswechselbaren Walzen.
2. Die Walzenzahl ist von 4 auf 5 zu erhöhen, davon eine Umkehrwalze.
3. Der Transportmechanismus soll variabler gestaltet werden, als bei der bisherigen Maschine. Spezielle Anordnungen werden noch auf ihre sicherheitssteigernde Wirkung geprüft.
4. Kleinere Ausmasse und kleineres Gewicht sind sehr wünschbar.
5. Der Walzenkonstruktion ist grösster Wert beizulegen im Sinne besserer Kontaktgabe und kleinerer Abnutzung.
6. Als Stromquelle diene der gleiche Batterietyp wie bisher, aber mit verbesserter Halterung in der Maschine.
7. Es sind pro Maschine zwei weitere Walzen in Reserve zu halten.

Um die Angelegenheit möglichst zu beschleunigen, senden wir Ihnen mit separater Post die E.-Maschine No.853 mit vollständigem Walzensatz, Schloss und zwei Schlüssel, sowie eine defekte Walze K413II. Die Walzen weisen die ursprüngliche Wicklung der Fabrik auf.

Für alle technischen Fragen, die mit der Maschine zusammenhängen, steht Ihnen Oblt. Weber jederzeit zur Verfügung.

ARMEEKOMMANDO
Der Stellvertreter

110 Die Spezifikation für die neue Chiffriermaschine wird formuliert. [BAR]

Kdo. Fl. & Flab Trp.
Verbindungsdienst.

K.P., 14.12.42

GEHEIM.

Abänderung der Chiffriermaschinen auf Stromschritt 4.

An Sdt. Riederer August,
z.Z. Stab Fl. & Flab Trp.

Sie erhalten Befehl, sämtliche Chiffrierwalzen, welche Ihnen vom Funkof. des Stabes Fl. & Flab Trp. ausgehändigt werden, auf Stromschritt 4 zu schalten.
Zudiesem Zweck erhalten Sie als Unterlage die Verdrahtungsschemata No. 4, Blätter 1,2 und 3.
Sämtliche Arbeiten sind im Bureau No. 34 auszuführen und stehen unter der persönlichen Kontrolle von Lt. Bolliger.

Arbeitszeit : 0800 - 1200 und 1400 - 1800 in verschlossenem Büro, welches von aussen durch Lt. Bolliger verriegelt wird.

Als Verbindungsmittel zum Verkehr mit dem Fk.-Dienst des Stabes Fl. & Flab Trp. (Oberst Wuhrmann oder Lt. Bolliger) steht Ihnen eine Tf.-Verbindung zur Verfügung.
Ueber dieses Tf. (No. 61.41.31) dürfen Sie nur mit dem Bureau von Oberst Wuhrmann (61.41.35) oder Lt. Bolliger (61.41.14) verkehren.

Wird die Arbeit eingestellt, sei es auch nur für kurze Zeit, so sind sämtliche geheimen Unterlagen und die in Arbeit befindlichen Walzen im Wandkasten einzuschliessen. Der Schlüssel des Wandkastens ist jeweils mittags und abends bei Lt. Bolliger zu deponieren.

Das Fenster ist immer dann, wenn weder Sie noch Lt. Bolliger sich darin aufhalten, zu schliessen und zu plombieren.

Sie verpflichten sich, über Ihre Arbeit mit niemandem zu sprechen und sämtliche Unterlagen als streng geheim zu behandeln.

Irgendwelche Notizen, selbst scheinbar geringfügiger Art, dürfen nicht gemacht werden.

Kommando
Flieger- & Fliegerabwehrtruppen
i.A. Der Chef des Funkdienstes :

Oberst Wuhrmann

Der Unterzeichnete bestätigt, von diesem Befehl Kenntnis genommen zu haben und sich streng daran zu halten. Er ist sich bewusst, dass die kleinsten Verfehlungen gegen diesen Befehl durch die Militär-Justiz geahndet werden.

Sdt. Riederer August.

K.P., 14.12.42

111 Unter strengsten Sicherheitsvorkehrungen wurden die Enigma-Rotoren neu verdrahtet. Die entscheidenden Fehler, die zum Brechen des Schweizer Enigma-Codes führten, waren jedoch nicht auf Verrat zurück zu führen, sondern auf untaugliche Schlüsselbefehle. [BAR]

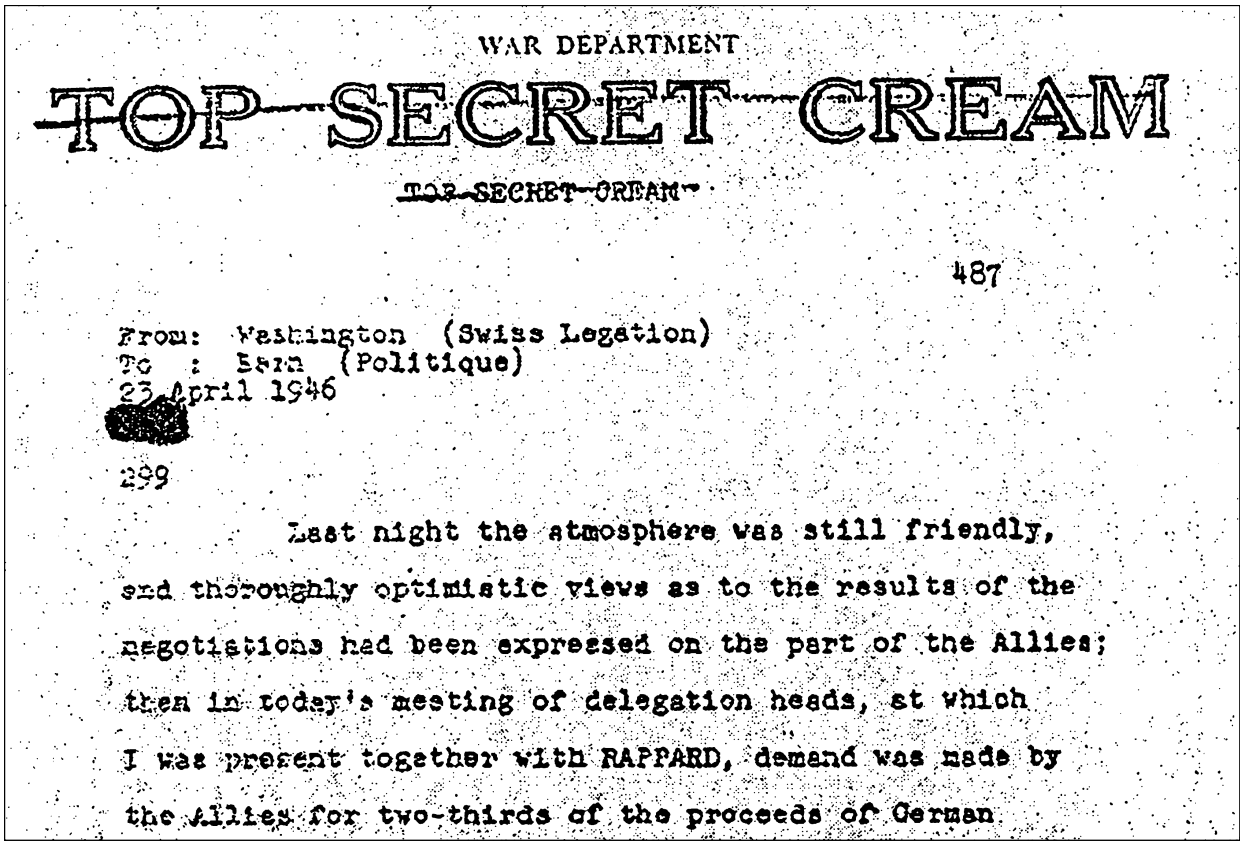
Schatten des Zweiten Weltkriegs

Wer verriet den Amerikanern die Zahl von 250 Millionen Franken?

Abhöraktion und Intrigen an der Washingtoner Konferenz von 1946

Von Thomas Maissen*

In den Washingtoner Verhandlungen von 1946 willigt die Schweiz in eine Zahlung von 250 Millionen Franken ein, viel mehr als ursprünglich geplant. Der Verdacht, das schweizerische Höchstangebot sei den Alliierten verraten worden, richtete sich rasch gegen Alfred Hirs, Direktor der Schweizerischen Nationalbank. Die Kontroverse blieb damals ungelöst. Heute klären Akten aus dem Bundesarchiv und jüngst freigegebene Abhörprotokolle aus dem Nationalarchiv in Washington das Rätsel weitgehend.



WAR DEPARTMENT

TOP SECRET CREAM

TOP SECRET CREAM

487

From: Washington (Swiss Legation)
To : Bern (Politique)
23 April 1946

[redacted]

299

Last night the atmosphere was still friendly, and thoroughly optimistic views as to the results of the negotiations had been expressed on the part of the Allies; then in today's meeting of delegation heads, at which I was present together with RAFFARD, demand was made by the Allies for two-thirds of the proceeds of German

112 ▲▲ Die Verhandlungsstrategie der Schweizer Delegation wurde damals verraten. Im Nachhinein erfuhr man, dass die USA den Enigma-Code brachen. [NZZ Online Dossier, 15. Nov. 1999]

113 ▲ Die abgehörte und gebrochene Meldung der Schweizer Botschaft in Washington an das EPD. Es wurde noch mit der Enigma chiffriert, ein Jahr später hätte man die sichere Nema zur Verfügung gehabt! [National Archives, Washington]

Die Erfinder wehren sich

Die drei Erfinder der Nema hatten ihre Arbeit als Wehrmänner und nicht als Bundesbeamte gemacht. Sie stellten sich deshalb auf den Standpunkt, dass ihnen eine Entschädigung zustehe. Nicht für die geleistete Arbeit, die taten sie als Soldaten im regulären Militärdienst, sondern für die gemachte Erfindung. Im Mai 1946 stellten sie eine entsprechende Eingabe an das Militärdepartement, siehe Abb. 114. Sie wären auch damit einverstanden gewesen, dass man ihnen die Erfindung zur eigenen Verwertung überlassen hätte.

Die Bundesbehörden wollten nicht auf die Forderung eingehen, man befürchtete einen Rattenschwanz ähnlicher Begehren. Den drei Männern wurde entgegengehalten, dass sie die Erfindung in Erfüllung ihrer dienstlichen Pflicht gemacht hätten. Die KTA verneinte einen patentierbaren Neuheitsanspruch, sie stufte die Enigma noch immer als absolut sicher ein! Siehe Abb. 109.

Auch das Amt für Geistiges Eigentum wurde zu einer Stellungnahme gebeten. Seine Beamten sahen ebenfalls keine patentierbare Erfindung. Einer ihrer Ingenieure verstieg sich zur Behauptung, dass er binnen 20 Minuten auf die Idee der Rotorsteuerung mit den Zahnscheiben gekommen sei; und das, ohne Vorinformationen gehabt zu haben! Da kann man nur den Kopf schütteln und sagen: Jede geniale Erfindung ist einfach; im Nachhinein haben es immer alle besser gewusst und besser gekonnt.

Die Erfinder präzisierten ihre Arbeit nochmals und beharrten darauf,dass sie die Arbeit freiwillig als Wehrmänner im Militärdienst ge-macht hätten. Sie stellen die konkrete Forderung auf eine Entschädi-gung von 6000 Franken für das ganze Team oder die Überlassung ihrer Erfindung zur Vermarktung im Ausland. Die genannte Summe scheint nicht viel zu sein, aber in heutigem Geld wäre das etwa das 20fache, also gegen 120'000 Franken, kein Pappenstiel. Bezüglich des ganzen Auftragsvolumens sind das 0,5 %, sicher keine überris-sene Forderung der Erfinder für das Ausdenken und die Umsetzung einer wirklich genialen Idee bis hin zur Konstruktionsreife.

Deren späte Anerkennung

Mehr als ein Jahr lang wurden Gutachten, Stellungnahmen und Präzisierungen verfasst. Anfänglich wollte die KTA den Erfindern die Vermarktung ihrer Idee im Ausland zugestehen, das hätte nichts gekostet! Man verknüpfte diese Zusage aber mit Bedingungen, die eine Verwertung verunmöglicht hätten. In recht scharfem Ton wiesen die Erfinder auf diesen Pferdefuss hin. Das EPD, das damalige Aussenministerium war jedoch strikte gegen eine Freigabe der Erfindung, weil es die Nema für den Verkehr mit seinen Aussenstationen einsetzte. Die Sicherheitsansprüche wurden beim Politischen Departement wesentlich schärfer eingestuft als sie beim Militär definiert waren, das dürfte auch heute noch so sein.

Langsam gingen der KTA die Argumente gegen den Entschädigungsanspruch aus. Auf Wunsch der Erfinder bat man deren ehemaligen militärischen Vorgesetzten um eine Stellungnahme. Dieser, Prof. Arthur Alder, Mathematikprofessor an der Universität Bern, kam zum Schluss, dass die Forderung der Erfinder von 6'000 Franken eher bescheiden sei. Er meinte, dass 10'000 Franken angemessen wären. Jetzt ging es schnell, vielleicht befürchtete man, dass es nur noch teurer werden konnte. Die Angelegenheit war inzwischen zur Chefsache geworden. Die Bundesräte Karl Kobelt (Militär) und Ernst Nobs (Finanzen) unterzeichneten die entsprechenden Dokumente. Der Militärminister Kobelt teilte den Erfindern am 3. Oktober 1948 mit, dass die 6'000 Franken umgehend ausbezahlt würden.

Bern, den 5.Juni 1946

An die
Abteilung für Genie
Eidgenössisches Militärdepartement
B e r n .

Auf dem Dienstweg.

Betrifft: Chiffriermaschine "Nema", Regelung der Patentfrage.

Die drei Unterzeichneten bildeten im Rahmen des Chiffrebureaus der Nachrichtenabteilung während den letzten Jahren des Aktivdienstes eine Arbeitsgemeinschaft. Unsere Aufgabe bestand vor allem darin, die auf dem Markt erhältlichen, sowie die von der Armee eingesetzten Chiffriermittel zu studieren und ihre zweckmässige Anwendung in Bezug auf grösste Sicherheit herauszufinden. So wurden in der Folge an der Enigma-Maschine verschiedene wichtige Verbesserungen vorgenommen. Trotzdem wurden wir uns klar darüber, dass nur eine Maschine mit vielfach erhöhter Sicherheit unserm beschränkten Ausbildungsstand der Chiffreure Rechnung tragen könne. Auf Grund unserer umfassenden Studien (die Berichte liegen bei der Nachrichtensektion der G.St.Abt.), durch gegenseitige Kontrolle von Vorschlägen und Anregungen in Diskussionen entstand das Projekt der neuen Maschine, bevor die KTA unsere Mitarbeit anforderte. Die KTA hiess unsern Vorschlag gut und erteilte der Firma Zellweger A.G. in Uster den Auftrag zur konstruktiven Ausgestaltung. Im Frühling 1945 erfolgte nach gründlicher theoretischer und praktischer Ueberprüfung einer Prototypserie eine Bestellung von 600 Maschinen im Betrag von ca einer Million Franken. Auch das Politische Departement bestellte eine Anzahl solcher Maschinen.

Eine Patentanmeldung wurde unterlassen in Anbetracht der damaligen Zeitumstände und des heiklen Charakters des Erfindungsgegenstandes. Wir möchten dies nachholen,,möchten aber keine weitern Schritte unternehmen ohne Ihre Einwilligung. Rechtlich wären folgende Regelungen denkbar:

Weitere Dokumente zur Geschichte

1. Der Bund erhebt das Eigentumsrecht auf die Erfindung in vollem Umfang. Ob er das Patent anmeldet oder nicht, ist für uns belanglos. Da die Erfindung in dienstlicher Stellung der Beteiligten gemacht wurde, sofern die Aktivdienstleistung mit der Beamtendienstleistung in Parallele gesetzt werden kann, ergaben sich mindestens die gleichen Rechte wie sie der Artikel 16 des Beamtengesetzes für Erfindungen von Beamten vorsieht.
2. Der Bund erhebt den Anspruch nur auf das Schweizer-Patent und überlässt uns die ausländische Verwertung. Auch dann steht uns rechtlich eine Entschädigung zu, wenn auch kleiner als im ersten Fall.
3. Der Bund überlässt uns die Verwertung der Erfindung im In- und Ausland. In diesem Fall dürfte der Bund uns für entgangene Lizenzgebühren teilweise schadlos halten.

Soweit unsere Auffassung über die verschiedenen Regelungsmöglichkeiten.

In Erwartung Ihres wohlwollenden Entscheides zeichnen hochachtungsvoll

H. Weber (H.Weber, Oblt.Ing.Of.
Jubiläumstr.57, Bern.)

H. Hadwiger (H.Hadwiger,Lt.Stabssekretär
Hochfeldstr.31, Bern.)

Prof. Dr. Hugo Hadwiger
(Uni Bern)

Paul Glur (P.Glur, Wm.Uem.Pk.Kp.55
Kirchgasse 6, Bern.)

◄ 114A ▲ 114B Die Erfinder stellen das Gesuch um Entschädigung, oder dass ihnen die Erfindung zur eigenen Verwertung überlassen werde. [BAR]

EIDGENÖSSISCHES POLITISCHES DEPARTEMENT
DÉPARTEMENT POLITIQUE FÉDÉRAL

Bern, den 12. Dezember 1947.

EIDGENÖSSISCHES MILITÄRDEPARTEMENT
13. DEZ. 1947
214.2 v.46

A.22.13.10. - HG.
Bitte dieses Zeichen in der Antwort wiederholen
Prière de rappeler cette référence dans la réponse
ad. No. 214.2.v.46

An die Direktion der Militärverwaltung
des Eidgenössischen Militärdepartements,
B e r n .

Herr Oberstbrigadier,

Mit Schreiben vom 3.d.M. teilen Sie uns mit, dass Sie sich gegenwärtig mit der Frage einer Entschädigung an die drei Erfinder der Chiffriermaschine "NEMA" beschäftigen und fragen uns gleichzeitig an, welche Bedeutung diese Maschine für unseren Dienstbetrieb hat, und ob für uns ein Interesse bestehe, die Auswertung im In- und Auslande zu verhindern.

Wir beehren uns, Ihnen darauf folgendes zu antworten. Im Jahre 1943 haben wir davon Kenntnis erhalten, dass Ingenieure und Techniker, die der Nachrichtensektion des Armeestabes zugeteilt worden sind, auf Grund der an der "ENIGMA" gemachten Erfahrungen, an einer Neukonstruktion arbeiteten. Da unser Chiffrierdienst auch damals schon mit der "ENIGMA" arbeitete, haben wir stets ein grosses Interesse an der Entwicklung dieser Arbeiten bekundet.

Aus keinem der mit diesen Spezialisten geführten Gespräche, noch aus dem Schreiben vom 20. März 1945 des Armeekommandos - Gruppe Ib, wovon eine Kopie in der Anlage, konnten wir entnehmen, dass die neue Chiffriermaschine je für eine Auswertung im In- und Auslande freigegeben würde. Im Gegenteil, aus der geübten Diskretion und der Tatsache, dass diese Erfindung in Ausführung dienstlicher Pflichten im Armeekommando durch verantwortungsbewusste Offiziere zustande gekommen ist, schien uns eine andere Möglichkeit, als dass die Neukonstruktion einzig der schweizerischen Landesverteidigung zugute kommen sollte, gar nicht in Frage zu kommen.

Diese Erwägungen waren denn auch ausschlaggebend für den Chef des Politischen Departements, als er im Frühling 1945 die Bewilligung für die Anschaffung von vorläufig 12 Stück NEMA gab.

Aus Artikel 16 des Bundesgesetzes über das Dienstverhältnis der Bundesbeamten vom 30. Juni 1927 geht einwandfrei hervor, dass Erfindungen, die in Ausübung einer dienstlichen Tätigkeit gemacht werden, dem Bunde gehören und der Erfinder Anspruch auf eine angemessene Vergütung hat.

