CHIFFRIEREN MIT GERÄTEN UND MASCHINEN

Eine Einführung in die Kryptographie

von

DOZENT DR. SIEGFRIED TÜRKEL

Wissenschaftl. Leiter des Kriminalistischen
Institutes der Polizei-Direktion Wien

GRAZ 1927

Verlag von Ulr. Mosers Buchhandlung (J. Meyerhoff)

CHIFFRIEREN MIT GERÄTEN UND MASCHINEN

Eine Einführung in die Kryptographie

von

DOZENT DR. SIEGFRIED TÜRKEL

Wissenschaftl. Leiter des Kriminalistischen
Institutes der Polizei-Direktion Wien

GRAZ 1927

Verlag von Ulr. Mosers Buchhandlung (J. Meyerhoff)

Universitäts-Buchdruckerei „Styria“ in Graz

Herrn Univ.-Prof. Dr. Egon Ranzi

in Dankbarkeit und Verehrung
gewidmet

vom Verfasser

I.

Eine unverändert niedergeschriebene Mitteilung nennt man in der Kryptographie einen „Klartext", da der Inhalt der Mitteilung jedem dieser Sprache Mächtigen klar ist. Verschiedenartige Gründe können den Absender bestimmen, den Klartext seiner Mitteilung derart zu verändern, daß diese uneingeweihten Lesern unverständlich werde.

Um eine Mitteilung in eine Geheimmitteilung (Geheimschrift) zu verwandeln, kann man z. B. den Klartext derart mit textfremden Buchstaben oder Silben durchsetzen, daß der sprachliche Zusammenhang zerrissen und der Gedankeninhalt unverständlich wird. Derartige eingeschaltete textfremde Buchstaben oder Silben nennt man Nieten, Blender oder Non valeurs.

Nehmen wir z. B. an, der Absender der Geheimmitteilung (Geheimschreiber, Chiffreur) hätte mit dem eingeweihten Empfänger der Mitteilung (Entzifferer, Dechiffreur) verabredet, daß jeweils vor den ersten Buchstaben der Klarschrift ein, vor den zweiten Buchstaben der Klarschrift zwei, vor den dritten Buchstaben drei textfremde Buchstaben eingeschaltet werden und daß sich diese Einschaltungen immer wieder serienweise wiederholen, dann würde die Mitteilung „Leugne alles" mit Nieten durchsetzt folgendes Bild geben:

SLOWEREFUAGSKNOFTEPAKVLFGULAESJSJRK.

Hat der Geheimschreiber mit dem Entzifferer vereinbart, daß der Geheimtext in gleiche Gruppen, z. B. von je fünf Buchstaben, geteilt werde, dann würde obiger Text lauten:

SLOWE REFUA GSKNO FTEPA KVLFG ULAES JSJRK.

Ein primitives Beispiel für die Einschaltung textfremder Silben ist die bekannte „Be"-Sprache der Kinder.

Die Einschaltung textfremder Silben kann mit der Einschaltung textfremder Buchstaben kombiniert werden.

Klartext: Leug - ne - al - les

Silbenvernietung: Alt - leug - schaft - ne - von - al - ist - les.

Hiezu Buchstabenvernietung: rasgloqwtelbqemvhuyg etc.[1])

Kehren wir der Einfachheit halber zur Geheimschrift durch Einschaltung textfremder Buchstaben zurück.

Zur leichteren Herstellung einer Buchstabennietenschrift kann man sich eines einfachen Behelfes bedienen. Man schneidet einen Pappendeckel in der Größe des zu beschreibenden Briefpapieres. Auf diesen z. B. rechteckigen Pappendeckel zeichnet man so viele Quadrate, als man auf eine Seite des zu beschreibenden Briefpapieres Buchstaben schreiben will. Jene Quadrate, welche die Stellen der Nieten bezeichnen, werden nicht ausgestanzt. Jene Quadrate aber, welche die Stellen der durch die Nieten auseinanderzureißenden Buchstaben des Klartextes anzeigen, werden lochförmig oder quadratisch ausgestanzt.

Der Geheimschreiber legt diesen ausgestanzten Pappendeckel, „Gitter" genannt, auf das Blatt Papier. In die ausgestanzten Öffnungen schreibt er seinen Klartext. Dann legt er das Gitter sozusagen als „Faulenzer" unter das Papier. Jene Stellen, wo die nicht durchgestanzten vorgezeichneten Quadrate des Gitters durchleuchten, füllt er mit Nieten aus.[2])

Dieses Gitter ist ein technisches Hilfsmittel, welches dem Geheimschreiber das Vernieten des Klartextes und dem Entzifferer das Verdecken der Nieten und das Lesen des Klartextes erleichtert.

Zur Erhöhung der Sicherheit des geheimen Schriftwechsels wird die Gittertype z. B. an bestimmten Tagen oder nach einer bestimmten Anzahl von Mitteilungen gewechselt werden müssen.

Da es zu umständlich wäre, stets eine größere Anzahl von Gittertypen bereitzuhalten oder mit sich zu führen, lag es nahe, ein Gerät zu konstruieren, bei welchem durch Verschiebung oder Drehung seiner Bestandteile die Gittertype jeweils in eine neue Gittertype umgewandelt werden kann. Ein solches veränderliches Gerät ist in Tafel A, Fig. I, abgebildet. Das Gerät besteht aus einem äußeren, höherliegenden (2), und einem

---

1) Nach der gleichen Vernietungsformel wie oben:

$$1 + x + 2 + y + 3 + z + 1 + x \text{ etc.}$$

2) Vgl. das deutsche Reichspatent Nr. 89.897 (ausgegeben 17. Dezember 1896, Beginn 12. März 1896), weiters 273 (Beginn 2. Juli 1877).

inneren, tieferliegenden Rahmen (1). Dieser innere Rahmen ist durch eine kleine Leiste (3) in eine obere und eine untere rechteckige Hälfte geteilt. Die beiden Rahmenhälften gestatten, vier Gitterplättchen oberhalb und vier Plättchen unterhalb der Leiste 3 auf den inneren Rahmen (1) nebeneinander aufzulegen. Die acht Gitterplättchen lassen sich untereinander vertauschen. Jedes der Gitterplättchen (z. B. 4 und 5) läßt sich überdies, da es rechteckig ist, an derselben Stelle des Rahmens in zwei Lagen verwenden. Die schmale Rechteckseite des Plättchens, die in der einen Lage die Leiste 3 berührt, wird in der andern Lage (Drehung um 180°) den Rahmen 2 berühren.

Das Gitterplättchen 4 z. B. gibt:

in der einen Lage das Bild:	in der andern Lage das Bild:
S W W S[3])	W S W W
W S W W	W W W S
W W S W	W S W W
S W W W	W W S W
W W S W	S W W S

Dieses in Tafel A, Fig. I, abgebildete Gittergerät besteht angesichts der Umkehrungsmöglichkeit jedes der acht Gitterplättchen also sozusagen aus 16 Gitterplättchen und gestattet daher $1 \times 2 \times 3 \ldots . \times 16$ Variationen.

Es existieren verschiedenartige, teils ähnlich, teils anders konstruierte Gittergeräte, welche eine handliche Verwendung ein und desselben Gitters bei Schreibpapieren verschiedener Größe ermöglichen oder welche bei Anwendung desselben Gerätes die Verwendung verschiedener Gittertypen gestatten.[4])

[3]) „S" bedeutet „schwarz", d. h. ein ausgestanztes, „W" bedeutet „weiß", d. h. ein nicht ausgestanztes Quadrat.

[4]) So beschäftigt sich das am 28. Mai 1925 ausgegebene deutsche Patent Nr. 414.283 (Beginn des Patentschutzes 7. März 1924) mit einem Gitter, welches zwecks Eintragung der zu versetzenden Buchstaben gelöchert ist. Jedes solche Gitter hat eine besondere Löcherverteilung. Jedes solche Gitter ist gegen andere Gitter mit anderer Löcherverteilung auswechselbar. Diese Gitter können über ein darunter befindliches Schreibblatt schrittweise bewegt werden. Auf dem Schreibblatte ist entsprechend der zu chiffrierenden Buchstabenanzahl der zur Aufnahme des Chiffrates bestimmte Raum einstellbar. Vgl. auch das Patent Unit. St. 1,370.870.

Ein ähnlicher technischer Behelf beruht wiederum auf einer andern Methode der Geheimschrift, der sogenannten „Versetzungsmethode".

Der Geheimschreiber kann seinen Klartext für den uneingeweihten Leser schwer entzifferbar machen, wenn er — ohne diesen Klartext mit Nieten zu durchsetzen — die Buchstaben des Klartextes in einer bestimmten Weise versetzt.

Schon seit dem 3. Jahrhunderte v. Chr. ist unter dem Namen „Anagramm" eine angeblich von Lykophron erfundene Methode bekannt, durch Versetzung der Buchstaben neue Wörter und neue Sätze zu bilden.[5]) Noch in der Neuzeit bedienten sich Gelehrte dieser Methode, wenn sie anderen Männern der Wissenschaft Mitteilungen machen wollten, die vorläufig nur für den engen Kreis der Fachkollegen bestimmt waren. Galilei z. B. beschrieb 1610 den Saturn als eine große Kugel mit zwei Kügelchen an jeder Seite. Andere Astronomen glaubten eine Kugel mit henkelartigen Ansätzen zu sehen. Erst dem Astronomen Huygens gelang die Lösung des Rätsels. Er wagte jedoch nicht, der Öffentlichkeit seine Entdeckung sofort bekanntzugeben. Er wollte vielmehr erst die Bestätigung derselben durch zukünftige Beobachtungen abwarten. Am Schlusse einer seiner wissenschaftlichen Arbeiten über den hellsten Saturntrabanten findet sich folgendes Anagramm:

aaaaaaa ccccc d eeeee g h iiiiii llll mm nnnnnnnnn oooo pp q rr s ttttt uuuuu.

Dieses Anagramm heißt richtig gelesen:

„Annulo cingitur tenui, plano, nusquam cohaerente, ad eclipticam inclinato."[6])

Auf einer Buchstabenversetzung beruhte auch die griechische Methode des Schreibens mit Hilfe des Briefstabes, eines höchst einfachen Chiffriergerätes. Absender und Empfänger hatten genau gleich gedrechselte Geheimbriefstäbe. Der Absender wickelte um seinen Stab einen Riemen und schrieb seinen Text in der

---

5) Vgl. Lalanne: Curiosités Littéraires (Paris 1857); Wheatley: On anagrams etc. (London 1862); Dobson: Literary frivolities (London 1880).

6) „Er wird von einem dünnen, ebenen, nirgends (mit Saturn) zusammenhängenden, gegen die Ekliptik geneigten Ringe umgürtet." (Vgl. Newcomb-Engelmann, Astronomie, 5. Aufl., 1914, S. 423 ff.)

Längsrichtung des Stabes, also quer über die Riemenspirale. Dann wurde der Riemen vom Stabe abgewickelt und ohne Geheimstab an den Adressaten gesandt. Der Adressat besaß einen Geheimstab derselben Länge und Dicke und dechiffrierte mittels desselben den Text.[7])

Auch dem in der Kryptographie nicht bewanderten Laien ist eine Methode der Versetzung bekannt, der sogenannte Rösselsprung, eine Form des Silbenrätsels. Nach derselben Methode, also nach Art der Schachzüge, können selbstverständlich auch einzelne Buchstaben versetzt werden.

Das Schreibpapier stellt ein oder mehrere Schachbretter dar. Die Buchstaben werden vom Chiffreur in die einzelnen Schachbrettfelder eingeschrieben. Die zusammengehörigen Buchstaben sind vom Dechiffreur im Sinne vereinbarter Schach- oder schachähnlicher Züge durch Striche miteinander zu verbinden und ergeben dann den Klartext.

Der Chiffreur bedient sich zur Herstellung solcher Geheimschriften eines Faulenzers, auf welchem der Platz für den Buchstaben mit einer schwarzen Kreisfläche, die Zugrichtung mit einer schwarzen Linie bezeichnet erscheint. Auf diesen Chiffrierfaulenzer legt er ein weißes Papier, welches den Faulenzer durchscheinen läßt. Der Dechiffreur hat eine ganz gleiche Zeichnung auf einer durchsichtigen Cellit- oder Zelluloidplatte angebracht. Die Stelle der Buchstaben ist durch eine schwarze Kreislinie, die Richtung des Zuges durch eine schwarze Linie angedeutet. Er legt diese Cellitplatte auf die Geheimschrift und faßt — die Züge des Chiffreurs wiederholend — die zusammengehörigen Buchstaben zu Worten und Sätzen zusammen.

Die in der Praxis am häufigsten zur Anwendung kommenden Versetzungsmethoden sind die Richtungsmethoden, d. h. die Methoden der Buchstabenversetzung in bestimmten horizontalen und vertikalen Richtungen. Diese Geheimschriften werden oft auch kurz, je nach ihren Kriterien, als Verkehrtschriften, Zeilenschriften, Spaltenschriften od. dgl. bezeichnet.

---

[7]) Vgl. Dr. Franz Feldhaus, Die Polizei und Technik (aus „Abegg: Die Polizei in Einzeldarstellungen"), S. 91, wo unter Abb. 49 eine im Postmuseum zu Berlin befindliche Nachbildung eines solchen in Griechenland schon zur Zeit Lysanders (405 v. Chr.) in Verwendung gestandenen Geheimschriftstabes abgebildet ist.

Diese Richtungsmethoden sind am besten geeignet, neben der „Versetzung im engeren Sinne“ auch die „Verwürfelung im engeren Sinne“ verständlich zu machen.

Zuerst ein einfaches Beispiel der spaltenweisen Versetzung:[8])

Nehmen wir z. B. an, der Schreiber der Mitteilung: „Verbrenne alle Papiere, entleere die Kassa, beseitige Akte“ würde kolonnenweise, u. zw. stets in die erste Kolonne von oben nach unten, in die zweite Kolonne von unten nach oben, in die dritte Kolonne von oben nach unten, in die vierte Kolonne von unten nach oben usw., also seinen Klartext im Zickzack niederschreiben, so würde die Geheimschrift folgendes Bild ergeben:

1	2	3	4	5	6	7
V	P	A	E	D	T	I
E	E	P	R	I	I	G
R	L	I	E	E	E	E
B	L	E	E	K	S	A
R	A	R	L	A	E	K
E	E	E	T	S	B	T
N	N	E	N	S	A	E

In horizontaler Linie, also zeilenweise gelesen, würde die Mitteilung lauten:

VPAEDTI EEPRIIG etc.

In Gruppen zu fünf Buchstaben geordnet, würde diese Mitteilung lauten:

VPAED TIEEP RIIGR LIEEE EBLEE KSARA RLAEK EEETS BTNNE etc.

Dies ein Beispiel der vertikalen Zickzackmethode oder des Schreibverfahrens in vertikaler Schlangenlinie.

Wenn jedoch der Geheimschreiber seinen Klartext unvernietet und wie jede andere Klarschrift zeilenweise niederschreibt und diesen Klartext nunmehr nach bestimmten, mit dem De-

[8]) Figl z. B. zählt in seinem „Systeme des Chiffrierens“ als Methoden der Versetzung auf: Die hebräische Methode der Verkehrtschrift, die chinesische Methode der Spaltenschrift, den Würfel, u. zw. den einfachen Würfel, den Würfel mit Zeilenversetzung, den Nihilistenwürfel, den Doppelwürfel etc.

chiffreur getroffenen Vereinbarungen „verwürfelt", dann spricht man von einer Verwürfelungsmethode.[9])

Ein Beispiel soll dies klarmachen.

1	3	7	2	5	4	6
V	E	R	B	R	E	N
N	E	A	L	L	E	P
A	P	I	E	R	E	E
N	T	L	E	E	R	E
D	I	E	K	A	S	S
A	B	E	S	E	I	T
I	G	E	A	K	T	E

Die über dem horizontalen Striche angebrachten arabischen Ziffern sind Indizes, welche anzeigen, in welcher Reihenfolge die Spalten zu verwürfeln sind.

Der verwürfelte Text lautet:

1	2	3	4	5	6	7
V	B	E	E	R	N	R
N	L	E	E	L	P	A
A	E	P	E	R	E	I
N	E	T	R	E	E	L
D	K	I	S	A	S	E
A	S	B	I	E	T	E
I	A	G	T	K	E	E

In Gruppen zu fünf Buchstaben:

VNAND AIBLE etc. oder
VBEER NRNLE etc.

Man bezeichnet diese Methode gewöhnlich als den „einfachen Würfel". Man muß bei der Methode des einfachen Würfels selbstverständlicherweise nicht gerade „spaltenweise" verwürfeln.

Das folgende Beispiel zeigt eine einfache Verwürfelung mit zeilenweiser Verwürfelung.

---

[9]) Die Verwürfelungsmethode ist also eine der vielen „möglichen" Versetzungsmethoden. (Vgl. Anm. 8.)

Text vor der Verwürfelung:

6	V	E	R	B	R	E	N
4	N	E	A	L	L	E	P
7	A	P	I	E	R	E	E
2	N	T	L	E	E	R	E
5	D	I	E	K	A	S	S
3	A	B	E	S	E	I	T
1	I	G	E	A	K	T	E

Text nach der Verwürfelung:

1	I	G	E	A	K	T	E
2	N	T	L	E	E	R	E
3	A	B	E	S	E	I	T
4	N	E	A	L	L	E	P
5	D	I	E	K	A	S	S
6	V	E	R	B	R	E	N
7	A	P	I	E	R	E	E

In Gruppen zu fünf Buchstaben:

AVDNA NIPEI etc. oder
INAND VAGTB etc.

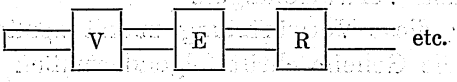
Die einfache Verwürfelung läßt sich auch mit „Geräten“ durchführen.

Es wird der noch unverwürfelte Text in einem Setzkasten, z. B. nach Art der Kinderspielzeuge (Bildersetzkasten) aus kleinen Holzwürfeln zusammengesetzt:

V	E	R	B	R	E	N

Jeder dieser Holzwürfel ist an zwei Stellen derart doppelt durchlocht, daß die ganze aus Holzwürfeln bestehende Zeile

mit einem haarnadelartigen Drahtinstrumente fixiert, gehoben und an eine andere Stelle des Setzkastens gebracht werden kann.



Ein komplizierteres Gerät besteht aus Streifen, welche z. B. bei der Methode des „einfachen Würfels mit spaltenweiser Verwürfelung“ von oben nach unten laufen, so daß auf diesen Streifen der Text fortlaufend horizontal geschrieben und dieser Text dann spaltenweise verwürfelt werden kann:

↓	↓	↓	↓ usf.									
V	E	R	B	R	E	N	N	E	A	L	L	E
P	A	P	I	E	R	E	E	N	T	L	E	E

etc.

etc.

An den Enden dieser aus einem festeren Materiale hergestellten Streifen sind nach Art der Buchdrucksetzmaschinen kleine Vorrichtungen angebracht, so daß der Streifen automatisch an jene Stelle gelangt, an welche er gemäß der Indexziffer gelangen soll.

Bisher wurde der „einfache Würfel mit spaltenweiser Verwürfelung“ und der „einfache Würfel mit zeilenweiser Verwürfelung“, jeder als selbständige Methode der „Verwürfelung“, dargestellt.

Es kann spalten- und zeilenweise Verwürfelung aber auch kombiniert werden. Im Falle dieser Kombination spricht man von der Methode des Doppelwürfels. Ein Beispiel wird dies erläutern:

	5	1	4	6	3	7	2
2	V	E	R	B	R	E	N
7	N	E	A	L	L	E	P
5	A	P	I	E	R	E	E
1	N	T	L	E	E	R	E
3	D	I	E	K	A	S	S
6	A	B	E	S	E	I	T
4	I	G	E	A	K	T	E

Die auf der Abszisse und auf der Ordinate, also spalten- und zeilenweise angebrachten Zahlen sind die Indizes für die beiden vorzunehmenden Verwürfelungen.

Führen wir diese Verwürfelung zuerst spaltenweise durch, so wird sich die Geheimschrift folgendermaßen darstellen:

	1	2	3	4	5	6	7
2	E	N	R	R	V	B	E
7	E	P	L	A	N	L	E
5	P	E	R	I	A	E	E
1	T	E	E	L	N	E	R
3	I	S	A	E	D	K	S
6	B	T	E	E	A	S	I
4	G	E	K	E	I	A	T

Verwürfelt man nunmehr auch zeilenweise, so gibt die Geheimschrift folgendes Bild:

	1	2	3	4	5	6	7
1	T	E	E	L	N	E	R
2	E	N	R	R	V	B	E
3	I	S	A	E	D	K	S
4	G	E	K	E	I	A	T
5	P	E	R	I	A	E	E
6	B	T	E	E	A	S	I
7	E	P	L	A	N	L	E

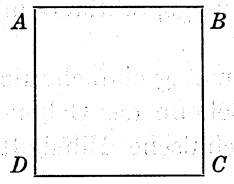
In horizontaler Richtung zeilenweise gelesen und in Gruppen zu je fünf Buchstaben geordnet, würde die Geheimmitteilung nunmehr lauten:

TEELN, ERENR, RVBEl, SAEDK, SGEKE usw.

Auf der Methode der Verwürfelung beruht ein dem Gitter verwandtes technisches Hilfsmittel des Chiffreurs.

Wiederum schneidet man einen Pappendeckel in der Größe des zu beschreibenden Briefpapieres aus. Wiederum zeichnet man auf diesen z. B. rechteckigen Pappendeckel so viele Qua-

drate, als man auf eine Seite des zu beschreibenden Briefpapieres Buchstaben schreiben will. Einen solchen viereckigen Pappendeckel



kann man, ohne die obere und untere Fläche des Deckels zu wechseln, viermal wenden.

Das erstemal wird die Seite A bis B
„ zweitemal „ „ „ B „ C
„ drittemal „ „ „ C „ D
„ viertemal „ „ „ D „ A

die obere horizontale Seite des Parallelogrammes bilden.

Man kann nun die auf dem Pappendeckel vorgezeichneten Quadrate derart stanzen, daß das Papier, ganz mit Buchstaben bedeckt, keine leere Stelle mehr zeigt, wenn man den quadratischen Pappendeckel hintereinander in die vier oben angedeuteten Lagen bringt und jedesmal die ausgestanzten Öffnungen mit Buchstaben des Klartextes füllt. Zuerst wird also der Pappendeckel in der ersten Lage aufgelegt und es werden in alle ausgestanzten Öffnungen Buchstaben des Klartextes geschrieben. Dann wird der Pappendeckel in die zweite Lage gebracht. Unter den ausgestanzten Öffnungen muß nun bei einer geeigneten Art der Ausstanzung leeres, unbeschriebenes Papier liegen, welches durch die ausgestanzten Öffnungen mit Buchstaben des Klartextes ausgefüllt wird. Wird nun der Pappendeckel in die dritte und vierte Lage gebracht, so müssen jedesmal in jeder dieser Lagen unter den ausgestanzten Öffnungen weiße, unbeschriebene Stellen des Papieres liegen, so daß durch die ausgestanzten Öffnungen jedesmal Buchstaben des Klartextes geschrieben werden können.

Tafel A, Fig. II, zeigt ein Beispiel dieser Art der Ausstanzung.

Dieser viermal wendbare, ausgestanzte Pappendeckel (Patrone oder auch Füllgitter, u. zw. Drehgitter genannt) ist ein Instrument, um den Klartext mit anderen Buchstaben desselben Klar-

textes zu vernieten, bzw. um die Buchstaben eines Klartextes zu verwürfeln. Die prinzipielle Idee dieses technischen Behelfes könnte daher ebenso dem Kopfe eines Vernietungstechnikers als dem eines Verwürfelungspraktikers unter den Kryptographen entsprungen sein!

Derartige, verhältnismäßig einfache Behelfe kann man jedoch nicht als maschinelle Behelfe des Geheimschreibers bezeichnen. Es sind höchstens technische Hilfsmittel, technische Behelfe oder Chiffriergeräte!

Die eigentlichen maschinellen Hilfsinstrumente des Geheimschreibers kommen erst bei einer andern Methode der Geheimschrift zur Anwendung, nämlich bei der Methode des Ersatzverfahrens.

Das sogenannte Buchstabenersatzverfahren besteht darin, daß alle Buchstaben des Klartextes einzeln durch Ziffern oder durch Zeichen oder endlich durch andere Buchstaben ersetzt werden.[10]) Der Ersatz durch Ziffern („Chiffrieren") hat bekanntlich der Geheimschrift ihren Namen gegeben.

Eine einfache Chiffre, welche in dem Ersatze von Buchstaben durch Zahlen besteht, ist z. B.:

a	12	f	13	l	87	q	31	v	94
b	59	g	45	m	21	r	19	w	25
c	63	h	81	n	51	s	37	x	32
d	41	i	79	o	24	t	18	y	29
e	23	k	52	p	22	u	65	z	67

Text: Verbrenne . . .

Chiffre: 942319591923515123,

bzw. in Dreiergruppen: 942, 319, 591, 923, 515, 123.

Statt die Ziffern wirklich anzuschreiben, benützt man manchmal horizontale Hilfslinien (s. Tafel B, Fig. I), deren jede einer einziffrigen oder zweiziffrigen Zahl (nämlich den Chiffrenzahlen) entspricht. Der Chiffretext bietet dann nicht mehr das Bild einer Ziffernreihe oder irgendwie gruppierter Ziffern, sondern das Bild einer Zickzackkurve. Der Chiffreur und der Dechiffreur benützen aber nicht etwa horizontal liniiertes Papier. Sie

10) Wenn nicht einzelne Buchstaben, sondern ganze Silben durch Silben ersetzt werden, spricht man von Silbenersatzverfahren. Werden ganze Wörter durch andere Wörter ersetzt, so spricht man von Wortersatzverfahren. Wenn ganze Phrasen ersetzt werden, so spricht man von Phrasenersatz.

bedienen sich vielmehr eines Hilfsgerätes, u. zw. der Chiffreur eines Faulenzers, der mit der entsprechenden Linienrastrierung versehen ist, — der Dechiffreur einer durchsichtigen Cellitplatte, auf welche die entsprechenden Horizontallinien eingraviert sind. Er legt diese Cellitplatte auf die Geheimschrift und sieht die Geheimschrift nunmehr wie Tafel B, Fig. II.[11])

Eine einfache Form des Buchstabenersatzes mittelst anderer Buchstaben ist der sogenannte „Julius Cäsar". Man benannte diese Form des Ersatzverfahrens mit dem Namen des großen Feldherrn, weil eine primitive Form dieses Ersatzverfahrens angeblich schon von ihm angewendet worden sein soll.

Wenn der Geheimschreiber und der Dechiffreur zwecks Chiffrierung z. B. folgendes Chiffrenalphabet gewählt haben:

Klaralphabet	Chiffre	Klaralphabet	Chiffre
A	e	N	f
B	g	O	n
C	l	P	i
D	o	Q	w
E	b	R	a
F	x	S	z
G	c	T	u
H	p	U	k
I	r	V	d
K	h	W	q
L	v	X	s
M	t	Z	m

so würde die Mitteilung:

„Verbrenne alle Papiere, entleere die Kassa, beseitige Akte" lauten:

dbagabffbevvbieirbabbfuvbbaborbhezzegbzbrurcbehub.

