Manuelle Kryptografie

(weitere Verschlüsselungsverfahren)

In diesem Dokument finden Sie viele weitere unbekanntere historische oder modernere Verfahren, die wegen des begrenzten Umfangs des Buches dort leider nicht integriert werden konnten. Diese Verfahren werden kurz, aber dennoch verständlich beschrieben.

Zusammenhänge mit den Begriffen und Verfahren aus dem Buch werden erwähnt und in einer Fußnote konkret gekennzeichnet, aber nicht noch einmal erklärt.

Version 1.00

Inhaltsverzeichnis

1 Transposition

1.1 Sudoku-Chiffre

Eine interessante Transposition kann mithilfe eines Sudoku-Quadrates durchgeführt werden.[1] Zusätzlich wird noch ein Schlüsselwort der Länge 9 benötigt. Natürlich kann auch wie in diesem Beispiel mit `SUDOKUQUADRAT` ein längeres Schlüsselwort gewählt werden, das dann entsprechend verkürzt wird.

Klartext	`Dies ist ein geheimer Text mit wichtigen Informationen`
Schlüssel	`Sudoku-Quadrat SUDOKUQUADRAT`

Für das dargestellte Beispiel wird das nachfolgende Sudoku-Quadrat gewählt.

1	4	2	5	8	9	3	7	6
5	3	9	6	7	4	8	1	2
6	8	7	2	1	3	4	5	9
2	6	4	9	5	1	7	3	8
9	7	3	8	4	2	1	6	5
8	1	5	3	6	7	9	2	4
3	5	6	1	9	8	2	4	7
7	2	8	4	3	5	6	9	1
4	9	1	7	2	6	5	8	3

Der Klartext wird horizontal in ein leeres 9 x 9 - Quadrat geschrieben und aus dem Schlüsselwort ein numerischer Schlüssel mit den Ziffern 1 bis 9 erstellt. Diese neun Ziffern sollten zur einfacheren Verschlüsselung über das Sudoku-Quadrat mit dem Klartext platziert werden.

S	U	D	O	K	U	Q	U	A
6	7	2	4	3	8	5	9	1

Den Buchstaben der oberen Zeile des Klartext-Quadrates werden die Zahlen des numerischen Schlüssels als Kennzahlen zugeordnet und in die Zeilen der ersten Spalte des Zielquadrates platziert, die mit der Kennzahl übereinstimmt. Dem ersten Buchstaben `D` ist die 6 zugeordnet, die sich in der dritten Zeile der ersten Spalte des Sudoku-Quadrates befindet. Damit wird dieser Buchstabe auch in die entsprechende Zelle des Zielquadrates geschrieben.

Dem zweiten Buchstaben `I` ist die Zahl 7 zugeordnet, die in der zweiten Zeile von unten des Sudoku-Quadrates zu finden ist. Damit ist auch für diesen Buchstaben die zugehörige Zelle im Zielquadrat gefunden. Wenn nach dieser Regel alle Buchstaben der oberen Zeile des

[1] Cryptogram [144]

Klartext-Quadrates übertragen sind, ist die linke Spalte des Zielquadrates vollständig gefüllt.

6	7	2	4	3	8	5	9	1
D	I	E	S	I	S	T	E	I
N	G	E	H	E	I	M	E	R
T	E	X	T	M	I	T	W	I
C	H	T	I	G	E	N	I	N
F	O	R	M	A	T	I	O	N
E	N							

Klartextquadrat

I								
T								
D								
E								
E								
S								
I								
I								
S								

Zielquadrat

Entsprechend werden dann die Buchstaben aller anderen Klartextzeilen in die Spalten des Zielquadrates übertragen.

I	H	X	N	T				
T	E	W	C	O				
D	I	E	T	N				
E	N	T	I	I				
E	G	M	E	M				
S	R	T	G	F	N			
I	M	T	N	O				
I	E	I	I	A				
S	E	I	H	R	E			

Abschließend wird das Quadrat horizontal ausgelesen und man erhält den Geheimtext.

Geheimtext	IHXNT TEWCO DIETN ENTII EGMEM SRTGF NIMTN OIEII ASEIH RE

1.2 Rubik's Cube

Douglas W. Mitchell schlug 1992 ein Verschlüsselungsverfahren vor, das auf dem bekannten Würfel von Ernő Rubik basiert.[2] Dieser Würfel besteht aus 26 sichtbaren Teilwürfeln, von denen nur die jeweils mittleren der sechs Seitenflächen mit dem unsichtbaren Zentrum fest miteinander verbunden sind. Diese Teilwürfel lassen sich in Höhe, Breite und Tiefe durch

[2] Mitchell [139], Müller [145] S. 4-24 ff, Van der Vieren [208]

Drehungen um die drei Raumachsen bewegen, sodass die Position und Lage von 20 der insgesamt 26 äußeren Steine fast beliebig verändert werden kann.

Obwohl die Farben für dieses Verfahren keine Rolle spielen, sollen sie beibehalten werden, um die durchzuführenden Schritte besser zu verdeutlichen.

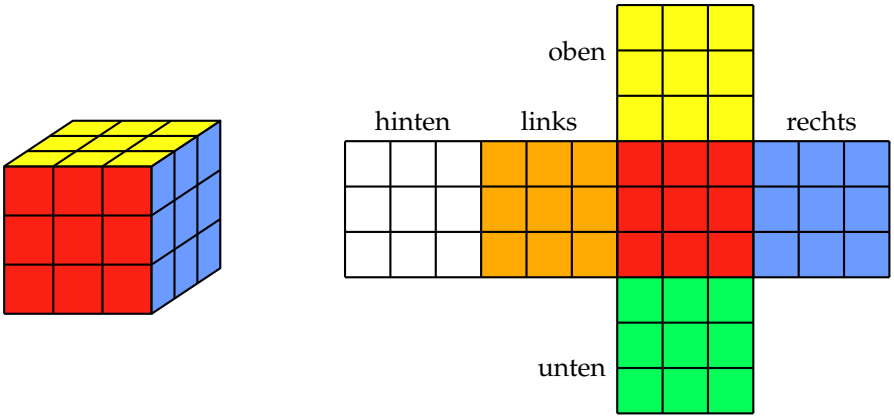


Abb. 1.1: Rubik's Cube mit Netz

Für eine übersichtliche Orientierung wird der linke obere Teilwürfel auf der roten Vorderfläche wie in Abbildung 1.3 mit 1 beschriftet. Diese Ausrichtung dient in allen Schritten als Grundeinstellung, die nie verändert wird.

Drehungen des Würfels werden durch die Bezeichnungen `Z` für Zeilen, `S` für Spalten und `E` für Ebenen bzw. Tiefen festgelegt. Dabei ist die Drehrichtung fest vorgegeben und wird mit den Zahlen 1, 2 und 3 für die Drehwinkel 90°, 180°sowie 270° gekennzeichnet. Die Codes 1 bis 3 legen gleichzeitig fest, dass nur die Zeile, Spalte oder Ebene gedreht wird, die sich entgegengesetzt zum linken oberen Teilwürfel mit der Zahl 1 befindet. Also die untere Zeile, die rechte Spalte sowie die hintere Ebene.

Als zweite Möglichkeit können jeweils zwei Zeilen, Spalten oder Ebenen gleichzeitig gedreht werden, die nicht den linken oberen Teilwürfel enthalten. Damit kann etwa eine nicht erlaubte Linksdrehung der oberen Zeile um 90° simuliert werden, indem diese durch eine Drehung der beiden unteren Zeilen um 270° unter Beibehaltung der Orientierung ersetzt wird. Bei diesen zweifachen Drehungen werden die Codes 1 bis 3 für die Einzeldrehungen um drei erhöht

und erhalten damit die Werte 4 bis 6.

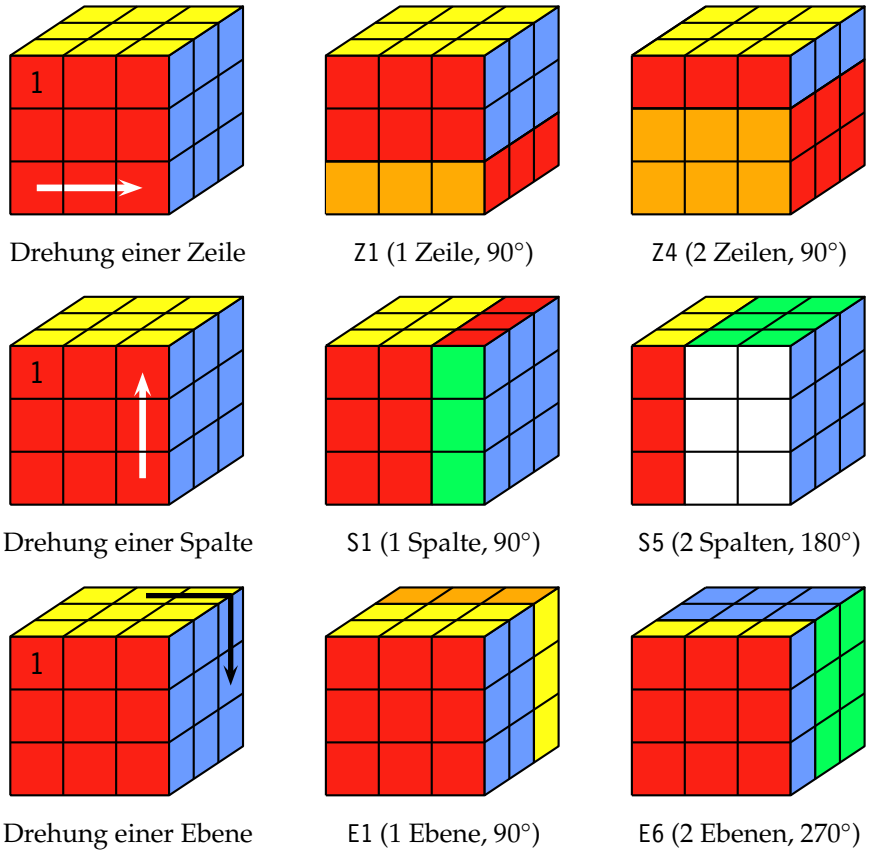


Abb. 1.2: Drehungen mit Kennzeichnungen

Um das Verfahren anwenden zu können, muss der Klartext aus 48 Zeichen bestehen und eventuell mit Füllzeichen verlängert werden.

Für das Eintragen werden die fünf noch leeren Seitenflächen mit den Zahlen von 2 bis 6 gekennzeichnet, wobei die jeweilige Position auf dieser Seitenfläche unter den neun Positionen beliebig gewählt werden kann. Die Reihenfolge der Nummerierung wird durch den ersten Schlüssel festgelegt. Dazu werden die Seitenflächen im Netz der Abbildung 1.1 etwa von oben nach unten und von links nach rechts mit den Buchstaben von `A` bis `F` gekennzeichnet.

Dann entspräche die Reihenfolge der Seitenflächen in Abbildung 1.3 dem Schlüssel `DCEFAB`.

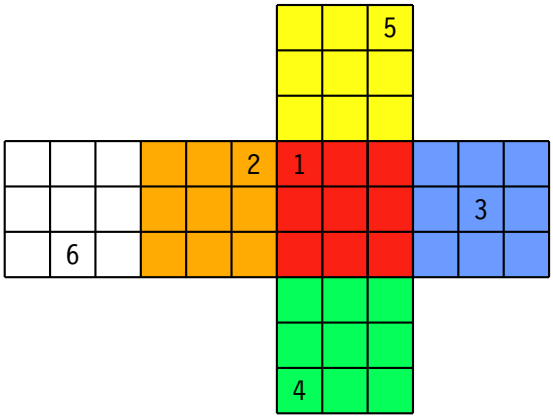


Abb. 1.3: Kennzeichnung der Seitenflächen

Für die Verschlüsselung wird zusätzlich ein zweiter Schlüssel benötigt, der die durchzuführenden Drehungen beschreibt.

Klartext	`Ein Text mit sehr wichtigen und geheimen Informationen`
Schlüssel	`DCEFAB Z1S3E4S6Z2`

Der Klartext wird in der Reihenfolge der Kennzahlen 1 bis 6 von links nach rechts und von oben nach unten in die Seitenflächen eingetragen. Dabei werden die bereits vorhandenen Zahlen von 1 bis 6 übersprungen, sodass auf jeder Seite nur acht Zeichen zusätzlich ihren Platz finden.

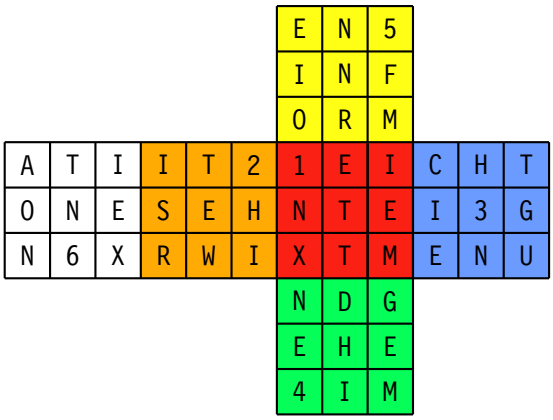


Abb. 1.4: Der Würfel nach den Drehungen

Um den Geheimtext zu erzeugen, wird der Würfel so gedreht, wie es mit dem zweiten Schlüssel festgelegt ist. Dabei darf nicht mehrmals hintereinander dieselbe Zeile, Spalte oder Ebene

gedreht werden, weil sich diese Drehungen dann überlagern würden.

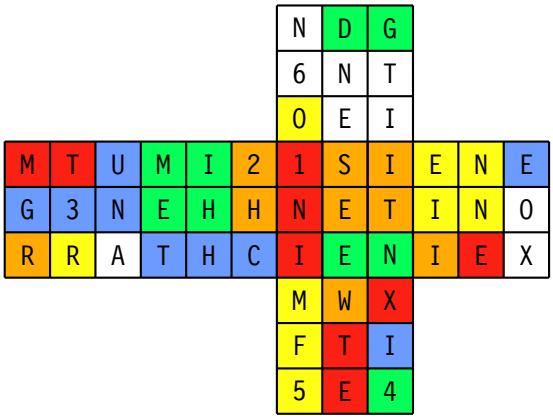


Abb. 1.5: Eintragen des Klartextes

Abschließend wird der Geheimtext in der durch den ersten Schlüssel festgelegten Reihenfolge der Seitenflächen abgelesen. Obwohl sich die Zahlen 2 bis 6 jetzt auf anderen Seitenflächen befinden, kann die Orientierung des Würfels durch die unveränderte Zahl 1 auf der Vorderfläche jederzeit wiederhergestellt werden.

Geheimtext	`1SINETIEN MI2EHHTHC ENEINOIEX MWXFTI5E4 NDG6NTOEI MTUG3NRRA`

Varianten

Neben den durch die beiden Schlüssel festgelegten Varianten, kann dieser Algorithmus durch weitere Veränderungen erweitert werden. So kann etwa die Nummerierung der Seiten mit den Zahlen von 2 bis 6 durch einen zusätzlichen Schlüssel variabel gestaltet werden und muss nicht mit der Reihenfolge beim Auslesen des Geheimtextes übereinstimmen.

Auch muss das Eintragen des Klartextes in die Seitenflächen nicht mit der beschriebenen Ausrichtung erfolgen. Durch den Wechsel der Schreibrichtung von unten nach oben oder von rechts nach links ergeben sich insgesamt vier Möglichkeiten.

1.3 Lazy Swagman

Eine vereinfachte und schnellere Variante der *Swagman*-Verschlüsselung wurde 1978 mit der *Lazy Swagman*-Chiffre vorgestellt.[3] Sie benutzt keine getrennten Tabellen, sondern eine einzige Tabelle sowohl für die Verschlüsselung als auch für die Entschlüsselung.

Klartext	`Dies ist ein geheimer Text mit einer sehr wichtigen Information`
Schlüssel	`4`

[3] Cryptogram [217], Cryptogram [189], Cryptogram [187], Cryptogram [190]

Für die Verschlüsselung wird ein lateinisches Quadrat als Schlüssel verwendet, welches in dem dargestellten Beispiel die Seitenlänge 4 besitzt.

4	3	1	2
3	4	2	1
1	2	4	3
2	1	3	4

Abb. 1.6: Lateinisches Schlüsselquadrat

Bei der gewählten Seitenlänge muss die Länge n des Klartextes ein Vielfaches von 4 sein und eventuell durch Füllzeichen verlängert werden. Die für die Verschlüsselung erforderliche Tabelle besitzt dann vier Zeilen und $\frac{n}{4}$ Spalten, um den Klartext aufnehmen zu können. Die obere Zeile dieser Tabelle besteht aus den periodisch angeordneten Zahlen der oberen Zeile des Schlüsselquadrates. Darunter folgen die Zahlen der weiteren Zeilen des Schlüsselquadrates.

4	3	1	2	4	3	1	2	4	3	1	2	4	3
3	4	2	1	3	4	2	1	3	4	2	1	3	4
1	2	4	3	1	2	4	3	1	2	4	3	1	2
2	1	3	4	2	1	3	4	2	1	3	4	2	1

Abb. 1.7: Tabelle für Lazy Swagman

Zum besseren Verständnis des Verfahrens werden in den folgenden Schritten die Zahlen dieser Tabelle nicht durch Klartextbuchstaben überschrieben, sondern für diese jeweils eine, eigentlich überflüssige, Leerzeile eingefügt. Die ersten $\frac{n}{4}$ Klartextbuchstaben werden spaltenweise von links nach rechts unterhalb der Zellen eingetragen, die die Zahl 1 enthalten. Die nächsten $\frac{n}{4}$ Buchstaben folgen dann bei den Zellen mit der Zahl 2.

4	3	1	2	4	3	1	2	4	3	1	2	4	3
3	4	2	1	3	4	2	1	3	4	2	1	3	4
1	2	4	3	1	2	4	3	1	2	4	3	1	2
2	1	3	4	2	1	3	4	2	1	3	4	2	1
		E				T				G			
			S				E				E		
D				I				I				H	
	I				S				N				E

DIESISTEINGEHE

4	3	1	2	4	3	1	2	4	3	1	2	4	3
3	4	2	1	3	4	2	1	3	4	2	1	3	4
1	2	4	3	1	2	4	3	1	2	4	3	1	2
2	1	3	4	2	1	3	4	2	1	3	4	2	1
		E	R			T	T			G	E		
		E	S			X	E			T	E		
D	M			I	E			I	I			H	N
I	I			T	S			M	N			I	E

IMERTEXTMITEIN

Abb. 1.8: Buchstaben für die Zellen mit den Zahlen 1 und 2

Daran schließen sich die Buchstaben für die Zellen mit de Zahl 3 und abschließend die restli-

chen Buchstaben des Klartextes für die Zahl 4 an.

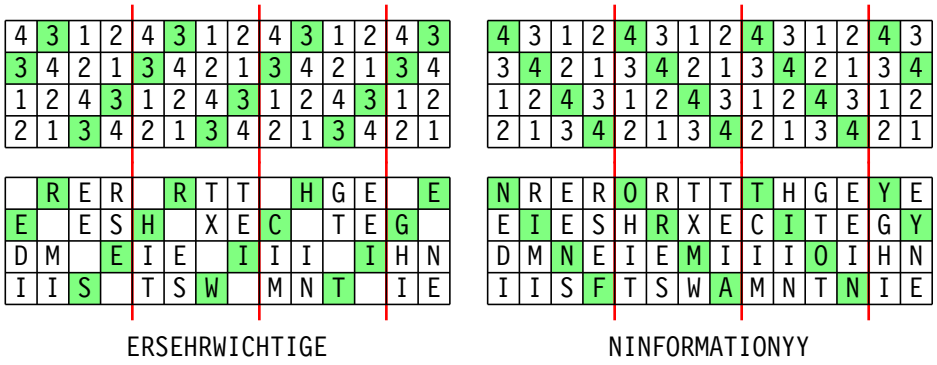


Abb. 1.9: Buchstaben für die Zellen mit den Zahlen 3 und 4

Mit diesen Schritten ist die Tabelle vollständig gefüllt und der Geheimtext kann abschließend spaltenweise ausgelesen werden.

Geheimtext	NEDI RIMI EENS RSEF OHIT RRES TXMW TEIA TCIM HIIN GTOT EEIN YGHI EYNE

Das *Lazy Swagman*-Verfahren ist mit nur einer Tabelle weniger aufwändig als das normale Swagman-Verfahren. Zudem ist die Verschlüsselung schneller und einfacher, die Entschlüsselung allerdings etwas langsamer.

1.4 Tabelle diagonal

Diese Transposition benötigt eine vollständig gefüllte Tabelle, sodass der zu verschlüsselnde Klartext notfalls mit Füllzeichen verlängert werden muss. Als weiteren Schlüssel wird eine Zahl n verwendet, die kleiner als die Tabellenbreite sein muss.[4]

Klartext	Dies ist ein geheimer Text mit vielen Informationen
Schlüssel	6

Das Verfahren arbeitet mit drei Schritten. In den nachfolgenden Abbildungen werden allerdings die fortlaufenden Zahlen ab 1 eingetragen, damit die Reihenfolge des Eintragens der Buchstaben besser ersichtlich wird.

Zunächst werden nacheinander $n = 6$ Buchstaben des Klartextes in die Zeilen der Tabellen eingetragen. Dabei verschiebt sich der Beginn mit jeder Zeile jeweils um eine Position nach

[4] Rubin [164] S. 78

rechts. Die Buchstabenfolgen werden nicht zyklisch in die Zeilen eingetragen, sondern enden in jeder Zeile am rechten Rand.

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	27	28	29

Im zweiten Schritt werden die noch leeren Zellen am rechten Rand von oben nach unten mit den nächsten Buchstaben des Klartextes gefüllt, bevor im dritten Schritt die restlichen Buchstaben in die noch leeren Zellen am linken Rand geschrieben werden.

1	2	3	4	5	6	30	31	32
	7	8	9	10	11	12	33	34
		13	14	15	16	17	18	35
			19	20	21	22	23	24
				25	26	27	28	29

1	2	3	4	5	6	30	31	32
36	7	8	9	10	11	12	33	34
37	38	13	14	15	16	17	18	35
39	40	41	19	20	21	22	23	24
42	43	44	45	25	26	27	28	29

Wenn man mit diesen drei Schritten statt der Zahlen gleich die Buchstaben des Klartextes eingetragen hätte, sähe die Tabelle folgendermaßen aus:

D	I	E	S	I	S	E	N	I
R	T	E	I	N	G	E	N	F
M	A	H	E	I	M	E	R	O
T	I	O	T	E	X	T	M	I
N	E	N	X	T	V	I	E	L

Abschließend kann der Geheimtext vertikal ausgelesen werden.