Es unterliegt keinem Zweifel, dass die in Frage stehende Erfindung in militärischer und wirtschaftlicher Hinsicht nur dann von Wert sein kann, wenn sie vom Bunde übernommen und nur für eigene Zwecke verwendet wird.

Eine Freigabe für die Verwertung im In- und Auslande würde die Sicherheit der Geheimhaltung im höchsten Masse gefährden, was vom militärischen wie vom politischen Standpunkte aus unbedingt verhütet werden muss.

Genehmigen Sie, Herr Oberstbrigadier, die Versicherung unserer vorzüglichsten Hochachtung.

Beilage: 1 Briefkopie.

◄ 115A ▲ 115B Das EPD wehrt sich gegen eine Vermarktung der Nema im Ausland. Die Forderung soll mit der Behauptung abgewehrt werden, dass Erfindungen *"in Ausübungen einer dienstlichen Tätigkeit"* dem Bund gehören. Der Direktor der Militärverwaltung war sich jedoch nicht so sicher, ob diese Bestimmung auch für Angehörige der Armee Gültigkeit haben. Er setzte darum eine Randnotiz: *"wenn sie Beamte wären!"*. [BAR]

EIDGENOSSISCHES FINANZ- UND ZOLLDEPARTEMENT
DÉPARTEMENT FÉDÉRAL DES FINANCES ET DES DOUANES
DIPARTIMENTO FEDERALE DELLE FINANZE E DELLE DOGANE

P.3010.1 Bern, den 1.Oktober 1948.

13
EIDGENÖSSISCHES MILITÄRDEPARTEMENT
– 2. OKT. 1948
214.2.v.46

An das
eidgenössische Militärdepartement,

Bern.

Chiffriermaschine "Nema";
Vergütung für Erfindung.
Ihre No 214.2. v.46

Herr Bundesrat,

Am 5.Januar dieses Jahres gab uns die Direktion der Militärverwaltung von einem Briefwechsel Kenntnis, den sie mit einer Gruppe von ehemaligen Angehöri[illegible]

– 3 –

mentes sind wir jedenfalls ohne weiteres in der Lage, Ihnen die Ausrichtung einer Erfinderbelohnung zu empfehlen. Bedingung wäre, dass die Neukonstruktion Eigentum der Eidgenossenschaft bleibt. Der verlangte Betrag von 6000 Franken erscheint nicht übersetzt. Herr Prof.Alder schlägt sogar eine höhere Vergütung von mindestens 10 000 Franken vor, die zu 1/2 Herrn Oblt.Weber und zu je 1/4 den Herren Lt.Hadwiger und Wm.Glur zufallen sollte. Es darf vorausgesetzt werden, dass Herr Prof.Alder als Chef des Chiffredienstes im Armeestab in der Lage ist, die Angemessenheit dieses Verteilungsschlüssels beurteilen zu können.

Genehmigen Sie, Herr Bundesrat, die Versicherung unserer ausgezeichneten Hochachtung.

Eidg. Finanz- u. Zolldepartement

Beilage: 2 Aktenstücke zurück

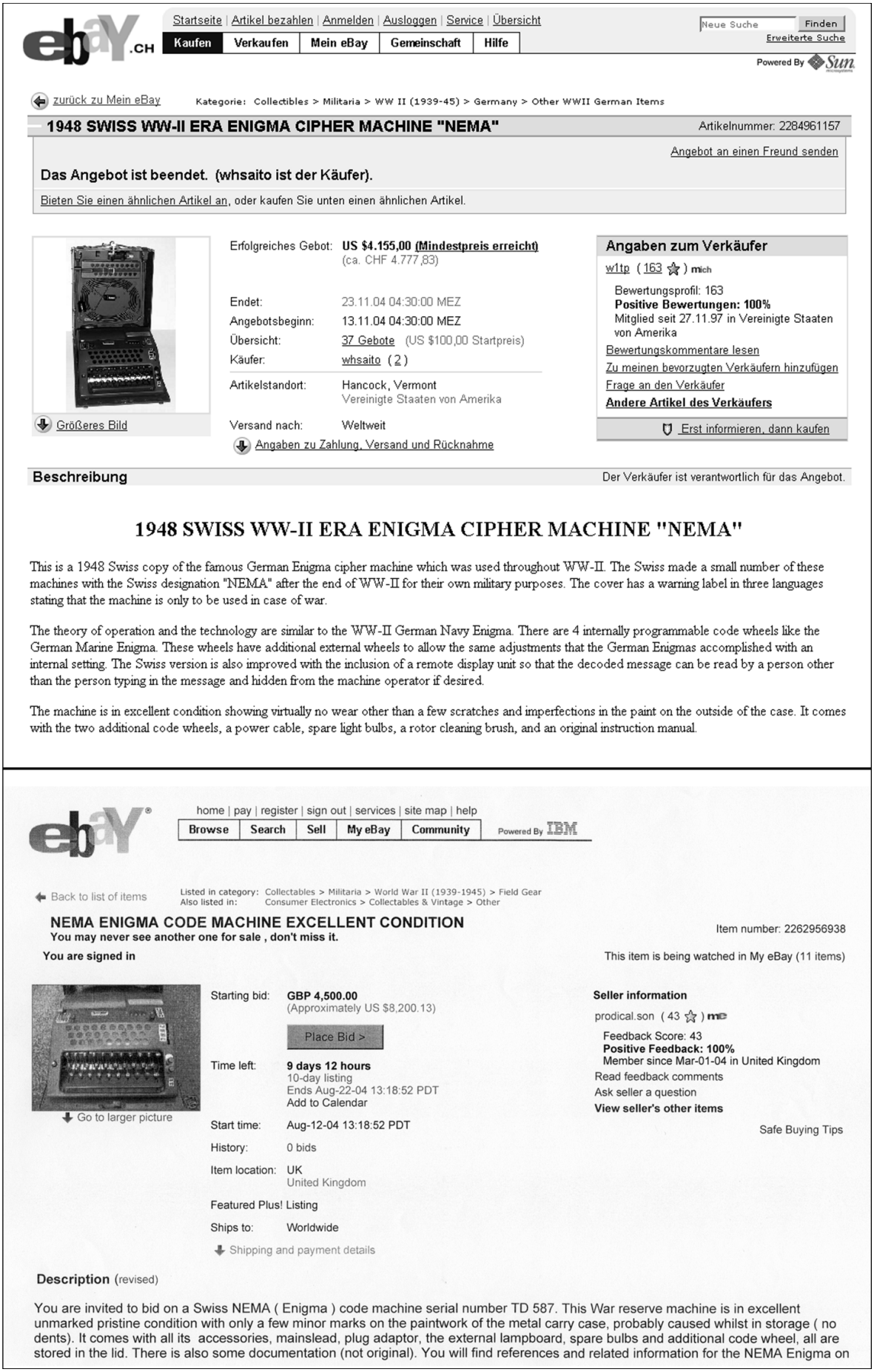
116 Anfang und Ende eines dreiseitigen Briefs. Die Angelegenheit war inzwischen zur Chefsache geworden. Nach der Expertise von Prof. Alder stand einer Vergütung an die Erfinder nichts mehr im Wege. [BAR]

Preisänderungen vorbehalten, sämtliche Artikel nur solange Vorrat

PREISLISTE **03.05.1994**

Anzahl	Artikel		Preis/Stk
___	Antenne zu SE 222, 13-teilig	Fr	10.–
___	Armeetelefon Modell 47 (max 2 Stk pro Person)	Fr	50.–
___	Chiffriermaschine NEMA (max 2 Stk pro Person) (am 4.5.94 nur 50.-)	Fr	150.–
___	Drehhocker	Fr	2.–
___	Eingrenzungsgerät EJ 83	Fr	10.–
___	Fernschreibertastgerät FSE 30 in Kiste	Fr	50.–
___	Handstanzer HDS-100P	Fr	40.–
___	Handstanzer HDS-12	Fr	40.–
___	Hilfsantenne AS 83 auf Wickler	Fr	2.–
___	Hochfrequenzempfänger 51j-4, E629	Fr	200.–
___	Impulsgenerator in Kiste	Fr	70.–
___	Kabeltrolle Metall mit verschiedenen Kabeln	Fr	10.–
___	Kabeltrolle mit 400m Telefonkabel, mit Auf -und Abspulvorrichtung (neu)	Fr	60.–
___	Kabeltrolle mit altem Telefonkabel ca 200m	Fr	5.–
___	Kabeltrolle mit Tragreff und Steckerkasten zu BB 65	Fr	20.–
___	Kabeltrollengestelle gross , teilweise mit Kabel	Fr	10.–
___	Kiste aus Aluminium leer, L40 B30 H35cm	Fr	5.–
___	Ladegerät zu BB 65	Fr	20.–
___	Ladegleichrichter No 61	Fr	20.–
___	Lärmgarnitur alt	Fr	5.–
___	Lärmgarnitur zu SE 206-209	Fr	5.–
___	Lenkgerät BB 65 (1 Stück pro Person)	Fr	40.–
___	Lochstanzer	Fr	30.–

117 Das letzte Kapitel der Geschichte. Im Mai 1994 wird die Nema an Sammler verkauft. Viele Maschinen kamen ins Ausland. [GSB]



Startseite | Artikel bezahlen | Anmelden | Ausloggen | Service | Übersicht

Kaufen | Verkaufen | Mein eBay | Gemeinschaft | Hilfe

Neue Suche | Finden | Erweiterte Suche

Powered By Sun

zurück zu Mein eBay

Kategorie: Collectibles > Militaria > WW II (1939-45) > Germany > Other WWII German Items

1948 SWISS WW-II ERA ENIGMA CIPHER MACHINE "NEMA" Artikelnummer: 2284961157

Angebot an einen Freund senden

Das Angebot ist beendet. (whsaito ist der Käufer).

Bieten Sie einen ähnlichen Artikel an, oder kaufen Sie unten einen ähnlichen Artikel.

Größeres Bild

Erfolgreiches Gebot: **US $4.155,00 (Mindestpreis erreicht)** (ca. CHF 4.777,83)

Endet: 23.11.04 04:30:00 MEZ

Angebotsbeginn: 13.11.04 04:30:00 MEZ

Übersicht: 37 Gebote (US $100,00 Startpreis)

Käufer: whsaito (2)

Artikelstandort: Hancock, Vermont, Vereinigte Staaten von Amerika

Versand nach: Weltweit

Angaben zu Zahlung, Versand und Rücknahme

Angaben zum Verkäufer

w1tp (163) mich

Bewertungsprofil: 163
Positive Bewertungen: 100%
Mitglied seit 27.11.97 in Vereinigte Staaten von Amerika

Bewertungskommentare lesen

Zu meinen bevorzugten Verkäufern hinzufügen

Frage an den Verkäufer

Andere Artikel des Verkäufers

Erst informieren, dann kaufen

Beschreibung Der Verkäufer ist verantwortlich für das Angebot.

1948 SWISS WW-II ERA ENIGMA CIPHER MACHINE "NEMA"

This is a 1948 Swiss copy of the famous German Enigma cipher machine which was used throughout WW-II. The Swiss made a small number of these machines with the Swiss designation "NEMA" after the end of WW-II for their own military purposes. The cover has a warning label in three languages stating that the machine is only to be used in case of war.

The theory of operation and the technology are similar to the WW-II German Navy Enigma. There are 4 internally programmable code wheels like the German Marine Enigma. These wheels have additional external wheels to allow the same adjustments that the German Enigmas accomplished with an internal setting. The Swiss version is also improved with the inclusion of a remote display unit so that the decoded message can be read by a person other than the person typing in the message and hidden from the machine operator if desired.

The machine is in excellent condition showing virtually no wear other than a few scratches and imperfections in the paint on the outside of the case. It comes with the two additional code wheels, a power cable, spare light bulbs, a rotor cleaning brush, and an original instruction manual.

home | pay | register | sign out | services | site map | help

Browse | Search | Sell | My eBay | Community

Powered By IBM

Back to list of items

Listed in category: Collectables > Militaria > World War II (1939-1945) > Field Gear
Also listed in: Consumer Electronics > Collectables & Vintage > Other

NEMA ENIGMA CODE MACHINE EXCELLENT CONDITION
You may never see another one for sale , don't miss it.

Item number: 2262956938

You are signed in

This item is being watched in My eBay (11 items)

Go to larger picture

Starting bid: **GBP 4,500.00** (Approximately US $8,200.13)

Place Bid >

Time left: **9 days 12 hours**
10-day listing
Ends Aug-22-04 13:18:52 PDT
Add to Calendar

Start time: Aug-12-04 13:18:52 PDT

History: 0 bids

Item location: UK
United Kingdom

Featured Plus! Listing

Ships to: Worldwide

Shipping and payment details

Seller information

prodical.son (43) me

Feedback Score: 43
Positive Feedback: 100%
Member since Mar-01-04 in United Kingdom

Read feedback comments

Ask seller a question

View seller's other items

Safe Buying Tips

Description (revised)

You are invited to bid on a Swiss NEMA (Enigma) code machine serial number TD 587. This War reserve machine is in excellent unmarked pristine condition with only a few minor marks on the paintwork of the metal carry case, probably caused whilst in storage (no dents). It comes with all its accessories, mainslead, plug adaptor, the external lampboard, spare bulbs and additional code wheel, all are stored in the lid. There is also some documentation (not original). You will find references and related information for the NEMA Enigma on

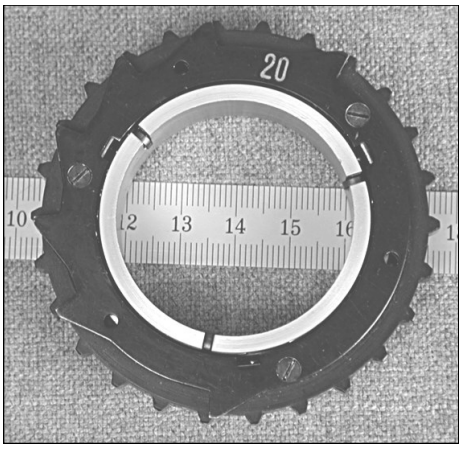
118 Die Nema ist bei Sammlern gesucht! Im WWW findet man gelegentlich eine Nema angeboten, hier zwei Beispiele. Im Moment liegt der Preis bei etwa 4'200 US$; er ist eher steigend. [WWW]

Zurückhaltung beim Telegrammverkehr! Nur ein nicht verschicktes Telegramm wird mit Sicherheit nicht gebrochen.

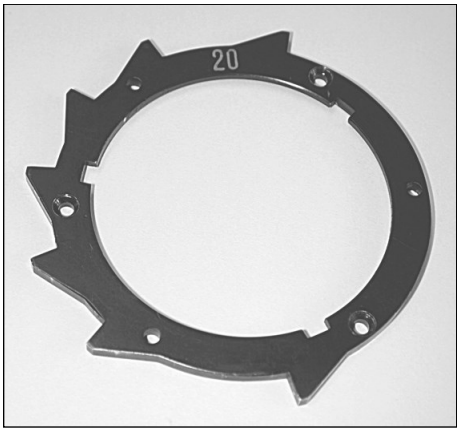
Anhang

Walzenvorschub der Nema

Abb. 121 zeigt das symbolische Prinzip der Vorschubmechanik. Der Antrieb der Walzen erfolgt über Zungen, die am Umfang auf eine Rasterung greifen und die Walzen weiterstossen. Aus diesem Grund können sich die Walzen nur in einer Richtung bewegen. Eine Mechanik verhindert, dass die Walzen bei einem zu kräftigen Tastendruck um mehr als einen Schritt weitertransportiert werden. Die Fortschaltwalzen werden von schmalen Zungen angetrieben, diejenigen für die Kontaktwalzen sind breiter. Die schmalen Zungen liegen immer an der Walze an und bewegen diese weiter, wenn die Zunge aktiv ist. Die breiten Zungen liegen zusätzlich über einer benachbarten Zahnscheibe (im Schema mit 'N' bezeichnet), die an der Fortschaltwalze angeschraubt ist. Abb. 119 zeigt eine Fortschaltwalze und Abb. 120 eine Zahnscheibe. Liegt ein Zahn (Nocken) unter der Zunge, wird diese angehoben und die Vorschubbewegung stösst ins Leere. Ein Vorschub der Kontaktwalzen erfolgt nur, wenn eine "Zahnlücke" vorhanden ist UND die Zunge eine Stossbewegung ausführt. Diese logische Verknüpfung ist durch das Zeichen '&' in einem Kästchen angedeutet. Die Fortschaltwalzen tragen nicht direkt zur Chiffrierung bei, ihre Aufgabe ist es, die Kontaktwalzen unregelmässig weiter zu bewegen.



119 Fortschaltwalze mit der Nocken- oder Zahnscheibe Nr. 20 versehen. [AUT]



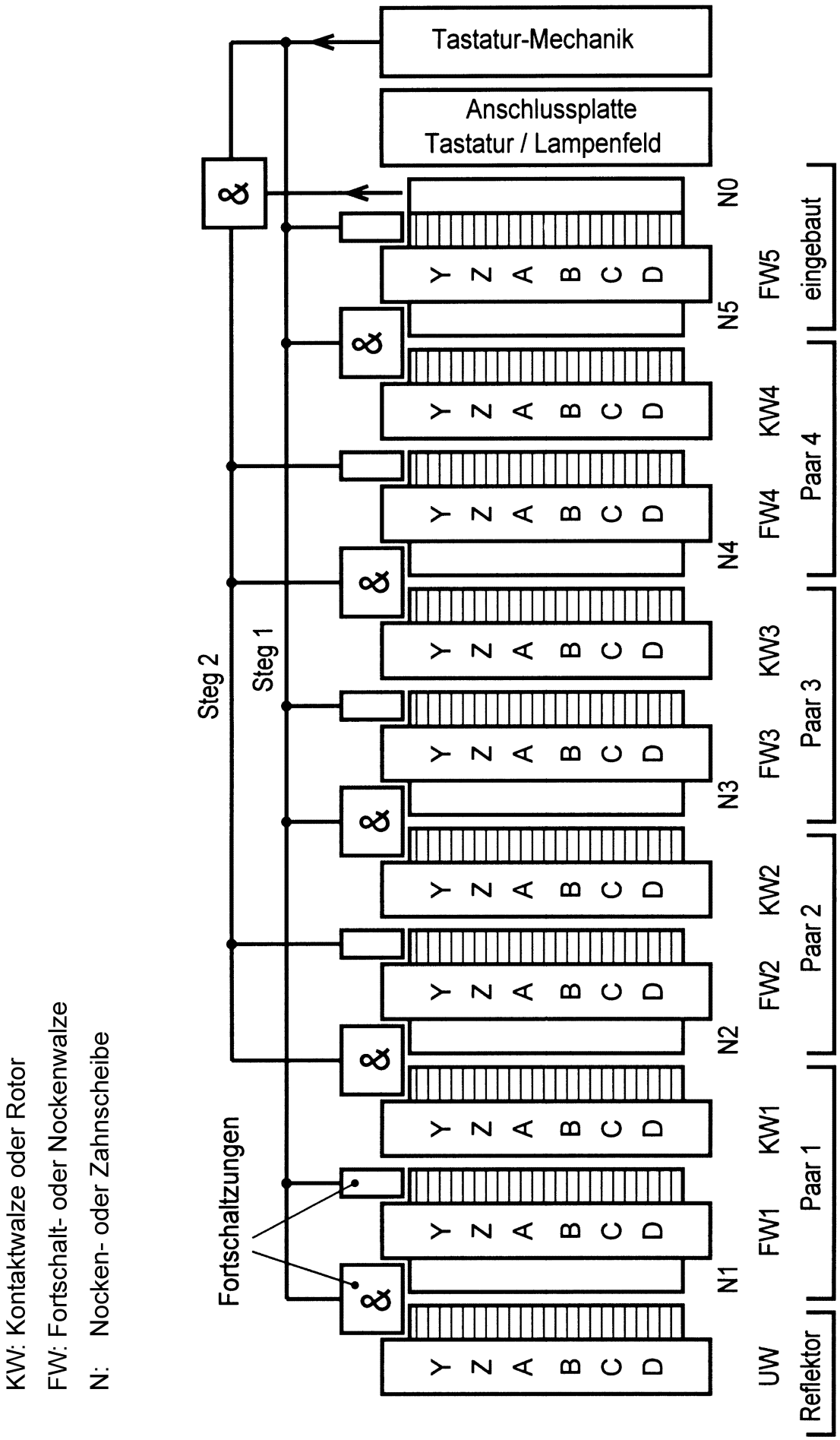
120 Eine Zahnscheibe, sie wird an die Fortschaltwalze geschraubt. [AUT]

Jede Tastenbetätigung erzeugt eine Fortschaltbewegung. Diese gelangt auf den Steg 1 und schaltet mit den schmalen Zungen die Fortschaltwalzen FW1, FW3 und FW5 weiter, die sich demnach bei jedem Tastendruck bewegen. Die Walze FW5 trägt auf beiden Seiten eine Zahnscheibe, jene rechts sorgt dafür, dass nur bestimmte Impulse auf den Steg 2 gelangen und die FW2 und FW4 weiterschalten. Diese beiden Fortschaltwalzen bewegen sich somit nicht bei jedem Tastendruck. Die Bewegung der Kontaktwalzen KW1 bis KW4 und der Umkehrwalze (drehbarer Reflektor) wird durch die rechts von ihnen liegende Zahnscheibe gesteuert und entweder über Steg 1 oder Steg 2 angetrieben. Mit dieser komplizierten Mechanik wird erreicht, dass die Bewegung der Walzen unregelmässig und undurchschaubar wird. Anderseits ergibt sich bei diesem System eine Periodendauer von $26^3 = 17'576$. Nach dieser Anzahl Tastenbetätigungen stehen alle Walzen wieder in ihrer Ausgangsposition.