[11]) Die Illustration Tafel B, Fig. I, ist aus Fleißner, Handbuch der Kryptographie, Wien 1881, Tafel XIX, entnommen. Vgl. ebenda auch Tafel XVIII und S. 183 ff. Statt einer Cellitplatte kann auch mit Transparentöl durchsichtig gemachtes, bedrucktes Papier verwendet werden.

In Gruppen von fünf Buchstaben geordnet, würde diese Mitteilung lauten:

dbaga, bffbe, vvbie, irbab, bfuvb, babor etc.

Das Chiffrieren nach dieser Methode kann man sich mit Hilfe einer Schreibmaschine sehr erleichtern. In einigen Schreibmaschinenschulen wird darauf Gewicht gelegt, daß die Schüler „blind" schreiben können. Man hat daher kleine Zelluloidkappen angefertigt, welche über die Taste gestülpt werden, damit der Schüler die Taste niederdrücken muß, ohne sich durch einen Blick auf die Tastenbezeichnung orientieren zu können.

Bei Anwendung des obigen Chiffrenschlüssels würde auf die Zelluloidkappe über der Taste „e" der Buchstabe „a" gezeichnet werden. Hat der Chiffreur ein „a" zu schreiben, so drückt er jenen Tastenhebel nieder, welcher durch die Zelluloidkappe a gekennzeichnet ist, es ist dies nämlich der dem Buchstaben e entsprechende Tastenhebel. Die Schreibmaschine schreibt sohin, wenn der Chiffreur die Zelluloidklappe „a" berührt, ein „e", sie chiffriert also.

Serge Kanschine und Emil Jellinek-Mercedes haben eine ähnliche Ausgestaltung der Klaviatur (Tastatur) einer Schreibmaschine zum Gegenstande ihrer Patentschrift, österr. Patent Nr. 51.351, ausgegeben 27. Dezember 1911, Beginn der Patentdauer 1. August 1911, betitelt „Einrichtungen an Schreibmaschinen zum Chiffrieren und Dechiffrieren", gemacht.

Jede Schreibmaschine beliebigen Systems ist mit der normalen Buchstabenbezeichnung versehen. Die Hebel weisen also normale Typierung auf und tragen übereinstimmende Chiffrenbezeichnung. Jede der auf einem der Tastenhebel sitzenden Tasten ist nun bei der patentierten Maschine mit einer Vierkantbohrung versehen. Zu dieser so ausgestatteten Schreibmaschine gehört eine Serie von Plättchen, welche der Größe der Flächen der Tasten entsprechen. An ihrer Unterseite mit einem Vierkantdorn versehen, passen diese Plättchen daher in die auf jeder Taste vorgesehene Vierkantbohrung hinein. Diese Plättchen können an den Tasten der Maschine auswechselbar angebracht werden. Sie tragen entweder die einzelnen Normalbuchstaben oder Chiffrenzeichen.

Will man mit Hilfe dieser Maschine einen normalen Text in chiffrierter Schrift schreiben, so steckt man die die Normalbuchstaben tragenden, losen Plättchen entsprechend dem Schlüssel auf die zugehörigen Chiffrentasten. Die Klaviatur gleicht nunmehr wieder der Tastatur einer normalen Schreibmaschine. Bei Betätigung der Maschine erscheint der Text jedoch nicht in Normalbuchstaben, sondern in Chiffrenzeichen.

Auch die Klaviatur der Dechiffriermaschine entspricht vollkommen der einer normalen Schreibmaschine. Auf den Tastenhebeln sind die normalen

Buchstaben angeordnet. Jede der Tasten ist wie im früheren Falle mit einer Durchlochung zur Aufnahme des Stiftes einer losen Tablette versehen.

Auch zu dieser Maschine gehört eine Serie loser Plättchen, die an der Unterseite mit einem in die Durchlochung der Tasten passenden Dorn versehen, an ihrer Oberseite die einzelnen zur Verwendung kommenden Chiffren tragen.

Um mit dieser Maschine dechiffrieren zu können, werden dem Schlüssel entsprechend die losen Chiffrenplättchen auf die Tasten aufgesteckt. Sodann wird der chiffrierte Text abgespielt. Die Maschine schreibt den Normaltext nieder.

An Stelle zweier Schreibmaschinen, nämlich einer Chiffrier- und einer Dechiffriermaschine, kann man auch eine einzige Maschine verwenden. Dann müssen aber an den Typenhebeln sowohl Normalbuchstaben als auch Chiffren angebracht sein. (Vgl. die Typenhebel der Remington-Maschine mit Umschaltung für kleine und große Buchstaben.) In der Ruhestellung des Umschaltrahmens werden von den Typenhebeln Normalbuchstaben, in der niedergedrückten Stellung des Umschaltrahmens Chiffrentypen geschrieben.

Auf den Tasten dieser Schreibmaschine werden die zu chiffrierenden Buchstaben und die zu dechiffrierenden Chiffren geschrieben. Jede Taste ist, wie früher beschrieben, mit einer Durchlochung zur Aufnahme des Dornes des Plättchens versehen.

Auch Edward Hugh-Hebern und Fred Hoffman haben sich mit dem gleichen Probleme beschäftigt. In der Patentschrift österr. Patent Nr. 70.448, betitelt „Vorrichtung für Schreibmaschinen zur Herstellung von Geheimschriften und zur Übertragung derselben in Normalschrift", beschreiben die Erfinder ihre Maschine folgendermaßen:

Über den Tasten wird ein Rahmen von treppenartigem Aussehen angebracht. In den wagrechten Gliedern dieses Rahmens sind Führungsbahnen für herausnehmbare Kodexstreifen vorgesehen. Auf diesen Kodexstreifen können die Zeichen willkürlich angeordnet werden. In den lotrechten Gliedern des Rahmens sind „Reihen von Aussparungen" angeordnet. Die zur Herstellung der Geheimschrift dienenden Hilfstasten sind aus gebogenem Bleche hergestellt. Sie bestehen aus einem vom Schreiber mit der Hand anzuschlagenden Fingerdruckstücke, einem Mittelteil, welches die Führung besorgt, und endlich einem Fußteil, welches auf der Schreibmaschinentaste aufsitzt, bzw. zum Aufsitzen gelangt. Dieser Fußteil ist ebenso wie das Fingerdruckstück nach vorne gebogen.

Soll ein Klartext chiffriert werden, so werden zuerst alle Streifen in entsprechende Lage gebracht. Die erwähnten Fingerdruckstücke werden nacheinander heruntergedrückt. Wird nunmehr die Schreibmaschine betätigt, so typt sie gedruckte Zeichen. Diese unterscheiden sich aber von denen des Klartextes. An Stelle des Buchstaben „S" des Klartextes würde z. B. bei einer bestimmten Einstellung der Buchstabe „V" geschrieben werden. Der Fuß der Hilfstaste „S" ruht nämlich auf der Taste „V" der Schreibmaschine. Die Maschine chiffriert also. Will der Empfänger die chiffrierte Nachricht dechiffrieren, so benützt er eine Schreibmaschine, die mit den gleichen Kodexstreifen versehen ist. Diese Kodexstreifen befinden sich aber bei der De-

chiffriermaschine selbstverständlicherweise in anderer Lage wie die Streifen der Sendemaschine. Der Empfänger schreibt die chiffrierte Nachricht auf seiner Schreibmaschine nieder, indem er jene Fingerstücke herabdrückt, welche den Chiffrenzeichen der geheimen Nachricht entsprechen. Er tippt sohin auf seiner Maschine die chiffrierte Nachricht, die Maschine aber schreibt sofort den Klartext. Es befindet sich nämlich — um bei obigem Beispiele zu bleiben — der Buchstabe „V" in einer solchen Lage auf dem Kodexstreifen, daß, wenn *a)* der Kodexstreifen von der für die Sendemaschine vorgesehenen Lage in die für die Empfangsmaschine vorgesehene Lage gebracht wird und *b)* die Taste „V" angeschlagen wird, an der Schreibmaschine die Taste „S" niedergedrückt und daher der Buchstabe „S" getypt wird. Die Dechiffriermaschine schreibt also, wenn „V" getippt wird: „S". Was bei der Sende- wie bei der Empfangsmaschine hier beispielsweise von den Zeichen „V" und „S" bemerkt wird, gilt selbstverständlicherweise analog von allen anderen Zeichen und Buchstaben.

Die oben beschriebene Erfindung hat eine einzige Maschine im Auge, bei welcher derselbe Kodexstreifen in einer Lage als „Sende"-, in einer anderen Lage als „Empfangsstreifen" verwendet wird.

Die Kodexstreifen selbst können abgeändert werden. Die die Zeichen enthaltenden Blöcke werden von den Streifen abgenommen und können in anderen Stellungen in die Streifen wieder eingesetzt werden.

In jeder Sprache gibt es nun bekanntlich eine Reihe von Buchstaben, welche in den Klartexten dieser Sprache besonders häufig vorkommen. Für die deutsche Sprache hat z. B. Fleißner folgende Häufigkeitstabelle zusammengestellt:

e 18·66	d 4·83	m 2·58	p 0·33
n 11·33	a 4·79	f 1·67	j 0·12
i 7·88	h 4·34	z 1·62	q 0·—
r 7·25	g 3·96	c 1·58	x 0·—
s 6·75	o 3·25	w 1·45	y 0·—
t 5·04	l 2·91	k 1·21	
u 5·—	b 2·67	v 1·08	

Wenn der Enträtseler z. B. in einer nach Julius Cäsar chiffrierten Geheimschrift die Häufigkeit der vorkommenden Chiffrebuchstaben zählt, wird es ihm gelingen, die wahrscheinliche Bedeutung der einzelnen Chiffren zu erraten.

Auch das Aufeinanderfolgen gewisser Chiffrebuchstaben, z. B. die häufigere Aufeinanderfolge zweier Chiffrebuchstaben, wird ihn daran denken lassen, ob nicht diese Chiffrebuchstaben Ersatzelemente sind für ein ch, pf, st, ei, en, eu, er, es od. dgl.

Der Chiffreur kann seinen Julius Cäsar durch eine vor oder

nach der Chiffrierung angewandte Vernietungs- oder Versetzungsmethode oder auch durch Anwendung beider Methoden zu einem schwer enträtselbaren gestalten.

Der nach der Methode Julius Cäsars arbeitende Geheimschreiber wird weiters sein Schlüsselalphabet innerhalb ein und derselben Mitteilung entsprechend oft wechseln, zumindest aber jede Mitteilung nach einem andern Schlüssel chiffrieren.

Hiebei wird er sich mit Vorliebe verschiedener mechanischer Hilfsmittel bedienen. Die einfache Form eines solchen mechanischen Hilfsmittels ist der sogenannte Chiffrierschieber. Er ist nach Art eines Rechenschiebers gebaut und besteht aus zwei gegeneinander verschiebbaren Stäben (Tafel C, Fig. I). In der praktischen Ausführung sind nicht beide Stäbe gegeneinander verschiebbar, sondern es wird einer der Stäbe fest, der andere aber innerhalb, unter oder auf dem festen Stabe beweglich konstruiert. Im folgenden soll der einfacheren Ausdrucksweise wegen der feste Stab als „Schiene", der bewegliche Stab als „Schieber" bezeichnet werden. In Tafel C, Fig. I, trägt der Schieber ein Alphabet, welches dem Klartext entspricht, also ein Klaralphabet. Die Schiene trägt ein Doppelalphabet, das sogenannte Chiffrendoppelalphabet. Wenn ein Buchstabe des Klartextes zu chiffrieren ist, so muß der Schieber vorerst in eine zwischen Chiffreur und Dechiffreur vereinbarte Stellung gebracht werden. Das Chiffrieren erfolgt in der Weise, daß nunmehr im Chiffrendoppelalphabet der Schiene jener Buchstabe abgelesen wird, der sich oberhalb des zu chiffrierenden Klarbuchstaben befindet.

Wenn die Schiene, wie in Tafel C, Fig. I, ein Doppelalphabet von je 24 Buchstaben enthält, dann läßt sich der Schieber in 23 verschiedene Stellungen[12]) bringen. Es lassen sich sohin mechanisch 23 der 26 Alphabete aus nachfolgender Tritheim-Buchstabenchiffre mit diesem Geräte einstellen.[13])

[12]) In 23 und nicht in 24 Stellungen, weil eine von den 24 Stellungen ja jene wäre, wo sich oberhalb jedes Klarbuchstaben genau derselbe Buchstabe als Chiffrebuchstabe befinden müßte. In dieser Schieberstellung wäre also eine Chiffrierung nicht möglich. Wenn der Schieber z. B. so gestellt wird, daß der Buchstabe a des Schiebers genau unter dem Chiffrebuchstaben a der Schiene stünde, dann hätten wir eine Gleichung zwischen zwei Identischen und würden wir keine Chiffrierung erzielen.

[13]) Das Alphabet 24 entspräche dem herrschenden Alphabete und wäre daher kein Chiffrenalphabet.

*	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
26	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Tritheims Buchstabenchiffre zeigt 26 und nicht 23 Alphabete, weil Tritheim in seine Tabelle auch das gebräuchliche Alphabet a bis z und in die einzelnen Alphabete auch die Buchstaben j und y aufgenommen hat.

In Tafel C, Fig. I, ist der Schieber derart gestellt, daß der Buchstabe a des Schiebers unter dem Buchstaben h der Schiene eingestellt ist. Es ergibt sich dann ein Julius Cäsar, welcher lautet:

Klarbuchstabe	Chiffrenbuchstabe
a	h
b	i
c	k
d	l
e	m

etc.

Das bisher beschriebene Chiffriergerät besteht aus einer Schiene und einem Schieber. Tafel C, Fig. II, zeigt jedoch auf ein und demselben Geräte zwei Schienen und einen Schieber. Jede Schiene trägt ein Chiffrendoppelalphabet ober und unter dem Schieber.

In Tafel C, Fig. II, ist der Schieber derart gestellt, daß oberhalb des Klarbuchstaben a sich der Chiffrebuchstabe h, und unterhalb des Klarbuchstaben a sich der Chiffrebuchstabe r befindet.

Das Wort „Warnung" würde bei dieser Einstellung des Schiebers chiffriert lauten nach dem oberen Schlüssel:

ehzocuo,

nach dem unteren Schlüssel:

uraewewel.

Im unteren Chiffrenalphabet Tafel C, Fig. II, sind die Chiffrebuchstaben nicht in der Reihenfolge des Klaralphabetes angeordnet. Das untere Chiffrenalphabet zeigt vielmehr die umgekehrte Reihenfolge wie der Schieber und wie das obere Chiffrenalphabet.

Das untere Chiffrendoppelalphabet gestattet daher nicht nur 23, sondern 24 verschiedene Stellungen des Schiebers.

Der Behelf Tafel C, Fig. II, gestattet daher 23 plus 24, das sind 47 verschiedene Stellungen des Schiebers, daher 47 verschiedene Schlüssel. Der Schlüssel kann selbstverständlicherweise nach jeder Mitteilung oder aber auch innerhalb einer und derselben Mitteilung, z. B. zeilenweise, gewechselt werden.

In Tafel C, Fig. II, bemerkt man sowohl an der oberen Schiene, bzw. im oberen Chiffrenstreifen, als auch an der unteren Schiene, bzw. im unteren Chiffrenstreifen, je zwei Schrauben, welche es ermöglichen, den oberen und den unteren Chiffrenstreifen abzuschrauben und anders gruppierte Chiffrenalphabete an die obere und untere Schiene anzuschrauben. Einen solchen Ersatzstreifen zeigt Tafel C, Fig. III.

Ermöglicht daher das Instrument Tafel C, Fig. II, in dieser Form 47 Schlüssel anzuwenden, so gestattet jeder weitere anschraubbare Chiffrenstreifen, 24 weitere Schlüssel anzuwenden. Ein Instrument wie Fig. II mit 10 Chiffrenersatzstreifen ermöglicht 47 plus 240, das sind also 287 verschiedene Schlüsselungen.

In dieser oder einer reichhaltigeren Ausstattung mit Alphabetstreifen stellt dieser Schieber ein mechanisches Hilfsmittel dar, welches denselben Zwecken dient wie z. B. das Werk von Krohn, von welchem eine Seite als Beispiel folgt:

131	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	l	i	g	f	e	d	c	b	a	k	r	o	h	n	z	y	x	w	v	u	t	s	q	p	m
132	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	p	q	t	v	w	x	y	z	d	u	h	r	s	e	n	a	b	c	f	g	i	k	l	m	o
133	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	p	q	r	s	u	v	w	x	y	z	n	a	g	o	t	h	e	b	c	d	f	i	k	l	m
134	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	r	v	u	w	x	q	y	b	s	c	h	m	i	d	t	a	z	e	f	g	k	l	n	o	p
135	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	r	s	g	d	t	u	f	w	v	k	z	y	i	x	e	m	a	h	l	b	n	o	p	q	c
136	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	a	d	f	g	k	c	u	r	t	i	o	s	e	p	h	n	q	z	l	b	m	y	v	z	w
137	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	x	c	q	z	u	a	p	v	e	f	d	g	i	l	s	o	n	k	h	w	b	t	r	m	y
138	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	r	z	v	s	p	m	f	d	c	h	i	k	a	g	o	b	x	t	w	y	q	u	n	e	l
139	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	w	l	v	k	u	h	t	s	q	g	r	f	b	o	i	z	e	n	a	c	d	y	p	x	m
140	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	g	k	o	q	s	x	u	r	v	z	t	y	w	p	l	h	d	b	m	i	n	e	a	c	f

Das Krohn'sche Buchstabensystem ermöglicht 3200, ja sogar 6400 gegebene Alphabete anzuwenden. Nach der Krohn'schen Methode werden Buchstaben durch Buchstaben, Ziffern und Zahlen in Ziffernchiffren ausgedrückt.

Der Einfachheit halber ist im vorstehenden bloß jener Teil der Krohn'schen Tabelle wiedergegeben, welcher die Buchstabenchiffren enthält.

Da das fortwährende Ab- und Anschrauben von Ersatzstreifen mühselig und zeitraubend ist, lag es nahe, daran zu denken, den raschen Wechsel der verschiedenen Chiffrenalphabete in der Weise zu ermöglichen, daß diese Chiffrenalphabete auf

einer Walze angebracht sind und durch Drehung dieser Walze jeweils ein anderes Chiffrenalphabet eingeschaltet werde. Diesem Gedanken begegnen wir in der österreichischen Patentschrift: Karl Haas und Heinrich Studt, „Geheimschriftapparat". Österr. Patent Nr. 33.211. (15. Jänner 1908.)[14]

Der Apparat besteht aus einer Walze, die sich in einem Gehäuse dreht; auf dieser Walze sind mehrere „Julius-Cäsar-Alphabete" angebracht. Diese Walze läßt sich sowohl durch einen Seitenknopf drehen als auch durch Niederdrücken einer Taste mittels eines geeigneten Schaltgetriebes um je eine Reihe weiterschalten.

Im Gehäuse, innerhalb welchem sich die Walze dreht, ist ein schmaler, horizontaler Schlitz angebracht. Durch diesen Schlitz ist die gerade unter diesem Schlitze befindliche Zeichenreihe der Walze, also stets nur eines der auf der Walze befindlichen Chiffrenalphabete sichtbar. Neben diesem Schlitz hat das Gehäuse noch eine weitere runde Öffnung (Index), hinter welcher „bei Einstellung eines bestimmten Julius Cäsar im Schlitze" jedesmal die Kennziffer des betreffenden Chiffrenalphabetes erscheint. Es ist daher sofort ersichtlich, welches Chiffrenalphabet durch den Schlitz hindurch lesbar ist. Unterhalb dieses Schlitzes ist am Gehäuse das Klaralphabet (die Buchstaben des Alphabetes und die Ziffern 0 bis 9) eingraviert.

Die sendende Person stellt die Walze mittels des Seitenknopfes so ein, daß eine bestimmte, verabredete Kennziffer in der Indexöffnung sichtbar wird. Nun schreibt sie jene Chiffrebuchstaben nieder, welche „ober dem jeweiligen Klarbuchstaben des am Gehäuse eingravierten Klaralphabetes" innerhalb des Schlitzes im Chiffrenalphabet abzulesen ist. Nach jedem in die Chiffreschrift übertragenen Buchstaben oder nach jeder chiffrierten Buchstabengruppe wird die Taste niedergedrückt. Sofort erscheint im Schlitze das nächste auf der Walze aufgezeichnete Chiffrenalphabet.

Chiffreur und Dechiffreur können verabreden, daß nach jedem einzelnen oder nach einer bestimmten Zahl von Buchstaben oder Wörtern die Taste nicht nur einmal, sondern je zweimal,

[14] Vgl. das österr. Patent Nr. 618, ausgegeben 25. November 1899, Beginn der Patentdauer 15. April 1899.

dreimal oder öfter niedergedrückt wird. Es wird dann im Schlitze nicht das nächste, sondern das zweit- oder drittnächste Alphabet der Walze sichtbar werden.

Sobald der Empfänger die erste Kennziffer kennt und weiß, wann und wie oft die Taste vom Chiffreur betätigt wurde, kann er seinen Apparat analog einstellen und den Chiffretext in den ursprünglichen Klartext zurückverwandeln.

Die in diesem Patente vorgesehene Walze stellt, wie aus obigen Ausführungen hervorgeht, eine walzenförmige Anordnung mehrerer Schienen dar. Die am Gehäuse eingravierte Klarschrift vertritt die Stelle des in den früher besprochenen Gerätschaften am Schieber angebrachten Klaralphabetes. Während aber bei den früher besprochenen Gerätschaften dieses Klaralphabet durch seine Anbringung auf dem Schieber gegenüber der Schiene verstellbar war, ist in dem patentierten Apparat die Klarschrift gegenüber der jeweiligen Chiffreschrift unverstellbar.

Dieses Patent gestattet daher nur, die auf der Walze angebrachten Schlüssel zur Anwendung zu bringen. Es gestattet jedoch mangels eines schiebbaren Klaralphabetes nicht, den Schlüssel innerhalb ein und desselben Walzenstreifens zu changieren.

Tafel D, Fig. I, zeigt eine zu Unterrichtszwecken hergestellte Chiffrenwalze, welche 13 Chiffrendoppelalphabete trägt.[15]) Der gelbe Streifen ist ein Klartextschieber. Die beiden Ringe, welche der Schieber verbindet, sind parallel verschiebbar. Der Klartextschieber läßt sich daher auch innerhalb eines Chiffrendoppelalphabetes verschieden einstellen. Eine so konstruierte Walze ermöglicht daher, innerhalb eines Chiffrestreifens 24 verschiedene Schlüssel zu benützen. Wenn die Walze 13 Chiffrenstreifen trägt, ermöglicht es dieser Apparat, $13 \times 24 = 312$ verschiedene Schlüssel anzuwenden.

Das kleine Fenster mit dem Griffe erleichtert es, am Schieber den zu chiffrierenden Buchstaben des Klartextes einzustellen. Bei dem kleinen, dreieckigen Zahn, welcher sich über dem Fenster befindet, läßt sich der entsprechende Chiffrebuchstabe leicht ablesen.

15) Ein Walzenstreifen ist das gewöhnliche Alphabet, daher kein Chiffrenstreifen. (In Tafel D, Fig. I, der Streifen 1.)

In Tafel D, Fig. I, ist die Walze auf Walzenstreifen 14 eingestellt. Der Schieber ist so gestellt, daß sich der Klarbuchstabe A unter dem Chiffrebuchstaben T des Walzenstreifens befindet. Für den Buchstaben H des Klartextes würde also die Chiffre B abgelesen werden müssen.

Auch dieses Instrument läßt sich auf verschiedene Weise ausgestalten, so z. B. durch auswechselbare Reservewalzen, deren jede 14 andere Julius-Cäsar-Alphabete trägt. Vier Reservewalzen entsprechen z. B. 56 Walzenstreifen. Jeder Streifen ermöglicht in Anbetracht des einstellbaren Schiebers 24 Variationen innerhalb des Streifens. Es könnten sohin weitere $56 \times 24 = 1344$ Schlüssel angewendet werden.

Statt die Walze auswechselbar zu konstruieren, kann der Apparat von vornherein aus zwei nebeneinanderliegenden gegeneinander drehbaren Walzen bestehen, über welchen der Schieber so angebracht ist, daß man bei einer bestimmten Schiebereinstellung sowohl an der einen Walze als auch an der andern Walze die Chiffrebuchstaben ablesen kann. Wir haben in diesem Falle einfach einen Apparat wie in Tafel C, Fig. II, vor uns, bei welchem das Chiffrendoppelalphabet der oberen und unteren Schiene nicht an- und abzuschrauben ist. Es werden vielmehr durch Drehen der einen, eventuell der anderen Walze jeweils zwei andere Chriffrendoppelalphabete eingestellt.

Eine kompliziertere, aber bedeutend wirkungsvollere Ausgestaltung des Apparates Tafel D, Fig. I, ist folgende: Auf der Walze sind keine fixen Walzenstreifen angepickt. Die Walze wird nicht ausgewechselt. Die Walze besteht vielmehr, wie Tafel D, Fig. II, zeigt, aus manschettenringförmigen Teilen.

Wenn auf jedem dieser Ringe 24 Buchstaben des Alphabetes aufgezeichnet sind und die Walze aus 24 solchen Ringen besteht, dann lassen sich mit einer und derselben Walze unzählige Chiffrenstreifen kombinieren. Geeignete Einschnappvorrichtungen können dieses Ringsystem nach Einstellung der Ringe so fixieren, als ob eine fixe Walze vorhanden wäre. Die Schiebervorrichtung ist auch bei dieser aus Ringen bestehenden Chiffrierwalze genau so angebracht wie bei dem Apparat Tafel D, Fig. I. (Vgl. auch das deutsche Patent Nr. 618 und das französische Patent Nr. 478.943.)

Chiffrierbehelfe für den Ersatz von Buchstaben durch Ziffern oder Ersatzbuchstaben gibt es zahlreiche.

Das in Tafel E, Fig. I, skizzierte Gerät entspricht einer von Fleißner beschriebenen Methode, nämlich der Methode der verschiebbaren Zahlenchiffre. Fleißner beschreibt diese Methode auf folgende Weise:

„Der Schlüssel besteht aus einem Alphabet und zwei verschiebbaren Ziffernreihen, so daß jeder Buchstabe durch eine beliebige zweiziffrige Zahl ausgedrückt werden kann. Hiedurch kommt man in die Lage, mit vielen geheimen Alphabeten chiffrieren zu können. Um aber zu wissen, mit welchem Alphabet chiffriert wurde, dient ein Wahlwort."

Wäre z. B. „Subordination" das Wahlwort, so wird der erste Buchstabe des Wahlwortes, also S, im Schlüssel durch Verschiebung der Ziffernreihen mit einer beliebigen Zahl, z. B. 97, bezeichnet. Diese Zahl, in diesem Beispiele also 97, wird an eine vereinbarte Stelle der Depesche gesetzt. Diese Zahl signalisiert dem Dechiffreur, daß ein Alphabet benützt werde, in welchem der erste Buchstabe des Wahlwortes, in obigem Beispiel also S, durch 97 bezeichnet wird.

„Will man während des Schreibens der Depesche das Chiffrenalphabet wechseln, so zeigt man die Tatsache des Alphabetwechsels zuerst durch ein Wechselzeichen an. Dem Wechselzeichen läßt man dann jene Zahl folgen, welche im neuen Chiffrenalphabet dem zweiten Buchstaben des Wahlwortes, beim Wahlworte ‚Sudordination' also dem u, entspricht."

