Reise 19-2019

Freitag, 4. Oktober 2019

ENIGMA UND NEMA

Ein Workshop für kluge GMS-Köpfe

DOKUMENTATION

Reiseleitung

Dr. Jürg Schucan, Küsnacht

Schweizerische Gesellschaft
für militärhistorische Studienreisen

Reise	09-2019 | ENIGMA UND NEMA
Autor der Dokumentation	Walter Schmid Jürg Schucan
Reiseleitung	Dr. Jürg Schucan, Küsnacht
Erstauflage	44 Exemplare
Layout	David Accola, RC GMS,
Druck und Bindung	Häfliger Druck AG, 5430 Wettingen
Herausgeber	Schweizerische Gesellschaft für militärhistorische Studienreisen (GMS), Reisechef, 5430 Wettingen

Alle Rechte vorbehalten

www.gms-reisen.ch

info@gms-reisen.ch

Inhaltsverzeichnis dieser GMS-Work-Shop-Dokumentation

Das Sammlungszentrum «Führungsunterstützung» in Uster Winikon 3
Standort 3
Grundlage 4
Stiftungen 4
Mitarbeit durch Vereine 5
Geheimsprachen - Von der «Handarbeit» zur Rotormaschine 6
Einführung 6
Grundlagen 7
Chiffrierverfahren 1 9
Kryptanalyse 1 14
Mit Intuition und Probieren zum Ziel 15
Statistiktabellen 16
Chiffrierverfahren 2 17
Kryptanalyse 2 20
Die Rotormaschine 24
Von Marconi zu Ultra 31
Einführung 31
«Come quick danger» 31
Die Risiken des Funkverkehrs - Tannenberg 32
Die Zimmermann Depesche 33
Das Wunder an der Weichsel 34
Die Polen und die Enigma 35
Der Weg einer verschlüsselten Meldung nach Bletchley Park 37
Die Turing Bombe 38
Fish 44
Bibliographie und weiterführende Unterlagen 46
Anhang 1: Bedienungs-Anleitung zur Chiffriermaschine «NEMA» 47
Anhang 2: Schlüsselungsverfahren für die NEMA-Maschine 58

Das Sammlungszentrum «Führungsunterstützung» in Uster Winikon

von Walter Schmid

Standort

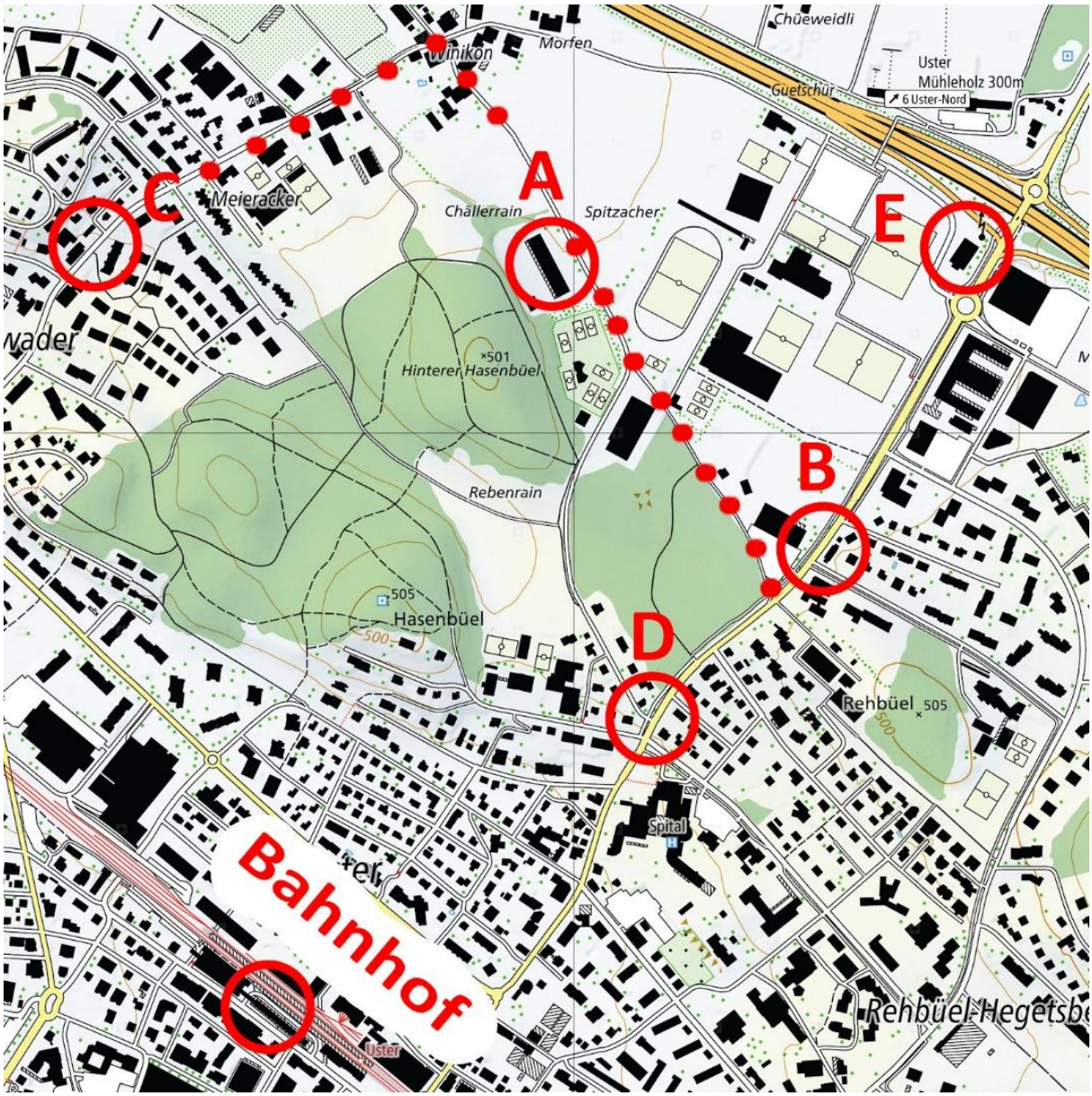


Abb. 1: Lageplan des «Sammlungszentrums Historisches Armeematerial Führungsunterstützung» an der Winikerstrasse 31, CH-8610 Uster

Legende:

A: Sammlungszentrum Historisches Armeematerial Führungsunterstützung. Parkplätze finden sich innerhalb der Umzäunung.

B: Bus-Haltestelle „Reithalle“

C: Bus-Haltestelle „Meieracher“

D: Abzweigung zur Winikerstrasse, gelber Wegweiser „Sammlungszentrum“.

E: Restaurant „Buchholz da Maria“, hier Mittagessen

Bahnhof Uster: Hier fahren die Busse ab nach „Reithalle“ und „Meieracher“

Punktiert: Fusswege

Grundlage

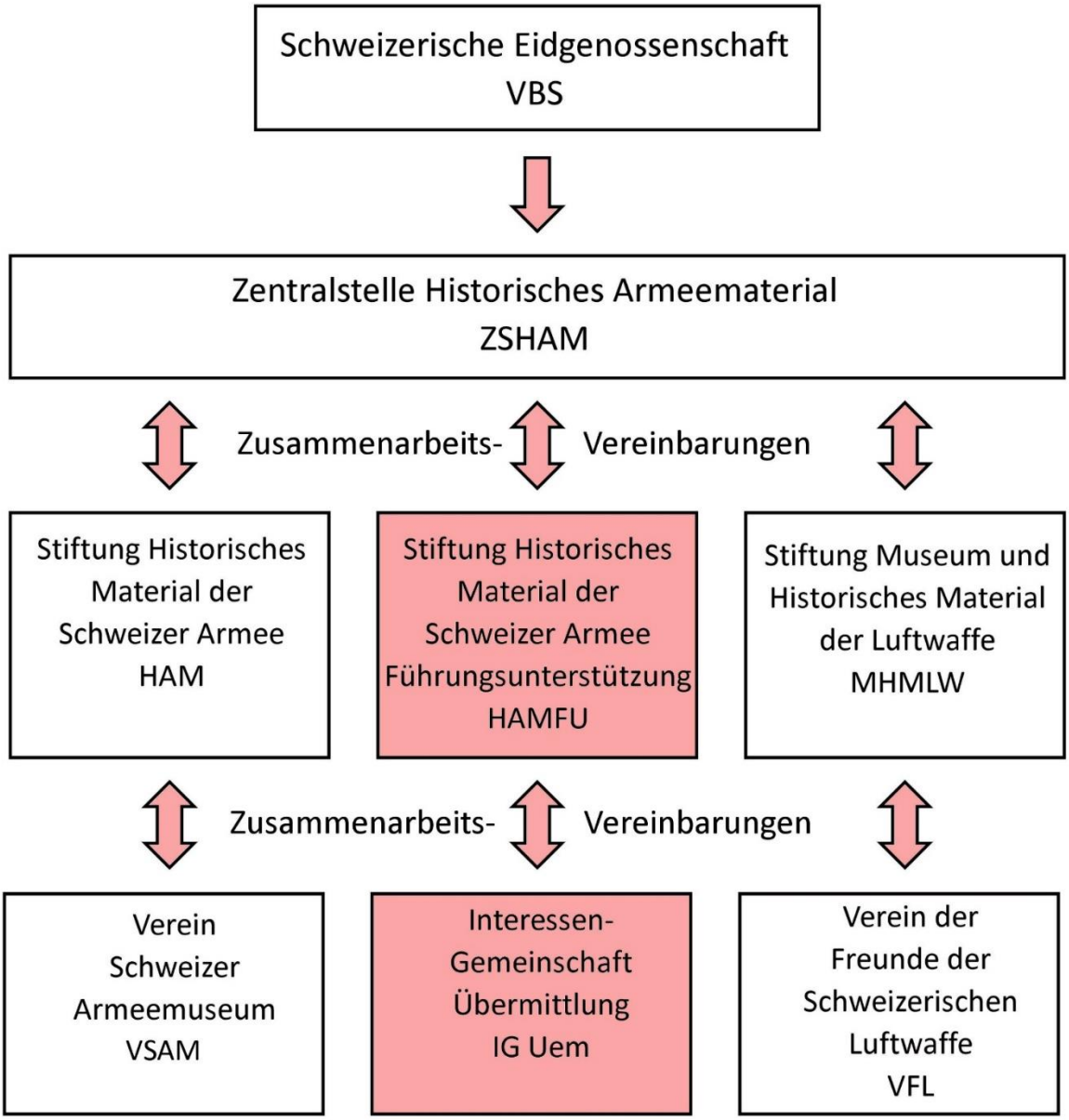


Abb. 2: Organisation und Zusammenarbeit der ZSHAM mit deren Stiftungsorganen

Rechtliche Grundlage für das bestehende Sammlungskonzept für historisches Armeematerial ist die Verordnung VBS vom 6. Dezember 2007 über das Armeematerial (Armeematerialverordnung, VAMAT), in Kraft seit 15. Dezember 2007.

Der Bundesrat gab dem VBS den Auftrag, eine repräsentative Auswahl des historischen Armeematerials für spätere Generationen zu sammeln, zu pflegen und wenn möglich in betriebsfähigem Zustand zu halten. Die dazu gehörenden Handbücher und Dokumente sollen ebenfalls aufbewahrt werden, etwa Hintergründe der Beschaffung, eingesetzte Technik, Ausbildungsmaterial und Erfahrungsberichte der Truppe. Im VBS koordiniert und organisiert die „Zentralstelle historisches Armeematerial, ZSHAM“ diesen Auftrag.

Stiftungen

Es wurden drei zivilrechtliche Stiftungen gegründet, die je für einen bestimmten Teil der Objekte zuständig sind. Die umfangreichste Stiftung, die HAM, sammelt bis auf zwei Ausnahmen alles Armeematerial, also von der Uniform bis zum Panzer. Sie hat ihren Sitz im ehemaligen Zeughaus in Thun.

Die erste Ausnahme bildet die Stiftung MHMLW. Sie sammelt alles zur Flugwaffe. Sie ist auf dem ehemaligen Flugplatzgelände in Dübendorf stationiert.

Die zweite Ausnahme ist die Stiftung

HAMFU, die das historische Material der Führungsunterstützung betreut, das sind die Objekte der ehemaligen Übermittlungstruppen. Sie ist in Uster, im Ortsteil Winikon beheimatet. Das der Stiftung vom VBS zugewiesene Gebäude ist eine ehemalige Dependance des Zeughauses Hinwil, die der Bund kürzlich für die besonderen Bedürfnisse eines Sammlungszentrums um- und ausgebaut hat. Die Stiftung beschäftigt wenige Personen, die meisten in Teilzeit. Das Gebäude ist Eigentum des Bundes, ebenso alles eingelagerte Material. Der Bund übernimmt die Kosten für den Unterhalt und den Betrieb des Zentrums, sowie die Löhne der Angestellten.

Das Gebäude ist dreistöckig gebaut. Zuoberst befindet sich ein Schaulager, das attraktive Geräte präsentiert, ein Rollauszuglager, ein Vortragssaal, ein grosses Arbeits- und Sitzungszimmer, ein Archiv, Büros und ein Pausenraum. Ein Ebene tiefer ist das Lager eingerichtet, das einen Grossteil der gesammelten Geräte und Anlagen enthält. Auf dem gleichen Boden befinden sich zwei grosse Werkstätten. Zuunterst sind die Fahrzeuge eingestellt, die mit den originalen Übermittlungsausrüstungen ausgestattet wurden.

Abb. 3: Aussenansicht des Sammlungszentrums Uster Winikon

Mitarbeit durch Vereine

Jede dieser drei Stiftungen arbeitet mit einem Verein zusammen. Bei der HAMFU ist das der Verein „Interessengemeinschaft Übermittlung, IG Uem“. Der Verein besteht aus etwa 180 Mitgliedern, grösstenteils sind es Ehemalige der Übermittlungstruppen oder sonst an der Übermittlungstechnik interessierte Personen. Etwa 30 Vereinsmitglieder bilden das Kernteam. Es trifft sich zweimal pro Monat im Sammlungszentrum zu einem freiwilligen Arbeitstag. Hauptsächlich werden neu angelieferte Geräte gereinigt, begutachtet, geprüft und bei Bedarf repariert. Im hausinternen Archiv wird der Geschichte der Geräte nachgegangen und es werden Berichte und Dokumentationen geschrieben; alles mit der Absicht, den damaligen Stand der Technik an die späteren Generationen weiterzugeben. Führungen durch das Schaulager und die Fahrzeughalle sind ebenfalls eine Aufgabe von instruierten Kernteammitgliedern. Bei Bedarf halten sie Vorträge und führen Workshops durch. Im Kernteam findet man zu fast jedem Gebiet Spezialisten, neben ehemaligen militärischen Fachleuten vor allem Amateurfunker und Ingenieure.

Geheimsprachen - Von der «Handarbeit» zur Rotormaschine

Ein Beitrag von Walter Schmid

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.

Abb. 4: Neugier und persönliche Vorteile sind der Antrieb, vom Inhalt vertraulicher Meldungen Kenntnis zu erlangen.

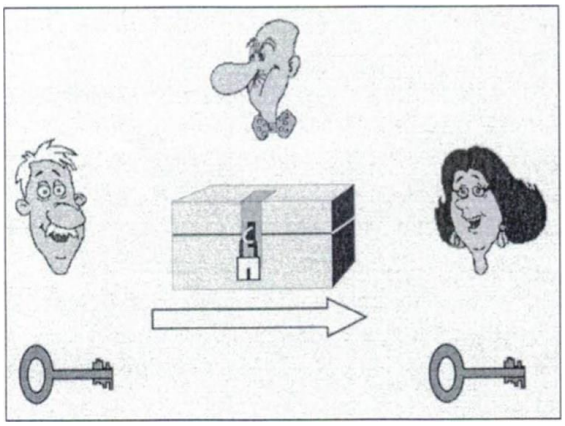


Abb. 5: Der Vorgang des Chiffrierens in symbolischer Darstellung.

Obenstehende Abbildung 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.

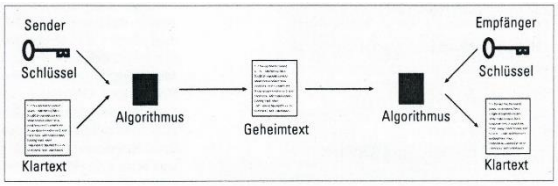


Abb. 6: Der Vorgang des Chiffrierens in einer anderen, etwas theoretischeren Darstellung.

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.

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

Abb. 7: 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.

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. 8.

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.

Grundlagen

Das Vor-Computer Zeitalter

Abb. 8: «Handarbeit» in früheren Zeiten. In einem Hinterzimmer des Londoner Oberpostamtes werden Briefe geöffnet und abgeschrieben.

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. 5 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. 5verwendet 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.

Abb. 9: Der Schlüssel ist der Inbegriff des Individuellen und Geheimen. Nur sein Besitzer kann bestimmte Vorgänge auslösen. (Autor)

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.

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

Abb. 10: Ein Telegramm lässt sich mit einem auf die 26 Kleinbuchstaben (und den Wortabstand) reduzierten Zeichensatz abfassen. (Autor)

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. 10.

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 irgendwelche 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
```

Abb. 11: Der besseren Übersicht wegen und als Hilfe für den Funker, wird der Geheimtext in Fünfergruppen aufgeteilt. (Autor).

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. 12.

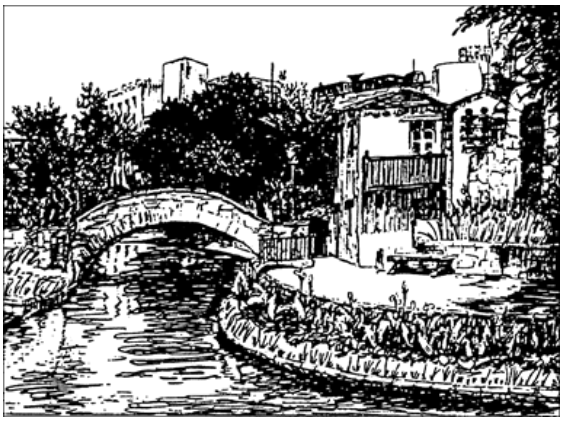


Abb. 12: Grafische Steganografie. Die Information ist in den verschieden langen Grashalmen verborgen, die man entlang des Kanals erkennt.

- Bei der linguistischen Steganografie versteckt man die geheime Botschaft in bestimmten Buchstaben eines harmlosen Textes. So können z. B. die ersten Buchstaben aller Worte, aneinandergereiht, die verborgene Mitteilung bilden, siehe Abb. 13. Man kennt in der linguistischen Steganografie noch verschiedene andere, raffiniertere und weniger leicht durchschaubare Methoden.

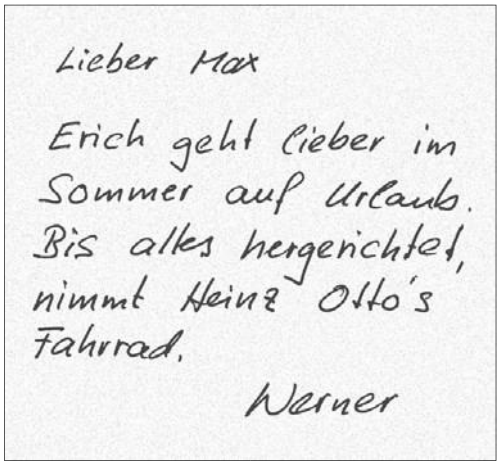


Abb. 13: Linguistische Steganografie: Die Anfangsbuchstaben des Textes (ohne Anrede und Unterschrift) ergeben den geheimen Text, er lautet hier: „Eglisau Bahnhof". (Autor)

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 aufwändigen Einrichtungen oder Hilfsmittel realisieren.

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 individuellen 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.

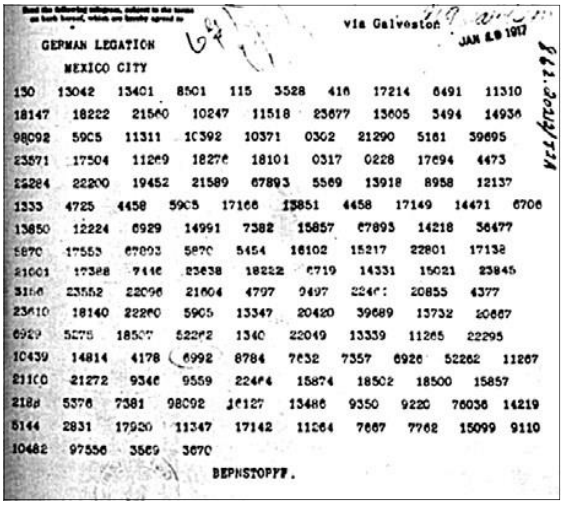


Abb. 14: Ein codiertes Telegramm (die Zimmermann Depesche). Die Codenummern haben eine variable Länge von drei bis fünf Stellen.

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.

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. 15.

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

Abb. 15: 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...." (Autor)

Der Geheimtext wird erhalten, indem man die Tabelle spaltenweise ausliest 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. 16. 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.

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.

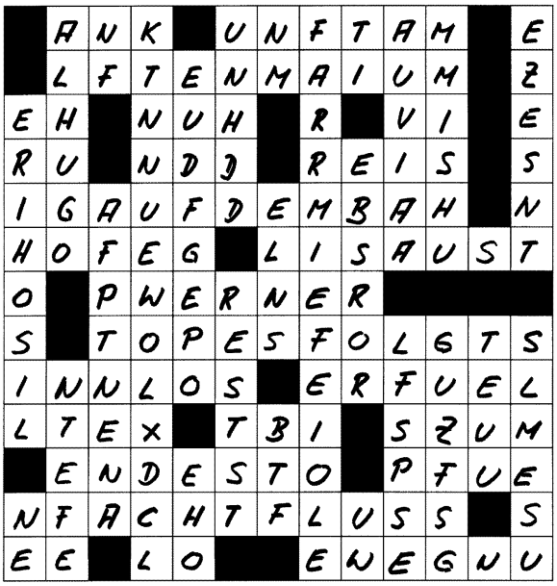


Abb. 16: Mit einer Schablone auf der Tabelle wird die Transposition etwas sicherer. Der Geheimtext beginnt mit: ERIHO SILNE ALHUG ONTEF ENFAF...(Autor)

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.

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. 17 erkennt man, worauf sie beruht.

Abb. 17: Zwei geordnete, gegeneinander verschobene Alphabete, sie sind die Grundlage der Substitutionsmethode nach Cäsar. (Autor)

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 Sicherheitsgründen lässt man sie aber meist weg. Die Buchstaben des Klartextes werden hier durch andere ersetzt, substituiert, daher die Bezeichnung "Substitutionsmethode". Es gibt 26 Möglichkeiten, die Buchstaben in der unteren Reihe geordnet einzutragen, aber nur deren 25 sind sinnvoll, die 26. bewirkt nichts.

Das Schema nach Abb. 17kann jederzeit und ohne weitere Anweisungen erstellt werden. Es lässt sich auch kreisförmig anordnen, siehe Abb. 18, so entsteht die "Chiffrierscheibe".

Man muss lediglich wissen, um wie viele Positionen die beiden Reihen gegeneinander 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 X 10^{26}. Eine dieser Permutationen, willkürlich ausgewählt, zeigt Abb. 19, 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.

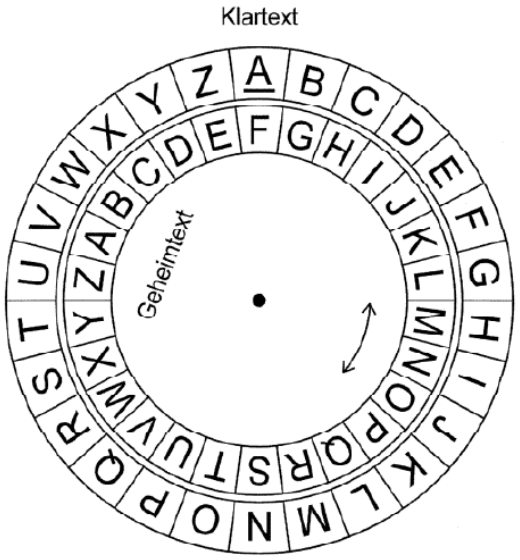


Abb. 18: Die Tabelle nach Abb. 17 ist hier kreisförmig auf einer Scheibe dargestellt. Der innere Ring lässt sich drehen, so dass sich alle 26 Schlüssel einstellen lassen. Hier ist der Schlüssel „F“ oder 5 eingestellt. (Autor)

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:

```
ZARUNDIME. . . . . .
. . . . . .
```

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:

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

Dechiffrieren

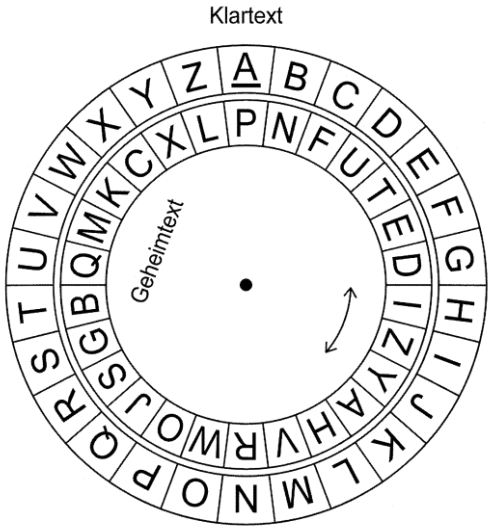


Abb. 19: Die Substitutionsscheibe mit ungeordnetem Alphabet im inneren Kreis. (Autor)

Zum Dechiffrieren wird der Geheimtext auf der unteren Reihe (Abb. 17) oder auf dem inneren Ring (Abb. 18 und 19) 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. 18 wesentlich schneller geht als bei jener nach Abb. 19, 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. 19, 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 Umsetztabelle arbeiten, haben die Eigenschaft, dass gleiche Buchstaben des Klartextes im Geheimtext wohl andere, aber ebenfalls gleiche Buchstaben erzeugen. Bei der Tabelle nach Abb. 17 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 Buchstaben in einem stetig fliessenden Strom verarbeitet wird.

Abb. 20: Leon Battista Alberti, 1404 in Venedig geboren, soll die Chiffrierscheibe erfunden haben.

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. 21.

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%

Abb. 21: Statistische Buchstabenhäufigkeit bei englisch- und deutschsprachigem Text.

Für die deutsche Sprache zeigt die Abb. 22 die Verteilung als Balkengrafik. Besonders auffallend ist die E-Spitze, die gut 17 % erreicht.

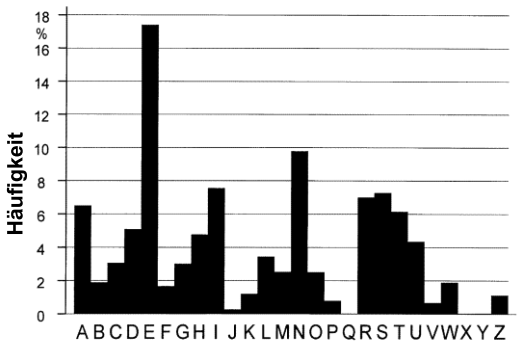


Abb. 22: Grafische Darstellung der Buchstabenhäufigkeit bei der deutschen Sprache. (Autor)

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. 22. 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. 22 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 24 und 25. 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.

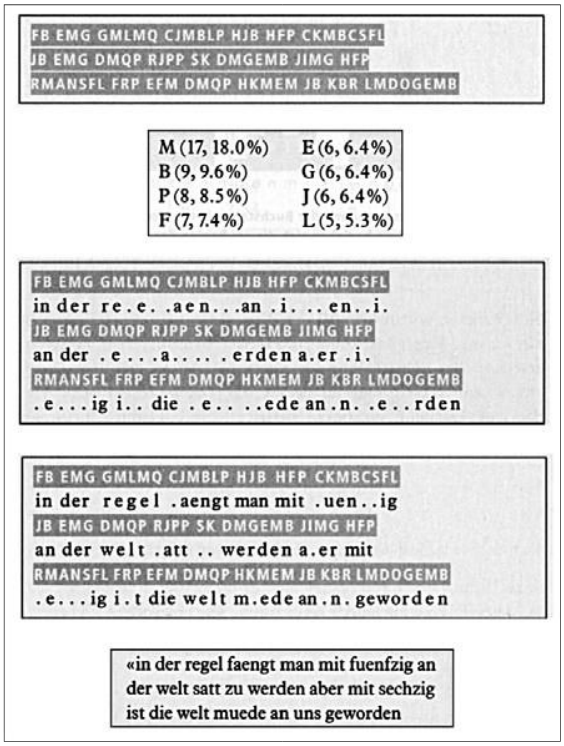


Abb. 23: Schrittweises Brechen eines monoalphabetisch chiffrierten Textes. Die beibehaltenen Wortzwischenräume erleichtern die Arbeit wesentlich. (Autor)

Abbildung 23 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. 22. 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

Abb. 24: Häufigkeit des Vorkommens aller Bigramme in deutschsprachigem Text. Zahlen in %% (pro 10'000).

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

Abb. 25: Die wichtigsten Trigramme in deutschsprachigem Text, ebenfalls in %%.

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. 26 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

Abb. 26: Tabelle zur Durchführung einer homophonen Substitution. (Autor)

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. 22 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. 27. 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. 27 brauchen wir eine leere Tabelle gemäss Abb. 28. 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 27 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. 18 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', genauso 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.

Schlüssel	Klartext: 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

Abb. 27: Tabelle für die Verschlüsselung nach Vigenère. Man kann sie als Erweiterung der Tabelle nach Abb. 14 sehen; es sind hier alle 26 möglichen «Cäsar-Schlüssel» aufgeführt. (Autor)

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	.	.

Abb. 28: Beispiel einer Vigenère-Verschlüsselung. (Autor)

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.

Abb. 29: Blaise de Vigenère, der Erfinder der polyalphabetischen Substitution.

Kryptanalyse 2

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!

Abb. 30: Charles Babbage. Ihm gelang das Brechen eines nach Vigenère chiffrierten Textes.

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. 32. 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 derselben 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. 33 zeigt dazu ein Beispiel. Identische Folgen sind unterstrichen. Sie sollten mehr als zwei Buchstaben umfassen, je länger eine Folge ist, umso mehr Gewicht wird man ihr beimessen. In Abb. 34 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. 22 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 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.

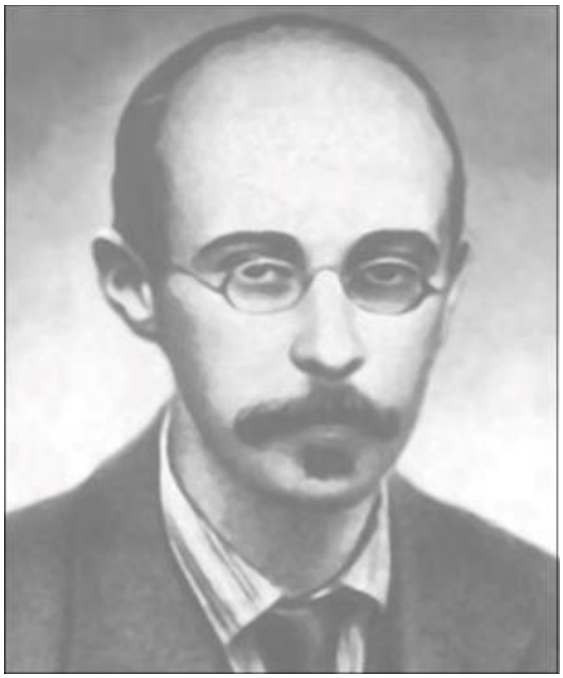


Abb. 31: William Friedman entwickelte ein mathematisches Verfahren zum Brechen der polyalphabetischen Verschlüsselung.

Er erfand ein Verfahren zur Ermittlung der Schlüsselwort-Länge, das auf rein mathematischer Basis beruht. Wir wollen hier nicht auf die Details eingehen. Nur so viel: Es ist ein statistisches Verfahren, das die Buchstabenhäufigkeit im Geheimtext mit jener im Klartext in Beziehung setzt. 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 nahelegt. 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 zehnmal mehr Text, also einige tausend Zeichen. Je länger bei einem "Vigenère" das Schlüsselwort ist, umso 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 . .

Abb. 32: Hier erkennt man, wie in speziellen Situationen gleiche Klartextpassagen identische Geheimtextmuster ergeben. (Autor)

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.

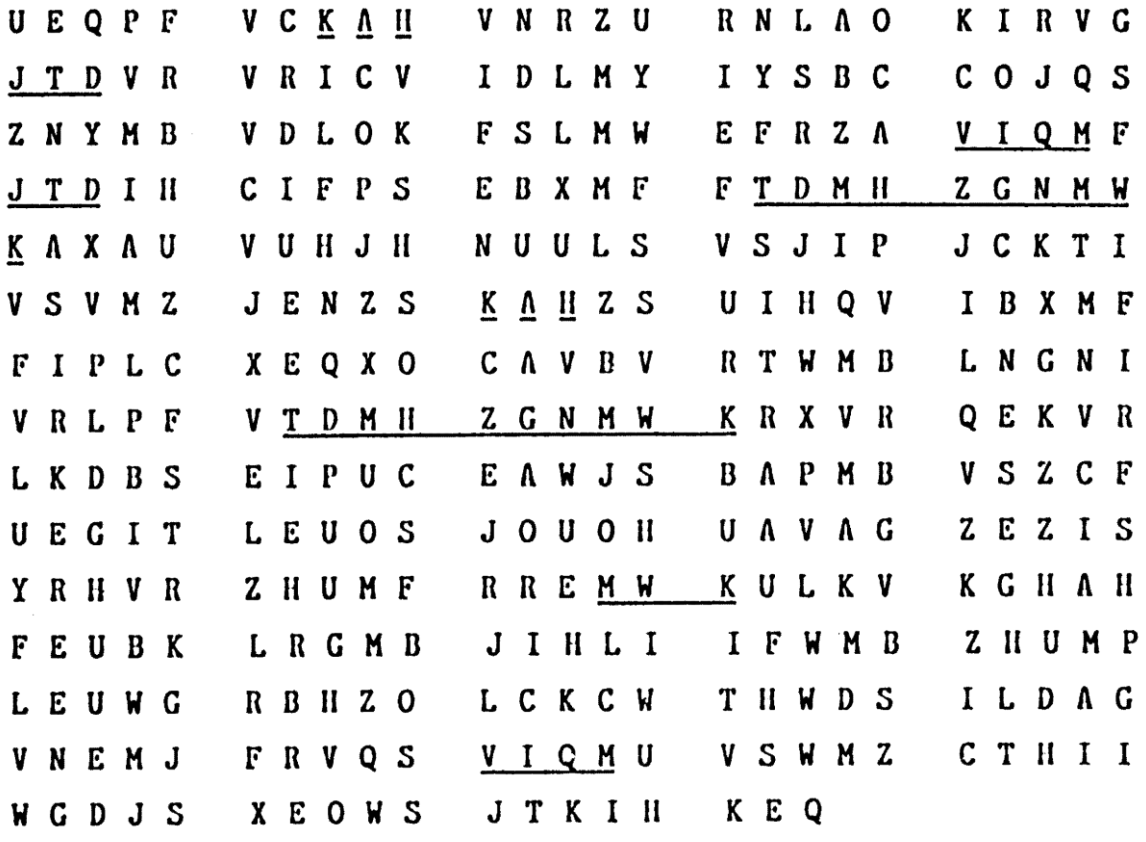


Abb. 33: Dieser Geheimtext entstand durch eine polyalphabetische Substitution. Für die Kryptoanalyse werden identische Folgen gesucht, die eine minimale Länge aufweisen sollten.

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

Abb. 34: Die Analyse des obigen Beispiels. Die Länge des Schlüsselwortes wird mit grosser Wahrscheinlichkeit den Wert 5 haben.

Unter den folgenden Bedingungen ist eine Verschlüsselung nach der polyalphabetischen Substitution absolut sicher, das können die Mathematiker sogar beweisen:

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

Die Befolgung dieser kryptologischen Forderungen führt zu einem polyalphabetischen Substitutionsverfahren, das als "Vernam-Chiffrierung" bekannt ist.

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.

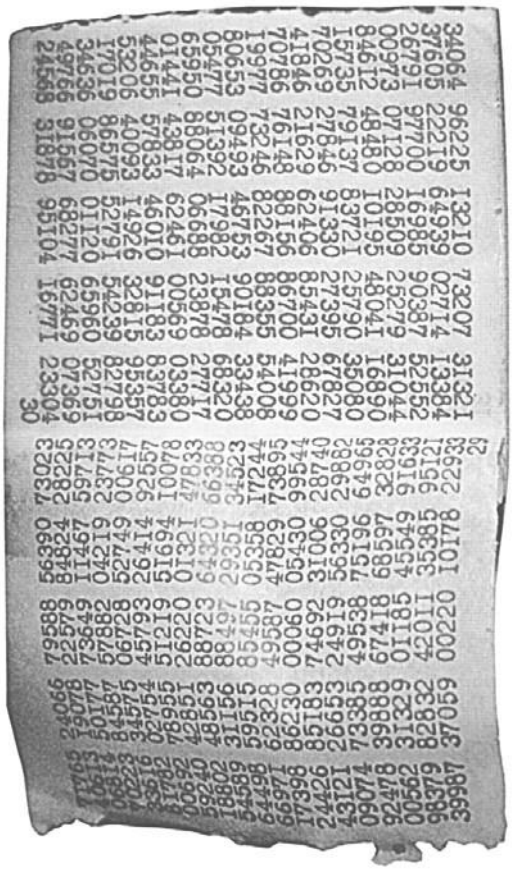


Abb. 35: Zufallszahlen für eine Vernam-Verschlüsselung. Zwei Seiten mit den Schlüsseln 29 und 30 zu je 100 Fünfergruppen wurden gedruckt.

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. 28, 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. 28, oder der Scheibe nach Abb. 18, 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.

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

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

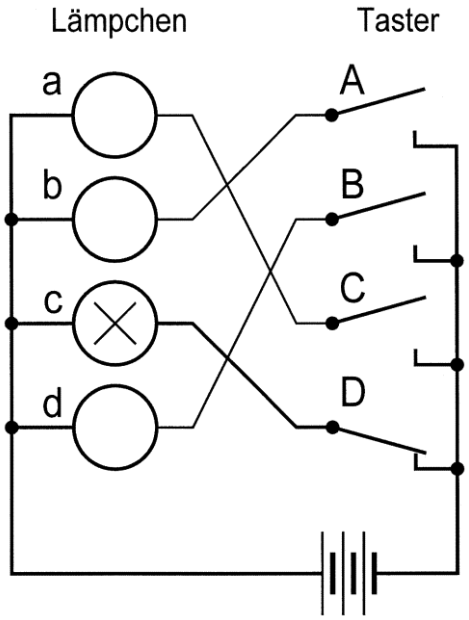


Abb. 36: Eine monoalphabetische Verschlüsselung, realisiert mit Tastern und Lämpchen. Es sind nur vier Einheiten gezeichnet, tatsächlich sind es deren 26. (Autor)

Abb. 36 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.

Der Rotor

Der Rotor ist ein zentrales Bauteil, dem wir noch oft begegnen werden. Abb. 37 zeigt einen Rotor aus einer Chiffriermaschine, der 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. 38 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.

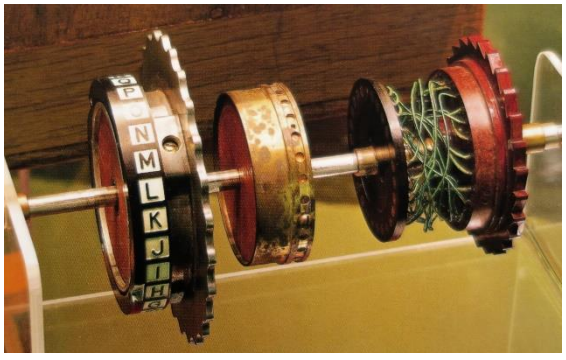


Abb. 37: Geöffneter Rotor einer Enigma Maschine. Gut sichtbar ist die Verdrahtung.

Automatischer Vorschub

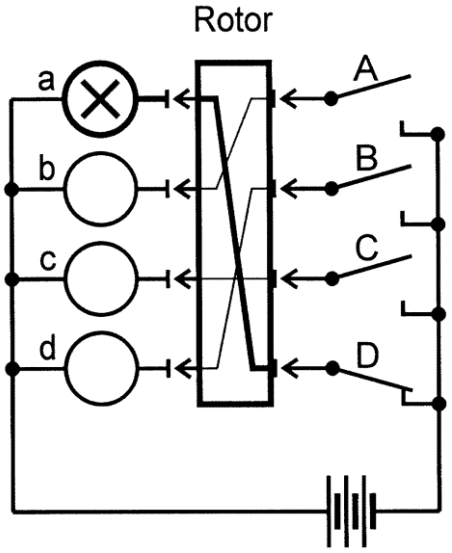


Abb. 38: Der Rotor wird eingesetzt. (Autor)

Jetzt versehen wir unsere Einrichtung nach Abb. 38 mit einer Vorschubmechanik. Bei jeder Tasterbetätigung soll der Rotor mit einer Antriebsklinke um eine Position weitergedreht werden. Es ist nicht wichtig, welcher Taster betätigt wird, der Rotor wird in jedem Fall um eine Position weitergedreht. 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 voneinander 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. 39. 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. 38 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.

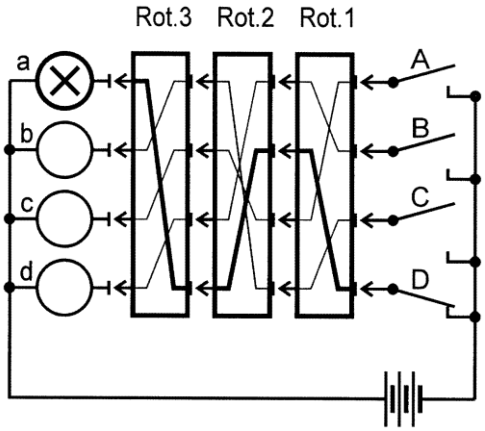


Abb. 39: Die Anordnung mit drei Rotoren. (Autor)

Die "Maschine" nach Abb. 39 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.

Abb. 40: Arthur Scherbius, der Urvater der Enigma

Wie dechiffrieren?

Wir können mit der Maschine nach Abb. 39 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 Chiffrierscheibe nach Abb. 18. 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.

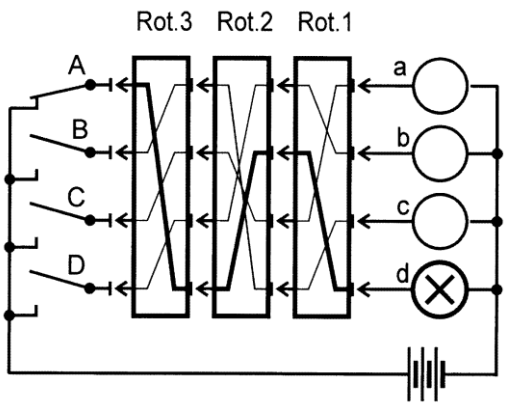


Abb. 41: Zum Dechiffrieren könnte man Tastatur und Lampenfeld miteinander vertauschen. (Autor)

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. 41. 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.

Einführung des Reflektors

1926/27 löste der Deutsche Willi Korn das Problem mit einer genialen Erfindung. Abb. 42 zeigt in vereinfachter Darstellung, was er im Prinzip gemacht hat.

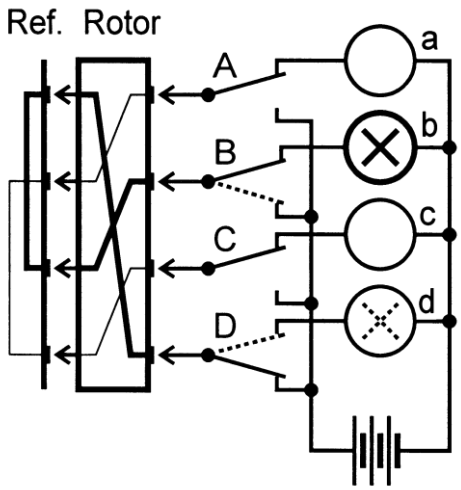


Abb. 42: Der Reflektor des Deutschen Willi Korn. Die gestrichelten Linien zeigen die Verhältnisse beim Dechiffrieren. (Autor)

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 Tasteturhebeln 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 fortlaufend 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!

Involutorische Permutation

Die Einführung des Reflektors bewirkt eine sogenannte involutorische oder reziproke Permutation. Abb. 43 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. 42 festgestellt. Man hat bei der involutorischen Permutation bedeutend weniger Möglichkeiten als z.B. bei der Tabelle nach Abb. 19, 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. 44 ist die umgezeichnete Abb. 43 zu erkennen, die Zuordnungen von der oberen zur unteren Reihe verlaufen "gradlinig".

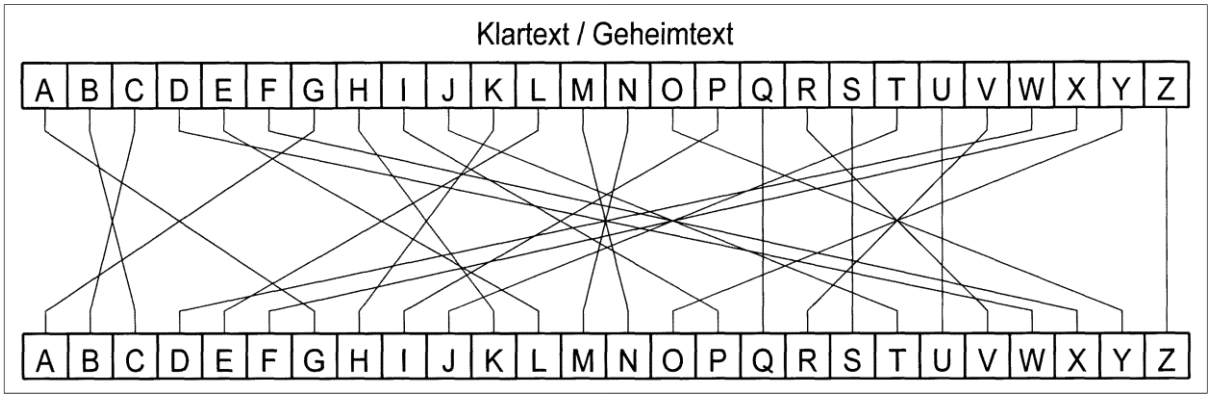


Abb. 43: Eine involutorische Umsetzung. (Autor)

Klartext / Geheimtext

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

Abb. 44: Die gleiche Zuordnung wie oben, die untere Zeile ist so geordnet, dass eine „gerade" Zuordnung entsteht zwischen den Zeilen. (Autor)

Die Enigma

Abb. 45: Nachbau einer Enigma Maschine (EnigmaMuseum.com). Funktionierende Originale werden heute zu einem Preis von gegen USD 200'000.- gehandelt. Der vordere Deckel enthält aus Geheimhaltungsgründen den Vermerk „Klappe schliessen", damit man die Steckerverbindungen nicht sehen konnte.

Wenn wir in der Anordnung mit den drei Rotoren (Abb. 39) 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. 46 ist das Prinzip dargestellt. Zusätzlich ist ein Steckerbrett vorhanden.

Um 1942 wurde bei den Marine-Maschinen noch ein vierter Rotor eingebaut, man wollte die Sicherheit erhöhen. Aus Platzgründen war dieser schmaler als die übrigen. Man beschriftete ihn mit einem griechischen Buchstaben, deshalb die Bezeichnung "Griechenwalze", siehe Abb. 49. Viel brachte dieser vierte Rotor nicht; er bewegte sich während des Chiffrierens höchstens einmal, man denke an die Verhältnisse beim Kilometerzähler.

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.

Das Steckerbrett

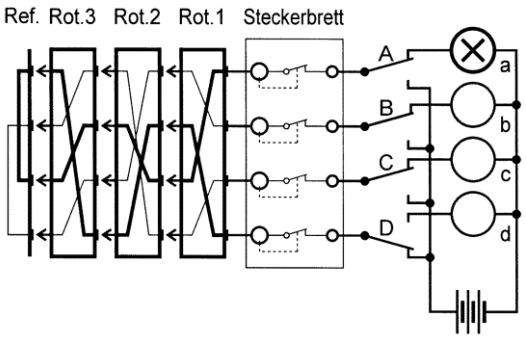


Abb. 46: Die Enigma: Drei Rotoren und der Reflektor; zusätzlich ist ein Steckerbrett vorhanden. (Autor)

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. 46 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.

Abb. 47: Doppelsteckerpaar

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. Die Abb. 50 zeigt einen symbolischen Ausschnitt des Steckerbretts, zwei Kabelverbindungen sind gesteckt. Man erkennt die aus Abb. 42 bekannte involutorische Vertauschung. Es muss unbedingt involutorisch vertauscht werden, sonst würde die Eigenschaft, dass man mit der gleichen Maschine Chiffrieren und Dechiffrieren kann, verloren gehen. Theoretisch könnte man bei 26 Buchsenpaaren 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.

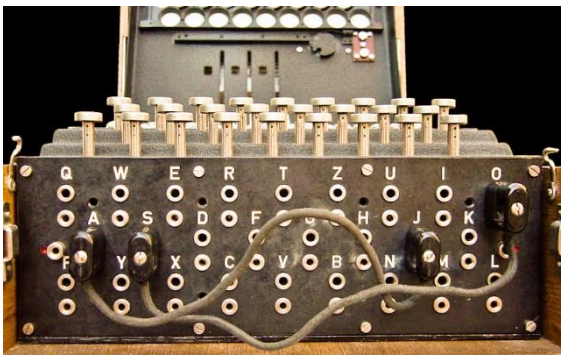


Abb. 48: Steckerbrett. Hier ist der Buchstabe „A“ mit „J“ verbunden („gesteckert“) und „S“ mit „O“.

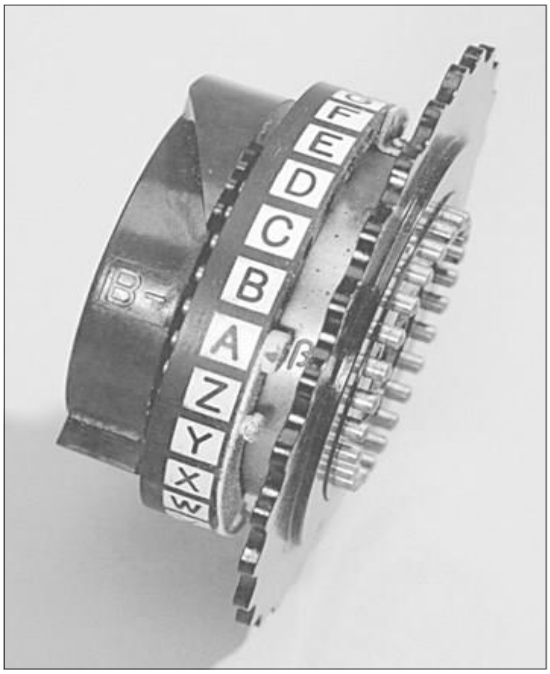


Abb. 49: Eine „Griechenwalze“. Diese vierte Walze bei der Marine-Enigma ist mit einem griechischen Buchstaben beschriftet. Hier die Walze Beta.

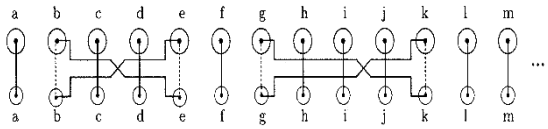


Abb. 50: Das Prinzip des Steckerbretts bei der Enigma. Zwei Doppelsteckerpaare sind verwendet, das erste von „b“ nach „e“, das andere von „g“ nach „k“

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 mechanischen Chiffriermaschine. Der Strom zeigt nur auf elegante Weise an, welche Zuordnung Taster – Lämpchen aktiv ist. Der elektrische Stromfluss hat mit der eigentlichen Kryptografie nicht direkt etwas zu tun.

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. Er muss darauf achten, dass er für jedes Telegramm eine andere, wirklich zufällige und sinnlose 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 Spruchschlüssel. 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 Gruppen 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.

Abb. 51: Der Verschlussdeckel der Holzkiste für die Enigma enthält eine Hinweisplakette zur Wartung der Maschine (Jersey War Tunnels, Foto J. Schucan 2013).

Von Marconi zu Ultra

Jürg Schucan

Einführung

«**Enigma**» war die Bezeichnung der deutschen Chiffriermaschine. «**Ultra**» dagegen war die Tarnbezeichnung für die nachrichtendienstlichen Informationen, die das britische Militär während des zweiten Weltkrieges aus der Entzifferung und Auswertung des verschlüsselten feindlichen Nachrichtenverkehrs gewinnen konnte. Eine entzifferte Meldung und das diesbezügliche Dokument wurden damit zum Bestandteil von Ultra. Das Wort «Ultra» bedeutete die höchste Stufe der Geheimhaltung und war die Kurzform von «Top Secret Ultra».

