Chiffriermaschinen Aktiengesellschaft

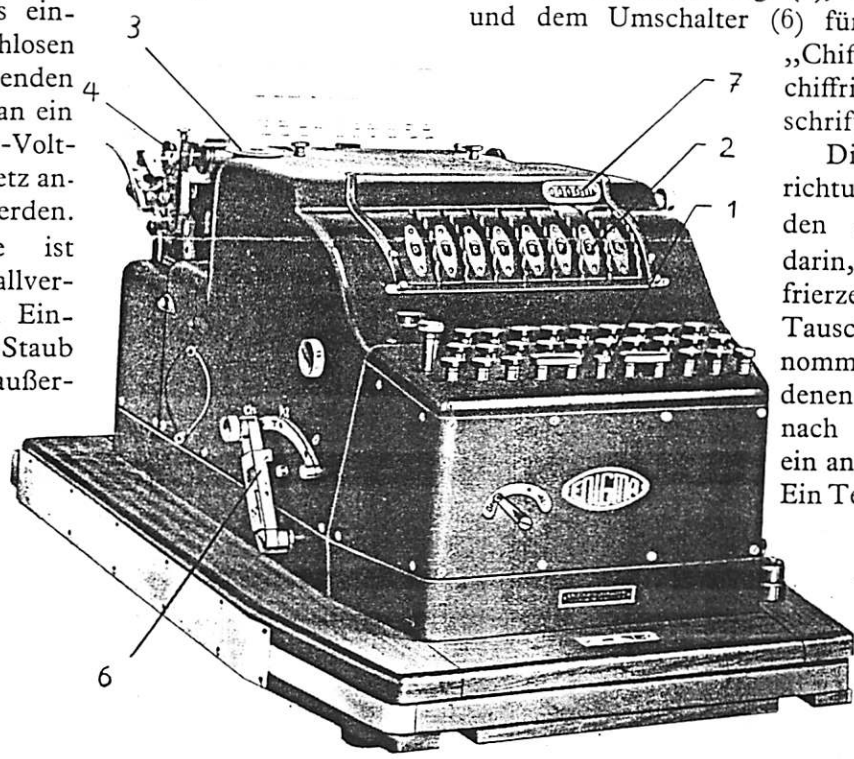
Berlin W 35, Steglitzer Straße 2

Fernsprecher: B 2 Lützow 2891 — Drahtanschrift: Chiffrier Berlin

Kurze Beschreibung der schreibenden „ENIGMA"-Chiffriermaschine.

Die schreibende ENIGMA Chiffriermaschine sieht in ihrer äußeren Form einer Schreibmaschine ähnlich. Die Maschine arbeitet elektrisch; sie ist für eine Gleichspannung von 80 bis 90 Volt gebaut und kann unter Vorschaltung von Widerständen an ein 110- bzw. 220-Volt-Gleichstromnetz oder, unter Zwischenschaltung eines einfachen, geräuschlosen nicht rotierenden Gleichrichters an ein 110- bzw. 220-Volt-Wechselstromnetz angeschlossen werden. Die Maschine ist durch eine Metallverkleidung gegen Eindringen von Staub geschützt und außerdem durch eine verschließbare Kappe aus Eichenholz abdeckbar. Durch zwei vorn und hinten herausziehbare Griffe kann die Maschine bequem getragen werden. Sie ist so konstruiert, daß die sie bedienende Person nicht mit stromführenden Teilen in Berührung kommen kann; außerdem sind Einrichtungen vorgesehen, welche bei nicht sachgemäßer Bedienung die Maschine elektrisch abschalten, so daß also empfindliche Teile nicht zerstört werden können. Durch einen normalen Installationsschalter erhält die Maschine Strom, was äußerlich durch ein Schauzeichen zu erkennen ist. Die größten Maße der Maschine ohne Holzkappe sind: Länge ca. 65 cm, Breite ca. 45 cm, Höhe ca. 38 cm, Gewicht ca. 60 kg.

Die Maschine besteht im wesentlichen aus der Tastatur (1), der Chiffriervorrichtung (2), der Schreibvorrichtung (3), dem Wagen (4) und dem Umschalter (6) für die Stellungen „Chiffrieren", „Dechiffrieren" und „Klarschrift".