Wird der Apparat z. B. so eingestellt, daß der Buchstabe „S" in Subordination durch die Zahl 97 bezeichnet wird und folgt dem Wechselzeichen die Zahl 53, so wird hiedurch signalisiert, daß der dem Wechselzeichen nachfolgende Chiffretext mit jenem Alphabete geschrieben wurde, in welchem u (zweiter Buchstabe von „Subordination") durch 53 ausgedrückt ist.

(Es ist wohl klar, daß der Chiffreur in der Praxis die Zahl 97 nicht an den Anfang der Depesche stellt, sondern an einer vereinbarten Stelle der Depesche unterbringt.)

Der Dechiffreur teilt sich vorerst die Geheimschrift zweiziffrig ab, streicht die etwaigen Nieten (z. B. 15, 35, 95) durch, bezeichnet sich die Wechselzeichen (z. B. 70, 00, 20, 90) und schreibt z. B. über die erste zweiziffrige Zahl der Depesche sowie

auch über die erste Zahl nach jedem Wechselzeichen die Buchstaben des Wahlwortes, daher z. B. über 97 s, über 53 u etc. „Er hat sich auf diese Weise die Alphabete bezeichnet, mit welchen chiffriert wurde." Er wird nun danach seinen Schlüssel verschieben, um die Depesche zu entziffern.

Für eine andere verschiebbare Zahlenchiffre, welche bei den Österreichern in Mexiko in Gebrauch war, dient der Apparat Tafel E, Fig. II, welcher mit einigen unbedeutenden Änderungen aus Fleißners Kryptographie entnommen ist. Fleißner beschreibt diese Methode folgendermaßen:

„Unter dem Alphabet sind die ungeraden, über demselben die geraden zweiziffrigen Zahlen angebracht, so daß jeder Buchstabe durch eine gerade und eine ungerade Zahl bezeichnet werden kann.

Um das Alphabet zu stellen, benötigt man einen Wahlbuchstaben. An einer vereinbarten Stelle der geheimen Depesche zeigt man an, auf welche Zahl der Wahlbuchstabe gestellt wurde und mit welchem Alphabet daher chiffriert wird."

Will man mit den Alphabeten wechseln, so gibt man als Wechselzeichen z. B. eine „Zahl an, die ober- oder unterhalb eines Striches (Pause) des Alphabetes ist, und lasse dieser Zahl die Zahl folgen, welche in dem neuen Alphabet den Wahlbuchstaben bezeichnet usw".

Bei allen bisher beschriebenen Geräten war das Chiffrenalphabet in Linien, bzw. Stabform angebracht.

Wird das Chiffrendoppelalphabet nicht auf einem Stabe angebracht, sondern auf einer Scheibe angeordnet und läßt sich im Mittelpunkte der Chiffrenscheibe eine auf der Chiffrenscheibe angebrachte Klartextscheibe um ihren Mittelpunkt drehen, so erfüllt ein solcher Behelf denselben Zweck wie die Schiebergeräte. Der äußere Scheibenrand entspricht der Schiene mit dem Chiffrierdoppelalphabet, die innere Klartextscheibe dem Schieber.

Die begrenzte Schiene (Tafel C, Fig. I oder II) ist umgewandelt in den unbegrenzten Ring, die sogenannte Zirkularscheibe. Auf der Chiffrierscheibe können selbstverständlich auch konzentrisch mehrere Chiffrendoppelalphabete angeordnet sein.

Eine aus dem Werke: Figl, „Systeme des Chiffrierens", entnommene Zirkularscheibe ist in Tafel F, Fig. I, reproduziert.

In dieser Zirkularscheibe sind vier Tritheim-Tafeln vereint. Figl beschreibt in seinem „Systeme des Chiffrierens" diese Zirkularscheibe folgendermaßen:

„Sie besteht aus einer größeren Grundscheibe und einer kleineren Einsatzscheibe, welche konzentrisch derart verbunden sind, daß sie drehbar bleiben.

Die Grundscheibe trägt in unserem Beispiel in konzentrischen Ringen von außen nach innen:

1. die Stellungsnummern; sie dienen dazu, die beim Schlüsseln den Scheiben zueinander zu gebende Stellung zu bezeichnen;

2. einen Kranz zweistelliger Zahlensigel, nach rechts mit Überspringen je eines Feldes steigend von 11 bis 58, unter Stellungsnummer 9 beginnend;

3. einen zweiten Kranz zweiziffriger Sigel, nach links mit Überspringen je eines Feldes steigend von 21 bis 78, unter Stellungsnummer 8 beginnend:

4. ein erweitertes Sigelalphabet, mit Überspringen von je zwei Feldern nach rechts geordnet, unter Stellungsnummer 40 beginnend, und

5. ein zweites erweitertes Sigelalphabet, mit Überspringen je eines Feldes nach links geordnet, unter Stellungsnummer 48 beginnend.

Die Einsatzscheibe trägt ein erweitertes Alphabet in natürlicher Anordnung — das Klaralphabet und zwei Wechselzeichen Wz-1 und Wz-2.

Stehen die Pfeile auf beiden Scheiben in Deckung, so ist das die Grundstellung."

Ein einfaches, sehr handliches Modell einer Zirkularscheibe könnte man für Unterrichtszwecke anfertigen lassen (Tafel F, Fig. II).

Das doppelte Chiffrenalphabet der festen Kreisscheibe (Tafel F, Fig. II) besteht aus Buchstaben, die sich in die Scheibe einschieben lassen. Diese Modifikation in der Anlage der Chiffrenscheibe des Zirkularapparates (der sog. festen Chiffrenscheibe der Zirkularscheibe) gestattet ohne Drehung der beweglichen inneren Scheibe bei 24 Buchstaben des Alphabetes: (24!) Variationen.

Selbstverständlich müssen die Buchstaben des zweiten Alphabetes des auf der festen Scheibe vorgesehenen Chiffrendoppelalphabetes stets genau in derselben Reihenfolge fortlaufend eingeschoben werden, wie das erste Alphabet des Chiffrendoppelalphabetes angeordnet ist, also beispielsweise:

„adrozwtbeckfmngpvhlqisuxadrozwtbeckfmngpvhlqisux".

Die drehbare innere Zirkularscheibe ermöglicht, wie aus den vorhergehenden Ausführungen hervorgeht, bei jeder Anordnung

des Chiffrendoppelalphabetes 23 bis 24 Variationen. Hiedurch erhöht sich die Anzahl der Variationen, welche der Apparat gestattet.

Die Burg'sche Erfindung, österr. Patent Nr. 26.892 (1. August 1906), hat zum Gegenstande eine Geheimschreibmaschine nach Art der Zirkularscheibe.

Der Wechsel der Kombination wird bei diesem Apparate durch Verstellen eines Schlittens erzielt. Man bewegt diesen Schlitten unmittelbar von Hand aus in hin- und hergehender Richtung. Sein Ausschlag ändert sich selbsttätig nach einem vorherbestimmten Gesetze. Diese veränderliche Verstellung des Schlittens wird auf einen Typenkranz übertragen, der um einen festen Typenkranz drehbar ist. Diese beiden Typenkränze dienen zur wechselweisen Übersetzung der Geheimschrift. Bei jedesmaliger Betätigung des Schlittens kommt ein neuer Stift in den Weg des Anschlages und ändert sich daher jedesmal der Weg des Schlittens und der Drehwinkel des Typenkranzes. Wie und wann der Schlitten zu betätigen ist, ist vorher zu vereinbaren.

Dieser Chiffrierapparat soll frei in der Hand gehalten werden können.

Am Schlitten und am Träger sind Griffe so angeordnet, daß sie mit einer Hand erfaßt werden können. Diese Griffe sind infolge der Wirkung von Federn bestrebt, sich voneinander zu entfernen. Es kann daher das Hin- und Herbewegen des Schlittens einzig durch die den Apparat haltende Hand erzielt werden.

Eine Art Zirkularscheibe hat Hubert Burg in seiner Patentschrift österr. Patent Nr. 40.982, ausgegeben am 10. Februar 1910, Beginn der Patentdauer 1. September 1909, „Schreibmaschine für Geheimschrift", im Auge. Die lesbaren Schriftzeichen und die Geheimschriftzeichen sind auf zwei konzentrischen Kränzen angeordnet. Einer dieser Kränze ist feststehend, der andere kann durch die Bewegungen eines Schlittens in unregelmäßiger, aber vorherbestimmter Weise verstellt werden. Zufällige Unregelmäßigkeiten des Mechanismus, welche infolge des Beharrungsvermögens des beweglichen Typenkranzes etc. auftreten könnten, sollen durch die patentierte Erfindung verhütet werden. Der bewegliche Typenkranz ist immer verhalten, in die richtige Stellung einzutreten. Er kann über dieselbe nicht hinausgehen, bevor nicht der Schlitten eine neue Hin- und Herbewegung vollführt hat.

Burg beschreibt das Wesentliche seiner Erfindung in folgender Weise: „Ein beweglicher Zeichenkranz wird in unregelmäßigen, aber vorher bestimmten Teilstrecken mittels einer Schaltvorrichtung weitergeschaltet. Die Schaltvorrichtung kann nach jedem Abdrucke eines oder mehrerer Zeichen durch Hin- und Herbewegen eines Schiebers in Tätigkeit gesetzt werden. Der den verdrehbaren Zeichenkranz bewegende Schlitten besitzt eine Einrichtung, welche bei jeder Teilverschiebung eine Rückbewegung des Schlittens so lange verhindert, bis derselbe nicht in die Endstellung dieser Bewegung überführt ist. Der bewegliche Zeichenkranz besitzt eine Einrichtung, die verhindert, daß derselbe unter der Wirkung des Beharrungsvermögens später aufgehalten werde als die ihn betätigende Schaltvorrichtung. Der Zeichenkranz wird daher stets genau in die erforderliche Stellung nach vorwärts geschaltet, ohne rücklaufen oder ohne aufs neue eine Vorwärtsbewegung

ausführen zu können, bevor nicht der Schlitten eine neuerliche Hin- und Herbewegung erfährt."

Burg hat zwei Ausführungsformen dieser Erfindung vorgesehen:

a) Der Rücklauf des Schlittens ist auf jedem Wege der Hin- und Herverschiebung durch einen Anker verhindert, dessen Arme abwechselnd mit einer feststehenden Zahnstange in Eingriff treten können. Dieser Anker wird durch schräge Anschlagflächen einer verschiebbaren Stange umgestellt. Diese Stange wird am Ende jedes Schlittenweges durch einen unveränderlichen Anschlag und einen mit jeder Schlittenverschiebung wechselnden Anschlag verstellt und stellt dabei mit der einen oder der andern Schrägfläche den Anker ein.

b) Der Zeichenkranz wird durch einen feststehenden Zahnkranz fortbewegt. Dieser Zahnkranz ist zu einem Schaltrade konzentrisch gelagert. Dieses Schaltrad wird unmittelbar vom Betätigungsschieber durch einen Trieb und eine Zahnstange in Bewegung versetzt. Auf dem Schaltrade des Zeichenkranzes ist eine durch das Schaltrad betätigte Klinke gelagert. Sobald das Schaltrad aufgehalten wird, steigt die Klinke über einen unter ihr befindlichen Zahn des Rades und drängt einen Ansatz in den feststehenden Zahnkranz.

Auch das deutsche Reichspatent Nr. 307.655, ausgegeben am 9. September 1919, Priorität 1. Juni 1917, schützt mehrere ringförmige, ineinanderpassende Papierblocks mit aufgedruckter radialer Einteilung zum Einschreiben oder Aufdrucken von Buchstaben, Ziffern usw. Diese Papierblocks werden auf mehreren konzentrisch um eine gemeinsame Achse drehbaren Scheiben befestigt. Der Patentanspruch nennt dieses Gerät „Chiffrieruhr".

Will man bei den im vorigen besprochenen Gerätschaften (Tafel C, Fig. II, Tafel F, Fig. II etc.) das Schlüsselalphabet ändern, so ist ein An- und Abschrauben der Schienenstreifen, ein Einschieben von Buchstabenplättchen od. dgl. erforderlich. Es bestand daher das Bedürfnis nach einfachen Maschinen, welche innerhalb des Klartextes eine automatische Änderung des Schlüsselalphabetes bewerkstelligen. Eine solche einfache Maschine ist in Tafel G, Fig. I, dargestellt.

Wir sehen in einer Kassette zwei schwarze runde Deckplatten. An diesen beiden Platten ist je ein Segment abgeschnitten, so daß man die unter dieser Platte liegenden gezahnten runden Metallscheiben, bzw. die einzelnen Zähne dieser Zahnräder freiliegen sieht.

An der kreisförmigen Platte des linken Zahnrades sind die Zahlen 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37 also im ganzen 25 Zahlen von links nach rechts angebracht. Auf 37 folgt begreiflicherweise wieder 11.

Auf der kreisförmigen Platte des rechten Zahnrades sind die Buchstaben a, b, c, d, e, f, g, h, i, k, l, m, n, o, p, q, r, s, t, u, v, w, x, z, also 24 Buchstaben, von rechts nach links angebracht. Auf z folgt begreiflicherweise wieder a.

Bei der linken Platte entspricht je eine „Zahl", bei der rechten Platte je ein „Buchstabe" einem Zahn des Zahnrades.

Das linke Zahnrad hat 25, das rechte Zahnrad 24 Zähne.

Damit die Zähne gleich groß sind und ineinandergreifen können, wird sich begreiflicherweise der Umfang des nicht eingekerbten Teiles des rechten Zahnrades zu dem des linken Zahnrades verhalten wie 24 zu 25.

Die schwarzen Deckplättchen haben je einen kreisförmigen Ausschnitt. In Tafel G, Fig. I, sieht man in dem kreisförmigen Ausschnitte des linken Deckplättchens eine auf dem Zahnrade stehende Ziffer, in dem kreisförmigen Ausschnitte des rechten Deckplättchens einen auf dem Zahnrade angebrachten Buchstaben. Über der linken und über der rechten schwarzen Deckplatte sieht man weiters einen Messingknopf. Beim Drehen dieses Messingknopfes dreht sich das unter der Platte liegende Zahnrad und es stellt sich beim Drehen links jeweils eine andere Zahl, rechts jeweils ein anderer Buchstabe ein.

In Tafel G, Fig. I, ist — durch Drehung des Metallknopfes — das linke Zahnrad so eingestellt, daß im kreisförmigen Ausschnitte die Ziffer 11 erscheint — das rechte Zahnrad so eingestellt, daß in der kreisförmigen Öffnung der Buchstabe a erscheint. Nunmehr wird in der Kassette in der Richtung der beiden Pfeile das linke zum rechten Zahnrad geschoben, bis die Zähne beider Räder ineinandergreifen, wie dies Tafel G, Fig. II, zeigt.

Ist die Grundeinstellung der beiden Zahnräder links 11, rechts a und dreht man den rechten Messingknopf von links nach rechts, so verschwindet im rechten kreisförmigen Ausschnitte der Buchstabe a und es wird der Buchstabe b sichtbar.

Automatisch hat sich inzwischen durch das Eingreifen der Zahnräder ineinander das linke Zahnrad von rechts nach links gedreht und es verschwindet im kreisförmigen Ausschnitte des linken Zahnrades die Ziffer 11 und erscheint die Ziffer 12.

Dreht man von Buchstaben zu Buchstaben weiter, so wird bei z die vierundzwanzigste Zahl der Zahlenreihe, nämlich 36,

in der linken kreisförmigen Öffnung erscheinen. Dreht man den rechten Knopf noch um einen Zahn weiter, so erscheint im rechten Ausschnitte ein a und in der linken Öffnung die Zahl 37. Bei einer neuerlichen, vollständigen Drehung wird dem Buchstaben a die Zahl 36 entsprechen und erst bei der sechsundzwanzigsten vollständigen Umdrehung der rechten Scheibe wird mit dem Buchstaben a wieder die Ziffer 11 korrespondieren.

Die Maschine gestattet daher mit der Grundeinstellung a = 11, fünfundzwanzig verschiedene Julius Cäsar anzuwenden.

Die Anzahl der in diesem Apparate zur Chiffrierung zur Verfügung stehenden Julius-Cäsar-Schlüssel ist jedoch eine größere, da die Grundeinstellung für a zwischen 11 und 37 (exklusive 20 und 30) also 25mal wechseln kann.[16])

Es soll jedoch hievon vorläufig abgesehen und lediglich jener automatische Wechsel der Schlüssel besprochen werden, welcher eintritt, ohne daß die einmal gewählte Grundeinstellung wieder geändert wird.

Die Chiffrierungsregel während des Chiffrierens besteht darin, daß bei diesem Apparat der Knopf des rechten Zahnrades stets nur in der einen Richtung, nämlich von links nach rechts, aber niemals rückläufig gedreht wird.

Es wird bei der Chiffrierung des Satzes: „Weigert euch standhaft" das rechte Zahnrad bereits mehreremale voll gedreht und eine weitere Drehung begonnen. Der Schlüssel hat also innerhalb eines Satzes bereits mehreremale, u. zw. nach jeder vollen Drehung, automatisch gewechselt.

Die Grundeinstellung kann vom Chiffreur dem Dechiffreur an irgendeiner Stelle der Depesche bekanntgegeben werden. Sie kann aber auch auf einer zwischen Chiffreur und Dechiffreur getroffenen Vereinbarung beruhen, z. B. bei der ersten Depesche a = 11, bei der zweiten Depesche a = 15 etc.

Kennt der Dechiffreur die vom Chiffreur gewählte Grundstellung, so wiederholt er beim Dechiffrieren von der Grundeinstellung an genau die Drehungen, die der Chiffreur am Knopfe des Apparates vorgenommen hat. Er wiederholt daher Schritt für Schritt die vom Chiffreur vorgenommenen Hand-

[16]) Die Zahlen 20 und 30 fehlen nämlich in obiger Ziffernreihe (11 bis 19; 21 bis 29; 31 bis 37).

griffe. Kennt der Dechiffreur die Grundeinstellung nicht, weiß er aber, welcher Klarbuchstabe der letzten Chiffre entspricht, so dreht er den Apparat in umgekehrter Richtung, er wiederholt daher in verkehrter Reihenfolge die Handgriffe des Chiffreurs und dechiffriert die Geheimmitteilung also vom Ende zum Anfang derselben.

Ein ähnliches Gerät scheint Figl im Auge gehabt zu haben, wenn er in seinem „Systeme des Chiffrierens" von einem Apparate spricht, dessen Räder konzentrisch gestellt sind. Figl beschreibt diesen Apparat, welchen ihm während des Krieges ein Offizier der Telegraphentruppe vorführte, folgendermaßen:

„Auf einer Unterlagsplatte waren zwei Zahnräder — ein größeres und ein kleineres — so befestigt, daß die gezahnten Ränder beider ineinandergriffen. Beide Räder waren um ihre Achsen drehbar und wurden durch Federn in Kontakt gehalten. Ein kleiner Knopf diente dazu, die Feder außer Wirksamkeit zu setzen und den Kontakt aufzuheben, worauf jedes Rad beliebig in die Ausgangs- oder Grundstellung gebracht werden konnte.

Auf der Oberfläche jedes Rades waren Alphabete eingestanzt, u. zw. entsprach jedem Zahn ein Buchstabe.

Bei dem ungleichen Durchmesser drehten sich die Räder verschieden rasch und war das Verhältnis so gewählt, daß erst nach einer Unzahl von Umdrehungen wieder die gleichen Buchstaben beider Räder zusammentrafen.

Das große Rad trug in mehrfacher Wiederholung ein gewöhnliches Alphabet als Sigel, das kleinere hingegen das Klaralphabet."

Zu den Buchstabenersatzverfahren gehört auch die sogenannte Vokalchiffre. Die Chiffrierung erfolgt mittels eines Schlüsselquadrates. An der oberen und an der linken Quadratseite sind in einer vereinbarten Reihenfolge die Vokale a, e, i, o, u angeschrieben. Das Quadrat ist in 25 kleinere Quadrate untergeteilt. In jedes dieser kleinen Quadrate ist einer der 25 Buchstaben des Klaralphabetes eingeschrieben, z. B.:

I \ II	a	e	i	o	u
a	f	l	j	n	b
e	r	z	v	d	t
i	x	h	a	w	i
o	p	e	u	s	q
u	c	o	k	m	g

Beim Chiffrieren werden statt jedes Buchstaben des Klartextes zwei Chiffrebuchstaben geschrieben, z. B. jener Vokal, welcher in der Vokalumrahmung I in der entsprechenden Zeile, und jener Vokal, welcher in der Vokalumrahmung II in der entsprechenden Spalte abgelesen wird. Dem Klarbuchstaben k z. B. entspricht in seiner Zeile in der Vokalumrahmung I ein „u". Demselben Klarbuchstaben entspricht in seiner Spalte in der Vokalumrahmung II ein „i". Der Klarbuchstabe k wird also ausgedrückt durch die Chiffre „ui".

Die Mitteilung „Komme sofort" würde nach obigem Schlüsselquadrate und nach obiger Methode (zuert Zeile, dann Spalte) chiffriert lauten:

ui ue uo uo oe oo ue aa ue ea eu.

Mit entsprechenden Nieten durchsetzt, würde diese Mitteilung lauten:

gummi lues duo kuno sonne do horus begann salut leben dank deus.

Sie täuscht einem unerfahrenen Enträtseler einen „Wortersatz" vor.

Eine sicherere, aber kompliziertere Methode, welche der Vokalchiffre nachgebildet ist, wäre:

✲	a l g o v	d p k t x	c h e m r	b i f q y	s n z w u
a f i q d	F	L	J	N	B
p n e z s	R	Z	V	D	T
m v y t h	X	H	A	W	I
g o u w l	P	E	U	S	Q
c k r b x	C	O	K	M	G

Bei dieser Vokalchiffre läßt sich z. B. der Klarbuchstabe F ausdrücken durch aa, ag, al, ao, av, fa, fg, fl, fo, fv, ia, ig, il, io, iv, qa, qg, ql, qo, qv, da, dg, dl, do oder dv.

Auch zur Anwendung der sogenannten Vokalchiffre läßt sich ein Gerät konstruieren, welches den raschen Wechsel des Schlüssels innerhalb einer Mitteilung gestattet (Tafel H, Fig. I).

Die obere und die seitliche Vokalumrahmung bei diesem Geräte ist keine feste. Jede dieser Umrahmungen besteht vielmehr

aus je einem drehbaren, in sich geschlossenen Bandstreifen, der die Vokale a, e, i, o, u, a, e, i, o, u trägt und daher folgende Einstellung gestattet:

a	e	i	o	u
e	i	o	u	a
i	o	u	a	e
o	u	a	e	i
u	a	e	i	o

Wir haben also fünf Variationen in der Einstellung des horizontalen und fünf Variationen in der Einstellung des vertikalen Streifens, also 25 mögliche Variationen.

Nachdem die Grundeinstellung der oberen und seitlichen Vokalreihe erfolgt ist, wird z. B. nach Chiffrierung jedes Klarbuchstaben durch Drehen einer Schraube die obere und die seitliche Vokalreihe um einen Buchstaben verschoben. Lautet z. B. die Grundeinstellung

*	a	e	i	o	u
i					
o					
u					
a					
e					

so wird beim nächsten Buchstaben folgender Schlüssel zur Anwendung kommen:

*	u	a	e	i	o
e					
i					
o					
u					
a					

Eine gewisse Ähnlichkeit mit der Vokalchiffre hat das gleichfalls in die Gruppe der sogenannten Alphabetquadrate gehörende „Schachbrett". Man unterscheidet Buchstaben- und Ziffern-

schachbrette. Ein Schachbrett mit Buchstaben würde z. B. folgendes Aussehen haben:[17])

*	v	q	r	l	z
y	e	f	k	n	p
o	q	a	g	l	o
u	u	r	b	h	m
i	x	v	s	c	i
a	z	y	w	t	d

Die Chiffre für einen Klarbuchstaben findet man, indem man verabredetermaßen z. B. in der Spalte und dann in der Zeile, in welcher der Klarbuchstabe steht, bis an den Rand des Quadrates fährt. Die beiden am Rande des Quadrates, u. zw. *a)* in der gleichen Spalte, *b)* in der gleichen Zeile stehenden Buchstaben bilden zusammen die Chiffre für den Klarbuchstaben. Also würde mit obigem Buchstabenschachbrett „Heinrich" chiffriert werden:

lu vy zi ly qu zi lu.

Verabredungsgemäß könnte auch zuerst der Zeilen-Randbuchstabe und dann der Spalten-Randbuchstabe angeschrieben werden.

Mit dieser Schachbrettchiffre hat eine gewisse Ähnlichkeit die sogenannte Mühlbrettchiffre, für welche ich zu Unterrichtszwecken ein kleines Chiffriergerät konstruiert habe.

Der Absender und der Empfänger der Geheimschrift besitzen beide ein Mühlbrett. Die Stellen, in welchen die Mühlbrettlinien sich schneiden oder aneinanderstoßen, sind kreisförmig ausgestanzt, wie die Text-Fig. 1 zeigt.

Außerdem besitzen der Absender und der Empfänger je 24 Kreisblättchen, welche genau in die obenerwähnten ausgestanzten kreisförmigen Löcher hineinpassen. Auf jedem dieser Kreisblättchen ist je ein Buchstabe geschrieben.[18]) Wenn diese

[17]) Nach Figl, Systeme des Chiffrierens.

[18]) Praktische Versuche haben gelehrt, daß der Absender und Empfänger, besonders wenn die Mühlbrettbesetzung häufig geändert wird, relativ zuviel Zeit brauchen, um jeweils das eine bestimmte Buchstabenbezeichnung tragende Kreisplättchen am besetzten Mühlbrett zu finden. Ich habe daher für

Kreisblättchen, was selbstverständlicherweise jedesmal in einer anderen Reihenfolge erfolgt, in das Mühlbrett eingelegt werden, so ist das Mühlbrett an allen Schnitt- und Treffpunkten mit Buchstaben des Alphabetes besetzt, wie z. B. Text-Fig. 2 zeigt.

Die Regeln der Chiffrierung sind folgende:

1. Zwei Buchstaben, welche im Mühlbrett nebeneinanderstehen, bedeuten, daß der nächstfolgende in der durch die zwei

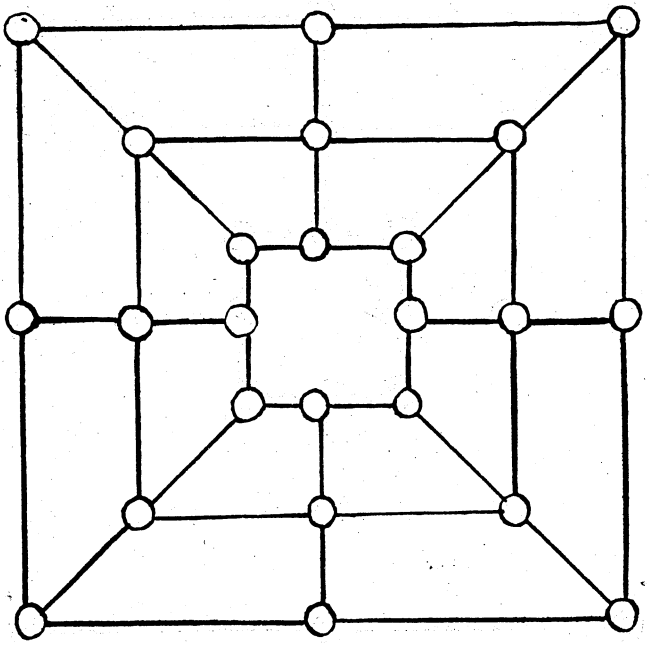


Fig. 1.