Geheimtext	`DRMTN ITAIE EEHON SIETX INIET SGMXV EEETI NNRME IFOIL`

1.5 Unregelmäßige Aufteilung

Bei einer weiteren Transposition werden die einzelnen Buchstaben sehr unregelmäßig getrennt.[5]

Klartext	`Dies ist ein sehr geheimer Text`
Schlüssel	1/7

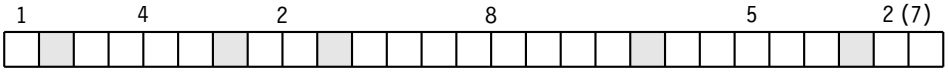
[5] Basic Cryptography [206] S. 94 – 95

Für die Verschlüsselung erstellt man ein Raster, in das die Buchstaben des Klartextes eingetragen werden. Allerdings ist dieses Raster zusätzlich in Bereiche unterteilt, deren Größe sich nach den Dezimalziffern des Schlüssels richtet.

Geeignet sind Brüche mit langen Perioden wie etwa $\frac{1}{7}, \frac{1}{13}, \frac{1}{17}, \frac{1}{19}, \ldots$ Bei dem hier gewählten Schlüssel

$$\frac{1}{7} = 0{,}142857142857142857\ldots$$

besteht der erste Bereich damit nur aus einer Zelle, der zweite aus vier Zellen und so fort. Beim sechsten Bereich lautet die zugehörige Ziffer eigentlich 7. Diese Zahl wird allerdings auf 2 verkleinert, damit die Länge aller Bereiche zusammen genau der Länge des Klartextes entspricht. Eine eventuell auftretende Dezimalziffer 0 wird grundsätzlich übersprungen.



Die Buchstaben des Klartextes werden der Reihe nach in die erste freie Position der Bereiche eingetragen. Nach jedem Buchstaben wird dann zum nächsten, weiter rechts liegenden Bereich gewechselt. Nach den ersten sechs Buchstaben ist bei diesem Beispiel in jedem Bereich ein Buchstabe platziert worden.

D		I					E			S								I						S	

Ist der am weitesten rechts liegende Bereich bearbeitet worden, fährt man am linken Rand fort. Beim siebten Buchstaben T ist der linke Bereich allerdings bereits vollständig gefüllt. In einem solchen Fall wechselt man zum nächsten weiter rechts liegenden Bereich, der noch eine freie Position enthält.

D		I	T				E			S								I						S	

Mit diesem Vorgehen trägt man alle Buchstaben des Klartextes ein.

D		I	T	E	I		E	E		S	I	H	M	R	E	X	T		I	N	E	E	T		S	G

Der Geheimtext kann abschließend von links nach rechts ausgelesen werden.

Geheimtext	DITEI EESIH MREXT INEET SG

1.6 Zyklische Spaltentransposition

Eine etwas verbesserte Version der einfachen Spaltenransposition verwendet zwei Schlüsselworte.[6]

Klartext	`Dies ist ein wichtiger geheimer Text`
Schlüssel	`ZYKLISCH INFO`

Der Klartext wird horizontal in eine Tabelle eingetragen, deren Breite durch die Länge des ersten Schlüsselwortes bestimmt wird. Die Länge des zweiten Schlüsselwortes muss mindestens so viele Buchstaben enthalten, wie die Tabelle Zeilen besitzt. Ist es sogar länger, werden nur die ersten Buchstaben benutzt.

Zu beiden Schlüsselworten wird der zugehörige numerische Schlüssel erzeugt. Der erste legt die abschließende Spaltentransposition fest, während der zweite die zyklische Verschiebung der Buchstaben in den einzelnen Zeilen der Tabelle bestimmt. Das in diesem Beispiel verwendete Schlüsselwort `INFO` besitzt den numerischen Schlüssel `2314`. Dies bedeutet, dass die Buchstaben der oberen Zeile um zwei Buchstaben zyklisch nach links verschoben werden und die der zweiten Zeile um drei. Die unteren beiden Zeilen werden dann um einen sowie um vier Buchstaben verschoben.

Z	Y	K	L	I	S	C	H
8	7	4	5	3	6	1	2
D	I	E	S	I	S	T	E
I	N	W	I	C	H	T	I
G	E	R	G	E	H	E	I
M	E	R	T	E	X	T	

Z	Y	K	L	I	S	C	H
8	7	4	5	3	6	1	2
E	S	I	S	T	E	D	I
I	C	H	T	I	I	N	W
E	R	G	E	H	E	I	G
E	X	T	M	E	R	T	

Abschließend müssen die Spalten nur noch in der Reihenfolge des numerischen Schlüssels ausgelesen werden.

Geheimtext	`DNIT IWG TIHE IHGT STEM EIER SCRX EIEE`

1.7 Kryptos ähnliche Chiffre

Diese Verschlüsselung orientiert sich ein wenig an dem geheimen Text im 4. Abschnitt der Kryptos-Skulptur. Diese Skulptur des US-amerikanischen Bildhauers James Sanborn steht auf dem Gelände der Central Intelligence Agency (CIA) in Langley (Virginia, USA) Bei dem hier dargestellten Verfahren handelt es sich um eine Kombination einer polyalphabetischen Verschlüsselung mit anschließender Transposition und wurde 2009 im Magazin der *American*

[6] Rubin [164] S. 85

Cryptogram Association vorgestellt.[7] Beide Verschlüsselungen verwenden dabei das gleiche Schlüsselwort.

Klartext	Dies ist ein ganz geheimer Text
Schlüssel	KRYPTOS

Im ersten Schritt wird eine beliebige polyalphabetische Verschlüsselung durchgeführt, wobei in diesem Beispiel die Vigenère-Tabelle benutzt wird.

Vigenère	NZCHB GLOZL VTBRQ VFTBA WBKCM M

Der sich ergebende Zwischentext wird horizontal in eine Tabelle eingetragen, deren Breite durch die Länge des Schlüsselwortes festgelegt wird. Dabei werden die Spalten mit fortlaufenden Zahlen ab 1 gekennzeichnet. Diese Zahlen werden auch zusätzlich in die Tabelle geschrieben und schließen sich unmittelbar an den erhaltenen Zwischentext an.

1	2	3	4	5	6	7
N	Z	C	H	B	G	L
O	Z	L	V	T	B	R
Q	V	F	T	B	A	W
B	K	C	M	M	1	2
3	4	5	6	7		

Für den Geheimtext wird zunächst die Spalte 7 am rechten Rand der Tabelle vertikal ohne die abschließende Zahl ausgelesen. Danach folgt diejenige Spalte, die durch die nach den Buchstaben folgende Zahl gekennzeichnet ist. Nach Spalte 7 folgt also zunächst Spalte 2 und danach die weiteren Spalten 4, 6, 1, 3 und 5. Damit bei diesem Schema alle Spalten der Tabelle berücksichtigt werden, müssen die Längen des Klartextes und des Schlüsselwortes relativ prim sein, also keinen gemeinsamen Teiler außer 1 besitzen. Sonst werden nicht alle vorhandenen Spalten erfasst.

Geheimtext	LRW ZZVK HVTM GBA NOQB CLFC BTBM

1.8 Schablonen

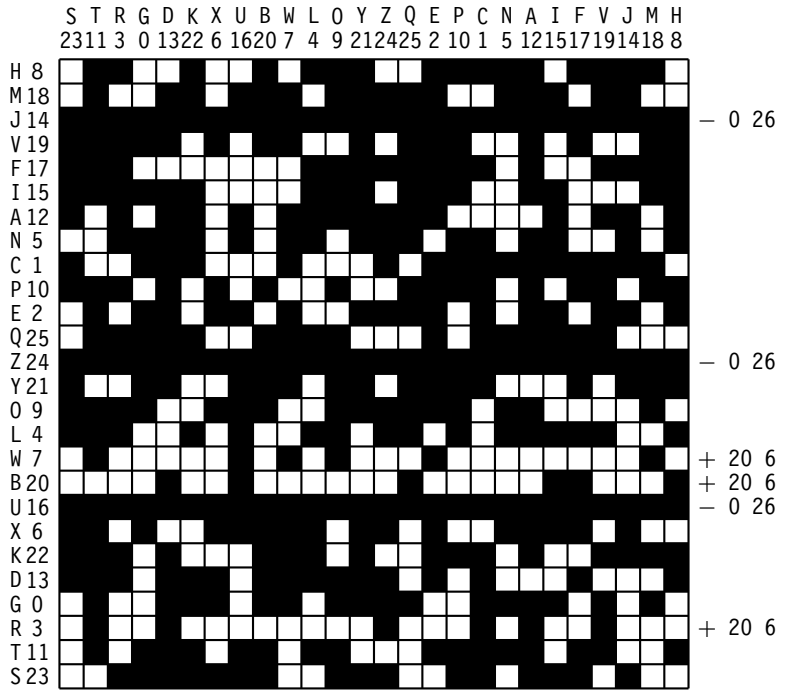
1.8.1 Cysquare

Im Jahr 1941 entwickelte der englische Kryptologe John Tiltman für das britische Kriegsministerium die *Cysquare*-Verschlüsselung. Das Verfahren benutzt ein quadratisches Raster der

[7] Cryptogram [70]

Seitenlänge 26 und die meisten Zeilen enthalten 10 freie Felder für die Buchstaben der zu übermittelnden Nachricht sowie 16 schwarze Felder, die keine Buchstaben aufnehmen können. Ausnahmen bilden drei *Plus*-Zeilen mit jeweils 20 weißen und 6 schwarzen Feldern sowie drei *Minus*-Zeilen, die nur schwarze Felder enthalten.[8]

Der täglich gewechselte Schlüssel besteht aus den 26 Buchstaben des Alphabets in zufälliger Reihenfolge sowie aus den Zahlen von 1 bis 26, die auch beliebig permutiert sind. Die Buchstaben werden oberhalb des Rasters von links nach rechts platziert und darunter die permutierten Zahlen. Zusätzlich werden die Buchstaben und Zahlen noch einmal links vom Raster von unten nach oben notiert.



Für jede Nachricht wird ein Indikator aus vier Buchstaben wie etwa `CABP` ausgewählt. Durch die den Buchstaben zugeordneten Zahlen stehen die Buchstaben für 1, 12, 20 und 10. Die erste Zahl bestimmt die Ausgangsposition des Rasters. Dies kann außer der normalen Lage durch Drehungen um 90°, 180° und um 270° auf vier Arten erreicht werden.

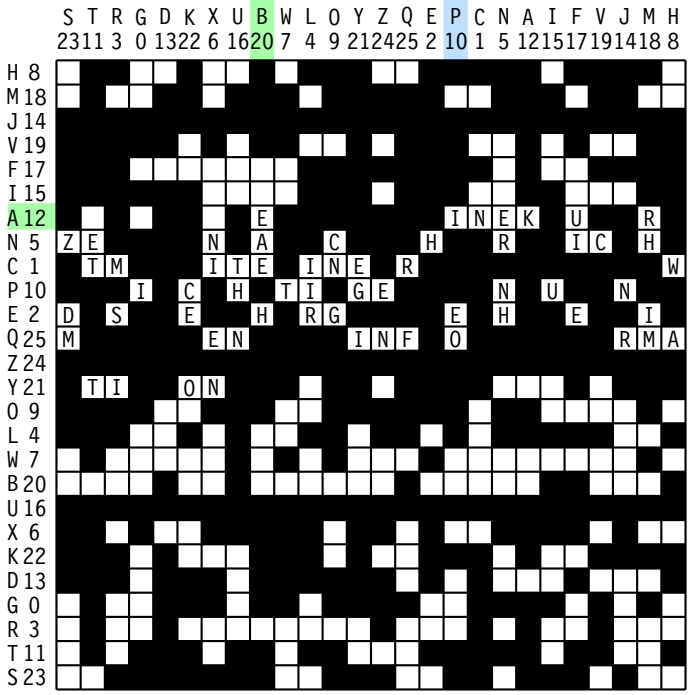
Die nächsten beiden Zahlen 12 und 20 legen die Zeile und die Spalte fest, an der der erste Buchstabe eingetragen werden soll. Handelt es sich um ein schwarzes Feld, beginnt man stattdessen mit dem nächsten freien Feld.

Klartext	`Eine kurze Nachricht mit einer wichtigen und sehr geheimen Information`

Die Buchstaben des Klartextes, werden zeilenweise ab der festgelegten Startposition eingetragen. Hat man das letzte freie Feld in der unteren Zeile erreicht, fährt man mit der oberen

[8] Tiltman [197]

fort. Insgesamt darf die Länge der Nachricht nicht 220 Buchstaben übersteigen, sonst sollte sie in mehrere Nachrichten unterteilt werden.



Das Auslesen des Geheimtextes beginnt mit der Spaltennummer 11, die mit dem Buchstaben P des Indikators festgelegt wurde. Da in der Beschreibung von Tiltman alle Grafiken entfernt worden sind und das Verfahren in keinem anderen Artikel oder Buch detailliert beschrieben wird, bleibt unklar, ob mit dieser Spalte beginnend die zyklisch gesehen nachfolgenden Spalten des Rasters von oben nach unten ausgelesen oder die Spalten mit den nachfolgenden Spaltennummern. In diesem Beispiel ist die erste Variante gewählt worden.

Geheimtext	IEO N ERNH K U UIE C NR RHIM WA ZDM ETT MSI
	I CEO NIEN THN EAEH T IIR CNG EGI EN RF H

Die endgültige Nachricht besteht aus dem Indikator, gefolgt vom Geheimtext, der Anzahl der Buchstaben, dem wiederholten Indikator, der Uhrzeit und dem Datum.

Das Verfahren wurde während des 2. Weltkrieges in Nordafrika eingesetzt. Tiltman schreibt allerdings später, dass sich dieses Verfahren ein ziemlicher Fehlschlag erwiesen hat, weil es nicht leicht umsetzbar war und die gesendeten Nachrichten zu viele Fehler enthielten.

1.8.2 Rasterschlüssel 44

Diese Verschlüsselung wurde im März 1944 von der deutschen Wehrmacht als Nachfolger des Doppelkastenschlüssels eingeführt.[9] Sie basiert auf der englischen *Cysquare*-Chiffre, deren

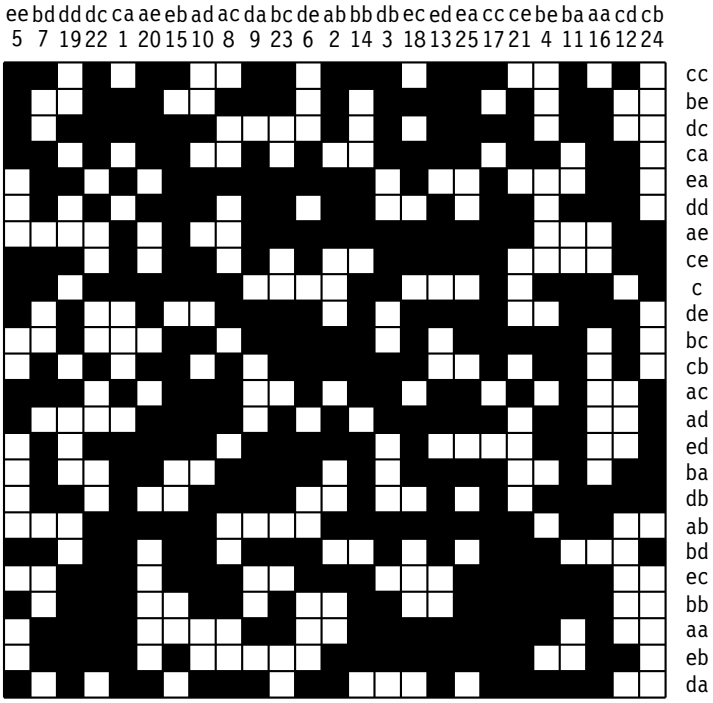
[9] Cryptologia [49], Schmeh [174] S. 62-66, 68-70, Rijmenants [161], Weierud [211]

Unterlagen während des Afrikafeldzugs erbeutet wurden.

Klartext	Eine kurze Nachricht mit einer wichtigen und sehr geheimen Information

Die Basis der Verschlüsselung eines Klartextes bildet eine Rasterschablone mit 24 Zeilen und 25 Spalten. In jeder Zeile befanden sich 10 weiße Felder für die Buchstaben und 15 schwarz gefärbte Felder. Die Anordnung der Felder war zufällig und die Rasterschablone wurde täglich gewechselt.

Oberhalb des Rasters befand sich eine Kopfzeile mit 25 Buchstabenpaaren von `aa` bis `ee`, die mit den Buchstaben `a`, `b`, `c`, `d` und `e` gebildet waren. Unter diesen Buchstaben waren die Zahlen von 1 bis 25 angeordnet. Eine weitere Anordnung von 24 der 25 Buchstabenpaare befand sich zusätzlich rechts vom Raster. Alle drei Anordnungen waren zufällig und wurden ebenfalls täglich gewechselt.



Zu Beginn der Nachricht werden die Uhrzeit und die Länge der eigentlichen Nachricht notiert. Danach folgt der Indikator, der das Feld für den ersten Buchstaben der eigentlichen Nachricht als Schnittpunkt einer Spalte und einer Zeile festlegt. Diese wird durch zwei Buchstabenpaare festgelegt, von denen das erste Paar die Spalte und das zweite die Zeile kennzeichnet.

Allerdings werden diese vier Buchstaben zuvor zusätzlich mithilfe einer Buchstabenumwandlungstabelle verändert. Dabei werden die Buchstaben `a`, `b`, `c`, `d` und `e` durch einen zufällig ausgewählten Buchstaben aus der zugehörigen Spalte dieser Tabelle ersetzt. Alle vier Buchstaben

sollten nach der Umwandlung voneinander unterschiedlich sein.

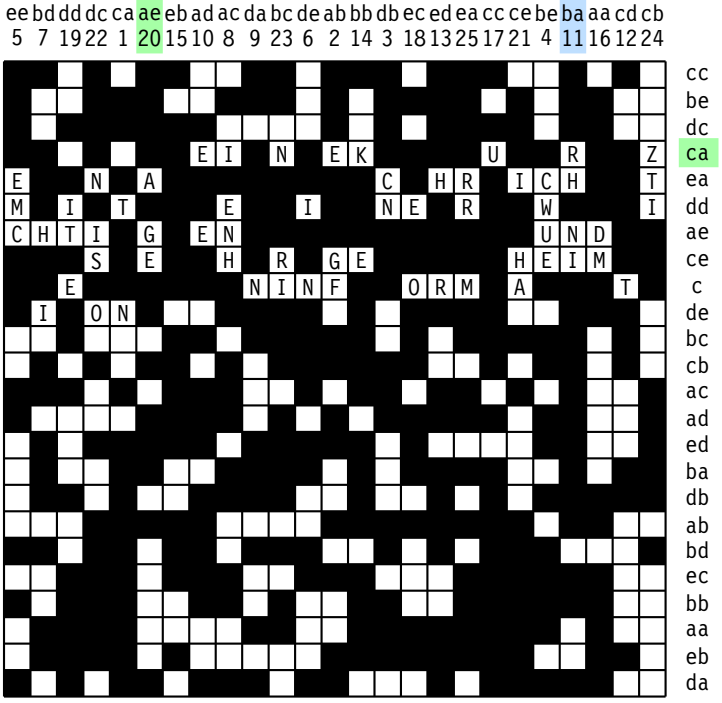
a	b	c	d	e
t	d	n	e	k
r	s	l	w	b
g	v	o	z	x
u	c	i	a	q
m	p	f	h	y

Tab. 1.1: Umwandlungstabelle für die Kennzeichnung der Spalten und Zeilen

In dem dargestellten Beispiel werden die die sechste Spalte und die vierte Zeile ausgewählt. Mit den zugehörigen Buchstabenpaaren `ae` und `ca` erhält man mit der Umwandlungstabelle etwa den Indikator `mxor`, sodass der Nachrichtenkopf beispielsweise folgendermaßen aussah:

```
13.27 61 mxor
```

Die Nachricht wurde zeilenweise von links nach rechts ab einer festgelegten Startposition eingetragen. Handelt es sich dabei, wie in diesem Beispiel, um ein schwarzes Feld, beginnt man stattdessen mit dem nächsten freien Feld in dieser Zeile. Hat man das letzte freie Feld in der unteren Zeile erreicht, fährt man mit der oberen fort. Insgesamt sollte die Länge der Nachricht zwischen 60 und 200 Buchstaben liegen.



Der Geheimtext wird spaltenweise aus der Tabelle ausgelesen. Dabei beginnt man aber nicht am linken Rand, sondern mit einer besonderen Spalte. Um diese zu bestimmen, werden die

Ziffern der Minuten aus der zu übermittelnden Uhrzeit und der Länge der eigentlichen Nachricht addiert.

$$2 + 7 + 6 + 1 = 16$$

Von der im Indikator angegebenen Startspalte `ae` zählt man nun zyklisch gesehen 16 Spalten weiter nach rechts und erhält die erste Spalte `ba` für den auszulesenden Geheimtext. Da diese Spalte mit dem Code 11 gekennzeichnet ist, werden die Spalten in der Reihenfolge der Nummern 11, 12, 13, ... ausgelesen.

Ab Oktober 1944 wurde ein neues, einfacheres Verfahren zur Bestimmung der Startspalte eingeführt. Nun konnte die Startspalte direkt und zufällig ausgewählt werden, musste allerdings nach dem Indikator im Nachrichtenkopf mit übermittelt werden. Da die Spalte mit der Kennnummer 11 den Code `ba` besitzt, konnte dieser mit der Umwandlungstabelle etwa mit `sm` gekennzeichnet werden. Damit lautet der Nachrichtenkopf

```
13.27 61 mxor sm
```

und der Geheimtext kann spaltenweise ausgelesen werden.

```
11   12 13 14  15 16 17 18 19  20  21  22   23
RHNI T  HR KE     DM U  EO ITE AGE IHA NISO NRI

24  25  1  2   3  4    5   6  7  8    9 10
ZTI RRM TN EGF CN CWUE EMC IN HI IENH N EE
```

Da der Geheimtext immer in Gruppen mit jeweils fünf Buchstaben übermittelt wurde, lautet die gesamte Nachricht dann

```
13.27 61 mxor sm
RHNIT HRKED MUEOI TEAGE IHANI SONRI ZTIRR
MTNEG FCNCW UEEMC INHII ENHNE E
```

Die Verschlüsselung gestaltete sich aber noch komplizierter, als sie bisher dargestellt worden ist. So wurden etwa sämtliche Ortsnamen zusätzlich verschlüsselt, wobei jedem Klartextbuchstaben ein fester Geheimtextbuchstabe zugeordnet war. Diese beiden Tabellen wurden jeden Monat geändert.

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

Abb. 1.10: Umwandlungstabelle für Ortsnamen

Außerdem wurde der Ortsname durch die Buchstabenpaare `aa` und `ee` umklammert. So wird `Berlin` mit `aa uxvqtg ee` verschlüsselt.

Auch Satzzeichen wurden ganz speziell notiert, etwa

Punkt	`stop`
Komma	`koma`
Fragezeichen	`frag`

Zahlen wurden bis auf einige Ausnahmen ziffernweise in Worten ausgedrückt.

