

„Enigma“ Chiffriermaschine

Von Dr.-Ing. Arthur Scherbius/ Elektrotechnische Zeitschrift 1923, Heft 47/48

Vorbemerkung zum Artikel: „Enigma“ Chiffriermaschine

Der Holländer Hugo Alexander Koch meldete im Jahre 1919 ein Patent für eine Geheimschriftmaschine an. Die Maschine erwies sich allerdings als kaum funktionsfähig. Der Ingenieur Dr. Arthur Scherbius aus Berlin erwarb die Patentrechte 1923 und entwickelte im gleichen Jahr daraus eine brauchbare Maschine, die er „Enigma“ (griechisch: Rätsel) nannte.

Die serienmäßige Produktion wurde im Juli 1923 aufgenommen. Der Absatz war allerdings begrenzt und nahm erst ab 1935, nachdem die „Enigma“ als Wehrmachtsschlüsselmaschine für den geheimen Nachrichtenverkehr eingeführt worden war, beträchtlich zu.

Den nachfolgenden Artikel (in der Elektrotechnischen Zeitschrift 1923, Heft 47/48) schrieb der Konstrukteur Arthur Scherbius im ersten Produktionsjahr der Maschine, wohl in der Absicht, dieses neuartige Gerät nicht nur der elektrotechnischen Fachwelt sondern - vor allem - den potentiellen Kunden vorzustellen. Ob ihm wohl seinerzeit der Gedanke gekommen ist, daß auch einmal die Nachwelt äußerst interessiert seine Konstruktions- und Funktionsbeschreibung lesen würde?
L.R.

Übersicht. Nachdem kurz auf die Anforderungen hingewiesen ist, welche an eine Chiffriermaschine gestellt werden müssen, damit dieselbe den Gebrauch der Geheimschrift allgemeinen Kreisen zugänglich macht, wird das neueste Modell der „Enigma“-Chiffriermaschine, welche für die verschiedensten Anwendungsgebiete brauchbar ist, an Hand von drei Abbildungen derselben in seinen wesentlichsten Konstruktionsteilen beschrieben.

An anderer Stelle* ist auf die Bedeutung der Geheimschrift für die Telegraphie und insbesondere für die Radiotelegraphie hingewiesen worden. Bisher haben hauptsächlich Militär- und Marinebehörden sowie der auswärtige Dienst chiffriert. Besonders im auswärtigen Dienst kann es unter Umständen noch nach Jahren wichtig sein, den Inhalt eines feindlichen Chiffrates zu ermitteln. Daß für staatliche Telegramme die Notwendigkeit der Geheimhaltung eine wesentlich zwingendere ist als für die normalen, von der Post übermittelten Handelsnachrichten, liegt auf der Hand. Da aber die Radionachrichten in der einfachsten Weise von jedem Unberufenen abgehört werden können, und in dem Gesamtverkehr Texte von solcher Länge auftreten, wie sie bei irgendwelchen Ämtern nie vorkommen, und da im allgemeinen die unberufene Lösbarkeit eines Chiffrates mit seiner Länge sehr viel leichter wird, so müssen auch für die Verwendung bei der Radiotelegraphie Chiffriersysteme mit großer Anforderung an die Sicherheit gewählt werden. Neben der Sicherheit muß die Radiotelegraphie noch die schärfsten Anforderungen an betriebsmäßige Verwendbarkeit, an Schnelligkeit, Einfachheit der Bedienung zur Vermeidung von Fehlerquellen und leichte Ausmerzbarkeit von Übertragungsfehlern stellen.

Soll die Geheimschrift für die Radiotelegraphie nutzbar gemacht werden, so kann dies nur mit Hilfe einer Maschine geschehen, denn nur eine solche ist imstande, so schnell und exakt zu arbeiten, wie dies bei der ungeheuren Menge des täglich zu bewältigenden Nachrichtestoffes notwendig ist. Auch nur eine Maschine kann die großen Vorteile, welche für die

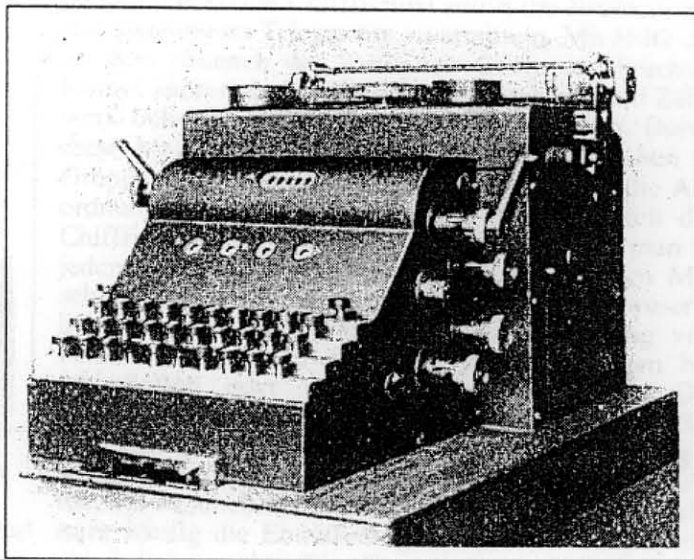


Abb. 1: Chiffriermaschine mit Verschlusskappen

Allgemeinheit in der Benutzung der Geheimschrift liegen, weiten Kreisen zugänglich machen.