Buchstaben angegebenen Richtung zu lesende Buchstabe gemeint ist. Nachdem in Fig. 2 b, i, v nebeneinanderstehen, würde „bi" bedeuten, daß man in der Richtung von „b" nach „i" weiterlesen und den nächstfolgenden Buchstaben „v" als Klarschrift anzunehmen hat. Würde die Chiffre aber „vi" lauten, dann hätte man in der Richtung „vi" zu lesen und wäre „b"

je vier Buchstaben Kreisplättchen bestimmter Farbe gewählt, u. zw. für „a bis e" rote, für „f bis k" gelbe, für „l bis p" grüne, für „q bis u" blaue, für „v bis z" graue Plättchen. Das Mühlbrett selbst ist weiß, die Striche auf demselben sind schwarz.

als Klarbuchstabe gemeint. Man kann also nach dieser Geheimschrift „b“ ausdrücken durch „vi“, „wg“ und „dm“.

2. Zwei im Mühlbrett nicht nebeneinander-, aber auf derselben Linie liegende Buchstaben bedeuten, daß der im Mühlbrett zwischen ihnen liegende Buchstabe als Klarbuchstabe gemeint ist. Also „bv“ oder auch „vb“ würden bedeuten, daß in

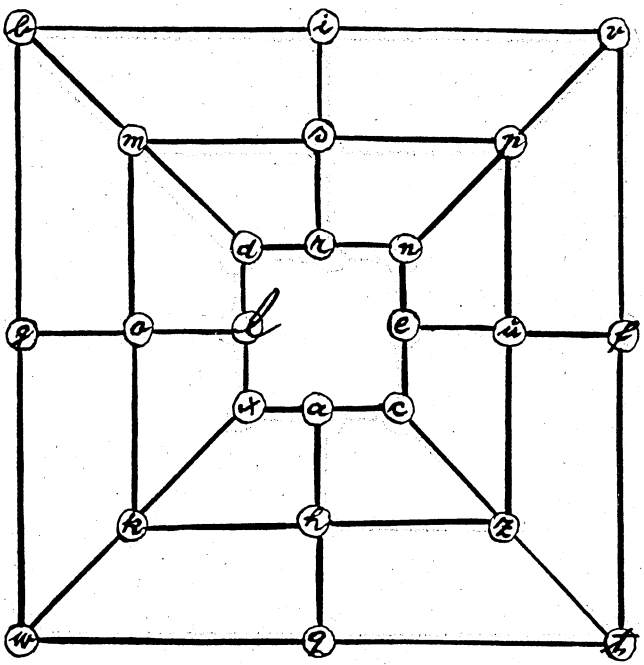


Fig. 2.

der Klarschrift statt dieser zwei Buchstaben „i“ zu setzen ist. Man kann nach dieser Methode also „i“ ausdrücken nach Regel 2 durch „bv“, „vb“ und nach Regel 1 durch „rs“. Um ein anderes Beispiel zu wählen: Man kann „u“ ausdrücken durch: „ef“, „fe“, „zp“ und „pz“, und man kann „z“ ausdrücken durch: „kh“, „ct“, „tc“ und „pu“.

Will nach einigen Worten oder Sätzen der Absender, um die Frequenz zu maskieren, die Besetzung des Mühlbrettes ändern und das Mühlbrett z. B. besetzen wie in Fig. 3, so braucht er dem Empfänger bloß zeilenmäßig die Reihenfolge der Blättchen,

also der Buchstaben, mitzuteilen, nämlich im konkreten Falle (Fig. 3):

o a l i k h u p s n v q t w m z x r e f g c b d.[19])

Das Wechselzeichen wäre z. B. ww, also nach Fig. 2 x k, b g.

Die Mitteilung „Komme sofort, ich erwarte dich" würde also bei gewechselter Mühlbrettbesetzung, u. zw. zuerst nach Fig. 2, dann nach Fig. 3, folgendermaßen lauten:

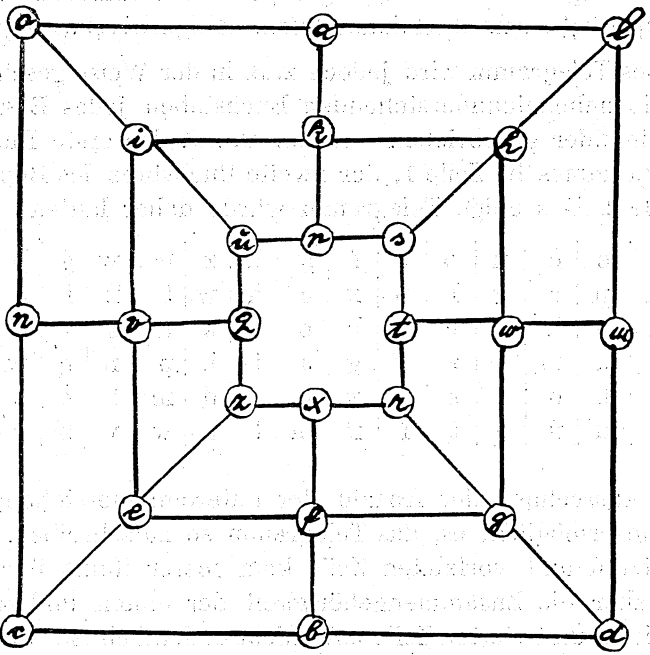


Fig. 3.

Angabe der ersten Besetzung des Mühlbrettes (Fig. 2):

b i v m s p d r n g o l e u f x a c k h z w q t.

Text: „Komme sofort":

wxglbdpsfu rimkeukmndcz.

W W „xkbg".

[19]) Statt die Stellung des Mühlbrettes anzugeben, genügt es auch, ein Stichwort zu vereinbaren, welches die Stellung der ersten Buchstabenreihen andeutet, auf welche dann die restlichen Buchstaben in alphabetischer Reihenfolge folgen. Ist das Stichwort z. B. „Oldenburg", so wäre das Mühlbrett wie folgt besetzt: „oldenburgacfhikmpqstvwxz".

Angabe der neuen Besetzung des Mühlbrettes (Fig. 3):

o a l i k h u p s n v q t w m z x r e f g c b d.

Text: „Ich erwarte dich“:

ouzesl gfzxtmoldgmwiv cbevongw.

Das ganze Telegramm würde also lauten:

„bivmspdrngoleufxackhzwqtwxglbdpsfurimkeukmndczxkbgoalik-
hupsnvqtwmzxrefgcbdouzeslgfzxtmoldgmwivcbevongw.“

Dieses Telegramm wird jedoch z. B. in der Weise geschrieben, daß die nebeneinanderstehenden Buchstaben jedes Bigrammes untereinander geschrieben werden, u. zw. der erste Buchstabe des Bigrammes in Zeile 1, der zweite Buchstabe des Bigrammes in Zeile 2. Das obige Telegramm würde daher lauten:

b	v	s	d	n	o	e	f	a	k	z	q	w	g	b	p	f
i	m	p	r	g	l	u	x	c	h	w	t	x	l	d	s	u
r	m	e	k	n	c	x	b	o	l	k	u	s	v	t	m	x
i	k	u	m	d	z	k	g	a	i	h	p	n	q	w	z	r
e	g	b	o	z	s	g	z	t	o	d	m	i	c	e	o	g
f	c	d	u	e	l	f	x	m	l	g	w	v	b	v	n	w

Ein Ausrechnen der Anzahl der untereinanderstehenden Bigramme ermöglicht es, das Telegramm so zu schreiben, daß in der letzten und vorletzten Zeile kein leerer Raum übrigbleibt und daher die Zusammengehörigkeit der ersten und zweiten, der dritten und vierten Zeile usw. nicht ersichtlich ist. Im übrigen könnte man den leeren Raum eventuell durch Nieten ausfüllen. Nieten sind in dieser Geheimschrift sehr leicht anzubringen. Je zwei Buchstaben des Mühlbrettes, die nicht in einer Linie liegen, müssen Nieten sein, z. B. nach Fig. 2:

„ba, bc, be, bf, bh, bk, bl, bn, bo, bp, bq, br, bs, bt, bu, bx, bz“,

und so ähnlich rücksichtlich aller anderen Buchstaben, z. B.:

ab, ad, ae, af, ag, ai, ak, al, am, an, ao usw.

Diese ganz unverhältnismäßig große Anzahl von Nieten macht ein häufiges Wechseln der Mühlbrettstellung ganz unnötig, da durch diese Nieten einerseits, durch die verschiedenen Varianten, welche für jeden Buchstaben möglich sind, und ander-

seits durch das Schreiben der Bigramme auf zwei verschiedenen Zeilen die Frequenzberechnung beinahe unmöglich wird.

Will man auch die Gefahr ausschließen, daß die Wiederholung zweier Buchstaben, die z. B. in Zeile 1 und 2, 3 und 4, 5 und 6 usw. etwa auffalle, so schreibt man die Bigramme gekreuzt jeweils in die 1. 3., 2. 4., 5. 7., 6. 8. Zeile, oder 1. 4., 2. 5. und 3. 6. Zeile usw.

Obiges Telegramm würde also lauten (Z. 1, 4, Z. 2, 5, Z. 2, 3 usw.):

b	v	s	d	n	o	e	f	a	k	z	q	w	g	b	p	f
r	m	e	k	n	c	x	b	o	l	k	u	s	v	t	m	x
e	g	b	o	z	s	g	z	t	o	d	m	i	c	e	o	g
i	m	p	r	g	l	u	x	c	h	w	t	x	l	d	s	u
i	k	u	m	p	z	k	g	a	i	h	p	n	q	w	z	r
f	c	d	u	e	l	f	x	m	l	g	w	v	b	v	n	w

Auch nach dem Prinzipe der sogenannten Multiplikationschiffre oder des sogenannten Chiffrierquadrates lassen sich Geheimschreibapparate konstruieren.

Im Multiplikations-Chiffrenquadrate[20]) sind 25 verschiedene, untereinander niedergeschriebene Julius-Cäsar-Alphabete von vier Alphabeten eingerahmt.

Das oberste und unterste dieser Alphabete nennt man die Sprachlinien, das rechte und das linke Alphabet die Wahllinien.

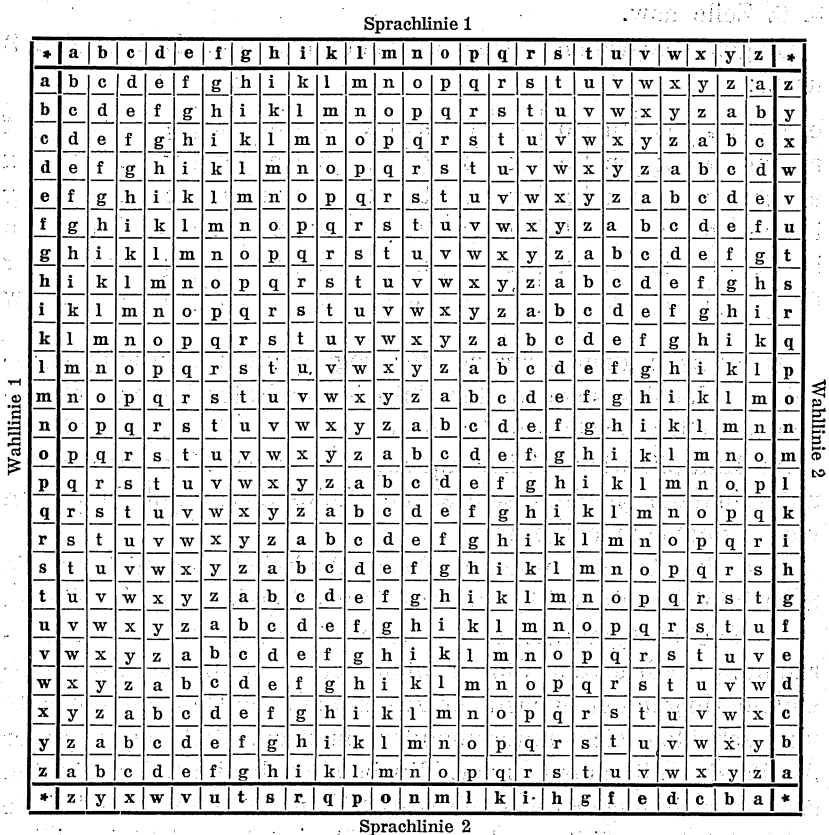
In obigem Quadrate setzen sich die innerhalb dieser Einrahmung gedruckten Chiffrenalphabete aus alphabetisch aufeinanderfolgenden Buchstaben zusammen. Die Chiffrenalphabete unterscheiden sich untereinander dadurch, daß jedes dieser Alphabete mit einem andern Buchstaben beginnt. Es könnten selbstverständlicherweise ebenso 25 verschiedene Alphabete solcher Art gewählt werden, deren Buchstaben nicht in alphabetischer Reihenfolge aufeinanderfolgen.

Der Geheimschreiber und der Empfänger besitzen beide dasselbe, nämlich das oben abgedruckte Chiffrenquadrat. Lautet der zu chiffrierende Klartext z. B.: „Komme sofort an den vereinbarten Ort“ und wurde „Amen“ als Wahlwort vereinbart, so schreibt der Geheimschreiber:

[20]) Man kann verwenden: Sprachlinie 1 mit Wahllinie 1 oder mit Wahllinie 2, weiters Sprachlinie 2 mit Wahllinie 1 oder mit Wahllinie 2.

„Komme sofort an den vereinbarten Ort“
amena menname na men amenamenamen ame

Der Geheimschreiber sucht nun z. B. auf der Quadratseite, welche mit Sprachlinie 1 bezeichnet ist, den jeweiligen Buchstaben des Klartextes und auf der Quadratseite, welche mit



*	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	*
a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	z
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	y
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	x
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	w
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	v
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	u
g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	t
h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	s
i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	r
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	q
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	p
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	o
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	n
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	m
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	l
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	k
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	i
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	h
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	g
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	f
v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	e
w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	d
x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	c
y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	b
z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
*	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	i	h	g	f	e	d	c	b	a	*

Wahllinie 1 bezeichnet ist, den unter diesem Klarbuchstaben stehenden Buchstaben des Wahlwortes auf. In jenem Quadrate, in welchem sich die beiden Streifen, nämlich der Vertikalstreifen des Klarbuchstaben und der Horizontalstreifen des Wahlbuchstaben, treffen, ist der Buchstabe zu finden, welcher im Chiffrentexte an Stelle des Klarbuchstaben zu treten hat. Also in unserem Falle:

Sprachlinie 1	Wahllinie 1	Chiffre
K	a	l
o	m	a
m	e	r
m	n	z
e	a	f
s	m	e
o	e	t
f	n	t
o	a	p
r	m	d
t	e	y

Ein Konsulent des kriminalistischen Laboratoriums der Polizeidirektion Wien, Herr Staatsanwalt Dr. Wladimir Fikeis, hat die Methode des chiffrierten Quadrates unter Benützung der Selbstchiffriermethode und insbesondere einer seinerzeitigen Chiffre der päpstlichen Kurie auf folgende Weise modifiziert:

Zwischen Geheimschreiber (Chiffreur) und Empfänger (Dechiffreur) wird kein Wahlwort vereinbart. Der erste Buchstabe des Klartextes ist auch der erste Buchstabe des Wahltextes. Der erste aus diesem Klar- und Wahlbuchstaben sich ergebende Chiffrebuchstabe ist gleichzeitig zweiter Wahlbuchstabe für den zweiten Buchstaben des Klartextes usw. Der zweite sich ergebende Chiffrebuchstabe wird als dritter Wahlbuchstabe verwendet und unter den dritten Buchstaben des Klartextes geschrieben usw. Also in unserem Beispiele unter Verwendung der Sprachlinie 1 und der Wahllinie 1:

Klarbuchstaben: K o m m e s o f o r t .
Wahlbuchstaben: K u i v h n f u a p g .
Chiffrebuchstaben: u i v h n f u a p g a .

Geheimschreiber (Chiffreur) und Empfänger (Dechiffreur) können vorsichtsweise vereinbaren, daß und wo in der chiffrierten Mitteilung der erste Chiffrebuchstabe versteckt werde.

Die Mitteilung „Komme sofort“ würde ohne Verstecken des ersten Chiffrebuchstaben lauten:

u i v h n f u a p g a.

Nach Verstecken des ersten Chiffrebuchstaben, z. B. an fünfter Stelle, würde diese Mitteilung lauten:

i v h n u f u a p g a.

Statt des Chiffrenquadrates kann man sich nun begreiflicherweise auch eines Gerätes bedienen, welches in Tafel H, Fig. II, dargestellt ist.

Auf der festen Schiene ist das Chiffrendoppelalphabet n bis z, a bis z, a bis m, auf dem Schieber das Klaralphabet a bis z angebracht. Würde man bei diesem Apparat einfach jenen Buchstaben ablesen, der nach entsprechender Einstellung des Schiebers sich auf der Schiene über dem jeweiligen Klarbuchstaben des Schiebers befindet, dann würde er sich von einem gewöhnlichen „Julius-Cäsar-Stab“ (Tafel C, Fig. I und II) nicht unterscheiden. Nun zeigt dieser Apparat aber eine weitere Einrichtung, nämlich ein Messingplättchen, das zwei Ausschnitte besitzt. Einer dieser Ausschnitte läßt einen Buchstaben des Schiebers (Index), einer einen Buchstaben der Schiene (Chiffre) frei.

Die Einstellung erfolgt in folgender Weise:

Das Alphabet auf der Schiene ist das Klaralphabet (die Sprachlinie), das Alphabet des Schiebers ist die Wahllinie. Die vereinbarte Einstellung des Messingplättchens bleibt während der Chiffrierung stets die gleiche. Als Chiffre gilt der im oberen Fenster des Plättchens ersichtliche Buchstabe. Ist z. B. das Wort „zurück“ zu chiffrieren und wurde als Wahlwort das Wort „Amen“ gewählt, so müßte der Schieber zur Schiene so gestellt werden, daß der Buchstabe a des Schiebers unter z der Schiene steht. Ist das Plättchen am Schieber so eingestellt wie in Tafel H, Fig. II, dann läßt dieses Plättchen am Schieber den Index g frei. Bei Einstellung des Schiebers a unter z erscheint im oberen Fenster als Chiffre f. Dieser Buchstabe ist bei Anwendung des Wahlwortes „Amen“ also Chiffre für z. Eine Variation ist aber nicht nur durch Veränderung des Wahlwortes möglich. Das Messingplättchen mit den zwei Ausschnitten läßt sich am Schieber verschiedenartig stellen. Im vorliegenden Falle ist es mittels Schraube derart am Schieber befestigt, daß

der Buchstabe g des Schiebers im Ausschnitte ersichtlich ist. Es läßt sich die Schraube selbstverständlich lockern, das Plättchen schieben und so einstellen, daß das untere Fenster einen andern Buchstaben des Schiebers freiläßt.

Derselbe Apparat muß nicht in Stabform, er kann auch, wie Tafel J, Fig. I, zeigt, in einer der Zirkularscheibe ähnlichen Form konstruiert werden.

In Tafel J, Fig. I, stellt das weiße Ringband die Wahllinie, das graue Ringband die Sprachlinie dar. Der Ausschnitt ist an der Wahllinie derart fest angebracht, daß er über dem Buchstaben c steht.

Wollte nun ein Chiffreur das Wort „zurück" chiffrieren und wäre das Wort „Pauline" Wahlwort, so müßte er P unter Z einstellen. Als Chiffre würde er dann den im Ausschnitte sichtbar werdenden Buchstaben G ablesen.

Tafel J, Fig. II, zeigt denselben Apparat mit verstellbarem Ausschnitte. Er ist in Uhrenform konstruiert. Der beim Uhrbügel befindliche Schraubenknopf dient dazu, die Wahllinie, welche sich im inneren Kreise befindet, zu drehen. Der seitliche Schraubenknopf läßt sich herausziehen und, nachdem er herausgezogen ist, drehen. Mittels dieser Drehung wird das in Form eines Uhrzeigers angebrachte schmale Plättchen mit seinen zwei Ausschnitten gedreht und kann also entsprechend eingestellt werden. Wird dieser seitliche Schraubenknopf wieder niedergedrückt, so bleibt das zeigerähnliche Plättchen über dem entsprechenden Buchstaben der Wahllinie eingestellt. Es dreht sich nicht mehr frei und unabhängig von der Wahllinie. Es dreht sich nunmehr nur bei Drehung des oberen Schraubenknopfes gleichzeitig mit der Wahllinie.

Der Apparat Tafel J, Fig. I und II, unterscheidet sich von dem Apparate Tafel H, Fig. II, nur dadurch, daß letzterer in linearer, endlich begrenzter Stabform, während ersterer als unbegrenzter Kreis, also nach Art der Zirkularscheibe konstruiert ist.

II.

Es existieren unzählige Chiffrier- und Dechiffriergeräte und -maschinen, welche Patentschutz genießen. Unter diesen patentierten Apparaten finden sich primitivste Geräte, welche man mit gutem Gewissen wirklich nicht als eine Erfindung bezeichnen kann, praktische und unpraktische Behelfe, einfachere und komplizierte Maschinen.

Diese Chiffrier- und Dechiffrierapparate werden meist in zwei Gruppen geteilt. In die eine Gruppe fallen jene Apparate, welche in keiner Verbindung zu einer Schreibmaschinentype stehen. In die andere Gruppe aber fallen solche Apparate, welche nach Art einer Schreibmaschine gebaut sind, bzw. solche Apparate, welche eine Chiffrierausgestaltung einer Schreibmaschine oder eines schreibmaschinenähnlichen Apparates bezwecken.

Eine vollständige Aufzählung aller patentierten Chiffrier- und Dechiffriergerätetypen ist schwer möglich. Es lassen sich nämlich Chiffrierapparate und andere Apparate nicht immer voneinander streng abgrenzen. Eine Schreibmaschine z. B., welche irgendeine Stenographieschrift schreibt, kann ja schließlich auch zum Schreiben von Geheimtexten verwendet werden.

Es folgt in diesem Abschnitte daher nur eine tabellarische Zusammenstellung der bekannteren Patente, welche für Chiffrier- und Dechiffriergeräte und -maschinen erteilt wurden. Die Patentschriften selbst sind in den Bibliotheken der Patentämter leicht zugänglich.

Da im letzten Abschnitte dieser Arbeit die Chiffriermaschine System Kryha und die von der Chiffrier-Maschinen-A.-G. in Berlin vertriebene, im Handel und daher in der Praxis am häufigsten vorkommende „Enigma"-Maschine genauer beschrieben wird, sollen in diesem Abschnitte nur jene Patente auszugsweise erörtert werden, bezüglich welcher Ing. Kryha und

Deutschland.

Nr.	Ausgegeben am:	Patentiert ab:
273	ohne Datum	2. Juli 1877
5.650	19. Juli 1879	8. Dezember 1878
14.877	20. August 1881	15. Jänner 1880
18.028	8. Mai 1882	27. April 1881
47.705	5. August 1889	11. August 1888
57.812	28. Juli 1891	6. Mai 1890
61.472	15. März 1892	16. August 1891
67.611	7. April 1893	24. Oktober 1891
67.792	4. April 1893	25. Mai 1892
68.167	25. April 1893	22. September 1892
69.144	17. Juni 1893	14. Dezember 1892
72.239	18. Dezember 1893	9. März 1893
89.897	17. Dezember 1896	12. April 1896
115.344	1. Dezember 1900	6. Juni 1899
116.828	15. Jänner 1901	23. Jänner 1900
125.536	5. Dezember 1901	20. April 1900
146.924	6. Jänner 1904	1. August 1902
147.918	8. Februar 1904	4. Mai 1902
190.965	19. November 1907	25. August 1906
191.568	16. November 1907	21. Jänner 1906
214.719	15. Oktober 1909	15. April 1908
256.905	24. Februar 1913	25. Juni 1912
266.583	28. Oktober 1913	14. Jänner 1912
274.556	23. Mai 1914	14. Juni 1913
275.011	5. Juni 1914	10. April 1913
275.390	18. Juni 1914	14. Februar 1913
275.848	29. Juni 1914	10. April 1913
277.366	21. August 1914	19. Dezember 1913
277.503	24. August 1914	4. März 1913
278.136	25. September 1914	21. Dezember 1913
280.874	3. Dezember 1914	10. April 1913
282.753	15. März 1915	19. Dezember 1913
283.697	4. Mai 1915	7. September 1912
299.994	21. August 1917	31. Dezember 1913
300.919	1. Oktober 1917	2. November 1915
307.655	9. September 1919	1. Juni 1917
307.895	16. September 1918	4. Februar 1917
311.955	3. Mai 1919	28. Februar 1917
311.999	23. April 1919	23. März 1917

Nr.	Ausgegeben am:	Patentiert ab:
326.739	4. Oktober 1920	17. Oktober 1913
329.067	12. November 1920	7. Februar 1919
336.669	7. Mai 1921	10. März 1920
364.184	18. November 1922	6. Juni 1920
366.614	8. Jänner 1923	6. Juni 1920
368.500	6. Februar 1923	8. September 1921
371.087	10. März 1923	10. Juli 1921
371.608	16. März 1923	20. November 1920
372.217	24. März 1923	8. Jänner 1921
380.042	31. August 1923	11. Jänner 1920
383.003	9. Oktober 1923	2. September 1921
383.593	15. Oktober 1923	23. März 1922
383.594	15. Oktober 1923	12. Februar 1922
385.682	27. November 1923	10. Mai 1922
400.795	19. August 1924	18. August 1923
407.804	22. August 1925	18. Jänner 1924
412.582	23. April 1925	25. März 1924
414.283	28. Mai 1925	7. März 1924
414.547	18. September 1925	17. Juni 1922
416.219	8. Juli 1925	23. Februar 1918
416.833	27. Juli 1925	2. Juni 1918
418.344	3. September 1925	1. März 1922
425.147	13. Februar 1926	26. September 1920
425.566	22. Februar 1926	28. Februar 1924

England.

Aus dem Jahre	Nr.	Accepted:	Application bzw. compl. Sp. Left:
AD 1893	7.848	26. August 1893	18. April 1893 21. Juli 1893
AD 1894	223	24. November 1894	4. Jänner 1894 4. Oktober 1894
AD 1895	11.256	18. Jänner 1896	8. Juni 1895 11. November 1895
AD 1896	7.153	5. September 1896	1. April 1896 4. August 1896
AD 1898	16.052	17. September 1898	22. Juli 1898

Aus dem Jahre	Nr.	Accepted:		Application bzw. compl. Sp. Left:	
AD 1899	14.321	12. August	1899	11. Juli	1899
AD 1900	9.908	25. August	1900	29. Mai	1900
AD 1901	12.947	27. Juli	1901	25. Juni	1901
AD 1901	10.526	27. Juli	1901	21. Mai	1901
AD 1902	28.111	19. November	1903	19. Dezember 19. Oktober	1902 1903
AD 1903	22.313	25. August	1904	16. Oktober 15. Juli	1903 1904
AD 1906	20.131	11. Juli	1907	10. September 19. Februar	1906 1907
AD 1907	21.950	4. Juni	1908	4. Oktober 20. November	1907 1907
AD 1907	15.016	29. Juli	1908	29. Juni 28. Dezember	1907 1907
AD 1907	27.010	15. Oktober	1908	16. Dezember	1907
AD 1907	5.259	5. Dezember	1907	5. März	1907
AD 1908	1.260	14. Jänner	1909	18. Jänner 18. August	1908 1908
AD 1908	16.707	6. November (publ. 15. Okt.	1909 1914)	8. August 8. März	1908 1909
AD 1910	22.477	21. September	1911	28. September 7. November	1910 1910
AD 1913	22.590	14. Mai	1914	7. Oktober	1913
AD 1914	7.557	24. Juni	1915	25. März 17. September	1914 1914
AD 1914	7.570	24. Juni	1915	25. März 17. September	1914 1914
	122.886	4. Februar	1919	4. Februar 13. August	1918 1918
	146.990	8. September	1921	6. Juli	1920
	154.962	6. Dezember	1920	5. August	1919
	155.996	6. Jänner	1921	24. Dezember	1919
	162.670	20. Oktober	1921	2. Mai	1921
	163.357	10. Mai	1920	10. November	1919
	176.061	2. März	1922	2. November	1920
	185.171	23. August	1922	23. Mai	1921
	194.375	7. März	1923	7. Dezember	1921
	197.046	10. Mai	1923	10. Februar	1922
	197.763	24. Mai	1923	28. Februar	1922
	214.313	14. April	1924	24. Juli	1923
	231.502	29. Oktober	1925	25. März	1925
	246.307	23. Jänner	1925	28. Jänner	1926

Frankreich.

