Rotor-Schlüsselmaschinen in der DDR

Studienarbeit

Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Informatik

eingereicht von Moritz Dulies

Inhaltsverzeichnis

1 Einleitung

Die Geschichte der Verschlüsselung in der DDR ist insofern einmalig, als dass man nach dem Zusammenbruch der DDR, und durch die darauf folgende Offenlegung der Akten des Minsterium für Staatssicherheit (MfS), einen Einblick in die Struktur und Techniken eines modernen Staates erhielt. Man konnte nun nicht nur einen Einblick in die allumfassende Überwachung der Bevölkerung der Deutschen Demokratischen Republik bekommen, sondern auch wie weit die kryptologische Technologie eines Geheimdienstes fortgeschritten war und auf welchen Geräten sie beruhte.

In den 41 Jahren, in denen die DDR existierte, kamen eine Vielzahl an Verschlüsselungsmaschinen zum Einsatz. Diese Studienarbeit konzentriert sich auf Rotor-Schlüsselmaschinen, die zur Vorchiffrierung genutzt wurden und die in der DDR auf Regierungsebene zum Einsatz kamen. Die aus dem Zweiten Weltkrieg bekannte deutsche Verschlüsselsmaschine *Enigma* kam noch in der DDR zum Einsatz, bis sie von den deutlich überlegenderen Geräten aus sowjetischer Entwicklung, wie der hier vorgestellten *Fialka* und *Koralle*, ersetzt wurden. Diese wurden noch bis zum Ende der DDR genutzt, wenngleich modernere Maschinen und Verfahren den Einsatz über die Jahre zurückdrängten.

Die Studienarbeit beginnt mit einer allgemeinen Einführung zu Rotor-Schlüsselmaschinen und betrachtet dann die drei, in der DDR genutzten, Maschinen genauer.

2 Rotor-Schlüsselmaschinen

Zwischen dem Ersten und Zweiten Weltkrieg wurden fast zeitgleich mechanische Rotor-Schlüsselmaschinen von unterschiedlichen Entwicklern erdacht und konstruiert. Die Nutzung dieser Klasse von Verschlüsselungsmaschinen reichte teilweise noch bis in die Neunziger Jahre des 20. Jahrhunderts.

2.1 Grundidee

Die hier vorgestellten Chiffriermaschinen haben alle einen ähnlichen Aufbau. Deren Gemeinsamkeiten und grundlegende Funktionsweise sollen folgend erläutert werden.

Zunächst einmal soll die Maschine einen Klartext über Eingabetasten erhalten und einen Geheimtext ausgeben. Die Ausgabe erfolgt auf unterschiedlichste Weise, zum Beispiel durch Aufleuchten einer Lampe, gedruckt auf Papier oder gestanzt auf Lochstreifen. Ein Eingabezeichen führt zu genau einem Ausgabezeichen und die Menge der möglichen Eingabezeichen entspricht ebenfalls der Menge der möglichen Ausgabezeichen. Dies soll heißen, dass wenn der Klartext aus den Buchstaben A bis Z besteht, auch der Geheimtext nur aus den Buchstaben A bis Z besteht.

Eine einfache und unsichere[1] Art der Verschlüsselung ist die monoalphabetische Substitution. Das bedeutet, jedem Eingangszeichen wird ein anderes Ausgabezeichen zugewiesen. Zum Beispiel entspricht jedes E im Klartext einem Y im Geheimtext. Die Zuordnung aller Eingabezeichen zu Ausgabezeichen wird im kryptografischen Sinn *Alphabet* genannt. Die Idee der Rotor-Schlüsselungsmaschinen besteht darin, jedes Eingabezeichen mit einem neuen Alphabet zu übersetzen. Dies geschieht mit Hilfe der Rotoren, auch Walzen genannt. Man spricht dann von einer polyalphabetischen Substitution.

Abbildung 2.1 zeigt eine Chiffriermaschine mit drei Rotoren und den möglichen Eingaben A, B, C und D auf der linken Seite. Folgt man dem Pfad für Eingabe C durch die drei Rotoren bis zur Ausgabe, ergibt sich als Ausgabezeichen ein A. Ähnlich kann man

[1] Bei einer monoalphabetische Substitution können beispielsweise 26 Buchstaben auf 26! = 403.291.461.126.605.635.584.000.000 unterschiedliche Arten zugewiesen werden. Mit Hilfe einer Häufigkeitsanalyse der Buchstaben kann man in der Regel jedoch schnell die Zuordnung bestimmen.

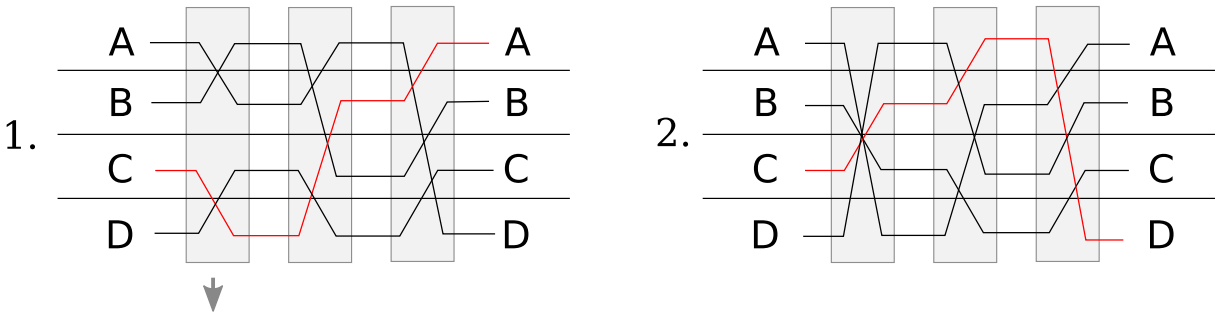


Abbildung 2.1: Schematische Darstellung der ersten beiden Schritte der Chiffrierung mit einer Rotor-Schlüsselmaschine

dies für die anderen drei Buchstaben machen. Es zeigt sich, dass A auf D, B auf B und D auf C abgebildet wird. Das Alphabet für ABCD lautet also DBAC.

Nach der Eingabe eines Zeichens dreht sich die erste Walze um einen Schritt weiter. Der Pfad ändert sich und somit auch das Alphabet. Es lautet nun ACDB.

Wie genau die anderen Walzen fortschreiten, hängt vom Fortschreitmechanismus ab. Im einfachsten Fall wird das Tacho-Prinzip genutzt, das nach einer vollen Rotation der ersten Walze die zweite Walze um eine Stelle weiter schiebt. Die dritte Walze wird wiederum nach einer vollen Rotation der zweiten Walze bewegt.

Bei den hier vorgestellten Maschinen findet immer noch eine Substitution vor und nach Verlassen der Walzen statt. Diese erste Verwürfelung der Buchstaben entspricht einer monoalphabetischen Substitution.

2.2 Enigma

Die wohl bekannteste Verschlüsselungsmaschine der Deutschen während des Zweiten Weltkrieges fasziniert auch noch heute viele Menschen und wurde Gegenstand vieler Bücher und Filme. Die Entschlüsselung der geheimen Nachrichten durch die Polen, Briten und Amerikaner führte vermutlich zu einem schnelleren Kriegsende und weniger Opfern. Weniger bekannt ist jedoch, dass die Enigma nach Kriegsende weiterhin genutzt wurde, wie zum Beispiel auch in der DDR.

2.2.1 Geschichte

Noch während des Ersten Weltkrieges wurde ausschließlich auf manuelle Chiffrierverfahren gesetzt, die entweder auf einfache Substitution und Transposition der Zeichen beruhte, oder aber auf Codebücher, bei denen eine geheime Abkürzung für einzelne Wörter,

Abbildung 2.2: Geöffnete Enigma I

Satzfragmente oder auch ganze Sätze stehen können. Diese Verfahren waren mühsam, zeitaufwendig und konnten leicht zu Fehlern führen.

Mit Beginn des 20. Jahrhunderts kamen erstmals elektronische Schreibmaschinen und Fernschreiber auf, und somit auch die Idee diese Technik für die Chiffrierung zu nutzen. Relativ zeitgleich kamen unterschiedliche Erfinder auf die Idee, Rotoren für die Chiffrierung zu nutzen. Am 23. Februar 1918 meldete Arthur Scherbius das erste, die Enigma betreffende, Patent an, verkaufte aber in den folgenden Jahren nur wenige Exemplare.

Die Briten veröffentlichten erstmals ab 1923 Details zu Vorgängen des Ersten Weltkrieges, durch die den Deutschen erst klar wurde, dass ihre geheimen Nachrichten mitgelesen werden konnten. Durch die Enthüllungen stieg das Interesse an der Enigma. Die deutsche Marine sowie das deutsche Heer nahm die Maschine über die folgenden Jahre in den laufenden Betrieb auf.

Während des Zweiten Weltkrieges bereitete die Enigma den Alliierten zunächst Probleme. Mitarbeiter des Biuro Szyfrów (zu Deutsch „Chiffrierbüro“), der Zentrale der polnischen Dechiffrierbemühungen, hatten früh Erfolge bei der Entschlüsselung der Nachrichten. Sie nutzen deutsche Verfahrensfehler und eine zu Anfang geringere Zahl an möglichen Walzen, um mit Hilfe einer Maschine (genannt *Bomba*) automatisiert mögliche Schlüssel zu

überprüfen. Als die Deutschen ihren Verfahren verbesserten und die Walzenauswahl vergrößerten, teilten die Polen ihre Erkenntnisse mit den Briten, die darauf aufbauend ihre Methoden verbesserten und weitere Maschinen bauten, die schließlich zu der weitgehenden Entschlüsselung der Enigma-Kommunikation führte.

2.2.2 Funktionsweise

Die Maschine verbindet je eine von 26 Eingabetasten, von A bis Z, mit einer von 26 Lampen, die wiederum einem Buchstaben zugeordnet sind. Wird eine Taste gedrückt schließt sich ein Stromkreis und eine Lampe leuchtet auf. Der Weg, den der Strom nimmt, um eine Lampe zum Leuchten zu bringen, verändert sich mit jedem Tastendruck und bildet somit die eigentliche Verschlüsselung ab.

In der Enigma werden, die Eingangs- und Ausgangswalze ausgenommen, drei Walzen mit je 26 Ein- und Ausgängen hintereinander geschaltet. Nur die erste Walze bewegt sich mit jedem Tastendruck um eine Stelle. Die zweite Walze bewegt sich, sobald die Übertragskerbe der ersten Walze die zweite um eine Stelle weiter bewegt. Da es nur eine Kerbe pro Walze gibt, geschieht dies spätestens nach 26 Buchstaben. Die dritte Walze wird wiederum von der zweiten Walze vorangetrieben.

Mit diesem Aufbau wäre es nun schon möglich einen Text zu verschlüsseln, die Startpositionen der Walzen bilden den geheimen Schlüssel. Die Dechiffrierung ist jedoch nicht ohne weiteres möglich. Diese Möglichkeit eröffnete erst die Umkehrwalze nach der dritten Walze. Sie unterscheidet sich zu den anderen Walzen darin, dass sie nur auf einer Seite Kontakte besitzt, und diese durcheinander verbindet. 13 Kontakte werden also mit den 13 anderen Kontakten verbunden. Somit durchläuft der Strom bei der Verschlüsselung die drei Chiffrier-Walzen erneut, bis er die Lampen erreicht. Durch die Umkehrwalze ist nun auch die Entschlüsselung gegeben, denn mit den gleichen Startpositionen durchläuft der Strom den Pfad in umgekehrter Richtung und bringt den Ausgangsbuchstaben zum leuchten. Die Eingangswalze diente nur der Verbindung der Drähte mit den Walzen und führte zu keiner Verwürfelung der Buchstaben.