Die rechts an der FW5 angebrachte Nockenscheibe hat relativ wenige Vertiefungen, deren fünf sind es beim Walzensatz der Schulmaschine. Auf eine volle Umdrehung dieser Walze (entsprechend 26 Tastenbetätigungen) werden demnach 5 Impulse auf den Steg 2 geleitet. Alle übrigen Nockenscheiben haben eher viele Vertiefungen, in der Grössenordnung von 17 bis 23. Jede Scheibe ist in der Form von den andern verschieden und besitzt eine andere Anzahl Vertiefungen. Beim Entwurf einer Zahnscheibe musste beachtet werden, dass die Anzahl der Vertiefungen ungerade und nicht 13 ist, (es darf kein Teiler von 26 sein) nur so wird die maximal mögliche Periodendauer von 17'576 erreicht.

Varianten der Fortschaltmechanik

Die in Abb. 121 und 122 gezeigten Fortschaltschemata sind eher symbolischer Art. Tatsächlich werden bei jeder Tastenbetätigung immer alle Zungen hochgestossen. Die



121 Fortschaltmechanik der Nema. [AUT]

Zur Periodendauer

Die Zeichnung 122 zeigt den Walzenantrieb der Nema in abstrakter Form. Mit der wirklichen mechanischen Ausführung der Maschine hat diese Darstellung nichts mehr zu tun. Sie dient lediglich dazu, die Logik des Walzenantriebs aus einer anderen Sicht zu zeigen und zu erklären, wie die Schlüsselperiode von 17'576 zustande kommt.

Die Tastatur treibt über eine Welle drei Zahnräder an, diese haben die fiktive Zähnezahl '1'. Pro Tastenbetätigung soll die Welle eine Umdrehung ausführen. Über einen formschlüssigen Antrieb, sei es ein Zahnriemen oder eine Zahnkette, werden die Fortschaltwalzen FW 1, FW 3 und FW 5 angetrieben. Entsprechend dem 26er-Raster der Walzen haben die angetriebenen Räder grundsätzlich 26 Zähne. FW 5 ist auf einer gemeinsamen Welle doppelt gezeichnet, einmal mit der Zahnscheibe 'L' und dann noch mit der Scheibe 'R'. In der Abb. 120 sind diese beiden Zahnscheiben als N5 und N0 bezeichnet. Diese drei (vier) Walzen gehören zur Gruppe 1 und werden von der Tastatur direkt angetrieben, pro Tastenbetätigung machen sie 1/26 Umdrehung, das entspricht bei den Walzen einem Vorschub von einem Schritt, von einem Buchstaben zum nächsten.

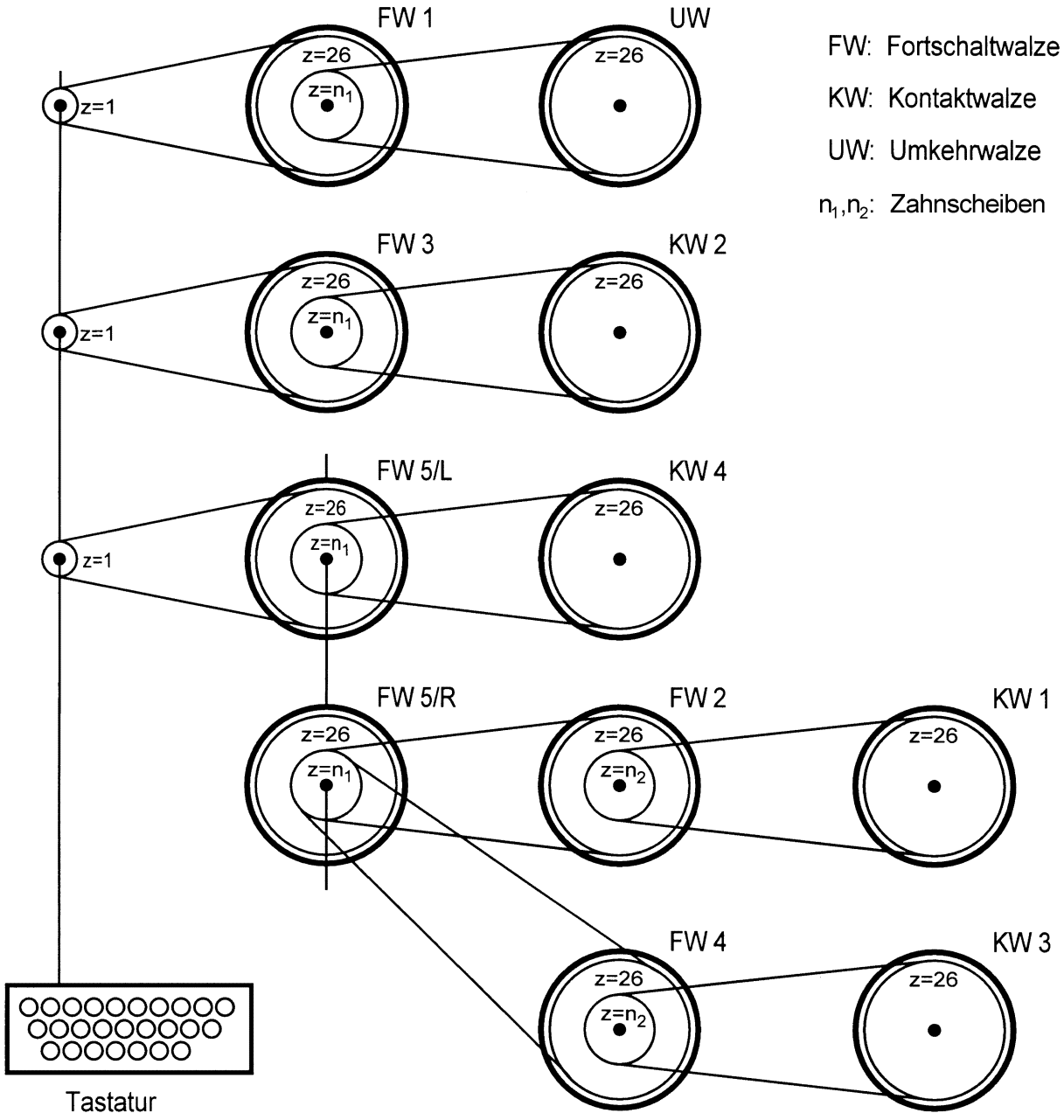
Die Walzen der Gruppe 2 werden von den Rädern der Gruppe 1 angetrieben. Die Zähnezahl 'n_1' der Treibräder entspricht der Anzahl Zahnlücken auf den Nockenscheiben und hat unterschiedliche Werte, der Index besagt hier nur, dass es sich um Räder der Gruppe 1 handelt. Die Walze FW 5/R treibt die zwei Fortschaltwalzen FW 2 und FW 4 an. Die Walzen der Gruppe 2 führen, wegen der Untersetzung, weniger Umdrehungen aus als die der Gruppe 1, nämlich pro Tastenbetätigung nur: $1/26 \cdot n_1/26$. Die beiden Walzen der Gruppe 3 werden in gleicher Weise von Rädern der Gruppe 2 angetrieben. Die Vorschubbewegung bei dieser Gruppe ist nochmals geringer als bei der Gruppe 2, pro Tastendruck sind es noch $1/26 \cdot n_1/26 \cdot n_2/26$ Umdrehungen. Das würde bedeuten, dass die Walzen der Gruppe 2 und 3 Bruchteile von Walzenschritten ausführen würden, denn 1/26 Umdrehung entspricht einem Schritt. Das ist natürlich nicht möglich, bei den angegebenen Formel handelt es sich um rein statistische Werte. Ein Beispiel soll das zeigen: Wenn bei einer FW die Zähnezahl z = 19 eingebaut ist, so bewirkt das, dass bei einer vollen Umdrehung (26 Schritte) dieser FW genau 19 ganze Vorschubtakte auf die angetriebene KW gelangen, oder anders ausgedrückt: nur bei 19 der 26 Tastenbetätigungen bewegt sich die KW um 1/26, bei den restlichen 7 Takten passiert nichts, es gibt nur ganze Vorschubschritte. Statistisch beträgt der Vorschub jedoch $1/26 \cdot 19/26 = 19/676$ Umdrehungen pro Takt. Die gleiche Überlegung gilt auch für die Walzen der Gruppe 3. Für unsere Betrachtung führen die "krummen" Vorschubschritte zu keinen Problemen; wir führen ohnehin so viele Tastenbetätigungen aus, dass die erfolgten Walzenrotationen in jedem Fall ganzzahlig sein werden.

Alle Walzen stehen wieder in der Ausgangslage

Die Schlüsselperiode ist dann erreicht, wenn alle Walzen wieder gleichzeitig auf ihrer Ausgangsposition stehen. Alle Walzen haben dann eine bestimmte, aber unterschiedliche Anzahl ganzer Umdrehungen ausgeführt. Man erkennt, dass die Formeln in der Tabelle Abb. 122 bei der Zeile "Umdrehungen pro Tastendruck" mit 17'576 erweitert werden müssen, damit in jedem Fall eine ganze Zahl erhalten wird. Bei den Walzen der Gruppe 2 wäre das zwar schon nach 676 Tastenbetätigungen der Fall, bei den Walzen der Gruppe 1 sogar schon nach deren 26.

Die Walzen der Gruppe 3 führen bei diesen 17'576 Tastenbetätigungen gegen 100 Umdrehungen aus, entsprechend dem Produkt "$n_1 \cdot n_2$". Sie führen demnach pro knapp 200 (17'576 / 100) Tastenbetätigungen eine volle Umdrehung aus. Nach dieser Anzahl Betätigungen steht wohl eine ausgewählte Walze wieder in ihrer Ausgangslage, aber die Stellung der restlichen neun Walzen ist unbestimmt, abhängig von den eingesetzten Nockenscheiben und deren Anfangsposition. Erst nach 17'576 Tastenbetätigungen stehen alle Walzen, unabhängig ihrer Ausgangslage und unabhängig der eingesetzten Fortschaltwalzen erstmals wieder in ihrer Ausgangsstellung. Es gibt keine kleinere Zahl, mit der das zu erreichen wäre. Das gilt allerdings nur dann, wenn alle 'n' teilerfremd sind zu 26 (ungerade und nicht 13), eine Bedingung die beim Entwurf der Nockenscheiben eingehalten werden musste.

Länger als 17'576 kann die Periodendauer in keinem Fall sein. Wenn die Forderung nach einer längeren Periodendauer gestellt würde, müssten weitere Gruppen eingeführt werden. Pro zusätzliche Gruppe würde sich die Periodendauer um den Faktor 26 vergrössern. Bei der gewählten Mechanik sind zusätzliche Gruppen nicht so leicht zu realisieren. Für eine längere Periode bestand jedoch niemals ein Bedarf, es wird wohl kaum je vorgekommen sein, dass mit der Nema ein Telegramm mit mehr als 17'576 Zeichen chiffriert wurde, schon aus Gründen des Zeitbedarfs wäre ein solches Unterfangen unsinnig! Die Länge der Periodendauer hat auf die kryptologische Sicherheit weder einen positiven noch einen negativen Einfluss.



Zugehörigkeit:	Gruppe 1	Gruppe 2	Gruppe 3
Antriebsart:	direkt	indirekt	doppelt indirekt
	Umdrehungen	Umdrehungen	Umdrehungen
Pro Tastendruck	1/26	$1/26 \cdot n_1/26$	$1/26 \cdot n_1/26 \cdot n_2/26$
Pro 26 "	1	$n_1/26$	$n_1/26 \cdot n_2/26$
Pro 676 "	26	n_1	$n_1 \cdot n_2/26$
Pro 17576 "	$26 \cdot 26$	$n_1 \cdot 26$	$n_1 \cdot n_2$

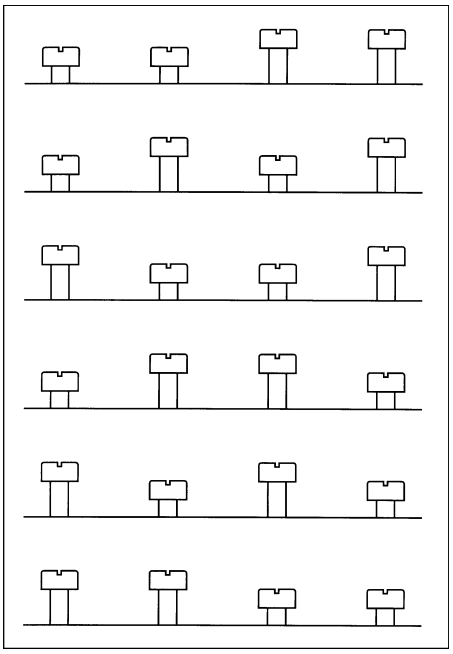
122 Das Vorschubsystem der Nema etwas anschaulicher dargestellt. [AUT]



123 "Service-Öffnung" auf der Rückseite der Nema. Die zehn Zungen, welche die Walzen weiterdrehen sind zu erkennen. Der Pfeil zeigt auf den Hebel 'A' der Abb. 126. [AUT]



124 Hier ist eine der vier Schrauben zu sehen, mit denen die Vorschubvariante eingestellt wird. [AUT]



125 Es gibt 6 Möglichkeiten, 2 von 4 Schrauben einzudrehen. [AUT]

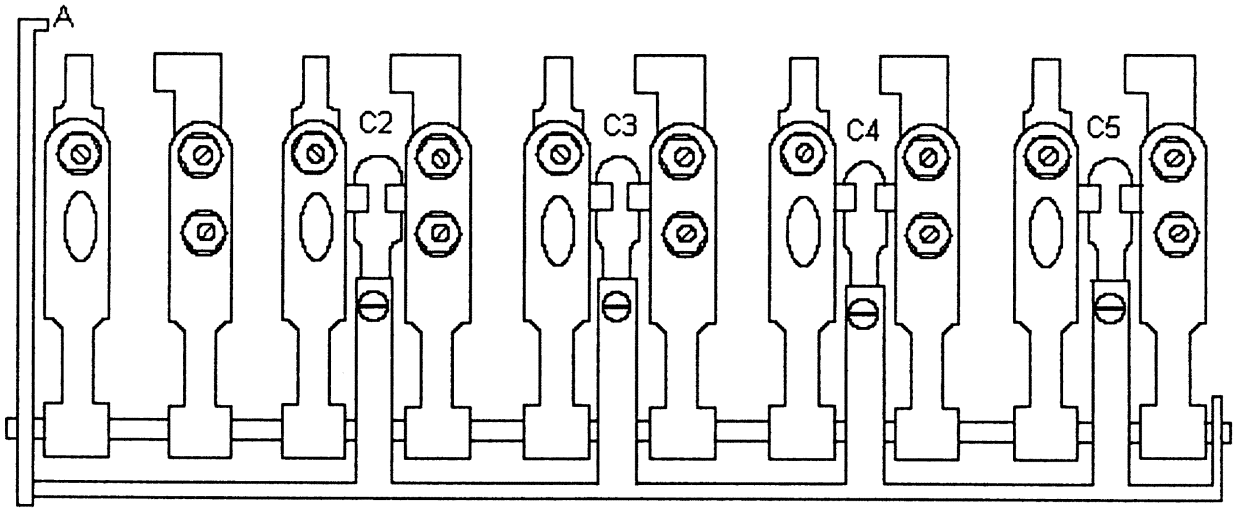
UND-Verknüpfung entsteht dadurch, dass die Zungen von den Walzen weggedrückt werden, so dass der Vorschub ins Leere stösst.

Wenn man die Maschine aus dem Koffer ausbaut, kann man hinten eine Abdeckung abschrauben und erhält dort Zugang zu den Zungen, siehe Abb. 123. Man erkennt die fünf schmalen und die fünf breiten Fortschaltzungen. Der Hebel 'A' (der Pfeil zeigt darauf), der von der Nockenscheibe N0 gesteuert wird, kann bestimmte Zungen wegdrücken. Sie bewegen sie sich dann zwar noch immer bei jedem Tastendruck, aber sie sind wirkungslos. Welche der Zungen von diesem Hebel beeinflusst werden, kann mit Schrauben (weiss eingekreist in Abb. 123 und 124) eingestellt werden. Die Schrauben sind entweder ein- oder ausgedreht und mit einer Kontermutter und Lack gesichert. Jede der Schrauben beeinflusst über einen Quersteg zwei Zungen, eine schmale für die Fortschaltwalze und eine breite für die benachbarte Kontaktwalze. Die rote Walze wird immer direkt angetrieben, ebenso die erste Kontaktwalze. Die Abb. 126 zeigt die Verhältnisse in einer technischen Zeichnung.