12	`eins zwo`	10	`zehn`
211	`zwo eins eins`	11	`elf`
320	`drei zwei null`	20	`zwanzig`
450	`vier fuenf null`	30	`dreiszig`

In der Schlüsselanleitung zum Rasterschlüssel 44 sind viele weitere spezielle Regeln aufgeführt.

1.8.3 Rubin - geometrische Muster

Geometrisch strukturierte Schablonen wurden zu allen Zeiten verwendet, um die Buchstaben eines Klartextes umzuordnen. Neben den bekannten Beispielen wie etwa der Fleißner-Schablone oder des Rasterschlüssels, kann man auch mit einfachen Mitteln eigene Schablonen konstruieren.[10]

Klartext	`Dies ist ein sehr geheimer Text`
Schlüssel	`1/13`

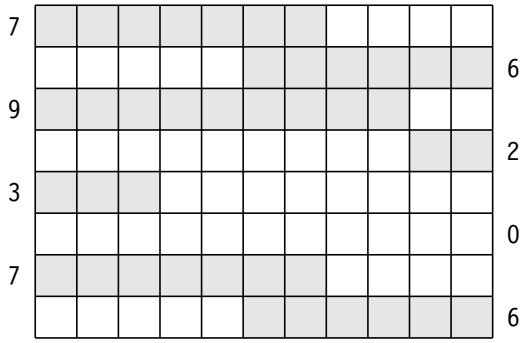
Ein unregelmäßiges und dennoch leicht zu merkendes Muster erhält man mit den Dezimalziffern von Brüchen, die wie etwa $\frac{1}{7}, \frac{1}{13}, \frac{1}{17}, \frac{1}{19}, \ldots$ lange Perioden aufweisen. Bei dem hier gewählten Schlüssel

$$\frac{1}{13} = 0{,}076923076923076923\ldots$$

benutzt man die Dezimalziffern ab der ersten von 0 unterschiedlichen Ziffer 7. Man wählt eine Tabelle mit der Mindestbreite 10, die genug Platz für alle Buchstaben des Klartextes sowie zusätzliche Markierungen bietet. Die Dezimalziffern geben der Reihe nach für jede Zeile von oben nach unten die Anzahl der Markierungen an, die zeilenweise abwechselnd am linken und rechten Rand der Tabelle eingefügt werden. Mit der ersten Ziffer 7 werden damit sieben Markierungen am linken Rand platziert, gefolgt von sechs Markierungen am rechten Rand.

[10] Rubin [164] S. 83

Bei der Ziffer 0 werden dementsprechend keine Markierungen eingefügt und die ganze Zeile steht für Buchstaben zur Verfügung.



Damit zum Abschluss in der unteren Zeile keine freien Zellen entstehen, wird an die bereits markierten Randzellen eine weitere Markierung hinzugefügt. Prinzipiell kann diese Zelle auch frei bleiben, allerdings gestaltet sich die Entschlüsselung dann etwas schwieriger.

Dann kann der gesamte Klartext zeilenweise in die Tabelle eingefügt werden, die nun vollständig mit Buchstaben und Markierungen gefüllt ist.

							D	I	E	S
I	S	T	E	I						
									N	G
E	H	E	I	M	E	R	T	E		
			X	T	M	I	T	W	I	C
H	T	I	G	E	N	I	N	F	O	R
							M	A	T	I
O	N	E	N							

Nach diesen Schritten wird der Geheimtext spaltenweise ausgelesen.

Geheimtext	IEHO SHTN TEIE EIXGN IMTE EMN RII DTTNM IEWFA ENIOT SGCRI

Variante

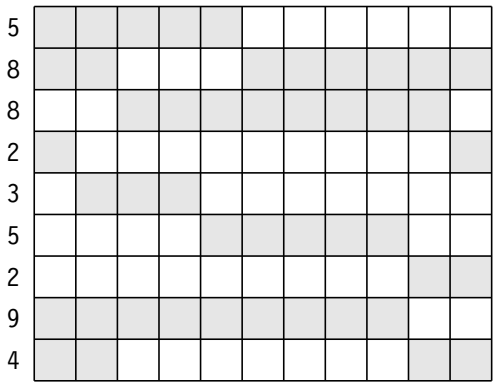
In dieser Variante werden die Markierungen nicht an den beiden Rändern, sondern unregelmäßiger angeordnet.

Klartext	Dies ist ein sehr geheimer Text
Schlüssel	1/17

Als Schlüssel werden die Dezimalstellen des Bruches $\frac{1}{17}$ ohne die erste Ziffer 0 benutzt.

$$\frac{1}{17} = 0{,}0588235294117647\ldots$$

Auch hier muss eine Tabelle mit der Mindestbreite 10 gewählt werden, die genug Platz für alle Buchstaben des Klartextes sowie die zusätzlichen Markierungen bietet. Die Dezimalziffern geben die Anzahl der Markierungen an, die der Reihe nach von oben nach unten eingefügt werden. Dabei wird die erste Markierung immer in der rechten Nachbarspalte der zuletzt in der vorherigen Zeile eingefügten Markierung platziert, sodass ein unregelmäßiges Treppenmuster entsteht. Dabei werden die Markierungen zyklisch angeordnet und nach einer Markierung am rechten Rand wird die nachfolgende Markierung am linken Rand notiert.



Wie bei der Hauptvariante schließen sich in der unteren Zeile sechs weitere Markierungen an, damit keine leeren Zellen entstehen und die Entschlüsselung somit einfacher wird.

Nach diesen Vorbereitungen wird der Klartext zeilenweise in die freien Zellen der Tabelle geschrieben.

					D	I	E	S	I	S
		T	E	I						
N	G									E
	H	E	I	M	E	R	T	E	X	
T				M	I	T	W	I	C	H
T	I	G	E						N	I
N	F	O	R	M	A	T	I	O		
									N	E
								N		

Abschließend kann der Geheimtext spaltenweise ausgelesen werden.

Geheimtext	NTTN GHIF TEGO EIER IMMM DEIA IRTT ETWI SEION IXCNN SEHIE

1.9 Skipping Tramp

Die Abzählmethode des *Skipping Tramp* kann auch zur Erstellung eines gemischten Alphabets und dann mit anderen Verschlüsselungsverfahren verwendet werden.[11]

Klartext	Dies ist ein geheimer Text
Schlüssel	2143

Als Schlüssel wird in diesem Beispiel die periodische Schrittfolge (2,1,4,3 verwendet. Im ersten Schritt werden mit der Schrittlänge 2 die ersten beiden Buchstaben des Klartextes übersprungen und der nachfolgende Buchstabe E markiert, der gleichzeitig den ersten Buchstaben des Geheimtextes bildet. Von der aktuellen Position ausgehend, wird im zweiten Schritt nur ein Buchstabe übersprungen und I markiert und an den bisherigen Geheimtext angehängt. Mit der nächsten Zahl 4 der Schrittfolge folgt der Buchstabe N und danach mit 3, 2 und 1 die weiteren Buchstaben E, E und T, die wie üblich markiert werden.

Da nach diesem Schritt wieder vier Positionen übersprungen werden müssen, landet man zyklisch gesehen beim Buchstabe I. Mit der nächsten Schrittweite 3 landet man beim Buchstaben E, da die bereits markierten Buchstaben nicht mitgezählt werden, .

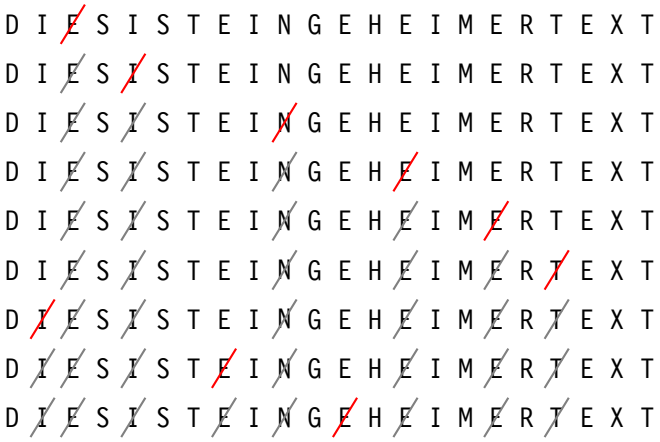


Abb. 1.11: Die ersten neun Buchstaben bei der Abzählmethode

Führt man dieses Verfahren für alle Buchstaben des Klartextes durch, erhält man den Geheimtext.

Geheimtext	EINEE TIEEI TTHRS ESGMX DI

[11] Cryptogram [195]

1.10 Penney Tramp

Der amerikanische Mathematiker Walter Penney veröffentlichte 1978 eine einfache Verschlüsselungsmethode in Kombination mit einem zugehörigen Rätsel.[12]

Klartext	Eine sehr wichtige Nachricht
Schlüssel	35142 24153

Der Klartext besteht aus exakt 25 Buchstaben, die horizontal in eine 5 x 5 - Tabelle eingetragen werden. Die beiden Ziffernfolgen geben die Kennnummern der Zeilen und Spalten an.

	2	4	1	5	3
3	E	I	N	E	S
5	E	H	R	W	I
1	C	H	T	I	G
4	E	N	A	C	H
2	R	I	C	H	T

Anschließend wird die Tabelle in der folgender Reihenfolge ausgelesen:

(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,1)	(3,1)	(4,1)	(5,1)
(2,2)	(2,3)	(2,4)	(2,5)	(3,2)	(4,2)	(5,2)		
(3,3)	(3,4)	(3,5)	(4,3)	(5,3)				
(4,4)	(4,5)	(5,4)						
(5,5)								

Mit dieser Reihenfolge ergibt sich folgende Buchstabenfolge:

11	12	13	14	15	21	31	41	51	22	23	24	25	32	42	52	33	34	35	43	53	44	45	54	55
T	C	G	H	I	C	N	A	R	R	T	I	H	E	E	E	S	I	E	H	I	N	C	H	W

Gruppiert man abschließend diese Buchstabenfolge in Gruppen von jeweils fünf Buchstaben, erhält man den Geheimtext.

Geheimtext	TCGHI CNARR TIHEE ESIEH INCHW

Dieses Verfahren bietet einige Möglichkeiten zur Abwandlung. Zunächst einmal können die Kennzahlen der Zeilen und Spalten beliebig permutiert werden. Zudem können die Tabellen auch andere Größen annehmen, damit der Klartext nicht unbedingt immer 25 Buchstaben umfassen muss.

[12] Cryptologia [185], Cryptogram [193], Cryptogram [186]

2 Substitution

2.1 Mühlebrett

Ein ausgefallenes Verfahren verschlüsselt einen Klartext mithilfe eines Mühlebrettes. Das zu benutzende Alphabet enthält 24 Buchstaben, sodass etwa `J` durch `I` und `Y` durch `X` ersetzt werden müssen. Die Buchstaben des Klartextes werden mit einem festgelegten Schlüssel auf einem Mühlebrett angeordnet. Dabei sind die 24 Positionen wie in Abbildung 2.1 durch 20 Linien verbunden, die jeweils drei Positionen miteinander verbinden.[13]

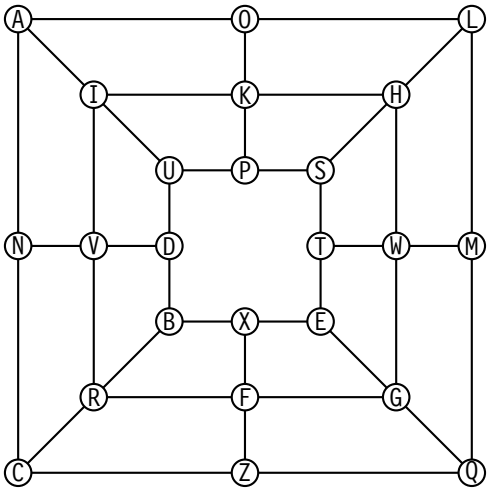


Abb. 2.1: Mit Buchstaben gefülltes Mühlebrett

Für die Verschlüsselung gelten folgende Regeln:

1. Befindet sich ein Klartextbuchstabe am Rand einer der 20 Linien, wird er durch die anderen beiden auf dieser Linie enthaltenen Buchstaben verschlüsselt. Die beiden Buchstaben müssen allerdings in der Reihenfolge angegeben werden, dass der Klartextbuchstabe in der durch die beiden Buchstaben festgelegten Richtung liegt.

   Der Buchstabe `L` in der rechten oberen Ecke wird also durch `AO` verschlüsselt und `A` in der linken oberen Ecke durch `LO`. Ungültig ist dagegen die Verschlüsselung von `A` durch `OL`, da sich dieser Buchstabe nicht als Endpunkt auf der Linie befindet, wenn man sich vom ersten angegebenen Buchstaben `O` zum zweiten Buchstaben `L` bewegt.

   Insgesamt kann der Buchstabe `A` in der linken oberen Ecke damit durch drei mögliche Buchstabenpaare verschlüsselt werden.

   ```
   LO  → A
   UI  → A
   CN  → A
   ```

[13] Türkel [204] S. 34 – 39

2. Liegt dagegen ein Klartextbuchstabe in der Mitte einer Linie, wird er durch die beiden anderen auf dieser Linie liegenden Buchstaben verschlüsselt. Dabei spielt die Reihenfolge dieser beiden Buchstaben keine Rolle. So kann der Buchstabe `Z` in der unteren Linie durch `CQ` und `QC` verschlüsselt werden. Nach Regel 1 existiert mit `XF` sogar noch eine dritte Möglichkeit der Verschlüsselung.

Nach Regel 2 existieren für einige Buchstaben, die sich in der Mitte von zwei Linien befinden, sogar vier Möglichkeiten. Dieser Fall tritt etwa bei dem Buchstaben `V` auf der linken Seite auf,

```
ND → V
DN → V
IR → V
RI → V
```

Es kann aber auch zu vier Möglichkeiten der Verschlüsselung eines Klartextbuchstaben kommen, wenn sich dieser in der Mitte einer Linie und am Rand von zwei anderen Linien befindet. Dies trifft etwa auf den Buchstaben `H` zu, der sich rechts oben auf dem Mühlebrett befindet und bei dem beide Regeln angewendet werden können.

```
SL → H
LS → H
IK → H
GW → H
```

Soll etwa der nachfolgende Klartext verschlüsselt werden,

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`AOLIKHUPSNVDTWMBXERFGCZQ 4`

ergeben sich mit dem Mühlebrett aus Abbildung 2.1 beispielsweise folgende Zuordnungen, die jeweils zufällig aus den zur Verfügung stehenden Möglichkeiten ausgewählt wurden.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
BU	KH	TS	ET		UA	UP	WM		XB	KH	VD		FR	TS	SL	XB	VR	LQ	QG	FG		SE	TS	BE	WM

Dieses Zwischenergebnis wird zusätzlich fragmentiert, indem der gesamte Text in vier oder sechs gleich lange Zeilen unterteilt wird, was durch einen zweiten Schlüssel festgelegt wird. Die erhaltenen Buchstabenpaare werden jeweils so lange untereinander platziert, bis die berechnete Zeilenlänge erreicht ist. Danach fährt man mit zwei neuen Zeilen fort.

In diesem Beispiel umfasst der Zwischentext 44 Buchstaben, sodass eine Aufteilung der Buch-

stabenpaare in vier Zeilen mit jeweils elf Buchstaben vorgenommen werden kann.

```
B K T E U U W X K V F
U H S T A P M B H D R
T S X V L Q F S T B W
S L B R Q G G E S E M
```

Den Geheimtext erhält man abschließend, indem man die Buchstaben der Zeilen von oben nach unten hintereinander notiert und in Gruppen mit jeweils fünf Buchstaben aufgeteilt wird.

Geheimtext	BKTEU UWXKV FUHST APMBH DRTSX VLQFS TBWSL BRQGG ESEM

Um die Zeilen alle gleich lang zu gestalten oder eine unbefugte Entschlüsselung zu erschweren, können an beliebigen Stellen des Zwischentextes Blender eingefügt werden. Hierunter versteht man Buchstabenpaare, die keine Buchstaben nach den beiden Regeln verschlüsseln. Sie werden vom richtigen Empfänger beim Entschlüsseln erkannt und übergangen.

Es ist auch denkbar, bestimmte Buchstabenpaare als Markierung für ein Zeilenende zu bestimmen, sodass auf den zweiten Schlüssel verzichtet werden kann.

2.2 Richelieu

Diese Transposition ist eine von vielen Verschlüsselungsmethoden, die Kardinal Richelieu (1585 - 1642) in seiner Zeit als *Erster Minister* (manchmal auch Premierminister genannt) unter König Ludwig XIII. benutzte.[14] Richelieu benutzt einen Schlüsselsatz, der periodisch verlängert werden kann, damit er genauso viele Buchstaben wie der Klartext enthält. Ist er dagegen länger als der Klartext, muss er entsprechend verkürzt werden.

Klartext	Dies ist ein geheimer Text
Schlüssel	Methode von Richelieu

Der Schlüsselsatz muss Leerzeichen enthalten, an denen er in einzelne Worte zerlegt werden kann. Für jedes einzelne Wort wird ein numerischer Schlüssel erstellt.

```
Methode von Richelieu Met
1375624 321 162538749 123
```

[14] Cryptogram [179], D'Agapeyeff [52] S. 43-44, Bei D'Agapeyeff findet sich aber auf Seite 44 ein Fehler bei der letzten Gruppe.

Im ersten numerischen Schlüssel 1375624 treten sieben Codes auf, sodass die ersten sieben Buchstaben des Klartextes abgetrennt werden und ihnen die entsprechenden Zahlen des numerischen Schlüssels zugeordnet werden. Ebenso verfährt man mit den weiteren numerischen Schlüsseln.

Diesist ein geheimerT ext
1375624 321 162538749 123

Für den Geheimtext werden die Zahlen der einzelnen Ziffernfolgen immer aufsteigend ab 1 angeordnet und darunter die zugehörigen Buchstaben notiert.

1234567 123 123456789 123
DSITSIE NIE GHIREEEMT EXT

Abschließend wird der Geheimtext nur noch wie üblich in Gruppen von jeweils fünf Buchstaben aufgeteilt.

Geheimtext	DSITS IENIE GHIRE EEMTE XT

Variante

Richelieu verwendete auch viele Varianten seiner Zahlenchiffre. Lange und Soudart beschreiben, dass Richelieu bei der *Versetzungsmethode* den Schlüssel 54321 benutzte. Die Ziffern können aber auch umgestellt oder ein anderer Schlüssel mit fortlaufenden Ziffern ab 1 gewählt werden.[15]

Klartext	Dies ist ein sehr geheimer Text
Schlüssel	53241

Der Klartext wird in Blöcke mit wachsenden Längen unterteilt, wobei die Länge des ersten Blocks genau der Schlüssellänge entsprechen muss. Den Buchstaben dieses Blocks werden die Ziffern des Schlüssels zugeordnet. Die nachfolgenden Blöcke sind jeweils um einen Buchstaben länger. Ihnen werden jeweils zunächst die Schlüsselziffern zugeordnet und den verbliebenen Buchstaben die nachfolgenden Ziffern in absteigender Reihenfolge.

DIESI STEINS EHRGEHE IMERTEXT
53241 532416 5324176 53241876

[15] Lange - Soudart [122] S. 139-140

Für den verschlüsselten Geheimtext werden die Buchstaben so umgeordnet, dass die ihnen zugeordneten Zahlen in aufsteigender Reihenfolge auftreten.

sortiert	12345 123456 1234567 12345678
Geheimtext	IEISD NETISS ERHGEEH TEMRITXE

Abb. 2.2: Verschlüsselung mit der Versetzungsmethode von *Richelieu*

2.3 Mirabeau

Der Comte de Mirabeau (1749 - 1791) war ein französischer Politiker, Physiokrat, Schriftsteller und Publizist in der Zeit der Französischen Revolution. Während eines Aufenthaltes im Gefängnis hat er ein sehr einfaches Verfahren entwickelt, um seine Botschaften an den Hof von König Ludwig XVI. zu schicken.[16]

Mirabeau benutzte ein Alphabet mit 25 Buchstaben ohne J und unterteilte dieses in fünf Gruppen. Dabei erhält jede Gruppe eine Kennzahl.

1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
I S U W B	K T D Q R	X L P A E	G O Y V F	Z M C H N
6	8	4	7	5

Ein Text wird verschlüsselt, indem jeder Buchstabe durch die Kennzahl der zugehörigen Gruppe und die Position innerhalb dieser Gruppe gekennzeichnet wird. Die einzelnen Buchstaben werden durch einen Punkt getrennt und Leerzeichen innerhalb der Nachricht bleiben erhalten.

Der Buchstabe D befindet sich beispielsweise an der Position 3 in der Buchstabengruppe mit der Kennzahl 8. Damit wird dieser Buchstabe als 83 codiert. Insgesamt ergibt sich der verschlüsselte Geheimtext, der sich deutlich von üblichen Schreibweisen unterscheidet.

D i e s	i s t	e i n	g e h e i m e r	T e x t
83.61.45.62	61.62.82	45.61.55	71.45.54.45.61.52.45.85	82.45.41.82

Varianten

Im Laufe der Zeit änderte Mirabeau sein Verfahren mehrfach, indem er beispielsweise die Positionsnummern innerhalb der Gruppen umdrehte oder den Gruppen andere Kennzahlen zuordnete. Man kann auch die Punkte und Zwischenräume vernachlässigen, damit sich der Geheimtext auf den ersten Blick nicht von Ergebnissen anderer Verfahren unterscheidet, die auch auf Ziffernfolgen basieren.

16 Nichols [149] S. 14 – 15 (Lesson 2), Schneickert [175] S. 45 – 46, Figl [77] S. 67 – 68,

Auch die Ausgabe des Geheimtextes wechselte er häufig. Während im dargestellten Beispiel die Zahlen durch einen Punkt getrennt werden, gab Mirabeau sie auch als Zähler und Nenner eines Bruches aus.

$$\frac{8}{3}\ \frac{6}{1}\ \frac{4}{5}\ \frac{6}{2}\quad \frac{6}{1}\ \frac{6}{2}\ \frac{8}{2}\quad \frac{4}{5}\ \frac{6}{1}\ \frac{5}{5}\quad \frac{7}{1}\ \frac{4}{5}\ \frac{5}{4}\ \frac{4}{5}\ \frac{6}{1}\ \frac{5}{2}\ \frac{4}{5}\ \frac{8}{5}\quad \frac{8}{2}\ \frac{4}{5}\ \frac{4}{1}\ \frac{8}{2}$$

Zusätzlich fügte er auch an beliebigen Stellen Blender ein, da die Ziffern 6, 7, 8, 9 und 0 bei der Verschlüsselung nicht auftreten konnten. So kann man den Bruch $\frac{1}{2}$ auf unterschiedliche Arten schreiben.

$$\frac{1}{2} \equiv \frac{1}{62} \equiv \frac{71}{2} \equiv \frac{810}{929}$$

Diese Verschlüsselung lässt sehr viele Variationen zu. Anstatt die Zahlen durch Punkte zu trennen, können stattdessen auch Leerzeichen oder beliebige andere Zeichen verwendet werden. Diese unterschiedlichen Trennzeichen können auch gleichzeitig innerhalb eines Geheimtextes verwendet werden.