Nr.	Publiziert (Publié):	Überreicht (Demandé):
342.924	21. September 1904	6. Mai 1904
385.630	19. Mai 1908	27. Dezember 1907
391.626	5. November 1908	24. Juni 1908
400.476	28. Juli 1909	22. Februar 1909
430.516	18. Oktober 1911	11. Mai 1911
443.808	3. Oktober 1912	14. Mai 1912
449.233	20. Februar 1913	27. Juni 1912
455.233	25. Juli 1913	17. März 1913
461.033	17. Dezember 1913	1. August 1913
472.453	8. Dezember 1914	20. März 1914
475.254	3. Mai 1915	31. Jänner 1914
478.943	19. Jänner 1916	1. Oktober 1914

Österreich.

Nr.	Ausgegeben am:	Beginn der Patentdauer:
618	25. November 1899	15. April 1899
5.415	10. Oktober 1901	1. Mai 1901
8.802	25. August 1902	1. Jänner 1902
9.518	25. Oktober 1902	15. Juni 1902
10.979	10. März 1903	15. Oktober 1902
25.405	25. August 1906	15. April 1906
26.892	27. Dezember 1906	1. August 1906
33.211	10. Juni 1908	15. Jänner 1908
40.822	10. Februar 1910	1. September 1909
40.982	10. Februar 1910	1. September 1909
47.390	10. April 1911	1. November 1910
51.351	27. Dezember 1911	1. August 1911
62.926	10. Jänner 1914	15. August 1913
62.927	10. Jänner 1914	15. August 1913
68.881	10. Juni 1915	15. November 1914
70.448	10. November 1915	15. Juni 1915
75.008	25. November 1918	15. Juli 1917
82.833	25. Februar 1921	15. September 1917
83.902	10. Mai 1921	15. Oktober 1919

Nr.	Ausgegeben am:	Beginn der Patentdauer
89.188	10. August 1922	15. Jänner 1922
92.970	11. Juni 1923	15. Dezember 1922
98.207	25. Oktober 1924	15. Mai 1924
98.642	25. November 1924	15. Juli 1924
102.254	11. Jänner 1926	15. August 1925
103.203	26. April 1926	15. Dezember 1925
104.352	11. Oktober 1926	15. März 1926

Schweiz.

Nr.	Veröffentlicht:	Überreicht:
4.985	ohne Datum	23. Mai 1892
65.752	16. Juli 1914	2. Juni 1913
69.656	16. Juli 1915	8. Dezember 1914
73.384	2. Oktober 1916	27. August 1915
97.076	1. Dezember 1922	21. März 1921
97.890	16. Februar 1923	23. August 1921
101.180	17. September 1923	24. Juni 1921
103.902	17. März 1924	23. Jänner 1923
105.263	2. Juni 1924	29. Mai 1923
106.233	16. August 1924	2. Februar 1923
106.569	1. September 1924	21. August 1923

Vereinigte Staaten.

Nr.	Erteilt:	Anmerkung
495.744	18. April 1893	Einige hievon samt Zusatzpatenten
527.112	9. Oktober 1894	
597.587	18. Jänner 1898	
637.049	14. November 1899	
641.004	9. Jänner 1900	
650.716	29. Mai 1900	
657.586	11. September 1900	

Nr.	Erteilt:	Anmerkung
657.587	11. September 1900	Einige hievon samt Zusatzpatenten
666.520	22. Jänner 1901	
678.363	16. Juli 1901	
703.391	1. Juli 1902	
723.288	24. März 1903	
724.786	7. April 1903	
744.041	17. September 1903	
850.091	9. April 1907	
901.957	27. Oktober 1908	
933.679	7. September 1909	
984.832	21. Februar 1911	
1,085.636	3. Februar 1914	
1,086.586	10. Februar 1914	
1,086.823	10. Februar 1914	
1,096.168	12. Mai 1914	
1,152.808	7. September 1915	
1,194.587	15. August 1916	
1,201.486	17. Oktober 1916	
1,205.180	21. November 1916	
1,210.656	2. Jänner 1917	
1,276.616	20. August 1918	
1,285.567	19. November 1918	
1,315.406	9. September 1919	
1,318.366	14. Oktober 1919	
1,326.116	23. Dezember 1919	
1,332.861	2. März 1920	
1,367.311	1. Februar 1921	
1,370.870	8. März 1921	
1,372.797	29. März 1921	
1,426.669	22. August 1922	
1,445.605	13. Februar 1923	
1,455.157	15. Mai 1923	
1,491.350	22. April 1924	
1,500.077	1. Juli 1924	
1,515.680	18. November 1924	
1,516.180	18. November 1924	
1,533.252	14. April 1925	
1,540.107	2. Juni 1925	
1,562.120	17. November 1925	
1,564.268	8. Dezember 1925	
1,568.991	12. Jänner 1926	

der Chiffrier-Maschinen-A.-G. Patentrechte zustehen. Hiedurch wird der dritte Abschnitt dieser Arbeit, welcher sich mit den verschiedenen Modellen der Chiffriermaschine System Kryha und der „Enigma"-Maschine beschäftigt, leichter verständlich.

A.

Österr. Patent Nr. 103.203.

Alexander von Kryha in Berlin: Chiffriervorrichtung. Angemeldet am 16. Jänner 1925. — Beginn der Patentdauer: 15. Dezember 1925.[21])

Die Buchstaben und Ziffern sind auf zwei konzentrischen Scheiben angebracht[22].) Die eine dieser Scheiben (X) liegt auf Stützen, die an der Wand des Gehäuses befestigt sind. Die andere Scheibe (Y) sitzt auf einer hohlen Achse. Letztere Scheibe (Y) ist auf einen Zapfen aufgesteckt, der sich gleichfalls im Gehäuse befindet. Sie trägt ein Sperrad (A) und ein Zahnrad (B_1). Dieses Zahnrad (B_1) steht mit dem eigentlichen Chiffrierrad (C) im Eingriff. Dieses ist auf einer hohlen Achse aufgekeilt. Auf der gleichen Achse sitzt ein zweites Zahnrad (B_2), welches mit dem Zahnrad eines Antriebswerkes (B_3) zusammenwirkt. Das obenerwähnte Sperrad (A) wiederum arbeitet mit einer Klinke und einer Feder zusammen. Ein Griff dient dazu, die Klinke in die gewünschte Sperrlücke zu bringen. Das eigentliche Chiffrierrad (C) ist mit Zahngruppen von regellos wechselnder Zähnezahl besetzt. Diese Zahngruppen sind durch Lücken im Chiffrierrad voneinander gesondert.

Damit in gleichbleibenden Zeitabständen abgelesen werden kann, beträgt die Umfangslänge je einer Zahngruppe zusammen mit der nachfolgenden oder vorhergehenden Zahnlücke — oder zusammen mit der nachfolgenden und der folgenden Zahnlücke — einen für alle Zahngruppen gleichbleibenden Bruchteil des Radumfanges.

Die Triebwerkgeschwindigkeit kann je nach der Bauart des

---

21) Deutsches Patent Nr. 434.642; vgl. Seite 66 bis Seite 71 dieses Buches und die Tafeln K, L.

22) Die Buchstabenbezeichnungen X, Y, A, B_1, B_2, B_3, C beziehen sich nicht auf eine Tafel, sondern dienen nur zur übersichtlichen Differenzierung der Bestandteile. Scheibe X (Klaralphabet) ist unbeweglich. Scheibe Y (Chiffrenscheibe) ist drehbar. Die Chiffrierscheibe ist nicht zu verwechseln mit dem Chiffrierrade C, einem inneren Bestandteile.

Bremshebels durch Hinein-, bzw. Herausschrauben einer Stange bis zu völligem Stillstand nach Belieben verlangsamt werden, um auch dem Ungeübten die Arbeit zu erleichtern.

Beachtet muß werden, daß sowohl beim Chiffrieren wie beim Dechiffrieren das gesamte Getriebe vorwärtsläuft. Eine Umkehrung des Drehsinnes durch Vermittlung eines Umkehrgetriebes nebst Kupplungen ist also nicht erforderlich.

Statt zweier konzentrischer Scheiben können auch zwei parallellaufende Bänder verwendet werden.

Die Patentansprüche lauten auszugsweise:

1. Chiffriervorrichtung, dadurch gekennzeichnet, daß die eine von zwei einander zugeordneten Buchstabenreihen durch Vermittlung eines einzigen Zahnrades mit Lücken am Umfange abwechselnd verstellt und zum Stillstande gebracht wird, derart, daß während der Stillstandspause je ein Buchstabe aus der offenen Schrift in die Geheimschrift oder umgekehrt übertragen werden kann.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß je eine Zahngruppe zusammen mit der nachfolgenden oder der vorhergehenden Lücke des mit Lücken versehenen Zahnrades mit jeder Hälfte der vorangehenden und der folgenden Lücke bei allen Zahngruppen den nämlichen Bruchteil des Radumfanges einnimmt.

3. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß jede der z. B. in Scheiben- oder Bandform ausgeführten Buchstabenreihen und das mit Lücken versehene Zahnrad je für sich zu Beginn der Arbeit einstellbar sind.

4. Vorrichtung nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, daß die zusammengehörigen Zeichen beim Chiffrieren und Dechiffrieren durch einen Zeiger bestimmt werden, der auf zwei konzentrischen Ringschienen des Deckels beweglich ist und ein Fenster und eine Spitze aufweist, die die zusammengehörigen Zeichen bestimmen.[23])

---

23) Der Zeiger hat ein Fenster und eine Spitze. Will der Anfänger chiffrieren, so schiebt er den Zeiger mit seinem Fenster über den der offenen Schrift entnommenen ersten Buchstaben der Scheibe (Y) und liest dann bei der Zeigerspitze den zugehörigen Buchstaben der Geheimschrift ab oder umgekehrt. Nach einiger Übung ist indessen die Benutzung des Zeigers nicht mehr notwendig, sondern es können mit bloßem Auge die zusammen-

5. Vorrichtung nach den Ansprüchen 1 bis 4, gekennzeichnet durch eine Sperrklinke mit einer Feder und Handgriff zur jeweiligen Feststellung der bewegten Typenscheibe in der Ablesestellung.

B.

1.

Patent Nr. 383.594.

Klasse 42 *n*, Gruppe 14, ausgegeben am 15. Oktober 1923.
Patentiert im Deutschen Reiche vom 12. Februar 1922 ab.
(Naamlooze Vennotschap Ingenieursbureau „Securitas“ in Amsterdam.)[24])

Zum Chiffrieren von Klartext und zum Dechiffrieren werden Maschinen verwendet, welche entweder ähnlich wie eine Schreibmaschine die chiffrierten Buchstaben schreiben oder einen chiffrierten Telegraphenlochstreifen herstellen od. dgl. Die Wirkungsweise dieser Maschinen beruht z. B. darauf, daß die Kraftschlüsse zwischen den mit den Buchstaben des Alphabetes bezeichneten Tasten einerseits und den Typenhebeln, bzw. den Hebeln eines Telegraphenlochers andererseits nach dem Geben eines oder einer bestimmten Anzahl von Buchstaben jedesmal vertauscht werden. Geht bei zwei derartigen Maschinen diese an sich regellose Vertauschung in der genau gleich fortschreitenden Weise vor sich, so kann ein mit Hilfe der einen Maschine chiffriertes Telegramm mit Hilfe der korrespondierenden Maschine dechiffriert werden. Allerdings muß dabei die von der gleichen Ausgangsstellung ab gerechnete Zahl der Buchstaben die gleiche geblieben sein. Bei Telegrammen, vor allem in der drahtlosen Telegraphie, muß aber damit gerechnet werden, daß einzelne Buchstaben oder ganze Buchstabengruppen ausfallen können. Dadurch käme die zum Dechiffrieren dienende Maschine aus dem Takte, so daß nicht nur die ausgefallenen Buchstaben entfallen würden, sondern

---

gehörigen Buchstaben erkannt werden. Auch das Umsetzen des Zeigers beim Übergang vom Chiffrieren zum Dechiffrieren ist nur für den Anfänger erforderlich.

24) Vgl. zu diesem und den folgenden Patenten Seite 71 bis Seite 94 dieses Buches und die Tafeln M, N, O, P, Q.

der gesamte, auf die Lücke folgende Text nicht mehr dechiffriert werden könnte.

Die Erfindung will diesen Übelstand dadurch vermeiden oder wenigstens beliebig einschränken, daß eine „Vorrichtung an der Chiffriermaschine" dem die Maschine Bedienenden die „Fertigstellung einer Buchstabenreihe von bestimmter Länge" jedesmal bemerkbar macht. Dieser kann dann den Beginn der neuen Buchstabenreihe in dem chiffrierten Text markieren, so daß die Stellung der zum Dechiffrieren dienenden Maschine nach jeder Buchstabenreihe verglichen und, wenn nötig, berichtigt werden kann. Am einfachsten kann die Fertigstellung der Buchstabenreihe durch Anschlagen einer Klingel oder durch das Aufleuchten einer Glühlampe bemerkbar gemacht werden. Auch könnte die Maschine nach Beendigung dieser bestimmten Buchstabenreihe selbsttätig ganz oder teilweise stillgesetzt oder abgeschaltet werden, u. zw. derart, daß ein Weiterschreiben unmöglich wäre. Es könnte z. B. der die Vertauschung der Buchstaben bewirkende Mechanismus sich abstellen, bzw. die Maschine derart umgeschaltet werden, daß sie Klartext schreibt. Das hat den Vorteil, daß ein sofort kenntlicher Vermerk im Klartext mitgegeben und nach dessen Wiedergabe mit der während dessen nicht verstellten Maschine weiterchiffriert werden kann. Ein solcher Vermerk kann z. B. in einer Kontrollziffer bestehen, etwa in der Anzahl der bisher gegebenen Buchstaben. Es kann auch für jede Buchstabenreihe ein neuer Schlüssel auf der Maschine eingestellt werden und dieser im Klartext, zur Sicherheit mehrmals, bekanntgegeben werden.

Beim Anfertigen schriftlicher Chiffrentexte durch unmittelbar schreibende oder anzeigende Maschinen hat die Angabe der Buchstabenanzahl je nach einer Buchstabenreihe von bestimmter Länge die gleichen Vorteile, da hiedurch das Dechiffrieren erleichtert wird. Auch hier ist es daher wichtig, den Chiffrierenden auf die Fertigstellung einer Buchstabenreihe bestimmter Länge aufmerksam zu machen.

Die Chiffriermaschine kann auch eine Vorrichtung haben, welche nach einer bestimmten Anzahl von Buchstaben selbsttätig eine Markierung durch einen größeren Zwischenraum, durch Überspringen einer Zeile oder durch Abdrucken einer Zahl anbringt.

Die verschiedenen Ausführungsformen dieser Maschine sind charakterisiert:

1. Durch eine selbsttätige Vorrichtung, durch welche die Fertigstellung einer Buchstabenreihe von bestimmter Länge jedesmal besonders bemerkbar gemacht wird.

2. Durch eine Zählvorrichtung, von welcher diese — die Fertigstellung der Buchstabenreihe bemerkbar machende — Vorrichtung gesteuert wird.

3. Durch ein gebräuchliches Zählwerk mit nach dem Dezimalsystem unterteilten Zifferscheiben als Zählvorrichtung. (Der Betriebsstrom wird mindestens für einen Teil der Bewegungsantriebe der Maschine durch Schleifkontakte über die einzelnen Zifferscheiben geführt und durch auf diesen angebrachte isolierte Teile bei bestimmten Stellungen des Zählwerkes unterbrochen.)

4. Dadurch, daß die Schleifkontakte parallel geschaltet sind. (Einzelne können abgeschaltet werden, u. zw. zu dem Zwecke, die Länge der chiffrierten Buchstabenreihe beliebig wählen zu können.)

5. Dadurch, daß durch die Zählvorrichtung ein Klingelzeichen betätigt oder eine Glühlampe zum Aufleuchten gebracht wird.

6. Dadurch, daß durch die Zählvorrichtung die Maschine mindestens teilweise außer Betrieb gesetzt wird.

7. Dadurch, daß durch die Zählvorrichtung nur das Schaltwerk der Chiffriermaschine einschließlich der Zählvorrichtung selbst außer Betrieb gesetzt wird.

8. Durch eine Vorrichtung, durch welche die Maschine auf Klartext umgeschaltet werden kann.

9. Dadurch, daß bei der Rückführung der Umschaltvorrichtung auf Klartext in ihre Ausgangsstellung die Maschine selbsttätig wieder betriebsfertig gemacht wird.

10. Dadurch, daß das Schaltwerk der Maschine einschließlich der Zählvorrichtung abgeschaltet ist, solange auf der Maschine Klartext geschrieben wird.

11. Dadurch, daß die Umschaltung auf Klartext von der Zählvorrichtung selbsttätig bewirkt wird.

12. Dadurch, daß die Maschine selbsttätig zwischen dem Chiffriertext nach bestimmten Abschnitten verabredete Zeichen oder Buchstabenzahlen, bzw. Gruppenzahlen einfügt.

13. Dadurch, daß die Maschine selbsttätig zwischen dem Chiffriertext nach bestimmten Abschnitten Abstände einfügt.

14. Dadurch, daß der zum Zwecke der Buchstabenzahlkontrolle eingefügte Text von der Maschine selbsttätig als Kontrolltext (beispielsweise durch gesperrte Schrift) kenntlich gemacht wird.[25])

2.

Patent Nr. 385.682.

Klasse 42*n*, Gruppe 14, ausgegeben am 27. November 1923.

Patentiert im Deutschen Reiche vom 10. Mai 1922 ab.

(Naamlooze Vennotschap Ingenieursbureau „Securitas" in Amsterdam.)

Die Erfindung will die Chiffriersicherheit solcher Chiffriermaschinen erhöhen, mit welchen zeilenförmig angeordnete Zeichenreihen geschrieben werden. Die Patentschrift erblickt das technisch Wesentliche früherer ähnlicher Erfindungen darin, *a)* daß die überhaupt zur Verwendung kommenden Zeichen untereinander vertauscht werden, *b)* daß außerdem noch in den einzelnen Zeilen des bereits chiffrierten Textes die Zeichen durcheinandergewürfelt werden. Der Nachteil dieser früheren Erfindungen bestehe aber darin, daß man — um bei solchen Maschinen das Dechiffrieren möglich zu machen — für die ganze Zeile das gleiche Tauschalphabet verwenden müsse.

Die Neuerfindung bestehe darin, daß trotz des „Umwürfelns des chiffrierten Textes innerhalb der Chiffrenzeile" für die ganze Zeile nicht mehr das gleiche Tauschalphabet verwendet werden müsse. Man könne vielmehr auch innerhalb der Zeile beliebig viele Tauschalphabete, also z. B. auch für jedes Zeichen ein neues Tauschalphabet anwenden.

In der Maschine ist nämlich eine Austauschvorrichtung (Vielfachschalter od. dgl.) so angebracht, daß sie „in Abhängigkeit von der Stellung der Klarzeichen oder von der Stellung der chiffrierten Zeichen innerhalb der Zeile, z. B. auch für jedes einzelne Zeichen, ein neues Tauschalphabet selbsttätig einstellt". Dadurch wird erreicht, daß beim Dechiffrieren jedes chiffrierte Zeichen mit demjenigen Tauschalphabete dechiffriert wird, mit welchem es chiffriert wurde, gleichgültig, in welcher Weise

25) Die in der Fachliteratur ungebräuchlichen Ausdrücke, wie z. B. „Chiffriertext", werden nur deshalb unverbessert in obigem „Auszuge aus der Patentschrift" wiedergegeben, um fachliche Bezeichnungen, deren sich der Erfinder bedient, nicht zu ändern.

die Umwürfelung der chiffrierten Zeichen innerhalb der Zeile vorgenommen wurde.

„Zur weiteren Vergrößerung der Zahl der verwendeten Tauschalphabete kann dann noch eine besondere Tauschvorrichtung vorgesehen werden. Sie wird nach jeder Zeile verstellt, um für jede Zeile neue Tauschalphabete benützen zu können. Jedes dieser Tauschalphabete wird durch die von der Zeichenstellung innerhalb der Zeile abhängige Tauschvorrichtung in eine der Zeichenzahl der Zeile entsprechende Anzahl neuer Tauschalphabete abgeändert."

Die Patentansprüche dieser Chiffriermaschine lauten im wesentlichen:

1. Chiffriermaschine zum Schreiben von zeilenförmig angeordneten Zeichenreihen, wobei die zu übermittelnden Zeichen (z. B. unter Verwendung von Tauschalphabeten) gegeneinander ausgetauscht und dann noch innerhalb der Zeilen durcheinandergewürfelt werden. Die Maschine ist gekennzeichnet durch eine besondere Austauschvorrichtung (Vielfachschalter usw.). Diese ist derart eingerichtet, daß sie in Abhängigkeit von der Stellung der Zeichen innerhalb der Zeile des Klartextes oder des chiffrierten Textes für verschiedene Buchstaben, gegebenenfalls jeden Buchstaben, selbsttätig ein neues Tauschalphabet einstellt.

2. Chiffriermaschine nach Anspruch 1, bei welcher aber neben der Austauschvorrichtung, welche für die Zeichen innerhalb der Zeile verschiedene Tauschalphabete einstellt, eine zweite in Reihe dazugeschaltete Austauschvorrichtung vorgesehen ist. Diese kann nach jeder Zeile verstellt werden, damit für jede Zeile neue Tauschalphabete benützt werden können.

3. Chiffriermaschine nach Anspruch 1 und 2. Sie besitzt eine der Zeichenzahl der Zeile entsprechende Anzahl von Vielfachschaltern. „Je einer von diesen wird in Abhängigkeit von der Stellung des Zeichens innerhalb der Zeile geschlossen." Sie sind in die Stromleitungen, die zur Zeichenübertragung dienen, so eingeschaltet, daß die Zeichen durch jeden Vielfachschalter in anderer Weise untereinander vertauscht werden.

4. Chiffriermaschine nach Anspruch 3, bei welcher aber nur die im Klartext am häufigsten vorkommenden Zeichen zur Vertauschung durch Vielfachschalter eingerichtet sind.

5. Chiffriermaschine nach Anspruch 3 und 4, bei welcher

einzelne oder alle Vielfachschalter in Abhängigkeit von der Stellung mehrerer Zeichen innerhalb der Zeile betätigt werden.

6. Chiffriermaschine nach Anspruch 1 und 2, gekennzeichnet durch die Verwendung nur eines Vielfachschalters zur Einstellung aller in einer Zeile verwendeten Tauschalphabete.

7. Chiffriermaschine nach Anspruch 1, 2 und 6, bei der zum Einstellen der Tauschalphabete eine Mehrzahl von gegeneinander verstellbaren Vielfachschaltern verwendet wird. (Einer dieser Vielfachschalter ist derart eingerichtet, daß er in Abhängigkeit von der Stellung des Zeichens innerhalb der Zeile verstellt wird.)

3.

Patent Nr. 400.795.

Klasse 42*n*, Gruppe 14, ausgegeben am 19. August 1924.

Patentiert im Deutschen Reiche vom 18. August 1923 ab.

(Naamlooze Vennotschap Ingenieursbureau „Securitas" in Amsterdam.)

Während Chiffriermaschinen gewöhnlich aus einer Tastatur einerseits, einer Schreibvorrichtung andererseits und endlich aus einer zwischen Tastatur und Schreibvorrichtung eingeschalteten Tauschvorrichtung bestehen, besitzt die Chiffriermaschine, auf welche sich dieses Patent bezieht, zwei Schreibvorrichtungen. Die eine Schreibvorrichtung kann nur unmittelbar mit der Tastatur verbunden werden. Sie schreibt daher den auf der Tastatur getypten Klartext. Die andere Schreibvorrichtung kann mit der Tastatur nur über eine Tauschvorrichtung verbunden werden. Diese Schreibvorrichtung chiffriert daher den auf der Tastatur getypten Klartext. Die Ausrüstung der Chiffriermaschine mit zwei derartigen Schreibvorrichtungen ermöglicht es, neben dem Geheimtexte zwecks Nachprüfung gleichzeitig auch den Klartext zu schreiben. Wird die Schreibwalze in einer bestimmten Weise[26]) verschiebbar angeordnet, dann kann jederzeit in den chiffrierten Text der Klartext eingefügt werden.

Der Chiffreur wird manchmal genötigt sein, in seinem chiffrierten Texte eine bestimmte Stelle des Klartextes zu suchen.

26) Der Teil der Chiffrierwalze, welcher vor der den chiffrierten Satz schreibenden Vorrichtung steht, kann vor die den Klartext schreibende Vorrichtung gestellt werden.

Es muß daher die Zahl der chiffrierten Zeichen von einer bestimmten Stelle bis zu einer andern bestimmten Stelle des Chiffrates ermittelt werden können. Schreibt eine Chiffriermaschine nicht auf fortlaufenden Streifen, sondern in Zeilen, so soll beim Chiffrieren von der Maschine in jeder Zeile nur eine ganz bestimmte, wenn möglich durch zehn teilbare Anzahl von Zeichen geschrieben werden.

Wird in den Chiffrentext Klartext „eingestreut", so würde hiedurch das Auffinden einer bestimmten Stelle im Chiffrentext erschwert werden.

Es wird daher von der patentierten Chiffriermaschine die Schreibfläche beim Hinüberschieben von der einen Schreibvorrichtung zur andern selbsttätig um einen Zeilenabstand verstellt.

Zu der den chiffrierten Text schreibenden Vorrichtung kann die Schreibfläche aber nur in dieselbe Stellung innerhalb der Zeile zurückgeführt werden, aus welcher sie entfernt wurde. Dies wird erreicht durch zwei getrennte Antriebsvorrichtungen, mit welchen die Schreibwalze gekuppelt wird, je nachdem, ob Chiffren- oder Klartext geschrieben werden soll. Solange Klartext geschrieben wird, bleibt die zum Schreiben des Chiffrentextes dienende Antriebsvorrichtung stehen.