Eine ausführliche Darstellung der kryptologischen Erfolge auf nicht-europäischen Kriegsschauplätzen, v.a. im Pazifik, würde den Rahmen dieser Arbeit sprengen. Darum beschränke ich mich auf ein paar Beispiele: Die Amerikaner knackten den japanischen «**Purpurcode**», den der diplomatische Dienst der Japaner verwendete (mit Maschinen, die an die Konstruktion der Enigma angelehnt waren) und den **JN25 Code** der japanischen Marine, eine Mischung von Code und Chiffre. Der für die Amerikaner erfolgreiche Ausgang der **Schlacht von Midway** anfangs Juni 1942 ist zu einem guten Teil den Kryptologen zu verdanken, die schon früh aufgrund abgefangener Meldungen erkannten, dass das Ziel der japanischen Flottenverbände Midway sein werde. Abgefangen wurde unter anderem die Meldung eines japanischen Aufklärungsflugzeuges, in der die Buchstaben «AF» vorkamen. Die Überprüfung mit einer erbeuteten japanischen Gradnetzkarte ergaben für A und F die Koordinaten für ein Gebiet, in dem Midway lag.

Weiter knackten die Amerikaner den «**Maru-Code**», der von den Versorgungsschiffen der Japaner verwendet wurde. Die Versenkung von weit über 1000 japanischen Handelsschiffen war die Folge.

In die Geschichte eingegangen ist die «**Operation Vengeance**»: Als den Amerikanern eine Inspektionsreise des Admirals Yamamoto nach Bougainville durch das Abhören und Dekodieren eines japanischen Funkspruchs bekannt wurde, führte dies zum Abschuss seines Flugzeuges am 18. April 1943 in der Nähe des Flugfeldes Buin durch «Lightning» - Langstreckenjäger. Yamamoto galt als der verantwortliche Admiral für den Angriff auf Pearl Harbour am 7. Dezember 1941.

Und schliesslich war auch die Versenkung des Superbattleships «**Yamato**» (deutsch: «grosser Frieden») mit seinen neun 46cm Kanonen auf die Entschlüsselung japanischer Meldungen zurückzuführen.

Abb. 52: Die «Yamato» und ihr bereits im Oktober 1944 versenktes Schwesterschiff «Musashi» waren mit rund 70'000t die grössten je gebauten Schlachtschiffe. Mit der Versenkung der «Yamato» am 7. April 1945 war die Zeit der Schlachtschiffe vorbei (Yasukuni Museum, Foto Autor 2018).

«Come quick danger»

1860 sagte der Schotte **James Maxwell** die Existenz von Radiowellen voraus und 1887 konnte der Deutsche **Heinrich Hertz** solche Wellen experimentell nachweisen. Um 1895 begann der italienischstämmige Ingenieur und Physiker Marchese **Guglielmo Marconi** mit seinen Versuchen zur drahtlosen Übermittlung von Radiowellen. Mit den vom ihm

konstruierten Sendern, Empfängern und Antennen gelang ihm die Überbrückung von ständig grösseren Entfernungen, zuerst 1899 über den Ärmelkanal und dann 1901 über den Nordatlantik von Poldhu in Cornwall nach Saint John's, Signal Hill, Neufundland.

1909 wurde erstmals der Funknotruf CQD für «Come quick danger» von einem Schiff (der «Republic» der White Star Linie) abgegeben.

Die «**Titanic**»-Katastrophe führte dann zu endgültigen Durchbruch des Schiffsfunks: In der Nacht zum 15. April 1912, um 22:25 Uhr, vernahm der Funker der Station auf Cape Race (Neufundland) das maritime Notrufsignal CQD (für «Come quick danger»). Zusätzlich wurde auch der neu eingeführte und einprägsamere SOS-Code gesendet. Der Hilferuf kam vom rund 600km entfernten Passagierschiff «Titanic», das soeben einen Eisberg gerammt hatte und am Sinken war. Die «Titanic» hatte schon vorher in Funkkontakt gestanden, u.a. für die Weiterleitung von Meldungen ihrer Passagiere. Das Schiff war mit einem Marconi Löschfunkensender (arbeitete auf Langwellen, noch ohne Röhren. Informationen zur Funktionsweise im Internet unter dem Suchbegriff «Löschfunkensender», Videobeitrag Präsentation Ustertag 2014) ausgerüstet. Je nach Tageszeit schwankte die Reichweite zwischen 350 und 2000 Seemeilen. Der Notruf wurde auch von der «RMS Carpathia» (RMS bedeutet Royal Mail Ship. Das Schiff gehörte der Konkurrenzlinie Cunard) empfangen, die sich vier Stunden später an der Unglücksstelle einfand. Die «Carpathia» lief mit den 710 geretteten Passagieren am Abend des 18. April 1912 in New York ein.

Die publikumswirksame «Titanic»-Katastrophe führte zu zahlreichen Verbesserungen der Sicherheit auf See, wozu auch die Ausrüstung der Schiffe mit Funkgeräten gehörte. Die neue Übermittlungstechnik, deren Nutzen nun ausser Zweifel stand, rief selbstverständlich auch die Militärs auf den Plan.

Die Risiken des Funkverkehrs - Tannenberg

Bereits im Russisch-Japanischen Krieg (1904/1905) wurde auf beiden Seiten mit drahtloser Telegrafie experimentiert, sowohl mit Geräten von Marconi als auch mit deutschen Geräten der Firma Slaby-Arco, die sich aber angeblich nicht bewährt haben.

Trotz der beachtlichen Fortschritte in den folgenden zehn Jahren steckte die Funktechnik auch nach 1914 noch in den Kinderschuhen. Die Anlagen waren sperrig und schwer zu transportieren, die Übertragung war langsam und erfolgte ausschliesslich in Morsetelegraphie, so dass die Armeen zeitweilig auch unverschlüsselt funkten. Per Morsetelegraphie war eine Übertragungsgeschwindigkeit von 60 bis 120 Buchstaben pro Minute machbar, abhängig von der Qualität der Verbindung und dem Können des Funkers. Pannen gab es auch bei der Verteilung von Chiffrierbüchern. Im Ersten Weltkrieg waren die Russen besonders nachlässig und die Deutschen wussten häufig sehr früh von den russischen Absichten.

In die Geschichte eingegangen ist der unverschlüsselte Funkverkehr vor der Schlacht von Tannenberg. **Ludendorff** führt in seinen Kriegserinnerungen (S.38) folgendes aus: «Auf der Fahrt von Marienburg nach Tannenberg [Anmerkung: am 24. August 1914] hatten wir einen aufgefangenen feindlichen Funkspruch, der uns ein klares Bild über die gegnerischen Massnahmen in den nächsten Tagen gab, zugesandt erhalten. Die **Narew-Armee** marschierte links gestaffelt mit dem VI. A.K. über Ortelsburg auf Bischofsburg, das am 26. erreicht oder durchschritten werden konnte, mit dem XIII. A.K. von Neidenburg über Passenheim auf Allenstein. Es folgten das XV. und XXIII A.K. mit denen General v. Scholtz in diesen Tagen gekämpft hatte. Ihre südlichste Staffel war am 26. etwa bei Waplitz zu suchen. Noch weiter links rückwärts und nach Westen herausgeschoben, marschierte über Mlawa und Soldau das I. A.K., durch einige Kavallerie-Divisionen gegen Lautenburg und Strasburg gedeckt».

Damit war Ludendorff praktisch das gesamte Dispositiv der russischen 2. Armee unter General **Alexander Samsonow** bekannt. Diese russische Armee bewegte sich Richtung Nordwest auf Tannenberg zu und für Ludendorff stellte sich nur noch die Frage, wann er genügend Kräfte gesammelt haben würde um «in diese Bewegung mit der südlichen Gruppe der 8. Armee von Westen her hineinzustossen».

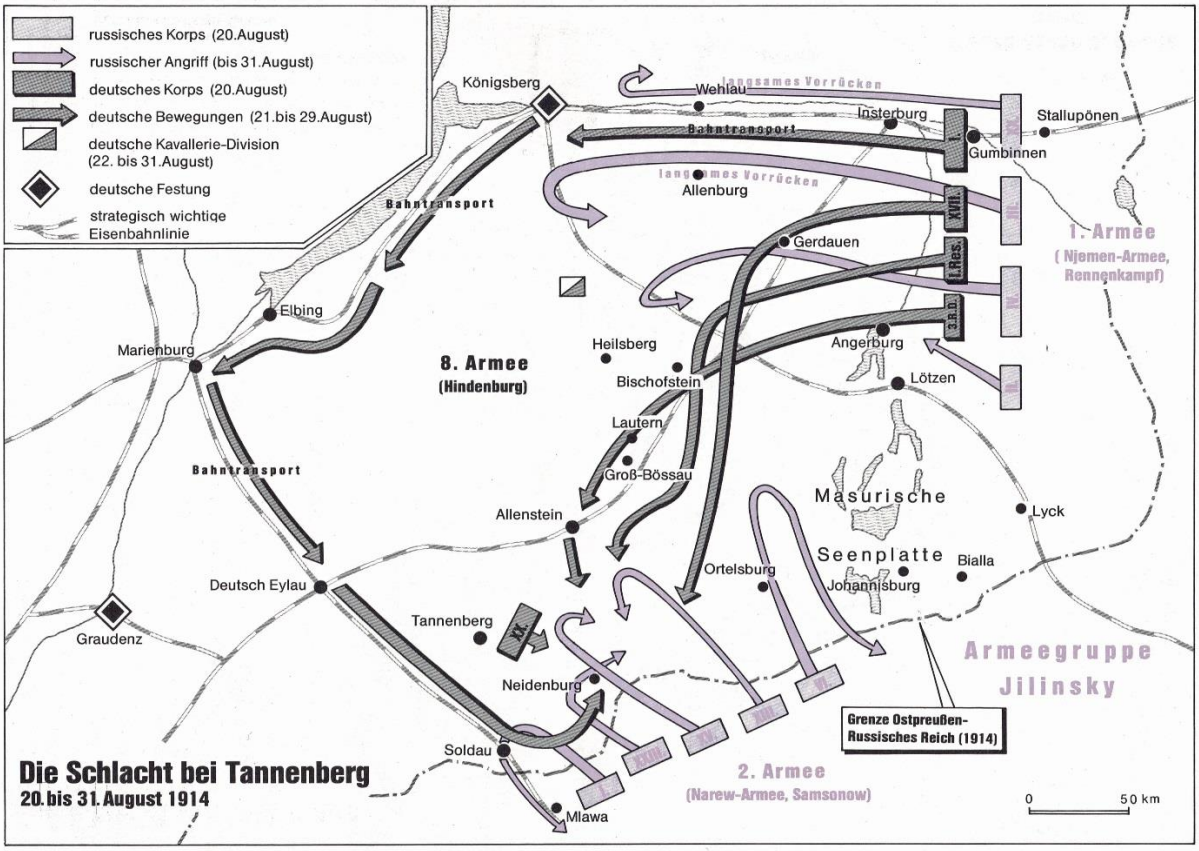


Abb. 53: Die Karte illustriert, dass die Einkesselung der drei russischen Korps (XXIII., XV, und XIII.) etwa 80km etwas nord-östlich der Ortschaft Tannenberg (heute Stebark) bei der heutigen Ortschaft Olsztynek stattgefunden hat (aus: Christian Zentner, Illustrierte Geschichte des Ersten Weltkriegs, 1980, S. 420). Die Deutschen zählten 92'000 russische Gefangene sowie 50'000 russische Gefallene und Verwundete.

Am Morgen des 25. August 1914 hatte Ludendorff ein weiteres Mal Glück: Man hatte den vollständigen unverschlüsselten Befehl an die russische **Njemen Armee** unter General **Rennenkampf** abgefangen. Diese hatte den Auftrag erhalten, nicht etwa nach Süden zu marschieren, um dort Samsonow zu unterstützen, sondern langsam nach Westen vorzurücken, um Königsberg zu belagern. Rennenkampf hatte zwar bemerkt, dass die ihm gegenüberstehenden deutschen Kräfte ausgedünnt wurden, vermutete aber zu Unrecht, die Deutschen würden sich in die Festung Königsberg zurückziehen. Aufgrund der Funkmeldung wussten nun Ludendorff und Hindenburg, dass ihrer 8. Armee von Osten her keine unmittelbare Gefahr drohte und man konnte in aller Ruhe über die Narew-Armee im Süden herfallen.

Die berühmte Umgehungsschlacht begann am 27. August 1914 und am 30. August waren drei russische Korps der **Narew-Armee** vernichtet und zwei weitere in die Flucht geschlagen. General Samsonow beging Selbstmord.

Die Zimmermann Depesche

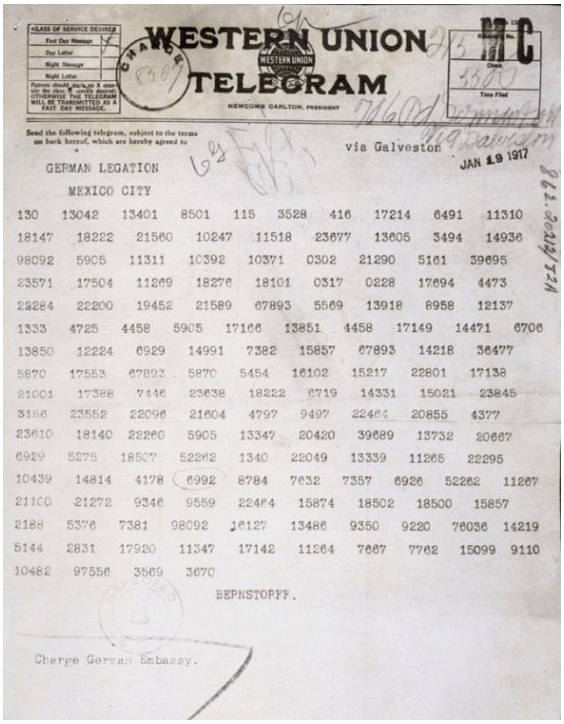

WESTERN UNION
TELEGRAM
via Galveston
JAN 19 1917
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670
BERNSTORFF.
Charge German Embassy.

Abb. 54: Die Zimmermann Depesche (aus Wikipedia)

Die Deutschen wussten, dass ihre Wiederaufnahme des uneingeschränkten U-Boot-Krieges ab dem 1. Februar 1917 die Amerikaner zum Kriegseintritt veranlassen

könnte. Im Hinblick darauf suchten sie neue Verbündete. Vielleicht könnte man die USA vor ihren eigenen Türen in einen Krieg verwickeln und damit den Kriegseintritt der USA in Europa hinauszögern. Dies war das Ziel der so genannten Zimmermann Depesche. Geschrieben hatte sie **Arthur Zimmermann**, ein Staatssekretär im Auswärtigen Amt, an den deutschen Botschafter in Washington. Zimmermann führte in seinem Telegramm aus, wie Mexiko zu einer Kriegserklärung an die USA zu bewegen wäre. Dafür hätte Deutschland finanzielle Unterstützung an Mexiko geboten. Ausserdem sollte Mexiko verlorene Gebiete im amerikanischen Südwesten zurückerhalten (Texas, Arizona und New Mexico). Die Übermittlung der Depesche geschah über ein Kabel, das die Briten bereits angezapft hatten.

Zwar war die Depesche mit einem Codebuch verschlüsselt worden, aber die britische Dechiffrierabteilung des legendären «**Room 40**» hatte nicht nur die meisten deutschen Codes gebrochen sondern war auch im Besitz von Codebüchern, die in ihre Hände gefallen waren. Nach einer ersten teilweisen Entschlüsselung (z.B. stand die Zahlenfolge «67893» für «Mexiko») hatten die Briten das Glück, dass der deutsche Botschafter in den USA, Bernstorff, das Telegramm mit einem älteren und ihnen bekannten Schlüssel nach Mexiko weiterleitete, was die vollständige Dechiffrierung erlaubte. Die Zimmermann Depesche wurde der amerikanischen Regierung vom Nachrichtendienst der britischen Marine aber erst übermittelt, als diese zögerte, auch nach der Wiederaufnahme des U-Boot-Kriegs in den Krieg einzutreten.

Die Zimmermann Depesche wurde am 1. März 1917 von der amerikanischen Regierung der Presse bekannt gegeben. Den Amerikanern wurde nun klar, dass die Zeit des Isolationismus vorbei war. Am 6. April erklärten die USA dem Deutschen Reich und seinen Verbündeten den Krieg.

Die Entschlüsselung der Zimmermann Depesche gilt seither als einer der bedeutendsten Einzelerfolge in der Geschichte des Dechiffrierens.

Das Wunder an der Weichsel

Polnische Mathematiker haben die Saat gesät, die es erlaubte, die Ernte in Bletchley Park einzubringen. Dies geschah nicht zufällig, sondern muss vor dem Hintergrund der polnischen Geschichte nach dem Ersten Weltkrieg gesehen werden.

Abb. 55: Jozef Pilsudski, Marschall der polnischen Republik, 5. Dezember 1867 bis 12. Mai 1935 (Foto aus NZZ, 10. November 2018)

Für die Polen bedeutete das Ende des Ersten Weltkriegs Befreiung, Unabhängigkeit und triumphaler Neuanfang. Der Sozialist, Kriegsheld und Diktator **Jozef Pilsudski** kehrte nach anderthalb Jahren in deutscher Festungshaft am 10. November 1918 mit einem Sonderzug nach Warschau zurück und übernahm am folgenden Tag den Oberbefehl über die polnischen Truppen. Das Land hatte keine klaren Grenzen. Die Gebietsforderungen Polens waren bei den Friedensverhandlungen in Versailles nur teilweise befriedigt worden. Eine zusätzliche Ausdehnung zulasten Deutschlands kam nicht in Frage, denn sie wäre auf den Widerstand der Briten gestossen, die Deutschland als Bollwerk gegen die Bolschewiki nicht weiter schwächen wollten. Pilsudski schwebte aber ohnehin die Bildung eines antikommunistischen, polnisch-litauisch-ukrainischen Blocks vor. In der Folge stiessen im April 1920 polnische Truppen überraschend bis Odessa und im Mai bis Kiew vor. Die dann einsetzende Gegenoffensive der Roten Armee drängte die Polen bis an die Weichsel zurück. Als die Sowjetarmee bereits kurz vor Warschau stand, gelang es der polnischen Abwehr, den

Schlüssel der Roten Armee zu brechen. Pilsudski war nun in der Lage, erfolgreich die Verteidigung Warschaus zu organisieren, was als «**Wunder an der Weichsel**» bekannt wurde. Danach konnte er die Sowjettruppen wieder weit nach Osten zurückdrängen. Im Frieden von Riga (2. März 1921) einigten sich Polen und Sowjetrussland auf eine Grenzziehung entlang dem militärischen Frontverlauf.

Zum «Wunder an der Weichsel» und damit zu einem polnischen Staat, der im Osten weit über die polnische Sprachgrenze hinausreichte, haben polnische Kryptologen entscheidend beigetragen. Die führende Figur der Kryptoanalytiker war **Jan Kowalewski**, der für seine Leistungen 1922 den höchsten polnischen Militärverdienstorden «Virtuti Militari» erhielt, allerdings ohne dass die Aussenwelt über seine Aktivitäten Bescheid wusste.

Abb. 56: Oberstleutnant Jan Kowalewski, 23. Oktober 1892-31. Oktober 1965 (Foto aus Wikipedia)

Die Polen und die Enigma

Die Polen, von mächtigen und bedrohlichen Gegnern umgeben, hatten zwischen den beiden Weltkriegen einen der erfolgreichsten Nachrichtendienste der Welt aufgebaut. Ihr Code- und Chiffrierbüro BS4 (Biuro Szyfrow bedeutet Chiffrierbüro und «4» war die Deutsche Abteilung) hatte seinen Sitz in Warschau. Leiter von **BS4** war Oberst **Givido Langer**, der schon zum Wunder an der Weichsel beigetragen hatte. Nach diesem Erfolg brachen die Polen den Schlüssel der deutschen Reichswehr, den sie ohne Probleme mitlesen konnten, bis 1928 ein neuer Schlüssel in Betrieb genommen wurde. Die Polen waren sich sicher, dass die Deutschen ihren militärischen Führungsfunk nun mechanisch verschlüsselten und dass dabei höchstwahrscheinlich eine Weiterentwicklung jener handelsüblichen Enigma verwendet wurde, die von polnischen Offizieren der Abwehr auf einer öffentlichen Ausstellung gesehen worden war.