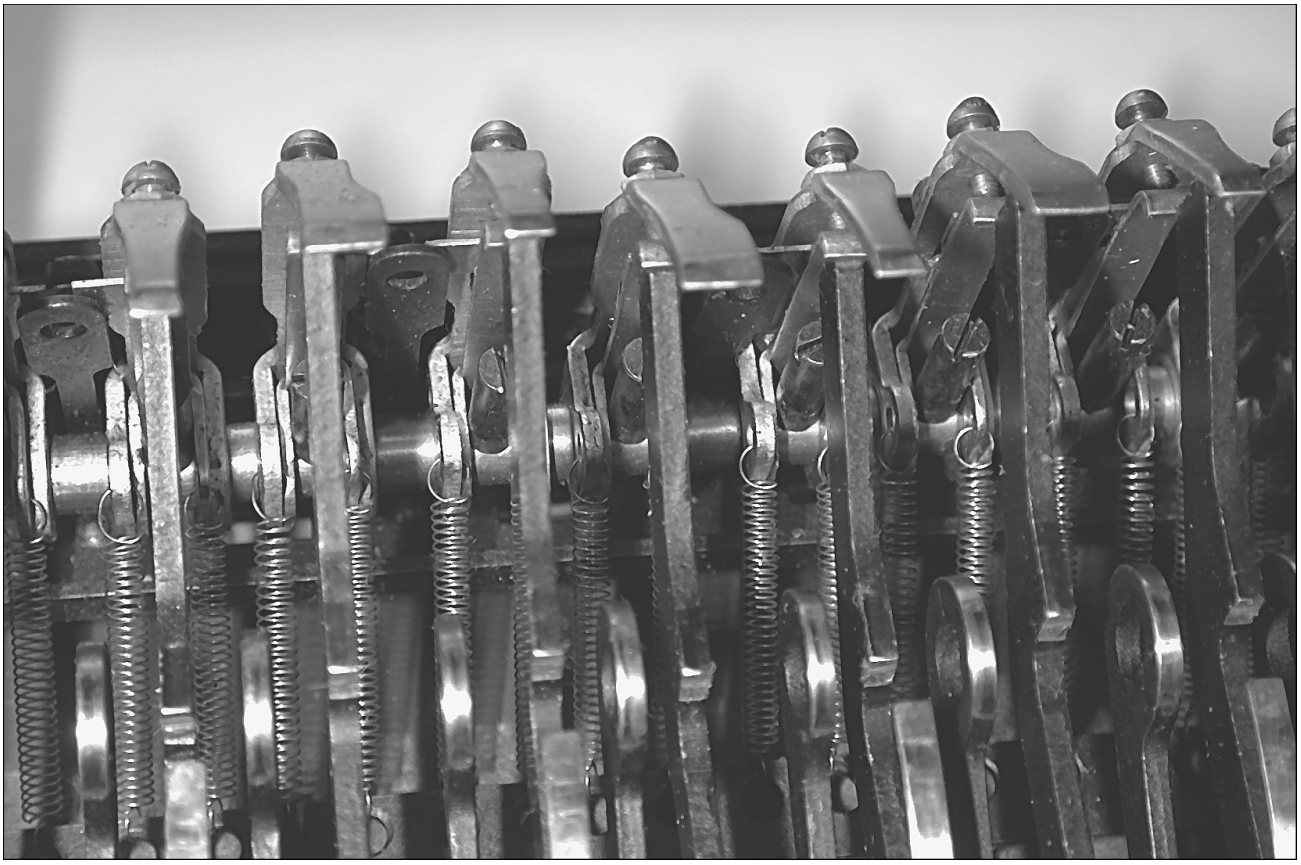
Die Botschaftsmaschinen waren anders eingestellt als die Militärmaschinen, bei der Maschine Nr. 117 vom diplomatischen Dienst konnte ich das feststellen. Wie man das mit wenigen Tastenbetätigungen herausfinden kann, ist auf Seite 87 beschrieben. Beim EPD waren drei verschiedene Maschinen-Varianten mit unterschiedlichen Walzen im Einsatz. Ob bei diesen drei Varianten auch der Fortschaltmechanismus unterschiedlich eingestellt war ist eher unwahrscheinlich, da schon die unterschiedlichen Walzensätze eine Nicht-Kompatibilität bewirkten, aber denkbar wäre es schon. Bei anderen als der erwähnten Maschine konnte ich die eingestellte Fortschaltvariante nicht überprüfen. Wenn man davon ausgeht, dass jeweils zwei der vier Steuerschrauben eingedreht sind, können sechs verschiedene Vorschub-Varianten realisiert werden, siehe Abb. 125. Bei den Botschafts-Maschinen waren auch die Umkehrwalzen anders verdrahtet als bei den Militärmaschinen, siehe Abb. 96, dort erkennt man die Umkehrwalze 'A'. Daneben standen im diplomatischen Netz noch die Umkehrwalze 'B' und 'T' im Einsatz.

Die Varianten beim Fortschaltmechanismus könnte man neben dem inneren und äusseren Schlüssel als dritten Schlüssel bezeichnen. Das wäre dann der Fabrikschlüssel, der nur von Fachspezialisten eingestellt würde. Da die Schrauben keinen definierten Anschlag haben, sind zur korrekten Einstellung der Fortschaltmechanik spezielle Werkzeuge und Einstell-Lehren erforderlich.

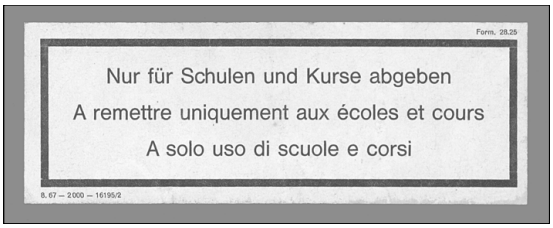
Eine Variation der Fortschaltmechanik trägt nicht viel zur Sicherheit bei, das war vermutlich auch nicht die Absicht. Es liesse sich damit aber z. B. verhindern, dass die Funker Telegramme mitlesen können, die aus einem anderen Netz stammen. Der Neugierde würde mit dieser Massnahme ein Riegel geschoben. Und das, obwohl in beiden Netzen die gleichen Walzen verwendet würden und der gleiche Schlüsselbefehl Geltung hätte.



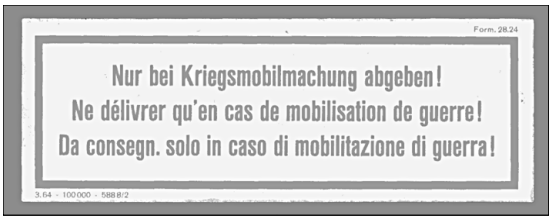
126 Die Zungensteuerung. Der Hebel 'A' (er wird gesteuert von der rechten Nockenscheibe an der roten Walze) drückt über ein Gestänge und die Platten C2, C3, C4 und C5 die Zungen von den Walzen weg, der Vorschub stösst dann ins Leere. Zwischen den Platten und dem Gestänge sind die vier Schrauben sichtbar für die Einstellung der Fortschaltmechanik. [17]



127 Blick aus der Rotoröffnung auf die Zungenmechanik. Gut zu erkennen sind die schmalen und breiten Zungen. Ganz links neben der schmalen Zunge eine der vier Platten, die die Zungen wegdrücken. Die Federn ziehen die Zungen an die Walzen. Mit verschiedenen Stellschrauben wird die Mechanik auf korrekte Funktion justiert. Die "Kellen" mit dem Loch, unten im Bild, drücken gegen die Walzen und erzeugen die Rastfunktion, mit der erreicht wird, dass die Walzen in nur in definierten Positionen stehen können. [AUT]



128 Klebezettel an einer Schul- oder Kursmaschine. Schwarze Schrift auf vergilbtem Weiss. [GSB]



129 Klebezettel an einer K-Mob-Maschine. Ziegelrote Schrift auf vergilbtem Weiss. [GSB]



130 Plombierbare Abdeckhauben für die zwei Reserve-Doppelwalzen, 78 x 28 mm. Oben Blick ins Innere der Haube. [AUT]

Varianten beim Walzensatz

Die Grundausführung der Nema wurde für verschiedene Einsatzgebiete mit unterschiedlichen Kontakt- und Fortschaltwalzen ausgerüstet. Bei den unterschiedlichen Walzen -Varianten sind teilweise auch unterschiedliche Einstellungen beim Fortschaltmechanismus anzutreffen.

Über die Ausrüstung der **Botschaftsmaschinen** ist wenig bekannt. Sicher ist, dass mindestens drei verschiedene Walzensätze im Einsatz standen, einer davon ist in den Abb. 95 und 96 zu sehen. Siehe auch Abb. 94, dort sind die inneren Schlüssel für drei Maschinen aufgeführt. Etwas mehr dazu ist in der Dokumentation "Botschaftsfunk damals" [20] zu finden.

Die **Schul- oder Kursmaschinen** des Militärs standen während etwa 30 Jahren bei der Truppe für die Instruktion und Übungen im Einsatz. An diesen Maschinen sind mehr oder weniger starke Gebrauchsspuren sichtbar. Alle Maschinen wurden jedoch immer gewartet und waren beim Verkauf in mechanisch einwandfreiem Zustand. Sie sind auf der Aussenseite des Koffers mit einem Klebezettel versehen. Er trägt den Hinweis (für das Zeughauspersonal), dass die Maschine nur an Schulen und für Kurse abgegeben werden dürfe, siehe Abb. 128. Diese Maschinen sind mit den folgenden Walzen ausgerüstet:

Kontaktwalzen:	A, B, C, D
Fortschaltwalzen:	16, 19, 20, 21, (23/2)

Die in Klammer gesetzten Angaben gelten für die rote Walze, die in der Maschine verbleibt und beidseitig mit einer Zahnscheibe ausgerüstet ist. Links trägt sie die Scheibe Nr. 23, rechts die Scheibe Nr. 2. Alle Zahnscheiben mit ein-stelligen Nummern können nur rechts an der roten Walze angeschraubt werden. Reserve-Walzen, Reserve-Zahnscheiben und Abdeckhauben waren bei den Schulmaschinen generell nicht vorhanden.

Die **K-Mob-Maschinen** (Kriegs-Mobilmachungs-Maschinen), auch K-Maschinen oder Kriegsmaschinen genannt, waren nie für Schulungen und Kurse im Einsatz. Auch an diesen Maschinen findet man einen Klebezettel. Auf weissem Grund ist in ziegelroter Schrift vermerkt, dass die Maschine nur bei einer Kriegs-Mobilmachung abgegeben werden dürfe, siehe Abb. 129. Das wäre bei einem Aufgebot der Truppe zu einem kriegsmässigen Einsatz der Fall gewesen. Bis 1992 waren die K-Mob-Maschinen in Waffenkammern eingelagert und befanden sich in absolut neuwertigem Zustand. Vor dem Verkauf im Jahre 1994 wurden sie dann leider teilweise unsachgemäss aufbewahrt. Aus diesem Grund findet man K-Mob-Maschinen, die Korrosionsschäden aufweisen. Diese Maschinen sind mit folgenden Walzen ausgerüstet:

Kontaktwalzen:	A, B, C, D, E, F
Fortschaltwalzen:	12, 13, 14, 15, 17, 18, (22/1)

Zwei Walzenpaare sind im Deckel unter zwei Hauben untergebracht, siehe Abb. 130. Gemäss Reglement sollten bei den Maschinen unter der mittleren Haube 8 Reserve-Zahnschei-

ben vorrätig sein. Bei keiner der Maschinen waren diese bei der Abgabe jedoch vorhanden. Der Grund für das Fehlen der Reserve-Zahnscheiben ist unklar. Es könnte durchaus sein, dass die Maschinen gar nie damit ausgerüstet waren. Die Montage der Zahnscheiben ist nicht einfach, man muss auf die korrekte Ausrichtung achten, siehe Abb. 131 und 132. Vielleicht traute man diese Arbeit den Soldaten im Feld nicht zu und lagerte deshalb die Zahnscheiben in den Zeughäusern ein; die Umrüstarbeit wäre dann von diesen Stellen vorgenommen worden. Denkbar ist auch, dass die Zahnscheiben vor dem Verkauf entfernt wurden, da es sich teilweise um die gleichen Scheiben gehandelte haben könnte, wie sie bei den diplomatischen Maschinen eingesetzt waren. Aber das traf auch für einen Teil der Kontaktwalzen zu: 'E' und 'F'; diese wurden jedoch in den Maschinen belassen.



131 Die Zahnscheiben mit zweistelliger Nummer werden links an den Fortschaltwalzen angeschraubt. Die Nummer muss bei 'U' zu liegen kommen. [AUT]

Es ist nicht bekannt und es deutet nichts darauf hin, dass jemals "**Hybride**" vorhanden waren, also Maschinen mit anderen als den in den Abb. 135 und 136 gezeigten Walzensätzen. Sollte jemals eine andere als die Originalbestückung angeboten werden, muss sie nach der Abgabe im Zeughaus von jemandem zusammengestellt worden sein. Eine Ausnahme bilden die Botschaftsmaschinen, aber die kamen nicht in den Verkauf. Anhand der in Abb. 94 gezeigten Liste mit "inneren Schlüssel" lässt sich feststellen, ob es sich dennoch um eine solche Maschine handeln könnte. Anhand der Maschinennummer kann eine Zuordnung nach den Angaben des folgenden Abschnitts erfolgen. Eine Überprüfung der Vorschubmechanik gibt weitere Aufschlüsse geben über die Herkunft:

- Den äusseren Schlüssel einstellen auf: "**A A A A A A A A A A**", "Leertaste" betätigen.
- 26 Tastenbetätigungen ausführen. Der Zähler muss jetzt auf 26 stehen.
- Bei den Militärmaschinen stehen die Walzen auf: "**x A x x x A x x x A**" (x bedeutet "unbestimmt")
- Eine Botschaftsmaschine zeigt die Walzenstellung: "**x x x A x x x A x A**"
- Bei einer anderen Walzenstellung kann es sich trotzdem um eine Botschaftsmaschine handeln. Es existierten drei verschiedene Walzensätze, möglicherweise für Maschinen mit unterschiedlichen Vorschubmechanismen.

Die Messing-Drahtbürste, Abb. 133, ist im Reglement nicht aufgeführt, im Ersatzteilkatalog dagegen ist sie enthalten.

Nummernzuteilung

Die 640 von der Kriegstechnischen Abteilung (K.T.A.) in Auftrag gegebenen Maschinen, siehe Abb. 108, wurden wie folgt eingesetzt:

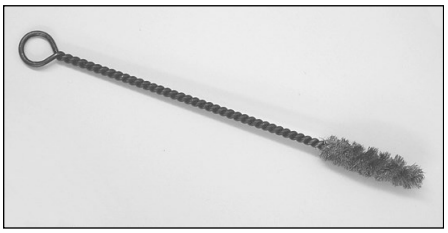
- Knapp 100 Stück waren beim EPD für den Verkehr mit den Botschaften (Funk, Draht und Briefpost), es handelte sich um die Nummern TD 100 bis gegen TD 199.
- TD 200 bis TD 419 waren als Schulmaschinen bei der Truppe im Einsatz. Zwischen 1947 und etwa 1975 wurden sie regelmässig bei den Übermittlungstruppen verwendet, am Schluss noch bei der Funkpolizei im Notfunknetz.
- TD 420 bis TD740 waren die K-Mob-Maschinen. Sie standen nie im Einsatz und waren immer in Waffenkammern sicher aufbewahrt.

Was geschah mit den Maschinen?

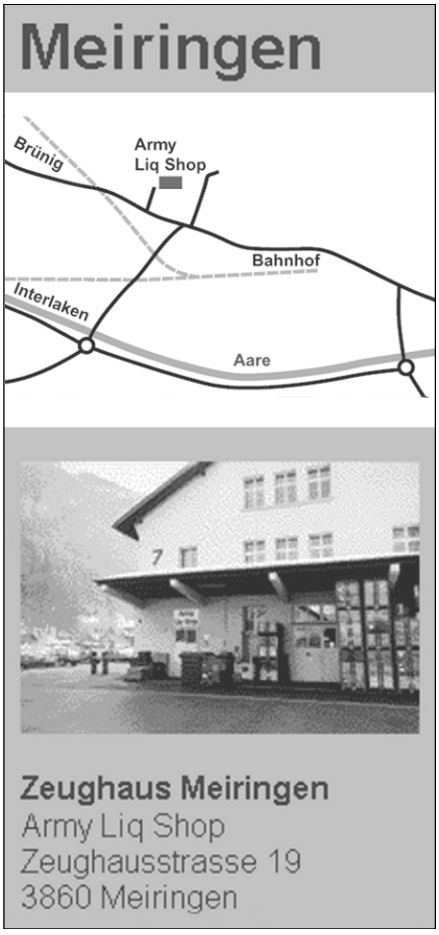
Mitte der 1970er-Jahre wurde die Nema aus ihren Einsätzen bei der Truppe und dem diplomatischen Dienst zurückgezogen. Nach einer längeren Sperrfrist entliess man die Maschinen am



132 Die Zahnscheiben mit einstelliger Nummer werden rechts an der roten Walze befestigt. Die Nummer muss bei 'L' zu liegen kommen. [AUT]



133 Messing-Drahtbürste, Länge 160 mm. Sie ist nicht bei allen Maschinen vorhanden. Wozu sie verwendet wurde, ist nicht so klar, für die Kontaktreinigung? [AUT]



134 In den Shops der Eidgenössischen Zeughäuser wird ausgemustertes Armeematerial verkauft. [www.armyliqshop.ch]

9. Juli 1992 aus der Geheimhaltung, siehe Entklassifizierungsstempel auf der Bedienungsanleitung, Abb. 55. Ein Teil der Auflage wurde später mit dem Entklassifizierungs-Datum 13. Feb. 1998 versehen.

Bei der Armee ist es üblich, dass geheimes Material nach dem Ausmustern vernichtet wird. Dieses Schicksal hätte auch die Nema ereilt. Die zuständigen Stellen erkannten jedoch, dass diese Maschine – auch wegen der Verwandtschaft zur berühmten Enigma – eine grosse historische Bedeutung besitzt. Es wurde deshalb angeordnet, dass die 220 Schul- und die 320 K-Mob-Maschinen an Sammler zu verkaufen seien. Verraten konnte man mit der Abgabe kaum etwas; die Maschinen waren entweder nie im Einsatz, oder dann nur für Übungszwecke benutzt worden.

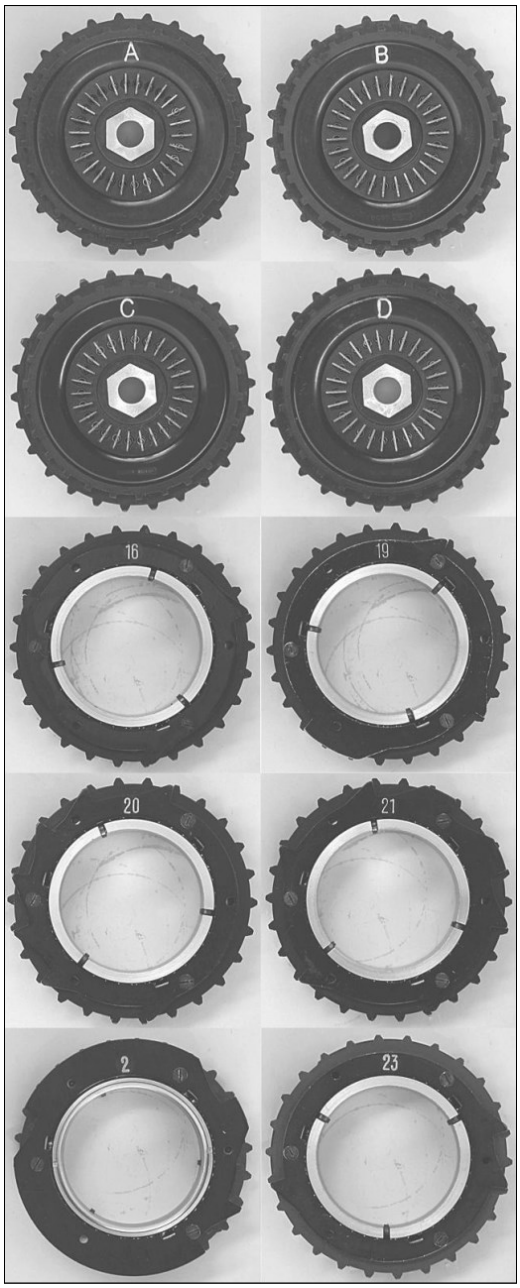
Die etwa 100 Botschaftsmaschinen dagegen wurden bis auf die TD 117 (siehe Abb. 93) und die TD 102 (gemäss Auskunft GSB) verschrottet. Bestimmt wollte man mit der Vernichtung verhindern, dass noch Jahrzehnte später der geheime Funkverkehr des Botschaftsfunks dechiffriert werden kann. Diese beiden letzten Zeitzeugen einer vergangenen Chiffrier-Ära werden als Erinnerungsstücke im Chiffrierbüro des früheren EPD, des heutigen EDA (Eidgenössisches Departement für Äusseres) aufbewahrt.