Ein mit einer derartigen Vorrichtung geschriebener Text (z. B. Zeilenlänge 30 Zeichen) würde folgendermaßen aussehen:

1. Zeile: qscft zgvbh njmki ngrdw rdxcf pojzg
2. Zeile: dzgvh zb

Jetzt folgt z. B. Klartext in einer beliebigen Quantität, dann als weiterer Chiffrentext:

. . . . . frd tfgkp mhtrs vdwqa kuipo.

4.

Patent Nr. 408.949.

Klasse 15*g*, Gruppe 23, ausgegeben am 14. Mai 1925.

Patentiert im Deutschen Reiche vom 9. September 1923 ab.

(Chiffrier-Maschinen-A.-G. in Berlin.)

Betrifft eine Bremsvorrichtung für umlaufende Typenräder, welche zum Abdrucke eines bestimmten Buchstaben mittels eines auf der gleichen Welle mitumlaufenden Sperrades durch einen einfallenden Haken an einer bestimmten Stelle festgehalten werden, etc.

5.

Patent Nr. 411.126.

Klasse 42 *n*, Gruppe 14, ausgegeben am 24. März 1925.
Patentiert im Deutschen Reiche vom 18. August 1923 ab.
(Naamlooze Vennotschap Ingenieursbureau „Securitas“ in Amsterdam.)

Bei der oberwähnten Chiffriermaschine ist zwischen die Zeichengeber (Tastatur) und die Zeichenempfänger (Schreibvorrichtung) eine aus einem oder mehreren Gliedern bestehende Tauschvorrichtung eingeschaltet. Die Glieder dieser Tauschvorrichtung sollen nun nach dem Geben eines oder mehrerer Zeichen jedesmal verstellt werden. Ihre Stellung bei Beginn des Chiffrierens bildet den sogenannten Schlüssel. Seine Kenntnis ermöglicht das Entziffern des Chiffrates auf jeder gleichgebauten Chiffriermaschine.

Der Patentanspruch dieser Erfindung lautet:

„Chiffriermaschine mit einer aus einem oder mehreren Gliedern bestehenden Tauschvorrichtung zwischen den Zeichengebern und den Zeichenempfängern, dadurch gekennzeichnet, daß die die Stellung der Tauschvorrichtung und des Antriebes anzeigenden Zeichen (z. B. Buchstaben), welche den Schlüssel für das Chiffrieren darstellen, auf besonderen Zwischengliedern aufgetragen sind, die sich auf ihren Unterlagen nach besonderer Verabredung mechanisch gegeneinander verschieben und einstellen lassen.“

Hiemit wollte der Erfinder den Vorteil erreichen, daß zu jedem Schlüssel jede beliebige Stellung der Tauschglieder gehören könne. Der Schlüssel brauche daher nicht mehr geheimgehalten zu werden. Man könne ihn sogar dem Chiffrate in Klartext beifügen.

6.

Patent Nr. 412.582.

Klasse 42 *n*, Gruppe 14, ausgegeben am 23. April 1925.
Patentiert im Deutschen Reiche vom 25. März 1924 ab.
(Chiffrier-Maschinen-A.-G. in Berlin.)

Betrifft die Blockierung von Chiffrierelementen bei Chiffriermaschinen.

Bei Chiffriermaschinen, besonders bei elektrischen Chiffrier-

maschinen, sind eine Anzahl von Chiffrierelementen vorhanden. Durch diese wird hintereinander der elektrische Strom hindurchgeleitet. Durch ihre Stellung zueinander ergeben sie das bestimmte Chiffriersystem, nach welchem die Vertauschung der Zeichen erfolgt. Diese einzelnen Chiffrierelemente werden während des „Chiffrierens einer größeren Anzahl von Zeichen" selbsttätig durch die Chiffriermaschine unregelmäßig verstellt, so daß das Tauschsystem verändert wird. Das durch eine solche Chiffriermaschine hergestellte Chiffrat kann nur durch eine gleichgebaute Chiffriermaschine dechiffriert werden, bei welcher die Veränderung des Tauschsystems nach genau den gleichen Gesetzen erfolgt wie bei der ersten Maschine. Die beiden Maschinen müssen also gewissermaßen in gleichem Tritte arbeiten.

Solche Chiffrierelemente bestehen vielfach aus Walzen mit Kontakten an den Stirnseiten; die Verstellung der Walzen geschieht durch Zahnräder, bei denen die Zähne in unregelmäßiger Weise auf den Umfang verteilt sind und bei welchen ein Zahn oder mehrere Zähne hintereinander ausgelassen sind.

An der Walze selbst ist ein Zahnkranz angebracht. Bei einem solchen Antriebe kann es nun vorkommen, daß z. B. trotz einer Sperrung die Walze infolge des beim Antrieb erhaltenen Drehmomentes dann statt eines Schaltschrittes mehrere Schritte macht, wenn gerade eine solche zahnlose Stelle des Antriebsrades dem Zahnkranz der Walze zugewendet wird.

Die Kontakte zweier benachbarter Walzen ruhen zum Zwecke der sicheren Kontaktgebung mit einem gewissen Drucke aufeinander. Bei Bewegung zweier Walzen kann daher eine zwischen den bewegten Walzen liegende dritte Walze durch Reibung an den Kontaktflächen dann mitgenommen werden, wenn das Antriebsrad dieser dritten Walze sich nicht gerade im Eingriff mit dem betreffenden Zahnkranze befindet, sondern diesem eine zahnlose Stelle zukehrt.

Durch solche ungewollte Verstellungen eines Chiffrierelementes würde die gesamte Dechiffrierung unmöglich werden. Um solche Zwischenfälle zu vermeiden, sieht das Patent eine besondere Blockierung vor. Diese tritt jedesmal selbsttätig dann in Wirksamkeit, wenn das die Verstellung bewirkende Mittel, z. B. das Zahnrad mit stellenweise ausgelassenen Zähnen, kurz „Lückenzahnrad" genannt, sich in unwirksamer Stellung befindet.

7.

Patent Nr. 416.219.

Klasse 42*n*, Gruppe 14, ausgegeben am 8. Juli 1925.

Patentiert im Deutschen Reiche vom 23. Februar 1918 an.

Schon vor der gegenständlichen Erfindung waren elektrische Chiffriermaschinen bekannt, bei denen Zeichensender und Zeichenempfänger in beliebiger Weise durch elektrische Leitungen miteinander verbunden waren. Die Veränderung der Anschlüsse (Änderung des Chiffrierschlüssels) erfolgte entweder durch Auswechseln fester Platten, welche entsprechende Leitungen trugen, oder durch Drehen eines nach dem Grundschlüssel angeschlossenen biegsamen Kabels oder durch Drehen eines Leitungsmagazins. Die mit obigem Patente geschützte Erfindung beabsichtigt die Anschlußveränderung zu vereinfachen.

Zum Zwecke der Vertauschung von Zeichen werden zwischen Zeichensender und Zeichenempfänger ein oder mehrere Zwischenleitungsträger geschaltet. Diese Zwischenleitungsträger sind zwischen festen Endleitungsträgern mit Energieeintritts- und -austrittsstellen (Kontaktstellen) frei beweglich. Die Kontaktstellen dieser Zwischenleitungsträger sind paarweise beliebig miteinander verbunden. Der oder die Zwischenleitungsträger lassen sich an den Reihen der festen Kontaktstellen derartig vorbeibewegen, daß die Bewegung der Kontaktstellen in Richtung der Verbindungslinie dieser Kontaktstellen erfolgt. Die Weiterbewegung der Zwischenleitungsträger kann auch nach Größe, Richtung und zeitlicher Aufeinanderfolge unregelmäßig erfolgen. Die Art der Weiterbewegung der Zwischenleitungsträger kann auch wahlweise eingestellt werden. Es kann auch wahlweise ein Teil der Zwischenleitungsträger bewegt werden oder in Ruhe bleiben. Die Zwischenleitungsträger können auch derartig miteinander gekuppelt sein, daß jeder hintere Zwischenleitungsträger immer dann um eine Kontaktstelle weiterrückt, wenn der vorliegende Zwischenleitungsträger eine volle Umdrehung gemacht hat.

Die Zuleitung zwischen Zeichensendern und Zeichenempfängern einerseits, den beiden Seiten der Leitungszwischenträger andererseits führt — z. B. zum Zwecke der Umstellung von „Chiffrieren“ in „Dechiffrieren“ — über einen Umschalter.

Der Zeichenempfänger muß nicht in einer Schreibvorrichtung, er kann z. B. auch aus Glühlampen bestehen etc., etc.

8.

Patent Nr. 425.147.

Klasse 42*n*, Gruppe 14, ausgegeben am 13. Februar 1926.
Patentiert im Deutschen Reiche vom 26. September 1920 ab.

Durch eine hohe Zahl willkürlicher Einstellmöglichkeiten der Maschine und durch eine Veränderung des Schlüssels während des Schreibens soll verhindert werden, daß ein Kenner der Maschine aus einer Geheimschrift die Klarschrift theoretisch oder praktisch in absehbarer Zeit ermitteln könne.

Dies soll mit möglichst einfachen Mitteln erzielt werden:

1. In den Energieübertragungsweg (zwischen Zeichengeber und Zeichenempfänger und auch zwischen den Führungs- und Anschlußteilen für die Leitungen der Energie) sind ein oder mehrere bewegliche „Zwischenwegeträger" eingeschaltet, deren Energieeintrittsstellen mit den Energieaustrittsstellen in möglichst regelloser Weise verbunden sind.

2. Die Bewegung der Zwischenwegeträger erfolgt automatisch beim Niederdrücken der Buchstabengeber.

3. Die Bewegung eines oder mehrerer Zwischenwegeträger erfolgt sowohl in der zeitlichen Aufeinanderfolge als auch mit Bezug auf die gegenseitige Bewegung der Zwischenwegeträger möglichst unregelmäßig.

4. Die Art der Bewegung der Zwischenwegeträger läßt sich durch Einstellung der Antriebsvorrichtung in möglichst vielseitiger Weise variieren.

5. Der Antrieb der Zwischenwegeträger erfolgt durch eine oder mehrere laufende Wellen und mittels auf diesen Wellen angebrachter „Mitnehmerräder". Letztere sind gegenüber ihren Wellen zweckmäßig verdrehbar.

6. Es läßt sich wahlweise ein Teil der Zwischenwegeträger bewegen und der andere Teil derselben in Ruhe halten.

7. Die Anfangseinstellung der Zwischenwegeträger ist beliebig einstellbar.

8. Die Energiezuleitungswege oder auch die Energieableitungswege zu den Zwischenwegeträgern lassen sich durch einen Umschalter miteinander vertauschen.

9. Die räumliche Umstellung der im Klartexte aufeinanderfolgenden Zeichen lassen sich durch einen besonderen, schrittweise nach jedem Zeichen weiterrückenden Wegeumschalter bewirken.

10. Zum Zwecke der Umwürfelung der Zeichen in bezug auf ihre Aufeinanderfolge läßt sich eine Relativverschiebung zwischen Drucktype und Papier vornehmen. Deren Größe ist bei jedem einzelnen Buchstaben derart verschieden, daß die Buchstaben in ganz anderer Reihenfolge als im Klartext abgedruckt werden.

11. Diese in ihrer Reihenfolge umstellbaren Buchstaben lassen sich gleichzeitig durch andere Buchstaben ersetzen.

12. Es erfolgt eine selbsttätige Umschaltung des „Umwürfelungs-Vielfachwegeschalters" jedesmal nach Niederschrift einer Zeile.

13. Ein Zählwerk vermag die Anzahl der chiffrierten Zeichen und Zeilen zu zählen.

9.

Patent Nr. 425.566.

Klasse 42 *n*, Gruppe 14, ausgegeben am 22. Februar 1926.
Patentiert im Deutschen Reiche vom 28. Februar 1924 ab.
(Chiffrier-Maschinen-A.-G. in Berlin.)

Das internationale Telegraphieralphabet besteht aus 26 Buchstaben. Buchstaben mit Akzenten oder Umlaute (wie ä, ö, ü) sind nicht vorhanden. Ein chiffriertes Telegramm kann also nur Elemente enthalten, die aus diesen 26 Buchstaben entnommen sind. Es ist aber erforderlich, auch die Wortzwischenräume zu chiffrieren und von Buchstaben auf Ziffern oder Interpunktionszeichen umzuschalten. Die Ziffern und Interpunktionszeichen sind, ähnlich wie bei Schreibmaschinen, auf den 26 Buchstabentasten untergebracht. Es sind daher außer den 26 Buchstaben noch zwei weitere Umschalttasten erforderlich, bei deren Druck im Chiffrat aber ebenfalls Buchstaben erscheinen müssen. Es schien daher zweckmäßig, zwei Buchstaben für zwei verschiedene Zwecke zu verwenden, nämlich einerseits als Buchstaben in der eigentlichen Bedeutung und andererseits als Umschaltbuchstaben.

Das Patent versucht dies dadurch zu ermöglichen, daß als Umschaltbuchstaben solche Buchstaben verwendet werden, die

— ohne den Text unleserlich zu machen — durch andere etwa gleichlautende Buchstaben ausgedrückt werden können, wie beispielsweise j und q, welche durch i und k ersetzt werden können.

Bei Chiffrierung eines Klartextes, der j und q enthält, wird daher auf der Tastatur mit 26 Buchstaben für jedes j ein i und für jedes q ein k gedrückt. Wird dagegen j oder q gedrückt, so bedeutet dies die Umschaltung. Dies könnte nun leicht zu Verwechslungen Veranlassung geben, dadurch, daß sich der Schreibende irrt und beim Schreiben von j oder q tatsächlich diese Buchstaben schreibt. Es werden daher in der patentierten Erfindung 28 Tasten vorgesehen. Von diesen tragen 26 die Buchstaben, zwei von ihnen aber sind besondere Umschalttasten und als solche auch kenntlich gemacht. Wesentlich ist ferner ein Schalter, welcher bei Schalten der Maschine auf „Chiffrieren" die beiden Leitungen, welche an j und i angeschlossen sind, und die beiden Leitungen, welche an q und k angeschlossen sind, untereinander verbindet. Es ist daher gleichgültig, ob beim Chiffrieren die Taste i oder die Taste j, bzw. welche der Tasten q und k gedrückt werden. Im Chiffrat erscheint immer der dem i oder der dem k entsprechende Buchstabe. Nach dem Niederdrücken der Umschalttasten aber erscheinen im Chiffrat beim Niederdrücken von j oder q nicht mehr die dem i oder k entsprechenden, sondern die den Buchstaben j oder q entsprechenden Chiffren.

III.

1. Chiffrier- und Dechiffriermaschine System „Kryha“.[27])

Diese Chiffriermaschine liefert keine Niederschrift des chiffrierten Textes. Sowohl bei der Chiffrierung wie bei der Dechiffrierung muß der Text abgelesen und mit der Hand übertragen werden.

Der Mechanismus dieses Apparates ist in einen durch einen Deckel verschlossenen Kasten eingebaut.

Beim Modell „Commerce“, Tafel K, Fig. I, ist in den Deckel des Kastens ein 26teiliger Halbkreis fest und unbeweglich eingelagert. Auf diesem Halbkreise sind die 26 Buchstaben des Alphabetes angebracht. Innerhalb dieses Halbkreises befindet sich eine — nicht in den Kastendeckel eingelagerte — um eine Achse drehbare 52teilige Scheibe. Diese (Fig. II, b) besteht aus zwei gleichen Hälften. Auf jeder dieser Hälften sind je 26 Buchstaben des Alphabetes und die Zahlen 3 bis 28 lesbar angebracht. Der äußere feste Halbkreis dient als Klaralphabet, die innere drehbare Scheibe als Chiffrierbehelf.

Der Antrieb der Maschine erfolgt durch ein in das Gehäuse eingebautes, mit der Hand aufzuziehendes Uhrwerk.

Im Inneren des Apparates (Tafel K, Fig. II) befindet sich ein mit verschiedenen Zahngruppen versehenes, also unregelmäßig gezahntes Chiffrierrad. Dieses Chiffrierrad (a) ist gegen anders gezahnte Räder auswechselbar. Die Auswechselbarkeit des Chiffrierrades ermöglicht neue Kombinationen (Schlüssel). Das Uhrwerk setzt das Chiffrierrad in Bewegung, das Chiffrierrad wiederum bringt die drehbare Scheibe (Chiffrierscheibe) zur Rotation.

27) Vgl. den Auszug aus der Patentschrift auf Seite 51 ff. und Professor Dr. Georg Hamel, „Die Chiffriermaschine System ‚Kryha‘“, ein mathematisches Gutachten, Berlin 1927, bei Reinhold Kühn.

Das von außen unsichtbare Chiffrierrad (nicht zu verwechseln mit der von außen sichtbaren Chiffrierscheibe) hat bei jeder Zahngruppe ein Loch; je nach der Type im ganzen 10 bis 25 numerierte Löcher. Diese Löcher dienen als Haltepunkte (s. d. Abb. Tafel K, Fig. IIa). Beim Chiffrieren kann — je nach der Verabredung — von jedem dieser Haltepunkte aus begonnen werden. Die Möglichkeit, beim Chiffrieren bei Anwendung eines und desselben Chiffrierrades von verschiedenen Haltepunkten zu beginnen, gestattet mehrere weitere Kombinationen.

Die verschiedenen auswechselbaren Chiffrierräder sind nicht nur mit anderen Zahngruppen versehen, sondern auch anders gelocht. Diese auswechselbaren Chiffrierräder sind zur Vermeidung von Irrtümern durch „Phantasienamen" unterschiedlich kenntlich gemacht. Die Differenzierung der Haltepunkte innerhalb eines Rades erfolgt durch „Nummern".

Jedem Buchstaben oder jeder Zahl des sichtbaren Klartextringes entspricht ein Buchstabe oder eine Zahl auf der anliegenden — durch das Chiffrierrad in Rotation versetzbaren — sichtbaren Chiffrierscheibe. Ebenso wie bei der Zirkularscheibe, Tafel F, Fig. I, muß der Dechiffreur außer dem Namen des Chiffrierrades und der Nummer des Haltepunktes, mit welchem begonnen wurde, auch die Scheibenanfangsstellung, d. h. die Einstellung des Klartextringes zur Chiffrenscheibe kennen. Eine Änderung dieser Einstellung ermöglicht neue Kombinationen (Schlüssel). Entspricht z. B. bei der ersten Einstellung dem „E" des Klartextringes ein „X" auf der Chiffriertextscheibe, so kann bei einer geänderten Einstellung diesem „E" ein „K", ein „Z", ein „B" od. dgl. auf der Chiffrierscheibe entsprechen.

So wie bei der Zirkularscheibe mit auswechselbaren Buchstaben, Tafel F, Fig. II, ist auch bei dieser Maschine eine Austauschung der auf der Chiffrierscheibe angebrachten Buchstaben vorgesehen. Die Buchstaben lassen sich untereinander willkürlich vertauschen. Die Buchstaben befinden sich daher auf kleinen Plättchen, die aus der Scheibe herausgezogen und an einer anderen Stelle in die Scheibe hineingeschoben werden können. Nach Angabe des Erfinders lassen sich bei 26 Buchstaben nach der Formel:

$26! = 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16.17.18.19.$
$.20.21.22.23.24.25.26,$

im ganzen

403,202.552,074.329,047.040,000.000

voneinander abweichende Chiffrierscheiben aufbauen. Auch diese Auswechselbarkeit der Buchstaben ermöglicht daher eine Reihe neuer Kombinationen (Schlüssel).

Wenn man bei dieser Maschine vom „Schlüssel" im allgemeinen spricht, so meint man darunter sowohl die Grundstellung (Anfangsstellung) der Chiffrierscheibe zum Klartextring, den Namen des Chiffrierrades, die Nummer des Haltepunktes, mit welchem zu chiffrieren angefangen wurde, endlich die Reihenfolge der einzelnen auswechselbaren Buchstaben auf dem Klartextringe und auf der Chiffrierscheibe. Über alle diese Schlüsselelemente hat sich Chiffreur und Dechiffreur zu einigen. Die beiden Korrespondenten müssen aber auch verabreden, wie lange der vereinbarte Schlüssel zur Gänze oder teilweise unverändert bleiben soll, bzw. welche Schlüsselelemente und wann dieselben zu ändern sind.

Hat der Dechiffreur z. B. mit dem Chiffreur vereinbart „ChR. Fortuna HP 12 — ACGMUYKVBEHNPDIWFORXLSZQTJACG etc. — H = K", so bedeutet dies, daß der Chiffreur das unsichtbare, unregelmäßig gezahnte und gelochte Chiffrierrad „Fortuna" in die Maschine einsetzt, den Haltepunkt Nummer 12 einstellt, die auswechselbaren Buchstabenplättchen der Chiffrierscheibe in der Reihenfolge der obigen Buchstaben einschiebt und endlich die beiden Scheiben zueinander so einstellt, daß dem Buchstaben „H" des „Klartextringes" der Buchstabe „K" der „Chiffrierscheibe" entspricht. Nunmehr wäre der Schlüssel vereinbarungsgemäß eingestellt.

Nun chiffriert der Chiffreur den ersten Buchstaben seines Klartextes in der Weise, daß er auf der Chiffrierscheibe den Buchstaben abliest, welcher mit dem zu chiffrierenden „Buchstaben des Klartextes im Klartextring" in einer Radiallinie liegt. Der zweite Buchstabe des Klartextes wird jedoch nicht mehr in dieser Einstellung des Ringes zur Scheibe chiffriert. Nach der Chiffrierung jedes Buchstaben des Klartextes drückt der Chiffreur nämlich auf einen Knopf. Dieser löst die Rast aus und setzt das Uhrwerk in Bewegung. Die Chiffrierscheibe (in-

nere Scheibe) beginnt zu rotieren und macht so viele Schritte, als die nächste Zahngruppe des Chiffrierrades Zähne enthält. Bei jedem der Zahngruppe nachfolgenden Loche (Haltepunkt) bleibt die Chiffrierscheibe wieder stehen. In diesem Momente der Arretierung entspricht selbstverständlich einem Buchstaben des Klartextringes ein anderer Chiffrebuchstabe als vor der Rotation der Chiffrierscheibe. In dieser neuen Stellung der Chiffrierscheibe wird nunmehr der zweite Buchstabe chiffriert, der Knopf des Uhrwerkes wieder gedrückt usf.

Die Periode, bis bei gleichem Modelle und gleichem Schlüssel ein Klarbuchstabe wieder durch den gleichen Chiffrebuchstaben ersetzt wird, ist von der Beschaffenheit des Chiffrierrades abhängig und schwankt bei den 10- bis 20löchrigen Chiffrierrädern angeblich zwischen 260 und 520.

Der beschriebene Chiffrierapparat wird aber auch in einem anderen Modelle ausgeführt. Dieses führt den Namen „Doppelchiffriermaschine Type ‚Diplomat'". Bei dieser Type ist nicht bloß eine Rotation der Chiffrierscheibe, sondern auch eine Rotation des Klartextringes vorgesehen. Selbstverständlicherweise ist bei dieser Type der Klartextring kein Halbkreis, sondern ein geschlossener Kreis. Klartextring und Chiffrierscheibe sind bei dieser Type 52teilig und tragen je zwei Alphabete. Die Buchstabenplättchen sind wiederum gegeneinander austauschbar. Während bei der Type „Commerce" aber nur die Buchstaben der Chiffrierscheibe herausgezogen und versetzt werden konnten, können bei dieser Type auch die Buchstaben des Klartextringes gegeneinander vertauscht werden. Ließen sich bei der Type „Commerce" daher durch Vertauschen der Buchstabenplättchen

$$26! = 403{,}202.552{,}074.329{,}047.040{,}000.000$$

Chiffrierscheiben aufbauen, so gestattet die Type „Diplomat" bei 26 Buchstaben des Alphabetes, zweimal so viele, also:

$$806{,}404.104{,}148.658{,}094.080{,}000.000$$

abweichende Scheiben- und Ringkombinationen aufzubauen.

Die Rotation des Klartextringes muß von der der Chiffrierscheibe unabhängig sein. Die Type „Diplomat" enthält daher ein Uhrwerk und ein Chiffrierrad, welches mit der Chiffrierscheibe in Verbindung steht, weiters ein zweites Uhrwerk und

ein zweites Chiffrierrad, durch welche der Klartextring in Bewegung gesetzt wird.

Der Erfinder berechnet die Zahl der Schlüssel aus der Formel $(26!)^2\,(20!)$, u. zw.:

$$(26!)^2 = 162.572,297.999,252.026,914.036,899.393,874.532,761\text{-}600,000.000,000.000;$$

$$(20!) = 87.159,072.000;$$

$$(26!)\,(20!) = 14.169,650.626,522.262,359.946,479.924,927.466,759\text{-}934,653.235,200.000,000.000,000.000.$$

Bei Konstruktion dieser Chiffriermaschine mußte jedoch an die Möglichkeit gedacht werden, daß die wichtigsten Schlüsselelemente (Name des Chiffrierrades, Anfangshaltepunkt, Buchstabeneinstellung auf Ring und Scheibe und Stellung Ring zur Scheibe) verraten werden und der Enträtseler dann nach einer gewissen Anzahl von Versuchen experimentell feststellen könnte, wann und wie oft auf den Knopf des Uhrwerkes zu drücken sei. Dies soll auf folgende Weise verhindert werden: Wennschon die Chiffrierscheibe „regelmäßig nach jedem Buchstaben" in Rotation versetzt wird, soll der Eintritt der Rotation der Klartextscheibe vom Zufall oder richtiger von der Beschaffenheit des zu chiffrierenden Textes abhängig gemacht werden. Bei der Type „Diplomat" sehen wir daher eine kleine Platte aus durchsichtigem, roten Glase in der Breite eines oder mehrerer Buchstaben. Das Uhrwerk der Klartextscheibe wird zwecks Rotation derselben nur dann in Bewegung gesetzt, wenn ein chiffrierter Buchstabe, also ein abzulesender Chiffrebuchstabe, bei Stillstand der Chiffrierscheibe gerade unter diese durchsichtige Glasplatte zu liegen kommt. Ein solcher Chiffrebuchstabe, welcher unter die bunte Platte zu liegen kommt, wird vom Erfinder „Influenzbuchstabe" genannt.

Durch diese Einrichtung (carré influent) glaubt der Erfinder die Möglichkeit zu schaffen, die Perioden der Maschine ohne Änderung des Systems auszudehnen.

Von der Chiffriermaschine System Kryha existiert endlich noch eine dritte Type (elektrische Type).

Die sogenannte elektrische Type dieser Chiffriermaschine (Tafel L) ist nach gleichem Prinzipe konstruiert wie die Type „Diplomat". Diese dritte Type gestattet aber die Anwendung

des elektrischen Stromes. Vor und hinter der Chiffriermaschine, welche die Chiffrierung ausführt, ist bei dieser Type je eine Schreibmaschine beliebigen Modells angeschaltet. Der Chiffreur schreibt auf der einen Maschine („Sender") den Klartext, die Chiffriermaschine chiffriert und übermittelt das Chiffrat der zweiten Schreibmaschine. Der Chiffreur erhält sohin auf der zweiten Maschine („Empfänger") den bereits chiffrierten Text niedergeschrieben.[28]) Beim Dechiffrieren schreibt der Dechiffreur auf dem „Empfänger" den chiffrierten Text und erhält am „Sender" den Klartext.

Der Chiffreur und Dechiffreur kann die Chiffrierarbeit seines Chiffrierapparates daher in diesen Niederschriften selbst kontrollieren. Will der Empfänger einer chiffrierten Mitteilung dieselbe mit seiner elektrischen Type sofort in eine Klartextniederschrift übertragen, so muß er sich allerdings desselben Modells des Chiffrierapparates und desselben Schlüssels bedienen wie sein Korrespondent.