Anfangs gab es nur drei Walzen, die in der Reihenfolge, entsprechend des Tagesschlüssels, frei in die Enigma eingelegt werden konnten. Später musste der Operator drei aus einem Satz von fünf Walzen wählen, die aber auch in beliebiger Reihenfolge eingesetzt werden konnten. Die deutsche Marine besaß eine Version, in der drei aus acht Walzen gewählt wurden. An jeder Walze befindet sich ein Ring mit aufgedruckten Zahlen, anhand derer die Startposition eingestellt wird. Dieser Ring kann verschoben werden und ändert somit den Zeitpunkt, zu dem der Übertrag, also die Fortschreitung der nächsten Walze, stattfindet.

Als zusätzliche Sicherheit gibt es zudem ein Steckerbrett, mit Hilfe dessen Buchstaben-

paare vor und nach Walzenaustritt miteinander vertauscht werden. Zunächst wurden nur 6 von 13 Buchstabenpaaren miteinander getauscht, später dann 10.

2.2.3 Kryptografische Sicherheit

Als Schlüsselraum ergibt sich bei der Enigma I mit drei aus fünf Walzen und 10 Steckern: 60 Walzenlagen $*$ 676 Ringstellungen $*$ 16.900 Walzenstellungen $*$ 150.738.274.937.250 Steckermöglichkeiten = 103.325.660.891.587.134.000.000. Dies entspricht einer Bitlänge von etwa 76 Bit.

Die Enigma als Gerät besitzt mehrere Schwächen, die die effektive Schlüssellänge reduziert. Durch die Umkehrwalze ist es nicht möglich, dass ein Buchstabe auf sich selber abgebildet wird, denn dies hätte einen Kurzschluss zur Folge. Somit kann ein Buchstabe im Geheimtext nur von einem der anderen 25 Klartextbuchstaben kommen. Weiß man, oder vermutet man, dass sich ein bestimmtes Wort im Text befindet, kann man durch Vergleichen und Verschieben des vermutenden Wortes mögliche Positionen im Geheimtext für das Wort ausmachen, denn es kann nicht in der Position sein, in der sich im Klartext und Geheimtext die gleichen Buchstaben finden.

Das Steckerbrett sorgt zwar für eine große Menge an unterschiedlichen Schlüsseln, bietet aber im Endeffekt nur eine einfache monoalphabetische Substitution, die dazu auch noch selbstinvers ist. Das heißt, wenn X mit Y substituiert wird, dann wird auch Y mit X substituiert. Die Steckerung der Buchstaben ändert sich nicht während des Verschlüsselungvorgangs. Die monoalphabetische Verschlüsselung kann leicht durch Häufigkeitsanalyse oder durch *Cribs*[2] entziffert werden.

Auch durch die Ringstellung wird die Sicherheit der Enigma nicht erhöht, schließlich bedeutet eine Verschiebung des Ringes nur eine Verschiebung der Startposition der Walze. Probiert man alle möglichen Walzenstellungen einer Ringstellung durch, beinhaltet die Ausgabe auch alle anderen Ringstellungen.

Eine andere Art von Problem waren Fehler in der Art, wie die Enigma genutzt wurde. Der Tagesschlüssel, der die Einlegereihenfolge der Walzen, die Startpositionen der Walzen, die Ringstellung und die Steckerverbindungen beinhaltete, wurde nicht direkt genutzt, um Nachrichten zu chiffrieren. Stattdessen galt es, mit dem Tagesschlüssel einen Spruchschlüssel zu chiffrieren, der dann genutzt wurde, um die eigentliche Nachricht zu chiffrieren. Der verschlüsselte Spruchschlüssel wurde an den Anfang der Nachricht gestellt,

[2] Die Briten bezeichneten mit *cribs* bekannte oder vorhersehbare Wörter und Phrasen, die im Geheimtext enthalten sind. Bei deutschen Nachrichten war dies Beispielsweise „OBERKOMMANDOWEHRMACHT“ oder „KEINE BESONDEREN VORKOMMNISSE“

so dass der Empfänger den Spruchschlüssel ermitteln konnte. Dieses durchaus sehr sinnvolle Verfahren wurde jedoch dadurch abgewertet, als dass man den Spruchschlüssel zwei mal in Folge verschlüsselte, um eventuelle Übertragungsfehler auszuschließen. Die Angreifer wussten nun, dass der jeweils erste Buchstabe dem vierten entsprach, der zweite dem fünften und der dritte dem sechsten. Man änderte das Verfahren später und verschlüsselte den Spruchschlüssel nur noch einmal.

Der Spruchschlüssel einer Nachricht sollte vom Operator frei gewählt werden. Das führte dazu, dass leicht zu erratende Kombinationen wie ABC oder AAA verwendet wurden, oder immer wieder die Initialen der Geliebten des Operators gewählt wurde.

Die Briten nutzen Cribs, um automatisiert durchprobierte Schlüsselkombinationen auf Korrektheit zu überprüfen, aber auch um Rückschlüsse auf mögliche Schlüsselkombinationen zu ziehen.

2.2.4 Nutzung in der DDR

In der DDR wurde die Enigma noch bis 1956 verwendet, jedoch in weit geringerem Ausmaß als während des Zweiten Weltkrieges[11].

In den Erinnerungen des Fregattenkapitäns Riebe[13] wird beschrieben, wie das ZCO[3] noch im Sommer 1954 der Seepolizei 100 Enigmageräte zur Verfügung stellte. Um welche Ausführung der Enigma es sich handelte wird nicht explizit erwähnt, jedoch kann man aus der Beschreibung des, weiter unten beschriebenen, DORA-Verfahrens ableiten, dass es wahrscheinlich die Enigma I sein musste. Die spätere Herstellerfirma der Enigma, Heimsoeth & Rinke, existierte nur noch bis 1945[10], so dass die 100 Geräte noch aus einem größeren Bestand stammen mussten, und dies nur auf die Enigma I, die Enigma M3 und die M4 zutraf. Das DORA-Verfahren geht von 3 Walzen aus, was die M4 ausschließt, und gibt Zahlen für die Startposition der Walzen an. Die M3 verwendete jedoch Buchstaben.

Aus den Erinnerungen geht hervor, dass die Verdrahtungen der Walzen neu gelötet wurden, und somit nicht mit denen des Zweiten Weltkrieges identischen waren. Die ZCO wies ebenfalls an, das Gerät auf Batteriebetrieb umzubauen, vielleicht aus Gründen der Abstrahlung. Die alten Geräte und der Umstieg auf den Batteriebetrieb führten zu einer hohen Anfälligkeit, so dass immer ein Ersatzgerät bereitgehalten werden musste. Ein genaues Datum oder Jahr, bis wann die Geräte genutzt wurden, ist nicht zu ermitteln. Durch die Fehleranfälligkeit dürfte es sich jedoch auf wenige Jahre, wenn nicht sogar Monate, beschränkt haben.

Anfang der 50er Jahre wurde die Enigma auch in Ost-Berlin noch verwendet. Für die Kommunikation wurden eindeutige Bezeichnungen verwendet, wie zum Beispiel `GCPB 00101`.

[3] Zentrales Chiffrierorgan der DDR, identisch mit Abteilung XI im MfS

`GC` stand dabei für die DDR, `P` für Polizei, `B` für den Kommunikationsmodus „Handbuch Morse“, `001` für die Bezeichner des Netzwerkes und `01` für das Netz innerhalb des Netzwerkes. `GCPB 00101` war das letzte Kommunikationsnetzwerk, dass durch die Enigma verschlüsselte Signale übertrug[11].

Die Amerikaner hatten Zugriff auf `GCPB 00101` und konnten deren Inhalt entschlüsseln. Die Art der Nachrichten war auf den ersten Blick von geringerem Interesse: es handelte sich um Berichte über Schäden durch Feuer, Bereitschaft der Feuerwehr und Polizeiberichte, vorrangig über bedeutende Verhaftungen. Für die Amerikaner waren die Nachrichten in Zusammenhang mit *Operation Gold* dennoch von Interesse.

2.2.5 Operation Gold

Operation Gold[4] war eine von der CIA und dem britischen Secret Intelligence Service durchgeführte Abhöraktion in Berlin. Vorangegangen war die britische *Operation Silver*, die von 1949 bis 1955 in Wien Telefonleitung der Sowjetunion abhörte und daraus wichtige Erkenntnisse zur Vorbereitung des Koreakrieges erlangte[4]. Der Erfolg der Operation veranlasste den damaligen Direktor der CIA Allen Dulles auf eine ähnliche Abhöreinrichtung in Ost-Berlin hinzuarbeiten.

Man wusste, dass Berlin ein wichtiger Knotenpunkt der osteuropäischen Kommunikation darstellte. Alle Gespräche aus Osteuropa, auch Verbindungen nach Moskau, gingen über Berlin[12]. Durch einen Informanten innerhalb der Ost-Berliner Post wurde eine Kabeltrasse unterhalb der Schönefelder Chaussee ausgewählt, über deren Kabel wichtige telefonische und telegrafische Verbindungen des sowjetischen Militärs, der Sicherheitsdienste und Diplomaten liefen.

Die Arbeiten am Tunnel, der 450 Meter lang, über die Grenze bis ins Gebiet der DDR, verlaufen sollte, begann im Februar 1954 und wurden hauptsächlich am Tage durchgeführt, da der Straßenlärm die Geräusche der Bauarbeiten überdeckte. Der Abstand zwischen Tunnel und Oberfläche betrug teilweise nur 47 cm, so dass innerhalb das Abhörraums das Auftreten von Pferdehufen und sogar das stampfen von Polizisten hörbar war, die bei einer Straßensperre sich warm hielten, in dem sie von einem Fuß auf den anderen stampften[4]. Ein Jahr später wurde der Tunnel fertiggestellt und die Abhöraktion konnte beginnen.

Bis zum 22. April 1956 wurden um die 40.000 Gesprächsstunden und 6.000.000 Stunden telegrafischer Nachrichten aufgezeichnet[20]. Diese wurde in London durch zwischenzeitlich 317 Personen, sowie in Washington zur Hochzeit durch 350 Personen transkribiert und ausgewertet. Nach dem es in der Nacht des 16. April stark geregnet hatte, kam es zu mehreren Störungen der Telefonleitungen in der Region von Berlin. Für die Amerikaner

[4] Von der CIA/NSA auch *Operation REGAL* und *Operation PBJOINTLY* genannt, sowie von den Briten *Operation Stopwatch*

sah es so aus, als ob sowjetische Wartungsarbeiter defekte Kabel austauschen und dadurch zufällig auf den Abhörraum stießen. Erst 1961 stellte sich heraus, dass die Russen die Gelegenheit der starken Regenfälle nutzen, um den ihnen seit Anfang an bekannten Tunnel auffliegen zu lassen. Georg Blake, ein Doppelagent, der sowohl im britschen Geheimdienst als auch für den KGB tätig war, berichtet dem KGB bereits während der Planungsphase von Operation Gold. Um Blake als hochkarätigen Agenten jedoch nicht gefährden, wollten, vielleicht auch um gezielt falsche Informationen zu übermitteln, die Russen den Tunnelbau nicht früher auffliegen lassen.