Den Polen spielte nun der Zufall in die Hände, indem es ihnen gelang, sich während einem Wochenende im Januar 1929 auf einer Zollstation Zugang zu einer Versandkiste zu verschaffen, die für die deutsche Botschaft in Warschau bestimmt war. Die Kiste enthielt eine nagelneue militärische Enigma Maschine, die durch die Experten des BS4 gründliche untersucht und dann wieder verpackt wurde. Die Polen kannten nun die Schaltverbindungen der drei Chiffrierwalzen und die Funktionsweise des Steckerbretts.

Um mit der Entwicklung Schritt zu halten, verpflichtete BS4 drei hervorragende junge Mathematiker von der Posener Universität, die damit auch die deutsche Sprache beherrschten, da Posen bis 1918 deutsch gewesen war. Es handelte sich um **Mirian Rejewski**, **Jerzy Rozycki** und **Henryk Zygalski**. Nach Ergänzungsstudien nahmen sie 1932 ihre Tätigkeit bei BS4 auf und es gelang ihnen, den Enigma Schlüssel innerhalb von viereinhalb Monaten zu brechen.

Hilfe kam zudem aus einer ganz anderen Quelle. Irgendwann zu Beginn des Jahres 1931 meldete sich ein Mitarbeiter in der Chiffrierstelle des deutschen Reichswehrministeriums bei **Hauptmann Gustave Bertrand**, Leiter des Chiffrierbüros der französischen Abwehr. Der Mann, **Hans-Thilo Schmidt**, erhielt von den Franzosen die Tarnbezeichnung «HE», die sich französisch als «**Asche**» ausspricht. Asche konnte über seinen Bruder, der ebenfalls bei der Reichswehr tätig war, gegen Bezahlung geheime Informationen beschaffen: die deutsche Heeresdienstvorschrift «Gebrauchsanleitung für die Chiffriermaschine Enigma», dazu ein Verschlüsselungsbuch mit den Schlüsseln und ein Übungsbeispiel für eine verschlüsselte Meldung mit dazugehörigem Klartext.

Abb. 57: Mirian Reyewski (Foto aus Wikipedia)

Kopien dieser Unterlagen liess Bertrand an die polnische Abteilung BS4 weiterleiten, die mit der französischen Abwehr zusammenarbeitete. Die Unterlagen wurden auch an die Briten weitergeleitet, die sich aber nicht sonderlich interessiert zeigten, so dass im Bereich von 1932 die Polen die einzigen waren, die Enigma-Meldungen dechiffrieren konnten. Zum Beispiel fingen sie im Zusammenhang mit dem Röhm-Putsch im Juni 1934 eine Meldung des Reichsluftfahrtsministeriums an die deutschen Flughafenkommandanten ab, mit dem diese aufgefordert wurden, Röhm zu verhaften, sollte er auftauchen. Die Polen waren imstande, etwa 75% der verschlüsselten deutschen Meldungen zu entziffern. Beim deutschen Einmarsch in Österreich im März 1938 (Unternehmen «Otto») konnten allerdings keine Meldungen abgefangen werden, da Funkstille befohlen war.

Die Polen konnten bis 1938 mit den von den Deutschen vorangetriebenen Verbesserungen der Enigma mithalten. Die Einführung einer vierten und fünften Walze im Dezember 1938 und die Erhöhung der Zahl der Steckerpaare überforderte sie jedoch. Sie brauchten Hilfe. Ein erstes Treffen mit den Franzosen und Briten in Paris verlief ergebnislos. Bei einem zweiten Treffen in der Nähe von Warschau im Juli 1939 offenbarten die Polen den Briten und Franzosen ihr gesamtes Wissen. Die Briten waren vertreten durch **Commander Alistair Denniston**, der bis Februar 1942 Leiter von Bletchley Park war, durch den Kryptologen **Dillwyn Knox** und durch eine dritte Person, deren Identität nicht klar ist. Die französische Delegation bestand aus **Hauptmann Bertrand** und dem Kryptologen **Hauptmann Braquenié**. Die Polen schliesslich waren durch die **Obersten Langer und Mayer, Major Ciezki,** sowie durch die drei erwähnten Kryptologen vertreten.

Die Polen überreichten den Franzosen und Engländern ihre Enigma-Nachbauten (gebaut in den AVA Fernmeldewerkstätten in Warschau) inklusive aller fünf Walzen und erläuterten ihnen ihre erfolgreichen Methodiken zur Entzifferung der deutschen Funksprüche. Sie demonstrierten ihre verschiedenen mechanischen Hilfsmittel für die Dechiffrierung, darunter ein Gerät, das sie „**Bomba**“ nannten. Dieses Gerät, von dem es nur Näherungszeichnungen gibt, durchlief alle möglichen Buchstabenkombinationen für die drei Schlüsselwalzen, bis die richtige Einstellung gefunden war, mit der dann eine Meldung auf den polnischen Enigma Nachbauten entziffert werden konnte. „Ce fut un moment de stupeur“ erinnerte sich Bertrand später an dieses Treffen.

Die polnischen Enigma Maschinen wurden im Diplomatengepäck nach Paris gebracht und Bertrand brachte eine davon am 16. August 1939 nach London. Die Mitarbeiter des BS4 setzten sich ins damals neutrale Rumänien ab und von dort weiter nach Paris. Die «Bomba»-Geräte mussten unterwegs zerstört werden, damit sie nicht in deutsche Hände fielen.

Bald nach dem beschriebenen Dreiertreffen waren die Kryptologen der britischen «Government Code and Cypher School» (Nachfolgeorganisation des «Room 40» im Ersten Weltkrieg) nach **Bletchley Park** umgezogen, wo die Arbeiten zur Entschlüsselung der Enigma-Meldungen anliefen.

Eine heimliche und gründliche Anwerbung wurde unter den Mathematikern der Universität Cambridge vorgenommen. Zu den ersten angeworbenen Mitarbeitern gehörten **Gordon Welchman** und **Alan Turing**, zwei von Bletchley’s führenden Denkern.

Nach einer abenteuerlichen Flucht gelangten Reyewski und Zygalski im August 1943 nach Grossbritannien, wurden dort aber nicht zur Entschlüsselung von Enigma Meldungen beigezogen. Reyewski dürfte erstmals aus dem Buch von Winterbotham erfahren haben, welche Bedeutung seine eigene Arbeit hatte. Reyewski starb am 13. Februar 1980 in Warschau.

Der Weg einer verschlüsselten Meldung nach Bletchley Park

Stufe 1: Y Services

«Y» steht phonetisch für die beiden ersten Buchstaben von «wireless» (deutsch für «drahtlos», also Funk). Aufgabe des «Y» Dienstes war es, den feindlichen, insbesondere den deutschen Funkverkehr abzufangen und aufzuzeichnen, dies mit einer Kette von 39 Funkabhör- und teilweise Peilstationen in Grossbritannien. Solche Stationen gab es übrigens schon im Ersten Weltkrieg.

Im Zeiten Weltkrieg wurden «Y» Stationen betrieben durch die Army, die Navy, die RAF, den Geheimdienst (MI6 und MI5), das General Post Office und die Marconi Company. Die wichtigsten Stationen der Navy waren in Scarborough und Flowerdown (in der Nähe von Winchester), diejenige der Army befand sich in Chatham (Kent) und die wichtigste RAF Station war Cheadle (Staffordshire). Hinzu kamen zahlreiche Stationen in Übersee, so in Malta (Rinella «Y» Naval Station Service), Kairo und Sarafand (heute Libanon). Zur Überwachung des japanischen Funkverkehrs befanden sich Stationen im damaligen Indien (Abbottabad und Dehli), in Singapur und später in Colombo und Mombasa.

Die ortsfesten Anlagen wurden ergänzt durch Funkabhörstationen auf Schiffen und durch mobile Stationen in Begleitung der Bodentruppen.

Die Peilstationen waren von besonderer Bedeutung im U-Boot-Krieg. Auf deutscher Seite ging man irrtümlich davon aus, dass Sendezeiten unter 30 Sekunden keine Peilung erlauben würden. Geschickte Peiler konnten jedoch ein sendendes U-Boot innert weniger Sekunden orten.

Die Funkabhörstationen verwendeten primär den National HRO Communication Receiver, ein amerikanisches Produkt, dessen technische Daten auf www.crypto-museum.com zu finden sind. Daneben wurden verschiedene weitere Empfänger eingesetzt: RCA AR-88, Hallicrafters SY-28, die britischen Modelle R-107, R-109 und andere.

Die Aufzeichnung der verschlüsselten Meldungen mit Papier und Bleistift erforderte höchste Konzentration. Es wurde verlangt, insbesondere den Anfang einer Meldung absolut genau festzuhalten, da dieser Teil meistens den Schlüssel zur Dechiffrierung lieferte. Im Falle eines fehlenden Buchstabens musste die Position genau angegeben werden. Bei schlechtem Empfang war zudem anzugeben, wie viele Textteile entgangen waren. Nach Möglichkeit wurde mehr als ein Empfänger auf eine bestimmte Frequenz eingestellt.

Abb. 58: Eine Angehörige des Womens' Royal Naval Service, eine so genannte WREN, bedient ein HRO Empfänger in Bletchley Park, wo sich auch eine Funkabhörstation befand. (Foto aus Wikipedia)

Stufe 2: Der Weg nach Bletchley Park

Die von den näher gelegenen «Y» Stationen, z.B. Chicksands Priory, abgefangenen Meldungen wurden per Motorrad-Kurier nach Bletchley Park gebracht. Für die übrigen Meldungen verwendete man Fernschreiber-Verbindungen (Kabel).

Stufe 3: Registrierung

Die Meldungen wurden in einem Registrierungsbüro erfasst und indexiert, dann nach verschiedenen Kriterien aussortiert, beispielsweise nach den Rufzeichen derselben deutschen Funkstation. Man versuchte auch herauszufinden, ob dieselbe Meldung von verschiedenen Stationen abgesetzt wurde, da die Dechiffrierung einer Meldung die Dechiffrierung einer anderen (mehr oder weniger) gleichlautenden Meldung erleichtern würde.

Abb. 59: 1943 Registrierung der Meldungen in Hut 6 (Foto Bletchley Park Museum)

Stufe 4: Auswahl von Meldungen, die sich zur Dechiffrierung eignen

Von den Stapeln der sortierten Meldungen wurden diejenigen ausgewählt, die sich am besten für die Dechiffrierung eigneten. Es ging darum, die Ringstellungen, die Walzenlage und die verwendeten Steckerverbindungen der Enigma herauszufinden. Für den Abgleich der verschlüsselten Meldung mit einem möglichen Klartext musste im Zusammenhang mit der Herkunft der Meldung eine Annahme von verwendeten Wörtern getroffen werden. Solche Wörter wurden als „crib" bezeichnet (siehe nächstes Kapitel). Geeignete Meldungen gingen nun in den Bombe room.

Die Turing Bombe

Problemstellung

Die Grundidee besteht darin, eine abgefangene codierte Meldung mit einem angenommenen Wort, das wahrscheinlich aufgrund der Situation im Text vorkommt („crib"), abzugleichen und die getroffene Annahme mit den verschiedenen möglichen Einstellungen der Enigma zu überprüfen. Mit dieser Methode gelingt es, die überwiegende Mehrzahl aller möglichen Schlüssel auszuschliessen und so zum gesuchten Tagesschlüssel zu gelangen.

Folgende Einstellungen der Enigma sind möglich:

- **Walzenstellungen**: Jeder Rotor (oder Walze) der Enigma kann in eine von 26 möglichen Stellungen gebracht werden.
- **Ringstellungen**: Mit ihr wird vorgegeben, bei welcher Walzenposition die benachbarte linke Walze einen Vorschubschritt ausführt. Zum Beispiel bei einem mechanischen Kilometerzähler ist das immer beim Übergang von 9 auf 0. Bei der Enigma ist das einstellbar, es ist somit nicht zwingend bei A auf Z. Jeder Rotor kann in eine der 26 möglichen Ringstellungen gebracht werden. Die Ringstellung kann durch Drehen des äusseren Anzeigerads gegenüber dem inneren fest verdrahteten Teil des Rotors verändert werden (siehe Abb. 67). Gleichzeitig wird auch die Übertragungskerbe verschoben. Diese bewirkt, dass bei einer vollen Umdrehung der nächste Rotor um eine Stelle weitergeschaltet wird.
- **Walzenlage**: Die drei Rotoren lassen sich in sechs verschiedenen Reihenfolgen einsetzen. Abbildung 60 zeigt, dass hier fünf Rotoren zur Verfügung stehen (römisch I bis V), von denen drei ausgewählt werden.
- **Steckerverbindungen**: Schließlich sind die doppelpoligen Steckbuchsen an der Frontplatte mit entsprechenden doppelpoligen Kabeln zu beschalten. In der Regel wurden zehn (am Anfang sechs) Kabel eingesteckt. Die jeweils obere Buchse eines Buchsenpaars hat einen etwas größeren Durchmesser (4 mm) als die untere (3 mm), so dass die Stecker nur in einer Orientierung eingesteckt werden können. So wurde sicher die gewünschte elektrische Überkreuzung und damit die Vertauschung der beiden Buchstaben erreicht.

Durch Multiplikation der unter den verschiedenen Einstellungen vorhandenen Möglichkeiten erhält man die Anzahl der bei einer Maschine gegebenen Möglichkeiten, den so genannten Schlüsselraum.

Die Ringstellungen, die Walzenlage und die Steckerverbindungen waren in einem Schlüsselbefehl für jeden Tag enthalten. Dazu kam eine Anzahl **Kenngruppen**. Diese informierten den Meldungsempfänger darüber, dass eine Nachricht für ihn bestimmt ist und von ihm entschlüsselt werden darf und hat somit keine kryptologische Bedeutung.

Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

№ 00014

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
0	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
0	28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	yko	fpz
0	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
0	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	FT	RK	YC	XQ	GB	crl	rht	ksz	ego
0	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
0	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	FR	AS	nbt	pvd	eqo	wyn
0	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
0	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vya	pbf
0	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	jlc	jbl	pvi
0	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	ctx	gns	xeg	nvo
0	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jua	zju	nss
0	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
0	17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
0	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	FS	HP	afp	uah	tpn	npf
0	15.	II	V	III	03	20	14	JD	BM	XR	LG	PC	OF	ZI	YH	VK	EW	nfk	pvm	vue	cpr
