[illegible]

ENIGMA

CHIFFRIERMASCHINEN

Generalstaben
[illegible]
[illegible] 1935
[illegible]

[illegible]

HANDELSMASCHINE

ENIGMA
CHIFFRIERMASCHINEN

HANDELSMASCHINE

Wer hat Interesse an der Übermittlung geheimer Nachrichten und wer wendet Geheimschrift an?

Nicht nur jedes politische und militärische Handeln, sondern auch jede weiterreichende geschäftliche Tätigkeit ist aufgebaut auf Plänen, Kombinationen, Befehlen, Anweisungen und Nachrichten, deren unbedingte Geheimhaltung für kürzere oder längere Zeit die Vorbedingung für das Gelingen ist.

Zur Wahrung von Geheimnissen oder Nachrichten gehören vor allem zwei Dinge: Die Zuverlässigkeit und Geschicklichkeit der Beteiligten und ein unbedingt zuverlässiges Chiffriersystem bei der schriftlichen und telegrafischen Übermittlung. Durch Abfangen wichtiger Nachrichten sind Schlachten gewonnen, durch Entziffern fremder Staatsdepeschen sind wichtige politische Maßnahmen durchkreuzt, andererseits sind durch frühzeitige und geheime Übermittlung geschäftlicher Nachrichten große Vermögen erworben worden.

Aber nicht nur bei einzelnen markanten Ereignissen aus der Geschichte hat die geheime Nachrichtenübermittlung eine wichtige Rolle gespielt. Im täglichen Geschäftsgetriebe der Diplomatie ist sie von ausschlaggebender Bedeutung. Im Geschäftsverkehr bildet die geheime Übermittlung von Preisen, Kursen, Kauf- und Verkaufsorders, von allgemeinen Dispositionen, Anordnungen, Ereignissen, die geheime aktenmäßige Festlegung und Aufbewahrung von geschäftlichen Abmachungen, von Erfindungen, Erfahrungen, Personalauskünften usw. einen grundlegenden Faktor. Interesse an der geheimen Übermittlung oder auch an der geheimen aktenmäßigen Festlegung haben also Behörden und weite Kreise von Kaufleuten und Industriellen.

Es muß angesichts dieser Tatsache Wunder nehmen, daß die Geheimschrift bisher fast ausschließlich im diplomatischen Verkehr, bei Militär und Marine Verwendung findet, daß man sich derselben im Geschäftsleben dagegen fast überhaupt nicht bedient, abgesehen von den geringfügigen Ausnahmen, bei denen der Code, dessen Hauptzweck die Kürzung und die Ersparnis von Telegrammspesen ist, gleichzeitig zur Wahrung des Telegrammgeheimnisses herangezogen wird. Zur Lösung dieses Widerspruches bedarf es eines genaueren Eingehens auf das, was man Chiffrierkunst nennt.

Was ist Chiffrierkunst?

Die meisten haben sich in ihrer Jugend wohl eine Geheimschrift erdacht, indem sie an Stelle der Buchstaben des Alphabets andere Buchstaben oder andere Zeichen setzten. Schon Julius Cäsar hat eine solche Geheimschrift praktisch verwandt. Heute weiß fast jeder, daß diese „Geheimschrift" ihren Namen zu Unrecht führt und daß es keines großen Chiffrierkünstlers bedarf, um aus wenigen Zeilen bald die e, die n, die i und die r und s wegen ihrer größeren und fast immer gleichen Häufigkeit als solche festzustellen, um dann mit etwas Kombinationsgabe das ganze Alphabet herauszufinden.

Dem Kriegsmittel der Geheimschrift ist es ähnlich gegangen wie dem der Kanonen und Panzerplatten, die sich gegenseitig zu immer größerer Vervollkommnung entwickelten. Das Cäsar'sche Chiffriersystem oder der Cäsar, wie dasselbe von den Chiffriersachverständigen genannt wird, wurde verbessert, aber auch diese verbesserte Geheimschrift wurde gelöst. Es wurden Chiffriersysteme erdacht, die teilweise eine Zeit lang der unberufenen Entzifferung standhielten, aber immer wieder fanden sich findige Köpfe, die auch die kompliziertesten Systeme lösen konnten. Der Weltkrieg hat die Chiffrierkunst in nie dagewesener Weise gefördert. Neue Systeme sind ausgearbeitet und erstaunliche Leistungen auf dem Gebiet der Lösung von Geheimschriften vollbracht worden. Die ganze Chiffrierkunst ist zu einer weitreichenden Wissenschaft geworden, von der nur der allerkleinste Teil der Allgemeinheit zugänglich ist. Das Hauptergebnis dieser umfassenden Forschungen besteht darin, daß man heute weiß, wie ungeheuer schwierig es ist, Chiffriersysteme großer Sicherheit aufzustellen und richtig anzuwenden. Es ist nicht schwierig, ein einzelnes Telegramm sicher zu chiffrieren: die Schwierigkeiten beginnen erst dann, wenn einem großen Kreis von Personen ein Chiffriersystem anvertraut werden soll, welches mindestens für den Fall absoluter moralischer Zuverlässigkeit dieser Personen genügende Sicherheit gegen Entzifferung bietet.