Nichtsdestotrotz geht die CIA davon aus, dass der Großteil der abgefangenen Informationen korrekt waren und durchaus sehr nützlich. Die Auswertung der Aufzeichnungen dauerte noch über zwei Jahre nach Entdeckung des Tunnels an, bis zum 30. September 1958.

Die abgefangenen Nachrichten waren teilweise verschlüsselt. Ein deklassifiziertes Dokument der CIA[4] beispielsweise benennt „VHE CHE“ (und meint damit WTsch), womit jegliche Form von verschlüsselter Sprachübertragung von sowjetischer Seite gemeint ist.

Die NSA wurde nicht von Anfang in die Operation mit einbezogen, wenngleich dies eigentlich durch die CIA hätte initiiert werden müssen. Erst als die CIA Probleme hatte, genug vertrauenswürdiges deutsch- und russisch-sprechendes Personal einzustellen, wurde die NSA informiert.

Inwiefern die verschlüsselte Kommunikation ausgewertet werden konnte, ist nicht mit Sicherheit zu sagen. Allerdings beschäftigt sich die Einleitung in eines NSA Dokuments[12] mit einer Verschlüsselungsmaschine namens SIGTOT, entwickelt von Bell System. Es wird ausgeführt, dass dieses Gerät nicht in den Gebrauch genommen wurde, als man feststellte, dass während der Nachrichtenübertragung ein schwaches Echo des Originaltextes mitgesendet wurde und ausgelesen werden konnte. Diese Erkenntnisse sollten nun auch auf Sowjetische Drahtverbindungen in Ost-Berlin angewandt werden. Der Abschnitt, der mutmaßlich mehr über diese Bemühungen, gerade in Hinblick auf Operation Gold, preisgibt, ist jedoch in dem 2012 veröffentlichen Dokument immer noch zensiert.

2.2.6 DORA-Verfahren

In einem Entwurf der 8. Abteilung der Volkspolizei[24] wird der „Fernschreibschlüssel DORA“ näher erläutert. Es handelt sich dabei um die Aufbereitung einer zu versendenden Nachricht, sowie dem Aufbau der zu sendenden Daten, die per Draht übermittelt werden sollten. Eine handschriftliche Notiz deutet darauf hin, dass der Entwurf abgelehnt wurde, jedoch wird das Verfahren in späteren Erinnerungen[13] ausdrücklich erwähnt.

Eine fertig aufbereitete Nachricht besteht aus folgenden Elementen:

Uhrzeitgruppe Gruppenzahl Kennzahl Schlüsselgruppe	Text	An-/Unterschrift
Unverschlüsselt	Teilverschlüsselt	Unverschlüsselt

Die *Uhrzeitgruppe* ist beispielsweise 17,35 für die Uhrzeit 17:35. Die *Gruppenzahl* gibt die Länge einer Nachricht in „Gruppen“ an. Je vier Buchstaben entsprechen einer Gruppe. Die *Kennzahl*, eine vom Absender ausgewählte (möglichst zufällige) Zahl, ergibt zusammen mit der Uhrzeit und der Nummer des Tages im Monat den Spruchschlüssel nach folgendem Beispiel:

Uhrzeitgruppe + Datum	1	7	3	5	0	6
willkürl.gew.Kennzahl		4		3		8
	2	1	3	8	1	4

Die Kennzahl wird mit je zwei Ziffern der oberen Zahlenreihe addiert, also im Beispiel zum Beispiel $17 + 4 = 21$. Diese Zahl soll einer Walzeneinstellung zugeordnet werden, die, gleich der Anzahl der Buchstaben, zwischen 1 und 26 liegen kann. Ist eine Zahl größer als 26, so wird so lange durch 2 geteilt, bis sie dieses Kriterium erfüllt. Bei der späteren Übermittlung der Kennzahl findet nochmal eine tagesabhängige Substitution statt.

Der Absender stellt die Walzenpositionen auf die errechneten Zahlen und wählt vier zufällige Buchstaben, die er auf der Tastatur eingibt und verschlüsselt. Die resultierenden vier Buchstaben ergeben die *Schlüsselgruppe*.

Zur Vorbereitung, um die eigentliche Nachricht zu verschlüsseln, werden die drei ersten Buchstaben der (unverschlüsselten) Schlüsselgruppe genommen, und entsprechend einer tagesabhängigen Substitutionstabelle in Zahlen umgewandelt, die die Startposition der Walzen ergeben. Der Nachrichtentext wird mit Hand in zwei Spalten geschrieben, je abwechselnd ein Buchstabe in die linke und rechte Spalte. Nach vier Buchstaben ist eine Zeile voll und man beginnt eine neue Zeile. Folgendes Original-Beispiel erläutert das Verfahren für die Nachricht `betrifftxsofortmeldungxx`:

	Schlüsselgruppen							
1	b	t	i	f				
2					e	r	f	t
3	x	o	o	t				
4					s	f	r	m
5	e	d	n	x				
6					l	u	g	x

Also B in das 1. Kästchen der linken 1. Gruppe
E " " 1. " " rechten 2. "
T " " 2. " " linken 1. "
R " " 2. " " rechten 2. "
i " " 3. " " limken 1. "

u. s. w.

Nun werden nur die Buchstaben der rechten Spalten in die Enigma eingegeben und verschlüsselt. Der resultierende Geheimtext besteht zeilenweise aus der unverschlüsselten linken Spalte und der verschlüsselten rechten Spalte.

Zuletzt besteht eine Nachricht noch aus einem unverschlüsselten Absender und Adressaten, die durch Tarnwörter ersetzt wurden.

Bei der Entschlüsselung werden die Schritte rückwärts angewandt.

Für jeden Tag des Jahres sollte es eine „Parole“ geben, die die Einstellungen der Enigma abdeckten. Dazu gehörten die Steckerverbindungen des Tages, welche zumindest 1954 aus 12 Paaren bestand. Ein Buchstabenpaar blieb somit ohne Vertauschung. Die anderen beiden Komponenten der Tagesparole sind die bereits erwähnten Substitutionen der Kennzahl und des Spruchschlüssels.

Außer der Tagesparole und der Verdrahtung der Walzen scheint die Sicherheit des Verfahrens auch darauf zu bauen, dass die Schritte des Verfahrens an sich geheim bleiben. Immerhin besteht die Hälfte des Nachrichtentextes aus Buchstaben aus der Originalnachricht in korrekter Reihenfolge, wenn auch nur mit jedem zweiten Buchstaben, und durch Gruppen verschlüsselter Buchstaben unterbrochen.

Um auf den geheimen Spruchschlüssel zu kommen, muss man sowohl die Verdrahtung der Walzen, die Steckeranordnung als auch die Substitutionswerte der Kennzahl kennen. Es fällt jedoch auf, dass die möglichen Startpositionen der Walzen zu jedem Zeitpunkt auf nur 10 mögliche Werte pro Walze beschränkt sind. Am 1. eines Monats beispielsweise ergibt die Addition eines Kennziffer zwischen 0 und 9 stets eine Zahl zwischen 1 und 10. Da die Uhrzeit in der Nachricht unverschlüsselt mitgesendet wird und der Tag bekannt ist, ergeben sich nur maximal $10 * 10 * 10 = 1000$ mögliche Walzenstellungen.

Im Zweiten Weltkrieg wurde der Spruchschlüssel immer mit der gleichen Startposition verschlüsselt und übermittelt, so dass eine entschlüsselte Nachricht die Startposition der Walzen, und damit auch die Spruchschlüssel aller anderen Nachrichten preisgab.

Im Gegensatz dazu würde eine entschlüsselte Nachricht des DORA-Verfahrens zwar die Steckeranordnung und Walzenreihenfolge preisgeben, nicht jedoch die Startpositionen der Walzen. Allerdings dürfte es nicht lange dauern, die 1000 Positionen ebenfalls zu überprüfen.

2.3 M-125 „Fialka“

Eine der weitverbreitesten Chiffriermaschinen des Warschauer Pakts war die M-125, deren Chiffrieralgorithmus den Codenamen *FIALKA* (russisch ФИАЛКА) trägt. Vom Aufbau her ähnelt sie der Enigma und arbeitet ebenso mit mehreren Rotoren, die den Großteil der Chiffrierung übernehmen. Wenngleich die Erfolge der Dechiffrierung der Enigma durch

Abbildung 2.3: Polnische Fialka M-125-3MP2

die Alliierten noch viele Jahre vor der Öffentlichkeit geheim gehalten wurden, schienen die Sowjets doch aus den Nachteilen der Enigma gelernt zu haben. Sie hatten während des Krieges mehrere Enigmas erbeutet und wussten vermutlich, wie man die Nachrichten in der Theorie dechiffrieren konnte. Der technische Wissensstand hingegen reichte nicht aus, um ein der Turing-Bombe ähnliches Gerät zu bauen[8]. Es ist auch nicht ganz ausgeschlossen, dass die Alliierten ihre Erfolge mit den Russen geteilt hatten.

Noch viele Jahre nach dem Auseinanderbrechen der Sowjetunion gab es kaum Informationen zur Fialka, geschweige denn Geräte, die man hätte untersuchen können. 2005 gelang eine Fialka in den Besitz der Niederländer Paul Reuvers und Marc Simons, die die Funktionsweise durch Reverse Engineering ergründeten und die Ergebnisse auf ihrer Webseite veröffentlichten.

In den folgenden Abschnitten wird der Begriff Fialka verwendet, wenn sowohl die M-125, als auch die verbesserte Version M-125-3 gemeint ist.

2.3.1 Geschichte

Die M-125 wurde in der Sowjetunion entwickelt und war in der ersten Version ab 1956 in Gebrauch. Eine verbesserte Version, die M-125-3, wurde 1965 eingeführt. Es gibt bei beiden Modellen jeweils nationale Varianten, die, soweit bekannt, in Tabelle 2.1 aufgelistet

Modell-Bezeichnung	**Land**	**Bemerkung**
M-125-MN	DDR	
M-125-MR	Tschechoslowakei	Auf russisch: M-125-MP
M-125-M	Polen	
M-125-??	Russland	Genaue Bezeichnung nicht bekannt
M-125-??	Ungarn	Genaue Bezeichnung nicht bekannt
M-125-3MN	DDR	
M-125-3MR3	Tschechoslowakei	Auf russisch: M-125-3MP3
M-125-3MR2	Polen	Auf russisch: M-125-3MP2
M-125-3M	Russland	
M-125-3??	Ungarn	Genaue Bezeichnung nicht bekannt, da bisher nur die Walzen gefunden wurden

Tabelle 2.1: Bekannte Varianten der Fialka

sind. Diese Varianten unterscheiden sich in der jeweils an die Landessprache angepassten Tastaturbelegung, und daraus resultierend auch angepassten Druckerkopf, sowie eine jeweils andere Verdrahtung der einzelnen Rotoren (siehe Tabelle 2.2).