0	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgo	cmz	pdf	xuq
0	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	RE	zor	ccm	odl	ijs
0	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JF	AX	eqk	whq	avc	zpf
0	11.	V	II	I	08	20	14	HV	FP	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	icd	nxo	yxk
0	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xka	gsg	sgs
0	9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	EV	OF	RA	myh	ncz	xvx	ees
0	8.	IV	III	I	09	18	14	RG	XU	WZ	AP	LF	IY	SQ	DO	VJ	HT	ooq	xeo	ocn	kde
0	7.	II	I	V	18	13	24	EK	RO	JX	WV	HS	QP	BZ	MU	TN	CA	fmc	mkh	lhe	tmq
0	6.	III	II	IV	23	01	17	DC	VG	OL	UA	EK	ZH	YX	PW	IM	RP	tlc	wbj	sre	kjd
0	5.	V	III	I	19	23	15	QP	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd
0	4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KP	LZ	CS	WJ	NV	clc	jdh	yoq	hwt
0	3.	V	III	II	01	02	23	EI	DY	FO	SJ	FN	LB	RK	GX	AH	CU	jty	bzy	kdh	asq
0	2.	I	V	III	16	07	02	ZO	IA	VM	CT	PX	YB	HU	SD	RN	EL	uqn	nsx	jqk	pzb
0	1.	IV	I	V	20	05	10	SX	KU	QP	VN	JG	TC	LA	WM	OB	ZF	sro	eej	fnz	szk

Abb. 60: Schlüsselbefehl für einen Monat mit 31 Tagen. Zuerst war eine Schlüsseleinstellung gültig bis Mitternacht. Dann aber verlegte man den Schlüsselwechsel auf 03:00 Uhr, somit in eine Zeit mit geringerem Funkverkehr.

Um sicherzustellen, dass nicht alle Funksprüche eines Schlüsselnetzes mit identischen Schlüsseln verschlüsselt werden, was die Texte angreifbar machen würde, war vorgeschrieben, für jeden Spruch eine individuelle Anfangsstellung der drei Rotoren einzustellen, „**Spruchschlüssel**“ genannt.

Das Verfahren zur Einstellung des Spruchschlüssels ist im Beitrag von Walter Schmid unter dem Titel „Chiffrieren mit der Enigma“ beschrieben.

Abb. 61: Zeitgenössische Aufnahme von vier „Bombes“. Jede Maschine hatte einen eigenen Namen, der auf einem Schild auf der Frontseite angebracht war. Um japanische Codes zu brechen, bauten die Amerikaner aufgrund der ihnen zur Verfügung stehenden britischen Technologie Bombes mit vier übereinanderliegenden Rotorreihen. Die Turing Bombe wurde konstruiert von der British Tabulating Machine Company. Etwa 30 Stück wurden gebaut und an verschiedenen Standorten eingesetzt. (Foto Bletchley Park Museum)

Mit der Turing Bombe konnten drei Aufgaben gelöst werden:

- Finden der Ausgangsstellung der drei Enigma Rotoren durch das Testen jeder möglichen Position;
- Finden einer (angenommenen) Steckerverbindung auf dem Steckerbrett der Enigma;
- Bestätigen der Auswahl der Rotoren und von deren Reihenfolge, wie sie in die Enigma eingesetzt wurden.

Was die Turing Bombe nicht konnte, war

- weitere Steckerverbindungen herausfinden und
- den verschlüsselten Text als Klartext wiedergeben.

Die Codebrecher traten in die geheime Welt der Enigma Meldungen ein indem sie für deren Inhalt Annahmen trafen und sich dabei auf immer wieder vorkommende Textteile wie „Wetterbericht", „Keine besonderen Ereignisse" oder „Heil Hitler" stützten.

Ein solcher Textteil wurde als „crib" (engl. für illegale Übersetzung eines klassischen Textes) bezeichnet. Ohne crib funktionierte die Bombe nicht. Das Prinzip der Bombe bestand darin, dass ausgetestet wurde, ob es eine bestimmte Anfangsposition der Rotoren gibt, die verschiedene Buchstaben einer angenommenen Meldung in den abgefangenen chiffrierten Text verschlüsseln würde.

Dabei konnten Schwächen der Enigma Maschine ausgenützt werden, vor allem der Umstand, dass ein Buchstabe aufgrund der Konstruktion des Reflektors nie in sich selbst verschlüsselt werden konnte. Auch die vorschriftsgemässe Übermittlung des Spruchschlüssels lieferte Hinweise auf den verwendeten Schlüssel, indem die ersten sechs Buchstaben im Klartext zwei identische Gruppen zu drei Buchstaben bildeten. Somit war der erste und der vierte, der zweite und der fünfte, der dritte und der sechste Buchstabe im Klartext identisch (siehe Beitrag Schmid, S. 29). Die folgenden Ausführungen stützen sich im Wesentlichen auf das Buch von Dermot Turing.

Stelle im Text	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
abgefangener chiffrierter Text	S	L	Y	A	R	O	P	X	J	Q	K	E	B	K	Q	Z	A	N	Y	G
Crib (angenommener Klartext)	*K*	*E*	*I*	*N*	*E*	*X*	*B*	*E*	*S*	*O*	*N*	*D*	*E*	*R*	*E*	*N*	*X*	*E*	*R*	*E*

Abb. 62: Der obige Text „Keine besonderen Ere" (sprich: Keine besonderen Ereignisse) ist während längerer Zeit jeden Tag von einem Beobachtungsposten südlich von Alamein in der Qattara Senke in Nord Afrika gesendet worden. Bei der Entschlüsselung diente er deshalb als „Crib". Übrigens ersetzte der Funker diese Meldung später durch „Ein paar Araber und ein Kamel".Bei unserem Beispiel nimmt man aufgrund der Umstände an, dass der Absender den Satz „Keine besonderen Ereignisse" übermittelte. Der Buchstabe „X" wurde für den Leerschlag verwendet. Der Abgleich mit dem abgefangenen Text ergibt, dass kein Buchstabe in sich selbst verschlüsselt ist. Somit könnte bei unserem Beispiel der Klartext im Geheimtext enthalten sein und ist für einen Testlauf geeignet.

Nun testet die Bombe für jede Konfiguration der drei Rotoren (insgesamt 17'576), ob es möglich ist, alle ausgewählten Buchstaben des crib dem abgefangenen chiffrierten Text in den jeweiligen Positionen zuzuteilen. Erreicht werden soll ein „loop", eine Schlaufe. Dies ist in unserem Beispiel anhand der gelb markierten Positionen möglich:

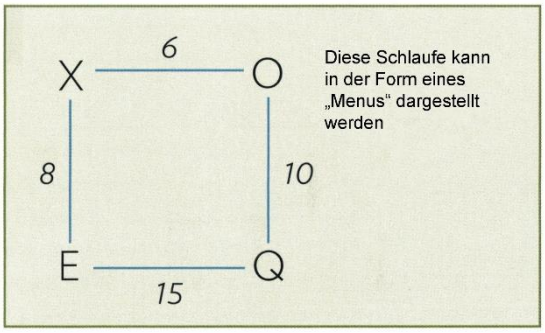


Abb. 63: 12: Schlaufe in Form eines Menus.

Vorab wird angenommen, dass der Testbuchstabe „A" mit „X" gesteckert ist;

„X" wird zu einem „O" chiffriert, wenn sich die Rotoren um sechs Stellen ab Anfangsposition gedreht haben;

„O" wird zu einem „Q" zehn Stellen ab Ausgangsposition;

„E" wird zu einem „Q" fünfzehn Stellen ab Ausgangsposition und

„E" wird zu einem „X" acht Stellen ab Ausgangsposition. Wenn somit „A" mit „X" verbunden worden ist, erhält man am Ende eines Testlaufs wieder den Buchstaben „A".

In Position 15 schliesst sich die Schlaufe. Wenn die Enigma so eingestellt ist, dass ein „E" zu einem „Q" verschlüsselt wird, dechiffriert dieselbe Maschine auch ein „Q" in ein „E".

Solche Menus wurden als Anweisungen verwendet, um eine Anzahl Rotoren der Bombe über 26- polige steckbare Kabel zusammenzuschalten, die sogenannten Letchworth Enigmas. Die Eingabe- und Ausgabebuchstaben stellten ein Buchstabenpaar dar. Einmal zusammengeschaltet konnten die

Rotoren gleichzeitig alle ausgewählten Buchstabenpaare testen um zu sehen, ob sie alle mit einer Enigma Maschine mit gleicher Anfangsposition der Rotoren verschlüsselt werden konnten. Das Menu wurde dazu verwendet eine elektrische Schlaufe zu bilden. Im Beispiel werden vier Rotor-Trios so eingestellt, um jeweilen eine Ausgangsposition für die Meldung zu testen. Bei unserem Beispiel wird das erste Rotor-Trio 6 Positionen, das zweite 8 Positionen, das dritte 10 Positionen und das vierte 15 Positionen vorgestellt. Der Output des ersten Rotor-Trios wird dann verwendet als Input für das nächste usw.

Wenn der Crib eine zutreffende Annahme war und infolge der richtigen Position (6) der Buchstabe „X“ als verschlüsselter Buchstabe „O“ erscheint, fliesst der Strom (gemäss Menu) weiter in das zweite Rotor-Trio, das sich auf Position 10 befindet, zum Buchstaben „O“. Wenn sich das zweite Rotor-Trio in der richtigen Position (10) befindet, wird der Buchstabe „Q“ erscheinen usw. Sind alle vier Positionen richtig, wird am Schluss des Tests wieder der Ausgangsbuchstabe „X“ erscheinen. Dieser Erfolg führt zum Stillstand der Bombe.

Wenn die Einstellungen nicht richtig sind und statt des gewünschten Buchstabens „X“ beispielsweise ein „L“ erscheint, wird die Bombe einen erneuten Testlauf mit der nächsten Ausgangsposition der Rotoren starten usw.

Das Steckerbrett

Bei der Enigma Maschine erreicht der elektrische Strom den ersten Rotor nachdem er das Steckerbrett durchlaufen hat. Die Bombe hat kein eigentliches Steckerbrett sondern auf der linken Seite vier Reihen von 26 Schaltern (vgl. Abb. 61). Die drei Reihen links sind mit jeweilen einer Reihe der Rotor-Trios verbunden.

Zuerst wird ein zentraler Buchstabe des Menus festgelegt. Auch hier geht man von einer Annahme aus. Bei unserem Beispiel wird angenommen, dass „X“ mit „A“ verbunden („gesteckert“) wurde. Wenn dies richtig ist, muss der Testbuchstabe „A“ am Schluss eines erfolgreichen Durchlaufs wieder als „A“ erscheinen. Auf der linken Seite der Bombe befindet sich ein Anzeigeinstrument (vgl. Abb. 64), das für jede Reihe von Rotor-Trios eine alphabetische Anzeige mit einem Anzeigestift enthält. Wenn in unserem Beispiel der Buchstabe „G“ angezeigt wird, bedeutet dies, dass „X“ nicht mit „A“, sondern mit „G“ gesteckert ist. Auch in diesem Falle wird die Bombe anhalten.

Die Auswertung der angenommenen Steckerverbindungen bei einfachen Menus führte zu oft zum Anhalten der Bombe. Hier setzt nun die Erfindung des „Diagonal Board“ durch Gordon Welchman ein, der sich den simplen Umstand zunutze machte, dass wenn z.B. der Buchstabe „A“ mit dem Buchstaben „X“ gesteckert ist, damit auch „X“ mit „A“ gesteckert ist. Das Diagonal Board bestand aus 26 Reihen mit 26 Steckerbuchsen, die durch 26-polige Kabel miteinander verbunden waren, d.h. das Diagonal Board ermöglichte die gegenseitige Verbindung von allen Buchstabenpaaren. In unserem (zutreffenden) Beispiel wird der Buchstabe „A“ in der Kolonne „X“ mit dem Buchstaben „X“ der Kolonne „A“ verbunden, was dann ermöglicht, dass der Strom am Verbindungspunkt „A“ in ein weiteres Rotoren-Trio eintritt.

Die Bombe stoppte, sobald sie eine plausible Ausgangsstellung der drei Enigma Rotoren und eine richtige Steckerverbindung des zentralen Buchstabens des Menus gefunden hatte.

Die Rotorstellung wurde auf dem zusätzlichen dreizehnten Rotor-Trio auf der rechten Seite der mittleren Rotor-Reihe angezeigt. Die Anzeige für die Steckerposition des zentralen Buchstabens des Menus befand sich an der rechten Seitenwand der Bombe in einem vorstehenden Gehäuse.

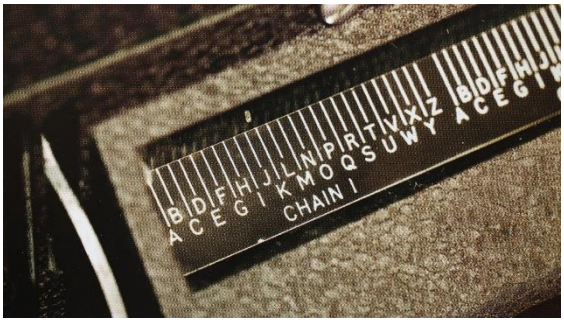


Abb. 64: Hier wird der Buchstabe „K“ angezeigt.

Die „Checking Machine“

Abb. 65: Replika einer „Checking Machine“

Die weiteren notwenigen Arbeiten wurden manuell erledigt und zwar mit Hilfe der Checking Machine, bei der es sich im Wesentlichen um einen Nachbau einer Enigma-Maschine handelte. Die Checking Machine hatte kein Steckerbrett und einen vierten Rotor, der zur Entschlüsselung von Meldungen von Vier-Rotoren-Enigmas verwendet wurde.

Die erste Aufgabe bestand darin, die weiteren (in der Regel) neun Steckerverbindungen zu finden.

Zurück zu unserem Beispiel: Durch den Testlauf der Bombe wissen wir, dass der zentrale Buchstabe des Menus „A“ mit dem Buchstaben „X“ gesteckert ist. Wenn somit der Funker den Buchstaben „X“ drückt, wird dieser aufgrund der Steckerverbindung zum Buchstaben „A“, bevor er in den ersten Rotor eintritt.

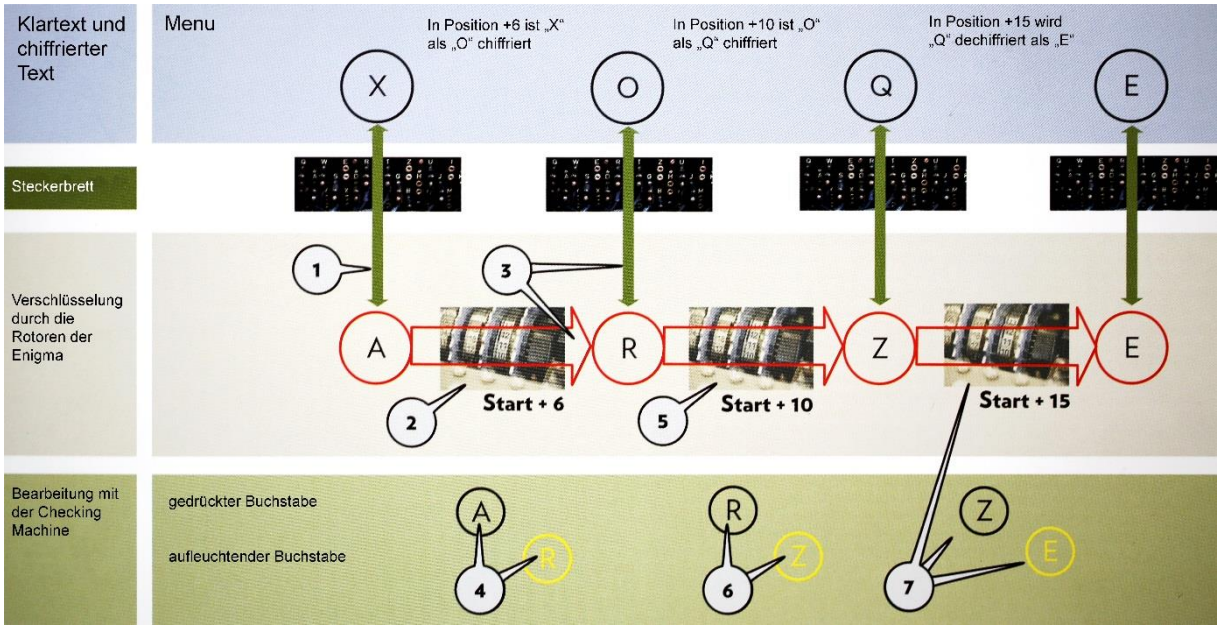


Abb. 66: Darstellung der Prüfung mit der Checking Machine

1. Der Test mit der Bombe hat ergeben, dass „X“ mit „A“ gesteckert ist und dass sich die Rotoren der Enigma in der Startposition „+6“ befinden.
2. Die Rotoren der Checking Machine werden nun um 6 Positionen nach vorne bewegt.
3. Im Menu wird „X“ zu „O“. Im Rotor der Enigma wird „A“ zu „R“.
4. Wenn nun bei der Checking Machine der Buchstabe „A“ gedrückt wird, leuchtet der Buchstabe „R“ auf. Damit wird „R“ zum Steckerbrett-Partner von „O“.
5. Nun werden die Rotoren der Checking Machine auf Position 10 gebracht. Damit wird „R“ zum Steckerbrett-Partner von „Q“. Im Rotor der Enigma wird „R“ zu „Z“.
6. Bei der Eingabe von „R“ in Position 10 leuchtet „Z“ auf.
7. Nun werden die Rotoren in Position 15 gebracht. Im Rotor der Enigma wird „Z“ zu „E“. Bei der Eingabe von „Z“ leuchtet „E“ auf, was bedeutet, dass „E“ nicht gesteckert ist.

Der Ablauf zur Ermittlung der Steckerverbindungen zeigt, dass mit Hilfe des Diagonal Boards und der Bearbeitung mit der Checking Machine die zehn gesteckten Buchstaben relativ einfach gefunden werden konnten. Das Steckerbrett bot damit nicht die zusätzliche Sicherheit, die man aufgrund der Anzahl Möglichkeiten im Millionenbereich erwarten könnte.

Die Ringstellungen

Wie bereits erwähnt, kann jeder Rotor der Enigma in eine der 26 möglichen Ringstellungen gebracht werden und zwar durch Drehen des äusseren Anzeigerads gegenüber dem inneren fest verdrahteten Teil des Rotors. Gleichzeitig wird auch die Übertragungskerbe verschoben, die bewirkt, dass bei einer vollen Umdrehung der nächste Rotor um eine Stelle weitergeschaltet wird.

Abb. 67: Die drei voranstehenden Abbildungen zeigen die Veränderung der Ringstellung bei der Enigma Maschine.

Nach spätestens 26 Buchstaben einer Meldung wird der Text unverständlich, was bedeutet, dass der mittlere Rotor durch die Kerbe des rechten Rotors um eine Stelle weitergeschaltet worden ist. Durch das Weiterschieben des mittleren Rotors auf der Checking Machine wird die Verständlichkeit wieder hergestellt und man kennt nun die Ringstellung des rechten Rotors. Jetzt muss noch die Ringstellung des mittleren und allenfalls des linken Rotors gesucht werden. Die Ringstellungen dieser Rotoren können gefunden werden entweder aufgrund des (mangelhaften) Verfahrens zur Einstellung des Spruchschlüssels oder dann durch manuelles Durchtesten, „Clonking" genannt. Dabei wird der Klartextbuchstabe auf der Checking Machine gedrückt gehalten und der Rotor von Hand gedreht. Beim Aufleuchten eines Lämpchens ist der entsprechende Buchstabe ein Anwärter auf die Ringstellung für einen Tag.