Welchen Anforderungen muß ein Chiffriersystem genügen?

Ein solches Chiffriersystem muß mit Rücksicht auf die Sicherheit die Eigenschaft haben, daß es ganz mechanisch und für beliebige Texte verwendet werden kann. Schon dies ist eine Eigenschaft, die die wenigsten Systeme haben. Gewöhnlich muß bei der Handhabung derselben mit großer Vorsicht vorgegangen werden. Unter Umständen sind einfache Systeme in den Händen geübter Chiffreure besser als wesentlich bessere Systeme in der Hand von halben Laien. Den meisten Systemen wird eine laienhafte Anwendung zum Verderben. Ein brauchbares Chiffriersystem muß

aber noch anderen Bedingungen genügen. Es darf vor allem nicht kompliziert in der Anwendung sein. Es darf nicht zu große Anforderungen an die Aufmerksamkeit und die Exaktheit des Chiffreurs stellen. Kleine Fehler beim Chiffrieren dürfen die berufene Lösung des Telegramms nicht derart erschweren, daß die Dechiffrierung nur dem gewiegten Chiffriersachverständigen unter großen Zeitopfern, nicht aber dem normalen Chiffreur möglich ist.

Aus diesen Tatsachen ergibt sich die Beantwortung der Frage, die wir uns vorgelegt haben, warum trotz eines großen, offenbar vorhandenen Bedürfnisses so wenig chiffriert wird. Die bisher bekannten guten, handschriftlichen Verfahren benötigen so viel Fachkenntnis, so viel Zeit und Aufmerksamkeit, daß sie nur dort praktisch verwendet werden können, wo man ohne Chiffrieren absolut nicht auskommt, und wo daher auch die nötigen geschulten Kräfte, Zeit und Geld zur Verfügung stehen müssen. Trotzdem sind diese Verfahren nicht unbedingt sicher, wenn sie nicht ausschließlich von geschulten Fachleuten gehandhabt werden. Der Weltkrieg hat gezeigt, daß es auf beiden Seiten gelungen ist, auch solche Verfahren zu lösen, welche man für unlösbar hielt. Wenn man auch nicht alle einzelnen Telegramme entziffern konnte, so ist es doch immer und immer wieder gelungen, einzelne Telegramme zu lösen, wenn die Verhältnisse günstig waren. Ein großer Mangel haftet fast allen Schreibsystemen an, der darin besteht, daß die unberufene Lösung sehr stark erleichtert wird, wenn die Chiffrate lang sind. Dies ist ein Grund dafür, daß lange schriftliche Geheimberichte bisher fast garnicht chiffriert werden, sondern daß sich die Verwendung der Geheimschrift auf die kurzen telegrafischen Mitteilungen beschränkt. Ein anderer Grund ist der, daß die Chiffrierung langer Berichte so viel Zeit beim Absender und Empfänger in Anspruch nimmt, daß man geheime schriftliche Berichte lieber einem Kurier übergibt, anstatt sie mit der Post zu versenden.

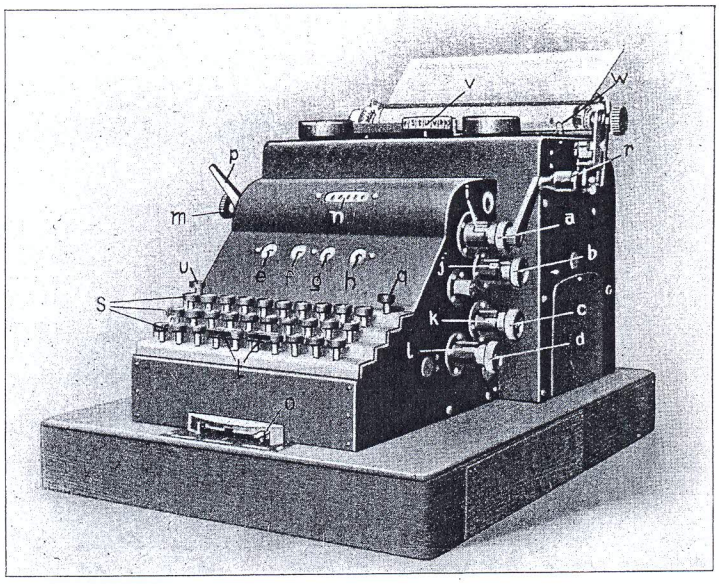
Interesse der Post am Chiffrieren von Telegrammen.