Der spezielle Walzensatz mit der Serie 0K sollte innerhalb des Warschauer Pakts nur im Kriegsfall Anwendung finden, und auch erst dann durch Russland verteilt werden. Ohne diesen einheitlichen Walzensatz war eine Kommunikation zwischen den Vertragsteilnehmer nicht möglich, da die Verdrahtung innerhalb der Walzen sich von Land zu Land unterschied. Soweit bekannt kam der 0K-Walzensatz nie zur Anwendung.

Das Chiffriergerät war bis zum Zerfall der Sowjetunion in Gebrauch, und in manchen ehemaligen Ländern der Sowjetunion noch darüber hinaus. In der ehemaligen Tschechoslowakei soll die M-125-3 noch bis 1993 genutzt worden sein[2].

2.3.2 Funktionsweise

Die Ausgabe erfolgt nicht über eine Leuchtanzeige, sondern wird direkt auf einen Papierstreifen gedruckt, und optional zusätzlich auf einen maschinenlesbaren Lochstreifen, kodiert als 5-Bit-Code.

Der Tastatur und der Walzen liegt die Zahl 30 zur Grundlage. Es gibt 30 unterschiedliche Zeichen, die kodiert werden können, und jede Walze besitzt 30 unterschiedliche Positionen, die mit je einem Buchstaben aus dem russisch-kyrillischen Alphabet gekennzeichnet sind.

Der Kodieralgorithmus verläuft, beispielhaft in Abbildung 2.4 gezeigt, so, dass eine Taste gedrückt wird und sich somit ein Stromkreis schließt, der bestimmt, welcher Ausgangs-

Bezeichnung	**Land**
1K	Tschechoslowakei
3K	Polen
4K	DDR
6K	Tschechoslowakei
0K	Verdrahtung für Kriegsfall, gleich für alle Länder des Warschauer Pakts

Tabelle 2.2: Bekannte Bezeichnungen der Rotor-Verdrahtungen

buchstabe auf das Papier gedruckt wird. Zunächst läuft der Strom in einen Kartenleser, innerhalb dessen der Eingangsbuchstabe durch einen anderen Buchstaben substituiert werden kann (aber nicht muss). Dies wird mit einer 30x30 Lochkarte erreicht, die jedem Eingangsbuchstaben einem Ausgangsbuchstaben zuordnet. Nach Verlassen des Kartenlesers läuft der Strom über die Eingangswalze durch die 10 Chiffrierwalzen, deren interne Verkabelung jedem Eingangsbuchstaben wiederum einen Ausgangsbuchstaben zuordnet. Diese Walzen können sich nach jedem Tastendruck weiter drehen, wobei das Fortschreiten der Walzen unregelmäßig ist und von sperrenden Stiften abhängig ist. Am Ende der Kodierwalzen sitzt, wie schon bei der Enigma, die Umkehrwalze, die für eine weitere Substitution verantwortlich ist, und das Signal zurück in die Kodierwalzen leitet, so dass der Strom die Walzen und den Kartenleser erneut durchläuft. Nun wird das Signal in einen 5-Bit Code umgewandelt und auf ein Stück Papier gedruckt. Optional kann auch der Lochstreifen gestanzt werden, oder das Signal an ein externes Gerät (beispielsweise für die direkte Übertragung über ein Nachrichtenmedium) weiterleitet werden.

2.3.3 Dreipunktschaltung

Als Besonderheit der Fialka ist die Dreipunktschaltung innerhalb der Umkehrwalze zu nennen, die es ermöglicht, dass ein Buchstabe auch auf sich selbst abgebildet werden kann. Dieser bedeutende Schwachpunkt der Enigma wurde durch diese Schaltung ausgeschlossen. Wie bereits bei der Enigma erwähnt, würde eine Abbildung auf den gleichen Buchstaben zu einem Kurzschluss führen, da der Strom auf den gleichen Eingangspfad gelegt werden würde. Um dies zu umgehen, sind vier Eingänge der Umkehrwalze von der normalen Substitution ausgenommen. Ein Eingang (bei der ersten Version M-125 Eingang 13) sendet den Strom auf einem gesonderten Pfad, der nicht erneut die Walzen durchläuft, sondern der Ausgabe anweist, den aktuell gedrückten Buchstaben zu drucken. In Abbildung 2.4 ist dieses Signalpfad gestrichelt eingezeichnet. Für die verbleibenden drei Eingangspfade wählt die Dreipunktschaltung einen der anderen beide Pfade aus (ver-

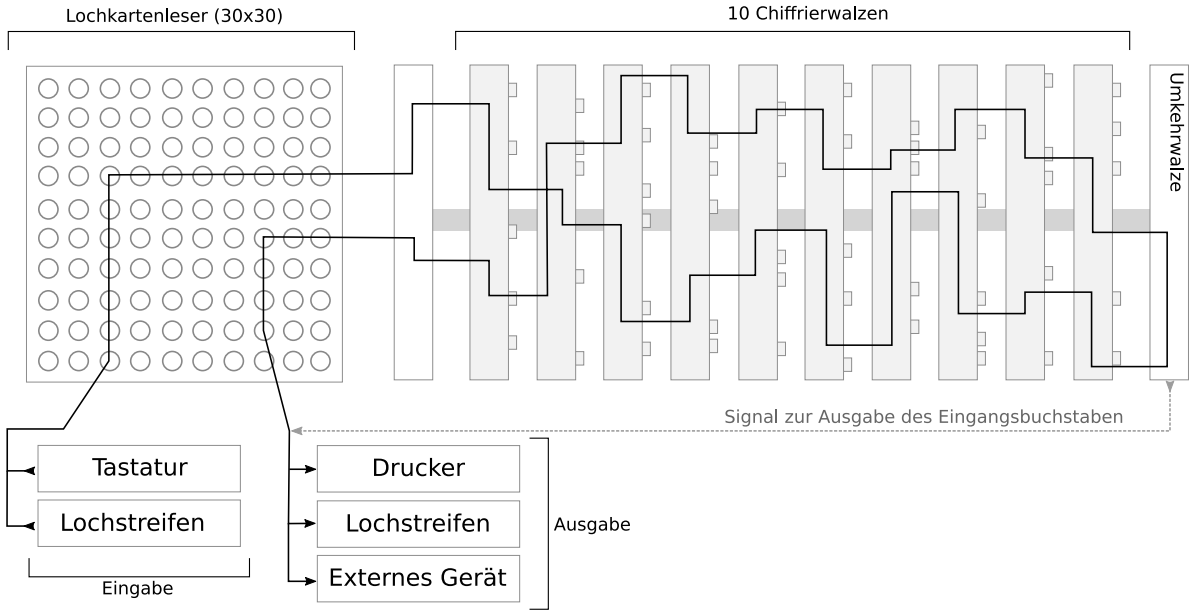


Abbildung 2.4: Schema der Verschlüsselung der Fialka mit Beispielpfad

gleiche Tabelle 2.3). Da diese Permutation nun nicht mehr reziprok ist, muss am Gerät ausgewählt werden, ob verschlüsselt oder entschlüsselt wird, um die Umkehrbarkeit zu gewährleisten.

2.3.4 Walzen

Es gab zwei unterschiedliche Versionen der Walzen. Die erste, frühere, hatte weniger Einstellungsmöglichkeiten als die spätere Version, die *PROTON-2* genannt wird. Zunächst wird die erste Version betrachtet, die als fixierte Walze bezeichnet wird.

Modus	**Substitution**
Verschlüsseln	
	$16 \longrightarrow 18$
	$18 \longrightarrow 24$
	$24 \longrightarrow 16$
Entschlüsseln	
	$16 \longrightarrow 24$
	$18 \longrightarrow 16$
	$24 \longrightarrow 18$

Tabelle 2.3: Pfade der Dreipunktschaltung einer M-125

Die fixierten Walzen wurde mit dem ersten Modell M-125 geliefert. Ein Walzenset besteht aus 10 Walzen, wobei jede Walze eine andere Verdrahtung aufweist. Zwischen den einzelnen Ländern unterscheiden sich die Verdrahtungen ebenfalls. Auf der einen Seite einer Walze gibt es 30 unter Federspannung stehende Eingangskontakte, die durch Drähte mit einem der 30 Ausgangskontakte auf der gegenüberliegenden Seite verbunden sind. Jede Walze wird eindeutig durch einen von 10 kyrillischen Buchstaben identifiziert. Des weiteren besitzt jede Walze eine variable Anzahl von blockierenden Metallstiften, die für ein unregelmäßiges Fortschreiten der Walzen erforderlich sind. Darauf wird später noch einmal eingegangen.

Die Einstellungsmöglichkeiten, als Teil des geheimen Schlüssels, ergeben sich bei einem fixierten Walzensatz aus der Reihenfolge der Walzen, die auf einer Spindel in beliebiger Reihenfolge aufgereiht werden können, sowie den Startpositionen der einzelnen Walzen, sobald die Spindel eingesetzt ist. Die Startpositionen sind am seitlichen Rand der Walze mit 30 russisch-kyrillischen Buchstaben gekennzeichnet.

Die PROTON-2-Walzen sind deutlich komplexer aufgebaut und erweitern den Schlüsselraum beträchtlich. Der Aufbau einer Walze ist zunächst der fixierten recht ähnlich. Einem Eingangskontakt wird einem Ausgangskontakt zugewiesen, jedoch ist die innere Verdrahtung nun nicht mehr mit der Walze fixiert, sondern kann entfernt und in einer beliebigen anderen Position wieder angebracht werden. Es ergeben sich 30 unterschiedliche Stellungen, indem man die herausnehmbare Verdrahtungsscheibe schrittweise dreht. Wendet man die Scheibe, ergeben sich 30 weitere Positionen, da die Verdrahtung nun gespiegelt ist. Beide Seiten sind mit der Zahl 1 oder 2 beschriftet, um sie korrekt einsetzen zu können. Zu beachten ist, dass die Verdrahtungsscheiben untereinander zwischen den verschiedenen Walzen getauscht werden können. Daher besitzt jede Scheibe neben der Seitenangabe auch einen von 10 Buchstaben, der die Verdrahtungsscheibe identifiziert.

Eine weitere Einstellungsmöglichkeit bietet der äußere Ring der Walze, auf denen die 30 kyrillische Buchstaben aufgebracht sind. Der Ring kann an eine andere Position gedreht werden, so dass die Bezeichnungen zum Einstellen der Startpositionen einer anderen Verdrahtung entspricht.

Somit ergeben sich als Teil des Tagesschlüssels die Reihenfolge der Walzen auf der Spindel (10 von 10 Buchstaben), die äußere Ringstellung (10 von 30 Buchstaben, einer für jede Walze), welche Verdrahtungsscheibe in welche Walze eingelegt wird (10 von 10 Buchstaben), sowie mit welcher Seite (1 oder 2 für jede Walze) und in welcher Position (10 von 30 Buchstaben, einer für jede Walze) die Verdrahtungsscheibe in eine Walze eingesetzt wird.