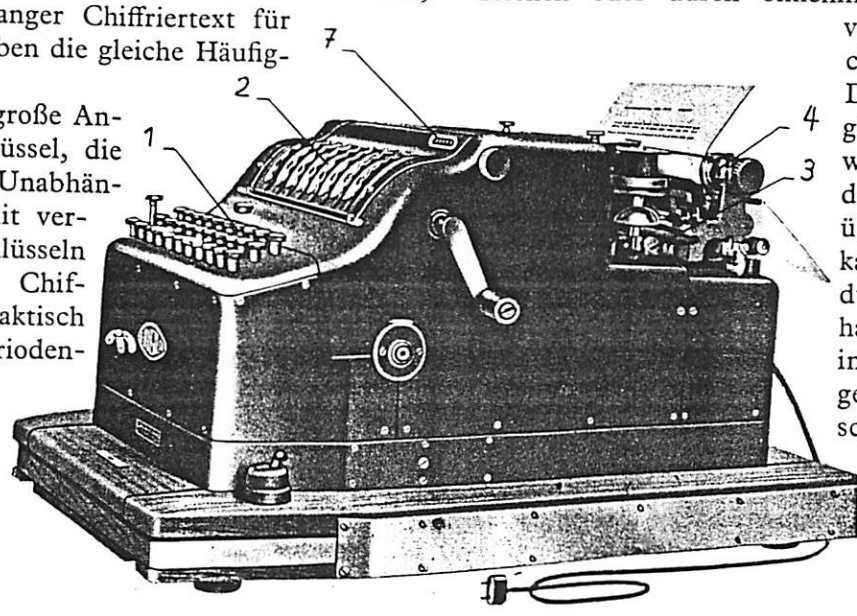


In die Maschine ist ein Briefbogen eingespannt, auf dem ein Chiffrat von 150 Buchstaben, eingeteilt in 3 × 10 Gruppen zu je 5 Buchstaben, zu sehen ist. Der Umschalter (6) steht auf „Chiffrieren". Am Kopf des Briefes ist der Schlüssel und die Zählwerkstellung angegeben. Das Zählwerk (7) stand beim Beginn des Chiffrates auf 00 000 und steht jetzt auf 00 150. Die in der vordersten Reihe der Tastatur liegenden 2 großen Tasten sind die Umschaltetasten für „Zahlen und Zeichen" und für „Buchstaben". Zwischen diesen beiden liegt die Weiterschalttaste, mit welcher in der Dechiffrierstellung bei etwa vorhandenen Textverstümmelungen die komplette Chiffriervorrichtung und der Wagen und in der Klarschriftstellung für die Abstände nur der Wagen weitergeschaltet werden kann. Die große Taste links der Tastatur wird zum Schreiben von großen Buchstaben in der Klarschriftstellung benötigt.

Die Chiffriervorrichtung der schreibenden ENIGMA besteht darin, daß die Chiffrierzeichen 456 976 Tauschalphabeten entnommen werden, von denen sich selbsttätig nach jedem Zeichen ein anderes einschaltet. Ein Teil dieser Tauschalphabete wird innerhalb einer Chiffrierperiode, das heißt bis zur mechanischen Rückkehr der Chiffriermechanismen in ihre Anfangsstellung, mehrmals, jedoch immer in ganz anderer Reihenfolge angewendet. Die Länge einer Chiffrierperiode beträgt 15 777 450 Zeichen, das heißt, erst nach 15 777 450 mit dem gleichen Schlüssel geschriebenen Zeichen tritt wieder die gleiche Tauschalphabetfolge auf. Es können also etwa 8000 Schreibmaschinenseiten, was etwa der fünffachen Textlänge der Bibel entspricht, ge-

schrieben werden, ohne eine Periode zu erschöpfen. Die Maschine verfügt über 17 576 verschiedene Perioden von solcher Länge. Sie bietet die Möglichkeit 277 304 451 200 verschiedene Schlüssel einzustellen. Die außerordentlich große Anzahl von Tauschalphabeten und die in dem Mechanismus der Maschine begründete ungeheure Variationsfähigkeit in der Reihenfolge derselben bewirken, daß weder innerhalb einer Periodenlänge von 15 777 450 Zeichen noch zwischen den 17 576 verschiedenen Perioden irgendwelche Ähnlichkeiten vorkommen. Die dem Klartext anhaftenden Häufigkeiten von Buchstaben oder Buchstabenfolgen sind im Chiffrat vollkommen verschwunden, so daß ein langer Chiffriertext für jeden Buchstaben die gleiche Häufigkeit ergibt.