2.4 Nummerierter Schlüssel

Bei der *Numbered Key*-Chiffre handelt es sich um eine homophone Verschlüsselung, für die zwei Schlüssel benötigt werden.[17]

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`SCHLUESSEL 13`

Mit dem ersten Schlüssel wird zunächst ein gemischtes Klartextalphabet erstellt. Im Unterschied zu vielen anderen Verfahren, werden doppelt vorkommende Buchstaben nicht entfernt. An diesen Schlüssel werden dann alle Buchstaben des Alphabets, die nicht bereits im Schlüssel vorhanden sind, in ihrer normalen Reihenfolge angehängt. Damit die Reihenfolge der Buchstaben nicht so leicht zu erraten ist, werden sie zyklisch um die Anzahl von Positionen nach links verschoben, die als zweiter Schlüssel festgelegt ist. In diesem Beispiel beträgt die Verschiebung 13.

Schlüsselsatz	`SCHLUESSELABDFGIJKMNOPQRTVWXYZ`
verschoben	`FGIJKMNOPQRTVWXYZSCHLUESSELABD`

Nach der Verschiebung werden den Buchstaben natürliche Zahlen einschließlich der Zahl 0 als Codes zugeordnet, wobei den Zahlen kleiner als 10 eine führende Null vorangestellt wird.

F	G	I	J	K	M	N	O	P	Q	R	T	V	W	X	Y	Z	S	C	H	L	U	E	S	S	E	L	A	B	D
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

[17] Cryptogram [15]

Je nach Wahl des Schlüsselwortes werden einzelnen Buchstaben auch mehrere Codes zugeordnet. In diesem Beispiel betrifft das den Buchstaben E mit den Codes 22 und 25, L mit den Codes 20 und 26 sowie den Buchstaben S, dem sogar die drei Codes 17, 23 und 24 zugeordnet werden.

Der Geheimtext lässt sich nun leicht erstellen, indem zu jedem Klartextbuchstaben der zugeordnete Code notiert wird. Stehen sogar mehrere Codes zur Auswahl, wird aus ihnen einer zufällig ausgewählt.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
29	02	22	24		02	23	11		22	02	06		01	25	19	22	02	05	22	10		11	25	14	11

Damit lautet der Geheimtext

Geheimtext	29022	51702	24112	50206	01221	92202	05221	01125	1411

Es ist klar, dass die Stärke dieser Verschlüsselung entscheidend von der Länge des Schlüssels abhängt, damit die Zuordnungen nicht mehr so leicht zu rekonstruieren sind. Daher ist zu empfehlen, nicht nur ein einzelnes Wort als Schlüssel zu wählen, sondern einen ganzen Satz.

2.5 Vimark

Die *Vimark*-Chiffre ähnelt der *Gromark*-Chiffre und stellt gleichzeitig eine Erweiterung der Verschlüsselungsmethode von Gronsfeld dar.[18] Wie bei der *Gromark*-Chiffre wird ein gemischtes Schlüsselalphabet sowie ein fortlaufender Schlüssel benutzt, dessen Anzahl an Zahlen sich nach der Länge des Klartextes richtet.

Klartext	Dies ist ein geheimer Text
Schlüsselalphabet	RMOWPZQTVYEGLCHUBNAKFSDJXI
fortlaufender Schlüssel	6,10,9,19,13,...

Während die Chiffre von Gronsfeld nur zehn Schlüsselzeilen verwendet, werden bei diesem Verfahren 26 Zeilen benutzt. Sie entstehen aus dem vorgegebenen Schlüsselalphabet durch

[18] Cryptogram [202]

zyklische Verschiebungen um jeweils eine Position nach links. Damit entsteht eine Vigenère-Tabelle, die zur Ver- und Entschlüsselung benutzt wird.

Klartext

Schlüssel	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
0	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I
1	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R
2	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M
3	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O
4	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W
5	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P
6	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z
7	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q
8	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T
9	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V
10	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y
11	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E
12	L	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G
13	C	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L
14	H	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C
15	U	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H
16	B	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U
17	N	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B
18	A	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N
19	K	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A
20	F	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K
21	S	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F
22	D	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S
23	J	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D
24	X	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J
25	I	R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X

Tab. 2.1: Tabelle für Vimark

Der erste Klartextbuchstabe D wird in der Kopfzeile der Tabelle gesucht und legt die zu benutzende Spalte fest. Die Schlüsselzeile ergibt sich aus der ersten Zahl 6 des fortlaufenden Schlüssels. Der Schnittpunkt der so festgelegten Spalte und Zeile liefert den ersten Geheimtextbuchstaben Y.

Alternativ kann man auch auf diese Tabelle verzichten und schreibt zunächst den Klartext und die Zahlen des fortlaufenden Schlüssels untereinander. Für die Bestimmung der Geheimtextbuchstaben platziert man zusätzlich noch darunter das normale Alphabet sowie das Schlüsselalphabet.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
6	10	9	19	1	3	16	19	2	6	3	9	21	8	9	12	4	3	17	2	11	6	7	20

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
R	M	O	W	P	Z	Q	T	V	Y	E	G	L	C	H	U	B	N	A	K	F	S	D	J	X	I

Für den zweiten Klartextbuchstaben I ergibt sich mit der zugehörigen Zahl 10 des fortlaufenden Schlüssels der Geheimtextbuchstabe A, der sich im Schnittpunkt der zugehörigen Spalte sowie der Schlüsselzeile befindet. Bei der alternativen Darstellung findet man den Geheimtextbuchstaben 10 Positionen weiter rechts vom Buchstaben V in der vierten Zeile.

```
D I E S I S T E I N G E H E I M E R T E X T
6 10 9 19 13 16 19 2 6 3 9 21 8 9 12 4 3 17 21 16 7 20

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
R M O W P Z Q T V Y E G L C H U B N A K F S D J X I
```

Beim vierten Buchstaben S ergibt sich eine kleine Besonderheit. Man sucht diesen im Klartextalphabet der dritten Zeile und wechselt zu dem darunterliegenden Buchstaben des Schlüsselalphabets. Von dessen Position aus bewegt man sich wegen der aktuellen Schlüsselzahl um 19 Positionen nach rechts, wobei der rechte Rand überschritten und am linken Rand weitergezählt wird. Damit ergibt sich der zugehörige Geheimtextbuchstabe G.

```
D I E S I S T E I N G E H E I M E R T E X T
6 10 9 19 13 16 19 2 6 3 9 21 8 9 12 4 3 17 21 16 7 20

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
R M O W P Z Q T V Y E G L C H U B N A K F S D J X I
```

Führt man dieses Vorgehen mit der Verschlüsselungstabelle oder den alternativen Verschiebungen für alle Klartextbuchstaben durch, erhält man den Geheimtext.

Geheimtext	YSCGF VLQHB UIUCK BTVHK PC

2.6 Phillips-RC

Die *Phillips-RC* Chiffre ist eine Modifikation der normalen Phillips Chiffre.[19] Es wird auch mit acht Quadraten gearbeitet und bis auf eine Änderung unterscheidet sich die Verschlüsselung prinzipiell nicht.

Klartext	Dies ist ein geheimer Text
Schlüssel	PHILLIPSRC

In diesem Beispiel wird aber zusätzlich noch eine weitere Änderung vorgenommen, da das gemischte Alphabet im Ausgangsquadrat immer abwechselnd von links nach rechts und von

19 ACA [5] S. 68

rechts nach links eingetragen wird.

	1	2	3	4	5
1	P	H	I	L	S
2	D	B	A	C	R
3	E	F	G	K	M
4	U	T	Q	O	N
5	V	W	X	Y	Z

Dieser Unterschied besteht darin, dass beim Austausch der Zeilen auch die Spalten vertauscht werden. Wenn also bei den ersten beiden Quadraten die Zeilen 1 und 2 vertauscht werden, dann auch die Spalten 1 und 2. Dieses Prinzip gilt ebenso für die weiteren Quadrate. Vertauscht man zwei Zeilen, müssen auch die entsprechenden Spalten vertauscht werden.

	1	2	3	4	5
1	P	H	I	L	S
2	D	B	A	C	R
3	E	F	G	K	M
4	U	T	Q	O	N
5	V	W	X	Y	Z

a) Quadrat 1

	2	1	3	4	5
2	B	D	A	C	R
1	H	P	I	L	S
3	F	E	G	K	M
4	T	U	Q	O	N
5	W	V	X	Y	Z

b) Quadrat 2

	2	3	1	4	5
2	B	A	D	C	R
3	F	G	E	K	M
1	H	I	P	L	S
4	T	Q	U	O	N
5	W	X	V	Y	Z

c) Quadrat 3

	2	3	4	1	5
2	B	A	C	D	R
3	F	G	K	E	M
4	T	Q	O	U	N
1	H	I	L	P	S
5	W	X	Y	V	Z

d) Quadrat 4

	2	3	4	5	1
2	B	A	C	R	D
3	F	G	K	M	E
4	T	Q	O	N	U
5	W	X	Y	Z	V
1	H	I	L	S	P

e) Quadrat 5

	3	2	4	5	1
3	G	F	K	M	E
2	A	B	C	R	D
4	Q	T	O	N	U
5	X	W	Y	Z	V
1	I	H	L	S	P

f) Quadrat 6

	3	4	2	5	1
3	G	K	F	M	E
4	Q	O	T	N	U
2	A	C	B	R	D
5	X	Y	W	Z	V
1	I	L	H	S	P

g) Quadrat 7

	3	4	5	2	1
3	G	K	M	F	E
4	Q	O	N	T	U
5	X	Y	Z	W	V
2	A	C	R	B	D
1	I	L	S	H	P

h) Quadrat 8

Wie bei der normalen Phillips-Chiffre wird der Klartext in Gruppen mit jeweils fünf Buchstaben unterteilt, die der Reihe nach mit den fortlaufenden Quadraten verschlüsselt werden. Bei

längeren Klartexten fährt man nach dem achten Quadrat wieder mit dem allerersten fort.

	1	2	3	4	5
Klartext	DIESI	STEIN	GEHEI	MERTE	XT
Geheimtext	FCTDC	FVQKW	PLQLU	TNFIN	LX

3 Polyalphabetische Substitution

3.1 Historische Verfahren

3.1.1 Larrabee

Diese Verschlüsselung funktioniert im Wesentlichen wie die Vigenère-Chiffre. Allerdings können bei dieser Chiffre auch Zahlen verschlüsselt werden.[20]

Dazu werden den Zahlen von 1 bis 10 die Buchstaben A bis J zugeordnet. Dabei wird die Zahl 10 durch die Ziffer 0 dargestellt.

Ziffern	1	2	3	4	5	6	7	8	9	0
Codes	A	B	C	D	E	F	G	H	I	J

Bei der Verschlüsselung werden Zahlen durch den Code Q eingeleitet, gefolgt von der durch Buchstaben codierten Anzahl von Ziffern. Danach folgen die codierten Ziffern der Zahl. 2026 wird damit folgendermaßen codiert:

Zahl	2026
Codierung	Q D BJBF

Überschreitet bei einer Zahl die Anzahl der Ziffern den Wert 10, muss diese Zahl in mehreren Abschnitten verschlüsselt werden. Da der Buchstabe Q eine besondere Bedeutung besitzt, darf er natürlich entweder nicht im Klartext auftauchen oder muss besonders verschlüsselt werden, etwa durch QQ.

Klartext	Diese Nachricht mit dem Code 42 ist wichtig
Schlüssel	LARRABEE

Die Zahl 42 wird codiert und in den Klartext eingefügt. Erst danach erfolgt die eigentliche Verschlüsselung mit dem Verfahren von Vigenère.

Klartext	Diese Nachricht mit dem Code QBDB ist wichtig
Geheimtext	OIVJE OEGSR ZTHUQ MEDVD CPHIB BUSIT XATCY KIH

[20] Larrabee [123]

3.1.2 Lovell

James Lovell (1737 - 1814) kann als einer der Begründer der amerikanischen Kryptoanalyse angesehen werden. Eine von ihm Ende des 18. Jahrhunderts verwendete Chiffre stellt eine sehr einfache polyalphabetische Verschlüsselung dar, die als Geheimtext Zahlen statt Buchstaben verwendet.[21]

Klartext	Dies ist ein geheimer Text
Schlüssel	JL

Als Alphabet werden die 26 Buchstaben des lateinischen Alphabets sowie für besondere Zwecke das Sonderzeichen & verwendet. Die ersten beiden Buchstaben eines Schlüsselwortes legen die konkrete Verschlüsselung fest. Dazu werden zwei Alphabete einschließlich des Sonderzeichens zyklisch so verschoben, dass die beiden Schlüsselbuchstaben jeweils am Beginn stehen. Diese beiden Buchstabenfolgen werden untereinander notiert und ihnen jeweils die Zahlen von 1 bis 27 zugeordnet.

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	27
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
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

Für die Verschlüsselung des ersten Klartextbuchstabens D sucht man diesen Buchstaben in der oberen Buchstabenzeile und ordnet ihm die oben stehende Zahl 22 zu. Beim zweiten Buchstaben I wird die untere Zeile für die Verschlüsselung gewählt, sodass diesem Buchstaben die Zahl 25 zugeordnet wird. So fährt man alternierend mit allen Buchstaben des Klartextes fort.

D	I	E	S		I	S	T		E	I	N		G	E	H		E	I	M	E	R		T	E	X	T
22	25	23	8		27	8	11		21	27	3		25	21	26		21	27	2	23	7		11	21	15	9

Es hat sich allerdings herausgestellt, dass der ständige Wechsel der Zeilen sehr fehleranfällig war. Außerdem kam es bei den aufeinanderfolgenden Zahlen häufig zu Mehrdeutigkeiten, da die Zwischenräume nicht immer deutlich zu erkennen waren.

3.1.3 Napoleon

Napoleon Bonaparte (1769 - 1821) verwendete als General der Ersten Französischen Republik und später als Kaiser verschiedene Verfahren zur Verschlüsselung seiner Anweisungen und Berichte.

[21] Tomokiyo [200], Kahn [107] S. 181-186

Eine seiner Verschlüsselungen ist der Tabelle von Porta angepasst, kann aber durch unterschiedliche Anordnungen der Schlüsselbuchstaben am linken oder rechten Rand der Tabelle variiert werden.[22]

Schlüssel 1													Schlüssel 2
AB	A N	B O	C P	D Q	E R	F S	G T	H U	I V	K W	L Y	M Z	YZ
CD	A O	B P	C Q	D R	E S	F T	G U	H V	I W	K Y	L Z	M N	VW
EF	A P	B Q	C R	D S	E T	F U	G V	H W	I Y	K Z	L N	M O	TU
GH	A Q	B R	C S	D T	E U	F V	G W	H Y	I Z	K N	L O	M P	RS
IK	A R	B S	C T	D U	E V	F W	G Y	H Z	I N	K O	L P	M Q	PQ
LM	A S	B T	C U	D V	E W	F Y	G Z	H N	I O	K P	L Q	M R	NO
NO	A T	B U	C V	D W	E Y	F Z	G N	H O	I P	K Q	L R	M S	LM
PQ	A U	B V	C W	D Y	E Z	F N	G O	H P	I Q	K R	L S	M T	IK
RS	A V	B W	C Y	D Z	E N	F O	G P	H Q	I R	K S	L T	M U	GH
TU	A W	B Y	C Z	D N	E O	F P	G Q	H R	I S	K T	L U	M V	EF
VW	A Y	B Z	C N	D O	E P	F Q	G R	H S	I T	K U	L V	M W	CD
YZ	A Z	B N	C O	D P	E Q	F R	G S	H T	I U	K V	L W	M Y	AB

Tab. 3.1: Tabelle von Napoleon

Die Tabelle ordnet den 24 Buchstaben des Alphabets ohne die Buchstaben J und X paarweise jeweils zwei Buchstaben zu. Links und rechts der Tabelle befinden sich die zu benutzenden Schlüsselbuchstaben in auf- oder absteigender Reihenfolge.

Da zwei Anordnungen für die Schlüsselbuchstaben existieren, können diese nach Absprache benutzt werden. Dies kann entweder mit einer Anordnung oder auch mit beiden Anordnungen geschehen, die nach einem festen Schema gewählt werden. Bei dem hier dargestellten Beispiel wurden die Schlüsselbuchstaben am linken Rand verwendet.

Klartext	Dies ist ein geheimer Text
Schlüssel	NAPOLEON

[22] Figl [77] S. 86 – 87, Fleißner [78] S. 17 – 18, British War Office [151] S. 88 – 89

Die Verschlüsselung erfolgt wie bei Porta. Man sucht in den beiden Zeilen des aktuellen Schlüsselbuchstabens den Klartextbuchstaben und wählt den darüber- oder darunterliegenden Buchstaben für den Geheimtext. So ergibt sich bei dem ersten Klartextbuchstaben D und dem zugehörigen Schlüsselbuchstaben N der Geheimtextbuchstabe W.

Klartext	DIES IST EIN GEHEIMER TEXT
Schlüssel	NAPO LEO NNA POLEONNA POLE
Geheimtext	WVZM ODA YPA OYNTPSYE MYME

Dieses Verschlüsselungsprinzip wurde von Napoleon in verschiedenen Varianten benutzt. Dabei können sich sowohl einzelne Buchstaben des Alphabets als auch deren Anordnung ändern. Eine derartige Tabelle ist beispielsweise bei Schneickert dargestellt.[23]

3.1.4 Marie Antoinette

Während der französischen Revolution flüchteten König Ludwig XVI. und seine Frau Marie-Antoinette aus Paris. Sie wurden jedoch gefasst und am 25.07.1791 nach Paris zurückgebracht und dort inhaftiert.

Die Flucht wurde vom schwedischen Grafen Fersen organisiert, der nach der Gefangennahme als Vermittler zwischen dem französischen Königspaar und u.a. dem schwedischen König fungierte. Von den vielen verschlüsselten Briefen zwischen Marie Antoinette und Fersen konnte u.a. ein im französischen Nationalarchiv entdeckter Brief vom 08.07.1791 entschlüsselt werden.[24]

Das Alphabet der Verschlüsselungstabelle 3.2 besteht aus 23 Buchstaben und dem aus der lateinischen Sprache stammenden ET-Zeichen & für *und*. Die Buchstaben I und J sowie U und V wurden als identisch angesehen und der in der französischen Sprache seltene Buchstabe W

[23] Schneickert [175] S. 16 – 17

[24] Tomokiyo [198], Gylden [96], Müller [145] S. 7-6 und 7-7, Nachef - Patarin [147],

fehlt ganz.

A	AB	CD	EF	GH	IK	LM	NO	PQ	RS	TU	XY	Z&
B	AC	BK	DU	EI	FL	GN	HO	MY	PS	QX	RT	Z&
C	AD	BG	CZ	EK	FM	HT	IX	LR	NP	OQ	S&	UY
D	AE	BZ	CT	DK	FI	GS	HY	LQ	MX	NR	O&	PU
E	AF	BL	CI	DH	EU	GK	MT	NQ	OR	P&	SX	YZ
F	AH	BF	CL	DG	EQ	IY	KP	MU	NS	O&	RX	TZ
G	AG	BI	CL	DN	ER	FP	HT	KU	M&	OX	QY	SZ
H	AI	BT	CS	DO	EL	F&	GH	KM	NQ	PR	UY	XZ
I	AK	BT	CS	DX	EI	FL	GZ	HY	M&	NP	OQ	RU
K	AL	BO	CP	DG	ER	FS	HU	IX	KY	MZ	N&	QT
L	AM	BZ	CD	EG	FI	HK	LN	OR	PS	QU	TY	X&
M	AN	BO	CP	DQ	ER	FS	GT	HU	IX	KY	LZ	M&
N	AO	BC	DM	EP	FS	GN	HY	IU	KT	LQ	R&	XZ
O	AP	BL	CK	DQ	ES	FU	GX	HZ	I&	MO	NR	TY
P	AQ	BX	CU	DZ	ES	FO	GY	HT	IN	KR	L&	MP
Q	AR	BZ	CT	DH	EU	FQ	GO	IL	KN	MP	SY	X&
R	AS	BN	CQ	DT	EU	FY	G&	HO	IP	KR	LX	MZ
S	AT	BP	CQ	DR	E&	FS	GU	HX	IY	KZ	LN	MO
T	AU	BY	CM	DX	E&	FH	GQ	IR	KZ	LS	NP	OT
U	AX	BL	CO	DQ	ES	FU	GT	HY	IN	KZ	M&	PR
X	AY	B&	CZ	DE	FX	GU	HI	KT	LS	MR	NP	OQ
Y	AZ	BU	CG	DH	EX	FY	IO	K&	LN	MP	QS	RT

Tab. 3.2: Verschlüsselungstabelle von Marie Antoinette

Die polyalphabetische Verschlüsselung ähnelt der Verschlüsselung von Porta, bei der die Buchstaben immer symmetrisch verschlüsselt werden. Soll etwa die mit A gekennzeichnete obere Zeile benutzt werden, wird der Buchstabe A mit B verschlüsselt und entsprechend B mit A. Ebenso C mit D sowie D mit C. Die Festlegung, welche Zeile für die Verschlüsselung eines Buchstabens zuständig ist, richtet sich nach einem Schlüssel, den sie häufiger wechselten.

Klartext	Dies ist ein geheimer Text
Schlüssel	ANTOINETTE

Die Buchstaben des Klartextes werden der Reihe nach bearbeitet und der zugehörige Buchstabe des periodisch zu benutzenden Schlüssels am linken Rand der Tabelle bestimmt die Zeile, mit der dieser Buchstabe verschlüsselt wird.

Der Klartextbuchstabe D wird also mit der A-Zeile verschlüsselt und ergibt den Geheimtextbuchstaben C. Danach wird die N-Zeile für den nächsten Buchstaben I benutzt und der zugehörige Geheimtextbuchstabe lautet U. So werden der Reihe nach alle Buchstaben des Klartex-

tes verschlüsselt und ergeben den Geheimtext.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
A	N	T	O		I	N	E		T	T	E		A	N	T	O	I	N	E	T		T	E	A	N
C	U	&	E		E	F	M		&	R	Q		H	P	F	S	E	D	U	I		O	U	Y	K

Allerdings verschlüsselten Marie Antoinette und Fersen in dem Brief vom 08.07.1791 nur jeden zweiten Buchstaben mit diesem Verfahren und übernahmen die anderen Buchstaben unverändert.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
A	-	N	-		T	-	O		-	I	-		N	-	E	-	T	-	T	-		E	-	A	-
C	I	P	S		R	S	Y		E	E	N		N	E	D	E	R	M	&	R		M	E	Y	T

Variante

Im Jahr 1792 verwendete Marie Antoinette in Briefen an zwei ihrer Schwestern und andere Verwandte in Italien eine andere Chiffre, die nach dem Prinzip der Verschlüsselungstabelle von Porta aufgebaut ist. Das verwendete Alphabet umfasst nur 22 Buchstaben, da der Buchstabe K für die Briefe in italienischer Sprache entfernt wurde.