Neuerdings ist bei den Postbehörden in den verschiedenen Ländern immer dringender das Bedürfnis aufgetreten, die drahtlos übersandten Telegrammme zu chiffrieren, denn den Postbehörden, die bemüht waren, das Postgeheimnis für den Briefverkehr und für die Draht-Telegramme unbedingt zu wahren, ist dies bei der drahtlosen Übermittlung von Telegrammen nicht mehr möglich, insbesondere in neuester Zeit, nachdem es die Erfindung der Verstärkerröhren in Zusammenarbeit mit den kleinen Rahmen-Antennen ermöglicht, den Funkverkehr ohne weithin sichtbare Antenne in einem abgeschlossenen Raum anzuhören, und weil

daher kein Gesetz der Welt im Stande ist zu verhindern, daß jeder Interessent die Nachrichten der drahtlosen Stationen abhört. Den ganzen telegrafischen Verkehr der drahtlosen Stationen mit Hilfe von schriftlichen Verfahren zu chiffrieren würde vollkommen unmöglich sein, da dies viel zu teuer, zu zeitraubend und zu unzuverlässig ist.

Chiffriermaschinen.

In Anbetracht aller dieser Verhältnisse ist es nicht verwunderlich, daß in allen Staaten Hunderte von Patenten auf Chiffriermaschinen angemeldet worden sind, von denen allerdings



wohl nur wenige wirklich ausgeführt wurden. Diese Erfindungen leiden fast alle an dem Mangel, daß den Erfindern nicht bekannt sein konnte, wie weit die Chiffrier-Büros der modernen Staaten in der Entzifferung von Geheimschriften vorgedrungen sind. In den Kreisen der Chiffriersachverständigen hatte sich daher der Glaube festgesetzt, daß es prinzipiell unmöglich wäre, Chiffriermaschinen zu bauen, die an Chiffriersicherheit auch nur annähernd das leisten könnten, was die guten schriftlichen Systeme zu leisten im Stande sind. Infolge neuerer Erfindungen mußte diese Auffassung vollkommen revidiert werden. Es gibt heute maschinelle Chiffriermethoden, welche die handschriftlichen Systeme an Chiffriersicherheit bei weitem übertreffen. Nachdem das System gefunden war, war es für den Ingenieur keine unüberwindliche Aufgabe mehr, einen Apparat zu bauen, welcher alle diejenigen Lücken ausfüllt, welche bisher noch zwischen chiffriersicheren Systemen und der praktischen Verwendbarkeit derselben klafften. Das Ergebnis ist die „Enigma"-Chiffriermaschine.

Die „Enigma"-Chiffriermaschine.

Die „Enigma"-Chiffriermaschine sieht in der äußeren Form einer Schreibmaschine ähnlich. Vor dem Chiffrieren wird durch einen einfachen Mechanismus der Schlüssel, der dem Absender und dem Empfänger bekannt sein muß, eingestellt. Die Variationsfähigkeit dieser Schlüssel ist so groß, daß hunderte von Personen die gleiche Maschine haben können und trotzdem durch Verabredung der Schlüssel in beliebigen Gruppen vollkommen geheim untereinander verkehren können. Wird ein Text auf die Maschine geschrieben, so entsteht ein Chiffrat, welches folgendermaßen aussieht:

lbpyl aiisd aiprj nqkcn dprks zbqhw vdyzn pqtur wadmf tgxjy
cyghc fvago sqbüt txdnt yzcaä trxmo üxcjl zojql ghsqg iäcaz

Werden nun die einzelnen Buchstaben dieses Chiffrates zum Zweck des Dechiffrierens auf der korrespondierenden Maschine abgeschrieben, so entsteht der ursprünglich gegebene Klartext in der folgenden Form:

wasserstand der spree am 24. april . oberpegel:
+32.28, unterpegel : +30.62-| morgenpost |.----

Man erkennt, daß das Chiffrat aus Gruppen von 5 Buchstaben besteht, und daß in jeder Zeile zehn solcher Gruppen stehen, sodaß die Zeile 50, die Doppelzeile 100 Buchstaben enthält. Diese Einteilung in Gruppen und die Begrenzung der Zeile auf 50 Buchstaben geschieht automatisch. Man sieht ferner, daß das Chiffrat lediglich aus Buchstaben besteht, während der Klartext mit Ausnahme der großen Buchstaben alle Zeichen und Zahlen einer normalen Schreibmaschine aufweist. Die Maschine hat außerdem ein Zählwerk, welches zusammen mit der automatischen Gruppeneinteilung die Bedienung der Maschine so einfach gestaltet, daß sie jedermann ohne Übung sofort vornehmen kann, daß Fehler fast vermieden werden und wirklich vorkommende Fehler mit kleiner Mühe wieder auszuscheiden sind.

Vor allem hat die Maschine eine für den praktischen Gebrauch grundlegend wichtige Eigenschaft. Sollte beim Niederschreiben, beim Entziffern oder bei der Übertragung (etwa bei telegrafischer Übermittlung) ein Fehler entstanden sein, so wird lediglich der fehlerhafte Buchstabe falsch entziffert, während die Entzifferungsmöglichkeit des ganzen übrigen Textes in keiner Weise leidet. Die Chiffrierung und die Dechiffrierung nehmen nicht viel mehr Zeit in Anspruch als die Niederschrift eines Briefes auf der Schreibmaschine.