Die sehr große Anzahl der Schlüssel, die vollkommene Unabhängigkeit der mit verschiedenen Schlüsseln geschriebenen Chiffrate und die praktisch unendliche Periodenlänge bieten die Grundlage für die unerreichte Chiffriersicherheit der Maschine auch bei stärkstem Chiffrierverkehr zwischen einer großen Anzahl mit genau gleichen Maschinen ausgerüsteter Stellen.



Auf der rechten Maschinenseite oben in der Mitte ist der Knopf zur Nullstellung des Zählwerkes. Mit der darunter befindlichen Kurbel kann die gesamte Chiffriervorrichtung mit dem Zählwerk um eine beliebige Zeichenzahl vorwärts oder rückwärts gedreht werden. Für den Betrieb muß die Kurbel abgezogen werden. Der weiter unten sichtbare größere Knopf dient zum Entkuppeln der Chiffrierwalzen und Antriebsräder, damit diese für den verabredeten Schlüssel eingestellt werden können. Mit dem auf dem Holzsockel angebrachten Hauptschalter wird der elektrische Strom ein- und ausgeschaltet.

Einer der wichtigsten Vorteile der schreibenden ENIGMA aber ist der, daß die in der Maschine liegenden Möglichkeiten praktisch auch in der einfachsten Weise ausgenutzt werden können. Es wurde bei der Konstruktion der größte Wert darauf gelegt, die Schlüsseländerung so einfach und schnell wie möglich zu gestalten. Zur Änderung des aus acht Zeichen bestehenden äußeren Schlüssels dienen die acht aus der Kappe herausragenden Einstellräder, durch die vermittels Drehens die gewünschten Zeichen unter den Fenstern einzustellen sind, wenn vorher der an der Kurbelseite der Maschine befindliche große Knopf entrastet und nach innen gedrückt ist. Nach Beendigung der Schlüsseleinstellung wird der Knopf wieder nach außen gezogen; die Maschine ist dann schreibbereit.

Die vollkommene Änderung des Schlüssels erfordert 30 Sekunden. Schon die Änderung eines Zeichens, die nur etwa 5 Sekunden in Anspruch nimmt, ändert aber das Chiffrat so grundlegend, daß irgendwelche Ähnlichkeiten nicht mehr vorhanden sind. Es besteht daher die Möglichkeit, ohne praktischen Zeitverlust jede Nachricht mit einem anderen Schlüssel zu geben.

Ein sehr wesentliches Moment besteht noch darin, daß die Schlüsseländerung gegenüber einem für längere Zeit, beispielsweise für einen Monat, verabredeten Grundschlüssel jedem Telegramm klar durch besondere Schlüsselzeichen oder durch ohnehin im Telegramm vorkommende Zeichen, wie Uhrzeit, Datum oder dergleichen, nach gewissen Verabredungen ganz offen übermittelt werden kann, ohne hierdurch die Geheimhaltung auch nur im geringsten zu gefährden. Die Maschine bietet also die Möglichkeit, auch für größten Chiffrierverkehr einfache und absolut einwandfreie Vorschriften und Regeln für den Chiffrierverkehr zu schaffen.