AB	ABCDEFGHILM OPQRSTVXYZN	CD	MABCDEFGHIL ZNOPQRSTVXY
EF	LMABCDEFGHI NOPQRSTVXYZ	GH	ILMABCDEFGH NOPQRSTVXYZ
IL	HILMABCDEFG NOPQRSTVXYZ	MN	GHILMABCDEF NOPQRSTVXYZ
OP	FGHILMABCDE NOPQRSTVXYZ	QR	EFGHILMABCD NOPQRSTVXYZ
ST	DEFGHILMABC NOPQRSTVXYZ	VX	CDEFGHILMAB NOPQRSTVXYZ
YZ	BCDEFGHILMA NOPQRSTVXYZ		

Tab. 3.3: Zweite Verschlüsselungstabelle von Marie Antoinette

Mit dieser Verschlüsselungstabelle führt der bereits im ersten Beispiel verwendete Klartext mit demselben Schlüssel ANTOINETTE zu dem nachfolgenden Geheimtext.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
A	N	T	O		I	N	E		T	T	E		A	N	T	O	I	N	E	T		T	E	A	N
R	P	O	M		O	A	E		O	S	L		V	Y	R	Z	O	R	T	H		L	T	H	B

3.1.5 Kircher

Der Jesuitenpater Kircher hat die Tabula Recta von Trithemius umgewandelt und die Buchstaben von A bis Z ohne J durch die Zahlen von 1 bis 25 ersetzt, die jedoch nicht die Geheimtextzeichen darstellten. Zusätzlich verwendete er wie Vigenère ein Schlüsselwort.[25]

Klartext	Dies ist ein geheimer Text
Schlüssel	KIRCHER

Kircher benutzte ein beliebiges Dokument und markierte dort Buchstaben in Abständen, die den Zahlen aus der Tabelle entsprachen. Daher nannte sein Schüler Gaspar Schott dieses Verfahren auch *Abacus numeralis*.

	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	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	Z
B	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	Y
C	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	X
D	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	W
E	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	V
F	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	U
G	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	T
H	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	S
I	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	R
K	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	Q
L	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	P
M	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	O
N	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	N
O	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	M
P	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	L
Q	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	K
R	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	I
S	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	H
T	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	G
U	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	F
V	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	E
W	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	D
X	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	C
Y	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	B
Z	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	A

Tab. 3.4: Verschlüsselungstabelle von Kircher

Für den ersten Buchstaben D des Klartextes sucht man diesen in der Kopfzeile und den ersten Schlüsselbuchstaben K am linken Rand der Tabelle. Im Schnittpunkt der zugehörigen Spalte und Zeile befindet sich die Zahl 13. Anstatt diesen Code wie üblich als Geheimtext zu notieren, nahm Kircher jedoch ein beliebiges Dokument und markierte dort das durch diesen Code festgelegte Zeichen w. In diesem Beispiel das dreizehnte Zeichen vom Beginn des Dokumentes.

[25] Kircher [115] S. 128ff, Fleißner [78] S. 51 – 52, Schneickert [175] S. 45

Da für das Beispiel das Gedicht *Die Loreley* von Heinrich Heine gewählt wurde, müssen natürlich die Umlaute und das Zeichen ß durch zwei Buchstaben dargestellt werden. Zusätzlich werden die Satz- und Leerzeichen nicht gezählt.

Für den zweiten Buchstaben bestimmen die beiden Buchstaben I aus der Kopfzeile und dem Schlüsselwort den Code 17. Wie bei allen weiteren Codes wird immer der Abstand zum nächsten zu markierenden Buchstaben festgelegt, der hier D lautet.

D	I	E	S		I	S	T		E	I	N	G	E	H		E	I	M		E	R		T	E	X	T
K	I	R	C		H	E	R		K	I	R	C	H	E		R	K	I		R	C		H	E	R	K
13	17	21	20		16	22	10		14	17	4		9	12		12	21	18		20	21	19		1	9	14	3
w	D	n	i		i	s	e		h	n	G		B	t		e	...										

Mit den Markierungen ergibt sich folgende Darstellung der ersten beiden Strophen des Gedichtes, das dann dem Empfänger übergeben werden muss.

Ich weiss nicht, was soll es bedeuten,
Dass ich so traurig bin;
Ein Maehrchen aus alten Zeiten,
Das kommt mir nicht aus dem Sinn.

Die Luft ist kuehl und es dunkelt,
Und ruhig fliesst der Rhein;
Der Gipfel des Berges funkelt
Im Abendsonnenschein.

Im Gegensatz zu den Tabellen von Trithemius und Vigenère und befindet sich auch am rechten Rand ein zweites Alphabet in umgekehrter Reihenfolge der Buchstaben. Dieses kann nach Absprache statt des Alphabets am linken Rand für die Schlüsselbuchstaben verwendet werden. Auch ist es möglich, beide Alphabete abwechselnd oder nach einem festen Schema zu benutzen.

Man erkennt, dass bei dem Verfahren von Kircher und längeren zu verschlüsselnden Mitteilungen ein umfangreiches Dokument vorhanden sein muss, sodass es sehr umständlich zu handhaben ist.

3.1.6 Schott

Eine etwas vereinfachte Form als die von Kircher stammt von seinem Schüler Gaspar Schott. Dieser verwendet für die Verschlüsselung keine Tabelle, sondern bei ihm sind den Buchstaben ohne J Zahlen von 1 bis 25 in beliebiger Reihenfolge zugeordnet.[26]

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
10	18	1	2	6	11	20	3	7	4	12	25	15	5	21	14	24	8	9	13	16	22	17	23	19

[26] Schott [177] S. 75ff, Fleißner [78] S. 50 – 51, Schneickert [175] S. 51-52

Bei diesem Verfahren wird ein Dokument benötigt, bei dem für den verschlüsselten Klartext Buchstaben markiert werden. Wie beim vorherigen Beispiel wird das Gedicht *Die Loreley* von Heinrich Heine gewählt, das entsprechend aufbereitet wird.

Klartext	Dies ist ein geheimer Text

Dem ersten Buchstaben des Klartextes D ist die Zahl 2 zugeordnet, sodass der zweite Buchstabe c im Dokument markiert wird. Da zu dem zweiten Buchstaben I die Zahl 7 gehört, wird vom zuletzt markierten Buchstaben aus sieben Positionen weitergezählt und der dort vorhandene Buchstabe n markiert. Die nachfolgenden Markierungen werden also im Gegensatz zu Kircher nicht aus einer Tabelle, sondern mit den Zahlen festgelegt, die den Buchstaben zugeordnet sind.

D I E S	I S T	E I N	G E H E I M E R	T E X T
2 7 6 8	7 8 9	6 7 15	20 6 3 6 7 25 6 24	9 6 17 9
c n a b	n s b	M e n	d n e s u s h n	e n ...

Für den zu verschlüsselnden Klartext sind die Markierungen auch bei dieser Verschlüsselung für die ersten beiden Strophen des Gedichtes *Loreley* von Heinrich Heine angegeben.

Ich weiss nicht, was soll es bedeuten,
Dass ich so traurig bin;
Ein Maehrchen aus alten Zeiten,
Das kommt mir nicht aus dem Sinn.

Die Luft ist kuehl und es dunkelt,
Und ruhig fliesst der Rhein;
Der Gipfel des Berges funkelt
Im Abendsonnenschein.

Wie bei Kircher muss das markierte Dokument dann dem Empfänger übergeben werden.

3.2 Verfahren mit Zahlen

3.2.1 Österreichische Militärchiffre

Bei der *Österreichischen Militärchiffre* handelt es sich prinzipiell um eine Variante der Gronsfeld-Verschlüsselung und damit um eine abgeschwächte Variante der Verschlüsselung von Vigenère. Außerdem besteht der Geheimtext aus zweiziffrigen Zahlen. Diese Chiffre wurde vom österreichischen Militär bis Ende des 19. Jahrhunderts benutzt.[27]

Klartext	Dies ist ein geheimer Text
Schlüssel	MILITAERCHIFFRE

[27] Figl [77] S. 84

Am oberen Rand der Verschlüsselungstabelle werden die Buchstaben des Alphabets platziert und am linken Rand die Buchstaben des Schlüsselwortes einschließlich sich wiederholender Buchstaben.

In jeder Zeile der Tabelle werden die 26 Zahlen von 11 bis 36 eingetragen. Ordnet man wie üblich den Buchstaben von A bis Z die Zahlen von 0 bis 25 zu, beginnt jede Zeile mit der Summe aus dem Code des aktuellen Buchstabens des Schlüsselwortes und der Zahl 11. In den rechts danebenliegenden Zellen dieser Zeile werden die nachfolgenden Zahlen platziert und am Ende der Zeile die eventuell fehlenden Zahlen ab 11 aufwärts.

		Klartext																								
		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
Schlüssel	M	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22
	I	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18
	L	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21
	I	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18
	T	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
	A	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
	E	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14
	R	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
	C	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12
	H	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17
	I	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18
	F	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15
	F	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15
	R	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
	E	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14

Tab. 3.5: Verschlüsselungstabelle

Der erste Buchstabe D des Klartextes wird mit einer Zahl aus der ersten Zeile der Tabelle verschlüsselt. Im Schnittpunkt der gewählten Zeile und der Spalte mit dem Buchstaben D liegt dann die zugehörige Geheimtextzahl 26. Entsprechend ergibt sich für die Spalte mit dem zweiten Klartextbuchstaben I und der nachfolgenden Zeile die Zahl 27. Insgesamt ergeben sich folgende Zahlen an den Schnittpunkten der Spalten und Zeilen.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
M	I	L	I	T	A	E	R	C	H	I	F	F	R	E	M	I	L	I	T	A	E
26	27	26	11	12	29	34	32	21	31	25	20	23	32	23	35	23	13	12	34	34	34

Damit lautet der Geheimtext

Geheimtext	26272	61112	29343	22131	25202	33223	35231	31234	3434

3.2.2 Russische Sprungchiffre

Eine Variante der *Österreichischen Militärchiffre* sowie der *Italienischen Taschenchiffre* ist die *Russische Sprungchiffre*, die 1914 von der russischen Armee eingesetzt wurde.[28]

Passt man das Verfahren auf das lateinische Alphabet an, wird eine Verschlüsselungstabelle mit 26 Spalten für die Buchstaben verwendet. Sie besitzt acht Zeilen, die mit den Ziffern von 1 bis 8 in beliebiger Reihenfolge gekennzeichnet werden.

Die Zellen dieser Tabelle sind mit den Zahlen von 12 bis 98 gefüllt. Keine dieser Zahlen enthält jedoch die Ziffer 0 oder besteht aus zwei gleichen Ziffern. In diesem Beispiel treten 64 der 72 Zahlen dreimal und acht Zahlen nur zweimal auf, sodass insgesamt 208 Zahlen in der Tabelle vertreten sind. Links neben diesen Zahlen wird die Anordnung der Kennzahlen 1 bis 8 für die Zeilen als Schlüssel in einer beliebigen Reihenfolge verwendet. Die Anordnung der Zahlen sowie die Reihenfolge der acht Schlüsselzahlen wurden in regelmäßigen Abständen gewechselt.

Klartext

	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
2	48	56	35	14	72	19	19	98	82	93	68	96	21	15	25	82	52	75	54	68	96	49	53	46	51	52
7	68	32	16	14	76	34	23	28	85	17	17	41	34	37	72	12	63	19	67	78	27	79	42	48	15	29
4	97	32	13	35	27	91	97	24	83	53	51	25	93	47	43	41	84	59	42	73	59	78	74	57	85	35
3	95	89	97	76	84	74	12	91	69	71	75	65	86	52	62	37	41	54	45	38	57	86	18	29	37	73
8	13	36	72	71	38	83	18	25	26	81	47	62	91	89	47	96	94	87	23	67	79	64	24	73	89	71
1	79	31	28	21	81	83	46	31	18	63	86	26	54	26	21	78	43	36	58	36	75	45	27	49	56	31
6	58	84	43	16	23	32	59	53	98	13	17	67	94	34	24	93	39	95	69	76	45	16	57	64	74	94
5	51	29	65	65	64	15	49	87	61	39	63	42	92	69	81	39	95	92	61	92	82	87	38	62	46	48

Für die Verschlüsselung werden zunächst fünf gleiche Signalziffern wie etwa 33333 als Beginn des Geheimtextes gesendet. Da bei den Zahlen der Tabelle keine gleichen Ziffern auftreten, ist diese Ziffernfolge nicht mit Zahlen aus der Tabelle zu verwechseln.

Diese Signalzahlen geben an, wie viele Buchstaben des Klartextes mit den unterschiedlichen Zeilen der Tabelle verschlüsselt werden. In diesem Beispiel werden die ersten drei Buchstaben mit der Zeile verschlüsselt, die die Kennzahl 1 besitzt, also der sechsten Zeile von oben. Die nächsten drei Buchstaben werden anschließend mit den Zahlen aus der Zeile mit der Kennzahl 2 verschlüsselt. Sind alle acht Zeilen verwendet worden, beginnt man wieder mit der Zeile der Kennzahl 1.

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`27438165`

Der erste Buchstabe des Klartextes `D` wird mit einer der Zahlen aus der Zeile verschlüsselt, die die Kennzahl 1 besitzt. Im Schnittpunkt dieser Zeile mit der Spalte des Buchstabens `D` befindet sich die Zahl 21, die die erste Zahl des eigentlichen Geheimtextes bildet. Entsprechend findet

[28] Figl [77] S. 84

man zu den nachfolgenden Buchstaben I und E in dieser Zeile die Zahlen 18 und 81 für den Geheimtext.

Mit dem vierten Buchstaben S wird die zu benutzende Zeile gewechselt und die Zeile mit der Kennzahl 2 gewählt. Für diesen Buchstaben lautet damit die Geheimtextzahl 82. Insgesamt ergeben sich die nachfolgenden Zahlen des Geheimtextes.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
21	18	81	54	82	54	38	84	69	47	97	27	87	64	61	94	23	95	78	76	48	67

Anschließend werden die Ziffern aller Zahlen in Gruppen von jeweils fünf Ziffern unterteilt. Mit den fünf gleichen Signalziffern am Anfang erhält man dann abschließend den zu übermittelnden Geheimtext.

Geheimtext	33333 21188 15482 54388 46947
	97278 76461 94239 57876 4867

Innerhalb der Verschlüsselung können zusätzlich die Signalziffern gewechselt werden, indem diese einfach als Block von fünf Ziffern eingefügt werden. Eine Verwechslung mit den Geheimtextzahlen ist wegen der mehrfach auftretenden identischen Ziffern nicht möglich.

Diese Verschlüsselung wurde aber bereits Ende 1914 wieder aufgegeben, da dem Gegner die Entschlüsselung der Nachrichten gelang. Dies war u.a. auf Fehler bei der Verschlüsselung und eine zu geringe Anzahl an Wechseln mit eingefügten Signalzahlen zurückzuführen.

3.3 Auto Dinomic

Der Name dieser Verschlüsselung verrät, dass ein Autokey-Mechanismus verwendet wird, da sich ein zweistelliger Geheimtextcode immer mithilfe des vorhergehenden Klartextbuchstabens ergibt.[29]

Klartext	Dies ist ein geheimer Text
Schlüssel	AUTODINOMIC

Für die Verschlüsselung wird zunächst ein gemischtes Alphabet erzeugt, dessen Buchstaben ihre Positionen 1 bis 26 als zweistellige Zahlen mit eventuell führender Ziffer 0 zugeordnet werden.

A	U	T	O	D	I	N	M	C	B	E	F	G	H	J	K	L	P	Q	R	S	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

[29] Cryptogram [13]

Der erste Klartextbuchstabe D wird abweichend von den weiteren Buchstaben durch die ihm zugeordnete Zahl 05 codiert. Die Codes aller anderen Buchstaben ergeben sich aus dem Unterschied ihrer Positionen im Vergleich zu der Position des vorhergehenden Buchstabens. Vom Buchstaben D zu I muss man sich nur um eine Position nach rechts bewegen, also erhält dieser Buchstabe den Code 01. E erhält damit den Code 05, da sich dieser Buchstabe fünf Positionen weiter rechts von I befindet, und S dementsprechend den Code 10.

Die Unterschiede in den Positionen der Buchstaben werden zyklisch betrachtet, wie man etwa am Code 05 für den letzten Buchstaben T erkennt, der sich fünf Positionen weiter rechts vom vorletzten Buchstaben X befindet. Insgesamt ergeben sich folgende Codes,

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
05	01	05	10		11	15	08		08	21	01		06	24	03	23	21	02	03	09		09	08	13	05

aus denen dann der Geheimtext gebildet werden kann.

Geheimtext	05010	51011	15080	82101	06240	32321	02030	90908	1305

4 Checkerboard

4.1 Tri Square irregulär

Diese Verschlüsselung verwendet drei Polybios-Tabellen der Größe 6 x 5, die verschiedene Schlüsselworte besitzen.[30]

Klartext	Dies ist ein geheimer Text
Schlüssel	VIETA MATHE MATIK

Die mit den Schlüsselworten erzeugten gemischten Alphabete werden zudem unterschiedlich in die Tabellen eingetragen. Für das Verfahren ist es allerdings wichtig, dass die Struktur der Tabellen hinsichtlich der gefüllten Zellen identisch ist. In diesem Beispiel wird zuerst das gemischte Alphabet horizontal in die mittlere Tabelle eingetragen und legt die Struktur der beiden äußeren Tabellen fest.

In die linke Tabelle wird das gemischte Alphabet vertikal eingetragen, wobei die ersten drei Spalten von oben nach unten und die letzten drei Spalten von unten nach oben gefüllt werden. Die rechte Tabelle wird vertikal mit dem dritten gemischten Alphabet gefüllt. Allerdings wechselt die Richtung hier mit jeder Spalte.

Alle Zeilen und Spalten werden jeweils mit den gleichen Zahlen gekennzeichnet, deren Reihenfolge aber beliebig gewählt werden kann.

	6	3	1	5	4	2
5	V	B	H	P	U	Z
4	I	C	J	O	S	Y
1	E	D	K	N	R	X
3	T	F	L	M	Q	W
2	A	G				

a) Tabelle 1

	6	3	1	5	4	2
5	M	A	T	H	E	B
4	C	D	F	G	I	J
1	K	L	N	O	P	Q
3	R	S	U	V	W	X
2	Y	Z				

b) Tabelle 2

	6	3	1	5	4	2
5	M	F	G	Q	R	Z
4	A	E	H	P	S	Y
1	T	D	J	O	U	X
3	I	C	L	N	V	W
2	K	B				

c) Tabelle 3

Die Länge des Klartextes muss durch drei teilbar sein und notfalls durch Füllzeichen entsprechend verlängert werden. Damit kann er in Trigramme unterteilt werden, deren Buchstaben nach folgenden Regeln verschlüsselt werden.

1. Für den ersten Buchstaben werden in Tabelle 1 die Koordinaten bestimmt und der Buchstabe in Tabelle 2 mit diesen Koordinaten bildet den ersten Buchstaben eines Zwischencodes.
2. Der mittlere Buchstabe des Trigramms wird in Tabelle 2 gesucht und der Buchstabe an dieser Position in Tabelle 3 an den Zwischencode angehängt.
3. Für den dritten Buchstaben wird entsprechend Tabelle 3 für die Suche gewählt und der Buchstabe aus Tabelle 1 gewählt.

[30] Cryptogram [48]

Für das erste Trigramm DIE lauten die Koordinaten des Buchstabens D im linken Quadrat (1,3). An dieser Position findet sich in Tabelle 2 der Buchstabe L. Der zweite Buchstabe I besitzt in Tabelle 2 die Koordinaten (4,4) und Tabelle 3 verweist auf den zugehörigen Buchstaben S. Schließlich liefern die Koordinaten (4,3) von E in der dritten Tabelle den Buchstaben C aus Tabelle 1. Insgesamt ergeben sich folgende Zwischencodes für die Trigramme:

DIE	SIS	TEI	NGE	HEI	MER	TEX	TXX
LSC	ISS	RRT	OPC	TRT	VRU	RRX	RWX

Der endgültige Geheimtext ergibt sich dann, indem alle Zwischencodes umgekehrt werden.

Zwischencode	LSC	ISS	RRT	OPC	TRT	VRU	RRX	RWX
Geheimtext	CSL	SSI	TRR	CPO	TRT	URV	XRR	XWR

4.2 Polybios diagonal

In dieser Variante der Polybios-Verschlüsselung wird das Polybios-Quadrat verändert und die hiermit erstellte Ziffernfolge fragmentiert und einer zusätzlichen Veränderung unterzogen.[31]

Klartext	D	i	e	s		i	s	t		e	i	n		g	e	h
Schlüssel	P	O	L	Y	B	I	O	S	6							

Im ersten Schritt wird mit dem Schlüsselwort POLYBIOS ein gemischtes Alphabet erstellt. Dieses wird aber zusätzlich noch um die mit der Schlüsselzahl 6 festgelegte Anzahl von Positionen zyklisch gesehen nach rechts verschoben.

gemischtes Alphabet	P	O	L	Y	B	I	S	A	C	D	E	F	G	H	K	M	N	Q	R	T	U	V	W	X	Z
Verschiebung	T	U	V	W	X	Z	P	O	L	Y	B	I	S	A	C	D	E	F	G	H	K	M	N	Q	R

Die sich aus der Verschiebung ergebende Buchstabenfolge wird dann zeilenweise in das Polybios-Quadrat eingetragen.

	1	2	3	4	5
1	T	U	V	W	X
2	Z	P	O	L	Y
3	B	I	S	A	C
4	D	E	F	G	H
5	K	M	N	Q	R

31 Rubin [164] S. 101

Im nächsten Schritt werden die Buchstaben des Klartextes mithilfe des Polybios-Quadrates verschlüsselt.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
41	32	42	33	32	33	11	42	32	53	44	42	45	42	32	52	42	55	11	42	15	11

Anschließend wird die Zahlenfolge fragmentiert, wobei die linke Zahl 4 zunächst direkt in die darunterliegende Zeile übernommen wird. Danach wird die nächste Zahl 1 mit der ersten Zahl 4 der unteren Zeile addiert und die Summe $4+1=5$ als nächste Zahl der unteren Zeile notiert.