Dechiffrierung und Übersetzung

Nachdem der Tagesschlüssel für die Enigma bekannt war, konnten alle Meldungen entziffert werden. Dazu wurden britische Type-X Verschlüsselungsmaschinen verwendet, die so modifiziert worden waren, dass sie wie Enigma Maschinen verwendet werden konnten. Der chiffrierte Text wurde nun mit der korrekten Schlüsseleinstellung eingegeben und die Type-X Maschine produzierte den originalen Klartext in deutscher Sprache und in Gruppen zu fünf Buchstaben. Die Type-X Maschinen hatten den Vorteil, dass sie den Text nicht mit Lämpchen wiedergaben sondern über einen Streifendrucker. Die Streifen konnten dann auf ein Blatt Papier geklebt werden.

Die anschliessende Übersetzung in die englische Sprache wurde von Experten geprüft und jede Meldung erhielt einen Prioritätsvermerk, von „Z" (=niedrig) zu „ZZZZZ" (=hoch). Weitere Experten verglichen dann die aktuellen mit früheren Meldungen und brachten entsprechende Kommentare an. Schliesslich wurde entschieden, wer eine Meldung erhalten sollte.

Ultra Meldungen

Alliierte Kommandanten in Grossbritannien und natürlich Churchill selbst erhielten Ultra Meldungen per Motorrad-Kurier oder per Fernschreiber. Die anderen Militärs erhielten die Meldungen über Funkverbindungen, wobei britische Verschlüsselungsmaschinen vor allem des Typs Type-X verwendet wurden. Den Kommandanten waren vor Ort Special Liaison Units zugeteilt, die sich nicht nur um den Funkverkehr kümmerten, sondern auch dafür sorgten, dass die Meldungen mit der nötigen Zurückhaltung verwendet wurden. Die wirkliche Quelle durfte nie erwähnt werden. Man sprach dann von „verlässlichen

Quellen“ oder von „verlässlichen Informationen“. Meldungen mussten immer „verifiziert“ werden. Geleitzüge von Italien nach Nordafrika mussten von Aufklärungsflugzeugen „entdeckt“ werden, obschon man die Route, den Standort und in den meisten Fällen auch die Ladung bereits kannte. Die Deutschen und die Italiener wunderten sich zwar, dass ihre Geleitzüge praktisch immer entdeckt wurden, zogen aber die Möglichkeit, dass der Enigma-Schlüssel gebrochen wurde, nicht in Betracht. Man suchte anderswo nach einem Leck. So wurde der italienische Hafenkommandant von Neapel, ein Admiral, seines Postens unter dem Verdacht enthoben, den Briten Informationen geliefert zu haben.

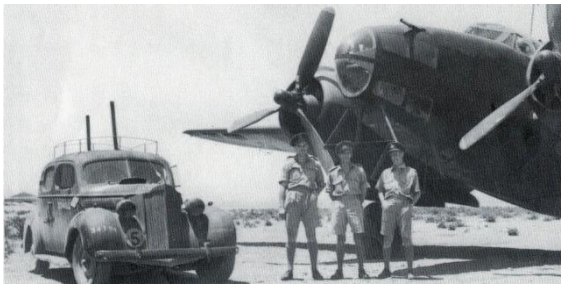


Abb. 68: Dieser Packard diente Libyen beim Hauptquartier der 8. Armee als mobile Funkstation einer Special Communication Unit (später als „Special Liaison Unit“ bezeichnet).

Die Existenz der Anlagen von Bletchley Park und ihre Funktion blieben bis 1974 geheim, was angesichts des Umstands, dass Tausende von Mitarbeitern und Mitarbeiterinnen involviert waren, wohl beispiellos ist. Diese Leute waren für Churchill die „geese that laid the golden eggs but never cackeled“ (die Gänse, die die goldenen Eier legten, aber nie schnatterten). Die Öffentlichkeit erfuhr von der Aktion Ultra erstmals durch das Buch von Colonel Frederick Winterbotham, das dieser aus dem Gedächtnis niedergeschrieben hatte. Winterbotham war damals Verbindungsmann der Royal Air Force beim Secret Intelligence Service (SIS) und war verantwortlich für die Verteilung des Ultra-Materials.

Fish

Es ist weniger bekannt, dass die Deutschen neben der Enigma eine weitere noch ausgefeiltere Chiffriermaschine entwickelten, eine Maschine, die von Hitler selbst benutzt wurde, um mit seinen Kommandeuren zu kommunizieren.

Mit der Enigma wurden nur relativ kurze Nachrichten codiert im Maximum mit rund 250 Buchstaben. Entsprechend wurde die Enigma nie auf Stufe Armee verwendet.

Das deutsche Oberkommando brauchte eine Möglichkeit, um Berichte mit Hitler auszutauschen. Das waren umfangreiche Berichte, keine kurzen Nachrichten. Ein Bericht soll sogar 60'000 Zeichen umfasst haben. Das kann man nicht mehr per Morsecode funken. Im Jahr 1941 entwarf die deutsche Firma Lorenz eine Chiffriermaschine, die den schnellen Fernschreiberverkehr verschlüsseln konnte, die **Lorenz Sz 42** (Schlüsselzusatz 42).

Abb. 69: Lorenz Sz 42 mit Lorenz Fernschreiber T 32 (Wikipedia)

Jetzt hatte man eine schnelle Form der codierten Kommunikation. Die Verschlüsselung war um einiges komplexer als bei der Enigma und man konnte lange Nachrichten übermitteln. Diese Nachrichten hätten enthüllen können, wie Hitlers Pläne aussahen und ob Täuschungsaktionen wie im Vorfeld der Invasion erfolgreich waren.

Zunächst ahnten die Briten nichts von der Existenz dieser neuen Chiffriermaschine. Im Sommer 1941 wurde der Datenverkehr in einer Londoner Überwachungsstelle abgehört, scheinbar eine Übermittlung eines Fernschreibers, doch dem war nicht so. Die Briten hatten einen Fernschreiber an das Funkgerät angeschlossen und konnten etwas Klartext lesen, doch dann setzte die Verschlüsselung ein. Da war ihnen klar, dass es eine Chiffriermaschine für den Fernschreiberverkehr geben musste, aber sie hatten keine Ahnung, wie diese Maschine aussah oder wer sie hergestellt haben könnte.

Die Briten erfuhren, dass die Deutschen die Systeme für die drahtlose Übermittlung von Funkfernschreiben «Sägefisch» nannten. Dies bewog sie dazu, den Begriff «Fish» für das Schlüsselsystem der Fernschreiber zu verwenden. «**Tunny**» (Tunfisch) nannten sie

die erste Fernschreiberverbindung und nachher wurde der Begriff für die Lorenz Sz Maschinen und den durch sie verschlüsselten Funkverkehr gebraucht.

Die Deutschen waren sich ihrer Sache sicher. Sie vertrauten dem Code. Der war auch in der Tat recht sicher. Die Schwachstelle war – wie so oft – der Mensch vor der Maschine. Am 30. August 1941 schickte ein Funker von Athen aus eine Nachricht nach Salzburg. Der Empfänger forderte den Funker auf, die Nachricht nochmals neu zu senden, nachdem er sie beim ersten Mal nicht richtig empfangen hatte. Der Funker machte nun zwei verhängnisvolle Fehler. Er schickte die rund 4000 Zeichen lange Nachricht ein zweites Mal ohne den Spruchschlüssel zu ändern. Zudem ersetzte er einige Worte durch Abkürzungen. Die Briten hatten den Funkverkehr aufgezeichnet. Die Nachrichten wurden den Wissenschaftern in Bletchley Park übergeben und es gelang dem Kryptoanalytiker **John Tiltman** in wochenlanger manueller Arbeit der Einbruch in die logische Struktur des Schlüsselzusatzes, indem er die Differenz zwischen den beiden Nachrichten bildete, und versuchte, wahrscheinliche Wörter einzusetzen.

Das reichte jedoch noch nicht, um alle zukünftigen Übertragungen zu dechiffrieren. Aber ein 24 Jahre alter Mathematiker namens **Bill Tutte** sollte das Problem lösen. Er durchsuchte die Nachricht nach Mustern. Und tatsächlich findet er eins. Es gab Wiederholungen. Das waren die Stellen, wo sich die Walzen drehen sollten. Es dauerte drei Monate und man wusste, wie die Maschine arbeitete. Doch selbst dann wusste man noch nicht, wie die Maschine wirklich aussah.

Eine einzige Lorenz-Nachricht zu dekodieren dauerte bis zu sechs Wochen, da man alles manuell machen musste. Doch im Januar 1944 kam der Durchbruch. Der erste elektronische Computer wurde gebaut, **Colossus**, konstruiert von **Tommy Flowers**. Die Hauptaufgabe von Colossus war es, die Chiffrierung der Lorenz Maschine zu knacken und die Einstellung der zwölf Walzen herauszufinden, die der Funker vorgenommen hatte, als er die Nachricht losschickte. Die verschlüsselte Nachricht wurde über Lochstreifen in Colossus eingespeist. Die rund 2500 Röhren arbeiteten dann daran, den Code zu dechiffrieren.

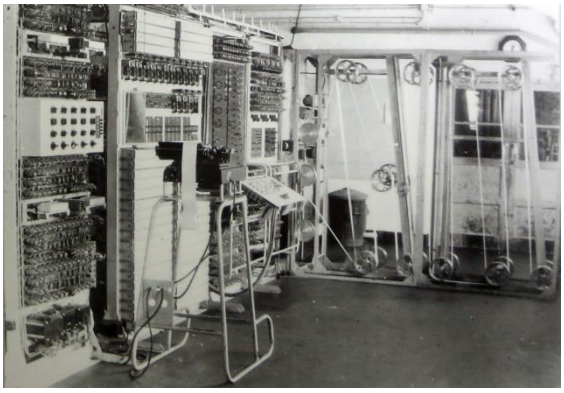


Abb. 70: Colossus Mark 10. Der heutige voll funktionsfähige Nachbau der Originalmaschine soll als eine Art Denkmal die Wissenschafter von damals ehren. Viele von ihnen waren bereits verstorben, als die Öffentlichkeit von Colossus erfuhr (Dokumentation Museum Bletchley Park, 2018).

Damals brauchte man zehn Monate für den Bau dieses Computers. Wofür die Analytiker zuvor sechs Wochen brauchten, erledigte die Maschine nun in vier Stunden. Die Briten konnten die Nachrichten der Lorenz-Maschinen mitlesen.

Die Röhren waren für die Verarbeitung zuständig. Sie waren das Herz der Maschine. Man konnte solche Verarbeitungsgeschwindigkeiten nur mit elektronischen Komponenten erreichen, damals Röhren. Am 1. Juni 1944, also unmittelbar vor der Invasion, konnte eine zweite und wesentlich schnellere Colossus Maschine in Betrieb genommen werden. Im Mai 1945 gab es bereits zehn solcher Maschinen in Bletchley Park. Insgesamt wurden vor Ende des Krieges zwölf Colossus Maschinen gebaut. Schätzungsweise 63 Millionen Zeichen von verschlüsselten Nachrichten konnten dechiffriert werden.

Neben der Lorenz Sz 42 erreichte auch der «Geheimschreiber» **Siemens & Halske T 52**, der bei der Luftwaffe zum Einsatz kann, eine gewisse Bedeutung. Allerdings wurde dieses Gerät, das vor allem im Verkehr über Kabel und beim Richtfunk eingesetzt wurde, unabhängig voneinander vom schwedischen Kryptologen Arne Beurling und in Bletchley Park gebrochen. Die Deutschen hatten nach der Besetzung Norwegens Meldungen über eine Telegraphenline durchgegeben, die vom schwedischen Geheimdienst angezapft worden war. In Bletchley Park erhielt der Geheimschreiber den Übernamen «**Sturgeon**» (Stör) Es wurden insgesamt etwa 1000 Maschinen gebaut. Davon erbeuteten die Briten während der Kämpfe in Nordafrika zwei Exemplare.

Bibliographie und weiterführende Unterlagen

«After the Battle» No. 37, *Breaking Enigma*, 1982

Beutelspacher Albrecht, *Geheimsprachen – Geschichte und Techniken*, München 5. A. 2012

Bischoff Jürgen, *Die Maschine und das Rätsel*, in GEO Epoche Nr. 67

Calvocoressi Peter, *Top Secret Ultra*, 2. A. 2011

Hinsley Francis Harry und Stripp Alan, *Code Breakers – The Inside Story of Bletchley Park*, Oxford University Press 1993, reissued 2001

Johnson Brian, *The Secret War*, 1978 (deutsche Ausgabe: "Streng geheim – Wissenschaft und Technik im Zweiten Weltkrieg»)

Jones R.V., *Most Secret War – British Scientific Intelligence 1939-1945*, 1978

Keen John, *Harold "Doc" Keen and the Bletchley Park Bomb*, 2. A. 2012, Nachdruck 2016

Kozaczuk Wladyslaw, *Im Banne der Enigma*, Militärverlag der DDR, 2. A. 1990

Lewin Ronald, *Ultra Goes to War*, 1978 (deutsche Ausgabe: «Entschied Ultra den Krieg?, 1981)

Ludendorff Erich, *Meine Kriegserinnerungen 1914-1918*, Berlin 1919

ntv-Beitrag zur «*Spionagekunst*» vom 15. Oktober 2018, 22:10 Uhr

Schmid Walter, *Die Chiffriermaschine Nema*, 3. A. 2004 (Dokumentation)

Singh Simon, *Geheime Botschaften*, Carl Hanser Verlag, 1999

Turing Dermot, *Bletchley Park – Demystifying the Bombe*, 2016

Welchman Gordon*, The Hut Six Story*, 7. A. 2018

Winterbotham Frederick, *The Ultra Secret*, 1974 (deutsche Ausgabe: «Aktion Ultra», 1976)

Wikipedia zu den Suchbegriffen: Hans-Thilo Schmidt/Mirian Rejewski/Ultra (Kryptologie)/Y-stations/Lorenz-Schlüsselmaschine/

Anhang 1: Bedienungs-Anleitung zur Chiffriermaschine «NEMA»

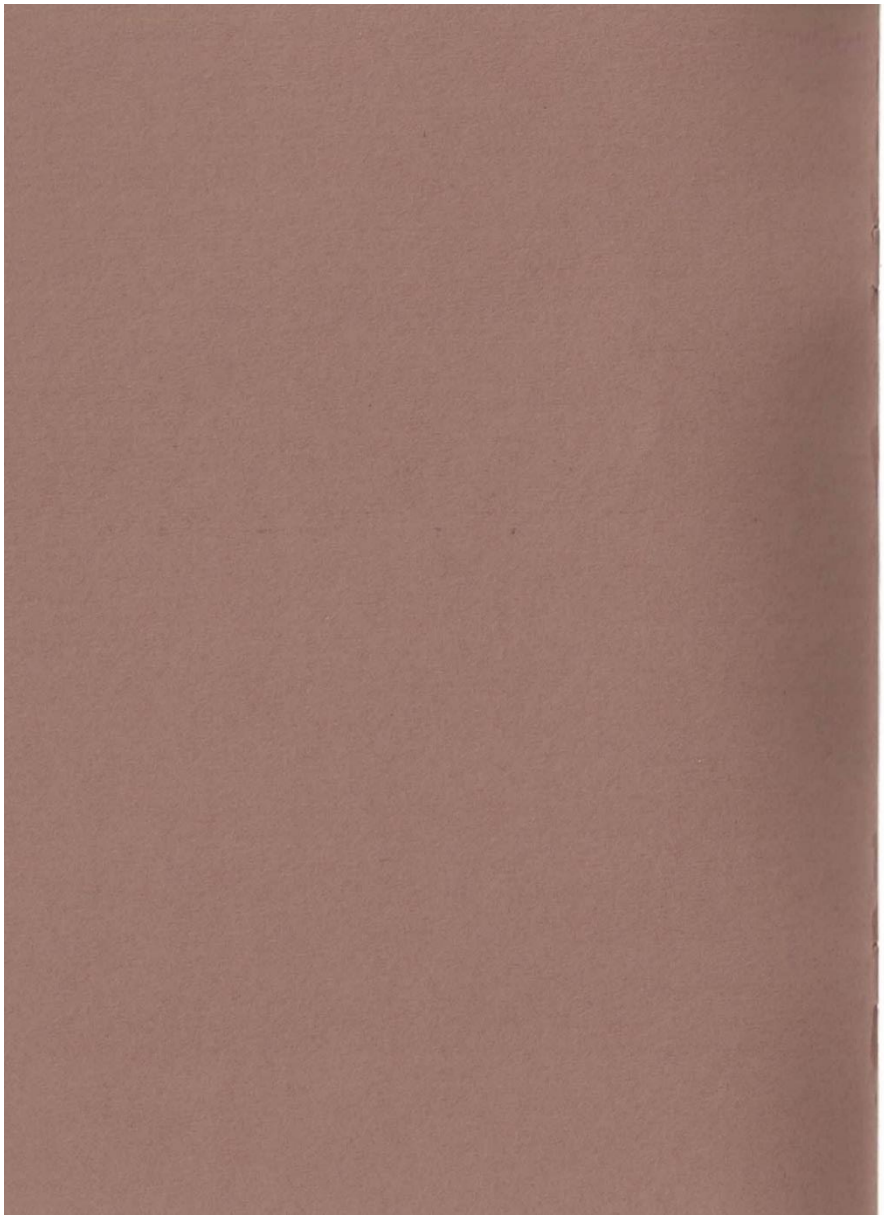
ENTKLASSIFIZIERT
DATUM : - 9. Juli 1992

465

GEHEIM
SECRET

Bedienungs-Anleitung zur Chiffriermaschine „NEMA“

Instruction de service de la machine à chiffrer „NEMA“



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 Fortschaltwalzen bestimmt. Durch Vertauschen dieser Walzen kann der Code beliebig und leicht verändert werden. Zur Drehstellungsmarkierung sind diese Walzen an der Außenzylinderoberfläche mit Alphabetbuchstaben von A—Z bezeichnet. Der **äußere Schlüssel** ist durch Einstellen der 10 Walzen mit den Bezeichnungsbuchstaben in eine Linie durch eine Gruppe von 10 Buchstaben bzw. durch ein 10stelliges Schlüsselwort bestimmt.

Zum Chiffrieren wird unter Beachtung der vorherigen Kennworteinstellung der zu chiffrierende Buchstabe auf der entsprechenden Taste gedrückt; das Chiffrat erscheint als Leuchtbuchstabe auf dem Lampenfeld. Umgekehrt wird zum Dechiffrieren der zu dechiffrierende Buchstabe auf der entsprechenden Taste gedrückt, wonach der Klarbuchstabe als Leuchtbuchstabe auf dem Lampenfeld erscheint. Jede Buchstabentaste muß bis zum Anschlag der Taste gedrückt und dann frei in die Ruhelage zurückgelassen werden, bevor die nächste Buchstabentaste betätigt wird. Die Tastung der Buchstaben muß mit angemessenem Druck sorgfältig mit den Zeigefingern erfolgen. Die Betätigung nach dem 10-Finger-System ist nicht möglich.

Jede Tastenbetätigung wird zu Kontrollzwecken mit einem auf Null zurückstellbaren Zählwerk gezählt. Die Tastatur besitzt die 26 Grundbuchstaben des Alphabets. Dazu sind Bedienungstasten für den Anschluß einer elektrischen Schreibmaschine, eines Fernschreibers, Hellschreibers oder Creedlochers vorhanden. Die Speisung der T-D-Maschine erfolgt entweder durch Netzanschluß, durch eine eingesetzte Trockenbatterie oder durch eine andere Fremdstromquelle von 4—6 Volt Nennspannung. Der für den Netzanschluß eingebaute Transformator transformiert die Netzspannung auf die Betriebsspannung von etwa 4,5 Volt.

Für die rasche Chiffrierung und Dechiffrierung kann die T-D-Maschine zur Ablesung durch den Anschluß eines zweiten Lampenfeldes erweitert werden. Damit wird bezweckt, daß die Ablesungen durch einen zweiten Bedienungsmann zu Papier gebracht werden können, während 1 Mann nur die T-D-Maschine bedient.

II. AUFBAU UND WIRKUNGSWEISE.

A. Allgemeines.

1. Größe und Gewicht.

332 × 384 × 148 mm über alles gemessen.
Gewicht: 10,7 kg inkl. Zubehör.

2. Zusammenbau.