Durch die „Enigma"-Chiffriermaschine ist nicht nur den Behörden, sondern auch Privaten die Möglichkeit gegeben, mit absoluter

Sicherheit Telegramme und schriftliche Mitteilungen beliebiger Länge in Geheimschrift anzufertigen. Irgend welche Rücksichten auf den Text oder sonstige Vorsicht in der Behandlung sind nicht erforderlich. Die Maschine ist so gebaut, daß sie dem Chiffrierenden alle diese Dinge abnimmt und auch die notwendige Aufmerksamkeit auf ein Minimum beschränkt. Dabei ist die Handhabung so einfach, daß in besonderen Fällen ganz wichtige Mitteilungen von den leitenden Persönlichkeiten selbst chiffriert werden können.

Die „Enigma"-Chiffriermaschine kann auch als gewöhnliche Schreibmaschine verwendet werden und gestattet, beliebig Klartext und chiffrierten Text abwechseln zu lassen, so daß man sich darauf beschränken kann, nur die geheimen Stellen eines Briefes, beispielsweise Preise oder dergleichen, zu chiffrieren.

Das Chiffriersystem der „Enigma"-Chiffriermaschine.

Das Chiffriersystem der „Enigma"-Chiffriermaschine besteht darin, daß die Chiffrierbuchstaben mehr als 600 000 Tauschalphabeten entnommen werden, von denen sich selbsttätig nach jedem Buchstaben ein anderes einschaltet. Ein Teil dieser Tauschalphabete wird innerhalb einer Periode, d. h. bis zur mechanischen Rückkehr der Chiffrier-Mechanismen in ihre Anfangsstellung mehrmals, jedoch immer in ganz anderer Reihenfolge angewendet. Die Länge einer Periode ist etwa 1 000 000 Buchstaben, d. h.: erst nach etwa 1 000 000 mit dem gleichen Schlüssel geschriebenen Buchstaben tritt wieder die gleiche Tauschalphabetfolge auf. Es könnte also ein Buch von ca. 450 Druckseiten in der Größe dieses Prospektes chiffriert werden, ohne eine Periode zu erschöpfen. Die Maschine verfügt nun über etwa 22 000 verschiedene derartige Perioden. Die außerordentlich große Zahl von Tauschalphabeten und die in dem Mechanismus der Maschine begründete ungeheure Variationsfähigkeit in der Reihenfolge der einzelnen Alphabete bewirken, daß innerhalb der Periodenlänge von 1 000 000 Buchstaben auch nicht einmal Ähnlichkeiten vorkommen. Infolgedessen findet der unbefugte Entzifferer keinerlei Anhalt für seine Arbeit. Erfahrungsgemäß ist ein Chiffrat erst dann lösbar, wenn eine größere Anzahl, allerwenigstens aber 20 mit gleichem Schlüssel geschriebene Textstellen vorliegen und als solche erkannt werden können. Nun bietet aber die Maschine die Möglichkeit, 22 Milliarden verschiedene Schlüssel zu verwenden. Es kann deshalb jedes Chiffrat mit einem anderen Schlüssel geschrieben werden, sodaß das Sammeln der zur unbefugten Entzifferung notwendigen, mit dem gleichen Schlüssel geschriebenen Chiffrate vollkommen unmöglich ist. Die große Anzahl der möglichen Schlüsselein-

stellungen bietet auch eine Gewähr dafür, daß niemand, der sich unbefugter Weise in den Besitz einer ganz gleichartig gebauten und in allen Teilen gleichgeschalteten Maschine gesetzt hat, den verabredeten Schlüssel durch Probieren herausfinden kann. Dies zeigt folgende Überlegung: falls jemand ununterbrochen Tag und Nacht in jeder Minute einen neuen Schlüssel einstellte, so wären rund 42000 Jahre erforderlich, um alle Einstellungsmöglichkeiten zu erschöpfen.

Die Konstruktion der „Enigma" - Chiffriermaschine.

Das Grundelement der „Enigma"-Chiffriermaschine ist ein Walzensystem, mit Hilfe dessen durch Herstellung elektrischer Verbindungen die Tauschalphabete gebildet und dauernd vertauscht werden. Das Walzensystem ist einerseits mit der Tastatur s (s. Abb.), andererseits mit der Schreibvorrichtung verbunden, welche mit Hilfe eines rotierenden Typenrades v einen dem angeschlagenen Buchstaben entsprechenden, von der jeweiligen Stellung des Walzensystems abhängigen chiffrierten Buchstaben zu Papier bringt. Die Anfangsstellung des Walzensystems — der Schlüssel — wird mit Hilfe der kordierten Griffe a, b, c, d, gemäß den getroffenen Vereinbarungen eingestellt, und zwar die ersten vier Buchstaben des aus acht Buchstaben bestehenden Schlüssels, welche in den Fenstern e, f, g, h, sichtbar sind, mit halbhineingeschobenen Griffen a-d, die folgenden vier Buchstaben, welche in den Fenstern i, j, k, l, erscheinen, mit ganz hineingeschobenen Griffen a-d. Nach bewirkter Einstellung sind die vier Griffe a-d soweit wie möglich herauszuziehen.