So fährt man fort, indem immer die nächste Zahl der oberen Zeile mit dem zuletzt berechneten Ergebnis aus der unteren Zeile addiert wird. Ist die Summe, wie in diesem Fall mit $3+5=8$ größer als 5, wird 5 von der Summe subtrahiert und das Ergebnis als nächste Zahl in die untere Zeile eingetragen.

```
4 1 3 2 4 2 3 3 3 2 3 3 1 1 4 2 3 2 5 3 4 4 4 2 4 5 4 2 3 2 5 2 4 2 5 5 1 1 4 2 1 5 1 1
  / /
4 5 3
```

Mit diesen Additionen ergibt sich insgesamt folgende Zahlenfolge:

```
4 1 3 2 4 2 3 3 3 2 3 3 1 1 4 2 3 2 5 3 4 4 4 2 4 5 4 2 3 2 5 2 4 2 5 5 1 1 4 2 1 5 1 1
  / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / / /
4 5 3 5 4 1 4 2 5 2 5 3 4 5 4 1 4 1 1 4 3 2 1 3 2 2 1 3 1 3 3 5 4 1 1 1 2 3 2 4 5 5 1 2
```

Die so erhaltene Zahlenfolge wird anschließend in Gruppen von jeweils zwei Ziffern unterteilt, die mithilfe des Polybios-Quadrates in Buchstaben umgewandelt werden.

45	35	41	42	52	53	45	41	41	14	32	13	22	13	13	35	41	11	23	24	55	12
H	C	D	E	M	N	H	D	D	W	I	V	P	V	V	C	D	T	O	L	R	U

Diese Buchstabenfolge bildet abschließend den Geheimtext, der durch die Fragmentierung der Zahlenfolge deutlich sicherer ist als die Verschlüsselung mit einem normalen Polybios-Quadrat.

Geheimtext	HCDEM NHDDW IVPVV CDTOL RU

4.3 Collon

Auguste Collon war Offizier der belgischen Armee und fasste zwischen 1899 und 1902 seinen Kenntnisstand der Kryptografie in mehreren Artikeln zusammen. In diesen legte er zeitgleich

mit Delastelle die Grundlagen für fragmentierte Verschlüsselungsverfahren.[32]

Klartext	Dies ist ein geheimer Text
Schlüssel	AUGUSTECOLLON 4

So stellte er etwa ein Verfahren vor, das ähnlich wie Polybios ein 5 x 5 - Quadrat verwendete. Er verwendete ein Schlüsselwort und schrieb das zugehörige gemischte Alphabet horizontal oder vertikal in das Quadrat. Während Collon bei seinem Alphabet den Buchstaben K ausließ, wird in dem hier aufgeführten Beispiel der Buchstabe J durch I ersetzt.

A	U	G	S	T
E	C	O	L	N
B	D	F	H	I
K	M	P	Q	R
V	W	X	Y	Z

Da die Zeilen und Spalten dieses Quadrates keine Kennungen durch Ziffern oder Buchstaben aufweisen, verwendete Collon stattdessen die Einträge in der unteren Zeile sowie der linken Spalte. So wird etwa der Buchstabe D durch BW und I durch BZ verschlüsselt. Die so erhaltenen Buchstabenpaare notierte er untereinander in zwei Zeilen, wobei er die Buchstabenfolge gleichzeitig in Gruppen von drei, vier oder fünf Buchstaben unterteilte. In diesem Beispiel werden Gruppen von jeweils vier Buchstaben gebildet.

Dies iste inge heim erTe xt
BBEA BAAE BEAE BEBK EKAE VA
WZVY ZYZV ZZXV YVZW VZZV XZ

Die gebildeten Buchstabengruppen werden gruppenweise von oben nach unten oder umgekehrt ausgelesen. Gleichzeitig kann man festlegen, ob die Buchstabenfolgen oder die beiden Zeilen jeweils von links nach rechts oder umgekehrt ausgelesen werden. In diesem Beispiel wird jeweils mit der unteren Zeile begonnen und die Buchstaben dieser Zeile werden von links nach rechts notiert. Die Buchstaben der oberen Zeile werden dagegen immer von rechts nach links ausgelesen.

BBEA	BAAE	BEAE	BEBK	EKAE	VA
WZVY	ZYZV	ZZXV	YVZW	VZZV	XZ
WZVY AEBB	ZYZV EAAB	ZZXV EAEB	YVZW KBEB	VZZV EAKE	XZ AV

[32] Collon [47] S. 13 – 15, Müller [145] S. 8.4, Sacco [168] S. 39 – 40

4.4 Homophones Straddling Checkerboard

Eine ungewöhnliche Chiffre, bei der die Klartextbuchstaben durch ein oder zwei Buchstaben verschlüsselt werden, wird in diesem Kapitel vorgestellt.[33]

Klartext	`Dies ist ein wichtiger geheimer Text`
Schlüssel	`VIETA CHECKERBOARD`

Sie ähnelt einem *Straddling Checkerboard*, wird aber zur besseren Verständlichkeit auf zwei Tabellen mit zwei Schlüsselworten aufgeteilt. Die ersten Buchstaben des gemischten Alphabets für die erste Tabelle werden zunächst in die obere Zeile platziert. Die weiteren Buchstaben werden dagegen vertikal von oben nach unten eingetragen, wobei man am rechten Rand der Tabelle beginnt.

In die rechte Tabelle wird das mit dem zweiten Schlüsselwort erstellte gemischte Alphabet horizontal eingetragen. Darüber platziert man zur einfacheren Durchführung der Verschlüsselung zusätzlich noch die Buchstaben der oberen Zeile aus der linken Tabelle.

V	I	E	T	A
Z	S	N	H	B
	U	O	J	C
	W	P	K	D
	X	Q	L	F
	Y	R	M	G

V	I	E	T	A
C	H	E	K	R
B	O	A	D	F
G	I	J	L	M
N	P	Q	S	T
U	V	W	X	Y
Z				

Für die Verschlüsselung sucht man zunächst den ersten Klartextbuchstaben `D` in der rechten Tabelle. Als Geheimtextbuchstabe wird zunächst ein beliebiger Buchstabe dieser Zeile aus der links danebenstehenden Tabelle gewählt. Zur Auswahl stehen in der entsprechenden Zeile `ZSNHB`, von denen beispielsweise `N` genommen wird. Der zweite Geheimtextbuchstabe ist dagegen eindeutig bestimmt, da er aus der durch `D` festgelegten Spalte der über der rechten Tabelle stehenden Zeile stammen muss. Dies ist der Buchstabe `T`.

V	I	E	T	A
Z	S	N	H	B
	U	O	J	C
	W	P	K	D
	X	Q	L	F
	Y	R	M	G

V	I	E	T	A
C	H	E	K	R
B	O	A	D	F
G	I	J	L	M
N	P	Q	S	T
U	V	W	X	Y
Z				

[33] Cryptogram [156]

Für den zweiten Buchstaben I stehen mit diesem Vorgehen für die Verschlüsselung die Bigramme UI, OI, JI sowie CI zur Auswahl.

Anders sieht es beim dritten Klartextbuchstaben E aus, da sich dieser in der oberen Zeile der rechten Tabelle befindet. In einem solchen Fall wird nur mit einem einzigen Geheimtextbuchstaben verschlüsselt, der aus dieser Spalte der darüberstehenden Hilfszeile gewählt wird und zufälligerweise auch E heißt. So entsteht etwa der nachfolgende Zwischencode.

D	I	E	S		I	S	T		E	I	N		G	E	H	E	I		M	E	R		T	E	X	T
NT	JI	E	DT		JI	WT	WA		E	OI	DV		CV	E	I	E	JI		CA	E	A		KA	E	QT	WA

Sind alle Klartextbuchstaben mit diesen zwei Regeln verschlüsselt worden, kann der Geheimtext zusammengefasst werden.

Geheimtext	NTJIE DTJIW TWAEO IDVCV EIEJ ICAEA KAEQT WA

5 Polygrafische Verfahren

5.1 Playfair Varianten

5.1.1 Playfair mit Blendern

Eine Möglichkeit, die normale Playfair-Chiffre zu verstärken, besteht darin, an einigen Stellen Blender einzufügen.[34] Diese Variante benötigt neben dem Schlüsselwort für die Playfair-Chiffre einen weiteren Schlüssel, aus dem die als Blender einzufügenden Buchstaben stammen, sowie eine Zahlenfolge für die Einfügestellen.

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`PLAYFAIRNULL BLENDER 234`

Im ersten Schritt wird die Playfair-Tabelle erstellt und der Klartext ganz normal verschlüsselt.

P	L	A	Y	F
I	R	N	U	B
C	D	E	G	H
K	M	O	Q	S
T	V	W	X	Z

Playfair	`CRHOBKWCRUHGCGRKDNWCZV`

In diesen Zwischencode werden anschließend Blender eingefügt. Die Positionen der Einfügestellen ergeben sich aus der festgelegten Schlüsselzahl, deren Ziffern angeben, nach wie vielen Buchstaben ein Blender folgen soll. In diesem Fall werden also jeweils nach zwei, dann nach drei und danach wieder nach vier Buchstaben der Reihe nach die Buchstaben des Schlüsselwortes `BLENDER` eingefügt.

Zwischencode	`CR HOB KWCR UH GCG RKDN WC ZV`
Geheimtext	`CRBHOBLKWCREUHNGCGDRKDNEWCRZV`

Frank Rubin hat ein subjektives Bewertungssystem für die Stärke von Verschlüsselungsverfahren entworfen, bei dem er Stufen von 1 bis 10 verwendet. Als Grundlage verwendet er aus seiner Erfahrung den Aufwand, die Verfahren mit bekannten Methoden zu knacken, und den Vergleich der Chiffren untereinander.[35]

[34] Rubin [164] S. 104
[35] Rubin [164] S. 24

Stufe 1 steht für Chiffren, die von einem Anfänger ohne Vorkenntnisse mit Papier, Bleistift und mäßigem Aufwand geknackt werden können, und etwa Stufe 3 für Chiffren, die von einem erfahrenen Hobby-Kryptologen allein mit Papier und Bleistift geknackt werden können. Für Chiffren der Stufen 4 und 5 ist schon ein Computer oder ein ausgebildeter Kryptologe oder beides erforderlich. Ab Stufe 6 muss die Rechenkraft des Computers höher sein und es wird zusätzlich spezielles Fachwissen erforderlich.

Während er das normale Playfair-Verfahren der Stufe 3 zuordnet, hält er diese Variante mit Blendern für stärker und ordnet sie in Stufe 5 ein.

5.1.2 Playfair binär

Eine einfache Erweiterung verändert den mit der Playfair-Chiffre verschlüsselten Geheimtext nachträglich, um die Verschlüsselung etwas stärker zu machen.[36] Sie benötigt ein Schlüsselwort sowie eine Zahl.

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`PLAYFAIRBINAER 203`

Im ersten Schritt wird die Playfair-Tabelle erstellt und der Klartext ganz normal verschlüsselt.

P	L	A	Y	F
I	R	B	N	E
C	D	G	H	K
M	O	Q	S	T
U	V	W	X	Z

Playfair	`CRNTN MZKRE KBKNC UIBZK ZS`

Anschließend werden einige der erzeugten Geheimtextbuchstaben verändert. Dazu wird eine Schlüsselzahl wie etwa 203 in ihre binäre Darstellung umgewandelt

$$\begin{aligned} 203 &= 0 \cdot 256 + 1 \cdot 128 + 1 \cdot 64 + 0 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 \\ &= (011001011)_2 \end{aligned}$$

und als periodischer Schlüssel verwendet. Ist einem Buchstaben die Ziffer 1 zugeordnet, wird er zyklisch gesehen durch den Nachfolger des aktuellen Buchstabens ersetzt. Bei der Ziffer 0 bleibt er dagegen unverändert.

C	R	N	T	N	M	Z	K	R	E	K	B	K	N	C	U	I	B	Z	K	Z	S
0	1	1	0	0	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0
C	S	O	T	N	N	Z	L	S	E	L	C	K	N	D	U	J	C	Z	L	A	S

[36] Rubin [164] S. 104

Mit dieser Erweiterung ist die Playfair-Chiffre etwas stärker als die normale Verschlüsselung.

Geheimtext	CSOTN NZLSE LCKND UJCZL AS

Dazu sollte die binäre Schlüsselzahl eine ungerade Anzahl von Ziffern besitzen, da die Bigramme der Playfair-Chiffre sonst eventuell Wiederholungen aufweisen und damit ein angreifbares Muster ergeben. Dazu wurde in diesem Beispiel eine führende 0 hinzugefügt.

Im Bewertungssystem von Frank Rubin wird diese Variante in Stufe 5 eingeordnet.

5.1.3 Playfair mit zwei Tabellen

Eine andere Variante der Playfair-Chiffre verwendet zwei Tabellen mit unterschiedlichen Schlüsselwörtern, die nach einem bestimmten Muster abwechselnd für die Verschlüsselung benutzt werden.[37]

Klartext	Dies ist ein geheimer Text
Schlüssel	POLYPLAYFAIR TABELLEZWEI

Auch bei dieser Variante von Playfair werden zunächst zwei Quadrate erstellt, die mit den Buchstaben der beiden aus den Schlüsselworten erzeugten gemischten Alphabete horizontal gefüllt werden.

P	O	L	Y	A
F	I	R	B	C
D	E	G	H	K
M	N	Q	S	T
U	V	W	X	Z

T	A	B	E	L
Z	W	I	C	D
F	G	H	K	M
N	O	P	Q	R
S	U	V	X	Y

Für die Verschlüsselung wird der Klartext in Bigramme unterteilt, die mit einer der beiden Tabellen verschlüsselt werden. Welche Tabelle jeweils verwendet wird, richtet sich nach dem numerischen Schlüssel, der aus den ersten zehn Ziffern des ersten Schlüsselwortes erstellt wird. Ist dieses kürzer, können die fehlenden Ziffern entweder periodisch oder mit einem fortlaufenden Schlüssel erzeugt werden. Die Zahl 10 wird dabei durch die Ziffer 0 repräsentiert.

[37] Rubin [164] S. 105

Ist die Ziffer des numerischen Schlüssels kleiner als fünf, wird die erste Tabelle benutzt, sonst die zweite. Damit ist eine gleichmäßige Verteilung für die Verwendung beider Tabellen gesichert.

Klartext	DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
	7	6	4	9	8	5	1	0	3	2	7
Tabelle 1			BN				KG	FN	GI	NK	
Tabelle 2	ZC	TX		AL	ZP	KA		DH			SE

Aus den Verschlüsselungen der Bigramme lässt sich dann der Geheimtext zusammensetzen.

Geheimtext	ZCTXB	NALZP	KAKGF	NGINK	SE

Im Bewertungssystem von Frank Rubin wird diese Variante mit normalen Schlüsseln in Stufe 5 eingeordnet. Mit fortlaufenden Schlüsseln erreicht diese Variante sogar Stufe 6.

5.1.4 Double Playfair

Die Playfair-Chiffre kann auch verstärkt werden, indem man sie zweimal hintereinander mit unterschiedlichen Schlüsselworten anwendet und zugleich die Bigramme aus der ersten Verschlüsselung fragmentiert.[38]

Klartext	Dies	ist	ein	geheimer	Text
Schlüssel	PLAYFAIREINS		TABELLEZWEI		

Mit den beiden Schlüsselworten werden zunächst zwei gemischte Alphabete erstellt, die horizontal in zwei 5 x 5 - Quadrate eingetragen werden. Danach wird der Klartext mit der ersten Tabelle verschlüsselt.

P	L	A	Y	F
I	R	E	N	S
B	C	D	G	H
K	M	O	Q	T
U	V	W	X	Z

T	A	B	E	L
Z	W	I	C	D
F	G	H	K	M
N	O	P	Q	R
S	U	V	X	Y

Um die unbefugte Entschlüsselung weiter zu erschweren, wird anschließend der erste Buchstabe abgetrennt und hinten wieder angefügt. Mit diesem Schritt wird die Struktur der Bigramme zerstört.

Zwischentext	BENIRIOSRSDNDSRKNEOSZQ
	ENIRIOSRSDNDSRKNEOSZQB

[38] Rubin [164] S. 105

Der so veränderte Zwischentext wird dann mit der zweiten Tabelle noch einmal verschlüsselt und man erhält den endgültigen Geheimtext.

Geheimtext	TQDPW PYNYZ RZYNF QAQTF PE

Frank Rubin erachtet diese Variante als besonders stark und ordnet sie in seinem Bewertungssystem in Stufe 6 ein.

5.1.5 Playfair diagonal

In dieser Variante der Playfair-Chiffre wird nicht der gesamte Klartext in Bigramme unterteilt und dann verschlüsselt, sondern besonders gebildete Buchstabenpaare.[39]

Klartext	Dies ist ein geheimer Text
Schlüssel	PLAYFAIRDIAGONAL

Mit dem Schlüsselwort wird im ersten Schritt ein gemischtes Alphabet erstellt, mit dem ein 5 x 5 - Quadrat gefüllt wird.

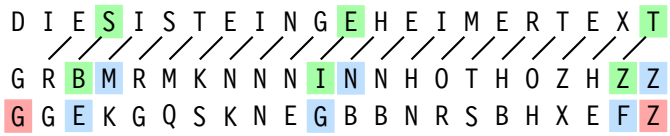
P	L	A	Y	F
I	R	D	G	O
N	B	C	E	H
K	M	Q	S	T
U	V	W	X	Z

Zunächst werden die ersten beiden Klartextbuchstaben DI mithilfe der Playfair-Tabelle verschlüsselt. Die beiden sich ergebenden Geheimtextbuchstaben GR werden eine Zeile tiefer unter den Klartext geschrieben. Der erste dieser beiden Buchstaben wird zusätzlich eine weitere Zeile tiefer an den Anfang platziert.

Anschließend wird der zweite Buchstabe R aus der mittleren Zeile mit dem dritten Buchstaben E des Klartextes kombiniert und das Buchstabenpaar RE verschlüsselt. Das Ergebnis GB wird direkt unter die beiden benutzten Buchstaben in die untere und mittlere Zeile übertragen.

[39] Rubin [164] S. 105, Friedman - Callimahos [81] S. 514

So fährt man fort und verschlüsselt immer das diagonale Buchstabenpaar aus der mittleren und der oberen Zeile. Die beiden so erhaltenen Geheimtextbuchstaben werden immer in der unteren und mittleren Zeile platziert.



Der Buchstabe am rechten Rand der unteren Zeile lässt sich nicht mehr aus einem diagonalen Bigramm erzeugen, sodass er als Kopie des darüberliegenden Buchstabens der mittleren Zeile eingefügt wird.

Damit lautet der mit diesem Verfahren erzeugte Geheimtext

Geheimtext	GGEKG QSKNE GBBNR SBHXE FZ

Im Bewertungssystem von Frank Rubin wird diese starke Variante in Stufe 6 eingeordnet.

5.1.6 Playfair - Two Square

Wenn wie bei der Variante mit zwei Tabellen verwendet werden, bietet es sich an, Playfair mit einer anderen Chiffre wie Two Square zu kombinieren.[40] Eine solche Kombination verschlüsselt deutlich stärker als eine einfache Playfair-Chiffre mit nur einer Tabelle.

Klartext	Dies ist ein geheimer Text
Schlüssel	PLAYFAIR TWOSQUARE 12332131323

Für diese Verschlüsselung werden zwei 5 x 5 - Quadrate benötigt, in die die beiden gemischten Alphabete notiert werden, die sich mit den festgelegten Schlüsselworten ergeben.

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

T	W	O	S	Q
U	A	R	E	B
C	D	F	G	H
I	K	L	M	N
P	V	X	Y	Z

Mit diesen beiden Tabellen können drei unterschiedliche Verschlüsselungen verwendet werden:

40 Rubin [164] S. 107

- Eine Playfair-Verschlüsselung mit der ersten Tabelle.
- Eine Playfair-Verschlüsselung mit der zweiten Tabelle.
- Eine Two Square-Verschlüsselung mit beiden Tabellen.

Die Entscheidung, welche der drei Verschlüsselungen für ein Buchstabenpaar benutzt werden soll, kann über einen dritten Schlüssel erfolgen. Dies kann, wie in diesem Beispiel, etwa über eine Zahlenfolge mit den Ziffern 1, 2 und 3 erfolgen. Es ist aber auch ein fortlaufender Schlüssel mit den Ziffern von 0 bis 9 denkbar.

Dabei sollte die Verteilung der Ziffern sicherstellen, dass die beiden Verschlüsselungen etwa gleich oft gewählt werden und das Two Square-Verfahren ungefähr so oft, wie die beiden Playfair-Verschlüsselungen zusammen.

In dem hier gewählten Beispiel werden die Bigramme des Klartextes damit folgendermaßen verschlüsselt:

Klartext	DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
	1	2	3	3	2	1	3	1	3	2	3
Playfair 1	IR					HG		DE			
Playfair 2		GE			KI					SU	
Two Square			EP	MD			GB		FI		PY

Zusammengefasst ergeben diese Bigramme abschließend den Geheimtext.

Geheimtext	IRGEE	PMDKI	HGGBD	EFISU	ZS

Frank Rubin erachtet diese Kombination von Verschlüsselungsverfahren als besonders stark und ordnet sie in seinem Bewertungssystem in Stufe 6 ein.

5.1.7 Playfair asymmetrisch

Die Playfair-Chiffre ist ein bekanntes und lange Zeit beliebtes Verschlüsselungsverfahren. Allerdings hat es den Nachteil, dass Sonderfälle eintreten, wenn die beiden Buchstaben in derselben Zeile oder Spalte liegen. Weiterhin muss ein Füllzeichen eingefügt werden, wenn ein Bigramm aus gleichen Buchstaben besteht. Das asymmetrische Playfair-Verfahren kommt dagegen ohne diese Sonderfälle aus.[41]

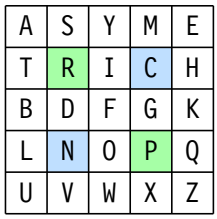
Klartext	Dies ist ein geheimer Text
Schlüssel	ASYMMETRISCH

[41] Cryptogram [184]

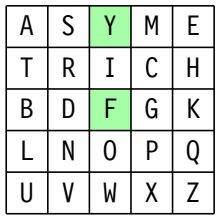
Im ersten Schritt wird mit dem Schlüsselwort ein gemischtes Alphabet erstellt und die sich ergebende Buchstabenfolge horizontal in ein 5 x 5 - Quadrat eingetragen.

A	S	Y	M	E
T	R	I	C	H
B	D	F	G	K
L	N	O	P	Q
U	V	W	X	Z

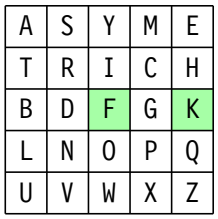
Bei diesem Verfahren werden grundsätzlich alle Bigramme mithilfe eines virtuellen Rechtecks verschlüsselt. Dies gilt auch, wenn das Rechteck zu einer Linie entartet. Daher werden zwei Buchstaben, die sich in derselben Spalte befinden, unverändert übernommen. Befinden sich dagegen zwei Buchstaben in derselben Zeile, werden sie wegen der unterschiedlichen Spalten umgedreht. Auch das Problem von gleichen Buchstaben wird vorläufig elegant gelöst, indem sie unverändert übernommen werden.



a) RP → CN



b) YF → YF



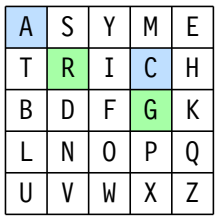
c) FK → KF

Nach diesen Regeln werden die Bigramme des Klartextes verschlüsselt.