Der Verkauf von ausgemustertem Armee-Material findet in Liquidationsshops statt (www.armyliqshop.ch). Diese sind Eidgenössischen Zeughäusern angegliedert. In Meiringen wurde bis Ende 2004 vorwiegend technisches Material verkauft, siehe Abb. 117 und 134. Hier gelangten im Mai 1994 die Militär-Nemas und ein kleiner Posten von 25 Schweizer Enigmas zum Verkauf [19]. Das Interesse war gross, in kurzer Zeit waren alle Maschinen weg. Für die Nema wurden 150 Franken verlangt. Gemäss der handschriftlichen Notiz auf der Liste sollen die Maschinen am Eröffnungstag gar nur 50 Franken gekostet haben! Die Enigmas sind wegen der geringen Stückzahl nicht auf der Preisliste aufgeführt, sie sollen für etwa 300 Franken abgegeben worden sein. Das reichlich vorhandene Reserve- und Reparaturmaterial für die Nema fand ebenfalls Abnehmer. Heute sind keine Nemas oder Enigmas mehr erhältlich, Anfragen sind zwecklos, der Shop in Meiringen wurde geschlossen. In Sammlerkreisen sind originalgetreue Kopien des Ersatzteilkatalogs im Umlauf, siehe Abb. 137.

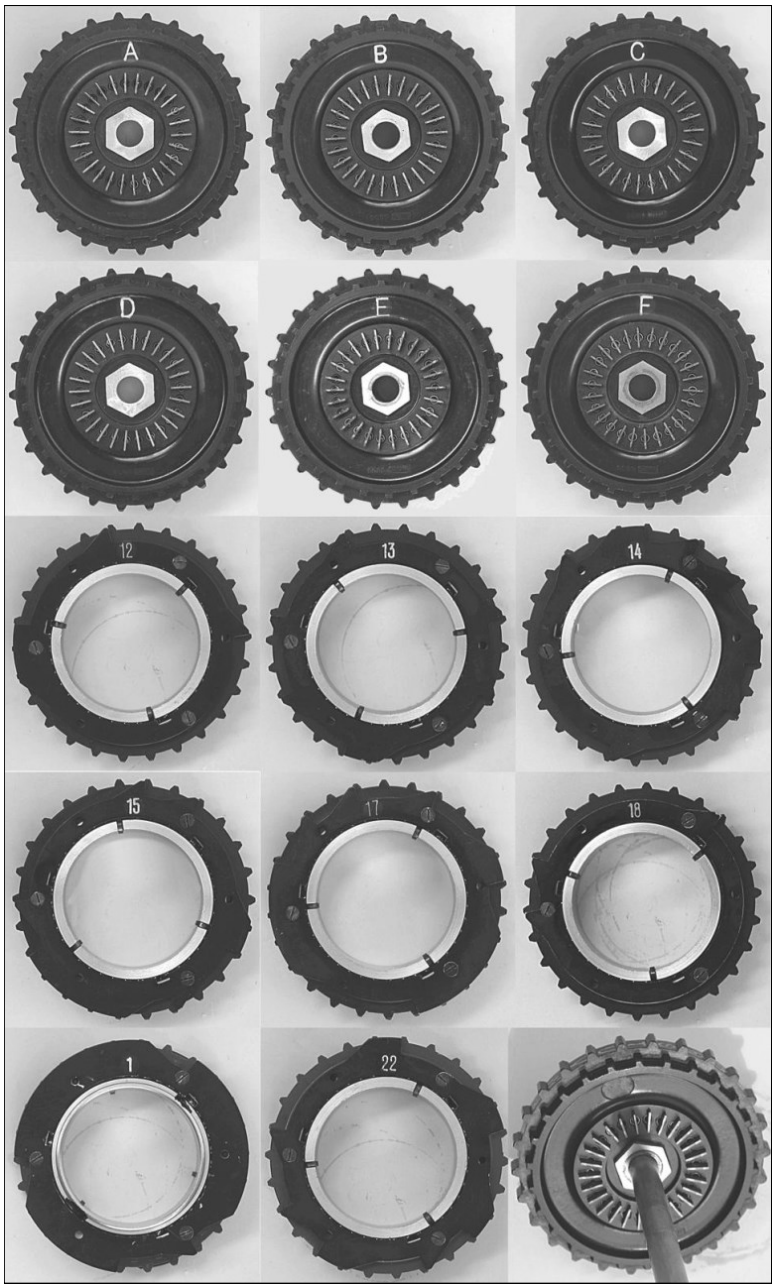
Die ehemaligen Militärmaschinen sind inzwischen weltweit im Besitz von Sammlern und Museen. Im Internet werden ab und zu Maschinen zum Kauf angeboten, siehe Abb. 118. Die Preise sind in den vergangenen Jahren stetig gestiegen und das Angebot wird geringer. Je nach Maschinentyp, Zustand und vorhandenem Zubehör werden einige tausend US-Dollar bezahlt. Die K-Mob-Maschinen sind geringfügig teurer als die Schulmaschinen. Zum Zubehör gehört die braune Bedienungsanleitung im Original, Abb. 55. Diese ist noch in grösseren Stückzahlen vorhanden, oft in ungebrauchtem Zustand. Die Schlüsselvorschrift, Abb. 82, ist im Original seltener zu finden. Ob sie zur Grundausrüstung der Nema gehörte ist unklar. Auf Grund der zugeteilten Nummer muss man das eher verneinen, das gezeigte Exemplar, Nr. 142, hätte dann nämlich zu einer diplomatischen Maschine gehört und wäre kaum von einer militärischen Stelle abgegeben worden.

Walzensätze der Militärmaschinen

Bei beiden Maschinentypen sind die Kontaktwalzen identisch, bei der K-Mob-Maschine ergänzt durch die Reservewalzen 'E' und 'F'. Die Fortschaltwalzen dagegen sind völlig unterschiedlich, ebenso die Zahnscheiben an den roten Walzen. Ein Austauschen des herausnehmbaren Walzenpakets ist deshalb nicht zulässig, es sei denn, man würde auch die rote Walze austauschen. Die Umkehrwalzen sind bei beiden Maschinentypen gleich. Es fällt auf, dass eine Bezeichnung an der Umkehrwalze fehlt, es sieht so aus, als sei sie weggefräst worden. Bei den Botschaftsmaschinen ist die Bezeichnung vorhanden, siehe Abb. 96.



135 Der Walzensatz der Schulmaschine. Die Umkehrwalze ist die gleiche wie bei der K-Mob-Maschine. Die rote Walze (23/2) ist von beiden Seiten abgebildet. [AUT]



136 Die Walzen der K-Mob-Maschine. Es sind die die beiden zusätzlichen Kontaktwalzen 'E' und 'F' vorhanden. Die Zahnscheiben sind alle verschieden zu denen der Schulmaschine. Auch hier ist die rote Walze (22/1) von beiden Seiten abgebildet. [AUT]

NUR FUER DIENSTLICHEN GEBRAUCH
A L'USAGE EXCLUSIF DU SERVICE

SCHWEIZERISCHE ARMEE / ARMEE SUISSE

ERSATZTEILKATALOG
CATALOGUE DE PIECES DE RECHANGE

ALN DES KATALOGES / NSA DU CATALOGUE:7610-607-0300

CHIFFRIERMASCHINE NEMA
MACHINE A CHIFFRER NEMA

ALN / NSA: 5810-607-0310



137 Der 38 Seiten umfassende Ersatzteilkatalog, siehe Literaturliste, Nachdruck GSB. [21]

Die letzten Geheimnisse der Nema

Wer selbst ein Simulationsprogramm schreiben möchte, benötigt zusätzliche Informationen, nämlich:

- Die Verdrahtungspläne der Kontaktwalzen
- Den Verdrahtungsplan der Umkehrwalze
- Die Verdrahtung Kontaktplatte – Tastatureinheit
- Die Position der Nocken auf den Fortschaltwalzen
- Die Arbeitsweise der Walzen-Fortschaltmechanik
- Die Verdrahtung und Steckerbelegung der Nema

Allgemein kann man den Chiffriervorgang bei der Maschine in zwei Schritte aufteilen:

- **Vorschub:** Bewegung der Walzen bei einem Tastendruck in Abhängigkeit der Stellung der Fortschaltwalzen.
- **Permutation:** Aufleuchten eines Lämpchens in Abhängigkeit der Stellung der Kontaktwalzen, der Umkehrwalze und der gedrückten Taste.

Die beiden genannten Funktionen werden in dieser Reihenfolge ausgeführt. Zuerst erfolgt ein kompletter Vorschubtakt. Sobald dieser durch die ganz niedergedrückte Taste abgeschlossen ist, wird ein Kontakt geschlossen, der das entsprechende Lämpchen aufleuchten lässt.

Nachfolgend stelle ich die beiden Funktionen "Vorschub" und "Permutation" an einem konkreten Beispiel vor. Die Erläuterungen dazu sind kompakt gehalten, sie sind als Hilfe gedacht zur Überprüfung der eigenen Überlegungen. Es ist von Vorteil, wenn man über eine Maschine verfügt, oder wenigstens über ein Simulationsprogramm. Sehr geeignet ist für diesen Zweck das Programm von Sullivan/Weierud, das ab Seite 106 vorgestellt wird. Die Betrachtungen gelten für eine K-Mob-Maschine, sie können sinngemäss auf die Schulmaschine übertragen werden, alle notwendigen Informationen sind in Tabellen vorhanden. Die Schlüssel werden auf die folgenden Werte eingestellt:

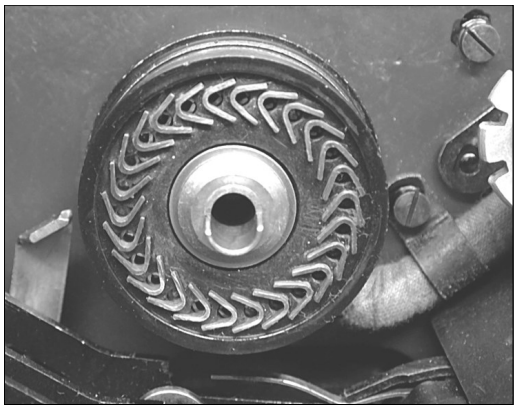
12-A / 13-B / 14-C / 15-D
D I S T E L F I N K

Bei der K-Mob-Maschine ist die rote Walze mit den beiden Zahnscheiben 22/1 ausgerüstet, die Schulmaschine trägt an dieser Stelle die Scheiben 23/2.

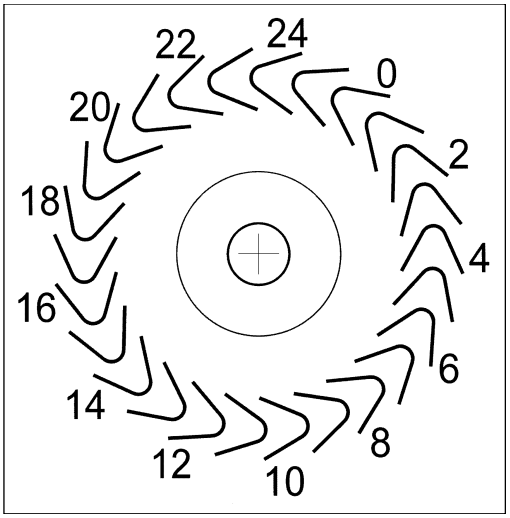
Beim Drücken einer Taste werden die Walzen hinten hochgestossen, deshalb bewegen sie sich bei einem Tastendruck "rückwärts". Aus der ursprünglichen Stellung 'A' dreht sich eine Walze durch die Vorschubbewegungen auf 'Z', 'Y', 'X' usw. und nicht etwa auf 'B', 'C', 'D' usw.

Abb. 138 zeigt die feststehende Kontaktplatte bei der roten Fortschaltwalze. Hier erfolgt der Übergang zur Kontaktwalze 4 (KW4) des eingesetzten Walzenpakets. Die Anschlussplatte ihrerseits steht in Verbindung mit den Umschaltern an den Typenhebeln, siehe Abb. 53 und 153.

Abb. 139 zeigt die für unsere Betrachtungen gewählte Nummerierung der Kontakte. Die Zeile des äusseren Schlüssels liegt auf der Position '0'. Die Wahl dieses Bezugsystems ist willkürlich, es gäbe gute Gründe, den Nullpunkt z. B. um 10 Einheiten gegen den Uhrzeiger nach hinten zu verlegen.



138 Die starre Anschlussplatte für das Walzenpaket. Die Kontakte führen zu den Tasten und den Lämpchen. Die rote Walze ist hier entfernt. [AUT]



139 Die willkürlich festgelegte Kontaktnummerierung bei der Anschlussplatte. [AUT]

Walze	U	FW1	KW1	FW2	KW2	FW3	KW3	FW4	KW4	FW5		Schritt
Nummer		12		13		14		15		22	1	
Initialschlüssel	D	I	S	T	E	L	F	I	N	K		
Wirksame Position		Y		J		B		Y		A	B	
Nocken		1		1		0		1		1	1	
Vorschub	+	+	+	+	--	+	+	+	+	+		
Neuer Schlüssel	C	H	R	S	E	K	E	H	M	J		1
Wirksame Position		X		I		A		X		Z	A	
Nocken		1		0		0		1		0	0	
Vorschub	+	+	--	--	--	+	--	--	--	+		
Neuer Schlüssel	B	G	R	S	E	J	E	H	M	I		2
Wirksame Position		W		I		Z		X		Y	Z	
Nocken		1		0		1		1		0	1	
Vorschub	+	+	--	+	+	+	+	+	--	+		
Neuer Schlüssel	A	F	R	R	D	I	D	G	M	H		3
Wirksame Position		V		H		Y		W		X	Y	
Nocken		1		0		0		0		1	1	
Vorschub	+	+	--	+	--	+	--	+	+	+		
Neuer Schlüssel	Z	E	R	Q	D	H	D	F	L	G		4
Wirksame Position		U		G		X		V		W	X	
Nocken		1		1		1		1		1	0	
Vorschub	+	+	--	--	+	+	--	--	+	+		
Neuer Schlüssel	Y	D	R	Q	C	G	D	F	K	F		5
Wirksame Position		T		G		W		V		V	W	
Nocken		0		1		0		1		1	0	
Vorschub	--	+	--	--	--	+	--	--	+	+		
Neuer Schlüssel	Y	C	R	Q	C	F	D	F	J	E		6

140 Schema zur Berechnung des Walzenvorschubs bei der Nema. [AUT]



141 Die Walzenstellung stimmt bei der realen Maschine mit den Berechnungen in obigem Schema überein. [AUT]

Berechnen des Walzenvorschubs

Aus den Vorschubschemata in Abb. 121 und 122 geht hervor, dass sich die Fortschaltwalzen FW1, FW3 und FW5 über den Steg 1 bei jedem Tastendruck bewegen. FW2 und FW4 drehen sich nur dann, wenn die Nockenscheibe N0 den Vorschubtakt auf den Steg 2 weiterleitet. Die Kontaktwalzen und die Umkehrwalze bewegen sich nur dann, wenn sich die rechts neben ihnen befindende Fortschaltwalze weiterbewegt UND deren Nockenscheibe den Vorschub frei gibt.

Die steuernden Nocken wirken nicht bei der Position '0', also auf der Position der Schlüsselzeile, sondern versetzt, hinten bei den Vorschubzungen.

Anhand des Schemas 140 wollen wir sechs Vorschubtakte berechnen, ausgehend vom Schlüssel "DISTELFINK". Als inneren Schlüssel verwenden wir die Angaben auf Seite 91.

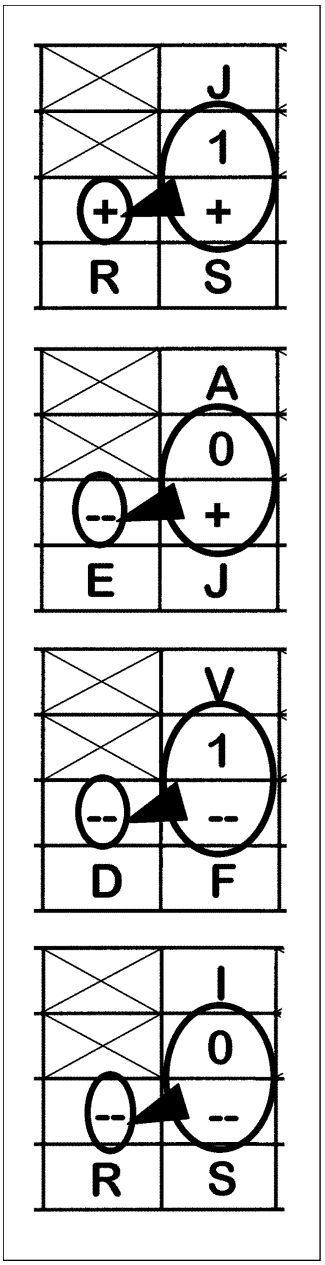
Zuerst wird die wirksame Position der Nocken bei den Fortschaltwalzen bestimmt. Die Scheiben mit den zweistelligen Nummern haben einen Versatz von 16 Einheiten. Bei der Nockenscheibe N0, beträgt der Versatz 17 Einheiten. Im Beispiel ist FW1 auf den Schlüssel 'I' eingestellt, der für die Steuerung wirksame Nocken befindet sich 16 Einheiten "weiter vorn" (J > K > L > M > N ... U > V > W > X > Y), also auf der Position 'Y'. Aus der Tabelle 146 kann für jede Scheibe die entsprechende Nockeninformation herausgelesen und im Schema eingetragen werden. Eine '1' bedeutet, dass ein Vorschub der benachbarten Walze stattfinden kann, die Zunge wird nicht angehoben. Bei einer '0' wird die Zunge angehoben, dadurch wird ein Vorschub verhindert, die Zunge stösst ins Leere. In der Tabelle finden wir für der Scheibe 12, Position 'Y', eine '1'; bei Nr. 14, unter 'B' eine '0' usw.

Da sich die Walzen FW1, FW3 und FW5 bei jedem Tastendruck bewegen, kann bei ihnen in der "Vorschubzeile" immer ein '+' eingesetzt werden. FW2 und FW4 erhalten ein '+', wenn in der "Nocken-Zeile" für die Scheibe Nr. 1 bei FW5 eine '1' eingetragen ist, andernfalls setzen wir ein '--'. Damit liegt fest, welche der fünf Fortschaltwalzen sich bewegen werden.

Die Kontaktwalzen und die Umkehrwalze erhalten ein '+' eingetragen, wenn die rechts von ihnen stehende Fortschaltwalze die Nockeninformation '1' trägt UND bei dieser im "Vorschub" ein '+' steht. Abb. 142 zeigt die vier Möglichkeiten, nur die erste erzeugt ein '+' im Vorschub. Nach dieser Logik kann die "Vorschubzeile" vervollständigt werden. Jede Walze, die im "Vorschub" ein '+' trägt, wird sich beim nächsten Tastendruck um eine Position "rückwärts" bewegen, die anderen bleiben stehen. Aus dem ursprünglichen Schlüssel "DISTELFINK" wird nach dem ersten Tastendruck "CHRSEKEHMJ". Gemäss diesem Muster werden die fünf weiteren Schritte berechnet. Nach dem sechsten Schritt steht der Schlüssel – nach unseren Berechnungen – auf "YCRQCFDFJE". Mit einem Simulator oder einer realen Maschine kann man sich vergewissern, dass dem tatsächlich so ist, siehe Abb. 141.

Die Kontaktwalzen haben keinen Einfluss auf die Vorschublogik. Wenn eine Kontaktwalze einen Vorschubschritt ausführen muss, wird dieser unabhängig von deren momentaner Position (Schlüsseleinstellung) gemacht.

In einem Computerprogramm kann es vorteilhaft sein, die Stellung der Walzen durch eine Zahl 0 ... 25 zu beschreiben. Der Zusammenhang ist aus der Tabelle 144 ersichtlich. Im nächsten Schritt, bei der Berechnung der Permutation, wird sich zeigen, dass dieses Vorgehen Vorteile bringt.