Die „Enigma"-Chiffriermaschine enthält weiter ein Zählwerk, das jeden chiffrierten Buchstaben selbsttätig zählt. Der Stand ist an den Fenstern n erkenntlich. Mittels des kordierten Griffes m und des Hebels p kann das Zählwerk vor Beginn des Chiffrierens auf Null gestellt werden und zeigt dann in jedem Augenblick die Anzahl der seit Beginn der Arbeit chiffrierten Buchstaben an. Werden mehrere Chiffrate hintereinander geschrieben, die für verschiedene Empfänger bestimmt sind, ohne daß die Maschine jedesmal auf Null gestellt wird, so muß den Empfängern, denen ja nur der Anfangsschlüssel bekannt ist, die Zahl mitgegeben werden, bei der das betreffende Chiffrat beginnt. Zu diesem Zweck wird vor Beginn des betreffenden Chiffrats der Hebel o auf „Klarschrift" umgestellt und die Stellung des Zählwerks, sowie die Adresse und sonstige unwichtige Mitteilungen in Klarschrift niedergeschrieben. Während dies geschieht, bewegt sich der Chiffrier-Mechanismus nicht weiter, sodaß beim nunmehrigen Wiederumschalten auf „Chiffrieren" das Chiffrat an der Stelle der Periode wieder ein-

setzt, an welcher das vorangegangene aufgehört hat. An jeder beliebigen Stelle des Chiffrats kann Klartext eingeschaltet werden.

Besonderer Wert ist darauf gelegt, daß beim Dechiffrieren in jedem Augenblick festgestellt werden kann, ob die dechiffrierte Maschine genau an der gleichen Stelle der Periode arbeitet, an welcher die chiffrierende Maschine gearbeitet hat, d. h., ob z. B. der als 3265ster chiffrierte Buchstabe auch als 3265ster dechiffriert wird, da dies Vorbedingung für die richtige Entzifferung ist. Zu diesem Zweck stellt die Maschine selbsttätig Gruppen von fünf Buchstaben her und ordnet diese zu je zehn Gruppen in einer Zeile an, sodaß jede Zeile 50 Buchstaben enthält. Es kann also bei vorkommenden Fehlern sofort die Stelle des Fehlers ermittelt und das Dechiffrieren wiederholt werden, nachdem der Chiffrier-Mechanismus mit Hilfe der Kurbel r auf die fragliche Zahl eingestellt worden ist. Wenn der Fehler beim Absender oder bei der telegrafischen Übermittelung vorgekommen ist, so kann, wenn der richtige Text sich nicht durch sinngemäße Ergänzung des dechiffrierten Textes herstellen läßt, die Berichtigung dadurch vorgenommen werden, daß man sich die in Frage kommenden Gruppen — und zwar nur diese — nochmals wiederholen läßt.

Das Entziffern wird in der Weise vorgenommen, daß das ankommende Chiffrat nach Umstellung des Hebels o auf „Dechiffrieren“ ohne Rücksicht auf die Gruppenabstände auf der Maschine abgeschrieben wird. Es erscheint dann der ursprüngliche Klartext in genau derselben Weise, wie er vom Absender niedergeschrieben worden ist, d. h. mit allen Wortabständen, Ziffern und Interpunktionszeichen. Es brauchen natürlich nur die Teile der Mitteilung umgeschrieben werden, welche chiffriert ankommen, während die in Klarschrift geschriebenen Teile, die ja ohne weiteres verständlich sind, übergangen werden.

Gebrauchsanweisung.

(Vergl. Abb.)

Einstellung des Schlüssels.

An der rechten Seite der Chiffriermaschine befinden sich vier kordierte Griffe a—d. Von diesen wird zunächst der oberste Griff a nach Lösen einer Feststellvorrichtung soweit als möglich in die Maschine hineingeschoben und dann zur Hälfte wieder herausgezogen. In dieser Lage des Griffes kann durch Drehen an ihm die erste Walze verstellt werden, bis der gewünschte Schlüsselbuchstabe in dem Fenster e erscheint. Darauf wird der Griff a ganz hineingeschoben und in dieser Lage solange gedreht, bis in dem Fenster i neben dem Griff der fünfte Schlüsselbuchstabe sichtbar wird. Dann ist der Griff wieder ganz herauszuziehen. In gleicher Weise werden mit den anderen Griffen b, c und d die weiteren sechs Schlüsselbuchstaben eingestellt. Damit ist die Schlüsseleinstellung beendet.

Das unter dem Fenster n sichtbare Zählwerk ist zu Anfang der Chiffrier-Periode auf Null einzustellen. Zu diesem Zweck wird der an der linken Seite der Maschine liegende Hebel p mit der rechten Hand an die Maschine herangedrückt und der daneben liegende Griff m mit der linken Hand gedreht, bis die Nullstellung erreicht ist.