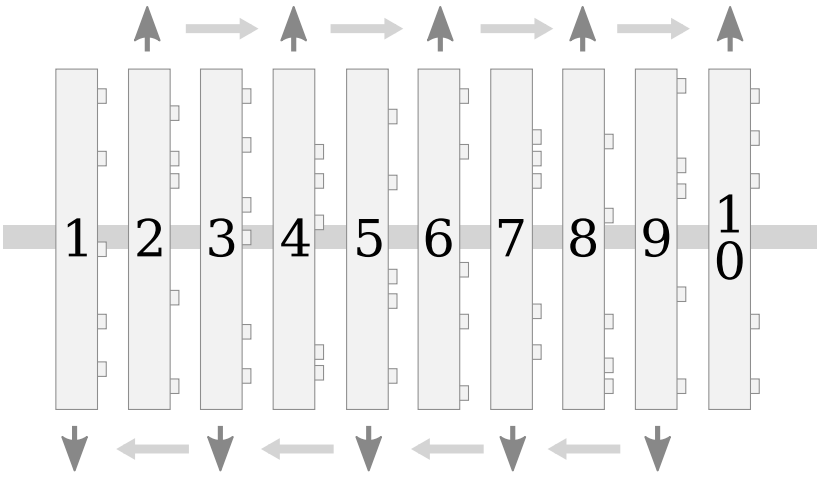


Abbildung 2.5: Fortschreitung der Walzen einer Fialka

2.3.5 Fortschreitung der Walzen

Die Fortschreitung der Walzen entspricht nicht, wie in der Enigma, einer Fortschreitung ähnlich eines Tacho, sondern ist unregelmäßig. Um die Fortschreitung genauer zu erklären, sollen die Walzen, wie in Abbildung 2.5, von 1 bis 10 benannt werden, von links nach rechts. Die Walzen mit gerader Zahl bewegen sich in entgegengesetzter Richtung zu den Walzen mit ungerader Nummerierung. Von oben gesehen bewegen sich die aufgedruckten Buchstaben weg von der Tastatur, hin zum hinteren Teil der Maschine. Die Buchstaben auf den ungeraden Walzen bewegen sich hin zur Tastatur.

Prinzipiell könnte sich jede Walze mit einem Tastendruck um eine Position weiter drehen. Jedoch kommen hier die Metallstifte an den Walzen zu tragen, die das Fortschreiten einer benachbarten, sich in gleicher Richtung bewegenden, Walze verhindern. Somit blockieren also die Stifte der Walze 2 die Bewegung der Walze 4, dieser wiederum Walze 6 und diese schließlich Walze 8. Die Stifte der achten Walze haben keine Auswirkung, da aber jede Walze prinzipiell an jede Position im Walzensatz gesetzt werden kann, sind sie dennoch wichtig. Bei den ungeraden Walzen beeinflussen sich die Walzen von rechts her, also blockiert Walze 9 die Walze 7, und so weiter.

Somit wird klar, dass die zweite und neunte Walze sich bei jedem Tastendruck weiterbewegen, die anderen jedoch nur in Abhängigkeit ihrer Vorgängerwalze. Jede Nachfolgerwalze bewegt sich insgesamt seltener als ihre Vorgängerwalze der gleichen Richtung.

2.3.6 Lochkarte

Anstatt der Steckerbrett-Substitution der Enigma besitzt die Fialka eine wesentlich komfortablere Einrichtung: eine Lochkarte, die vor Eintritt in die Walzen sowie auf dem Rück-

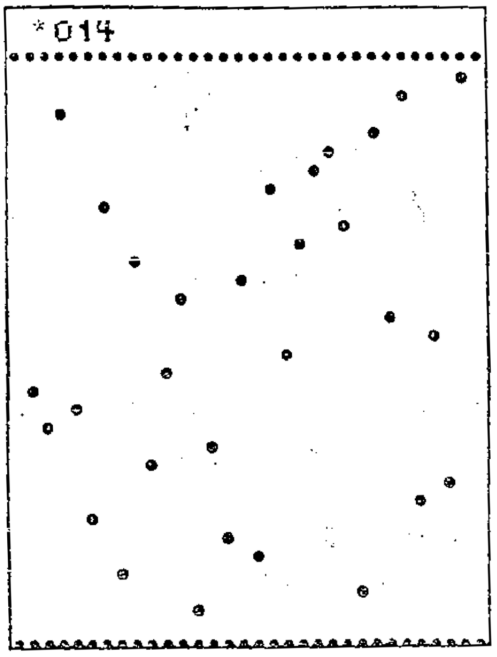


Abbildung 2.6: M-125 Lochkarte aus Anleitung DV A 040/1/321

weg jeweils einen Eingangsbuchstaben einem Ausgangsbuchstaben zuweist, der auch identisch mit dem Eingangsbuchstaben sein kann. Dadurch findet bei jedem Durchlauf eine Substitution statt. Die Lochkarte besteht aus einer 30x30 Matrix, also eine Spalte und eine Zeile für jede Taste.

Die Lochkarte bildet zusammen mit den Walzeneinstellungen den Tagesschlüssel. Die Lochkarte wurde für den jeweiligen Tag von einem Block von Lochkarten abgerissen und bestand aus sehr dünnem Papier, das beim Einlegen und Entfernen aus dem Lochkartenlesen leicht in Mitleidenschaft gezogen werden konnte, wodurch verhindert werden sollte, dass eine bereits benutzte Lochkarte erneut eingesetzt wird, und somit die Sicherheit vermindert hätte.

Für Tests, oder einer Verschlüsselung mit verminderter Sicherheit, gibt es ein Metalldreieck, das anstelle der Lochkarte eingelegt werden kann und somit die Einheitsmatrix darstellt. Sie bildet also A auf A, B auf B, usw. ab.

2.3.7 Tastatur und Zeichen

Es gibt 30 unterschiedliche Tasten für die Texteingabe, die für unsere 26 lateinische Buchstaben ausreichend ist, jedoch nicht für die 33 kyrillischen Buchstaben, die im russischen genutzt werden. Das Alphabet wurde deshalb auf die häufigsten 30 Buchstaben reduziert:

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ы Ь Ю Я Й

Bei den international Varianten sind die lateinischen Buchstaben, zusätzlich zu den russischen, auf die Tasten gedruckt. Bei der M-125 enthält der Druckkopf zwei Reihen, die, je nach Schalterstellung, auswählen, ob lateinisch oder kyrillisch gedruckt wird.

Die M-125-3 hingegen besitzt auswechselbare Druckköpfe, einen für lateinisch und einen für kyrillisch. Die zweite Zeichenreihe des Druckkopfes enthält zusätzlich Zeichen, die vormals nicht gedruckt werden konnten. Von den drei fehlenden Buchstaben des kyrillischen Alphabets wurde nur Й aufgenommen, Ё und Ъ konnten jedoch weiterhin bedenken los ausgelassen werden[5]. Hinzugekommen sind Zahlen und Satzzeichen.

Es gibt nun auch unterschiedliche Text-Modi. Im Buchstaben-Modus werden weiterhin nur 30 unterschiedliche Buchstaben gedruckt, somit ist er zur M-125 kompatibel. Im Zahlen-Modus wird der zweite Zeichensatz des Druckkopfes aktiv, der Zahlen, Satzzeichen und vorher nicht darstellbare Buchstaben beinhaltet. Im dritten Modus, dem gemischten Text-Modus, werden zwei Tasten zu Umschaltern umfunktioniert, deren Tastendruck die Maschine anweist, ob die nachfolgenden Zeichen dem Buchstaben- oder dem Nummern-Zeichensatz entspringen sollen.

Bei den internationalen Modellen der M-125-3 befanden sich daher 4 Zeichen auf einer Taste, die je nach Druckkopf und Textmodus gedruckt wurden.

Bei der Ver- und Entschlüsselung wird die linke obere Taste (J auf der deutschen Tastatur) gesondert behandelt. Im Chiffriermodus kann sie nicht gedrückt werden kann. Stattdessen kommt die Leertaste als 30. Zeichen zum Einsatz. Bei der Dechiffrierung hingegeben ist die Leertaste blockiert und die linke obere Taste erlaubt, schließlich kann der dort abgebildete Buchstabe im verschlüsselten Text vorkommen.

2.3.8 Lochstreifen

Neben der Druckausgabe kann die M-125 den verschlüsselten Text auf einem Lochstreifen stanzen, und ihn auch wieder einlesen. Somit konnten Fehler vermieden und die Entschlüsselung beschleunigt werden.

Der Kodierung der 5 Bits zu einem Zeichen entspricht keiner standardisierten Kodierung, sondern ist der Fialka eigen, und wurde lediglich bei einem anderen Verschlüsselungsgerät (M-105 AGAT) ebenfalls verwendet.

Die maximal möglichen 32 Zeichen werden durch die 30 Buchstaben der Tastatur belegt. Die zwei verbleibenden Zeichen sind das Leerzeichen und ein STOP-Signal, das dem Lochstreifenleser mitteilt, dass der Streifen an diesem Punkt endet.

[5] Durch eine Reform von 1918 wurde die Anwendung von Ъ extrem selten. Ё wird auch heute noch oft durch E ersetzt.

Im gemischten Textmodus, der mehr als 30 Zeichen erlaubt, werden zwei Zeichen reserviert. Das eine besagt, dass alle nachfolgenden Zeichen dem „Nummern"-Modus entsprechen, während das andere den „Buchstaben"-Modus aktiviert. Somit weiß der Drucker, welchen Zeichensatz er nehmen muss, um die Nachricht zu drucken.

2.3.9 Netzteil

Gegenüber dem Standard-Netzteil der Fialka gibt es noch ein abstrahlungssicheres Netzteil, beschriftet als *БПК-125*. Da die Fialka einen Digital-Anschluss für die weitere Übertragung besitzt, bestand die Gefahr, dass durch Abstrahlung der Maschine Klartextinformationen oder Hinweise auf die Schlüsseleinstellungen unbeabsichtigt mitgesendet wurden. Bei der amerikanischen NSA wurde diese Schwachstelle, als auch die Maßnahmen dagegen, als *TEMPEST* bezeichnet.

Außer Polen ist derzeit kein anderes Land bekannt, dass dieses Netzteil nutzte[16]. In der DDR wurde angewiesen, dass ein Mindestabstand von 0,5m zwischen Fialka (mit Netzteil und Stromkabel) und anderen Geräten, sowie deren Kabeln, eingehalten werden musste[23].

2.3.10 Kryptografische Sicherheit

Um den Schlüsselraum der Fialka zu ermitteln, muss zwischen den zwei Walzensätzen unterschieden werden.