Im folgenden soll das neueste Modell der „Enigma“-Maschine beschrieben werden. Es erfüllt vollkommen die Anforderungen, die die Post stellen muß, und ist gleichzeitig für amtliche Mitteilungen, für Handel und Industrie in weitestgehendem Maße verwendbar. Ohne auf die chiffriertheoretischen Grundlagen im einzelnen einzugehen, von denen nur bemerkt sei, daß das der Maschine zugrundeliegende Chiffriersystem in der Art, wie die Chiffriersicherheit gewahrt wird, prinzipiell neue, von den bis dahin verwendeten Schreibsystemen abweichende Wege geht, soll in dem vorliegenden Aufsatz im wesentlichen nur auf die Konstruktion der Maschine eingegangen werden.

In Abb. 1 ist die Maschine in vollkommen kompletten Zustand abgebildet, während in Abb. 2 die Verschlusskappen abgenommen sind, um die Einzelheiten der Maschine besser erkennen zu können. Die Maschine ist ganz ähnlich einer Schreibmaschine gebaut und wird auch genau wie diese bedient. Vorn sind die

*Radiotelegraphie und Geheimschrift, Zeitschrift für Fernmelde-technik, Heft 7 v. 16.7.1923, 4. Jahrgang

Schreibtasten zu erkennen, auf welchen auch ebenso wie bei einer Schreibmaschine erstens die 25 Buchstaben des Alphabetes und darunter auf jeder Taste je eine Zahl und ein Zeichen steht. Hinter den Tasten sind in Abb. 2 vier Walzen zu sehen. Diese Walzen tragen je einen mit Buchstaben beschrifteten Ring auf der linken und ein Zahnrad auf der rechten Seite. Auf der rechten Seitenwange der Maschine erkennt man vier kordierte Griffe. Diese Griffe sind mit vier Wellen verbunden, von denen je eine unter Vermittlung eines Zahnrades auf eine der vier Walzen arbeitet. Die Zahnräder sind nicht gleichmäßig verteilt, vielmehr ist bei ihnen ein Teil der Zähne weggelassen, so daß der Transport der Rolle ungleichmäßig erfolgt. Die ganze Chiffrierung geschieht auf elektrischem Wege. Außerdem wird die Maschine von einem Elektromotor angetrieben. Die vier Walzen bilden zusammen einen elektrischen Vielfachumschalter. Vor der hinten oben liegenden Schreibwalze ist ein auf einer waagerechten