Der Kasten ist als tragbare Panzerholzkiste ausgebildet. Die Chiffriermaschine ist durch 3 unverlierbare Schrauben am Kastenboden befestigt. Im Deckel sind das separate Lampenfeld, die Zubehör- und Reserveteile untergebracht. Der Deckel kann durch die beiden Stellscheren in zwei Stellungen, offen nach rückwärts oder halbgeöffnet über die Maschine gestellt, festgehalten werden. Die über die Maschine geneigte Deckelstellung ist von Nutzen zur Lichtabschirmung der Tastatur oder als Regenschutz.

Im Deckel sind zwei Halter angebracht, welche gestatten, das Textblatt übersichtlich im Blickfeld des Chiffrierenden aufzuhängen.

3. Verschluß.

Der Kasten ist mit einem Sicherheitsschloß ausgerüstet. Zu seiner Entlastung sind zwei Kniehebelverschlüsse angebracht.

B. Chiffriermaschine (Bild 1).

Sie ist äußerlich ähnlich einer Schreibmaschine aufgebaut und besteht in der Hauptsache aus folgenden Einheiten:

1. Tastatur,
2. Lampenfeld,
3. Zählwerk,
4. Stromquelle,
5. Schalter,
6. Ausrückmechanismus des Walzenpaketes,
7. Walzenpaket,
8. Vorschubmechanismus.

1. Tastatur (Bild 1, 2).

Die dreireihige Anordnung der 26 Grundbuchstaben des Alphabets auf den Tasten entspricht derjenigen einer normalen Schreibmaschine. Die oberste Reihe weist ferner eine Doppelbezeichnung für die Zahlen auf. Zur Steuerung eines über ein spezielles Schaltkästchen anzuschließenden Fernschreibers, Hellschreibers oder Creedlochers sind folgende Tasten eingebaut:

WR-Taste für Wagenrücklauf,
ZL-Taste für Zeilenwechsel,
BU-Taste für den Fernschreiberstart,
Lange Taste für Zwischenraum.

Diese Tasten dienen nur zur Steuerung der Zusatzgeräte, sie betätigen den Chiffriermechanismus nicht.

In der untersten Tastenreihe sind lediglich zur Vervollständigung des Tastaturbildes zwei arretierte Blindtasten montiert.

Beim Drücken einer Buchstabentaste werden durch eine verschlüsselte Nockensteuerung eine veränderliche Anzahl Walzen des Walzenpaketes vorwärtsgeschaltet. Diese bilden gleichzeitig einen verschlüsselten Stromkreis Taste—Glühlampe, wobei die gedrückte Taste selbst hierzu einen Oeffnungs- und einen Schließkontakt betätigt. Diese Oeffnungs- und Schließkontakte sind je auf einem gemeinsamen Träger über und unter den Tastenarmen angebracht.

2. Lampenfeld (Bild 1, 2).

Die Anordnung der Buchstaben auf dem Lampenfeld ist dieselbe wie diejenige auf der Tastatur. Nur der von hinten beleuchtete Buchstabe ist für die Ablesung gültig.

3. Zählwerk (Bild 1, 2).

Jeder getastete Buchstabe, ausgenommen derjenige der ersten Tastung nach einem Vorgang **«Einstellen»** (vgl. Abschnitt III B e Seite 8), wird fortlaufend durch das Zählwerk gezählt. Das Zählwerk kann durch einen Rückstellhebel (Nullstellung) auf Null zurückgeführt werden. Die Zählung der gedrückten Buchstaben erleichtert die Kontrolle des zu

übermittelnden Textes. Wird beim Zählwerk eine Zahl nur halb vorwärtsgeschoben, so ist die Tastung nicht richtig, d. h. nicht bis zum unteren Anschlag durchgeführt worden. In diesem Fall muß das Chiffrat, bzw. Dechiffrat zu Vermeidung von Unstimmigkeiten von Anfang an wieder neu getastet werden!

4. Stromquelle (Bild 1, 2).

Für den Betrieb der Nema-Maschine wird eine Stromquelle (Gleich- oder Wechselstrom) von 4—6 Volt mit etwa 0,4 Amp. benötigt.

Folgende Möglichkeiten sind vorhanden:

a) Durch eine im Batteriefach eingesetzte Trockenbatterie von 4,5 Volt, entweder 1 Blockbatterie L. S. A Nr. 1004 oder eine gewöhnliche Taschenlampenbatterie.

b) Durch Anschluß der Nema-Maschine an die Netzspannung. Mit dem Spannungswähler wird die entsprechende Anschlußspannung eingestellt. Der eingebaute, kurzschlußsichere Transformator liefert sekundärseitig die notwendige Betriebsspannung.

c) Durch Anschluß einer separaten Gleich- oder Wechselstromquelle von 4 bis 6 Volt. Dieser Anschluß kann entweder an den beiden Klemmen «4 V» oder an den hierzu parallel geschalteten Steckerbüchsen erfolgen.

5. Schalter (Bild 1, 2).

Folgende Schalter sind eingebaut:

a) **Stromquellenschalter** mit den Stellungen:

Batt.: für die eingebaute Trockenbatterie.
Trafo: für Netzanschluß durch den eingebauten Transformator.
Accu: für die externe Stromquelle.

b) **Deckelschalter:** Er schaltet bei geschlossenem Transportkastendeckel den Stromquellenkreis ab.

6. Ausrückmechanismus des Walzenpaketes (Bild 1, 2, 3).

Der durch den roten Kupplungshebel zu betätigende Ausrückmechanismus erlaubt den Ein- und Ausbau sowie die Einstellung des Walzenpaketes. Die Funktionen seiner drei möglichen Stellungen sind folgende:

a) **ganz nach vorn geklappt:**

Stellung **«Betrieb»:** normale Betriebsstellung für die Tastung der Buchstaben;

b) **in die Mitte hochgeklappt:**

Stellung **«Einstellen»** (Walzendeckel geöffnet). Die Walzen können zum Einstellen des äußeren Schlüssels, d. h. der 10stelligen Buchstabengruppe, bzw. des Schlüsselwortes vor- oder rückwärts gedreht werden.

Bei der Tastung eines falschen Buchstabens kann die falsche Tastung richtiggestellt werden, wenn der rote Kupplungshebel **sorgfältig** (nicht «schnellen» lassen!) vor der neuen Tastung von der Stellung **«Betrieb»** auf **«Einstellen»** und zurück auf **«Betrieb»** gestellt wird. Die wiederholte Tastung wird vom Zählwerk nicht registriert.

c) **bei aufgeklapptem Maschinendeckel ganz nach hinten gestellt:**

Sofern der Ausrückmechanismus nicht durch die Plombierung arretiert wird, kann das ganze Walzenpaket — mit Ausnahme der roten Fortschaltwalze — herausgehoben werden.

7. Walzenpaket (Bild 2, 4).

Das Walzenpaket besteht aus:

1 Achse und der darauf festgemachten Umkehrwalze sowie 4 aufgeschobenen Doppelwalzen. Jede Doppelwalze kann in eine Kontakt- und eine Fortschaltwalze durch einfaches Auseinanderziehen zerlegt werden. Die in der Maschine verbleibende rote Fortschaltwalze kann ebenfalls durch seitliches Abziehen herausgenommen werden.

Die **Kontaktwalzen** haben einerseits V-förmige feste Kontakte und anderseits gerade, radial gerichtete federnde Kontakte. Sie sind auf der Seite der federnden Kontakte mit großen Buchstaben bezeichnet (z. B.: A B C usw.). **Es ist verboten, die Kontaktwalzen aufzuschrauben.**

Die **Fortschaltwalzen** werden auf den Zylinder der V-Kontakte der Kontaktwalze aufgeschoben. Der auf der linken Seite befindliche Zahnkranz ist mit einer arabischen Zahl bezeichnet (z. B. 13, 14, usw.).

Der Zahnkranz ist nach Lösen von drei Schrauben abnehmbar.

Die innere Verschlüsselung der Nema-Maschine ist u. a. durch die Gruppierung dieser Walzen und Wahl der auswechselbaren Zahnkränze gegeben.

8. Vorschubmechanismus (Bild 3).

Der Vorschubmechanismus für das Walzenpaket besteht aus elf Klinken, die auf einer Gußwiege gelagert sind. Diese Wiege wird durch die Buchstabentasten über einen gemeinsamen Stabarm betätigt. Die Klinken und indirekt die Arretierung der Walzen werden durch die Zahnkränze der Fortschaltwalzen gesteuert.

C. Separates Lampenfeld (Bild 1, 5).

Das separate Lampenfeld oder das nicht zur Nema-Maschinen-Ausrüstung gehörende Zusatzkästchen für die Steuerung einer elektrischen Schreibmaschine, eines Fernschreibers, Hellschreibers oder Creed-Lochers

kann mit dem Verbindungskabel am rechtsseitigen Mehrpolstecker angesteckt werden.

Das Buchstabenfeld des separaten Lampenfeldes ist dem Lampenfeld der T-D-Maschine parallel geschaltet und hat die gleiche Anordnung.

D. Zubehör und Reservematerial (Bild 1, 5).

Im Deckel des Transportkastens sind folgende Teile untergebracht:

1 separates Lampenfeld mit Stoffriemchen befestigt.
1 mehradriges Verbindungskabel zum sep. Lampenfeld.
1 Netzanschlußkabel (4 m lang, 3adr.).
1 Edison-Lampenfassung für Netzanschluß an Lampenfassungen.
16 Reservelämpchen für Lampenfeld (3,5 V — 0,2 Amp.).
2 Schutzdeckel (plombierbar) enth.: je
1 Reserve-Doppelwalze.
1 Schutzdeckel (plombierbar) enth.:
8 Reserve-Zahnkränze.
1 Haltebügel.

III. BEDIENUNGSANLEITUNG.

A. Anschluß der Stromquelle.

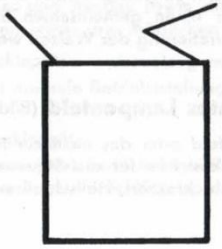
1. Einsetzen einer Trockenbatterie.

a) Roten Kupplungshebel auf **«Einstellen»** schieben und Maschinendeckel nach Lösen der beiden rotberingten Schrauben öffnen.

b) Batteriefach-Deckel öffnen durch Verschieben des Verschlußbügels in der Pfeilrichtung.

c) Schutzkarton, bzw. -papier der neuen Batterie entfernen.

d) Batterie einsetzen derart, daß bei einer **Blockbatterie L. S. A. 1004** die Kontaktlaschen auf die Kontaktfedern des Batteriefachs (vorne) zu liegen kommen, und bei einer **Taschenlampenbatterie** nach vorherigem Umbiegen der Kontaktlaschen, gemäß nachstehender Skizze



dieselben an die Kontaktfedern im Batteriefach gedrückt werden, wobei die Batterie flach gegen den Boden in der hinten angebrachten Aussparung gehalten wird.

e) Batteriefach schließen.

f) Maschinendeckel schließen und mit den beiden rotberingten Schrauben festziehen.

g) Roten Kupplungshebel auf **«Betrieb»** stellen.

h) Stromquellenschalter auf **«Batt»** stellen.

2. Netzbetrieb mit eingebautem Transformator.
(Unbekannte Netzspannungen an Glühlampen ablesen, nicht an Steckern oder Schaltern!)

a) Spannungswähler an der rechten Seitenwand neben dem Netzanschlußstecker auf die zur Verfügung stehende Wechselstrom-Netzspannung einstellen, durch Lösen der weiß markierten Schraube, Drehen der Zentrumplatte und Wiedereinschrauben an der mit der vorhandenen Spannung bezeichneten Stelle.

b) Maschine mit dem Netzkabel an die nächste Steckdose oder mittels der Edison-Steckerfassung an eine benachbarte Lampe anschließen.

c) Stromquellenschalter auf **«Trafo»** stellen.

3. Betrieb mit fremden Stromquellen von 4—6 Volt Spannung (z. B. Akkumulator).

a) Fremde Stromquelle entweder an die beiden Klemmen **«4 V»** oder an die beiden Steckbuchsen anschließen.

b) Stromquellenschalter auf **«Accu»** stellen.

B. Betrieb der Maschine.

Chiffrieren, bzw. Dechiffrieren durch Einstellen nur des äußern Schlüssels.

In diesem Fall sind die einzelnen Walzen des Walzenpaketes und ihre Reihenfolge, welche den sog. **inneren Schlüssel** bestimmen, bereits eingesetzt und evtl. plombiert. Bei plombierter Maschine kann das Walzenpaket nicht herausgenommen werden, die Walzen können nur zur Einstellung des sogenannten **äußern Schlüssels**, d. h. der 10stelligen Buchstabengruppe, bzw. des Schlüsselwortes, wenn der rote Kupplungshebel auf **«Einstellen»** gestellt ist, betätigt werden.

a) Roten Kupplungshebel in Stellung **«Einstellen»** bringen.

b) An den einzelnen Walzen ist die 10stellige Buchstabengruppe, bzw. das Schlüsselwort längs der vorderen Kante der Walzenöffnung einzustellen. Die einzustellenden Buchstaben sind in eine Linie auszu-

richten. Durch die vorhandene Rasterung werden sie automatisch in der richtigen Stellung festgehalten.

c) Roten Kupplungshebel in Stellung **«Betrieb»** bringen.

d) Zählwerk auf Null stellen.

e) Nach jeder Neueinstellung des Schlüsselwortes muß eine beliebige Alphabettaste «leer» gedrückt werden. Diese **erste** Tastung nach dem Betätigen des roten Kupplungshebels von **«Einstellen»** auf **«Betrieb»** wird weder vom Zählwerk registriert, noch steuert sie das Walzenpaket (darum die Bezeichnung «leer»). Sie muß unbedingt durchgeführt, darf aber für die Textübermittlung **nicht** berücksichtigt werden. Sie ist zur Funktionskontrolle der Maschine gedacht, indem bei der Tastung eines beliebigen Buchstabens **ein** Buchstabe **einwandfrei** im **Lampenfeld** aufleuchten muß.

f) Erneut kontrollieren, ob das 10stellige Schlüsselwort richtig eingestellt ist und das Zählwerk auf Null steht. (Wenn nicht in Ordnung, vorbeschriebene Punkte a—f wiederholen.)

g) Walzendeckel schließen.

h) Chiffrieren, bzw. Dechiffrieren.

Die Taste jedes umzuwandelnden Buchstabens ist bis zum Anschlag zu drücken und dann frei in die Ruhelage zurückgehen zu lassen, bevor der nächste Buchstabe betätigt wird. Die Tastung jedes Buchstabens muß mit angemessenem Druck sorgfältig mit den Zeigfingern erfolgen. Sobald eine Taste nicht einwandfrei bis zum Anschlag gedrückt wird, treten Fehlschaltungen beim Vorschub des Walzenpaketes auf und es entstehen unentwirrbare Textkonfusionen. Bei der heruntergedrückten Taste leuchtet im Lampenfeld der entsprechende chiffrierte, bzw. dechiffrierte Buchstabe auf.

i) Repetieren:

Ist infolge eines Versehens eine falsche Taste gedrückt worden und wird dies sofort, d. h. vor dem Tasten des nächsten Buchstabens bemerkt, so kann dieser Fehler auf folgende Art ohne Störung des Chiffrates korrigiert werden:

Roten Kupplungshebel **sorgfältig** (ohne schnellen zu lassen!) auf **«Einstellen»** und dann wieder auf **«Betrieb»** stellen. Richtige Taste drücken und Leuchtbuchstaben ablesen.

Dieses sogenannte «Repetieren» wird vom Zählwerk nicht gezählt, auch die Walzen des Walzenpaketes werden dabei nicht weitergeschaltet. Dasselbe Verfahren kann natürlich auch im Zweifelsfalle bei Unsicherheit im Ablesen angewandt werden. **Es kann jedoch nur ein Buchstabe «repetiert» werden, mehrere aufeinanderfolgende Buchstaben können nicht korrigiert werden.**

(Es sei hier noch eine vereinfachte Repetiermöglichkeit erwähnt, welche dann zulässig ist, wenn der Tastirrtum bereits festgestellt wird, wenn die falsche Taste sich noch in **einwandfrei hinuntergedrücktem Zustand** befindet. In diesem Falle wird die **richtige Taste** gedrückt **bevor** die falsche losgelassen wird. Letztere wird erst losgelassen, wenn die richtige Taste ebenfalls einwandfrei bis zum Anschlag gedrückt ist. Der neu aufleuchtende Buchstabe entspricht nun der richtigen Tastung.)

C. Veränderung des «innern Schlüssels».

