Dennis Gottschalk

Die ENIGMA

Schlüsselverfahren *ist das Gesetz, nach dem verschlüsselt wird*
Schlüssel *bezeichnet die wechselnden Unterlagen, nach denen bei den einzelnen Verfahren das Schlüsselmittel zum Schlüssel vorbereitet wird.*
Schlüsseltafel *ist die Zusammenstellung einzelner Schlüssel für einen längeren Zeitraum.*
Schlüsselmittel *ist der zum Schlüssel erforderliche Behelf, z.B. Schlüsselmaschine (auch als Chiffriermaschine bezeichnet).*
Kenngruppe *dient zur Kennzeichnung des in einem Spruch verwendeten Schlüssels.*

- *Aus der geheimen „Schlüsselanleitung zur Schlüsselmaschine Enigma“, Berlin 1940*

Die Erfinder

Die erste technische Realisierung des Walzenprinzips gelang 1915 dem Amerikaner Eduard Hugo Hebern. Seine Technik war verhältnismäßig simpel: Er verdrahtete einfach 2 elektrische Schreibmaschinen, die Tasten der einen mit den Hebeln der anderen. So konnten verschiedene monoalphabetische Verschlüsselungen erzeugt werden.
1917 entdeckte er bereits das Prinzip der Walze.
Mit dieser sind 26 verschiedene monoalphabetische Verschlüsselungen möglich, da sie 26 unterschiedliche Positionen gegenüber den festen Schalter- und Glühlampenkontakten einnehme kann.
Ordnet man nun jedoch 2 Walzen nebeneinander an, der Strom fließt nun also von der rechten Seite der ersten Walze durch die Verdrahtung zur linken Seite, wird anschließend zum rechten Kontakt der zweiten Walze geleitet. (**Abbildung 1**)
Werden die beiden Walzen nicht bewegt, kommt nur eine monoalphabetische Verschlüsselung zustande. Da man jedoch jede der Walzen bei unserem Alphabet mit 26 Buchstaben gegenüber der anderen Walze um 25 Stellungen drehen kann und zwei Walzen als Ganzes wiederum auf 26 Arten miteinander verbunden werden können, ergeben sich also 26x26 = 676 verschiedene Stellungen.
Dreht man die erste Walze jedoch nach jedem Buchstaben um einen Schritt und die zweite Walze jeweils nach einem Umlauf der ersten um eine Stellung, so wiederholen sich die Verschlüsselungen in einem Abstand von 676 Zeichen, was einem Vignere-Prinzip mit einem Schlüsselwort von 676 Zeichen Länge entspricht.
Um jedoch die versendeten Nachrichten entschlüsseln zu können, muss nicht unbedingt dieses „Lösungswort“ bekannt sein. Wenn jede Nachricht mit der gleichen Ausgangsstellung der Walzen beginnt, so werden jeweils die ersten Buchstaben aller Nachrichten (wie auch die zweiten und dritten) auf die gleiche Weise monoalphabetisch verschlüsselt. Dieser Verschlüsselungstyp hat jedoch den großen Nachteil, dass mithilfe einer Häufigkeitsanalyse der Geheimbuchstaben die Nachricht entschlüsseln kann.
Wird hingegen die Anfangsstellung der Walzen und die Positionen der festen Kontakte des Gehäuses immer wieder variiert (möglicherweise nach jedem Wort), so versagt dieses Verfahren.
Heberns erste Verschlüsselungsmaschine besaß 5 Walzen. Es gab also:
26x26x26x26x26=11.881.376 verschiedene Einstellungen für das Räderwerk.
(**Abbildung 2**)
So genial diese Erfindung auch war, reich wurde Hebern nicht mit ihr.
1921 gründete er in den USA eine Firma für Schlüsselmaschinen. Er verkaufte Aktien und erhoffte sich so eine Steigerung seines Eigenkapitals. Die US-Marine interessierte sich zwar für diese neuartige Maschine, kaufte jedoch nur 2 Exemplare; auch das britische und das italienische Heer, sowie eine Privatfirma erwarben insgesamt nur 9 Stück und das, obwohl die Preise nur bei einigen hundert Dollar lagen. Daraufhin fielen auch die Kurse der Aktien und seine Firma musste Konkurs anmelden.
Während des 2. Weltkrieges und auch noch zur Zeit des kalten Krieges verwendeten die Amerikaner Chiffriermaschinen, die nach Heberns Prinzip funktionierten.
Nach einem langen gerichtlichen Prozess wurde Hebern dann mit einer Summe von 30.000 US-Dollar „entschädigt“, die jedoch nur ein möglichst schnelles Ende des Prozesses