142 Auszug aus 140. Rechts die Spalte der Fortschaltwalze, nur die Kombination: Nocken (1) und Vorschub (+) erzeugt bei der KW oder UW (linke Spalte) ein (+) in der Vorschubzeile. [AUT])

Eingebaute Walze:	Um		A		B		C		D
Äusserer Schlüssel:	D	I	S	T	E	L	F	I	N	K
Nach Tastendruck:	C	H	R	S	E	K	E	H	M	J
Walzendrehung:	2		17		4		4		12	

Eingangstaste: G → Absolute Eingangsposition (AP) = 10

Absolute Position	Walzendrehung	Summe	Modulo 26	Eingang Walze	Offset in Walze	Absolute Position	Summe	Mod. 26 = AP neu	Bemerkung
10	12	22	22	W	10	10	20	20	D
20	4	24	24	Y	25	20	45	19	C
19	4	23	23	X	6	19	25	25	B
25	17	42	16	Q	21	25	46	20	A
20	2	22	22	W	5	20	25	25	Um
25	17	42	16	Q	5	25	30	4	A'
4	4	8	8	I	9	4	13	13	B'
13	4	17	17	R	22	13	35	9	C'
9	12	21	21	V	25	9	34	8	D'

Absolute Ausgangsposition: 8 → Lämpchen: J

143 Schema zur Berechnung der Permutation im Walzenpaket bei gegebener Walzenstellung. [AUT]

Berechnen der Permutation

Bei diesem Schritt wird rechnerisch der Strompfad verfolgt, der von einer gedrückten Taste durch das Walzenpaket zur Umkehrwalze und wieder zurück zu einem Lämpchen führt. Ausgehend von den bekannten Walzenstellungen und den ebenfalls bekannten Walzenverdrahtungen lässt sich dieser Pfad eindeutig bestimmen.

Als Beispiel soll bei eingestelltem Schlüssel "DISTELFINK" die Taste 'G' gedrückt werden. Der innere Schlüssel ist nach den Angaben auf Seite 91 eingestellt. Wir wollen berechnen, welches der Lämpchen aufleuchten wird. Es ist bekannt, dass der Stromkreis erst nach erfolgtem Walzenvorschub geschlossen wird. Im Abschnitt "Berechnen des Walzenvorschubs" haben wir festgestellt, dass der äussere Schlüssel nach einem Schritt auf "CHRSEKEHMJ" stehen wird, siehe Schema 140. Bei diesen Walzeneinstellungen führen wir unsere Berechnungen aus.

Zuerst wird der Drehwinkel der Umkehrwalze und der Kontaktwalzen bezüglich einer Referenzposition bestimmt. Diese definieren wir als die Stellung 'A' auf der Schlüsselzeile. Es wird festgestellt, um wie viele Schritte eine Walze gegenüber dieser Grundstellung 'A' gedreht ist. Steht eine Walze z. B. auf 'C', so beträgt die Verdrehung 2 Einheiten. Es wird von 'A' ausgehend in aufsteigender alphabetischer Folge gezählt. Die entsprechenden Werte werden für die Umkehrwalze und die Kontaktwalzen im Schema Abb. 143 eingetragen. Die Stellung der Fortschaltwalzen interessiert uns bei dieser Berechnung nicht, diese sind für die Permutation bedeutungslos.

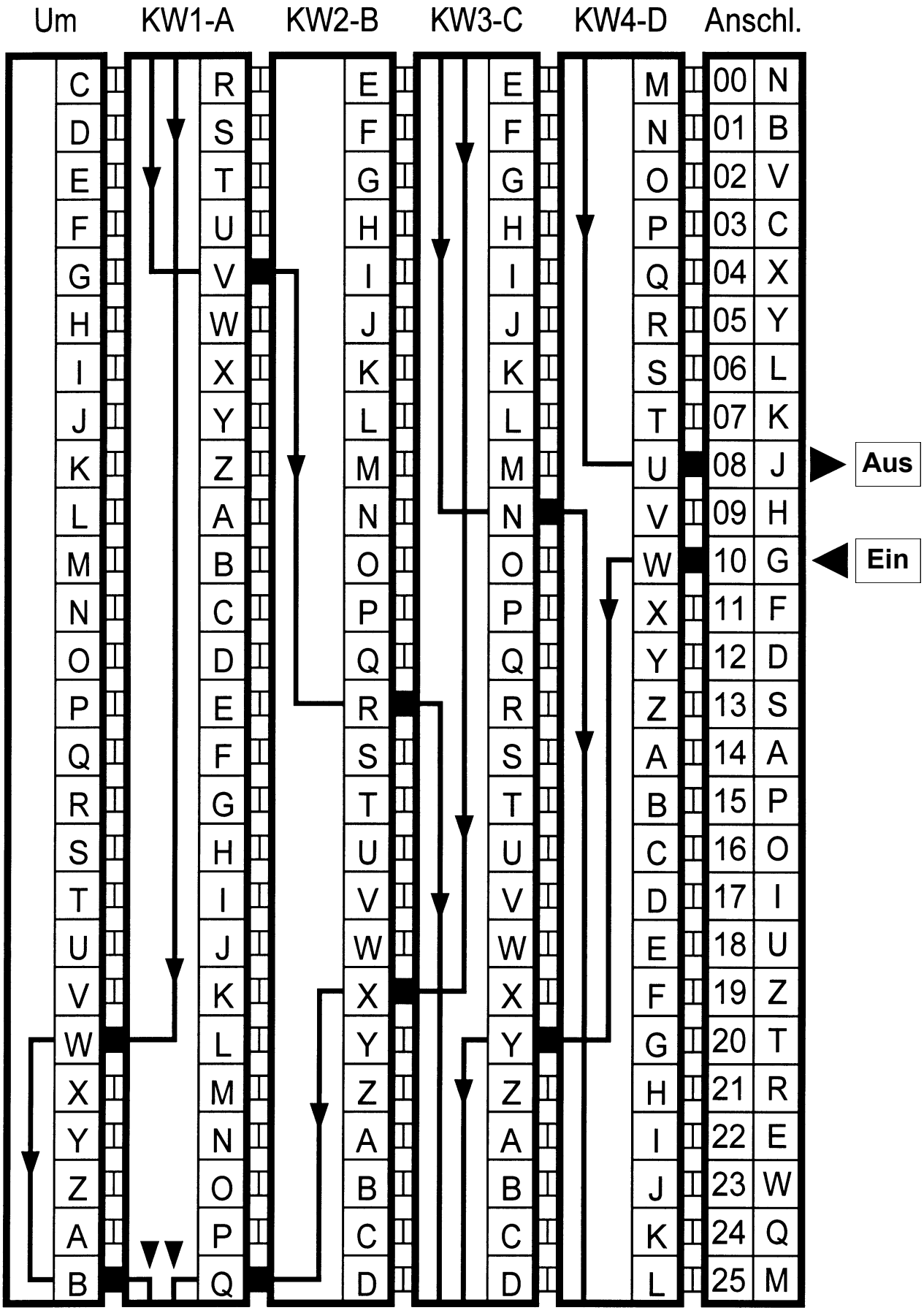
Der Weg des Stroms beginnt bei der Taste 'G'. Der Tabelle 147 entnimmt man, dass diese Taste mit dem Kontakt 10 der Anschlussplatte verbunden ist. Im Schema 143 wird dieser Wert als absolute Position (AP) eingetragen. Mit der Anschlussplatte steht die Kontaktwalze 4 in Verbindung, in unserem Beispiel ist das die Walze 'D'. Zuerst müssen wir wissen, welcher Walzenkontakt den Plattenkontakt 10 berührt. Wäre die Walze in der Grundstellung 'A' würde der Strom bei der Position '10' d. h. bei 'K' (Abb. 144) in die Walze eintreten. Da die Walze um 12 Einheiten gedreht ist, steht der Plattenkontakt 10 mit dem Walzenkontakt 22 in Verbindung, der Summe aus 10 + 12. Sollte dieser Wert grösser als 25 werden, wird 26 subtrahiert, er wird modulo 26 genommen. Das Ergebnis muss immer zwischen 0 und 25 liegen. Bei allen Walzen ist die Position 22 mit 'W' identisch. In der Tabelle 148 finden wir, dass die Walze 'D' eine Verbindung hat von 'W' nach 'G' (vom Eingang rechts zum Ausgang links). Man kann auch sagen, dass der Offset in der Walze 10 Einheiten betrage, von 'W' sind 10 Schritte vorwärts zu zählen um nach 'G' zu gelangen. Diesen Wert (er steht in der Tabelle) tragen wir als "Offset" im Schema ein. Die absolute Position des Austritts aus der Walze 'D' ergibt die Addition: AP + Offset = 10 + 10 = 20. Auch hier wird modulo 26 gerechnet. Der Wert 20 ist die absolute Position für den Eingang in die nächste Walze, im Beispiel also in 'C'.

Die gleiche Berechnung wird für die verbleibenden drei Kontaktwalzen durchgeführt. Anschliessend durchläuft man die Umkehrwalze in analoger Weise, die notwendigen Informationen finden sich in der Tabelle 149. Dann geht es in umgekehrter Richtung durch die vier Kontaktwalzen zurück zur Kontaktplatte. Zur Bestimmung des Offsets verwenden wir jetzt die Angaben in der Tabelle 150. Die Tabellen 148 und 150 sind im Grunde identisch. Einmal ist die Darstellung so gewählt, dass die Kontakte auf der rechten Seite alphabetisch geordnet sind, im andern Fall sind sie auf der linken Seite geordnet. Die Summe der Offsets aus einem Hin- und Rückweg muss 26 ergeben. Bei der Walze 'D' beträgt der Offset 'W' -> 'G' 10 Einheiten, von 'G -> 'W' sind es deren 16. Die Summe beträgt somit 26 Einheiten (oder NULL, wenn modulo 26 gerechnet wird).

Am Schluss erhält man die absolute Position, bei der das Signal wieder an der Anschlussplatte ankommt. Im Beispiel ist es die Position 8. Aus der Tabelle 151 lässt sich ablesen, dass der Kontakt 8 der Anschlussplatte zum Lämpchen 'J' führt. Auch die Tabellen 147 und 151 enthalten im Grunde die gleichen Informationen, lediglich die

A — 00
B — 01
C — 02
D — 03
E — 04
F — 05
G — 06
H — 07
I — 08
J — 09
K — 10
L — 11
M — 12
N — 13
O — 14
P — 15
Q — 16
R — 17
S — 18
T — 19
U — 20
V — 21
W — 22
X — 23
Y — 24
Z — 25

144 Buchstaben lassen sich durch Zahlen ersetzen. [AUT]



145 Das Berechnungsschema nach Abb. 143 ist hier in grafischer Form dargestellt. [AUT]

Darstellung ist anders, nämlich so, dass man, resp. ein Computerprogramm, leichter den Zugang findet.

In Abb. 145 ist der geschilderte Vorgang als Grafik dargestellt. Man kann sich vorstellen, dass die Walzen bei der Schlüsselzeile aufgetrennt und "abgewickelt" sind. Bei 'G' tritt das Signal in das Walzenpaket ein und durchläuft die Kontaktwalzen und die Umkehrwalze. Die Verbindungen in den Walzen sind so gezeichnet, dass das Signal immer "von oben nach" unten läuft, d. h. einen positiven Offset aufweist. Wenn eine Verbindung die Walze unten verlässt, tritt sie oben wieder ein. Bei einem solchen "Übertrag" wird das Rechenergebnis in der Tabelle 143 grösser als 25 und das Resultat muss modulo 26 genommen werden. Bei der KW3-C ist das besonders deutlich: Die Verbindung läuft von 'Y' nach 'X' und hat demnach einen Offset von 25. Man könnte die Verbindung auch "rückwärts" einzeichnen, von 'Y' direkt nach 'X' mit einem Offset von -1. Im Hinblick auf eine Programmierung ist es jedoch günstiger, konsequent mit positiven Offsets zu arbeiten.

Mit den Grundlagen für die Berechnung des Walzenvorschubs und der Permutation sind wir in der Lage ein Modul zu programmieren, mit dem man chiffrieren und dechiffrieren kann. Natürlich gehören zu einem Simulator noch viele andere Funktionen, etwa die Einstellung der Schlüssel, die Lämpchenanzeige usw.

Nr.	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

146 Angaben für die Fortschaltwalzen. Eine '1' bedeutet, dass kein Nocken vorhanden ist, die Zunge liegt an der Walze an, ein Vorschub kann stattfinden. Eine '0' steht für einen Nocken, die Zunge wird angehoben, der Vorschub wird unterdrückt. [AUT]

Tabellen für Programmierer

Die Tabellen 146 bis 151 enthalten Informationen zur Zuordnung Taste/Lämpchen/Kontaktplatte, sowie Angaben über die Fortschalt- und Kontaktwalzen. Die Beschreibung der Verbindungen in den Kontaktwalzen kann man auf verschiedene Art vornehmen, abweichend ist z. B. die Form in [17]. Man darf sich nicht verwirren lassen, letztlich handelt es sich um die gleiche Information. Man findet schnell heraus, wie die beiden Formen ineinander überführt werden können.

Tasten

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
14	1	3	12	22	11	10	9	17	8	7	6	25	0	16	15	24	21	13	20	18	2	23	4	5	19

Anschlussplatte

147 Die Kontaktbelegung auf der Anschlussplatte, alphabetisch nach Tasten geordnet. [AUT]

Kontakt auf der rechten Seite

Walze	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
A	N	S	K	I	T	C	O	Y	M	V	W	A	U	J	D	R	L	Z	X	H	F	Q	E	G	P	B
	13	17	8	5	15	23	8	17	4	12	12	15	8	22	15	2	21	8	5	14	11	21	8	9	17	2
B	K	J	Y	N	T	M	E	H	L	O	Z	Q	B	W	P	S	X	I	R	F	A	G	U	D	V	C
	10	8	22	10	15	7	24	0	3	5	15	5	15	9	1	3	7	17	25	12	6	11	24	6	23	3
C	P	N	F	U	T	E	D	I	Z	Y	A	H	V	R	W	O	J	S	G	B	Q	M	K	C	X	L
	15	12	3	17	15	25	23	1	17	15	16	22	9	4	8	25	19	1	14	8	22	17	14	5	25	12
D	W	J	B	E	Y	F	U	C	M	D	T	A	Z	K	X	P	I	Q	H	S	V	L	G	O	N	R
	22	8	25	1	20	0	14	21	4	20	9	15	13	23	9	0	18	25	15	25	1	16	10	17	15	18
E	H	R	Q	T	Y	V	X	M	N	A	C	F	U	J	E	S	W	L	Z	I	G	D	P	O	K	B
	7	16	14	16	20	16	17	5	5	17	18	20	8	22	16	3	6	20	7	15	12	8	19	17	12	2
F	Z	V	G	E	Q	M	U	T	W	L	N	S	H	P	O	A	F	Y	I	X	K	B	D	R	J	C
	25	20	4	1	12	7	14	12	14	2	3	7	21	2	0	11	15	7	16	4	16	6	7	20	11	3

führt zu Kontakt auf der linken Seite

148 Die Verdrahtung der Kontaktwalzen, alphabetisch geordnet nach den Eingängen auf der rechten Seite. Die Zahl gibt den Offset an. [AUT]

Umkehrwalze

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
K	W	P	N	G	H	E	F	V	T	A	Z	U	D	Y	C	X	S	R	J	M	I	B	Q	O	L
10	21	13	10	2	2	24	24	13	10	16	14	8	16	10	13	7	1	25	16	18	13	5	19	16	12

149 Die Verdrahtung der Umkehrwalze, die Zahl gibt den Offset an. [AUT]

Kontakt auf der linken Seite

Walze	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
A	L	Z	F	O	W	U	X	T	D	N	C	Q	I	A	G	Y	V	P	B	E	M	J	K	S	H	R
	11	24	3	11	18	15	17	12	21	4	18	5	22	13	18	9	5	24	9	11	18	14	14	21	9	18
B	U	M	Z	X	G	T	V	H	R	B	A	I	F	D	J	O	L	S	P	E	W	Y	N	Q	C	K
	20	11	23	20	2	14	15	0	9	18	16	23	19	16	21	25	21	1	23	11	2	3	17	19	4	11
C	K	T	X	G	F	C	S	L	H	Q	W	Z	V	B	P	A	U	N	R	E	D	M	O	Y	J	I
	10	18	21	3	1	23	12	4	25	7	12	14	9	14	1	11	4	22	25	11	9	17	18	1	11	9
D	L	C	H	J	D	F	W	S	Q	B	N	V	I	Y	X	P	R	Z	T	K	G	U	A	O	E	M
	11	1	5	6	25	0	16	11	8	18	3	10	22	11	9	0	1	8	1	17	12	25	4	17	6	13
E	J	Z	K	V	O	L	U	A	T	N	Y	R	H	I	X	W	C	B	P	D	M	F	Q	G	E	S
	9	24	8	18	10	6	14	19	11	4	14	6	21	21	9	7	12	10	23	10	18	10	20	9	6	19
F	P	V	Z	W	D	Q	C	M	S	Y	U	J	F	K	O	N	E	X	L	H	G	B	I	T	R	A
	15	20	23	19	25	11	22	5	10	15	10	24	19	23	0	24	14	6	19	14	12	6	12	12	19	1

führt zu Kontakt auf der rechten Seite

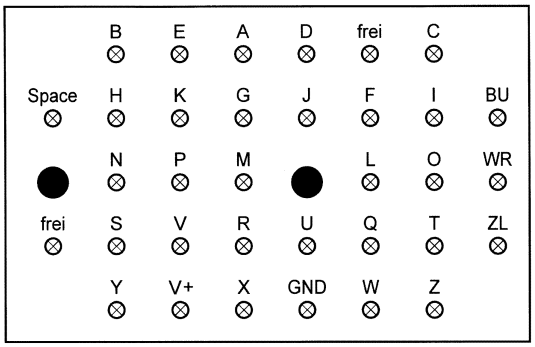
150 Die Verdrahtung der Kontaktwalzen, alphabetisch geordnet nach den Eingängen auf der linken Seite. Die Zahl gibt den Offset an. [AUT]

Anschlussplatte

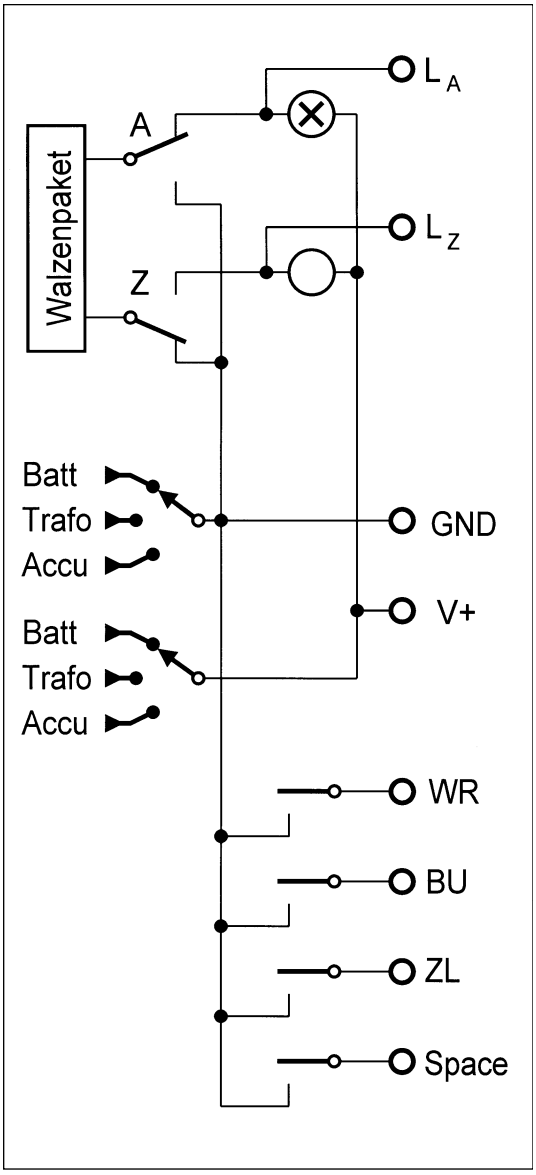
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N	B	V	C	X	Y	L	K	J	H	G	F	D	S	A	P	O	I	U	Z	T	R	E	W	Q	M

Lämpchen

151 Die Kontaktbelegung der Anschlussplatte, geordnet nach der Nummer der Anschlusskontakte. [AUT]



152 Die Belegung des Steckers an der Nema. [AUT]



153 Die Interne Verdrahtung und die Steckerbelegung bei der Nema, vereinfacht dargestellt. [AUT]

Elektrische Verdrahtung

Das Prinzip der elektrischen Verbindungen wurde schon auf der Seite 34 dargestellt, kompliziert ist die Sache nicht.