Chiffrieren.

Der an der Maschine vorn angebrachte Hebel o wird auf „Chiffrieren" gestellt und der Wagen mit der Schreibwalze soweit wie möglich nach rechts geschoben. Hierauf wird der Motor eingeschaltet und mit dem Schreiben begonnen. Am Anfang ist die Taste „Buchstaben-Zwischenraum" oder die Taste „Zahlen-Zeichen-Zwischenraum" anzuschlagen, je nachdem, ob der Text mit einem Buchstaben oder einer Zahl anfängt.

Auf der Maschine wird geschrieben wie auf einer gewöhnlichen Schreibmaschine, es ist nur darauf zu achten, daß die Tasten nicht zu kurz angeschlagen werden. Die Umschalttasten sind jedoch im Gegensatz zur Schreibmaschine loszulassen, bevor die umzuschaltende Taste angeschlagen wird. Soll also z. B. ein Komma geschrieben werden, so wird die Taste „Zahlen-Zeichen-Zwischen-

raum" niedergedrückt und wieder losgelassen. Dann erst wird die Taste n, auf der sich auch das Komma befindet, angeschlagen. Sollen nach dem Komma wieder Buchstaben geschrieben werden, so muß vorher die Umschalttaste „Buchstaben-Zwischenraum" angeschlagen werden. Beim Schreiben von Buchstaben erhält man einen Zwischenraum durch Anschlagen der „Buchstaben-Zwischenraum"-Taste, beim Schreiben von Ziffern und Zeichen dagegen durch Anschlagen der „Ziffern-Zeichen-Zwischenraum"-Taste. Die Buchstaben ä, ö, ü können beim Chiffrieren nicht in einem Zeichen geschrieben werden, sondern müssen durch ae, oe, ue ersetzt werden.

Dechiffrieren.

Zunächst wird in der beschriebenen Weise der Schlüssel eingestellt, dann der Hebel o auf „Dechiffrieren" gestellt und der Wagen soweit wie möglich nach rechts geschoben. Beim Niederschreiben des Chiffrates ist auf die Gruppenabstände keine Rücksicht zu nehmen. Für die Buchstaben ä und ü sind die beiden Tasten „Ziffern-Zeichen-Zwischenraum" bezw. „Buchstaben-Zwischenraum", auf denen sich auch die Buchstaben ä und ü befinden, anzuschlagen. Hin und wieder ist darauf zu achten, daß das Zählwerk mit der Anzahl der bisher geschriebenen Buchstaben übereinstimmt.

Besonderes.

Das Chiffrieren kann in jedem Augenblick unterbrochen und Klartext weitergeschrieben werden. Dazu ist es nur erforderlich, den Hebel o auf „Klartext" zu stellen. Solange Klartext geschrieben wird, bleibt das Zählwerk und der Chiffrier-Mechanismus stehen. Bei Fortsetzung des Chiffrierens ist der Hebel o auf „Chiffrieren" und der Wagen an die Stelle zu stellen, wo das vorangegangene Chiffrat aufgehört hat. Nach Schreiben einer vollen Zeile von 50 Buchstaben wird die Maschine sowohl beim Chiffrieren als Dechiffrieren automatisch stillgesetzt und arbeitet erst weiter, wenn der Wagen der Schreibvorrichtung wieder auf den Anfang der Zeile gestellt ist. Zum blinden Weitertransport des Wagens dient die Taste u.

Instandhaltung.

Von Zeit zu Zeit sind alle bewegten Teile der Maschine mit gutem harzfreiem Öle zu schmieren. Um an die bewegten Teile der Maschine leicht herankommen zu können, können die Blechverkleidungen der Maschine leicht entfernt werden.

Die Chiffriersicherheit der „Enigma"-Chiffriermaschine.

Die „Enigma"-Chiffrier-Maschine mit Tausch-Alphabeten arbeitet mit nach jedem Buchstaben wechselnden Tausch-Alphabeten. Die gleichen Tauschalphabetfolgen treten erst nach etwa einer Million Buchstaben wieder ein, d. h. die Periodenlänge dieser Maschine beträgt eine Million. Von den Perioden dieser Länge sind etwa 22000 in der Maschine. Ein einziges Chiffrat von jeder praktisch vorkommenden Länge (viele Folioseiten), welches mit der „Enigma"-Chiffrier-Maschine ausgeführt wird, muß als prinzipiell unlösbar gelten, da die Anzahl der durch die Maschine herstellbaren Tausch-Alphabete so groß, und die Variationsfähigkeit, mit der diese einzelnen Tausch-Alphabete hintereinander gereiht werden, so durchgreifend ist, daß Aehnlichkeiten innerhalb der Periode von etwa einer Million Buchstaben nicht auftreten.

Eine prinzipielle Lösungsmöglichkeit tritt erst ein, wenn eine große Anzahl von Chiffraten aus der gleichen Periode und von genau den gleichen Stellen dieser Periode vorliegen.