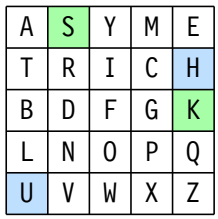
```
DI ES IS TE IN GE HE IM ER TE XT
FR SE RY HA RO KM HE CY SH HA UC
```

Allerdings bieten die Regeln für die Behandlung der Sonderfälle natürlich deutliche Ansatzpunkte für eine ungewollte Entschlüsselung. Daher schließt sich ein zusätzlicher Schritt an, der die beiden Buchstaben der Bigramme unterschiedlich verändert.

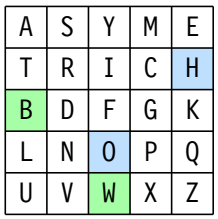
Der linke Buchstabe wird jeweils durch den Buchstaben ersetzt, der sich in der Tabelle eine Zeile darüber und eine Spalte weiter links befindet. Dagegen wird der rechte Buchstabe durch den Buchstaben ersetzt, der sich genau eine Zeile darüber befindet. Alle Änderungen werden, wie bei Tabellen üblich, immer zyklisch betrachtet.



a) RG → AC



b) SK → UH



c) BW → HO

Angewendet auf den Zwischencode des ersten Teilschrittes, ergibt sich mit diesen Regeln der Geheimtext.

	FR	SE	RY	HA	RO	KM	HE	CY	SH	HA	UC
Geheimtext	RS	UZ	AW	MU	AF	CX	MZ	YW	UE	MU	QM

5.1.8 Playfair 6 x 6

Andreas Figl hat 1926 ein modifiziertes Playfair-Verfahren mit einem Quadrat der Größe 6 x 6 vorgestellt, bei dem neben den 26 Buchstaben auch die Ziffern von 0 bis 9 verwendet werden.[42] Neben der besonderen Größe des Playfair-Quadrates zeichnet sich seine Chiffre dadurch aus, dass die zehn Ziffern sehr gut mit den Buchstaben des Alphabets gemischt werden.

Klartext	Dies ist ein geheimer Text
Schlüssel	ANDREASFIGL F

Im ersten Schritt wird mit dem Schlüsselwort ein gemischtes Alphabet erstellt. Die Ziffern hängt er aber nicht einfach an diese Buchstabenfolge an, sondern fügt sie der Reihe an ganz bestimmten Stellen ein. Die erste Ziffer 0 platziert er unmittelbar hinter dem Startbuchstaben F, der in diesem Beispiel als zweiter Schlüssel festgelegt ist. Die weiteren neun Ziffern werden anschließend hinter den Buchstaben eingefügt, die alphabetisch auf den Startbuchstaben folgen. In diesem Fall schließen sich die weiteren Ziffern 1 bis 9 also unmittelbar an die Buchstaben FGHIJKLMNO an.

ANDRESFIGLBCHJKMOPQTUVWXYZ
AN8DRESF I G L BCH J K M O PQTUVWXYZ
AN8DRESF0I3G1L6BCH2J4K5M7O9PQTUVWXYZ

Diese Folge aus Buchstaben und Ziffern wird horizontal in das Playfair-Quadrat eingetragen.

A	N	8	D	R	E
S	F	0	I	3	G
1	L	6	B	C	H
2	J	4	K	5	M
7	O	9	P	Q	T
U	V	W	X	Y	Z

42 Figl [77] S. 91-92

Abschließend kann der Klartext mit den Regeln des normalen Playfair-Verfahrens verschlüsselt werden.

DI ES IS TE IN GE HE IM ER TE XT
IB AG 3F ZG FD HG MG GK AE ZG ZP

Die erhaltenen Bigramme bilden dann den Geheimtext.

Geheimtext	IBAG3 FZGFD HGMGG KAEZG ZP

Variante 1

Um die Zeichenfolge von Buchstaben und Ziffern noch stärker zu durchmischen, schlägt Figl eine Variante vor.

Klartext	Dies ist ein geheimer Text
Schlüssel	FIGLVARIANTE A

Wie bei dem vorherigen Verfahren werden die Ziffern wieder unmittelbar hinter den Buchstaben des gemischten Alphabets eingefügt, die auf den Startbuchstaben A folgen.

FIGLVARNTEBCDHJKMOPQSUWXYZ
F I G LVA RNTE B C D H J KMOPQSUWXYZ
F5I8G6LVA0RNTE4B1C2D3H7J9KMOPQSUWXYZ

Da die Ziffern allerdings noch nicht besonders gut durchmischt sind, werden die Buchstaben und Ziffern zunächst horizontal in eine Tabelle geschrieben, deren Breite durch die Anzahl der unterschiedlichen Buchstaben im Schlüssel einschließlich eventuell zugehöriger Ziffern bestimmt ist. In diesem Beispiel sind dies zehn unterschiedliche Buchstaben und fünf zugehörige Ziffern. Somit besitzt diese Hilfstabelle 15 Spalten.

F	5	I	8	G	6	L	V	A	0	R	N	T	E	4
B	1	C	2	D	3	H	7	J	9	K	M	O	P	Q
S	U	W	X	Y	Z									

Diese Tabelle wird vertikal ausgelesen und die Zeichen horizontal in das eigentliche Playfair-

Quadrat eingetragen.

F	B	S	5	1	U
I	C	W	8	2	X
G	D	Y	6	3	Z
L	H	V	7	A	J
O	9	R	K	N	M
T	O	E	P	4	Q

Mit diesem Quadrat wird die eigentliche Playfair-Verschlüsselung durchgeführt.

DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
GC	SW	WF	OP	2O	YT	VO	XO	SE	OP	IQ

Der Geheimtext wird abschließend aus den erhaltenen Bigrammen gebildet.

Geheimtext	GCSWW FOP2O YTVOX OSEOP IQ

Variante 2

Eine zweite Variante von Figl verläuft prinzipiell wie die erste Variante. Allerdings ändert sich der Zeitpunkt, an dem die Ziffern in das gemischte Alphabet eingefügt werden.

Klartext	Dies ist ein geheimer Text
Schlüssel	VARIANTEZWEI V

Mit dem Schlüsselwort wird zunächst ein gemischtes Alphabet erzeugt und horizontal in eine Hilfstabelle eingetragen. Die Breite dieser Tabelle wird durch die Anzahl der unterschiedlichen Buchstaben im Schlüssel festgelegt, in diesem Beispiel also neun.

Diese Hilfstabelle wird wieder vertikal ausgelesen und die Inhalte horizontal in das Playfair-Quadrat eingetragen. Erst in diesem Schritt werden die zehn Ziffern direkt hinter den zugeordneten Buchstaben platziert.

V	A	R	I	N	T	E	Z	W
B	C	D	F	G	H	J	K	L
M	O	P	Q	S	U	X	Y	

V	O	B	6	M	A
5	C	7	O	R	D
8	P	I	F	Q	N
G	S	T	H	U	E
9	J	X	2	Z	4
K	Y	3	W	1	L

Mit diesem Quadrat kann nun verschlüsselt werden

DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
7N	GT	PT	HG	F8	SG	UG	QB	UD	HG	3X

und man erhält abschließend den Geheimtext.

Geheimtext	7NGTP THGF8 SGUGQ BUDHG 3X

5.1.9 Playfair 5 x 6

Das *Playfair*-Verfahren lässt sich auch mit anderen Tabellen anwenden, die nicht quadratisch sind.[43] Um die Verschlüsselung etwa mit einem Rechteck der Größe 5 x 6, also sechs fünf Zeilen und sechs Spalten, durchführen zu können, müssen 30 Einträge festgelegt werden. Mit den getrennten Buchstaben I und J fehlen noch vier weitere Einträge.

Klartext	Dies ist ein geheimer Text
Schlüssel	PLAYFAIR

Friedman hat ein Rechteck dieser Größe vorgestellt, indem er einen Buchstaben entfernt und durch die Kombination mit den fünf Vokalen ersetzt hat.

Es wird zunächst ein normales gemischtes Alphabet mit dem Schlüsselwort PLAYFAIR erstellt. Dann wird in diesem Beispiel der Buchstabe G entfernt und durch die Buchstabenkombinationen GA, GE, GI, GO und GU ersetzt. Mit diesen Buchstaben und Buchstabenkombinationen ergibt sich folgende Tabelle.

P	L	A	Y	F	I
R	B	C	D	E	GA
GE	GI	GO	GU	H	J
K	M	N	O	Q	S
T	U	V	W	X	Z

Die Verschlüsselung des Klartextes geschieht dann wie beim normalen Playfair-Verfahren, nur dass der Buchstabe G durch eine der fünf Buchstabenkombinationen aus der Tabelle ersetzt wird.

G ⟶ GA GE GI GO GU

[43] Friedman - Callimahos [80] S. 139-140

Abbildung 5.1 zeigt einige Beispiele, bei denen der Buchstabe G auftritt. In den beiden äußeren Beispielen wird neben dem ursprünglichen Bigramm auch dessen Ersetzung dargestellt.

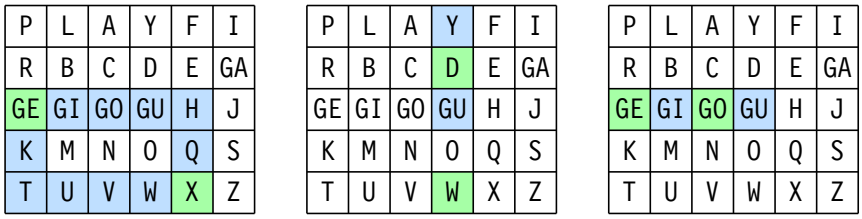


Abb. 5.1: Verschlüsselung mit einer 5 x 6 - Tabelle

Mit diesen Vorschriften ergibt sich die folgende Verschlüsselung:

	DI ES IS TE IN GUE HE IM ER TE XT
	GAY GAQ GAZ XR AS HD QH LS GAB XR ZU
Geheimtext	GAYGA QGAZX RASHD QHLSG ABXRZ U

Wie an diesem Beispiel zu erkennen ist, ergeben sich für ein Bigramm Geheimtextblöcke, die aus zwei oder drei Buchstaben bestehen. Dies bereitet aber keine Probleme bei der Entschlüsselung, da der Buchstabe G nie einzeln auftritt, sondern mit dem nachfolgenden Vokal eine eindeutige Zelle in der Polybios-Tabelle bestimmt. Mit dem dritten Buchstaben kann dann eine der drei Regeln zur Entschlüsselung angewendet werden.

5.2 Fracfair

Eine weitere Variante der *Playfair*-Verschlüsselung ist *Fracfair*. Es werden auch hier Bigramme verschlüsselt, die jedoch nicht fortlaufend, sondern aus Gruppen von jeweils vier Buchstaben gebildet werden.[44]

Klartext	Dies ist ein geheimer Text
Schlüssel	FRACFAIR

Im ersten Schritt wird wie bei Playfair eine Tabelle mit einem aus dem Schlüssel gebildeten gemischten Alphabet erstellt.

F	R	A	C	I
B	D	E	G	H
K	L	M	N	O
P	Q	S	T	U
V	W	X	Y	Z

44 Cryptogram [4]

Danach wird der Klartext buchstabenweise von oben nach unten in vier Zeilen platziert, wobei die letzte Spalte eventuell nicht vollständig gefüllt ist.

Zeile 1	D I I H E X
Zeile 2	I S N E R T
Zeile 3	E T G I T
Zeile 4	S E E M E

Die Verschlüsselung erfolgt dann so, dass für jede Spalte zuerst das Bigramm DS mit den Buchstaben aus den Zeilen 1 und 4 und dann das Bigramm IE aus den beiden mittleren Zeilen mit der normalen Playfair-Chiffre verschlüsselt wird. Diese beiden Bigramme ergeben die Geheimtextbuchstaben EQ und AH, die in die Zeilen eingetragen werden, aus denen auch die Klartextbuchstaben stammen.

Nun kann der Sonderfall eintreten, dass das Bigramm aus zwei gleichen Buchstaben besteht. Dieser Fall tritt in diesem Beispiel in Spalte 5 ein, da sich in den beiden Zeilen 1 und 4 jeweils der Buchstabe E befindet. Da sich für die Playfair-Chiffre die beiden Buchstaben eines Bigramms unterscheiden müssen, muss auch bei diesem Verfahren ein Füllzeichen wie Y eingeschoben werden. Damit lautet der untere Buchstabe in dieser Spalte jetzt Y und die restlichen Buchstaben verschieben sich um eine Position.

Damit wird die Länge des Klartextes aber ungerade, sodass am Ende ein weiteres Füllzeichen angehängt werden muss.

Zeile 1	D I I H E X	D I I H E E
Zeile 2	I S N E R T	I S N E R X
Zeile 3	E T G I T	E T G I T T
Zeile 4	S E E M E	S E E M Y Y

Mit der Korrektur des Klartextes werden folgende Bigramme verschlüsselt:

DS	IE	IE	ST	IE	NG	HM	EI	EY	RT	EY	XT
EQ	AH	AH	TU	AH	TN	EO	HA	GX	CQ	GX	YS

Die mit der Playfair-Verschlüsselung erhaltenen Geheimtextbuchstaben müssen wieder vertikal in die zugehörigen Zeilen platziert werden.

Zeile 1	E A A E G G
Zeile 2	A T T H C Y
Zeile 3	H U N A Q S
Zeile 4	Q H H O X X

Abschließend liest man sie zeilenweise aus und aufgeteilt in Gruppen von jeweils fünf Buchstaben ergibt sich der Geheimtext. Durch die beiden Füllzeichen ist dieser um zwei Buchstaben länger als der Klartext.

Geheimtext	EAAEG GATTH CYHUN AQSQH HOXX

Als weiterer Sonderfall kann es geschehen, dass in der rechten Spalte des Klartextes nur die beiden oberen Zeilen einen Buchstaben enthalten. Dann wird aus ihnen ein Bigramm gebildet und die beiden verschlüsselten Geheimtextbuchstaben werden dennoch wie üblich in die beiden äußeren Zeilen 1 und 4 eingetragen.

5.3 Kruskal

Dieses trigraphische Verfahren orientiert sich am *Playfair*-Verfahren. Während dort mit Bigrammen ein Rechteck gebildet wird, werden hier Parallelogramme verwendet.[45]

Klartext	Dies ist ein geheimer Text
Schlüssel	TRIGRAPH

Mit dem Schlüssel wird zunächst ein gemischtes Alphabet erzeugt, das in eine 5 x 5 -Tabelle eingetragen wird.

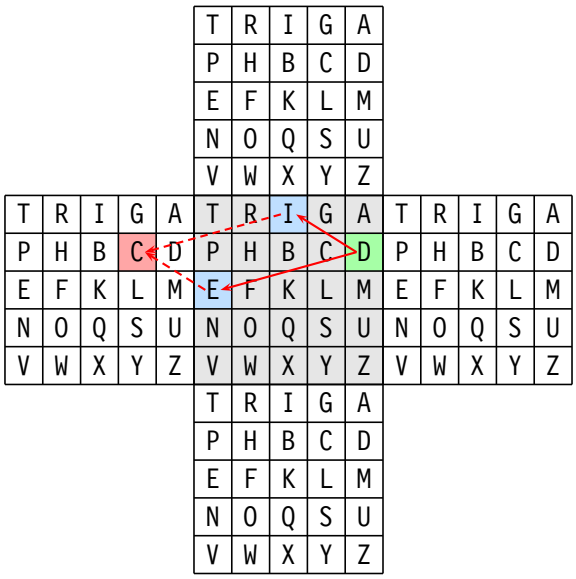
	0	1	2	3	4
0	T	R	I	G	A
1	P	H	B	C	D
2	E	F	K	L	M
3	N	O	Q	S	U
4	V	W	X	Y	Z

Der Klartext wird in Trigramme unterteilt, die der Reihe nach einzeln unabhängig voneinander verschlüsselt werden. Ist die Länge des Klartextes nicht durch 3 teilbar, muss er durch Füllzeichen verlängert werden.

Das erste Trigramm des Klartextes lautet DIE. Die Position des ersten Buchstabens D wird in der Tabelle bestimmt und die Verbindungen zu den beiden anderen Buchstaben gezogen, wobei die Tabelle bei Bedarf in alle Richtungen vervielfältigt werden kann. Diese beiden Linien

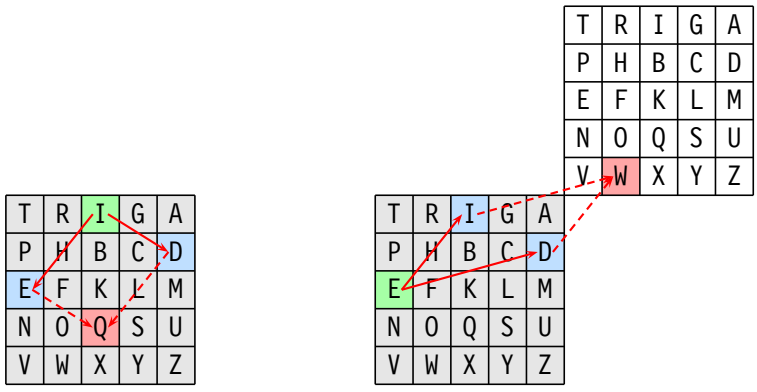
[45] Cryptologia [119]

werden zu einem Parallelogramm vervollständigt und die dem ersten Buchstaben D diagonal gegenüberliegende Ecke beinhaltet den ersten Geheimtextbuchstaben C.



a) DIE → C

Da ein solches Parallelogramm nur einen einzigen Geheimtextbuchstaben erzeugt, müssen die bisherigen Schritte noch zweimal wiederholt werden. Dazu werden die Buchstaben des Trigramms jeweils zyklisch gesehen um eine Position nach links verschoben, sodass der vordere Buchstabe immer ans Ende verschoben wird. Mit dem zugehörigen Parallelogramm werden dann zwei weitere Geheimtextbuchstaben bestimmt. Für das Trigramm DIE ergeben sich so die verschlüsselten Buchstaben CQW.



b) IED → Q c) EDI → W

Abb. 5.2: Verschlüsselung der drei Klartextbuchstaben DIE

Allerdings können Fälle eintreten, bei denen sich kein Parallelogramm erstellen lässt. Dann werden die drei Buchstaben eines Trigramms nach folgenden Sonderregeln verschlüsselt.

Fall 1) *Die drei Buchstaben des Klartextes liegen auf einer horizontal, vertikal oder schräg verlaufenden Linie mit jeweils fünf Buchstaben.*

Bei dieser Anordnung können zwei unterschiedliche Fälle auftreten.

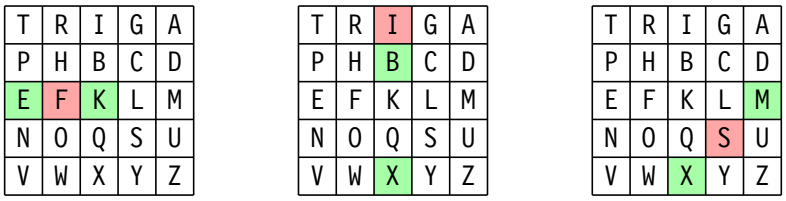
- Alle drei Buchstaben liegen in benachbarten Zellen, die auch zyklisch angeordnet sein können. Bei einer solchen Anordnung wird der mittlere Buchstabe als Sonderzeichen festgelegt und an der gleichen Position in das Trigramm des Geheimtextes eingefügt. In Abbildung 5.3 sind dies die Buchstaben `F`, `I` und `S`.

  Die Zuordnung der anderen beiden Buchstaben richtet sich nach den beiden unbenutzten Buchstaben der betreffenden Linie. Der unbenutzte Buchstabe, der nicht benachbart zu einem der zwei Klartextbuchstaben mit Ausnahme des Sonderzeichens ist, nimmt dessen Position im Geheimtext ein.

  In Abbildung 3a ist der Buchstabe `L` benachbart zu `K`, aber nicht zu `E`. Also wird es auf die durch den Buchstaben `E` festgelegte erste Position im Geheimtext platziert. Entsprechend ist der unbenutzte Buchstabe `M` nicht benachbart zu `K` und wird rechts im Geheimtext eingefügt.

  Der unbenutzte Buchstabe `K` in Abbildung 3b ist nicht benachbart zu `X` und wird daher am rechten Rand platziert, während `Q` nicht benachbart zu `B` ist und in die Mitte eingefügt wird.

  Im dritten Beispiel in Abbildung 3c erkennt man, dass `P` nicht benachbart zu `X` ist, während der zweite unbenutzte Buchstabe `R` benachbart zu `X`, aber nicht benachbart zu `M` ist. Damit sind deren Positionen im Geheimtext eindeutig bestimmt.



a) `EFK` → `LFM` b) `IBX` → `IQK` c) `XSM` → `PSR`

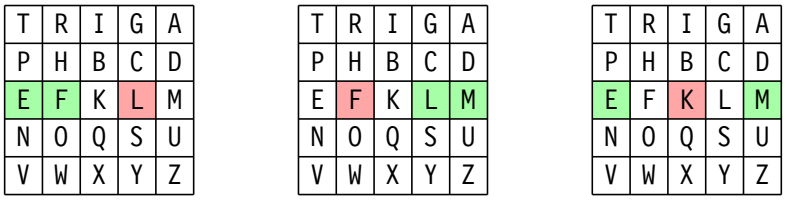
Abb. 5.3: Regel 1 - Drei benachbarte Buchstaben in einer Linie

- *Von den drei Buchstaben des Klartextes sind nur zwei benachbart und der dritte liegt isoliert zu diesen beiden Buchstaben.*

  Bei dieser Konstellation wird der isolierte Buchstabe als Sonderzeichen festgelegt und nimmt die gleiche Position im Trigramm des Geheimtextes ein. In den drei Tabellen aus Abbildung 5.4 sind `EF`, `LM` sowie `EM` benachbart, sodass `L`, `F` und `K` isoliert sind.

  Auch in diesem Fall bilden die beiden unbenutzten Buchstaben der Linie die beiden anderen Geheimtextzeichen. Im Unterschied zu Abbildung 5.3 ändern sich bei einem isolierten Sonderzeichen aber die Zuordnungen. Hier nimmt der unbenutzte Buchstabe, der zu einem der zwei Klartextbuchstaben mit Ausnahme des Sonderzeichens benachbart ist, dessen Position im Geheimtext ein.

In Abbildung 4a ist der unbenutzte Buchstabe K kein Nachbar von E, liegt aber neben F. Ebenso befindet sich der Buchstabe M entfernt von F, aber zyklisch gesehen neben E. Damit sind die beiden Positionen der unbenutzten Buchstaben dieser Linie im Geheimtext festgelegt.



a) EFL → MKL b) FLM → FKE c) EKM → FKL

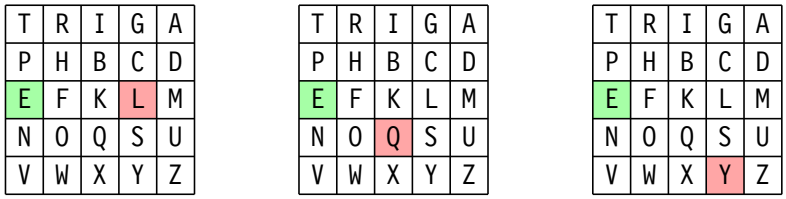
Abb. 5.4: Regel 2 - Drei Buchstaben in einer Linie mit einem isolierten Buchstaben

Fall 2) *Von den drei Buchstaben tritt ein Buchstabe doppelt auf.*

Bei diesen Anordnungen spielt es keine Rolle, ob sich die Buchstaben auf einer Linie befinden oder nicht. Der Einzelbuchstabe wird immer zweimal auf die Positionen des doppelt auftretenden Buchstabens kopiert.