Um den Grundschlüssel sogar für den Chiffrierenden oder Dechiffrierenden geheim zu halten und die Schlüsseländerung noch weiter zu vereinfachen, sind nach dem Öffnen einer plombierbaren Klappe die Ringe mit den Schlüsselzeichen gegen die Walzen, welche nach diesen Schlüsselzeichen eingestellt sind, verdrehbar angeordnet. Der Grundschlüssel kann also durch Einstellung dieser Ringe auf den Walzen eingestellt werden, während die Schlüsseländerungen durch Einstellung der Zeichen unter den Fenstern in der oben angegebenen Weise erfolgen. Nur wenn der Schlüsselwechsel sehr einfach erfolgen kann und praktisch keine Zeitverluste bedingt, kann seine Anwendung im praktischen Chiffrierverkehr tatsächlich durchgeführt werden. Aus diesem Grunde hat auch der Konstrukteur der

schreibenden ENIGMA auf jegliche Schlüsseländerung verzichtet, die durch langwieriges Umschalten oder gar durch auswechselbare Teile erfolgen müßte. Er war hierzu in der Lage, da das Chiffriersystem der Enigma-Chiffriermaschine derartige praktisch unbrauchbare Maßnahmen zur Aufrechterhaltung einer unbedingten Geheimhaltung nicht erfordert.

Die Konstruktionseinzelheiten, welche der einfachen Schlüsseländerung dienen, haben mit der theoretischen Chiffriersicherheit der Maschine an sich nichts zu tun. Trotzdem gehören sie, auch vom Standpunkt der tatsächlichen Chiffriersicherheit, zu den wichtigsten Konstruktionselementen der Maschine; denn es leuchtet ein, daß es im praktischen Chiffrierbetrieb vollkommen gleichgültig ist, ob Nachrichten infolge prinzipieller theoretischer Fehler des Systems oder infolge unsachgemäßer Anwendung überlasteter Chiffreure kompromittiert werden.

Die Tauschalphabete werden von vier elektrisch hintereinander geschalteten Chiffrierwalzen erzeugt, deren Stirnseiten je 26 Kontakte tragen, die innerhalb jeder Chiffrierwalze vollkommen unregelmäßig und in jeder Walze verschieden miteinander verbunden sind. Die Verdrehung einer Walze um einen Schritt ergibt ein neues, gegenüber allen anderen vollkommen verwürfeltes Tauschalphabet. Da die vier Walzen je 26 Kontakte tragen, so ist die Anzahl der Tauschalphabete $26^4 = 456\,976$. Die Chiffrierwalzen werden durch vier Zahnräder, die nicht nur verschiedene Durchmesser, sondern auch unregelmäßige an ihrem Umfang verteilte Zahnlücken aufweisen, angetrieben. Hierdurch wird die sehr lange Periode und ein Ablauf der Walzen mit verschiedener Geschwindigkeit und verschiedener Reihenfolge erreicht, so daß die mit verschiedenen Schlüsseln geschriebenen Chiffrate keinerlei Ähnlichkeit aufweisen. Die Chiffrierwalzen und die Lückenzahnräder tragen entsprechend ihren Zähnezahlen die einstellbaren und feststellbaren Zeichenringe, auf welchen die 26 Buchstaben des internationalen Alphabetes und bei einigen außerdem die Zahlen 1; 1, 2, 3; 1, 2, 3, 4, 5 eingraviert sind.

Mit der Chiffriervorrichtung ist ein fünfstelliges Zählwerk (7) gekuppelt. Es dient zum Zählen der niedergeschriebenen Zeichen; es läuft nur bei Chiffrieren und Dechiffrieren mit und wird bei Zwischentexten in Klarschrift automatisch stillgesetzt. Es ist mit einer Null-Einstellvorrichtung versehen, um jede Nachricht mit der Nullstellung beginnen zu können.

Mit der Maschine kann chiffriert, dechiffriert und Klarschrift geschrieben werden; die Schreibgeschwindigkeit beträgt bis zu 250 Zeichen in der Minute. In der Stellung „Klarschrift" des Umschalters können große und kleine Buchstaben, Zahlen, Interpunktionszeichen und Zwischenräume geschrieben werden. Das Chiffrat besteht nur aus kleinen Buchstaben und wird automatisch in Gruppen zu fünf und in Zeilenlängen zu fünfzig Buchstaben (zehn

CHIFFRIERMASCHINEN AKTIENGESELLSCHAFT
BERLIN W 35 · STEGLITZERSTR. 2

ENIGMA

BETRIFFT Th / R
Schluesselvariation : B O B

DEN 1.Oktober 1931

Fa .
Wilhelm F o r s t e r
M a n c h e s t e r

Wir erhielten Ihr Schreiben vom 25. September 1931 und teilen Ihnen nach besten Wissen darauf folgendes mit :