Es liegt aber in dem System der Maschine, daß bei Befolgung einfacher Betriebs-Vorschriften, wie sie weiter unten noch gekennzeichnet sind, die Möglichkeit gegeben ist, bei intensivstem Chiffrierbetrieb über Jahre hinaus nie mit demselben Schlüssel zu arbeiten. Hierdurch kann die Eventualität, Telegramme mit gleichchiffrierten Anfängen abzugeben, praktisch vollkommen ausgeschlossen werden. Für den unberufenen Entzifferer bleibt dann die einzige Möglichkeit für den Fall, daß ihm ein ungeheuer großes Material vorliegt, aus diesem Material zunächst einmal 2 Stellen herauszufinden, welche an der gleichen Stelle derselben Periode geschrieben sind. Bei der enormen Länge der einzelnen Perioden und der großen Anzahl der Perioden ist schon die Wahrscheinlichkeit, daß derartige nach dem gleichen Prinzip chiffrierte Stellen überhaupt v o r h a n d e n sind, ganz außergewöhnlich unwahrscheinlich. Als noch viel unwahrscheinlicher muß es aber gelten, diese Stellen, die nur unter ganz besonderen Zufälligkeiten als solche zu erkennen sind, nun auch wirklich zu finden; denn die Wahrscheinlichkeit der auffindbaren unter den vorhandenen Parallelstellen ist so gering, daß nur eine genaue Durcharbeit eines ungeheuren Materials die Feststellung solcher Stellen ermöglichen könnte.

Der große Umfang des notwendigen Materials erfordert außerdem ganz besondere Vorsichtsmaßregeln bei der Aufsuchung der Parallelstellen, da nach Möglichkeit ausgeschlossen werden muß, daß zwischen die echten Parallelstellen scheinbare Parallelstellen kommen, die in Wirklichkeit keine sind. Diese Vorsichtsmaßregel bedeutet, daß das Verhältnis der auffindbaren zu den wirklich vorhandenen Parallelstellen noch wesentlich kleiner wird.

Sollte es aber wirklich einmal gelungen sein, zwei Texte der gleichen Periode und genau der gleichen Stelle dieser Periode als solche erkannt zu haben, so ist hiermit eine Entzifferung noch nicht möglich. Vielmehr müssen von derartigen Texten im allergünstigsten Falle zwanzig bis dreißig, meistens aber wesentlich mehr vorhanden sein.

Die einzige Anweisung, die dem Chiffrierenden zu geben ist, um zu vermeiden, daß mehrere Telegramme an den gleichen Stellen einer Periode anfangen, ist die, daß ein je nach der Menge der gesamten chiffrierten Texte monatlich, wöchentlich oder täglich zu wechselnder Grundschlüssel, der vorher verabredet ist, benutzt wird, und daß jedes Telegramm außerdem einen individuellen Schlüssel von ein oder zwei Buchstaben erhält, welcher aber unbeschadet der Sicherheit der Maschine dem Telegramm mitgegeben werden kann. Dieser Schlüssel, in geeigneter Weise kombiniert mit dem vorher verabredeten Grundschlüssel, verändert sowohl die Stelle in der Periode, als auch die Periode selbst in weitgehendster Variation, sodaß hierdurch jedes einzelne Telegramm wieder mit einer anderen Periode chiffriert wird. Wird diese einzige Betriebsvorschrift beachtet, der Art, daß möglichst jedes Telegramm an einem Tag einen andern individuellen Schlüssel erhält, was durch die Auswahl aus einer Tabelle für die individuellen Schlüssel in einfachster Weise möglich ist, so hat der Chiffrierende nicht notwendig, irgendwelche Vorsicht mit Rücksicht auf gleiche Telegrammanfänge oder häufigere Verwendung gleicher Worte, Stellung von Subjekt und Prädikat im Satz oder dergleichen, walten zu lassen. Er ist mit Bezug auf den übermittelten Text vollkommen frei und hat dabei bei der Maschine noch den Vorteil, den Text mit Buchstaben, Ziffern, Zeichen und Abständen geben zu können, wie einen normalen Schreibmaschinenbrief, eine Verbesserung, die bei den meisten anderen Chiffrier-Verfahren mit Bezug auf die Chiffrier-Sicherheit sehr gefährlich werden könnte. Bei Berücksichtigung der angegebenen einfachen Betriebsvorschrift kann nicht nur ein Telegramm als solches, sondern auch ein ausgedehnter Chiffrierverkehr mit der „Enigma"-Chiffriermaschine als unbedingt sicher gelten, falls keine Entwendung der Maschine und keine Veruntreuung der Schlüssel vorkommen.

Die Gesellschaft baut noch eine zweite Chiffriermaschine, welche das Chiffrier=System der Tausch=Alphabete mit dem der Umwürfelung kombiniert. Bei dieser müßte die Anzahl der Texte, die an der gleichen Stelle einer Periode chiffriert sind und als solche erkannt werden können, noch ganz bedeutend größer sein, sodaß die Sicherheit dieses Systems auch dann noch gewahrt bliebe, wenn die Betriebsvorschriften für die Chiffrierung nicht mit aller Strenge eingehalten würden.