hervorrufen sollten, damit keine kryptologischen Geheimnisse an die Öffentlichkeit kommen konnten. Dies geschah erst später, als Hebern schon 6 Jahre tot war, also im Jahre 1946.
Hebern war zu seiner Zeit nicht der einzige Erfinder einer Chiffriermaschine. In Holland meldete Hugo Alexander Koch 1919 ein Patent für seine „Geheimschriftmaschine“ an.
1927 verkaufte er diese Patentrechte dann an den deutschen Ingenieur Artur Scherbius.
Dieser wiederum hatte schon 1918 eine Verschlüsselungsmaschine, die mit einem Rotorprinzip arbeitet, in Deutschland zum Patent angemeldet. Er ließ sich jedoch nicht nur seine Ideen patentieren, sondern baute die erfundenen Maschinen auch selbst.
Einzelheiten zu seiner Maschine gehen aus der Patentanmeldung hervor, die er in den USA einreichte. **(Abbildung 3)**
Seine Erfindung wies jedoch eine Besonderheit auf: Sie besaß eine *Umkehrwalze*.
Bei der Scherbiusschen Maschine dreht sich nach jeweils einem Buchstaben ein Rotor um eine Stellung weiter und nach jedem Umlauf der Nächste. Über Getriebe mit unterschiedlichen Übersetzungen werden auch andere Walzen um eine bestimmte Anzahl von Schritten weiterbewegt. (**Abbildung 4**)
Der Vorteil der Umkehrwalze besteht darin, dass mit der gleichen Maschine sowohl chiffrieren, als auch dechiffrieren kann. Zum Beispiel tippt man bei einer bestimmten Anfangsstellung der Walzen der Reihe nach die Buchstaben des Klartextes ein („adac“).
Während dieses Vorgangs leuchten zum Beispiel an der Maschine die Lampen DCBA auf.
Wird nun bei derselben Anfangsstellung der Walzen („dcba“)eingegeben, so leuchten an der Maschine die Buchstaben ADAC auf. Dies liegt daran, dass beim Entschlüsseln die Walzen bei jedem eingegebenen Buchstaben dieselbe relative Position zueinander haben, die sie beim Verschlüsseln hatten. Somit sind bei einer solchen Schaltung niemals Klar- und Geheimtextbuchstabe identisch.
Um mit dieser Maschine Geheimnachrichten entschlüsseln zu können, müssen also die Verdrahtung der einzelnen Walzen, die Reihenfolge der einzelnen Maschinen, die Verdrahtung der Umkehrwalze und die Regeln, nach denen die Walzen gegeneinander gedreht werden, bekannt sein.
Scherbius dachte sich aus Marketinggründen einen Namen für seine Maschine aus: ENIGMA. Das griechische Wort für „Rätsel“.
Er baute mehrere voneinander abweihende Modelle und gründete 1923 eine AG, die im gleichen Jahr noch in Berlin mit der Produktion der Maschinen begann.
Wie auch bei Hebern, blieb der wirtschaftliche Erfolg jedoch trotz großer Bemühungen und mehrer Präsentationen auf Kongressen aus.
Die Reichswehr zeigte jedoch Interesse an der Maschine und kurze Zeit später wurde diese auch nicht mehr für die Öffentlichkeit, sondern ausschließlich für das Militär produziert.
1934, Scherbius kam vor 3 Jahren ums Leben, erlebte die Enigma einen großen Aufschwung, als Hitler an die Macht kam und aufzurüsten begann.