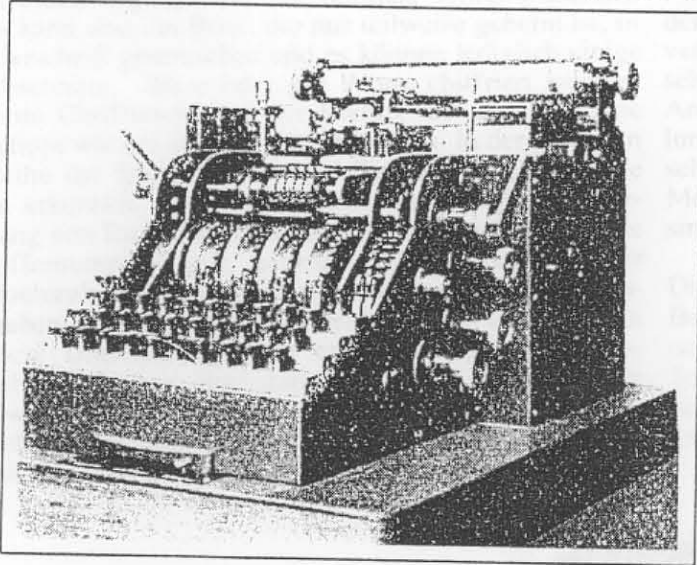


Abb. 2: Chiffriermaschine ohne Verschlussschlüssel

Welle befestigtes und mit dieser drehbares Typenrad zu erkennen. Wird ein Buchstabenkontakt niedergedrückt, so wird durch dieses Typenrad ein Buchstabe abgedruckt. Die Verbindung zwischen Schreibvorrichtung und Schreibkontakten wird durch die vier Walzen in ungeheurer großer Variationsfähigkeit geändert, und zwar tritt dadurch, daß nach jedem Niederschreiben eines Buchstabens die vier Wellen mit Hilfe eines gemeinsamen Antriebes jedesmal um eine Teilung weitergestellt werden, diese Veränderung nach jedem Buchstaben ein, und zwar derart, daß nach Niederschreiben von etwa 1 Mill. Buchstaben wieder die gleiche Variationsfolge auftritt, das heißt, erst wenn ein normales Buch von etwa 1000 Seiten abgeschrieben ist, wird ein genau gleicher Text wieder das gleiche Chifftrat ergeben. Den Text einer solchen Länge kann man als Chiffrierperiode bezeichnen. Derartige Chiffrierperioden sind etwa 20 000 in der Maschine, das heißt: es können 20 000 derartiger Bücher mit immer anderen Variationen abgeschrieben werden. Diese verschiedenen Variationen werden erreicht durch Einstellung verschiedener Schlüssels, das heißt durch veränderte Einstellung der Anfangsstellung der Rollen auf verschiedene Buchstaben. Die Einstellung geschieht mit Hilfe der vier rechts zu sehenden, kordierten Griffe. In Abb. 1 sind da, wo bei Abb. 2 die Rollen liegen, vier Fenster zu sehen. In diesen Fenstern erscheinen die jeweiligen Schlüsselbuchsta-

ben der vier Rollen. Links neben den kordierten Griffen sind abermals vier kleine, rechteckige Fenster zu sehen. Auch unter diesen erscheinen Buchstaben, welche die Stellung der Wellen und der mit diesen verbundenen Zahnräder zum Antriebsmechanismus festlegen. Auch diese vier Buchstaben können durch die kordierten Griffe nach Hereinschieben derselben eingestellt werden. Der gesamte Schlüssel besteht also aus acht Buchstaben. Über den vier Rollen sind in Abb. 2 fünf kleine Rollen zu sehen, die ein Zählwerk bilden. Das Zählwerk kann vermittelt des kordierten Griffes, welcher links außen an der Maschine zu sehen ist, auf Null gestellt werden. Die Zahlen des Zählwerkes erscheinen in den fünf oberen kleinen Fenstern (Abb. 1). Das Zählwerk zählt die Anzahl der in einem Telegramm, einer Telegrammserie oder in einem Bericht geschriebenen Buchstaben. Der Transportmechanismus der Papierwalze ist so eingerichtet, daß die Chifftratbuchstaben automatisch ohne Hinzutun des Schreibenden in Gruppen zu fünf auf dem Papier erscheinen. Halbautomatisch wird die Zeile auf je 50 Buchstaben begrenzt, so daß die Doppelzeile 100 Buchstaben enthält. Durch diese Anordnung ist es möglich, in einem Chiffriertext sofort die Nummer des Buchstabens im Telegramm zu ermitteln. Mit Hilfe der an dem obersten der kordierten Griffe angebrachten Kurbel kann man den Chiffriermechanismus und Zählwerk beliebig vorwärts und rückwärts drehen. Durch diese Maßnahmen: die Einteilung der Buchstaben in Gruppen und Zeilen genau bestimmter Länge, die Anordnung des Zählwerkes und die Verstellbarkeit des Chiffriermechanismus durch die Kurbel kann man in jedem Augenblick die Korrespondenz zwischen Maschine und Schriftstück herstellen. Dies ist ein wesentlicher Faktor zur Vermeidung und Aufklärung von Fehlern und zur Erleichterung von Rückfragen bei fehlerhaften oder unvollständigen Chifftraten. Die Kombination dieser Einrichtungen ermöglicht es, alles das richtig zu dechiffrieren, was richtig übergeben ist, im Gegensatz zu anderen Chiffrierverfahren, bei welchen ein fehlerhafter oder fehlender Buchstabe häufig die Entzifferung des ganzen Telegramms unmöglich macht. Die Begrenzung der Zeilen geschieht praktisch folgendermaßen:

Ist die Zeile von 50 Buchstaben beendet, so wird der Schreibmechanismus der Maschine elektrisch abgeschaltet. Ein Weiterschreiben auf derselben ist erst dann wieder möglich, wenn die Papierwalze auf ihre Anfangsstellung zurückgeschoben ist. Es ist also weder möglich über die Zeile hinaus zu schreiben noch die Zeile zu spät zu beginnen.