Da das Chiffriersystem dieser elektrischen Type des Chiffrierapparates das gleiche ist wie bei den mechanischen Typen, so können in der Praxis elektrische und — nach dem gleichen System konstruierte — mechanische Typen korrespondierend verwendet werden.

2. Die „Enigma"-Maschine.[29])

Die „Enigma"-Maschine hat die äußere Form einer Schreibmaschine. Sie gestattet einerseits Klartext zu chiffrieren und Chiffrentext zu dechiffrieren; einige Modelle können auch als gewöhnliche Schreibmaschinen zur Niederschrift irgendeiner Mitteilung in Klarschrift verwendet werden. Sie gestatten weiters, Klar- und Chiffrentext jederzeit abwechseln zu lassen. Von einem Briefe, dessen Inhalt nicht unbedingt zur Gänze geheimgehalten werden muß, schreibt man daher mit der „Enigma" den Text als gewöhnliche, allgemein lesbare Maschinschrift nieder und beschränkt sich darauf, nur wichtige Wörter, z. B. die „Preise" od. dgl. zu chiffrieren.

[28]) Jede Maschine kann durch Umschaltung sowohl als Sender wie als Empfänger benützt werden.

[29]) Vgl. die Auszüge aus den Patentschriften auf Seite 53 bis Seite 65.

Allen drei Modellen der „Enigma" ist gemeinsam, daß vor dem „Chiffrieren" sogenannte „Schlüsselbuchstaben" eingestellt werden müssen. Diese vom Chiffreur gewählten Schlüsselbuchstaben (auch der „Schlüssel" genannt) müssen selbstverständlicherweise auch dem Dechiffreur bekannt sein, da Chiffreur und Dechiffreur sich sonst miteinander nicht verständigen könnten. Solch ein Schlüssel ist außerordentlich variationsfähig. Nehmen wir an, der Schlüssel sei stets nur den Mitgliedern einer bestimmten Personengruppe bekannt. Wenn hunderte von Personengruppen das gleiche Maschinenmodell der „Enigma" benützen würden, könnten wohl die Mitglieder jeder einzelnen Personengruppe untereinander verständlich ihre Mitteilungen austauschen, die Mitglieder anderer Personengruppen würden diese Mitteilung jedoch nicht lesen können. Verschiedene Personengruppen korrespondieren also mit dem gleichen Maschinenmodell, die eine der andern gegenüber, geheim.

Modell A.

Ein Walzensystem und entsprechende elektrische Kuppelungen ermöglichen es, die sogenannten „Tauschalphabete" zu bilden und diese wiederum zu vertauschen. Dieses Walzensystem steht einerseits mit der Tastatur, andererseits mit der Schreibvorrichtung der Maschine in Verbindung.

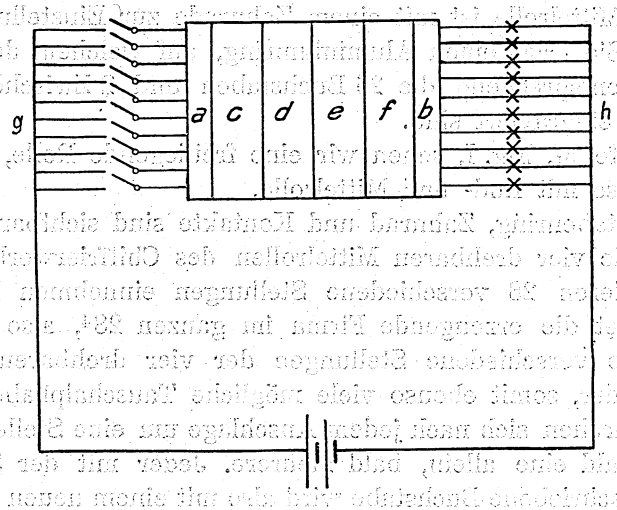
Beim Anschlagen der Taste wird der elektrische Kontakt geschlossen. Auf der Maschine wird ungefähr so geschrieben wie auf einer gewöhnlichen Schreibmaschine.

Die Schreibvorrichtung dieses Modells schreibt nach Art der älteren Schreibmaschinen mit Hilfe eines rotierenden Typenrades.

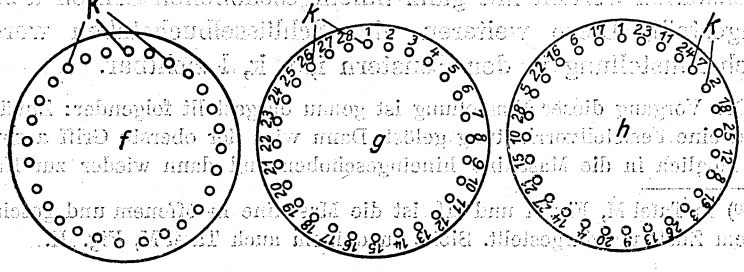
Vom gewöhnlichen Maschinschreiben abweichend ist es, daß (im Gegensatze zur Schreibmaschine) die Umschalttasten loszulassen sind, bevor die umzuschaltende Taste angeschlagen wird.

Welcher Chiffrebuchstabe dem auf der Tastatur angeschlagenen Buchstaben entspricht, hängt von der jeweiligen Stellung des Walzensystems ab, welches aus sechs Rollen besteht. Dieses Rollensystem, der eigentliche Chiffriermechanismus, ermöglicht als „Vielfachumschalter" zwischen Tasten und Schreibvorrich-

tung die „Vertauschungen". Eine solche Schaltung kann folgendermaßen skizziert werden:



Das Rollensystem ist mit den Buchstaben a bis d bezeichnet. Mit a ist die linke, mit b die rechte Endrolle, mit c, d, e, f sind die Mittelrollen kenntlich gemacht. Die Tasten, welche beim Niederdrücken den Kontakt auslösen, sind bei g, die Schreibvorrichtung bei h angedeutet. Es stehen also mit der linken Endrolle die Schreibtasten in Verbindung, an die rechte Endrolle dagegen sind die Typen der Schreibvorrichtung angeschlossen. Die Kontakte selbst sind an den Kreisflächen der Rollen angebracht, u. zw. befinden sich an jeder Fläche „nächst den Rändern im Kreisrund" 28 in der Richtung der Rollenachse federnde Kontakte. Eine Skizze dieser Kreisflächen der Rollen würde folgendes Bild geben:



Die Endrolle ist in f, die linke und rechte Grundfläche einer Mittelrolle in g und h skizziert. Die Kontakte sind mit k bezeichnet.

Jede Mittelrolle ist mit einem Zahnrade zur Einstellung versehen. Sie trägt einen Aluminiumring, auf welchem den Kontakten entsprechend die 26 Buchstaben und 2 Zwischenraumzeichen eingraviert sind.

In Tafel M, Fig. I, sehen wir eine freiliegende Rolle, weiters die Achse mit End- und Mittelrolle.

Buchstabenring, Zahnrad und Kontakte sind sichtbar.

Da die vier drehbaren Mittelrollen des Chiffrierwerkes jede zur anderen 28 verschiedene Stellungen einnehmen können, berechnet die erzeugende Firma im ganzen 28^4, also 614.656 mögliche verschiedene Stellungen der vier drehbaren Rollen zueinander, somit ebenso viele mögliche Tauschalphabete. Die Rollen drehen sich nach jedem Anschlage um eine Stelle weiter, u. zw. bald eine allein, bald mehrere. Jeder mit der Schreibtaste geschriebene Buchstabe wird also mit einem neuen Tauschalphabete geschlüsselt. „Alle Tritheim-Möglichkeiten oder Alphabete Krohn's wechseln in einer Maschine automatisch ab." (Figl.)

Die Anfangsstellung des Walzensystems nennt man den „äußeren Schlüssel der betreffenden Geheimschrift" oder die „Schlüsselstellung" oder kurz den „Schlüssel". Der Schlüssel besteht aus acht Buchstaben. Er wird den zwischen dem Chiffreur und Dechiffreur getroffenen Vereinbarungen entsprechend mit Hilfe der an der rechten Seite der Maschine angebrachten vier Griffe[30]) a, b, c, d nach Lösen einer Feststellvorrichtung eingestellt. Zuerst werden die ersten vier Schlüsselbuchstaben mit halb hineingeschobenen Griffen a bis d eingestellt. Die ersten vier Schlüsselbuchstaben werden nach Einstellung in den Fenstern e, f, g, h sichtbar. Die folgenden vier Schlüsselbuchstaben werden mit ganz hineingeschobenen Griffen a bis d eingestellt. Diese weiteren vier Schlüsselbuchstaben werden nach Einstellung in den Fenstern i, j, k, l sichtbar.

Der Vorgang dieser Einstellung ist genau dargestellt folgender: Zunächst wird eine Feststellvorrichtung gelöst. Dann wird der oberste Griff a soweit als möglich in die Maschine hineingeschoben und dann wieder zur Hälfte

[30]) In Tafel M, Fig. II und III, ist die Maschine in offenem und geschlossenem Zustande dargestellt. Siehe zu obigem auch Tafel M, Fig. III.

herausgezogen. In dieser Lage kann der Griff gedreht werden. Durch dieses Drehen des Griffes wird die erste Walze solange verstellt, bis der gewünschte erste Schlüsselbuchstabe in dem Fenster e erscheint. Ebenso wird der zweite, dritte und vierte Schlüsselbuchstabe eingestellt. Hierauf wird der, wie oben bemerkt, zur Hälfte herausgezogene Griff a wieder ganz hineingeschoben. In dieser hineingeschobenen Lage wird er so lange gedreht, bis in dem Fenster i der fünfte Schlüsselbuchstabe sichtbar wird. Dann wird der Griff a wieder ganz herausgezogen. In gleicher Weise werden mit den anderen Griffen b, c und d der sechste, siebente und achte Schlüsselbuchstabe eingestellt. Hiemit ist die Schlüsseleinstellung beendet. Nach beendeter Einstellung aller Schlüsselbuchstaben werden die vier Griffe a bis d wieder soweit wie möglich herausgezogen.

Ist der Hebel o auf „Klarschrift" gestellt, so schreibt die Maschine nur Klartext.

Wird der an der Maschine angebrachte Hebel o auf „Chiffrieren" gestellt, so muß der Wagen mit der Schreibwalze soweit wie möglich nach rechts geschoben, der Motor eingeschaltet und mit dem Schreiben begonnen werden. Nun chiffriert die Maschine. Auch während des Schreibens in Chiffren kann an jeder beliebigen Stelle des Chiffrats wieder Klartext eingeschaltet werden.

Die Maschine gruppiert den Chiffrentext automatisch in Gruppen von je fünf Buchstaben und schreibt je zehn Gruppen in einer Zeile, so daß in jeder Zeile genau 50 Chiffrebuchstaben stehen.[31])

In die Maschine ist ein Zählwerk eingebaut, welches jeden chiffrierten Buchstaben selbsttätig zählt. Das Zählwerk besteht aus kleinen Rollen. Sie sind ähnlich konstruiert wie die großen Mittelrollen. Am Mantel tragen sie die Ziffern. Diese kleinen Zählrollen drehen sich mit den Mittelrollen. Das unter dem Fenster n sichtbare Zählwerk wird zu Anfang der Chiffrierperiode auf Null eingestellt. Zu diesem Zwecke 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.

Im Fenster n kann in jedem Augenblicke die Anzahl der seit Beginn der Arbeit chiffrierten Buchstaben abgelesen wer-

[31]) Das Chiffrat besteht dabei nur aus den 26 Buchstaben des internationalen Telegraphenalphabetes, während das Dechiffrat wieder alle Buchstaben, Ziffern, Zeichen und Zwischenräume des Klartextes enthält wie ein gewöhnlicher Schreibmaschinentext.

den. Solange Klartext geschrieben wird, bleibt das Zählwerk ebenso wie der Chiffriermechanismus stehen.[32])

Das Entziffern wird in der Weise vorgenommen, daß der Hebel o auf „Dechiffrieren" umgestellt wird und das Chiffrat sohin, ohne auf die Gruppenabstände des Chiffrentextes Rücksicht zu nehmen, auf der Maschine abgeschrieben wird. Es erscheint dann der ursprüngliche Klartext mit allen Wortabständen.

Zeitweise ist darauf zu achten, ob das Zählwerk mit der Anzahl der geschriebenen Buchstaben übereinstimmt.

Beim Dechiffrieren kann in jedem Augenblick festgestellt werden, ob die dechiffrierende Maschine genau an der gleichen Stelle des Elaborates arbeitet, an welcher die chiffrierende Maschine gearbeitet hat. Es muß also z. B. jederzeit feststellbar sein, ob z. B. der 1435ste chiffrierte Buchstabe auch als der 1435ste dechiffriert wird.

Nach Angabe der Fabrik tritt bei unverändert bleibendem Anfangsschlüssel erst nach etwa 1,000.000 mit dem gleichen Schlüssel geschriebenen Buchstaben wieder die gleiche Tauschalphabetfolge auf.

Nun muß aber keineswegs bei verschiedenen Mitteilungen, ja nicht einmal innerhalb einer und derselben Mitteilung, der gleiche Schlüssel verwendet werden, es können vielmehr die verschiedenartigsten äußeren Schlüssel benützt werden. Korrespondiert eine behördliche Stelle mit mehreren Korrespondenten, so kann jeder dieser Korrespondenten mit einer Anzahl verschiedener Schlüssel „beteilt" werden.

Ein Kryptogramm mit Hilfe der Maschine zu entziffern ist nur demjenigen möglich, welcher in den Besitz des Schlüssels gekommen ist. „Der Schlüssel stellt also das kryptographische Geheimnis dar." „Die Maschine kann gestohlen werden; soferne der Schlüssel abgestellt ist, wird eben nur eine Schreibmaschine

---

[32]) Das Zählwerk der Maschine einerseits, die automatische Gruppeneinteilung andererseits ermöglichen es, etwa unterlaufene Fehler sofort wieder zu verbessern. Ein beim Niederschreiben, beim Entziffern oder bei der Übertragung (z. B. bei telegraphischer Übermittlung) etwa entstandener Fehler bleibt isoliert. Es wird lediglich der fehlerhafte Buchstabe falsch entziffert, während die Entzifferungsmöglichkeit des ganzen übrigen Textes in keiner Weise leidet.

gestohlen." „Der Fachkryptograph hat nicht nur mit der Arbeit der Enträtseler zu rechnen, sondern auch mit Diebstahl, Verkauf, Verrat. In den letzteren Fällen war es bisher — wenn es sich um weitverbreitete Befehle handelte — meist unmöglich, den Ort des Verbrechens und damit den Verbrecher zu ermitteln, weil moderner Diebstahl, Verkauf oder Verrat nie durch Enttragen des Originales selbst, sondern nur durch Photographie oder Abschrift erfolgt." (Figl.)

„Anders bei der ‚Enigma': Wird man gewahr, daß Unberufene Kenntnis vom Inhalte einer Geheimschrift haben, so kann nur ein Verrat usw. vorliegen. Nachschau, mit welchem Schlüssel die Schrift geschlüsselt war, lokalisiert den Verdacht auf die Besitzer dieses Schlüssels, einen Absender, einen Empfänger, also auf zwei Personen. Die Art des verratenen Geheimnisses, Zeitpunkt, Ort u. ä. werden es dem Kriminalisten nicht schwer machen, unter den zwei Beschuldigten den Schuldigen zu ermitteln." (Figl.)

Das Modell A der „Enigma"-Maschine wurde 1923 in Bern (Schweiz) und 1924 in Stockholm beim Weltpostkongreß vorgeführt.

Die deutsche Reichspost übermittelte im Welspostkongresse eine Depesche folgenden Inhaltes:

Kenntnis erhaltend von den wichtigen Versuchen zur telegraphischen Übermittlung verschlüsselter Nachrichten, die z:zt von der Chiffriermaschinen A.-G. Berlin zwischen Stockholm und Berlin mit der Chiffriermaschine „Enigma" ausgeführt werden, nehme ich gern Gelegenheit, diesen Weg zu benutzen, um die besten Wünsche der deutschen Reichspost für ein erfolgreiches Arbeiten des Weltpostkongresses auszusprechen.

Diese Depeschenklarschrift lautete chiffriert:

praesident schenk erudw ffpbf
knjkk btbye fifac tgzjz esqmv
vizpp odsed oeszj kanhs vivsm
kvgyu cmdov oezap bntgu fjzbp

zvluk ltnfk ygbju duoqj opovu
esslp mvipp qhuii kgdix plesi
yijqm yhnxy nrhdw orcyd ecnwb
glebh pmpit dgweg sxqki zkfhx
wbldx sralh sbhoc fhvmu ovgdu
owwof vahzy ybenc hcses zcyut
zocov ofcke sfndr hybqr xsvdr
vwtrg ubksj krmyl wavri ixdmk
lwili rcfsq ozouq yiuui mmsmu
jhobm jlnkn lazxq hhied vgyio
tonsd qdngs skhfd aijux kemfq
selkp bifxc dhbkf dcepb zcuzn
lqqmj ctimt szild cknwd xrchc
xnfgp x 416 reichspostminister

Der achte Weltpostkongreß in Stockholm dankt am 7. August 1924 auf diese Depesche wie folgt:

Reichspostminister Dr. Höfle, Berlin. Die Delegierten auf dem Weltpostkongress in Stockholm, die der interessanten Vorführung der Chiffriermaschine „Enigma" beigewohnt haben, beauftragen mich, Ihnen, Herr Minister, für die guten Wünsche zu danken, die Sie dem Kongress für den Erfolg seiner Arbeiten freundlichst übermittelt haben.

Schenk.

Chiffriert lautete dieser Klartext:

ztkuo abekc yzima xnuhr nuvoq rdpbl
hxtgo hnzsz rdevx ubaon ztkuo aoxgi
wvinr bwrey kaezq sdxey ftued vdxdw
hrsto uayzp hnjxi mrhhb saefc hmwaw
uiada lxlie eapgl ubnpl dbzmk rdccg
wgwqo odaiy igemf ggbkc srnne zvksf
jjeue othda wtknl jhqfd dtkos egxyq
thoij mvxbw ljefl wtnzg pofit bfofk
ofnax rrofs okzqi scojv flvqg rdpwx
garrx wuqff mlbyl ghqzr hynxc psdif
gnrkf lbwmh doxbk 315

Modell B.[33])

Modell B ist dargestellt auf Tafel N.[34])

Die Stromzuführung erfolgt durch das Zuleitungskabel 3 (I), welches in einen Steckkontakt endigt. Dieser Stecker 9 (II) ist in die Steckdose der Schalttafel zu stecken. Diese Schalttafel kann an ein Gleichstromnetz von 110 bis 220 Volt Klemmenspannung angeschlossen werden. Steht nur Wechselstrom zur Verfügung, so wird mittels eines Gleichrichters von vier Ampere Stromstärke der Wechselstrom von 220, bzw. 110 Volt Spannung auf 110 Volt Gleichstrom umgewandelt.

Wagen und Farbband unterscheiden sich nicht von den gleichen Bestandteilen einer gewöhnlichen Schreibmaschine. Das Farbband stellt sich aber nicht automatisch um.

Wenn die Glocke ertönt, können noch fünf Buchstaben geschrieben werden. Die Randeinstellung ist für „Klarschrift" und „Chiffrieren" verschieden. Während bei „Klarschrift" die ganze Zeile freigegeben ist, wird für „Chiffrieren" und „Dechiffrieren" die Zeile durch eine kleine Manipulation mit dem Arretierknopf und Fächeranschlag 8 (II) auf 50 Buchstaben begrenzt.

Das Tastenfeld 16 (II) hat 57 Schreibtasten (für 83 Schriftzeichen), zwei runde Umschalttasten US, eine runde Verriegelungstaste SS, eine längliche Umschalttaste rechts (für Buchstaben und Zwischenraum), eine längliche Umschalttaste links (für Zahlen und Zwischenraum) und (vor der ersten unteren Reihe in der Mitte) eine Weiterschalttaste. Die Tasten US dienen zum Heben des Typenkorbes, um große Buchstaben zu schreiben. Die Taste SS dient zum Heben und Feststellen

---

33) Dieses Modell der „Enigma" unterscheidet sich von der früheren Type durch Einfügung der großen Buchstaben. Hiedurch soll es ermöglicht werden, die Maschine für Klartextniederschriften wie eine normale Schreibmaschine zu benützen. Dieses Modell besitzt statt eines durch Motor bewegten Typenrades „Typenhebel". Die Fabrik hat nach ihrer Angabe das Typenradmodell deshalb verlassen, weil die Geschwindigkeit der früheren Type nicht ausreichte. Aus diesem Grunde hatte auch die Schreibmaschinenindustrie das System „Typenrad" aufgegeben. Der Chiffriermechanismus ist bei Typenradmodell und Typenhebelmodell im übrigen der gleiche.

34) In diesem Abschnitte sind mit den eingeklammerten römischen Zahlen die Figuren auf der zitierten Tafel gemeint.

des Typenkorbes. Vor dem Tastenfeld liegt die Weiterschalttaste 17 (II).

Die US-, SS- und Weiterschalttaste dürfen nur für Klarschrift verwendet werden. Beim Chiffrieren werden sie nicht benützt.

Beim Chiffrieren dürfen die sieben in der obersten Reihe befindlichen Tasten mit rot eingelegten Typenplättchen nicht geschrieben werden.[35])

Will man die Maschine als gewöhnliche Schreibmaschine benützen, so muß die Maschine auf Klartext gestellt werden. Es wird zu diesem Zwecke

1. der Umschalthebel 18 (I) auf Klarschrift gestellt,
2. der Wagen in die Mitte geschoben, der Fächeranschlag um 90° nach oben geschwenkt, bis der Arretierknopf 8 (II) in das Loch des Sektors einschnappt.
3. Die Randsteller 7 (II) werden, wie bei jeder Schreibmaschine, auf den gewünschten Zeilenanfang und das Zeilenende eingestellt.

Nun wird der Strom eingeschaltet.

Will man aber mit der Maschine chiffrieren, so wird:

a) der Strom eingeschaltet,

b) die Taste „Umschaltung für Buchstaben und Zwischenraum" gedrückt.

c) Es werden die beiden verstellbaren Anschläge (Randsteller 7 [II]) nach rechts und links in die Endstellung geschoben.

d) Weiters wird der Wagen in die Mitte gestellt,

e) der Fächeranschlag eingestellt,

f) das Zählwerk auf Null gestellt, eventuell durch Drehen mit der Kurbel die gewünschte Anfangszahl eingestellt.

g) Die verabredeten acht Schlüsseln werden eingestellt,

h) der Umschalthebel wird auf Chiffrieren gestellt,

---

35) Diese roten Tasten sind nur bei der Type B vorhanden. Sie tragen die im allgemeinen Sprachgebrauche seltener vorkommenden Zeichen. Diese roten Tasten sind mit der Chiffriereinrichtung nicht verbunden, weil sonst mehrere Relais vorgesehen werden müßten und die Apparatur hiedurch komplizierter würde. Diese Tasten hätten daher auch wegbleiben können. Sie wurden an der Maschine dennoch angebracht, weil diese Zeichen auch in der normalen „Smith-Premier-Tastatur" vorkommen.

i) der Wagen bis zum Anschlag nach rechts geschoben,
k) die Taste „Umschaltung für Buchstaben und Zwischenraum" niedergedrückt.

Hiezu sei im einzelnen noch bemerkt: Der Wagen mit dem eingespannten Papier wird ungefähr in die Mitte gestellt. Die beiden Randsteller für Zeilenanfang und Zeilenende werden nach rechts und links bis zum Anschlag herausgeschoben. Der Fächeranschlag 8 (II) wird durch Herausziehen des Arretierknopfes 8 (II) um 90° nach rückwärts gedreht. Hiedurch werden die Zeilen für „Chiffrieren" und „Dechiffrieren" auf 50 Buchstaben begrenzt. Das Zählwerk 22 (II) ist auf Null gestellt, wenn in den Fenstern 25 (III) lauter Nullen erscheinen. Soll das Chiffrat z. B. mit 00189 beginnen, so steckt man jetzt die Kurbel 26 (I, II, III) in das Kurbelloch 27 (III) rechts unterhalb des Zählwerkes. Man dreht die Kurbel dann im Sinne des Uhrzeigers so lange, bis in den Fenstern die gewünschte Zahl erscheint.

Der Schlüssel besteht stets aus acht Buchstaben. Die vier ersten Schlüsselbuchstaben können aus sämtlichen Buchstaben des Alphabetes gewählt werden. Für den fünften Schlüsselbuchstaben stehen jedoch nur die Buchstaben A bis K, für den sechsten nur die Buchstaben A bis O, für den siebenten nur die Buchstaben A bis Q und für den achten Schlüsselbuchstaben nur die Buchstaben A bis S zur Verfügung.

Lauten die Schlüsselbuchstaben z. B. ZSPRJNFR, so stellt man den ersten Buchstaben ein, indem man den vordersten Knopf 28 (III), der mit I bezeichnet ist, bis zum Anschlag in den Chiffrierkasten hineinschiebt. In dieser Stellung dreht man ihn so lange, bis im linken Buchstabenfenster 32 (III) der Buchstabe „Z" erschienen ist. Dann zieht man den Einstellknopf wieder ganz nach rechts heraus. Ebenso stellt man die folgenden drei Buchstaben mit den Einstellknöpfen II (29, Fig. III), III (30, Fig. III) und IV (31, Fig. III) ein. Um den fünften Buchstaben „L" einzustellen, schiebt man den kordierten Knopf I bis zur Hälfte (markierte Linie, vgl. z. B. bei 33, III) ein. Nun dreht man ihn, bis der Buchstabe „J" mit seinem Skalastriche (an der Abschrägung) genau mit dem feststehenden Markenstrich 34 (III) (am Zylinder) übereinstimmt. Dann wird der Knopf wieder ganz herausgezogen. In gleicher Weise wird der

sechste, siebente und achte Schlüsselbuchstabe mit den Walzen II, III und IV eingestellt.

Beim Chiffrieren werden sämtliche Zeichen benützt, mit Ausnahme der „rot" bezeichneten Tasten und der großen Tasten „US" und „SS". Man kann also beim Chiffrieren keine großen Buchstaben schreiben.

Das Chiffrat wird auch bei dieser Type automatisch in Gruppen zu je fünf Buchstaben eingeteilt. Nach zehn Gruppen ist die Maschine gesperrt. Man muß dann — wie bei der Schreibmaschine — die nächste oder übernächste Zeile einschalten. Das Zählwerk muß daher für je zwei Zeilen eine um je „Hundert" höhere Zahl anzeigen.

Das Chiffrat kann auch bei dieser Type an jeder Stelle — durch Umschaltung des Hebels auf „Klarschrift" — unterbrochen werden, die Maschine schreibt dann weiter Klarschrift. Von diesem Momente an bleiben auch bei dieser Type Zählwerk und Chiffriermechanismus von selbst stehen.

Beim Dechiffrieren ist der Umschalthebel statt auf „Chiffrieren" auf „Dechiffrieren" zu stellen.

Sind bei der Übermittlung eines Chiffrates, z. B. auf telegraphischem Wege, einzelne Buchstaben oder ganze Gruppen von Buchstaben ausgeblieben, so drückt man die schwarze Transporttaste so oft nieder, als Buchstaben fehlen. Der Chiffriermechanismus wird dadurch so weiterbefördert, als ob Buchstaben geschrieben worden wären. Man kann daher trotz der Lücken alle übermittelten Buchstaben entziffern.