Bezüglich des Rotorprinzips gab es jedoch noch einen weiteren Erfinder.
1919, 3 Tage nachdem Koch in Holland sein Patent anmeldete, beantragte ein Schwede namens Arvid Gerhard Damm, ein „Technik-Freak“, auch ein Patent.
Nach Ausbruch des 1. Weltkrieges meldete Damm zusammen mit einem englischen Textilfabrikanten 3 Patente für eine Chiffriermaschine in Deutschland an. Später gründete er eine Firma, wofür er Geld benötigte. Es fanden sich jedoch schnell Investoren, unter anderem den Neffen von Alfred Nobel, den Erfinder des Dynamits, welcher einen weiteren Geldgeber heranzog, ein Mann namens Hagelin.
Damm konstruierte wiederum mehrere Maschinen und warb mit ihnen. Auch hier blieb der Erfolg jedoch aus.
Dann kam Boris Caesar Wilhelm Hagelin in die Firma, der Sohn des erwähnten Teilhebers.

Dieser war Ingenieur mit Berufserfahrung und nahm mehrere Vereinfachungen an dem Damm´schen System vor, gab ihm eine Tastatur und versah sie mit Lampen ähnlich dem Hebernschen Modell.
1929 gelang es ihm eine größere Menge an Maschinen zu verkaufen. Als 1927 Damm starb, übernahm Hagelin die Firma und nahm weiterhin Verbesserungen vor. 1934 wurde dann die Lampen durch einen Drucker ersetzt, da für die Übersetzung immer eine zweite Person notwendig war.
Das französische Heer interessierte sich nun für die Chiffriermaschine und fragte, ob es möglich sein, ein Exemplar zu konstruieren, welches in eine Aktentasche passte.
Dies gelang Hagelin dann auch, sie war kleiner als ein damals üblicher Telefonapparat, woraufhin er 5000 Exemplare an die Franzosen verkaufte.
Als nun 1940 die Deutschen in Norwegen einmarschierten, sie hatten bereits Frankreich, Holland und Belgien erobert, fürchtete Hagelin, dass Schweden auch nicht mehr lange sicher sei und versuchte sich in die USA abzusetzen. Da jedoch von Schweden aus keine Schiffe mehr in diese Richtung fuhren, planten die Hagelins, sich nach Genua zu begeben und von dort aus weiter in die USA zu flüchten.
Innerhalb von 3 Tagen reisten sie mitten durch Hitler-Deutschland, die Pläne für die Maschine im Gepäck. In New York angekommen, konnte er noch 50 Maschinen von Schweden in die USA einführen und begann sofort mit der Produktion.
Der Vorteil seiner Maschine lag darin, dass sie 5 Walzen besaß, die sich in unregelmäßiger Art gegeneinander drehten und sich somit die Verschlüsselung erst nach ca. 100 Millionen Buchstaben wiederholte.
Das war ein Grund dafür, weshalb Hagelin während des Kalten Krieges 140.000 Maschinen verkaufte und somit Millionär wurde.
Ein Jahr vor Kriegsende kehrte Hagelin zurück nach Schweden und errichtete im südlichen Teil Stockholms eine Fabrik. Nach dem 2. Weltkrieg boomte das Geschäft weiterhin, da bei den Neuordnungen in den Nachkriegsjahren Staaten entstanden, die für ihre Kommunikation mit den Armeen und Botschaften massenweise Verschlüsselungsmaschinen benötigten.
Hagelin wusste jedoch, dass das schwedische Gesetz dem Staat erlaubt, sich Erfindungen, die der nationalen Sicherheit dienen, anzueignen.
Dieses Recht und die hohen Steuern bewogen Hagelin 1948 seine Entwicklungsabteilung in die Schweiz zu verlegen. Zehn Jahre später folgte der Rest des Unternehmens in die Schweiz, wo nun ca. 170 Mitarbeiter beschäftigt waren.
1959 starb Hagelin, der einzige Erfinder, der durch seine Erfindung an Reichtum kam.
Seine Firma, die Krypto AG, existiert heute immer noch in der Schweiz, hat Kunden in der ganzen Welt und produziert unter anderem Chiffriermaschinen für den Irak, den Iran und Libyen.