Die 10 Walzen des fixierten Walzensatzes können auf 10! unterschiedliche Arten eingesetzt werden und auf 30^{10} unterschiedliche Startpositionen gesetzt werden. Durch die Lochkarte ergeben sich 30! mögliche Substitutionen. Die Schlüssellänge ergibt somit:

$$\begin{aligned} 10! \cdot 30^{10} \cdot 30! &\approx 5.68 \cdot 10^{53} \\ &\approx 2^{178.57} \approx 178\ Bit \end{aligned}$$

Die Schlüssellänge des PROTON-2-Walzensatzes setzt sich zusammen aus den gleichen Einstellungen der fixierten Walzen, und zusätzlich aus 10! Möglichkeiten die Verdrahtungsscheiben auf die Walzen aufzuteilen, 2^{10} für die Auswahl welche der zwei Seiten der Verdrahtungsscheibe eingesetzt wird und 30^{10} unterschiedliche Positionen der Verdrahtungsscheiben innerhalb der Walzen. Die äußere Ringstellung liefert weitere 30^{10} Einstellungsmöglichkeiten. Somit ergibt sich eine maximale Schlüssellänge von:

$$\begin{aligned} 10! \cdot 30^{10} \cdot 30! \cdot 10! \cdot 2^{10} \cdot 30^{10} \cdot 30^{10} &\approx 7.36 \cdot 10^{92} \\ &\approx 2^{308.5} \approx 309\ Bit \end{aligned}$$

Dies entspricht der Maximalzahl der unterschiedlichen Einstellungsmöglichkeiten, jedoch gibt es dabei eine große Zahl an äquivalenten Schlüsseln. Dies bedeutet, dass unterschiedliche Schlüssel für den gleichen Klartext den gleichen Geheimtext produzieren. Die äußere Ringstellung hat keine kryptografische Relevanz, da sich nur die Bezeichnung der Walzenpositionen verschiebt. Dadurch entfallen 30^{10} Einstellungen. Die Metallstifte der letzten Walzen beider Drehrichtungen haben keine Auswirkung auf das Fortschreiten einer anderen Walze. Somit hat die Position der Verdrahtungsscheibe zu den Metallstiften keine Auswirkung auf die Verschlüsselung und ist gleichbedeutend mit einer Verschiebung der Walzenposition. Es berechnet sich ein effektiver Schlüsselraum von:

$$\begin{aligned} 10! \cdot 30^{10} \cdot 30! \cdot 10! \cdot 2^{10} \cdot 30^{8} &\approx 1.39 \cdot 10^{75} \\ &\approx 2^{249.62} \approx 250\ Bit \end{aligned}$$

Eugen Antal und Pavol Zajac haben in einem wissenschaftlichen Artikel[2] den Schlüsselraum der Fialka auf äquivalente Schlüssel hin analysiert, die eventuell durch unterschiedlichen Walzenreihenfolgen oder Rotationen der Verdrahtungsscheiben entstehen könnten. Sie fanden heraus, dass, zumindest bei den beiden zu der Zeit veröffentlichten Walzenverdrahtungen der 3K und 6K Serie, die Platzierung der blockierenden Stifte so gewählt wurde, dass keine äquivalenten Schlüssel möglich sind.

Man sagt, dass im Sechs-Tage-Krieg eine Fialka den Ägyptern in die Hände fiel, wodurch sie ab 1967 als kompromittiert betrachtet wurde. Dennoch blieb die Maschine noch lange im Gebrauch, wohl auch weil der PROTON-2-Walzensatz eine hohe Sicherheit versprach. Man sagte dennoch, dass eine mit der Fialka verschlüsselte Nachricht, die drahtlos übertragen wurde, nach 24 Stunden als entschlüsselt zu betrachten wäre[17]. Ein schriftlicher Nachweis darüber findet sich in den Dokumenten des MfS bisher nicht.

Es gibt mündliche Berichte gegenüber Paul Reuvers und Marc Simons von cryptomuseum.com aus drei unterschiedlichen Quellen, dass die NSA die Fialka in den Siebziger Jahren mit Hilfe des Cray-1 Supercomputers entschlüsseln konnte. Die abgefangenen Funksprüche sollen aus Österreich geliefert worden sein, die ihre Informationen mit den USA teilten. Schriftliche Beweise liegen jedoch auch hier nicht vor, genauso wenig wie Hinweise auf Schwächen der Fialka.

2.3.11 Nutzung in der DDR

Während das Modell M-125 in Russland bereits ab 1956 genutzt wurde, begann der Betrieb der lokalen Variante M-125-MN in der DDR erst 1968. Die verbesserte Version M-125-3MN folgte in der DDR 1978[5]. Verbreitung fand das Gerät auf allen Ebenen der

Fehlender Buchstabe	**Ersatz**
Ä	AE
Ö	OE
Ü	UE
ß	SZ
J	I
Q	KV
W	VV
X	KS
Y	I

Tabelle 2.4: Substitution fehlender Buchstaben

NVA und des Ministerium des Inneren. 1990 wurden die verbliebenen Geräte an Russland zurückgegeben, oder wurden zerstört.

Die 30 Tasten der DDR-Variante der M-125 setzen sich aus 22 Buchstaben und 8 Ziffern zusammen. Die Buchstaben `Q`, `W`, `X`, `Y`, sowie `0` und `1` wurden ausgelassen, da sie entweder zu selten vorkommen oder durch andere Zeichen ersetzt werden können (siehe Tabelle 2.4). Das `I` beispielsweise kann auch eine `1` oder ein `J` darstellen. Fehlende Zahlen wurden durch deren ausgeschriebene Wortrepräsentation wiedergegeben. Es gibt zwar eine Taste für `J`, jedoch hat sie in Bezug auf das Leerzeichen eine andere Bedeutung. Insofern können nur 21 Buchstaben wirklich genutzt werden.

Die M-125-3 kann durch den gemischten Textmodus alle Buchstaben und Zahlen, sowie Umlaute und Satzzeichen darstellen.

Mit Hilfe des Morse-Code-Geber *P-590A* konnte der verschlüsselte Text als Morse-Code übertragen werden[9]. Dazu konnte sowohl die Datenschnittstelle der Fialka, als auch der Lochstreifen genutzt werden. Alternativ konnten die chiffrierten Daten auch akustisch übertragen.

Die Fialka war mindestens bis 1978 noch für Informationen mit Geheimhaltungsgrad „Geheime Verschlußsache (GVS)“ zugelassen[6].

2.3.12 Chiffrierung und Dechiffrierung in der DDR

Der Tagesschlüssel unterschied sich je nach Walzentyp. Bei den fixierten Walzen bestand der Tagesschlüssel aus der Lochkarte und einem Zettel mit zwei mal zwei Buchstabengruppen zu je 5 kyrillischen Buchstaben. Die ersten beiden Gruppen gaben an, in wel-

[6] Nur Geheime Kommandosache (GKdos) unterliegt einer noch höheren Geheimhaltung

cher Reihenfolge die Walzen einzulegen sind. Die anderen beiden Gruppen bestimmen die Startposition der Walzen.

Für PROTON-2 bestand der Tagesschlüssel aus der Lochkarte und einem Zettel (vergleiche Beispielabbildung 2.7) mit 5 Zeilen zu je 10 kyrillischen Buchstaben oder Zahlen. Die erste Zeile gibt wieder die Reihenfolge der Walzen an. Die nächste Zeile ist die Ringstellung (welcher Buchstabe an einer kleinen roten Markierung positioniert wird) und die folgende bestimmt, welche Verdrahtungsscheibe in welche Walze gesteckt wird. Die vorletzte Zeile besagt mit welcher Seite die Verdrahtungsscheibe eingesetzt wird, während die letzte Zeile die Position der Scheibe innerhalb der Walze bestimmt. Eine Zahl im rechten oberen Rand bezeichnet den Tag zu dem der Tagesschlüssel gilt. Als Startposition der Walzen wird für jede Walze gleich A gewählt.

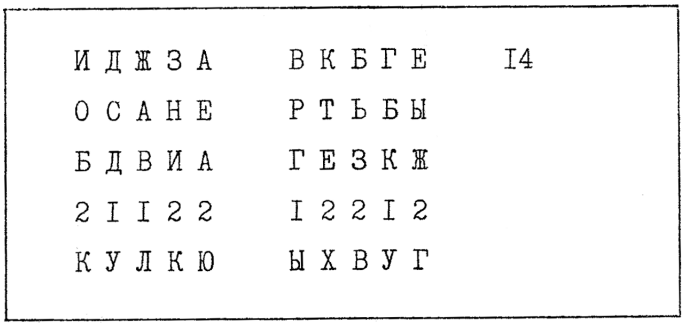
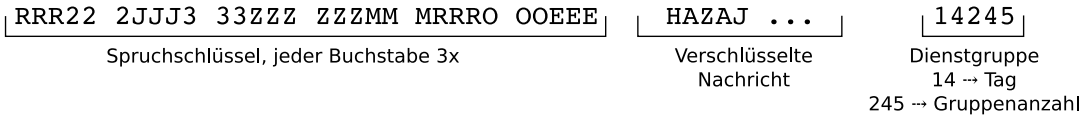


Abbildung 2.7: Beispiel eines Tagesschlüssel für PROTON-2-Walzen

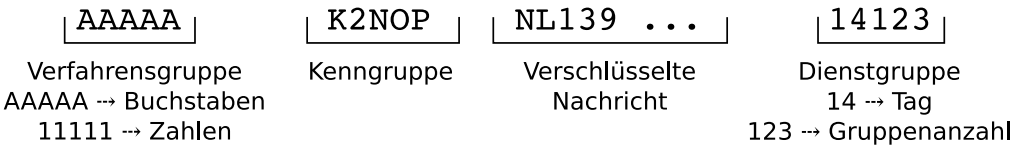
Die Art der Nachrichten wurden unterschieden zwischen *allgemein*, *individuell* und *zirkular*. Je nach Verkehrsart unterschied sich die Einstellung des Spruchschlüssels. Beim allgemeinen Verkehr kann jeder Teilnehmer mit jedem anderen kommunizieren. Jeder Teilnehmer verfügt über die gleichen Tagesschlüssel. Das Verfahren zum Einstellen des Spruchschlüssels des allgemeinen Verkehrs beginnt damit, dass man 10 kyrillische Buchstaben aus einem Kenngruppenheft mit dem eingestellten Tagesschlüssel verschlüsselte. Die Buchstaben wurden dann aus dem Heft gestrichen und mit Datum signiert, um sicherzustellen, dass jeder Spruchschlüssel nur einmal verwendet wird. Die verschlüsselten Buchstaben bilden die neuen Startpositionen und somit den Spruchschlüssel. Es wird folgend der eigentlich zu übermittelnde Text chiffriert. Ein Zähler an der Maschine zählt jede Fünfergruppe an Buchstaben. Sollte der letzte Buchstabe keine Fünfergruppe vervollständigen, wird solange die Leertaste gedrückt, bis dies der Fall ist[7]. Als zu übermittelnder Text ergeben sich zuerst der (unverschlüsselte) Spruchschlüssel, gefolgt vom Geheimtext

[7] Diese Anweisung kann von einem Angreifer als Crib genutzt werden, schließlich besteht eine Wahrscheinlichkeit von ⅘, dass der letzte Buchstabe ein Leerzeichen ist. Weiterhin besteht eine Wahrscheinlichkeit von ⅗, dass das vorletzte Buchstabe ein Leerzeichen ist, usw.

und zuletzt die Dienstgruppe, die aus fünf Ziffern besteht. Die ersten beiden Ziffern sind der Tag im Monat, zu dem der Tagesschlüssel gewählt wurde. Die letzten 3 Ziffern geben die Anzahl Fünfergruppen der kompletten, zu übermittelnden, Nachricht (ohne jedoch die Dienstgruppe) an. Der Aufbau einer Nachricht des allgemeinen Verkehrs ist demnach wie folgt:



Beim individuellen und zirkularen Verkehr unterschied sich das Verfahren geringfügig. Mit individuellem Verkehr ist gemeint, dass nur zwei Teilnehmer im Besitz der gleichen Schlüsselunterlagen sind. Im Gegensatz dazu sind beim zirkularen Verkehr auch mehr als zwei Teilnehmer möglich, jedoch chiffriert nur ein Teilnehmer, während alle anderen nur dechiffrieren dürfen. Während beim allgemeinen Verkehr der Spruchschlüssel Teil der Nachricht ist, werden bei den anderen beiden Verkehrsarten aus einem Kenngruppenheft von oben nach unten Fünfergruppen von Buchstaben entnommen. Eine Gruppe aus der dritten Zeile bedeutet, dass der dritte Spruchschlüssel aus einer Tagesschlüsseltabelle gewählt wird. Sobald eine Gruppe, und somit der Spruchschlüssel, ausgewählt wurde, mussten sie aus den Heften gestrichen werden, um sicher zu stellen, dass sie nicht noch einmal verwendet werden. Die Aufbau der Nachricht ergibt sich entsprechend:



2.4 M-130 „Koralle“

Eine weitere Rotor-Schlüsselmaschine, die in der DDR genutzt wurde, ist die M-130, auch *Koralle*, oder *Wetterkoralle* genannt. Die M-130 wurde in Russland entwickelt und dort ab 1965 in den Betrieb eingeführt. Im Unterschied zu den anderen beiden vorgestellten Geräten, unterstützt die M-130 nur die Chiffrierung von Zahlen. Die Nutzung der Maschine beschränkte sich auf das Chiffrieren von Wetterberichten, denn diese hatten durchaus militärische Relevanz, wie zum Beispiel im Falle eines Krieges, bei dem korrekte und unverfälschte Daten über die Durchführung eine Einsatzes entschieden. Der Austausch der Daten fand sowohl innerhalb eines Landes als auch zwischen den Staaten des Warschauer Paktes statt.