Die drehbaren Chiffrierwalzen können untereinander vertauscht werden. Aus den vier drehbaren Betriebswalzen können durch Vertauschung neue Kombinationen hergestellt werden. Die Chiffrierwalzen können aber auch durch vollkommen anders geschaltete Walzen ersetzt werden.

Der komplette Schlüssel besteht daher auch bei dieser Type nicht nur aus acht Buchstaben (und fünf Ziffern). Diese bilden vielmehr bloß den sog. „äußeren Schlüssel".

Die Stellung der Buchstabenringe und die Stellung der Walzen in der Maschine bilden den sog. „inneren Schlüssel". Diese Walzen können, wie bereits erwähnt, in beliebiger Anzahl beschafft und gegeneinander vertauscht werden. Der Dechiffreur

muß also den äußeren Schlüssel und überdies die Spezialschaltung der Maschine und Walzen und die Stellung der Buchstabenringe kennen.

Die Periodenlänge und die Anzahl der Perioden und Schlüssel der Typenhebelmaschine (B) ist die gleiche wie bei der Typenradmaschine (A).

Die Maschinen haben vier 26teilige Chiffrierwalzen, die durch vier Antriebsräder mit 11er-, 15er-, 17er- und 19er-Teilung angetrieben werden.

Das	11er-Antriebsrad	hat	5	stehengebliebene	Zähne	und	6	Lücken
„	15er- „	„	9	„	„	„	6	„
„	17er- „	„	11	„	„	„	6	„
„	19er- „	„	11	„	„	„	8	„

Es werden also nicht immer alle vier Walzen angetrieben.

Die Länge einer Chiffrierperiode ist nach Berechnung der Firma:

$$11 . 15 . 17 . 19 . 26 = 1{,}885.670 \text{ Schritte.}$$

Die Anzahl der Schlüssel:

$$11 . 15 . 17 . 19 . 26^4 = 24.354{,}535.920.$$

Die Anzahl der Perioden:

$$\frac{11 . 15 . 17 . 19 . 26^4}{11 . 15 . 17 . 19 . 26} = 26^3 = 17.576.$$

Die Anzahl der in der Maschine vorhandenen Tauschalphabete:

$$26^4 = 456.976.$$

Die Anzahl der überhaupt möglichen Tauschalphabete: 26!

Der Antriebsmechanismus (Zahnräder) komme nach $11 . 15 . 17 . 19 = 53.295$ Schritten wieder in seine Anfangsstellung.

Bei Berücksichtigung der Verstellung der Buchstabenringe auf den Chiffrierwalzen ist nach Berechnung der Firma die unter „Anzahl der Schlüssel" angegebene Zahl noch mit $26^4 = 456.976$ zu multiplizieren, da zu jedem bestehenden Tauschalphabet ein anderer Schlüssel oder umgekehrt zu jedem Schlüssel ein anderes Tauschalphabet gehört.

Weitere Sicherungsmöglichkeiten erblickt die Firma noch in dem sogenannten „Verbohren der Schlüsselknöpfe" für die 11er-, 15er-, 17er- und 19er-Räder. Hiedurch könne sich die Zahl der Schlüssel um das 53.295fache ($= 11 . 15 . 17 . 19$) vervielfältigen.

Erläuterung der Tafel N:

Fig. I	Detail	1	Traggriffe.
„ II	„	2	Wagen-Befestigungsschraube.
„ I	„	3	Zuleitungskabel.
„ I, II, III	„	4	Zeilenschalthebel.
„ II, III	„	5	Papierauslöser.

Fig. I, II	Detail	6	Lasche für den Walzenfreilauf (Stechwalze).
„ II	„	7	Randsteller (um Zeilenanfang- und -ende einzustellen).
„ II	„	8	Fächeranschlag und Arretierknopf für Zeilenbegrenzung bei „Chiffrieren", „Dechiffrieren" und „Klarschrift".
„ II	„	9	Stecker.
„ II, III	„	10	Kordelschrauben in den Stirnseiten des Wagens zum Herausnehmen desselben.
„ II	„	11	Griffe für die Wagenauslösung.
„ III	„	12	Laschen für das Herausnehmen des Wagens.
„ III	„	13	Zapfen für das Herausnehmen des Wagens.
„ II, III	„	14	Hebel in der Mitte der Seitenteile des Wagens zum Herausnehmen der Walze.
„ I	„	15	Umstellknöpfe für das Farbband.
„ II	„	16	Tastenfeld.
„ II	„	17	Weiterschalttaste.
„ I	„	18	Umschalthebel (Klarschrift, Chiffrieren, Dechiffrieren).
„ I, II	„	19	SS Taste.
„ I, II	„	20	US Taste.
„ I	„	21	Kordierter Knopf am Umschalthebel.
„ II	„	22	Zählwerk.
„ I, II	„	23	Glatter Knopf links vom Zählwerk.
„ I, III	„	24	Kordierter Knopf links vom Zählwerk.
„ III	„	25	Fenster für das Zählwerk.
„ I, II, III	„	26	Kurbel.
„ III	„	27	Kurbelloch.
„ III	„	28	Knopf I zum Einstellen der Schlüsselbuchstaben.
„ III	„	29	Knopf II zum Einstellen der Schlüsselbuchstaben.
„ III	„	30	Knopf III zum Einstellen der Schlüsselbuchstaben.

Fig. III Detail 31 Knopf IV zum Einstellen der Schlüsselbuchstaben.
„ III „ 32 Buchstabenfenster.
„ III „ 33 Markierte Linie am Zylinder (Einstellknöpfe).
„ III „ 34 Markenstrich am Zylinder (Einstellknöpfe).
„ II „ 35 Taste „Umschaltung für Zahlen, Zeichen und Zwischenraum".
„ II „ 36 Taste „Umschaltung für Buchstaben".

Modell C (ohne Schreibvorrichtung).

Die Type C (Glühlampentype) ist dargestellt auf Tafel O.[36]) Diese Type ist mit einer Trockenbatterie von vier Volt Spannung ausgerüstet. Außerdem sind Anschlußklemmen für einen Akkumulator von vier Volt Spannung vorhanden.

Innerhalb von etwa 17.000 Buchstaben wird selbsttätig nach jedem Buchstaben ein anderes Tauschalphabet eingeschaltet.

Die Sicherheit besteht auch bei dieser Type nicht nur in den vier Schlüsselbuchstaben oder Zahlen, sondern auch in der Reihenfolge der Walzen und in der Stellung der Buchstaben- oder Zahlenringe auf den vier Chiffrierwalzen.

Von den vier Chiffrierwalzen wird eine als sogenannte Umkehrwalze bezeichnet. Diese eine Walze läßt sich nur in zwei verschiedene Stellungen bringen. Um diese Umkehrwalze von einer dieser Stellungen in die andere zu bringen, muß man sie um 180° drehen. Diese Umkehrwalze ist von außen nicht einstellbar und ist von außen daher bei geschlossener Maschine überhaupt nicht sichtbar. Die restlichen drei Chiffrierwalzen lassen sich von außen einstellen. Jeder dieser Walzen können 26 verschiedene Stellungen gegeben werden.

Die Umkehrwalze hat nur zwei Stellungsmöglichkeiten.

Nach Berechnung der Fabrik sei die Länge einer Chiffrierperiode $26^3 - 26^2 = 16.900$ Schritte; die Anzahl der Schlüssel $26^3 . 6 . 2 = 210.912$; bei Berücksichtigung der zwei Stellungen der Umkehrwalze und der Vertauschung der drei drehbaren

[36]) In diesem Abschnitte sind mit den eingeklammerten römischen Zahlen die Figuren auf Tafel O bezeichnet.

Walzen sei die Anzahl der Perioden $2.6 = 12$. Unter Berücksichtigung der Buchstabenringverstellung bei den drei Walzen ergebe sich als Schlüsselzahl $26^6 . 12 = 3.706{,}989.312$; die Anzahl der Tauschalphabete in der Maschine sei, weil in der Umkehrwalze je 13 Kontakte miteinander verbunden sind, $26^3 . 13 = 228.488$.[37])

Um den verabredeten Schlüssel einzustellen, sind folgende Handgriffe auszuführen (Tafel O):

1. Die Umkehrwalze 11 (II) wird nach rechts geschoben und von ihrem Lagerzapfen abgezogen. Der Zahlen- oder Buchstabenring der Umkehrwalze 8 (II) wird durch Abheben der Feder 7 (II) so weit gedreht, bis der Zapfen der Feder in das Loch unter der verabredeten Zahl (Buchstaben) einschnappt. Die Walze wird dann wieder auf ihren Lagerzapfen gesteckt und so weit bis zum Anschlag nach links zurückgeschoben, daß der Schlitz in den Führungsstift 15 (II) greift.

2. Aus dem vorhandenen Chiffrierwalzensatz werden die für den verabredeten Schlüssel in Frage kommenden drei Chiffrierwalzen herausgenommen. Der Zahlen- oder Buchstabenring jeder Walze, z. B. 8 (II), wird durch Abheben der Feder so weit gedreht, bis der Zapfen der Feder 7 (II) in das Loch unter der verabredeten Zahl (Buchstaben) einschnappt.

3. Die Chiffrierwalzen werden in der verabredeten Reihenfolge auf die Achse gesteckt. (Achsenbund nach links, Zahlen- oder Buchstabenring auf der linken Walzenseite.) Die Walzen werden eingelegt und der Hebel 9 (II) bis zum Anschlag nach rückwärts umgelegt.

4. Die Stellräder werden gedreht, bis die verabredeten Zahlen in den Schaulöchern 3 (II) erscheinen.

Die Bedeutung des Schlüssels soll an einem dem Prospekte entnommenen Beispiele gezeigt werden:

1. Umkehrwalze: b bedeutet z. B. ein nach oben zeigendes „b".

2. *a)* Zahlenring: 07, 24, 13 oder

b) Buchstabenring: G, X, M, bedeutet, daß der Zapfen der Feder 7 (II) in die unter den Zahlen, bzw. Buchstaben gebohrten Löcher eingreifen muß.

[37]) Analog den Typen A, B. Die Berechnungen bei D basieren auf den Berechnungen ad C.

3. Reihenfolge der Walzen: II, III, I bedeutet, daß die Walzen, welche diese Kenn-Nummern tragen, in dieser Reihenfolge auf die Achse geschoben werden müssen.

4. *a)* Sichtbare Zahlen: 10, 03, 12 oder

b) Sichtbare Buchstaben: J, C, L. Sie bedeuten, daß diese Zahlen, bzw. Buchstaben in den Schaulöchern 3 (I und II) sichtbar sein müssen.

Will man chiffrieren, so stellt man den Schaltergriff 5 (I und II) auf „dunkel". Falls die Buchstaben zu schwach aufleuchten, stellt man ihn auf „hell". Der Text wird Buchstabe für Buchstabe, wie auf einer Schreibmaschine, durch Niederdrücken der Tasten chiffriert.

Jede Taste ist so weit niederzudrücken, bis eine Lampe aufleuchtet und so die Chiffre sichtbar macht.[38]) Das Chiffrat wird auf quadriertem Papiere aufgezeichnet.

Jede Maschine eignet sich ohneweiters auch zum Dechiffrieren. Ist der verabredete Schlüssel in allen Teilen eingestellt und ist der Strom durch Drehen des Schaltergriffes 5 (I und II) eingeschaltet, so wird das Chiffrat Buchstabe für Buchstabe durch Niederdrücken der Tasten getypt. Die aufleuchtenden Buchstaben ergeben nun den Klartext.

Hat man versehentlich eine falsche Taste gedrückt, so muß man die rechte Chiffrierwalze um einen Schritt zurückstellen. Es ist darauf zu achten, daß auch die mittelste und eventuell die linke Walze um diesen Schritt zurückgedreht werde, falls sie vorher mittransportiert wurde.

Erläuterung der Tafel O:

Fig. I, II	Detail	1	Tastenfeld.
„ I, II	„	2	Glühlampenfeld.
„ I, II	„	3	Schaulöcher.
„ I, II	„	4	Chiffrierwalzen.
„ I, II	„	5	Schaltergriff.
„ I, II	„	6	Anschlußknöpfe für Akkumulatorenbetrieb.

[38]) Als Glühlampen dürfen nur solche von 12·5 *mm* Durchmesser und Halbkugelform, wie sie in den meisten gewöhnlichen Taschenlampen vorhanden sind, benutzt werden.

Fig. II	Detail	7	Feder für Verstellen des Buchstaben(Zahlen)-ringes.
„ II	„	8	Buchstaben(Zahlen)ring.
„ II	„	9	Hebel.
„ II	„	11	Umkehrwalze.
„ I	„	12	Deckelschrauben.
„ II	„	14	Lokal-Trockenbatterie.
„ II	„	15	Führungsstift.
„ II	„	R	Reservelampen.

Modell D.

Während bei Modell C die von außen unsichtbare Umkehrwalze nur in zwei verschiedene Stellungen gebracht werden konnte, läßt sich bei dieser Type die Umkehrwalze in 26 verschiedene Stellungen bringen. Die Umkehrwalze ist auch von außen sichtbar. Es lassen sich daher auch von außen die 26 verschiedenen Positionen dieser Walze einstellen. In Tafel P, Fig. I und II, ist die Type D abgebildet. Die äußerste der vier Walzen auf der linken Seite ist die Umkehrwalze. Die konstruktive Anlage des Vierwalzensystems gestattet dem Chiffreur nicht, diese Umkehrwalze aus der Maschine herauszunehmen und durch eine andere Walze zu vertauschen. Er kann lediglich mit Hilfe des einstellbaren Zahnrades, welches sich rechts von der Walze befindet, derselben 26 verschiedene Stellungen geben. Der Buchstabenring läßt sich auf jeder der Walzen nach Lockern einer Feststellungsvorrichtung (Feder) drehen und also verschieden einstellen. Die weiteren drei Walzen können vor dem Arbeiten mit der Maschine auch herausgenommen und in ihrer Stellung gegeneinander vertauscht oder durch andere Walzen ersetzt werden. Walze 1 (Umkehrwalze) bleibt also immer in ihrer Stelle. Die Walzen 2, 3, 4 können sowohl in ihrer Stellung zueinander verändert als auch durch andere Walzen ersetzt werden. Es werden daher über Verlangen gleichzeitig mit dem Apparate auch Kästchen mit Ersatzwalzen geliefert. Diese Ersatzwalzen unterscheiden sich von den drei Originalwalzen, die sich in der Maschine befinden, dadurch, daß sie anders geschaltet sind. Die Anzahl der Möglichkeiten (Anzahl der überhaupt möglichen verschiedenen Walzen) be-

rechnet die erzeugende Fabrik — im Hinblicke darauf, daß jeder Kontakt jeder Seite mit jedem Kontakte der andern Seite verbunden werden kann — mit 26! Bei Betrachtung von Tafel P, Fig. II, hat es den Anschein, als wenn sich neben den vier mit Buchstabenzeichen versehenen Walzen noch eine fünfte nicht beschriebene Walze befinden würde. Dieser walzenförmige Bestandteil der Maschine ist jedoch nicht beweglich. Er dient dazu, die 26 Kabel zu den Walzen zu leiten. Der durch diese Kabel geführte elektrische Strom geht durch das Walzensystem hindurch. Tafel Q, Fig. I, zeigt eine der beweglichen Walzen von der einen, Fig. II von der andern Seite. Wir sehen bei Fig. I eine Reihe beweglicher, federnder Stifte, bei Fig. II eine Reihe von kreisförmig am Walzenrande angebrachten Kontakten. Die Walzen sind in ihrer Lage zueinander so angebracht, daß beim Drehen der Walzen die Kontaktstifte an den Kontaktflächen schleifen (Tafel Q, Fig. III). Hiedurch scheuern sie sich automatisch stets blank. Es ist selbstverständlich möglich, die durch den walzenähnlichen Bestandteil (die scheinbare fünfte Walze) eintretenden Kontakte und die Kontakte der drei beweglichen Walzen beliebig zu verbinden. Durch die Chiffrierwalzen wird bei den Modellen C und D jeder einzelne Buchstabe achtmal chiffriert, bevor er endgültig festgelegt wird. Man erhält also nach Angabe der Fabrik ein siebenmal überchiffriertes Chiffrat!

Auch bei dieser Type müssen wir die äußere und die innere Schlüsseleinstellung unterscheiden. Die äußere Schlüsseleinstellung erfolgt mit Hilfe der vier Zahnräder, Tafel P, Fig. I und II. Mit demselben äußeren Schlüssel erhält der Chiffreur aber selbstverständlich bei verschiedener innerer Schlüsseleinstellung vollkommen verschiedene Chiffrate. „Äußerlich völlig gleichlautende Schlüssel geben für den, der die Reihenfolge der Walzen und die Ringverstellung nicht kennt, absolut verschiedene Chiffrate.“ Der Dechiffreur muß, um arbeiten zu können, die äußere Schlüsseleinstellung kennen, weil er sonst das Dechiffrat nicht beginnen kann. Er muß aber, um das Dechiffrat fortsetzen zu können, auch die innere Schlüsseleinstellung kennen, d. h., er muß wissen, wie die Buchstaben auf jeder Walze eingestellt sind, ferner wie die einzelnen Walzen zueinander und wie die Kabel eingestellt sind.

„Bei Anwendung des gleichen äußeren Schlüssels ergibt sich eine Anzahl verschiedener Möglichkeiten, welche ziffernmäßig ausgedrückt wird durch das Produkt aus ungefähr 450.000mal der Anzahl der möglichen Walzenstellungen. Hat der Chiffreur bloß drei Walzen, so kann er dieselben zueinander in sechs verschiedene Stellungen bringen. Es sind daher sechsmal 450.000 = 2,700,000 Möglichkeiten gegeben. Besitzt er außerdem noch sieben Reservewalzen, so stehen ihm" unverhältnismäßig mehr „Möglichkeiten zu Gebote. Die verschiedenen Schaltungen der Kabel ermöglichen ihm bei jeder Walze eine ungeahnt große Zahl verschiedener Möglichkeiten. Um so mehr bei vier Walzen!"

Auch bei dieser Type wird natürlich bei jeder angeschlagenen Buchstabentaste das Austauschalphabet geändert.[39])

Die Maschine ist auf folgende Weise zu handhaben:

1. Schlüsseleinstellung:

a) Öffnen des Deckels und Herausnehmen der Walzen. Schaltergriff 5 (Tafel P, Fig. I und II) parallel zum rechten Rande stellen. Die beiden Deckelschrauben 12 (Tafel P, Fig. I) lösen, Deckel hochklappen. Hebel 9 (Tafel P, Fig. I) in die senkrechte Stellung bringen, Umkehrwalze 11 (Tafel P, Fig. I und II) bis zum Anschlag nach links schieben, die drei rechten Chiffrierwalzen 4 (Tafel P, Fig. I und II) an den Stellrädern zusammendrücken und gemeinsam nach oben heben; alsdann diese Walzen von der Achse ziehen.

Um den verabredeten Schlüssel einzustellen, sind folgende Handgriffe notwendig:

b) Auswahl der Walzen und Reihenfolge der Walzen. Aus dem vorhandenen Chiffrierwalzensatz die für den verabredeten Schlüssel in Frage kommenden drei Chiffrierwalzen herausnehmen und die Chiffrierwalzen in der verabredeten Reihenfolge auf die Achse stecken. (Achsenbund nach links, Buchstabenring auf der linken Walzenseite), Walzen einlegen und Hebel 9 (Tafel P, Fig. II) bis zum Anschlag nach rückwärts umlegen.

[39]) Bei allen Typen wird für jeden Buchstaben ein neues Tauschalphabet eingeschaltet. Es existieren in einem Chiffrat daher keine konstatierbaren Häufigkeiten.

c) Einstellen der Ringe auf den Walzen. Den Buchstabenring aller vier Walzen nacheinander durch Abheben der Feder 7 (Tafel P, Fig. II) so weit drehen, bis der Zapfen der Feder in das Loch unter dem verabredeten Buchstaben einschnappt.

d) Äußere Einstellung der Buchstaben in den Schaulöchern. Deckel schließen. Stellräder drehen, bis die verabredeten Buchstaben in den Schaulöchern 3 (I) erscheinen.

e) Zusammensetzung des Schlüssels.

„Der Schlüssel lautet also z. B. (stets von links angefangen):

1. Reihenfolge der Walzen: II, III, I bedeutet, daß die Chiffrierwalzen 4 (Tafel P, Fig. I und II), die auf den Stirnseiten der beweglichen Kontakte diese Kenn-Nummern tragen, z. B. in dieser Reihenfolge (Zählweise vom Bund der Achse aus) auf die Achse geschoben sind. Wenn mehr als drei Chiffrierwalzen vorhanden sind, bedeuten die römischen Ziffern auch zugleich die auszuwählenden Walzen (z. B.: VIII, IV, X).

2. Buchstabenringe: G, X, M, Z bedeutet, daß der Zapfen der Feder 7 (Tafel P, Fig. II) unter die (unter den Buchstaben) gebohrten Löcher eingreift, u. zw. sowohl für die Umkehrwalze wie für die drei Chiffrierwalzen.

3. Sichtbare Buchstaben: Z, S, A, N bedeutet, daß diese Buchstaben in den Schaulöchern 3 (Tafel P, Fig. I) sichtbar sind."

2. Chiffrieren:

„Der Schaltergriff 5 (Tafel P, Fig. I und II) ist auf ‚dunkel' zu stellen; falls die Buchstaben zu schwach aufleuchten, auf ‚hell'. Es empfiehlt sich, quadriertes Papier zum Aufzeichnen zu verwenden. Der Text wird Buchstabe für Buchstabe, wie auf einer Schreibmaschine, durch Niederdrücken der Tasten 1 (Tafel P, Fig. I und II) chiffriert. Jede Taste ist so weit niederzudrücken, bis eine Lampe 2 (Tafel P, Fig. I und II) aufleuchtet. Falls es erwünscht ist, Wortzwischenräume zu geben, so kann nach jedem Worte z. B. die X-Taste gedrückt werden."

Die Sicherheit des Chiffrates kann durch „Benützung eines Influenzbuchstaben beim Chiffrieren" erhöht werden. Man kennzeichne eine beliebige Taste (z. B. P) durch Aufstecken eines

Gummiknopfes oder durch Überkleben mit einem roten Zelluloidplättchen. Jedesmal, wenn man beim Abschreiben des Klartextes die Taste, also im beispielsweise gewählten Falle „P", niedergedrückt hat, bewegt man die linke (Umkehr-)Walze einen Schritt nach vorne, so daß z. B. statt „G" alsdann ein „F" im Fenster erscheint. Durch diesen Influenzbuchstaben ergibt jedes Chiffrat, auch wenn es mit der gleichen kompletten Schlüsseleinstellung geschrieben wird, auch mit der gleichen Maschine, eine vollständig andere Periode, die von der Häufigkeit eines beliebigen Buchstaben abhängt.

3. Dechiffrieren.

„Jede Maschine eignet sich ohneweiters zum Chiffrieren und zum Dechiffrieren. Nachdem der verabredete Schlüssel in allen Teilen eingestellt ist und der Strom durch Drehen des Schaltergriffes 5 (I und II) eingeschaltet ist, wird das Chiffrat Buchstabe für Buchstabe durch Niederdrücken der Tasten abgeschrieben. Die aufleuchtenden Buchstaben ergeben alsdann den Klartext."

Im Falle beim Chiffrieren ein Influenzbuchstabe benützt wurde, legt man vor dem Dechiffrieren ein rotes Zelluloidplättchen auf den Buchstaben „P" des Glühlampenfeldes und muß nun jedesmal, nachdem der Buchstabe „P" rot aufgeleuchtet hatte, die linke (Umkehr-)Walze wie oben einen Schritt bewegen, so daß alsdann wieder z. B. statt „G" ein „F" im Fenster erscheint.

4. Verschreiben.

„Hat man versehentlich eine falsche Taste gedrückt, so muß man die rechte Chiffrierwalze um einen Schritt zurückstellen. Es ist darauf zu achten, daß auch die mittelste und eventuell linke Walze um diesen Schritt zurückgedreht werden, falls sie vorher mittransportiert wurden. Man kann das Chiffrat zur Kontrolle an jeder beliebigen Stelle wiederholen."

Die Umkehrwalze ist in 26 Stellungen einstellbar. Die Länge einer Periode berechnet die Fabrik mit $26^3 - 26^2 = 16.900$.

Die Weiterschaltung der Walzen sei nämlich nicht eine rein „zählwerkmäßige", sondern die Hundertwalze (die erste angetriebene Walze von links) werde durch die Schaltklinke der

Zehnerwalze vorzeitig um einen Schritt beweg. Daher lautet die Formel $26^3 - 26^2$.

Die Anzahl der Schlüssel sei mit $26^4 . 6 = 456.976 . 6 = 2{,}771.856$, die größtmöglichste Schlüsselzahl unter Berücksichtigung der Buchstabenringverstellung mit $26^8 . 6 = 1{,}552.961{,}187.456$, die Anzahl der Tauschalphabete mit $26^3 . 13 = 228.488$ zu berechnen.[40])

Erläuterung der Tafel P:

Fig.	I, II	Detail	1	Tastenfeld.
„	I, II	„	2	Glühlampenfeld.
„	I	„	3	Schaulöcher.
„	I, II	„	4	Chiffrierwalzen.
„	I, II	„	5	Schaltergriff.
„	I, II	„	6	Anschlußknöpfe für Akkumulatorenbetrieb.
„	II	„	7	Feder für Verstellen des Buchstabenringes.
„	II	„	8	Buchstabenring.
„	II	„	9	Hebel.
„	II	„	11	Umkehrwalze.
„	I	„	12	Deckelschrauben.
„	II	„	14	Lokal-Trockenbatterie.
„	II	„	15	Führungsstift.
„	II	„	R	Reservelampen.

* * *

Die im zweiten Teile erwähnten Patente beziehen sich:

D. R. P. Nr. 416.219 } auf die Chiffrierwalzen,
„ „ 416.833 }
„ „ 425.147 auf das Chiffriersystem,
„ „ 378.238 auf die „Code"-Maschine,
„ „ 387.893 } auf die Umschaltung (Zahlen, Zeichen
„ „ 409.301 } und Buchstaben).
„ „ 383.594 auf den selbsttätigen Stillstand der Chiffriereinrichtung nach einer bestimmten Anzahl Buchstaben,

40) Die von der Fabrik dem Verfasser zu Modell A bis D bekanntgegebenen Ziffern konnten noch nicht mathematisch kontrolliert werden.

D. R. P. Nr. 385.682 auf die Verwürfelung auch innerhalb der Zeilen,

„ „ 411.126 auf die Verstellung der Buchstabenringe auf den Walzen,

„ „ 400.795 auf zwei Schreibvorrichtungen (eine für Chiffriertext und die andere für Klartext)

„ „ 408.949 auf die Bremsvorrichtung für umlaufende Typenräder,

„ „ 407.804 auf den Antrieb der Glühlampenmaschine,

„ „ 425.566 auf die Umschaltung für Zahlen, Zeichen und Buchstaben, bei Verwendung der Buchstaben j und q,

„ „ 412.582 auf die Chiffrierwalzenblockierung,

„ „ 429.122 auf den aperiodischen Walzenantrieb (Lükkenzahnräder, Einstellknöpfe).

Universitäts-Buchdruckerei „Styria“, Graz.