Der Nachteil der Umkehrwalze

Mit der Umkehrwalze in der Scherbiusschen Maschine hat man den Vorteil, dass man mit ihr ver- wie auch entschlüsseln kann, wodurch die Möglichkeiten der Verschlüsselung stark eingeschränkt wurden.
Jede Stellung der Walzen verbindet jeden Schalter mit je einer Glühlampe, die mit Buchstaben gekennzeichnet sind, was bedeutet, dass die Maschine jedem Buchstaben einen anderen zuordnet. Wir haben eine Substitution, eine Verwürfelung oder Permutation des Alphabets. Sie benutzt nur Permutationen, die, zweimal auf das Alphabet angewandt, die ursprüngliche Ordnung wiederherstellen.
Nimmt man nun ein vollständiges Alphabet, die Anzahl der Verwürfelungen ist dann siebenundzwanzig Dezimalzahlen lang und die Maschine soll in derselben Stellung zweimal

auf einen Klartext angewandt, wieder diesen Klartext liefern, so hat die Anzahl der möglichen Verwürfelungen dreizehn Stellen. Sie verringert sich um viele Billionen Mal, was die Möglichkeiten drastisch eingeschränkt.
Eine weitere Konsequenz war, dass beim Eintippen eines Buchstabens niemals die Lampe des gleichen Buchstabens aufleuchtete. In dem Moment, wo der Schalter gedrückt wird, kann der Strom nicht gleichzeitig durch die dazugehörige Lampe gehen. Kein Klarbuchstabe kann in den gleichen Geheimbuchstaben übergehen.
Mavis Lever, Deutschstudentin an der Universität in London, fiel auf, dass ein Funkspruch der italienischen Marine den Buchstaben „L“ nicht enthielt. Miss. Lever hatte den Verdacht, dass es sich um ein Täuschungsmanöver der italienischen Verschlüssler, die in ihrer Enigma als Klartext eine Aneinanderreihung des Buchstabens l gewählt hatten, um die Alliierten in die Irre zu führen. Dadurch würde im Geheimtext nie ein l erscheinen, da l nie in l übergeht. Der Geheimtext verriet, was die Maschine in aufeinanderfolgenden Rotorstellungen aus dem l gemacht hatte, woraus Hinweise auf die Verdrahtung folgten und es gelang die Verschlüsselung aufzulösen.
Die Funksprüche der italienischen Kriegsschiffe ermöglichten es den Engländern, im März 1941 in der Schlacht vor dem Kap Matapan, an der Südspitze Korinths, drei italienische Kreutzer und zwei Zerstörer zu vernichten, ein Schlag, von dem sich die italienische Marine nicht mehr erholte.
Hagelins Maschinen, die von den Amerikanern benutzt wurden, besaßen keine Umkehrwalze.

Hitlers Enigma

Als 1933 Hitler an die Macht kam, wurde die Scherbiussche Chiffriermaschine noch verbessert und in mehreren Variationen hergestellt. Heer, Marine und diplomatischer Dienst benutzten verschiedene Typen. Die Enigma der Wehrmacht hatte drei Walzen, eine Umkehrwalze und ein Steckbrett. Wurde sie auf einen Klartext und danach auf den permutierten Text angewandt, kam wieder der ursprüngliche Klartext zu Vorschein.

Von der Marine wurde gegen Ende des Krieges eine Maschine mit vier Walzen benutzt.
Jede Walze hat im Innenteil auf beiden Seiten elektrische Kontakte, die miteinander verdrahtet sind. Um den Innenteil schließt sich ein Ring. An der Außenseite befinden sich die sechsundzwanzig Buchstaben des Alphabets. Ein oder zwei Kerben sorgen für die Übertragung der Bewegung auf die nächste Walze. Ring, Kerbe und Innenteil der Walze können gegeneinander verdreht werden. Dadurch ergaben sich für den Verschlüssler mehrere Möglichkeiten sein Gerät einzustellen. Um sicher zu sein, dass die empfangene Nachricht entschlüsselt werden konnte, musste er alle Schritte gemäß einem ihm vorliegenden Tagesschlüssel vornehmen, der die Auswahl der Walzen, die Reihenfolge, die Ringstellungen, die Anfangsstellungen der Walzen sowie die Verbindung am Steckerbrett enthielt.
Die Walzenlage wurde im Zweiten Weltkrieg alle acht Stunden verändert.