Die Veränderung des inneren Schlüssels und die Entfernung der Plombe von plombierten Maschinen darf nur auf besonderen Befehl des Chefs der Uebermittlungstruppen erfolgen:

a) Roten Kupplungshebel auf **«Einstellen»** bringen.

b) Maschinendeckel öffnen nach Lösen der beiden rotberingten Schrauben.

c) Roten Kupplungshebel ganz nach hinten bis zum Anschlag drücken, damit wird das Walzenpaket freigegeben.

d) Walzenpaket ohne die rote Walze, welche in der Maschine bleibt, bzw. separat herausgenommen werden kann, mit beiden Händen fassen, leicht achsial zusammenpressen und nach hinten oben herausnehmen, d. h. waagrecht nach oben abheben.

Nicht forcieren!

e) Die vier Doppelwalzen von der Welle abziehen, die Umkehrwalze bleibt auf der Welle.

f) Zerlegen der vier Doppelwalzen in je eine Kontaktwalze (am Flansch mit einem großen Buchstaben bezeichnet) und eine Fortschaltwalze (am Zahnkranzflansch mit einer Zahl bezeichnet) durch achsiales Auseinanderziehen der beiden Walzen.

g) Zusammensetzen des Walzenpaketes gemäß neuem innerem Schlüssel: Paarweises Zusammenstecken von je einer Fortschalt- und einer Kontaktwalze. Die so gebildeten Doppelwalzen jeweils mit der V-förmigen Kontaktseite voran in der vorgeschriebenen Reihenfolge auf die Welle schieben (z. B. 15D-11A-14B-12F-10/1). Die letzte Zahlengruppe 10/1 bedeutet die Zusammenstellung der roten Fortschaltwalze.

h) Walzenpaket einsetzen, indem es mit beiden Händen gefaßt, leicht achsial zusammengepreßt, rechts in das Lager der Verteilerwalze und links in den Ausrückmechanismus eingehängt wird.

i) Roten Kupplungshebel auf Stellung **«Einstellen»** bringen, wodurch das Walzenpaket betriebsmäßig zusammengeschoben wird.

k) Evtl. Plombierung der Maschine, indem der Plombierwinkel bis zum obern Anschlag gehoben und der Plombendraht durch das freigewordene Loch eingeführt, verdreht, die Plombe aufgeschoben und zusammengedrückt wird.

l) Maschinendeckel schließen und mit den beiden rotberingten Schrauben festziehen.

m) Aeußeren Schlüssel, d. h. die 10stellige Buchstabengruppe bzw. das Schlüsselwort längs der vorderen Kante der Walzenöffnung einstellen und Maschine weiter betriebsfertig machen wie in Abschnitt III B b-h, Seiten 7—8 beschrieben.

Zur Verstellung des inneren Schlüssels können zusätzlich die Zahnkränze der Fortschaltwalzen ausgewechselt werden. Durch Lösen der 3 Schrauben kann der Zahnkranz vom eigentlichen Walzenkörper abgeschraubt und durch einen anderen ausgetauscht werden. **Es ist hierbei darauf zu achten, daß die am Zahnkranz eingravierte Typenziffer gegenüber dem Buchstaben U zu liegen kommt.** Bei der roten Fortschaltwalze ist die Typenziffer des linken Zahnkranzes ebenfalls gegenüber dem Buchstaben U und die des rechten Zahnkranzes gegenüber dem Buchstaben L einzustellen. Die rechte Seite darf nur mit Zahnkränzen einstelliger und die linke mit solchen zweistelliger Zahlenbezeichnungen versehen werden.

IV. WARTUNG DER MASCHINE.

Bei Nichtgebrauch ist der Transportkastendeckel zu schließen. Die Maschine ist wöchentlich mindestens einmal gründlich zu entstauben. Die Kontaktfedern sind in sauberem Zustande zu halten. Verbrauchte Trockenbatterien müssen entfernt werden, damit ihre Zersetzungsprodukte die Maschinenteile nicht angreifen.

Nach etwa 200 Betriebsstunden oder mindestens jährlich einmal sind die Lager sämtlicher beweglichen Teile mit nichtharzendem dünnflüssigem Apparate-Oel leicht zu ölen.

Sämtliche festen und beweglichen Kontakte der Kontaktwalzen sind ebenfalls von Zeit zu Zeit mit einem benzingetränkten Lappen zu reinigen und anschließend mit reiner Vaseline **leicht** zu fetten.

Nach zirka 1000 Betriebsstunden soll die Maschine einer Generalrevision unterzogen werden.

V. BEHEBUNG VON STÖRUNGEN.

A. Elektrische Fehler.

1. Im Lampenfeld brennt bei verschiedenen Tastungen keine Lampe.

a) Stellung des Stromquellenschalters kontrollieren.

b) Kontrollieren, ob der Druckknopf des Deckelschalters nicht steckengeblieben ist.

c) Bei Batteriebetrieb prüfen, ob die Batterie nicht verbraucht und ob sie richtig eingesetzt ist.

d) Bei Netzbetrieb prüfen, ob Netzspannung, und zwar Wechselstrom, vorhanden ist. (Mit Gleichstrom über dem Transformator funktioniert die Maschine nicht.)

Steckeranschlüsse und evtl. Kabelanschlüsse im Steckerinnern prüfen. Netzkabel auf Unterbruch prüfen.

e) Bei Fremdstromquelle diese selbst und die Anschlußverbindungen kontrollieren.

2. Die Lampen im Lampenfeld brennen abnormal schwach.

a) Bei Batteriebetrieb, Batterie evtl. ersetzen oder Kontaktfedern reinigen.

b) Bei Netzbetrieb: Richtige Netzspannung am Spannungswähler einstellen.

c) Bei der Hilfsstromquelle: Nennspannung (4—6 Volt) und Leistungsfähigkeit kontrollieren.

3. Die Lampen brennen abnormal hell.

a) Bei Netzbetrieb: richtige Netzspannung am Spannungswähler einstellen.

b) Bei Hilfsstromquelle: Nennspannung kontrollieren, darf nicht größer als 6 Volt sein.

4. Im Maschinenlampenfeld brennt eine Lampe nicht, während die gleichnamige Lampe im separaten Lampenfeld aufleuchtet.

Schlechter Kontakt im Lampengewinde: Lampengewinde in der Maschine und am Lämpchen selbst sowie Lämpchenspitze mit einer Messerklinge oder einem Schraubenzieher ausschaben. Lampengewinde in der Maschine mit Vaseline leicht fetten.

5. Im separaten Lampenfeld brennt eine Lampe nicht, während die gleichnamige Lampe im Maschinenfeld aufleuchtet.

a) Schlechter Kontakt im Lampengewinde: Vergleiche Abschnitt V/A/4.

b) Schlechter Kontakt an den Steckern des Verbindungskabels: bei gedrückter Taste sind die Stecker leicht hin und her zu bewegen und ganz hineinzustoßen. Wenn dabei die Lampe flackert, sind die Lötstellen in den Kupplungen zu kontrollieren oder die evtl. defekte Ader durch eine der zwei im Kabel vorhandenen Reserveadern zu ersetzen.

6. Beim Drücken einer bestimmten Taste brennt weder im Maschinen-Lampenfeld noch im separaten Lampenfeld die Lampe.

a) Wird nach jedem Walzenpaketvorschub das Tastenfeld nach Abschnitt «Bemerkung» (siehe unten) kontrolliert, bleibt immer dieselbe Lampe dunkel: Maschinendeckel öffnen, Kontrolle des Funktionierens der zugehörigen Ruhekontaktfeder der nicht brennenden Lampe durch leichtes Bewegen der ihr entsprechenden Buchstabentaste und evtl. Nachbiegen der betreffenden Kontaktfeder (zugänglich zwischen Lampenfeldträger und Tastenkamm).

b) Fehler im Tasten-Arbeitskontakt, d. h. beim wiederholten Tasten der fehlerhaften Taste leuchtet bei jedem weiteren Schritt keine andere Lampe auf: Kontrolle des Funktionierens der zugehörigen Arbeitskontaktfeder (unter dem Tastenhebel angebracht). Reinigen der betr. Kontaktfeder mit einem benzingetränkten Lappen.

c) Fehler im Walzenpaket, d. h. bei fortlaufendem Tasten und bei der Kontrolle aller Tasten leuchtet nach jedem Schritt eine andere Lampe (im Maschinen- und im separaten Lampenfeld) nicht auf: Kontrolle sämtlicher Kontakte bei allen Walzen. Ein allfällig hängengebliebener Kontakt kann durch Hin- und Herbewegen gängig gemacht werden.

Bemerkung: Zur Kontrolle, ob alle Lampen im Lampenfeld aufleuchten oder um eine nicht brennende Lampe herauszufinden, ist wie folgt vorzugehen:

In irgendeiner Walzenstellung wird zuerst die Taste «Q» gedrückt. Wenn die Taste «Q» noch heruntergedrückt ist, wird die Taste «W» gedrückt. Erstere wird erst losgelassen, wenn letztere einwandfrei hinuntergedrückt ist. Die ganze Alphabet-Tastatur wird nun der Reihe nach in dieser Weise betätigt, d. h. das ganze Alphabet wird **ohne Walzenpaketvorschub** abgetastet.

(Sobald ein mechanischer Vorschub gemacht wird — Zählwerk überwachen!!! — muß wieder mit der Taste «Q» neu begonnen werden.) Auf einem Blatt Papier ist das Alphabet von A—Z aufzuschreiben und jeder bei einer Tastung aufleuchtende Buchstabe durchzustreichen, wodurch am Schluß die fehlerhafte, d. h. die nicht aufleuchtende Lampe eruiert werden kann.

Irgendwelche andere Eingriffe an den Walzen dürfen von der Truppe nicht gemacht werden.

B. Mechanische Fehler.

1. Die beim Schlüsselwort einzustellende Walze nimmt eine benachbarte Walze mit:

a) Verkehrt eingesetzte Walze im Walzenpaket: Doppelwalzen mit den V-förmigen Kontaktseiten voran in der vorgeschriebenen Reihenfolge auf die Welle schieben.

b) Fremdkörper in der Kontaktbahn: Walzenpaket demontieren und Kontakte mit einem benzingetränkten Lappen reinigen und anschließend mit reiner Vaseline **leicht** fetten.

c) Walzenpaket nicht richtig nach «innerem Schlüssel» zusammengestellt: Richtige Zusammenstellung vgl. Abschnitt III C g, Seite 9.

2. Chiffrat- bzw. Dechiffratbeginn vollkommen richtig, Fortsetzung unverständlich.

a) Unsorgfältiges Tasten: Richtige Tastung vgl. Abschnitt III B h, Seite 8.

b) Zu scharfes Schnellenlassen des roten Kupplungshebels beim Repetieren: Richtiges Repetieren vgl. Abschnitt III B i, Seite 8.

30. April 1947. Z. A. G. No. 117.660—1

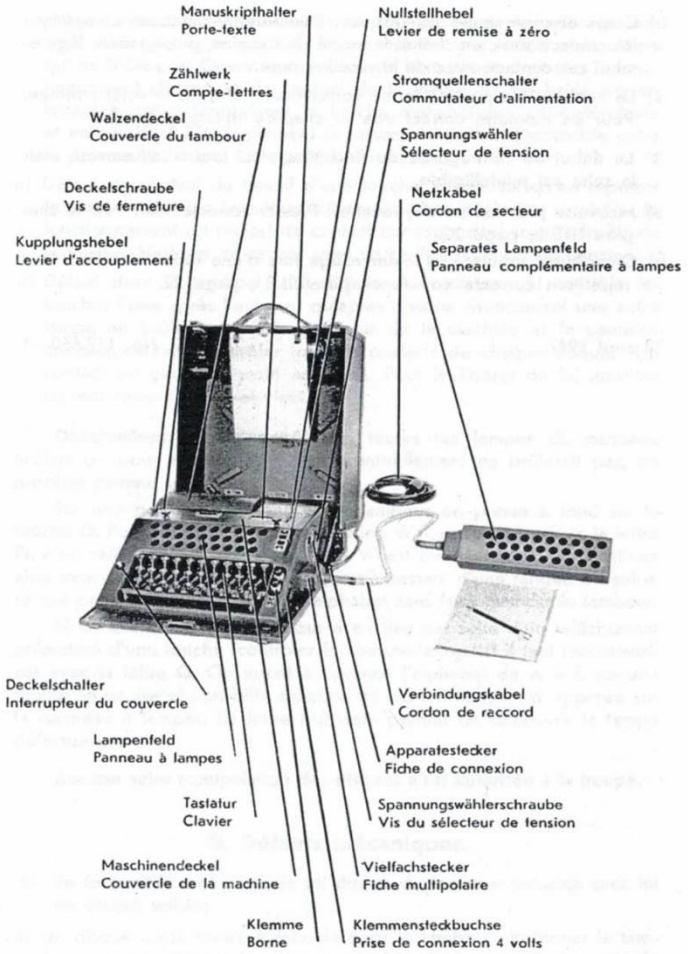


Bild
Illustration 1

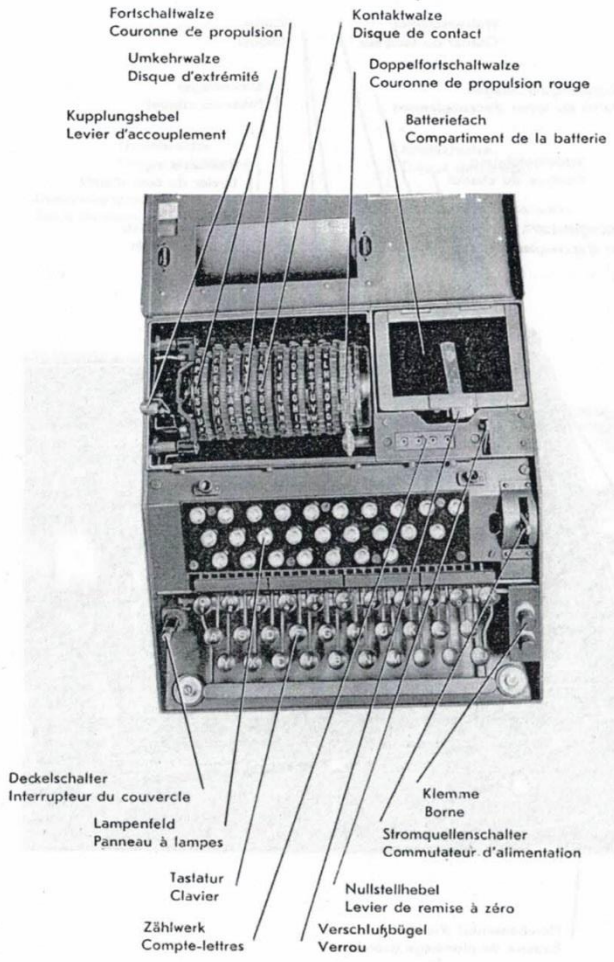


Bild
Illustration 2

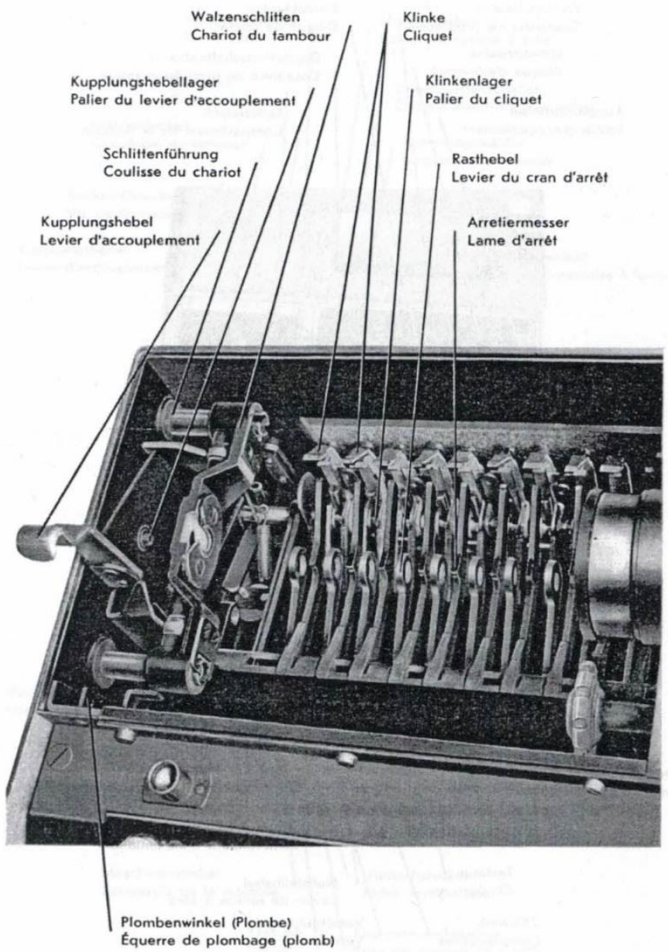


Bild
Illustration 3

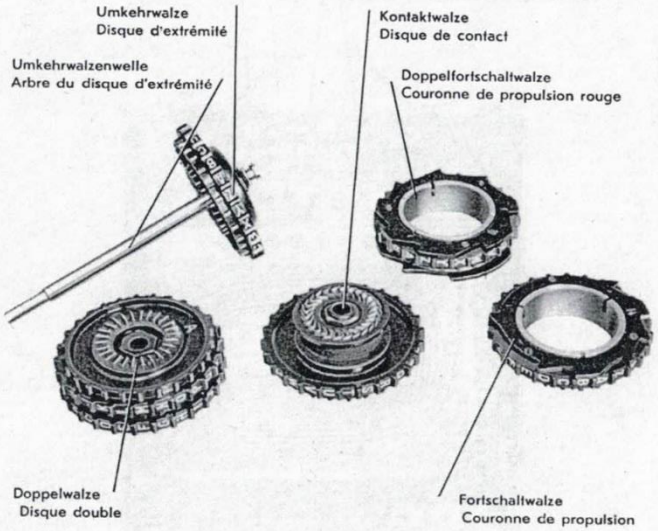


Bild
Illustration 4

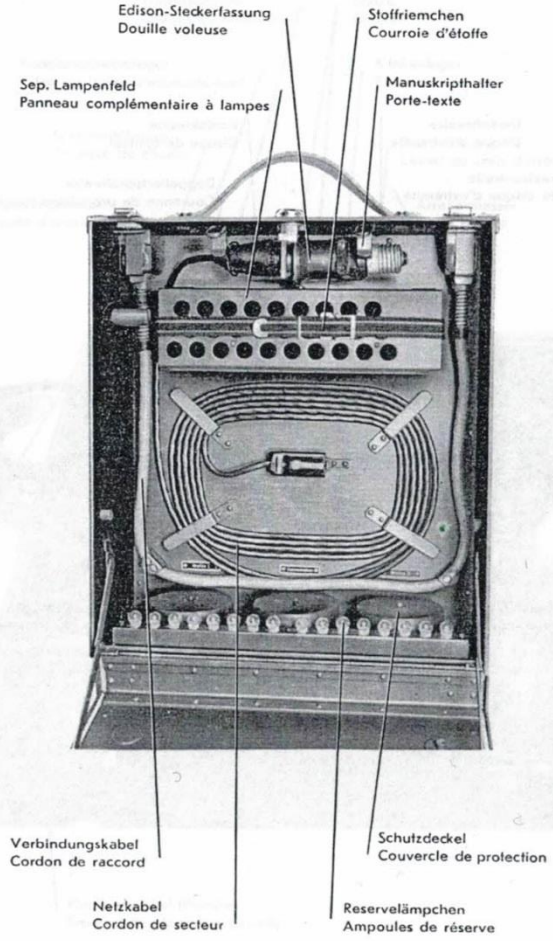


Bild
Illustration 5

Anhang 2: Schlüsselungsverfahren für die NEMA-Maschine

Nr. 142...

GEHEIM - SECRET

Der Chef
des Uebermittlungsdienstes der Armee

Le Chef
du Service des Transmissions de l' Armée

ENTKLASSIFIZIERT
ATUM 1-9. Juli 1992

SCHLUESSELUNGSVERFAHREN
für die
NEMA-MASCHINE.

PROCEDE DE CHIFFREMENT
pour la
MACHINE NEMA.

Ausgabe Mai 1948

Edition mai 1948

1)

58

1. DER GEHEIME SCHLUESSEL wird durch Schlüsselbefehl ausgegeben. Die Dauer seiner Gültigkeit richtet sich nach dem Verkehr und wird von Fall zu Fall befohlen.

   Er besteht aus zwei Teilen:

   a) dem innern Schlüssel, der die Reihenfolge der Kontakt- und Fortschaltewalzen bestimmt , welche wie folgt angegeben wird:

      11A - 15F - 12D - 14B

      Die Buchstaben bedeuten die Kontaktwalzen, auf welche die Fortschaltewalzen (durch zweistellige Zahlen gekennzeichnet) links aufgeschoben werden.

   b) einem Schlüsselwort, mit dessen Hilfe gemäss untenstehender Vorschrift der äussere Schlüssel gewonnen wird. Das Schlüsselwort soll 10 oder mehr Buchstaben enthalten, z. B.:

      ZAR UND ZIMMERMANN

2. VORSCHRIFT ZUR GEWINNUNG DES AEUSSERN SCHLUESSELS.

   Zur Gewährleistung der kryptographischen Sicherheit muss jedes Telegramm mit einem andern äussern Schlüssel chiffriert werden.

   a) An der Masohine mit dem zur Zeit geltenden innern Schlüssel werden die 10 ersten Buchstaben des geheimen Schlüsselwortes an den Buchstabenkränzen von links nach rechts eingestellt.

   b) Der Chiffreur schreibt 10 von ihm beliebig gewählte Buchstaben in Form von 2 Fünfergruppen als Anfang des Chiffrates auf. Diese Buchstabenfolge wird am Schluss des Chiffrates wiederholt.

2)

c) Mit der nach a) bereitgestellten Maschine werden die 10 Buchstaben chiffriert und auf einen besondern Zettel notiert.

d) Die so gewonnene Buchstabengruppe wird als äusserer Schlüssel an der Maschine eingestellt, der Zähler auf Null gebracht, und die Maschine ist bereit zur Chiffrierung oder Dechiffrierung der Meldung.

Für den Dechiffreur fällt die Wahl der 10 Buchstaben nach b) dahin. Er entnimmt dem ankommenden Telegramm die 10 ersten Buchstaben, kontrolliert und vergleicht sie mit den letzten 10 Buchstaben des Chiffrates und verfährt im übrigen nach obiger Vorschrift. Bei Nichtübereinstimmung werden zunächst die am Anfang stehenden Buchstaben zur Gewinnung des äussern Schlüssels benützt. Ergibt dies beim Dechiffrieren der Meldung keinen Klartext, so sind die am Ende stehenden Buchstaben zu verwenden. Führt auch dies nicht zum Ziel, so ist die Wiederholung der ersten beiden Gruppen vom Absender zu verlangen.

3. CHIFFRIEREN UND DECHIFFRIEREN. (Die technische Seite wird in der Bedienungsanleitung zur Chiffriermaschine "N e m a" behandelt.)

a) Der Chiffretext der Meldung schliesst an die unter 2b) erwähnten zwei Schlüsselgruppen an und wird in Fünfergruppen geordnet. Bei unvollständiger letzter Fünfergruppe wird nicht aufgeblendet. Die 10 Buchstaben der beiden Schlüsselgruppen werden anschliessend wiederholt, womit das Chiffrat beendigt ist. Beim Dechiffrieren werden die ersten beiden Gruppen und die letzten 10 Buchstaben als zum Schlüssel gehörig weggelassen.

b) Die Anzahl der Buchstaben des Chiffretextes ohne Schlüsselgruppen muss stets mit der Zählerangabe übereinstimmen.

c) Wird beim Chiffrieren ein Fehler begangen, der sinnstörend wirkt, und kann er nicht nach dem in der Bedienungsanleitung beschriebenen Verfahren korrigiert werden, so wird die den Fehler enthaltende Partie noch einmal anschliessend richtig chiffriert, wobei im Chiffrat der den Fehler aufweisende Teil stehen bleiben muss. Beim Dechiffrieren gilt die Wiederholung als richtig.

3)

d) Zahlen werden mit Y angezeigt und getrennt. Der Uebergang zu Buchstaben wird mit X bezeichnet, wie auch die Trennung von Worten, wenn eine solche sich als absolut notwendig erweist.

4. BEISPIEL.

a) Geheimer Schlüssel: 11A - 15F - 12D - 148
ZAR UND ZIMMERMANN

b) An der Maschine wird eingestellt: ZARUNDZIMM

c) Wahl der zu übermittelnden Schlüsselgruppen: Q Z A F J T M C A R

d) Chiffrat dieser Gruppen: Z O L M K A L R Q U wird an der Maschine eingestellt, Zähler auf Null gebracht, und die Maschine ist zum Chiffrieren oder Dechiffrieren der Meldung bereit.

e) Chiffretelegramm:

Adresse: . . . . . Chi: . . . . . .
Q Z A F J T M C A R . . . . . .
. . . . . Q Z A F J T M C A R

Unterschrift: . . . . . .