Werden Codes chiffriert, so erhöht sich die Sicherheit theoretisch noch bedeutend. Als sehr wesentlich muß noch hervorgehoben werden, daß die Lösung eines Telegrammes auf irgend eine Weise, sei es durch Verrat des Schlüssels oder dadurch, daß ein dem chiffrierten Text zu Grunde liegender Klartext durch Verrat bekannt geworden sei, auch nicht die leisesten Anhaltspunkte gibt für die Lösung von anderen Telegrammen, wenn sie auch mit derselben Maschine, jedoch mit anderen Perioden oder an anderen Stellen derselben Periode chiffriert sind.

Der Besitz einer Maschine mit absolut gleicher Konstruktion und Schaltung, wie diejenige Maschine, mit der das Telegramm chiffriert ist, erleichtert dem unberufenen Entzifferer seine Arbeit so unwesentlich, daß für die Beurteilung der Chiffrier=Sicherheit diese Erleichterung praktisch als Null angesehen werden kann. Das gleiche gilt für den Fall, daß dem Entzifferer die genauen Schaltungs=Schemata und Konstruktions=zeichnungen zur Verfügung ständen, die er sich ja übrigens aus der Maschine auch verschaffen könnte.

Zusammenfassend kann das Ergebnis der obigen Betrachtung folgendermaßen festgelegt werden:

1) Mit der „Enigma"=Chiffriermaschine können Texte praktisch beliebiger Länge ohne Schlüsseländerung von Hand und ohne die Gefahr der Entzifferungsmöglichkeit übermittelt werden. Dies bedeutet, daß auch die geheimsten schriftlichen Mitteilungen unbedenklich der Post anvertraut werden können, eine Möglichkeit, die weder bei einem Schreibverfahren noch mit einer der bisher bekannten Maschinen, welche meistens mit einer sehr kurzen Periode arbeiten, vorhanden ist, denn ein ähnlich langer Text würde bei diesen Verfahren unbedingt die Handhabe zur unberufenen Entzifferung bilden. Es kommt hinzu, daß lange Texte schriftlich wegen der zur Ver= und Entzifferung notwendigen Zeit praktisch nicht hergestellt werden können.
2) Der Chiffrierverkehr mit der „Enigma"=Chiffriermaschine ist bei Beachtung einfacher Betriebsvorschriften als vollkommen sicher anzusehen. Die Betriebsvorschriften bestehen darin, das ein Grundschlüssel des öfteren gewechselt wird, und daß jedem Telegramm ein individueller Schlüssel mitgegeben wird. Die Frequenz, mit

welcher der Grundschlüssel gewechselt werden muß, und die Länge des individuellen Schlüssels richtet sich nach der Anzahl der im ganzen unter den verschiedenen Stellen ausgetauschten Telegramme.

3) Bei Beachtung der unter 4) angegebenen Betriebsvorschriften hat der Chiffreur besondere Rücksichten auf gleiche Anfänge der Telegramme, Häufigkeiten der Verwendung gleicher Worte, Variationen in der Stellung von Subjekt und Prädikat nicht zu nehmen. Die Maschine konnte daher auch, ohne die Chiffriersicherheit zu beeinträchtigen, zur Uebermittlung von Buchstaben, Zahlen, Satzzeichen und Wortabständen konstruiert werden, was einerseits die Textlänge verkürzt und andererseits die gute Lesbarkeit des Dechiffrates erhöht.

4) Da ein Chiffrier-System oder eine Chiffrier-Maschine prinzipiell unmöglich ist, mit Hülfe deren auch der Unberufene bei Kenntnis sämtlicher Schlüssel einen Text nicht lösen könnte, so ist die Sicherheit der „Enigma"-Chiffriermaschine soweit getrieben, wie es prinzipiell überhaupt möglich ist. Die einzige Möglichkeit der Entzifferung besteht damit aber für den unberufenen Entzifferer auch in der Beschaffung einer genau gleichen Maschine und der jeweiligen Schlüssel. Auf die Geheimhaltung der Schlüssel ist daher ganz besondere Sorgfalt zu verwenden. Hierfür können noch verschiedene Vorsichtsmaßregeln Anwendung finden; beispielweise kann die Schlüsseleinstellung auf sämtlichen Stellen durch zwei oder mehr Personen erfolgen, der Art, daß jede Person nur einen Teil des Schlüssels einstellt, und daß keiner Person der ganze Schlüssel bekannt ist. Außerdem können beim geringsten Verdacht Reserveschlüsseltabellen verwendet werden, oder die vorhandenen Tabellen in anderer Art benutzt werden und zwar in der Weise, daß die Veränderung eintritt, wenn der ursprünglich geltende Schlüssel nicht mehr zur Entzifferung führt.