Über den Stecker des Zusatzlampenfeldes hat man Zugang zu wichtigen Stellen der Verdrahtung im Innern der Maschine. Abb. 152 zeigt die Belegung des Steckers. Im Schema 153 sind die Verhältnisse vereinfacht dargestellt, es sind nur 2 der 26 Lämpchen gezeichnet. Die vier speziellen Tasten: Space (lange Taste), BU, WR und ZL haben für die Nema keine Bedeutung, sie betätigen lediglich Kontakte, diese sind auf den Stecker geführt. Die Speisespannung ist über den Stecker zugänglich, im Schema sind die entsprechenden Anschlüsse mit 'GND' und 'V+' bezeichnet. Es besteht somit die Möglichkeit, aus der Maschine Strom zu beziehen, oder die Nema über den Stecker mit einer externen Speisespannung zu versorgen. Einige Punkte sind zu beachten, wenn man über den Stecker Anschlüsse herstellt:

- Zur Speisung wird eine Gleich- oder eine Wechselspannung verwendet, je nach gewählter Versorgungsquelle.
- Die Polarität der Speise-Gleichspannung ist nicht definiert, wie es das Schema vorgibt. Eine Flachbatterie kann "auf dem Bauch" oder "auf dem Rücken" liegend eingebaut werden. Das beeinflusst die Funktion der Maschine nicht, die Polaritätsverhältnisse dagegen werden invertiert. Für die externe 4V-Quelle besteht keine Vorschrift bezüglich Polarität oder Stromart. Der eingebaute Trafo liefert eine Wechselspannung, es erfolgt keine Gleichrichtung.
- Die Kontaktwiderstände bei den Tasten und den Kontaktwalzen sind nicht vernachlässigbar klein, deshalb leuchten die Lämpchen mehr oder weniger hell oder flackern. Man muss bedenken, dass 12 Kontaktübergänge in Serie zum Lampenkreis liegen! Dies hat zur Folge, dass bei einer gedrückten Taste die Spannung am entsprechenden Steckerstift nicht auf GND-Potential geht, sondern irgendwo zwischen fast 0 und etwa 2 Volt liegt. Bei losgelassener Taste misst man dagegen exakt V+.
- Sollen die gedrückten Tasten von einer externen Schaltung detektiert werden, legt man die Komparatorschwelle relativ hoch, etwa 0,5 Volt unterhalb V+. Es ist für eine ausreichende Entprellung zu sorgen.
- Falls die Stromversorgung über den Stecker erfolgt, muss man darauf achten, dass kein Konflikt mit einer anderen Spannungsquelle entsteht. Wenn eine Batterie eingebaut ist, muss der Quellenschalter auf "Accu" stehen, andernfalls ist auch die Stellung "Batt" erlaubt. Auf keinen Fall darf der Schalter auf "Trafo" gestellt sein, weil sonst über die Trafowicklung ein Kurzschluss entstehen würde. Die Speisung über den Stecker hat den Vorteil, dass die Polaritätsverhältnisse vom Anwender vorgegeben werden und somit definiert sind.
- Als externe Speisung könnte eine Stromquelle mit einem eingeprägten Strom von 0,2 Amp. verwendet werden. Die maximale Ausgangsspannung der Quelle ist zu begrenzen, z. B. auf 12V. Die Lämpchen leuchten beim Betätigen einer Taste gleichmässig hell, weil sie von einem definierten Strom durchflossen werden. Der Einfluss der Kontaktwiderstände kann auf diese Weise bis zu einem bestimmten Maximalwert eliminiert werden.

Simulationsprogramme

Um sich mit der Nema vertraut zu machen, ist es nicht zwingend erforderlich, über eine reale Maschine zu verfügen. Mit einem Simulator auf dem Computer kann die Funktion der Maschine ebenso gut erforscht werden. Solche Programme können von der Bedienung und dem Aussehen her von der realen Nema mehr oder weniger stark abweichen, wichtig ist lediglich, dass die Chiffrierschritte der Realität entsprechen.

Beim Autor ist für die Nema ein Programm kostenlos erhältlich. Eine Beschreibung dieses Programms ist auf den folgenden Seiten zu finden.

Für die Nema und die Enigma sind Simulationsprogramme, vorhanden, die vom Internet heruntergeladen werden können. Angaben zu den entsprechenden Seiten auf dem Netz findet man im Kapitel: "Informationen im Internet" auf Seite 109. Eine Suche im Internet fördert immer wieder Neues zu Tage.

Programm für die Nema

Die Programme "NEMAKURS.EXE" (Schulmaschine) und "NEMAKMOB.EXE" (K-Mob-Maschine) simulieren die Nema und sind auf einem PC unter DOS oder Windows lauffähig. Über die Programme kann man frei verfügen. Auf die Ausgestaltung einer realitätsnahen Bedieneroberfläche wurde verzichtet. Für den Start wird das Programm unter DOS aufgerufen oder unter Windows mit einem Doppelklick aktiviert.

Nach dem Start zeigt der Monitor das Bild gemäss Abb. 155. Falls man unter Windows das Fenster auf den ganzen Monitor ausdehnen möchte, lässt sich das mit der Tastenkombination [ALT-Enter] erzwingen.

Unter der Titelzeile wird der aktuell eingestellte äussere Schlüssel angezeigt (AAAAAAAAAA), rechts dane-ben befindet sich der Schrittzähler. Darunter erkennt man das symbolische Lämpchenfeld. Als Tastatur wird die des PC's verwendet. Nur die 26 Buchstabentasten sind wirksam, zwischen Gross- und Kleinschreibung wird nicht unterschieden. Alle übrigen Tasten – ausser denen, die für die Steuerung benötigt werden – sind nicht wirksam und werden ignoriert.

Die Tasten dürfen nur kurz angetippt werden, dauerndes Niederdrücken erzeugt die bekannte Zeichenwiederholung. Das angesteuerte Lämpchen leuchtet bis erneut eine Taste gedrückt wird, längstens jedoch zwei Sekunden. Man könnte für diese Anwendung einen speziellen Tastaturtreiber schreiben, aber damit handelt man sich oft andere Probleme ein. Der Aufwand sollte in einem vernünftigen Rahmen bleiben. Bei einem Simulator stösst man an Grenzen, irgendwo man muss Kompromisse eingehen.

Gegenüber der realen mechanischen Maschine sind bei diesem Simulator ein paar Unterschiede zu beachten:

- Nach dem Einstellen des äusseren Schlüssels muss keine Leertaste betätigt werden.
- Der Schrittzähler hat einen Bereich von fünf Stellen, im Gegensatz zu deren vier bei der realen Maschine.
- Der rote Hebel fehlt, er wird nicht benötigt.
- Unterhalb des Lampenfeldes wird eine Laufschrift eingeblendet. Auf der oberen Zeile erscheint der eingegebene Text in Kleinbuchstaben, darunter der umgesetzte Text in Grossbuchstaben, siehe Abb. 158.

```
  laufband();                    /* Laufband löschen, ist
 }

 void vorschub(void)             /* Tastendruck auf Walzer
  {
   zaehler_anpassen(1);          /* Zähler, 5-stellig nach
   /* die Rotoren 3 und 7 haben doppelte Abhängigkeit */
   /* die Rotoren 4 und 8 haben einfache Abhängigkeit von
   if (s0[((rotor[10]+17)%26)])
     {
     if (s4[((rotor[4]+16)%26)]) rotor[3] = (rotor[3]+25)%
     rotor[4] = (rotor[4]+25)%26;
     if (s8[((rotor[8]+16)%26)]) rotor[7] = (rotor[7]+25)%
     rotor[8] = (rotor[8]+25)%26;
     }
   /* die Rotoren 1, 5 und 9 haben einfache Abhängigkeit *
   if (s2[((rotor[2]+16)%26)])  rotor[1] = (rotor[1]+25)%2
   if (s6[((rotor[6]+16)%26)])  rotor[5] = (rotor[5]+25)%2
   if (s10[((rotor[10]+16)%26)]) rotor[9] = (rotor[9]+25)%
   /* die Rotoren 2, 6 und 10 werden bei jedem Tastendruck
   rotor[2] = (rotor[2]+25)%26;
   rotor[6] = (rotor[6]+25)%26;
   rotor[10]= (rotor[10]+25)%26;
  }

 void backstep(void)
 {
  zaehler_anpassen(-1);                /* Display um 1 z
  /* genau umgekehrte Reihenfolge wie beim Schritt vor!!,
  rotor[2] = (rotor[2]+1)%26;
  rotor[6] = (rotor[6]+1)%26;
  rotor[10]= (rotor[10]+1)%26;
  if (s2[((rotor[2]+16)%26)]) rotor[1] = (rotor[1]+1)%26;

  if (s6[((rotor[6]+16)%26)]) rotor[5] = (rotor[5]+1)%26;
  if (s10[((rotor[10]+16)%26)]) rotor[9] = (rotor[9]+1)%26
  if (s0[((rotor[10]+17)%26)])
     {
     rotor[4] = (rotor[4]+1)%26;
     if (s4[((rotor[4]+16)%26)]) rotor[3] = (rotor[3]+1)%
     rotor[8] = (rotor[8]+1)%26;
     if (s8[((rotor[8]+16)%26)]) rotor[7] = (rotor[7]+1)%
     }
  if (zeiger)                      /* bearbeiten nur bis Ze
     {
     klar[--zeiger] = 32;
     chiff[zeiger] = 32;
     laufband();
     }
 }

 char chiffrieren(int klartext)
  {                          /* Klartext wird als Kleinbuchsta
   int zwischen;
   zwischen = in[klartext-97];       /* Offset weg und Pos
   zwischen = (zwischen + r9[(zwischen+rotor[9])%26])%26;
   zwischen = (zwischen + r7[(zwischen+rotor[7])%26])%26;
   zwischen = (zwischen + r5[(zwischen+rotor[5])%26])%26;
   zwischen = (zwischen + r3[(zwischen+rotor[3])%26])%26;
   zwischen = (zwischen + um[(zwischen+rotor[1])%26])%26;
   zwischen = (zwischen + ir3[(zwischen+rotor[3])%26])%26;
   zwischen = (zwischen + ir5[(zwischen+rotor[5])%26])%26;
   zwischen = (zwischen + ir7[(zwischen+rotor[7])%26])%26;
   zwischen = (zwischen + ir9[(zwischen+rotor[9])%26])%26;
   return(ini[zwischen]);             /* von Anschlussplatt
  }

 void rotoren_anzeigen(void)
  {
   textcolor(YELLOW);
   gotoxy(16,7); cprintf("%c",rotor[1]+65);
   gotoxy(20,7); cprintf("%c",rotor[2]+65);
   gotoxy(24,7); cprintf("%c",rotor[3]+65);
   gotoxy(28,7); cprintf("%c",rotor[4]+65);
   gotoxy(32,7); cprintf("%c",rotor[5]+65);
   gotoxy(36,7); cprintf("%c",rotor[6]+65);
   gotoxy(40,7); cprintf("%c",rotor[7]+65);
   gotoxy(44,7); cprintf("%c",rotor[8]+65);
   gotoxy(48,7); cprintf("%c",rotor[9]+65);
   gotoxy(52,7); cprintf("%c",rotor[10]+65);
  }

 void aussen(void)                /* Äusseren Schlüssel ein
  {
   int tast, buff[1000],j;        /* Fenster bereitstellen
   gettext(13,9,59,18,&buff);
   window(13,9,59,18);
   clrscr();
   textcolor(WHITE);              /* Maske aufbauen */
   gotoxy(1,1);
   cputs("                                                  "
         "                                                  "
         "   Einstellen des äusseren Schlüssels (AS)        "
         "   ---------------------------------------        "
         "                                                  "
         "   mit Pfeiltasten  \033 \032  Walze wählen       "
         "   mit Pfeiltasten  \031 \030  Walze einstellen   "
         "                                                  "
         "   Ausführen und zurück mit Enter                 ");
   textcolor(YELLOW);
   gotoxy(1,1);
   cputs("   \030");              /* Pfeil einzeichnen */
   j=1;                           /* bei Walze 1 */
```

154 Das Simulationsprogramm des Autors für die Nema ist in Turbo-C geschrieben. [AUT]

Steuertasten

F8: Anzeige des inneren Schlüssels
Über den Walzen wird deren Bezeichnung eingeblendet. Ein erneutes Betätigen der Taste lässt die Anzeige wieder verschwinden.

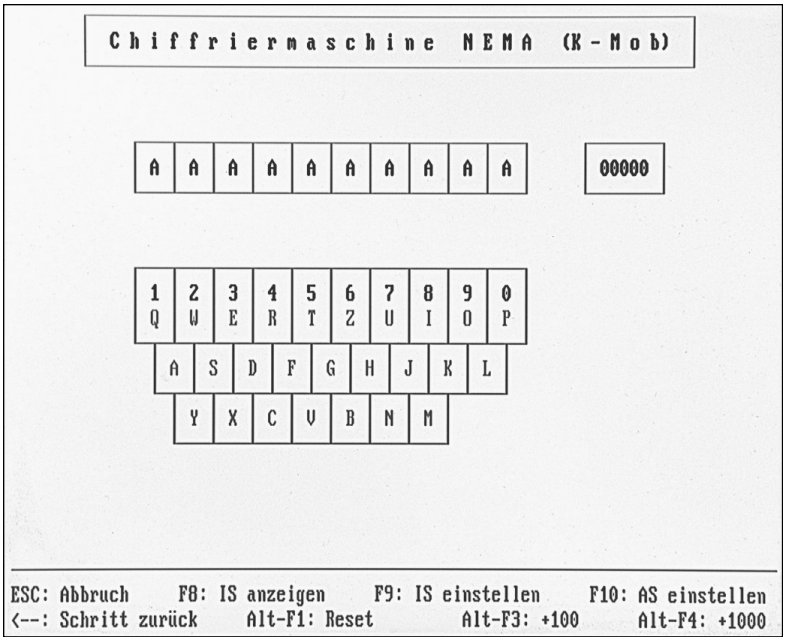
F9: Inneren Schlüssel einstellen
Ein Fenster öffnet sich, in diesem wird die Einstellung vorgenommen, siehe Abb. 157.
Achtung: Keine der Walzen doppelt verwenden, das Programm reklamiert sonst einen Fehler.

F10: Äusseren Schlüssel einstellen
Die einzelnen Walzen werden mit den Pfeiltasten links/ rechts angewählt und mit den Tasten auf/ab "gedreht", siehe Abb. 156.

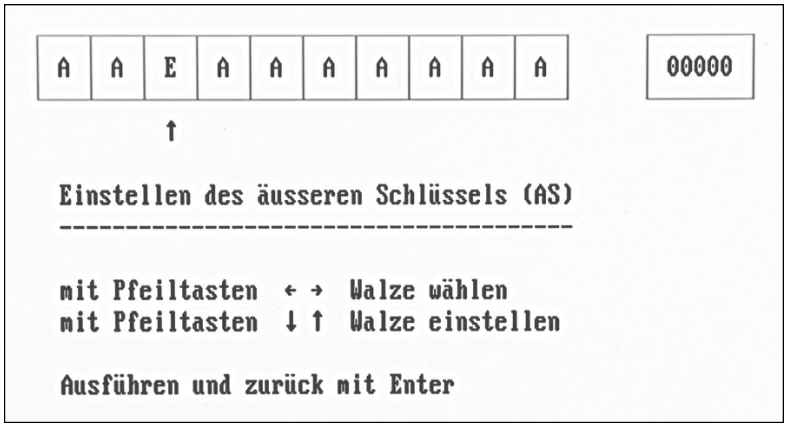
F1: Reset
Der Zähler wird auf NULL gesetzt, das Laufband wird gelöscht. An den anderen Einstellungen der Maschine verändert sich nichts.

Backspace: Schritt korrigieren
An Stelle des roten Hebels kann mit der Taste '←' ein Schritt rückwärts ausgeführt (korrigiert) werden. Im Gegensatz zur realen Maschine lassen sich beliebig viele Schritte korrigieren, indem man die Backspace-Taste mehrmals betätigt.

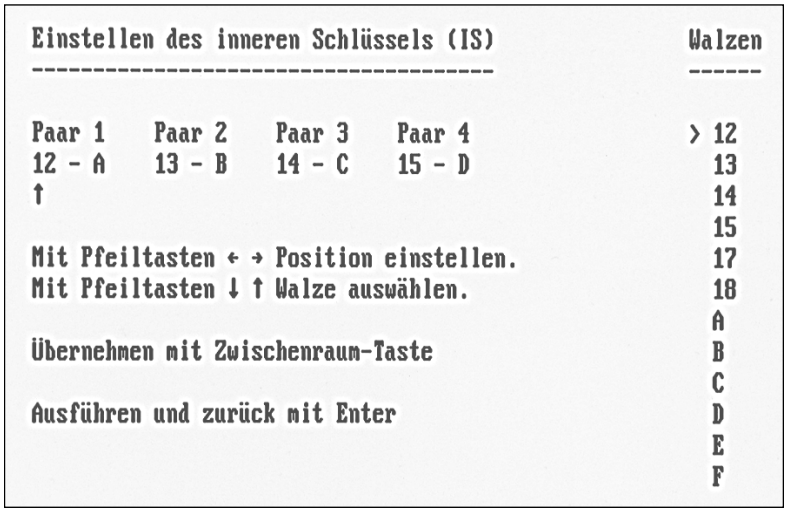
F3 / F4: Automatischer Vorschub
Mit diesen Tasten lassen sich 100, resp. 1000 Schritte automatisch generieren, ein Text wird nicht erzeugt. Diese Funktion ermöglicht z. B. die Überprüfung, ob die Walzen nach 17'576 Tastenbetätigungen tatsächlich wieder in ihrer Ursprungsposition stehen.