Im Februar 1942 führte die Marine eine weitere Walze ein, die mit dem griechischen Buchstaben Beta bezeichnet wurde und im Jargon als Griechenwalze bezeichnet wurde.
Trotz der kompliziert verschlüsselten Nachrichten war es möglich, bei gleichem Tagesschlüssel, diese zu entziffern. Daher war es nötig, die Einstellungen auch von Spruch zu Spruch zu modifizieren, wozu sich der Sender einer Nachricht einen Spruchschlüssel ausdenken musste, der aus drei Buchstaben bestand und unabhängig vom Tagesschlüssel die Ausgangsstellung der Walzen neu festlegte.

Das Geheimnis der Enigma wird gelüftet

Im Chiffrierbüro in Warschau arbeiteten drei junge Mathematiker daran, die Funksprüche des deutschen Heeres zu entschlüsseln. Das Büro hatte über einen schwedischen Kontaktmann eine zivile Enigma erworben. Die Walzen der Wehrmachts – Enigma waren jedoch anders verdrahtet.
1928 nahmen Zollbeamte heimlich und ohne Spuren zu hinterlassen Einsicht in ein Gepäckstück eines Beamten der Deutschen Botschaft, in dem sich eine nagelneue Enigma befand.
Die Schwächen der Enigma, bedingt durch die Umkehrwalze, ermöglichte den Polen, die deutschen Funksprüche mitzulesen.
Zusätzlich wählten die Verschlüssler aus Bequemlichkeit oft Spruchschlüssel mit drei gleichen Buchstaben, die auf der Enigma-Tastatur nebeneinander oder diagonal zueinander lagen. Dank dieses Leichtsinns hatten die drei polnischen Mathematiker an manchen Tagen keinen Mangel an Funksprüchen mit gleichem Spruchschlüssel.
1931 lieferte ein deutscher Spion Informationsmaterial über die Chiffrierung der Enigma an die französische Abwehr. Später folgte eine Kopie der deutschen Heeresdienstvorschrift über den Gebrauch der Enigma und darüber hinaus die Tagesschlüssel für September und Oktober des Jahres 1932. Im Dezember 1932 wurde das Material nach Warschau gesandt.
1934 hatten die Polen die Enigma-Verschlüsselung im Griff und konnten den Nachrichtenverkehr der Deutschen Wehrmacht und des deutschen Sicherheitsdienstes mitlesen. Trotzdem mussten mit jeder neuen Tageseinstellung der Enigma die polnischen Kryptologen von vorn beginnen. So entwarfen die drei Mathematiker ein Gerät, dessen Aufgabe es war, Charakteristika der durch verschiedene Rotorstellungen erzeugten Verwürfelungen des Alphabets zu erkennen. Die Maschine erhielt den Namen Zyklometer.
1938 wurde mit ihrer Hilfe ein Katalog angefertigt, der es schon nach wenigen aufgefangenen Meldungen ermöglichte den Tagesschlüssel zu finden.
1937 wurde von den Deutschen eine neue Umkehrwalze eingeführt, 1938 wurde die Zahl der zur Verfügung stehenden Walzen von drei auf fünf erhöht. Es gab sechzig Möglichkeiten aus fünf Walzen drei auszuwählen und in verschiedener Reihenfolge einzusetzen.
Das Zyklometer der polnischen Entschlüssler reichte nicht mehr aus und so wurde eine kompliziertere Maschine mit dem Namen bomba gebaut.
Am 25. Juli 1939 trafen sich Vertreter der polnischen, britischen und französischen Geheimdienste in Pyry bei Warschau. Die Polen übergaben den Alliierten die Ergebnisse ihrer Untersuchungen an der Enigma.
Kurz darauf erklärte Hitler den Polen den Krieg.

Die Leute von Bletchley Park

Im August 1939 gründete die englische Regierung nahe der Ortschaft Bletchley, etwa siebzig Kilometer nördlich von London, eine Chiffrierabteilung.
Turing konstruierte hier bombes, die leistungsfähiger waren als die polnischen bombas.
1940 gelang in Bletchley Park die erste Entschlüsslung.