100 lcbas fywsb dhgfs ixndu jjyte mmaew faxeq gyamu qepww uumig
vamlu dyhnq uzwsy tfupn afouy ugzsp wtyul uyego woqwf hpqeq

200 ubqfs hktei ckzhu mnnru nyper oprmo ehihc odoth legov uwlje
prvpf wkyxs gvvhg hwzeq neqkx zcdmt svaqb owsee zubvf ddmnl

300 fzrik vsyrw gsjjp btxbs niyzr wodfz azwuo pmbst ywjxw lmoqq
oncka kinjz gkaqn jgvzu wttmd rrsdk qwiux ulqpx rhnuf vjxrm

400 zsvuk xujhy ecvty sszsr typek pqujx hstqq yebeb dnzbz xdwof
lecca dkxpp jlkfg xmocw mobpy wfwek fudmj ftfzh qslwy bpidg

500 yocyx dwiao leweg umzzj mjbty rvvfw vaanj tinsn fqolu rotxx
gwldg tuowe jbzau fyums seosa kkout fgxx

Wir empfehlen uns Ihnen und zeichnen
hochachtungsvoll
Chiffriermaschinen Aktiengesellschaft .

Brief, dessen Text zum Teil chiffriert ist. Die Variation des Schlüssels als Zusatz für einen vorher verabredeten Schlüssel steht am Briefkopf. Adresse, Anfang und Schluß des Briefes sind in Klarschrift auf der Chiffriermaschine geschrieben. Die Doppelzeilen des Chiffrates sind fortlaufend numeriert; es ist mit Leichtigkeit hieraus zu erkennen, daß das Chiffrat eine Länge von 484 Zeichen hat.

Dechiffrat : Th / R vom 1.10.1931

......
100 wir halten es nach unseren erfahrungen nicht fuer
ratsam der in ihrem schreiben vom 20. v . mts . ge

200 nannten firma schultze a . g . einen kredit in hoe
he von 50 000 rm . einzuraeumen . wie wir von zuve

300 rlaessiger seite erfahren haben , ist die firma in
ihren zahlungen nicht sehr puenktlich . wir selbst

400 haben mit dieser firma schwierigkeiten gehabt rech
nungen in hoehe von 3.000 rm . bezahlt zu erhalten

500 diese mitteilung machen wir ihnen streng vertrauli
ch und ohne unsere verantwortung .
......

Der Empfänger hat mit der korrespondierenden Maschine, die natürlich die gleiche Schlüsseleinstellung hat, ein Dechiffrat angefertigt, das normalen Klartext mit Worten, Zwischenräumen, Zahlen und Zeichen zeigt.

Gruppen) eingeteilt, Maßnahmen, welche alle für das Ablesen und für die telegraphische Übermittlung sehr wichtig sind. Chiffriertechnisch von großer Bedeutung ist, daß das Chiffrat nur kleine Buchstaben aufweist, obwohl der zu verziffernde Text aus kleinen Buchstaben, Zahlen, Interpunktionszeichen und Zwischenräumen besteht. Im Dechiffrat erscheint der Klartext wieder mit den richtigen Zwischenräumen und mit Zahlen und Interpunktionszeichen und kann daher wie jeder normale Schreibmaschinenbrief sofort gelesen werden. Die Einteilung des Chiffrats in Gruppen zu fünf ist wieder verschwunden. Dem unberufenen Entzifferer sind keinerlei Angriffspunkte gegeben, zu ermitteln, ob die Buchstaben des Chiffrates Buchstaben, Zahlen, Zeichen oder Zwischenräume im Dechiffrat bedeuten. Die Tatsache, daß Zahlen und Zeichen nicht durch Worte ausgedrückt werden müssen, verkürzt das Chiffrat und erleichtert die Lesbarkeit.