Die Chiffrierung der Wetterdaten waren auch deshalb wichtig, da die Wetterberichte womöglich über einen anderen verschlüsselten Kanal, wie mit der Fialka, weitergeleitet

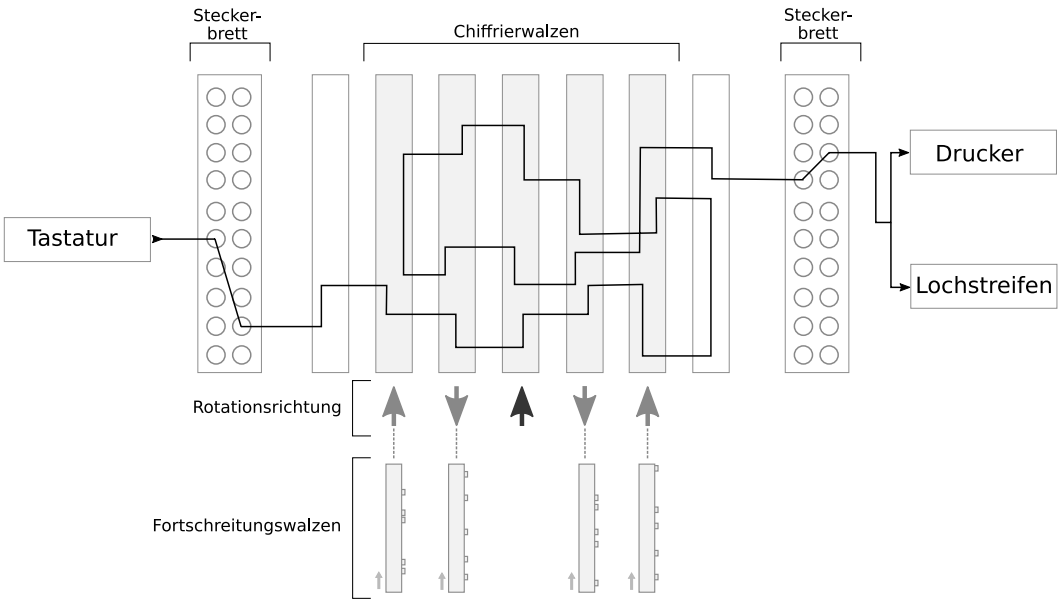


Abbildung 2.8: Schema der Verschlüsselung der M-130 mit Beispielpfad

wurden. Kennt der Gegner einen längeren Klartext mit dem dazugehörigen Chiffretext, vereinfacht dies die Analyse des verwendeten Schlüssels und kann somit wichtige Hinweise auf den Tagesschlüssel liefern, wodurch andere Nachrichten leichter entschlüsselt werden können.

2.4.1 Funktionsweise

Die Grundlage der M-130 bildet ein Fernschreiber, der um eine Chiffriereinheit erweitert wurde. Als Eingabetasten befinden sich die Ziffern `0` bis `9`, sowie `X`, Bindestrich und ein Zeilenumbruch an der Vorderseite der Maschine. Nur die Zahlen werden für die Chiffrierung genutzt, während die anderen Zeichen der Formatierung dienen. Als Ausgabe kann sowohl auf Papier gedruckt werden, als auch auf Lochstreifen gestanzt, wobei die Maschine so eingestellt werden kann, dass sie nur eine der beiden Ausgaben nutzt. Auf das Papier werden, genau wie bei einer Schreibmaschine, mit Hämmer die auszugebenden Zeichen gedruckt. Aus diesem Grund besitzt die Maschine eine Taste für den Zeilenumbruch, die sonst jedoch keinen Einfluss auf die Verschlüsselung hat.

Die 10 Ziffern bilden die möglichen Eingabewerte der Chiffriereinheit. Sie besteht aus zwei Steckerbrettern, fünf Walzen für die Verschlüsselung, vier Walzen für die Fortschreitung sowie zwei Kontaktstellen am Eingang und Ausgang der Einheit. Im Unterschied zur Enigma und Fialka entspricht die Anzahl der Kontakte einer Walze nicht der Anzahl der möglichen Eingabeparameter. Jede Walze der M-130 hat 30 Ein- und Ausgänge, also drei mal so viel wie eigentlich benötigt. Anstatt einer dedizierten Umkehrwalze wird das

elektrische Signal drei mal durch die Chiffrierwalzen geleitet, wodurch im Gegensatz zu den anderen hier vorgestellten Geräten, das Signal am anderen Ende die Einheit verlässt, und nicht nur einmal reflektiert wird.

Abbildung 2.8 stellt der Verlauf der elektrischen Stroms einer zu verschlüsselnden Ziffer dar. Eine Taste wird gedrückt. Zunächst findet eine Substitution über das Steckerbrett statt, wobei eine Ziffer auch mit sich selbst gesteckt werden kann, und somit keine Substitution stattfindet. Über die Eingangswalze durchläuft der Strom die fünf Chiffrierwalzen bis zur Ausgangswalze, wird dort aber reflektiert und nochmals durch die Walzen geleitet. Zurück an der Eingangswalze findet eine weitere Reflektion statt, die Chiffrierwalzen werden erneut durchlaufen bis hin, über die Ausgangswalze, zu einem weiteren Steckerbrett, das sich für eine erneute Substitution verantwortlich zeigt. Schlussendlich wird der Buchstabe auf Papier gedruckt und/oder auf einem Lochstreifen gestanzt.

Durch den Aufbau ist ein Umschalter zwischen Ver- und Entschlüsselung nötig, denn die Permutationen sind nicht reziprok. Mit gleichen Einstellungen wird die Eingabe einer verschlüsselten Ziffern nicht die Ursprungsziffer ausgeben. Der Umschalter sorgt dafuer, dass die Chiffriereinheit beim Entschlüsseln gewissermaßen von „rechts nach links“, und somit umgekehrt zur Verschlüsselung, arbeitet.

Aus Unterlagen geht hervor, dass es drei unterschiedliche Schlüssel gab, die vor der Nutzung als perforierte Papierblöcke ausgeliefert wurden. Der erste Schlüssel[8] betraf die Anordnung der Kabel auf den Steckbrettern. Wie oft dieser Schlüssel gewechselt wurde, ist nicht bekannt. Der zweite Schlüssel war der Wochenschlüssel und betrifft die interne Verkabelung der Walzen. Auf die Walzen wird im nächsten Abschnitt näher eingegangen. Dieser Schlüssel wurde, wie der Name schon aussagt, im Wochenrhythmus geändert. Der dritte Schlüssel, der Tagesschlüssel, beinhaltete die Startpositionen der Walzen und wurde täglich geändert.

Es ist derzeit nicht bekannt, zu welchem Schlüssel die Reihenfolge der Walzen innerhalb der Maschine gehörte, und somit, wie oft sie geändert wurde.

2.4.2 Walzen

Die Walzen ähneln denen der M-125 deutlich, schließlich sind sie in einer ähnlichen Zeit entstanden. Anstatt der kyrillischen Buchstaben sind die Zahlen von 0 bis 29 aufgedruckt und auf die blockierenden Stifte direkt an der Walze wurde verzichtet. Für das unregelmäßige Fortschreiten sorgt ein anderen Mechanismus, der im nächsten Abschnitt erklärt wird.

[8] In der DDR wurde dieser Schlüssel Dekadenschlüssel genannt, in Anspielung auf die 10 unterschiedlichen Stecker-Kabel.

Die innere Verdrahtung einer Walze ist nicht statisch und kann vom Nutzer geändert werden. Wird eine Walze geöffnet, finden sich im inneren 30 Kabel, bei denen ein Ende fixiert ist und das andere Ende in eine von 30 Positionen gesteckt werden kann. Daraus ergeben sich zwar eine Vielzahl unterschiedlicher Einstellungsmöglichkeiten, jedoch war eine Neuverdrahtung sehr fehleranfällig. In Erinnerungen von Mitarbeitern des Meteorologischen Dienst der Luftstreitkräfte/Luftverteidigung heißt es:

> Je nach aktuellem Schlüssel ergab sich eine Lage der Kabel innerhalb der Schlüsselscheibe, die 'völlig' ungeordnet war und damit mechanische Probleme auftraten, die Scheibe wieder zu schließen. Unabhängig davon berichten die handelnden Personen von größerem Stress beim Verschlüsseln. War die Gegenkontrolle negativ, mussten i.d.R. eine oder mehrere der fünf Schlüsselscheiben falsch kodiert sein oder es wurde beim Verschließen ein Verbindungsdraht eingeklemmt und dabei zerstört. Welche der Scheiben es betraf, war nicht definierbar. Daher musste alles kontrolliert sowie berichtigt bzw. der Draht zusammengelötet werden und dies alles normalerweise unter großem Zeitdruck. [7]

2.4.3 Fortschreitung der Walzen

Eigens für das unregelmäßige Fortschreiten der Chiffrierwalzen sind vier Fortschreitungswalzen zuständig, die darüber bestimmen, wann eine Walze sich, nach einem Tastendruck, um eine Position weiterbewegt. Das Grundprinzip ist dabei der Fialka ähnlich, insofern dass prinzipiell jede Walze mit jedem Tastendruck sich weiterdreht, solange sie nicht von einem blockierenden Stift davon abgehalten wird. Diese blockierenden Stifte befinden sich an den Seiten von je zwei Walzen zur linken Seite der Chiffrierwalzen, und zwei Walzen zur rechten.