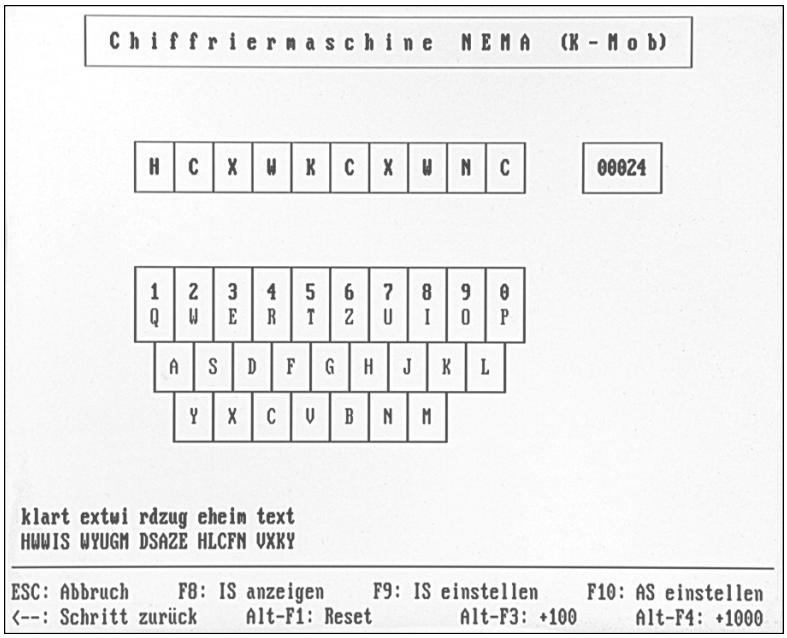
155 Nach dem Programmstart zeigt sich dieses Bild. Unter Windows lässt es sich mit der Tastenkombination [Alt-Enter] auf den ganzen Bildschirm vergrössern. [AUT]



156 Mit F10 lässt sich der äussere Schlüssel einstellen. Die Walzen werden mit den Pfeiltasten angesteuert und gedreht. [AUT]



157 F9 öffnet ein Fenster zur Einstellung des inneren Schlüssels. Mit den Pfeiltasten wird die gewünschte Position eingestellt und aus einer Liste die gewünschte Walze ausgewählt. Je nach gestartetem Programm sind entweder die Walzen der Schul- oder der K-Mob-Maschine verfügbar, hier die K-Mob-Version. [AUT]



158 Arbeiten mit dem Programm. Unter dem Lampenfeld erscheint ein Lauftext: Auf der oberen Zeile in Kleinbuchstaben der eingegebene Text, darunter in Grossbuchstaben der umgesetzte Text. [AUT]

Übungsbeispiele

Anhand der nebenan stehenden Beispiele kann man die theoretischen Kenntnisse in der Praxis erproben. Mit einer realen Maschine oder einem Simulator lassen sich die kurzen Geheimtexte dechiffrieren. Es stehen für die Schul- als auch für die K-Mob-Maschine je zwei Telegramme zur Verfügung. Eines ist mit dem Einmalschlüssel chiffriert, das andere nach dem Tageschlüssel-Verfahren (Methode "Botschaftsfunk"). Auf den Abbildungen findet man alle erforderlichen Angaben: Maschinentyp, Schlüsselverfahren, inneren und äusseren Schlüssel sowie den kurzen Geheimtext, der zu dechiffrieren ist.

Nachfolgend ist zur Vertiefung nochmals eine kurze Zusammenfassung des Vorgehens aufgeführt. Die Verfahren sind ausführlich auf den Seiten 44 und 45 beschrieben.

Allgemeine Vorbereitung

Zuerst wird auf der Maschine immer – unabhängig vom angewandten Verfahren – der im "Schlüsselbefehl" angegebene innere und äussere Schlüssel eingestellt.

Bei der realen Maschine wird der rote Hebel in die Stellung "Betrieb" gebracht und der Zähler auf Null gestellt. Eine beliebige Buchstabentaste wird gedrückt. Es muss nicht, wie im Reglement vorgeschrieben, die Taste 'Q' sein. Der Zähler muss noch immer auf Null stehen.

Wenn mit einem Simulationsprogrammen gearbeitet wird, muss das Vorgehen abgeklärt werden. Es gibt Programme, die sehr realitätsnah sind, bei diesen muss man mit dem Mauszeiger den roten Hebel "betätigen" und eine beliebige Taste "drücken". Die Eingabe des Textes erfolgt oft mit dem Mauszeiger auf einer virtuellen Tastatur. Andere Programme benutzen die Computertastatur zur Eingabe.

Einmalschlüssel-Verfahren

Der Geheimtext wird ab der ersten Fünfergruppe eingegeben. Nach dem ersten gedrückten Buchstaben muss der Zähler auf '1' stehen, sonst ist entweder der rote Hebel nicht auf "Betrieb" oder es wurde vergessen eine Buchstabentaste zu drücken. Den Klartext liest man an den aufleuchtenden Lämpchen ab und notieren in Buchstabe für Buchstabe auf einem Hilfsblatt als Bandwurm. Anschliessend erstellt der Chiffreur den bereinigten Klartext, den er an den Empfänger weiter gibt.

Tagesschlüssel-Verfahren

Die ersten beiden identischen Fünfergruppen des Telegramms werden in die Maschine eingegeben. Die zehn erhaltenen Buchstaben notiert man sich auf einem Hilfsblatt, sie bilden den Spruchschlüssel.

Auf der Maschine stellt man diesen Spruchschlüssel als äusseren Schlüssel ein. Am inneren Schlüssel wird nichts verändert, er bleibt so wie er eingestellt ist. Dann roter Hebel, Buchstabentaste und Zähler auf Null, wie oben beschrieben.

Der eigentliche Geheimtext beginnt ab der dritten Fünfergruppe. Ab hier wird mit dem neu eingestellten Schlüssel dechiffriert.

Hinweise

Bitte erinnern Sie sich an die auf Seite 52 vorgestellten Sicherheitsmassnahmen. Bei den Telegrammen nach dem Tagesschlüssel-Verfahren kommen Buchstabenverdreifachungen vor, ebenso die Umschaltung in die Ziffernebene. Lassen Sie sich nicht verwirren!

Es liegt in der Verantwortung des Chiffreurs, dass er alle Notizen zum Chiffrieren – besonders die erzeugten Spruchschlüssel – immer zuverlässig, gewissenhaft und eigenhändig zerstört. Sie dürfen unter keinen Umständen in falsche Hände geraten.

```
Schulmaschine                                  Einmalschlüssel

Innerer Schlüssel:  19-B / 16-C / 20-A / 21-D
Äusserer Schlüssel: D I S T E L F I N K

Y I J V E  K K E G D  W Z B T E  I Q X O E  P X C Q T
D Y U J X  I E M M C  I E H L W  H E C V T
```

159 Beispiel für die Schulmaschine mit Einmalschlüssel. [AUT]

```
Schulmaschine                                  Tagesschlüssel

Innerer Schlüssel: 19-B / 16-C / 20-A / 21-D
Äusserer Schlüssel: F E L D W E I B E L

E X T E R  E X T E R  L X H P N  B H W L J  Y F C D Z
Q E S X P  P S Y N U  J V O V X  C L Y Z P  L I L A L
Y P I K N  P R H P H  O D A Z C
```

160 Beispiel für die Schulmaschine mit Tagesschlüssel. [AUT]

```
K-Mob-Maschine                                 Einmalschlüssel

Innerer Schlüssel:  13-C / 15-B / 14-A / 12-D
Äusserer Schlüssel: D I S T E L F I N K

W T Q L L  G H P G P  Y L T X L  G T M O A  Q H G H W
U S J B L  Q M A B Y  K L Z D K  V O N X J  A I X A I
```

161 Beispiel für die K-Mob-Maschine mit Einmalschlüssel. [AUT]

```
K-Mob-Maschine                                 Tagesschlüssel

Innerer Schlüssel:  13-C / 15-B / 14-A / 12-D
Äusserer Schlüssel: F E L D W E I B E L

E X T E R  E X T E R  O A B B X  Y B L Z H  R R C P X
T G O C F  P E M R I  X C Z Q Y  G H R X W  U H I Y R
J O O K J  Y T U U I  W U F D E
```

162 Beispiel für die K-Mob-Maschine mit Tagesschlüssel. [AUT]

Ergebnis des Dechiffrierens:

Erzeugter Spruchschlüssel beim Tagesschlüssel-Verfahren: . . . . . .

Klartextwurm: . . . . . .

. . . . . .

. . . . . .

Bereinigter Text: . . . . . .

. . . . . .

. . . . . .



163 Die Visitenkarte der beiden Entwickler. [SUL]

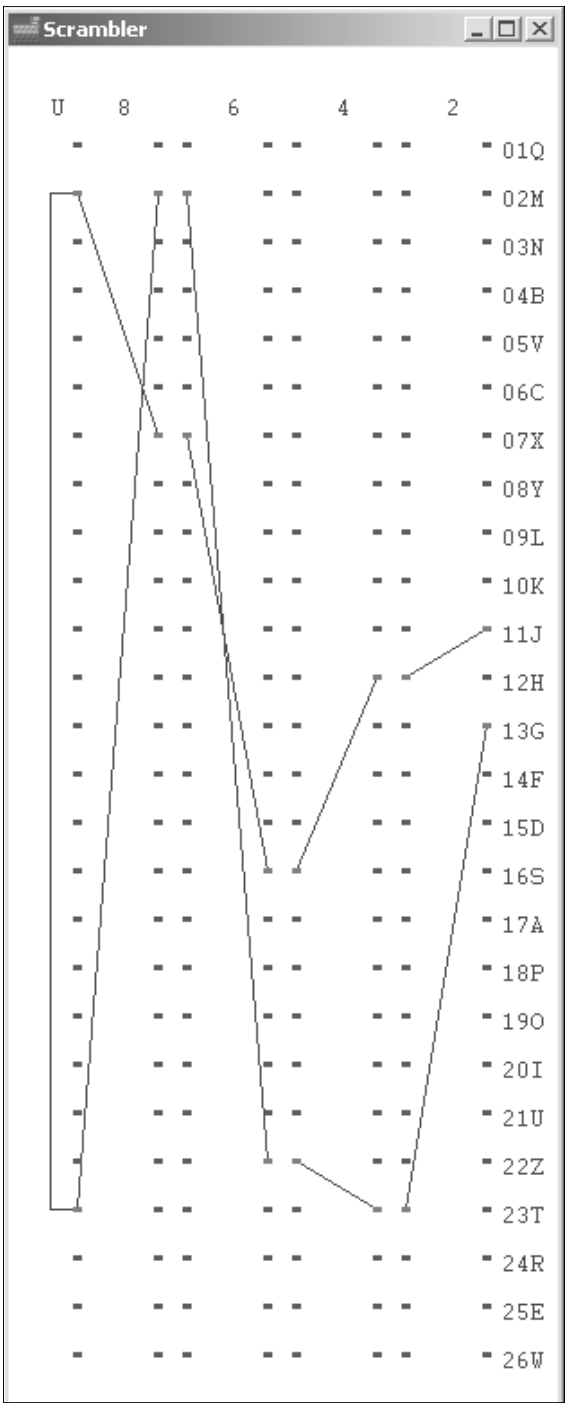
Simulator Sullivan / Weierud

Im Internet [B] ist für die Nema ein Simulator mit real wirkender Oberfläche abrufbar, siehe Abb. 164. Alle Funktionen können fast wie in der Wirklichkeit ausgeführt werden. Der äussere Schlüssel wird mit dem Mauszeiger eingestellt oder über die Tastatur eingetippt. Der innere Schlüssel lässt sich auf die Walzen der Schul- oder der Kriegsmaschine einstellen, siehe Abb. 167. In einem Hilfsfenster kann man sich den Pfad durch einzelne Walzen oder durch das ganze Walzenpaket anzeigen lassen. Abb. 165 zeigt als Beispiel den Weg des Signals durch das Walzenpaket. Alternativ lässt sich der ein- und der ausgegebene Text in Fenstern anzeigen, siehe Abb. 166. Alle angezeigten Informationen können auch ausgedruckt werden.

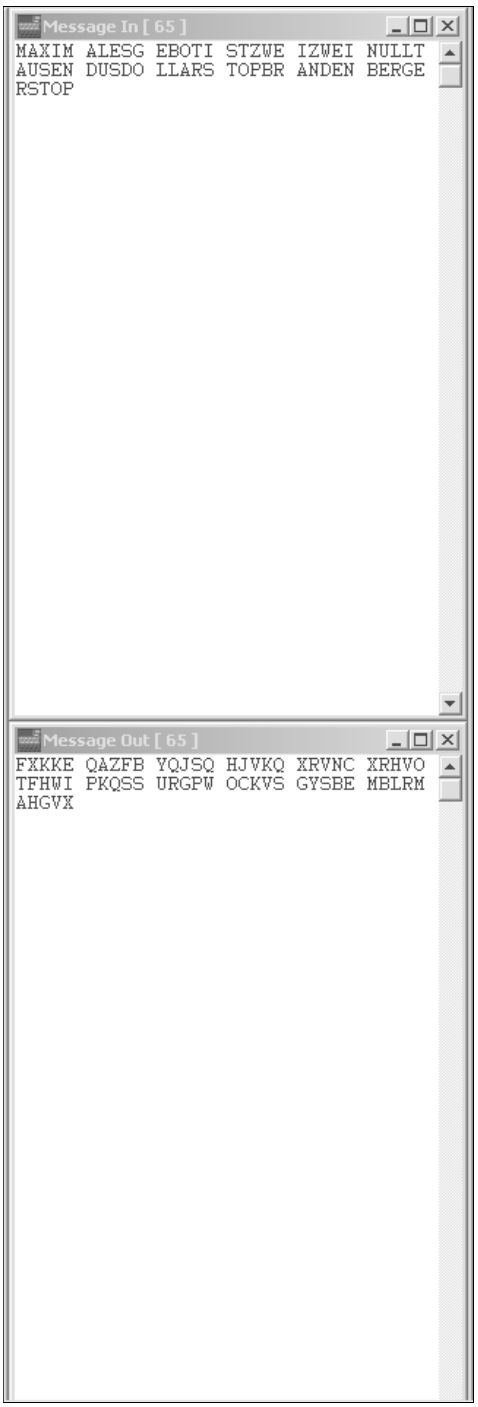
Ein mit viel Liebe zum Detail entwickeltes Programm, ein Kompliment an die Entwickler!

164 Das Programm präsentiert sich mit einer sehr realitätsnahen Oberfläche. [SUL]

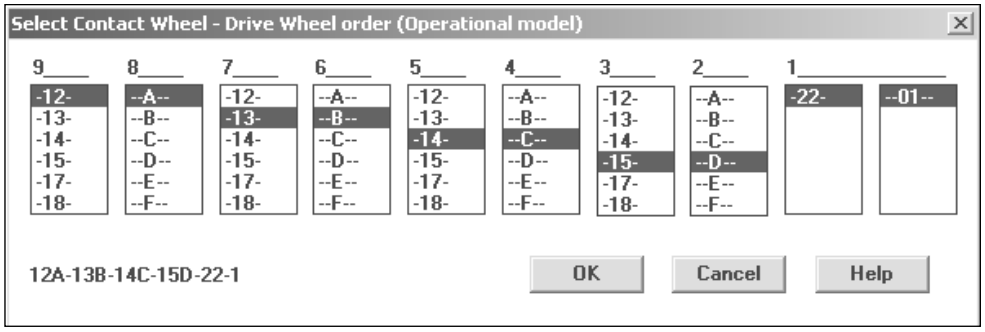




165 Der Pfad durch das Rotorpaket (Scrambler) wird grafisch dargestellt. Nullpunkt und Zuordnung sind hier anders gewählt als im Abschnitt "Die letzten Geheimnisse der Nema" vorgestellt. [SUL]



166 In zwei Fenstern erscheint der eingegebene und der umgesetzte Text. [SUL]



167 Der innere Schlüssel lässt sich auf die Schulmaschine (Taining model) oder die K-Mob-Maschine (Operational model) einstellen. [SUL]

Literatur

Für die Nema ist nur wenig Literatur zu finden. Viele Fachbücher gehen auf die Enigma ein, die Unterschiede zwischen diesen beiden Maschinen sind nicht gross; was für die Enigma gilt, trifft meist auch für die Nema zu.

[1] Kippenhahn, Rudolf; Verschlüsselte Botschaften
Rowohlt 1997

[2] Kozaczuk, Wladyslaw; Geheimoperation Wicher
Bernhard & Graefe 1989

[3] Harris, Robert: Enigma; Roman, der das Brechen der Enigma beschreibt, gut recherchiert. Wilhelm Heyne 1995

[4] Hodges, Andrew; Alan Turing, Enigma
Springer 1994

[5] Bauer, Friedrich L.; Entzifferte Geheimnisse
Springer 1997

[6] Schlüsselungsverfahren für die Nema-Maschine;
Übermittlungsdienst der Armee, Original Mai 1948

[7] Beutelspacher, Albrecht; Kryptologie
Vieweg 1987

[8] Bedienungsanleitung zur Chiffriermaschine "NEMA";
Original, April 1947

[9] Wobst, Reinhard; Abenteuer Kryptologie
Addison - Wessley 1998

[10] Beutelspacher, Albrecht; Moderne Verfahren der Kryptologie
Vieweg 1995

[11] Harper, Stephen; Kampf um Enigma - Die Jagd auf U-559
Roman um die Erbeutung einer Marine-Enigma, Ullstein 2004

[12] Bauer, Friedrich; Kryptologie, Methoden und Maximen
Springer 1993

[13] Singh, Simon; Geheime Botschaften
Carl Hanser 1999

[14] Sebag-Montefiore, Hugh; Enigma, The battle for the code
Weidenfeld & Nicolson 2000

[15] Winterbotham, Frederick W.; The Ultra Secret
Ullstein 1974

[16] Beyrer, Klaus (Hrsg.); Streng geheim
Umschau/Braus 1999

[17] Sullivan, Geoff and Weierud, Frode; The Swiss Nema Cipher Machine, Cryptologia 23(4), October, 1999
Technische Beschreibung der Nema

[18] Kommunikation für die Armee;
Generalstab, Untergruppe Führungsunterstützung, Bern

[19] Ritter, Rudolf J.; Das Fernmeldematerial der Schweizerischen Armee seit 1875, 10. Folge; Generalstab, Untergruppe Führungs-unterstützung, Bern 2002

[20] Schmid, Walter; Botschaftsfunk damals; in Vorbereitung
Eigenverlag, erscheint 2005

[21] Ersatzteilkatalog; Schweizerische Armee, ALN 5810-670-0310, 1972

[22] Geheimakte 2. Weltkrieg, Die Entschlüsselung des Enigma-Codes;
BBC Time Life Video

Informationen im Internet

[A] http://www.codesandciphers.org.uk/enigma/enigma1.htm
(zur Enigma)

[B] http://frode.home.cern.ch/frode/crypto/simula/nema/index.html
(zur Nema, Simulationsprogramm)

[C] http://www.eclipse.net/~dhamer/nema2.htm
(zur Nema)

Mit einer Suchmaschine findet man unter dem Stichwort "Nema" immer wieder Neues.

Dokumente im Bundesarchiv

Die erwähnten und gezeigten Dokumente des Bundesarchivs sind abgelegt unter der Signatur: E27 19007 1925/48

Bildnachweis

Alle Bilder sind mit ihrer Herkunft versehen. Die Zahlen in den eckigen Klammern beziehen sich auf die Literaturliste nebenan, zusätzlich:

[AUT] Bild oder Zeichnung des Autors

[BAR] Dokument aus dem Bundesarchiv in Bern

[BRS] Zeichnung von Brigitte Rudolf Schmid

[GSB] Bild von Gerhard Sulger Büel

[SUL] Geoff Sulivan / Frode Weierud

[UNB] Unbekannt oder nicht feststellbar

Dank

Paul Glur teilte mir anlässlich eines Gesprächs Interessantes zur Entwicklungsgeschichte der Nema mit. Er gehörte als Mathematiker zur Gruppe der drei Erfinder.

Gerhard Sulger Büel recherchierte im Bundesarchiv und informierte mich über Geschichtliches der Nema, er überprüfte das Manuskript auf Fehler und sachliche Ungereimtheiten.

Brigitte Rudolf Schmid fertigte Zeichnungen an und durchsuchte den Text auf Fehler, sie unterstützte mich bei der Gestaltung.

Francis Conus vom EDA liess mich einen Blick auf die noch vorhandenen Chiffrierunterlagen und die letzte Botschafts-Nema werfen.

Daniel Jenni steuerte die Kopie eines Bundesarchiv-Dokuments bei.

Das Bundesarchiv erlaubte die Publikation von Dokumenten.

Ihnen allen danke ich herzlich für die Mitarbeit.

Hinweise und Anregungen

Die Informationen, die ich hier wiedergegeben habe, stammen aus der aufgeführten Literatur und von den oben erwähnten Informanten. Daneben sind meine subjektiven, persönlichen Erfahrungen und Erinnerungen eingeflossen. Hinweise und Anregungen nehme ich gerne entgegen. Sie können bei einer Neuauflage berücksichtigt werden.

Anschrift des Autors

Walter Schmid HB9AIV
Lächlerstrasse 70, 8634 Hombrechtikon

E-Mail: hb9aiv@swissonline.ch