Die Einteilung in Gruppen zu fünf und die automatische Begrenzung der Reihen auf fünfzig Buchstaben erleichtert nicht nur die Dechiffrierung und die Übermittlung der Nachrichten, falls sie telegraphisch gegeben werden, vielmehr ist diese Einteilung im Zusammenhang mit dem obenerwähnten Zählwerk geeignet, etwaige Fehler oder Lücken in der Übertragung oder beim Chiffrieren schnell richtigstellen zu können. Die Gruppeneinteilung und Zeilenbegrenzung ermöglicht die sofortige Feststellung, der wievielte Buchstabe eines Chiffrates irgendein beliebiger Textbuchstabe ist. Vermittels einer Kurbel ist es möglich, das Chiffriersystem mit dem Zählwerk zusammen schnell auf die Zahl dieses Buchstabens einzustellen. Ist das geschehen, so kann der einzelne Buchstabe sofort chiffriert oder dechiffriert werden. Diese Vorrichtung ermöglicht es auch, alle Buchstaben eines Chiffrats, welche übermittelt worden sind, auch dann noch zu entziffern, wenn ein Teil des Telegramms nicht übermittelt werden konnte. Dies ist ein großer Vorteil gegenüber einer Reihe anderer Chiffrierverfahren, bei denen bei teilweise verstümmelten Telegrammen auch die Entzifferung des richtig übertragenen Restes nur mit großem Zeitverlust möglich oder vielleicht überhaupt unmöglich ist.

Eine einfache Umschaltung ermöglicht es, bei derselben Nachricht zwischen Klartext und Chiffriertext abzuwechseln; beispielsweise können die Adresse eines Briefes und unwesentlichere Nachrichten offen geschrieben werden, während nur wichtigere Nachrichten, wie beispielsweise Preise usw., chiffriert werden.

Die Tastatur der schreibenden ENIGMA ist elektrisch derart blockiert, daß ein Typenhebel durch Tastendruck erst dann wieder anschlagen kann, wenn die vorher gedrückte Taste wieder losgelassen ist, so daß nie zwei Typen zusammenschlagen können. Die für die Umschalterstellungen „Chiffrieren" und „Dechiffrieren" nicht benötigten Tasten sind elektrisch gesperrt. Zur Umschaltung auf die einzelnen Schalterstellungen wird eine Sekunde benötigt.

Als Schreibvorrichtung ist ein bei Schreibmaschinen übliches normales Typenhebelsystem verwendet; die 26 Typenhebel sind mit den drei Zeichengattungen „kleine Buchstaben", „Zahlen und Interpunktionszeichen" und „große Buchstaben" versehen und schlagen gegen die Walze eines handelsüblichen Schreibmaschinenwagens.

Die schreibende ENIGMA arbeitet mit durch kurzseitige Stromstöße erregten Elektromagneten, also ohne Motor und die dadurch entstehenden Geräusche. Unmittelbar nach jeder Tastenbetätigung ist die Maschine wieder vollkommen stromlos, so daß Überhitzungen der Magnetspulen nicht auftreten können. Der Tastenanschlag ist leichter als bei einer normalen mechanischen Schreibmaschine, da nur Kontakte zu betätigen sind. Die Schrift ist sichtbar wie bei Schreibmaschinen.

Das Chiffriersystem der schreibenden ENIGMA korrespondiert nicht mit dem unserer Glühlampenchiffriermaschine. Dagegen ist es aber möglich, die schreibende ENIGMA durch ein mehrteiliges Steckerkabel mit einem für diesen Zweck umgearbeiteten Modell unserer Glühlampenchiffriermaschine elektrisch derart zu verbinden, daß der zu verziffernde Klartext auf der Glühlampenchiffriermaschine abgetippt und dabei selbsttätig auf der dann nur als Schreibmaschine dienenden schreibenden ENIGMA niedergeschrieben wird. Die Chiffriervorrichtung der schreibenden ENIGMA ist hierbei automatisch abgeschaltet, das Chiffrat erscheint ebenfalls in Gruppen zu fünf Buchstaben. In der gleichen Weise können natürlich auch umgekehrt mit der Glühlampenchiffriermaschine angefertigte Chiffrate direkt in Maschinenschrift entziffert werden. Für ganz besonders geheim zu haltende Nachrichten ist es auch ferner möglich, daß beide Maschinen räumlich voneinander getrennt arbeiten, so daß die die Glühlampenchiffriermaschine bedienende Person von dem Inhalt des auf der schreibenden ENIGMA erscheinenden Dechiffrates keine Kenntnis hat.