Während die mittlere Chiffrierwalze sich mit jedem Tastendruck weiterbewegt, hängt der Fortlauf der äußeren Chiffrierwalzen von jeweils einer Fortschreitungswalze ab. Jede Fortschreitungswalze bewegt sich um einen Schritt mit jedem Tastendruck. Befindet sich in der aktuellen Position ein Stift, dann blockiert ein Mechanismus das Fortschreiten der ihr zugehörigen Chiffrierwalze. Abbilung 2.8 zeigt die Zugehörigkeit der Fortschreitungswalzen zu den Chiffrierwalzen. Jeweils benachbarte Walzen bewegen sich gegensätzlich zueinander, genau wie bei der Fialka.

Jede Fortschreitungswalze hat eine andere Anzahl und andere Anordnung der blockierenden Stifte, um die Länge bis zur Wiederholung des gleichen Blockiermusters zu maximieren.

2.4.4 Lochstreifen

Als maschinelle Ein- und Ausgabe stehen ein Lochstreifenleser und Lochstreifenlocher zur Verfügung. Obwohl die M-130 auf einem Fernschreibegerät basiert, hat sie keine direkte Möglichkeit der Fernübertragung zu bieten. Somit wurde der verschlüsselte Text mit Hilfe des Lochstreifens weitergegeben und mit geeigneten Geräten übertragen.

Die Kodierung des Lochstreifens ist derzeit nicht geklärt.

2.4.5 Aufbereitung der Daten

Die Wetterdaten wurden mittels unterschiedlicher standardisierter Verfahren in Zahlenform umgewandelt. Für allgemeine Wettermeldung diente der Zahlenschlüssel SYNOP, der in Fünfgergruppen unterteilt in festem Format Auskunft über Niederschlag, Bewölkung, Luftdruck und Temperatur gibt. Der Zahlenschlüssel PILOT beschreibt Windprofile in höherer Luft, während TEMP den Druck, Temperatur und Feuchtigkeit höherer Luftschichten beschreibt.

Der Anfang einer Übertragung beinhaltete einen Zahlencode der Auskunft darüber gab, welcher Zahlenschlüssel folgt. So sollte zum Beispiel 11111 für SYNOP stehen und 99911 für den ersten Teil einer TEMP-Nachricht[21].

2.4.6 Kryptografische Sicherheit

Wie auch die M-125 kann die M-130 einen Buchstaben auf sich selbst abbilden, und vermeidet somit eine der größten Schwächen der Enigma. Außerdem wird das Steckerbrett nicht in Paaren vertauscht, sondern jeder Buchstabe für sich.

Der Schlüsselraum errechnet sich aus

- $2 \cdot 30!$ Möglichkeiten die Kabel der Steckerbretter zu setzen (Dekadenschlüssel),
- 30^5 Startpositionen der Walzen (Tagesschlüssel),
- $5!$ Walzenanordnungen,
- $(30!)^5$ Möglichkeiten der inneren Verdrahtungen aller Walzen,
- sowie 30^4 Startpositionen der Fortschreitungswalzen.

Daraus ergibt sich ein sehr großer Schlüsselraum von:

$$\begin{aligned} 10! \cdot 10! \cdot 30^5 \cdot 5! \cdot (30!)^5 \cdot 30^4 &\approx 4,08 \cdot 10^{190} \\ &\approx 2^{633,20} \approx 633\ Bit \end{aligned}$$

Es gilt zu bedenken, dass mindestens die innere Verdrahtung der Walzen nur wöchentlich geändert wurde und somit einer Verminderung der Sicherheit entspricht.

Ob es einen Spruchschlüssel gegeben hat, ist derzeit nicht bekannt. Gerade bei den strukturierten Daten eines Wetterberichtes wäre der Verzicht eines solchen aber ein bedeutendes Problem.

In Erinnerungen von Mitarbeitern des Meteorologischen Dienst der Luftstreitkräfte/Luftverteidigung wird berichtet, dass die M-130 im Betrieb erheblichen Lärm verursachte, wodurch man sich gezwungen sah, die Schalldämpfung im Raum der M-130 zu verstärken, um sich nicht der Gefahr einer Seitenkanalattacke auszusetzen[7].

Es ist nicht bekannt, ob es je einen erfolgreichen Angriff auf verschlüsselte Botschaften der M-130 gegeben hat. Zu der Sicherheit des Verschlüsselungsalgorithmus der M-130 gibt es bisher keine wissenschaftlichen Arbeiten.

2.4.7 Nutzung in der DDR

Eine erste Unterweisung in der Nutzung der M-130 erhielt der Meteorologischen Dienst der Luftstreitkräfte/Luftverteidigung der DDR in Moskau 1966[7]. In einem Dokument von Generaloberst Streletz geht hervor, dass die M-130 noch 1982 in Gebrauch war, wobei die Einführung eines Nachfolgegeräts bis 1986 angekündigt wurde[21]. Zu dieser Einführung soll es jedoch nie gekommen sein. In der Hauptnachrichtenzentrale (HptNZ) der NVA soll das Gerät noch bis 1990 verwendet worden sein, in der Hauptnachrichtenzentrale 4 (HNZ-4) zumindest noch bis 1983[6].

Es fanden regelmäßig Übungen zwischen den Teilnehmern des Warschauer Vertrages statt, in der jeder Teilnehmer einen Sendetermin und eine Frequenz zugeteilt bekam. Die empfangenden Wetternachrichten wurden dechiffriert und sollten laut Plan nach 3-5 Stunden vorliegen, jedoch dauerte die tatsächliche Aufbereitung deutlich länger. Fehlerhaft empfangende oder fehlende Lochstreifen wurden mitunter von anderen partizipierenden Flugwetterwarten angefordert[7].

Abbildungsverzeichnis

Literatur

[1] Eugen Antal und Viliam Hromada. "A New Stream Cipher Based on Fialka M-125". In: *Tatra Mountains Mathematical Publications* 57.1 (2013), S. 101–118.

[2] Eugen Antal und Pavol Zajac. "Key Space and Period of Fialka M-125 Cipher Machine". In: *Cryptologia* 39.2 (2015), S. 126–144. DOI: 10.1080/01611194.2014.915264. URL: http://dx.doi.org/10.1080/01611194.2014.915264.

[3] Jan Bury. "From the Archives: Inside a Cold War Crypto Cell. Polish Cipher Bureau in the 1980s". In: *Cryptologia* 32.4 (2008), S. 351–367. URL: http://dx.doi.org/10.1080/01611190802319036.

[4] CIA. *Clandestine Services History. The Berlin Tunnel Operation 1952 - 1956*. 24. Juni 1968. URL: https://fas.org/irp/cia/product/tunnel-200702.pdf (besucht am 10. 11. 2015).

[5] Jörg Drobick. *Der SAS- und Chiffrierdienst (SCD). FIALKA M-125 MN oder 3MN oder 3MP*. URL: http://scz.bplaced.net/m125.html (besucht am 10. 11. 2015).

[6] Jörg Drobick. *Der SAS- und Chiffrierdienst (SCD). Wetterchiffriergerät M-130 KORALLE*. URL: http://scz.bplaced.net/m130.html (besucht am 21. 01. 2016).

[7] Frank Wieczorek Frank Kammler. *Verschlüsselung meteorologischer Daten - Zentrale Flugwetterwarte · Meteorologischer Dienst der LSK / LV*. URL: http://zfww.de/HW/wiz_m130.htm (besucht am 15. 01. 2016).

[8] David Kahn. "SOVIET COMINT IN THE COLD WAR". In: *Cryptologia* 22.1 (1998), S. 1–24. DOI: 10.1080/0161-119891886731. URL: http://dx.doi.org/10.1080/0161-119891886731.

[9] H.-J. Kaiser. *Technikkatalog - Morse-Code-Geber P-590A*. URL: http://www.rwd-mb3.de/ntechnik/pages/p590a.htm (besucht am 05. 02. 2016).

[10] Karl Maria Michael de Leeuw und Jan Bergstra. *The history of information security: a comprehensive handbook*. Elsevier, 2007.

[11] NSA. *Cryptologic Almanac 50th Anniversary Series. The Last Days of the Enigma*. 20. Feb. 2007. URL: https://www.nsa.gov/public_info/_files/cryptologic_almanac_50th/The_Last_Days_of_the_Enigma.pdf (besucht am 10. 11. 2015).

[12] NSA. *UNITED STATES CRYPTOLOGIC HISTORY Special Series Number 4. Operation Regal: The Berlin Tunnel*. 1998. URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/on-the-front-lines-of-the-cold-war-documents-on-the-intelligence-war-in-berlin-1946-to-1961/art-7.html (besucht am 10. 11. 2015).

[13] Fregattenkapitän der Reserve Riebe. *Errinerungen über meine langjährige Tätigkeit im Chiffrierwesen der DDR seit 1951*. BStU, MfS, Abt XI BVfS Rostock, Nr. 000199. URL: http://scz.bplaced.net/abriss-ddr.html (besucht am 04. 02. 2016).

[14] Paul Reuvers und Marc Simons. *Fialka on cryptomuseum*. URL: http://cryptomuseum.com/crypto/fialka/m125/index.htm (besucht am 10. 11. 2015).

[15] Paul Reuvers und Marc Simons. *Fialka on cryptomuseum*. URL: http://cryptomuseum.com/crypto/ussr/m130/index.htm (besucht am 21. 01. 2016).

[16] Paul Reuvers und Marc Simons. *Tempest PSU*. URL: http://www.cryptomuseum.com/crypto/fialka/psu/tempest.htm (besucht am 22. 01. 2016).

[17] K Schmeh. "Codeknacker gegen Codemacher". In: *Die faszinierende Geschichte der Verschlüsselung* 2 (2008).

[18] Oberstleutnant Schürmann. *Lageeinschätzung des ZCO 1960*. BStU, MfS, HA II Nr. 033616. URL: http://scz.bplaced.net/mfs_zco.html#j1960 (besucht am 23. 01. 2016).

[19] Karel Šklíba. "Z dějin československé kryptografie, část V., Československé šifrovací stroje z období 1955 – 1960." In: *Crypto-World* 2008.1 (Jan. 2008), S. 17. URL: http://crypto-world.info/casop10/crypto01_08.pdf.

[20] Donald P. Steury. *On the Front Lines of the Cold War: Documents on the Intelligence War in Berlin, 1946 to 1961. V: The Berlin Tunnel*. 16. März 2007. URL: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/on-the-front-lines-of-the-cold-war-documents-on-the-intelligence-war-in-berlin-1946-to-1961/art-7.html (besucht am 10. 11. 2015).

[21] Generaloberst Strelitz. *Austausch chiffrierter metereologischer Informationen*. BStU, MfS, Abt XI Nr. 000162. URL: http://scz.bplaced.net/m130.html#streletz (besucht am 22. 01. 2016).

[22] Nationale Volksarmee. *Gebrauchsanweisung M-125. DV A 040/1/321*. URL: http://scz.bplaced.net/dv040-1-321.html (besucht am 22. 01. 2016).

[23] Nationale Volksarmee. *Gebrauchsanweisung M-125. DV A 040/1/321.* URL: `http://scz.bplaced.net/dv040-1-321.html` (besucht am 22. 01. 2016).

[24] Leutnant Weder. *Arbeitsanweisung über die Handhabung des Fernschreibschlüssel Dora (FSD).* BStU, MfS, Abt XI Nr. 000753. URL: `http://scz.bplaced.net/m.html#dora` (besucht am 04. 02. 2016).