An Abb. 3 sind die bereits erwähnten Walzen noch besonders abgebildet. Sie sind nach Montage auf der Welle, auf welche sie auf dem Bilde nur lose aufgesteckt sind, drehbar gelagert. Am linken Ende der Welle ist ein Endanschlußstück zu sehen, zu welchem eine Reihe von Zuleitungen in einem gemeinsamen Kabel führt. An diese Zuleitungen sind die Schreibkontakte angeschlossen. Auf der rechten Seite der beiden Rollen sind kreisförmig angeordnete, herausstehende Kontaktbutzen zu sehen. Diese werden in kleine Röhren geführt und durch Federn nach außen gedrückt. Die Rollen tragen auf der nicht sichtbaren Seite eine gleiche Anzahl von Kontakten, welche mit dem Isoliermaterial der Stirnseite eine Fläche bilden und nach dem Zusammenbau gegen die herausstehenden Butzen anliegen. Von diesen Kontakten der beiden

Immerseits einer Rolle ist je einer der einen mit je einem der anderen Seite verbunden, und zwar in möglichst unregelmäßiger Weise. Auf jeder Stirnseite sind ebensoviel Kontakte vorhanden wie Schreibkontakte an dem Tastenbrett liegen. Durch Drehen jeder Rolle um je eine Teilung werden die Verbindungen zwischen der Geber- und Empfängerseite in der Maschine grundlegend vertauscht (nicht zyklisch, sondern vollkommen neu durcheinandergewürfelt), aber immer so, daß für jede Stellung ein Schreibkontakt einem ganz bestimmten Buchstaben am Typenrad entspricht.

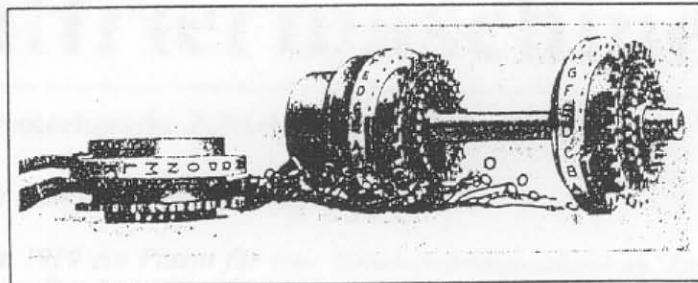


Abb. 3: Papierwalzen der Chiffriermaschine

Ganz vorn am unteren Rand der Maschine ist ein Hebel zu sehen, der auf drei Stellungen eingestellt werden kann. Mit Hilfe dieses Hebels kann die Maschine auf Chiffrieren, Dechiffrieren und Klartext eingestellt werden. Bei der Einstellung auf Klartext arbeitet dieselbe genau wie eine normale Schreibmaschine. Es kann also ein Brief, der nur teilweise geheim ist, in Klarschrift geschrieben und es können lediglich einige Abschnitte, Sätze oder gar Worte chiffriert werden. Beim Chiffrieren wird der Klartext auf der Maschine getippt wie bei einer Schreibmaschine. In der untersten Reihe der Tastatur sind zwei Tasten doppelter Breite zu erkennen. Dies sind Umschalttasten. Beim Übergang von Buchstaben auf Ziffern und Zeichen wird die Ziffernumschalttaste gedrückt. Sollen dann wieder Buchstaben geschrieben werden, so wird die Buchstabenumschalttaste angeschlagen. Das Chifftrat läßt diese Umschaltung nicht erkennen. Es besteht ausschließlich aus Buchstaben. Werden dagegen zum Zweck der Dechiffrierung diese Buchstaben wieder auf der Maschine abgetippt, nachdem der Umschalthebel auf Dechiffrieren eingestellt war, so erscheint

der Klartext wieder mit sämtlichen Zeichen und Buchstaben und, was für die leichte Lesbarkeit sehr wichtig ist, mit den richtigen Wortabständen. Das Dechifftrat hat also ungefähr die doppelte Anzahl von verschiedenen Zeichen wie das zu übermittelnde Chifftrat. Dies bedeutet einen großen Vorteil. Nachrichten, insbesondere solche, welche viele Zahlen enthalten, sind selbstverständlich wesentlich kürzer, wenn sie in Zahlen geschrieben werden als bei der Übermittlung in Worten. Andererseits ist es bei der telegraphischen Übermittlung von großem Vorteil, insbesondere bei Morse-schrift, nur Buchstaben übermitteln zu müssen, da die Morsezeichen für die Buchstaben wesentlich kürzer sind als die für Zahlen.

Die Maschine ist von der Firma Scherbius & Ritter in Berlin-Wannsee entwickelt worden. Das abgebildete neueste Modell dagegen ist von der Gewerkschaft Securitas, Berlin W 35, Steglitzer Straße 2, welche die sämtlichen Patente zwecks Verwertung übernommen hat, unter Mitarbeit der ersten Firma gebaut worden.