Die Schlacht auf dem Atlantik

1941 begannen die deutschen U-Boote mit Enigmas zu arbeiten, die jetzt mit vier Rotoren- der Griechenwalze, einer dünneren Betawalze und einer dünneren und anders verdrahteten Umkehrwalze ausgestattet waren. Im Vergleich zur alten Version bot die vierte Walze der Enigma die sechsundzwanzigfache Anzahl möglicher Einstellungen.

Vom 1. Februar 1942 an wurde die neue Maschine im Funkverkehr auf den U-Booten im Atlantik verwendet. Ende Oktober 1942 gelang es vier englischen Zerstörern , das in Messina stationierte deutsch U-Boot aufzuspüren und zu zerstören, wobei es englischen Seeleuten gelang, geheimes Material, ein Signalbuch und einen Schlüssel für Wettermeldungen aus dem sinkenden Schiff zu bergen.
Dadurch gelang es den Wissenschaftlern in Bletchley Park am 13. Dezember 1942 die Funksprüche der deutschen U-Boote zu lesen.

Die Enigma im Deutschen Museum

In Deutschland wurden etwa zweihunderttausend Enigmas gebaut. Die Alliierten haben sie nach Kriegsende massenweise vernichtet. Heute sind Enigma-Maschinen ein Sammlerobjekt. Das Deutsche Museum in München besitzt in seiner Abteilung „Informatik und Automatik“ eine Marine-Enigma mit vier Walzen und zwei Heeresmaschinen mit drei Walzen.
Seit einigen Jahren besteht auch im englischen Bletttchley Park ein Museum, in dem die Enigma gezeigt und die Methoden und Maschinen zur Brechung ihres Codes gezeigt werden. Historiker und Verschlüsselungsexperten beschäftigen sich seit Jahren mit der historischen Rolle der Enigma.

Quelle: Rudolf Kippenhahn
Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte
Reinbek 1997; Internet

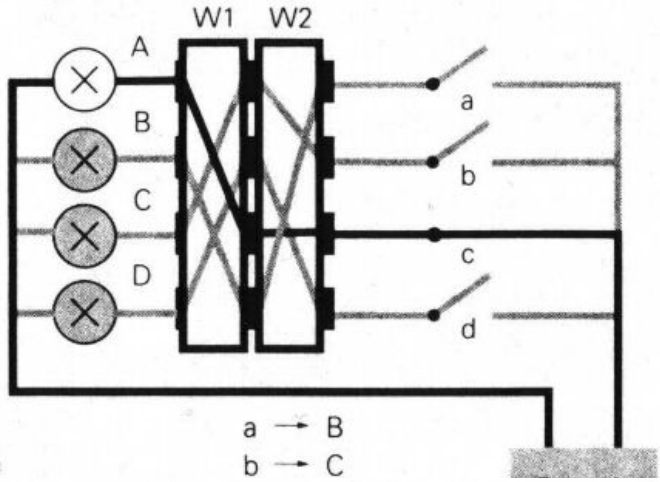

Abb. 1

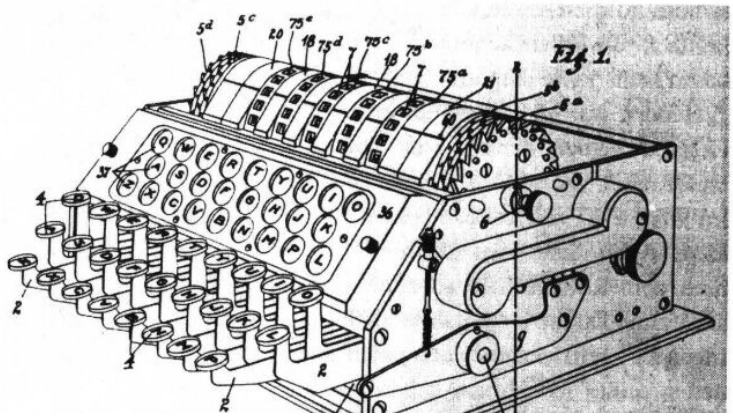

Abb. 2

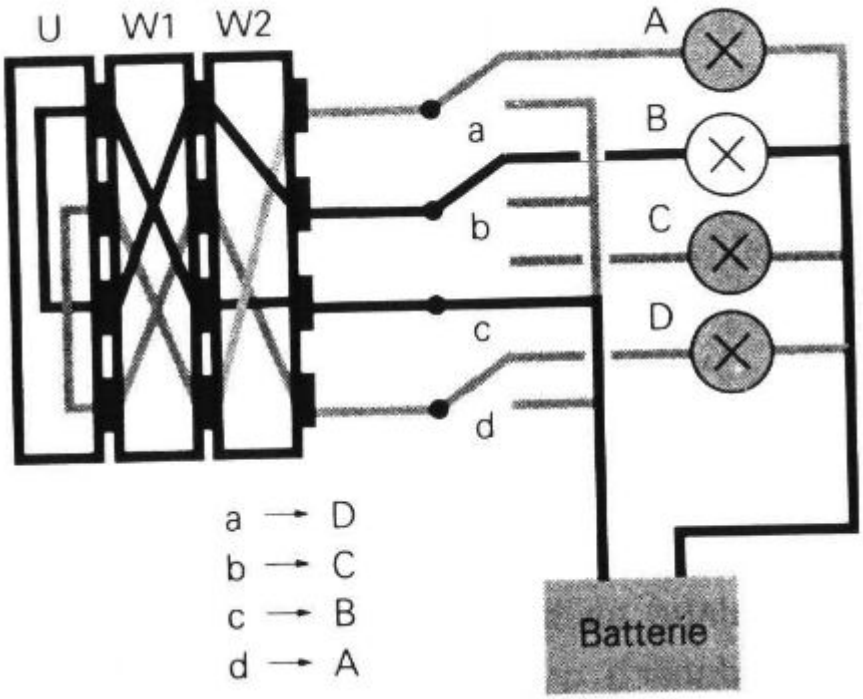

Abb. 3

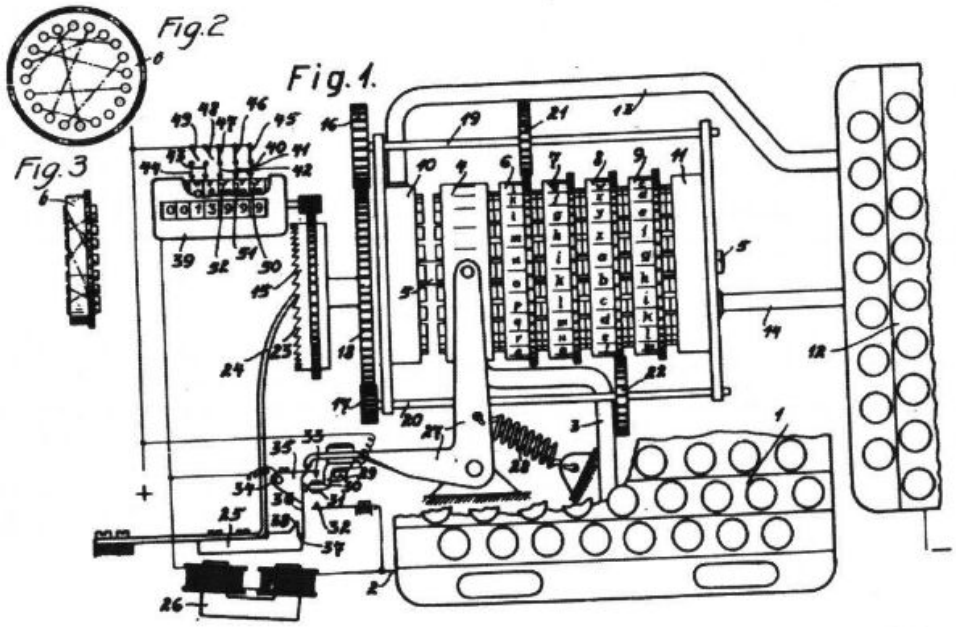

Abb. 4

Abb. 9.5: Schema der Scherbiusschen Maschine. Links oben eine Chiffrierwalze mit ihrer Verdrahtung (um 1923).