Für den dritten Buchstaben des Geheimtextes wird die Bewegung vom Einzelbuchstaben zum Doppelbuchstaben bestimmt. Diese Bewegung wird dann auch mit dem Doppelbuchstaben als Startposition ausgeführt und man gelangt so zum dritten Geheimtextbuchstaben.

In Abbildung 5a muss sich von L ausgehend entweder um drei Positionen nach links oder um zwei Positionen nach rechts bewegen, um zu E zu gelangen. Führt man eine der beiden Bewegungen von E aus, erhält man K als dritten Geheimtextbuchstaben.



a) EEL → LLK b) EEQ → QQC c) EEY → YYI

Abb. 5.5: Regel 3 - ein Doppelbuchstabe und ein Einzelbuchstabe

Im mittleren Beispiel der Abbildung 5b muss man sich von Q ausgehend um eine Zeile nach oben und zwei Spalten nach links bewegen, um zu E zu gelangen. Mit dieser Bewegung landet man von E ausgehend bei C als dritten Geheimtextbuchstaben.

Mit diesem Vorgehen erhält man in Abbildung 5c den Buchstaben I, weil man sich um zwei Zeilen nach oben und drei Spalten nach links bewegen muss.

Fall 3) *Das Trigramm besteht aus drei gleichen Buchstaben.*

In diesem Fall wird einfach ein Füllzeichen eingefügt, sodass einer der schon beschriebenen Fälle eintritt. Damit verlängert sich die Länge des Klartextes.

Mit diesen Regeln kann der Klartext in Trigramme unterteilt werden und dann verschlüsselt werden.

```
DIE SIS TEI NGE HEI MER TEX TXX
CQW IDI KQL YIC HYU ITY BKS UTT
```

Aufgeteilt in Gruppen mit jeweils fünf Buchstaben ergibt sich abschließend der Geheimtext.

Geheimtext	CQWID IKQLY ICHYU ITYBK SUTT

Algebraische Methode

Die Geheimtextbuchstaben lassen sich auch sehr einfach algebraisch berechnen, ohne dass man die vielen unterschiedlichen Fälle der geometrischen Anordnungen beachten muss.

	0	1	2	3	4
0	T	R	I	G	A
1	P	H	B	C	D
2	E	F	K	L	M
3	N	O	Q	S	U
4	V	W	X	Y	Z

Für die Buchstaben des ersten Trigramms DIE des Klartextes werden die Koordinaten aus der Tabelle bestimmt. Der erste Buchstabe D besitzt die Koordinaten $k_1 = (1,4)$, der Buchstabe I findet sich auf Position $k_2 = (0,2)$ und E auf $k_3 = (2,0)$. Aus diesen Koordinaten k_1, k_2 und k_3 können direkt die Koordinaten der zugehörigen Geheimtextbuchstaben berechnet werden.

$$\begin{aligned} g_1 &= -k_1 + k_2 + k_3 \\ g_2 &= k_1 - k_2 + k_3 \\ g_3 &= k_1 + k_2 - k_3 \end{aligned}$$

In diesem Beispiel liefert die Berechnung:

$$\begin{aligned} g_1 &= -(1,4) + (0,2) + (2,0) = (-1+0+2, -4+2+0) = (1,-2) \equiv (1,3) \\ g_2 &= (1,4) - (0,2) + (2,0) = (1-0+2, 4-2+0) = (3,2) \\ g_3 &= (1,4) + (0,2) - (2,0) = (1+0-2, 4+2-0) = (-1,6) \equiv (4,1) \end{aligned}$$

Die so berechneten Koordinaten ergeben mit der Tabelle die Geheimtextbuchstaben CQW.

Auch die Sonderfälle werden mit diesen Formeln abgedeckt, wie etwa an den Beispielen der nachfolgenden Trigramme zu erkennen ist, bei denen ein Buchstabe doppelt auftritt und drei Buchstaben auf einer Linie liegen.

g_1	=	$-(3,3)+(0,2)+(3,3)$	$\equiv$	$(0,2)$		g_1	=	$-(1,1)+(2,0)+(0,2)$	$\equiv$	$(1,1)$
g_2	=	$+(3,3)-(0,2)+(3,3)$	$\equiv$	$(1,4)$		g_2	=	$+(1,1)-(2,0)+(0,2)$	$\equiv$	$(4,3)$
g_3	=	$+(3,3)+(0,2)-(3,3)$	$\equiv$	$(0,2)$		g_3	=	$+(1,1)+(2,0)-(0,2)$	$\equiv$	$(3,4)$
a) SIS $\rightarrow$ IDI						b) HEI $\rightarrow$ HYU				

Abb. 5.6: Berechnungen von weiteren Geheimtextbuchstaben

Nur bei drei Buchstaben muss wie bei der grafischen Lösung ein Füllzeichen eingefügt werden, da sonst auch die Geheimtextbuchstaben übereinstimmen. Die Verschlüsselung mit der einfach durchzuführenden algebraischen Berechnung liefert sehr schnell den identischen Geheimtext.

DIE	SIS	TEI	NGE	HEI	MER	TEX	TXX
CQW	IDI	KQL	YIC	HYU	ITY	BKS	UTT

5.4 Savard Trigraph

John Savard stellt in seinem kryptografischen Kompendium eine Variante der *Playfair*-Chiffre vor, die Trigramme verwendet.[46] Die Verschlüsselung ist so konzipiert, dass in ihr die grundlegenden Prinzipien der Playfair-Verschlüsselung realisiert worden sind.

Klartext	Dies ist ein geheimer Text
Schlüssel	SAVARDPLAYFAIR

Mit dem Schlüssel wird zunächst ein gemischtes Alphabet erzeugt, dessen Buchstaben in eine 5 x 5 -Tabelle eingetragen wird.

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

[46] Savard [172]

Bei allen Regeln sind die Bewegungen innerhalb der Tabelle zyklisch zu betrachten. Führt man am rechten Rand einen Schritt nach rechts aus, landet man in der ersten Spalte am linken Rand. Ebenso folgt nach dem unteren Rand die Zeile am oberen Rand.

Die Verschlüsselung der Buchstaben eines Trigramms erfolgt nach verschiedenen Regeln, die sich u.a. darin unterscheiden, wie viele gleiche Buchstaben im Trigramm vorkommen. Ist die Länge des Klartexts nicht durch 3 teilbar, muss er um Füllzeichen verlängert werden.

- Wenn alle drei Buchstaben gleich sind, werden sie durch den Buchstaben ersetzt, der sich eine Spalte weiter rechts und eine Zeile tiefer befindet.

YYY → GGG

S	A	V	R	D
P	L	**Y**	F	I
B	C	E	**G**	H
J	K	M	N	O
T	U	W	X	Z

III → BBB

S	A	V	R	D
P	L	Y	F	**I**
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

XXX → DDD

S	A	V	R	**D**
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	**X**	Z

- Sind zwei Buchstaben gleich, werden die beiden unterschiedlichen Buchstaben wie bei der normalen Playfair-Chiffre verschlüsselt. Damit ist gleichzeitig die Verschlüsselung des dritten Buchstaben festgelegt.

ILL → PYY

S	A	V	R	D
P	**L**	**Y**	F	**I**
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

CCU → KKA

S	**A**	V	R	D
P	L	Y	F	I
B	**C**	E	G	H
J	**K**	M	N	O
T	**U**	W	X	Z

YZY → IWI

S	A	V	R	D
P	L	**Y**	F	**I**
B	C	E	G	H
J	K	M	N	O
T	U	**W**	X	**Z**

Sind alle drei Buchstaben unterschiedlich, müssen für die Verschlüsselung insgesamt sechs unterschiedliche Regeln angewendet werden.

- Wenn alle drei Buchstaben in einer Zeile liegen, wird jeder Buchstabe durch seinen rech-

ten Nachbarn ersetzt.

JNK → KOM

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

CHB → EBC

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

- Wenn alle drei Buchstaben in einer Spalte liegen, wird jeder Buchstabe durch seinen unteren Nachbarn ersetzt.

YEM → EMW

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

LKU → CUA

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

- Zwei Buchstaben liegen in einer gemeinsamen Zeile und der dritte Buchstabe in einer der Spalten, in der sich auch einer der ersten beiden angeführten Buchstaben befindet:

  In diesem Fall wird der Buchstabe, der eine horizontale und vertikale Verbindung zu den anderen beiden Buchstaben besitzt, durch den Buchstaben ersetzt, der sich diesem Buchstaben im virtuellen Rechteck diagonal gegenüberliegt. Im linken Beispiel ist dies der Buchstabe `O`, der durch `L` ersetzt wird. Die anderen beiden Buchstaben `K` und `I` des

Trigramms werden vertauscht.

KOI → ILK

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

MVN → RNV

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

NFL → LKN

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

- Zwei Buchstaben befinden sich in einer gemeinsamen Spalte und der dritte Buchstabe in einer anderen Spalte und in keiner der beiden Zeilen der erstgenannten Buchstaben:

  Bei einer solchen Anordnung werden die Buchstaben des Trigramms durch die Buchstaben ersetzt, die in der gleichen Zeile, aber der anderen der beiden auftretenden Spalten liegt.

SJE → VMB

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

SOB → DJH

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

DFX → RIZ

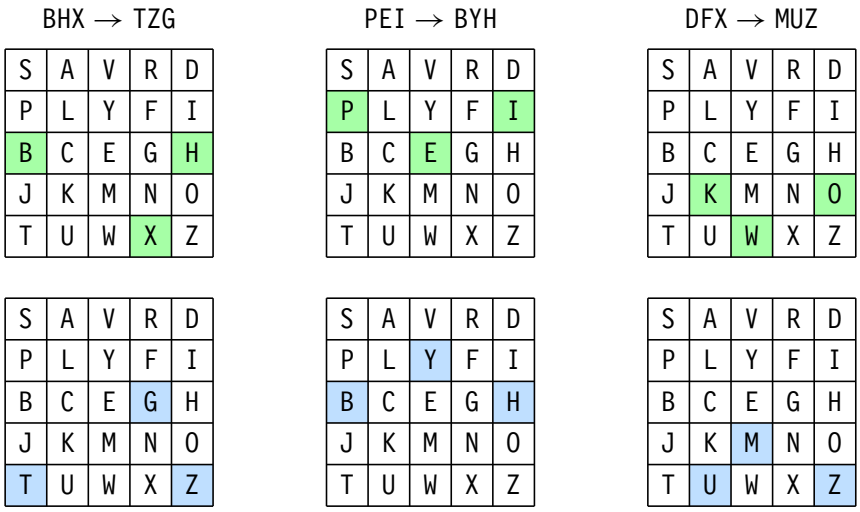
S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

S	A	V	R	D
P	L	Y	F	I
B	C	E	G	H
J	K	M	N	O
T	U	W	X	Z

- Zwei Buchstaben befinden sich in einer gemeinsamen Zeile und der dritte Buchstabe in einer anderen Zeile und in keiner der beiden Spalten der Buchstaben mit der gleichen Zeile:

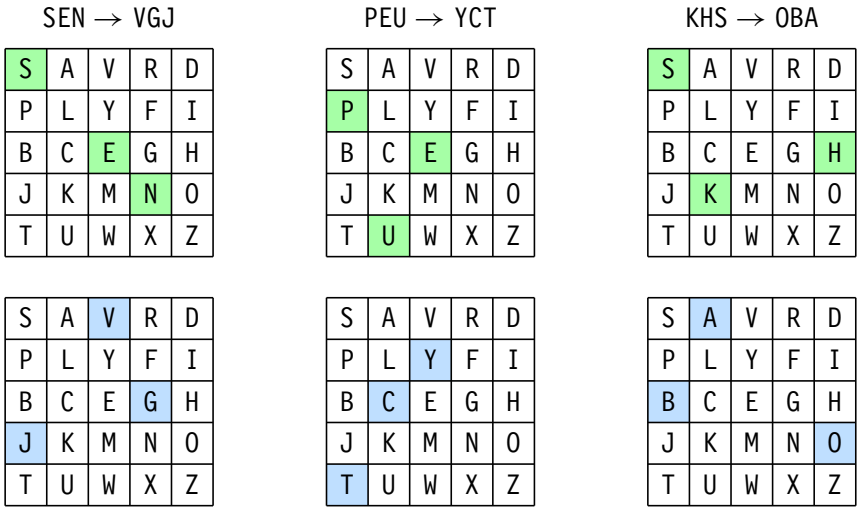
  Bei dieser Konstellation werden die Buchstaben des Trigramms durch die Buchstaben

ersetzt, die in der gleichen Spalte, aber der anderen der beiden auftretenden Zeilen liegen.



- Die drei Buchstaben besitzen weder eine gemeinsame Zeile noch eine gemeinsame Spalte:

  In diesem Fall werden sie jeweils durch den Buchstaben ersetzt, der in der gleichen Zeile, aber in der Spalte des nachfolgenden Buchstabens des Trigramms liegt. Dabei folgt nach dem dritten Buchstaben des Trigramms zyklisch gesehen wieder der erste.



Mit diesen umfangreichen Regeln ergeben sich für den Klartext die nachfolgenden Trigramme und deren Verschlüsselung.

DIE	SIS	TEI	NGE	HEI	MER	TEX	TXX
VYH	DPD	WHP	EMN	YIE	NGV	BWG	UZZ

Damit lautet der Geheimtext

Geheimtext	VYHDP DWHPE MNYIE NGVBW GUZZ

5.5 Five Square

Eine Variante der *Two Square*-Chiffre arbeitet mit fünf Quadraten, die abwechselnd benutzt werden.[47]

Klartext	Dies ist ein geheimer Text
Schlüssel	FIVESQUARE RECHTS UNTEN LINKS OBEN

Eines der Quadrate liegt zentral und wird bei jedem Verschlüsselungsschritt benutzt, während die anderen vier Quadrate um das zentrale Quadrat herum angeordnet werden. Jedes dieser Quadrate besitzt ein eigenes Schlüsselwort und wird mit dem zugehörigen gemischten Alphabet horizontal gefüllt.

O	B	E	N	A
C	D	F	G	H
I	K	L	M	P
Q	R	S	T	U
V	W	X	Y	Z

L	I	N	K	S
A	B	C	D	E
F	G	H	M	O
P	Q	R	T	U
V	W	X	Y	Z

F	I	V	E	S
Q	U	A	R	B
C	D	G	H	K
L	M	N	O	P
T	W	X	Y	Z

R	E	C	H	T
S	A	B	D	F
G	I	K	L	M
N	O	P	Q	U
V	W	X	Y	Z

U	N	T	E	A
B	C	D	F	G
H	I	K	L	M
O	P	Q	R	S
V	W	X	Y	Z

Die Verschlüsselung der Buchstabenpaare des Klartextes wird immer mit dem zentralen Quadrat und einem der vier äußeren Quadrate durchgeführt. Man beginnt mit dem rechts danebenliegenden Quadrat und wechselt dann im Uhrzeigersinn zu den anderen Quadraten. Dabei ist zu beachten, dass der erste Buchstabe des Bigramms grundsätzlich im zentralen

[47] Cryptogram [133]

Quadrat und der zweite in einem der äußeren Quadrate gewählt wird. Die Geheimtextbuchstaben ergeben sich dann mit den Regeln des *Two Square*-Verfahrens.

Das erste Bigramm DI wird also mit dem zentralen und dem rechten Quadrat verschlüsselt. Da sich die beiden Buchstaben in der gleichen Zeile befinden, werden sie einfach nur umgedreht. Mit dem zweiten Bigramm ES lässt sich mit dem zentralen und dem unteren Quadrat ein virtuelles Rechteck bilden, aus dem die Geheimtextbuchstaben SR ausgelesen werden. Die weiteren Paare des Klartextes lassen sich dann entsprechend verschlüsseln.

	DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
rechts	ID				RM				RE		
unten		SR				HT				YU	
links			SI				OR				YN
oben				XO				EK			
	ID	SR	SI	XO	RM	HT	OR	EK	RE	YU	YN

Der mit unterschiedlichen Quadraten gebildete Geheimtext lässt sich dann der Reihe nach zusammensetzen.

Geheimtext	IDSRS	IXORM	HTORE	KREYU	YN

5.6 Four Square numerisch

Eine Variante der *Four Square*-Chiffre benutzt dem Namen nach vier Quadrate, von denen zwei mit Buchstaben und die anderen beiden mit Zahlen gefüllt sind.[48]

Klartext	D	i	e	s		i	s	t		e	i	n		g	e	h	e	i	m	e	r		T	e	x	t
Schlüssel	F	O	U	R	S	Q	U	A	R	E	N	U	M	E	R	I	S	C	H						

Die Quadrate werden so angeordnet, dass das links oben und das rechts unten liegende Quadrat Buchstaben beinhalten. Beiden Quadrate sind unterschiedliche Schlüsselworte zugeordnet und die mit ihnen gebildeten gemischten Alphabete werden horizontal eingetragen. Die beiden anderen Quadrate werden systematisch mit Zahlenfolgen gefüllt, die beide bei 0 beginnen. Rechts oben findet sich eine arithmetische Folge mit der Schrittweite 25. Bei dem Quadrat links unten beträgt die Schrittweite dagegen 1, sodass sich dort außer der Zahl 0 die

[48] Basic Cryptography [206] S. 142-143, Cryptogram [87], Cryptogram [88]

natürlichen Zahlen bis einschließlich 24 befinden.

F	O	U	R	S
Q	A	E	B	C
D	G	H	I	K
L	M	N	P	T
V	W	X	Y	Z

0	25	50	75	100
125	150	175	200	225
250	275	300	325	350
375	400	425	450	475
500	525	550	575	600

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24

N	U	M	E	R
I	S	C	H	A
B	D	F	G	K
L	O	P	Q	T
V	W	X	Y	Z

Abb. 5.7: Tabellen für die *Four Square*-Variante mit Zahlen

Die Verschlüsselung geschieht dann prinzipiell wie beim *Four Square*-Verfahren, nur dass sich hier in den beiden anderen Ecken der virtuellen Rechtecke Zahlen befinden. Für das Bigramm AG ergeben sich etwa zunächst die Zahlen 200 und 11 und hieraus die Summe 211.

F	O	U	R	S
Q	A	E	B	C
D	G	H	I	K
L	M	N	P	T
V	W	X	Y	Z

0	25	50	75	100
125	150	175	200	225
250	275	300	325	350
375	400	425	450	475
500	525	550	575	600

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24

N	U	M	E	R
I	S	C	H	A
B	D	F	G	K
L	O	P	Q	T
V	W	X	Y	Z

Abb. 5.8: AG $\rightarrow 200 + 11 = 211$

Der Klartext wird verschlüsselt, indem für alle Bigramme die entsprechenden Summen aus den gebildeten Rechtecken berechnet werden. Da es für die Entschlüsselung äußerst wichtig

ist, dass alle Zahlen aus drei Ziffern bestehen, müssen bei Summen kleiner als 100 führende Nullen hinzugefügt werden.

DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
250 5	150 7	275 8	450 4	250 3	325 1	325 2	300 3	225 2	450 4	600 17
255	157	283	454	253	326	327	303	227	454	617

Diese Zahlen werden dann für den Geheimtext nur noch zusammengefügt.

Geheimtext	25515	72834	54253	32632	73032	27454	617

6 Fragmentierte Verfahren

6.1 Bifid Varianten

6.1.1 Bifid mit unterschiedlich großen Blöcken

Wie das normale Bifid-Verfahren verwendet diese Chiffre ein Polybius-Quadrat und einen festgelegten Schlüssel wie etwa BIFIDBLOECKE.[49]

Klartext	Dies ist ein geheimer Text
Schlüssel	BIFIDBLOECKE 4352

Das zugehörige gemischte Alphabet wird horizontal in das Quadrat eingetragen.

	1	2	3	4	5
1	B	I	F	D	L
2	O	E	C	K	A
3	G	H	M	N	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Die Koordinaten der Klartextbuchstaben werden wie bei Bifid untereinander geschrieben, doch werden sie bei dieser Variante in Blöcke mit unterschiedlichen Längen unterteilt. Als zweiter Schlüssel ist festgelegt worden, dass der erste Block vier Ziffern umfasst, der zweite drei, der dritte Block fünf Ziffern und der vierte zwei. Werden weitere Blöcke benötigt, werden diese Blockgrößen periodisch wiederholt. Wie beim normalen Bifid werden die Ziffern dieser Gruppen dann von oben nach unten und von links nach rechts zusammengefasst.

Klartext	DIES	IST	EINGE	HE	IMER	TEX	T
Zeile	1124	144	21332	32	1324	425	4
Spalte	4223	234	22412	22	2322	423	4
	11244223	144234	2133222412	3222	13242322	425423	44

Abschließend wird diese Ziffernfolge in Paare unterteilt, die mithilfe des Polybios-Quadrates in die Buchstaben des Geheimtextes umgewandelt werden.

paarweise	11	24	42	23	14	42	34	21	33	22	24	12	32	22	13	24	23	22	42	54	23	44
	B	K	R	C	D	R	N	O	M	E	K	I	H	E	F	K	C	E	R	Y	C	T
Geheimtext	BKRCD RNOME KIHEF KCERY CT																						

[49] Rubin [164] S. 113

Frank Rubin hat ein subjektives Bewertungssystem für die Stärke von Verschlüsselungsverfahren entworfen, bei dem er Stufen von 1 bis 10 verwendet. Als Grundlage verwendet er aus seiner Erfahrung den Aufwand, die Verfahren mit bekannten Methoden zu knacken, und den Vergleich der Chiffren untereinander.

Stufe 1 steht für Chiffren, die von einem Anfänger ohne Vorkenntnisse mit Papier, Bleistift und mäßigem Aufwand geknackt werden können, und etwa Stufe 3 für Chiffren, die von einem erfahrenen Hobby-Kryptologen allein mit Papier und Bleistift geknackt werden können. Für Chiffren der Stufen 4 und 5 ist schon ein Computer oder ein ausgebildeter Kryptologe oder beides erforderlich. Ab Stufe 6 muss die Rechenkraft des Computers höher sein und es wird zusätzlich spezielles Fachwissen erforderlich.

Während er das normale Bifid-Verfahren der Stufe 3 zuordnet, hält er diese irreguläre Variante für deutlich stärker und ordnet sie in Stufe 6 ein.

6.1.2 Bifid diagonal

In einer weiteren Bifid-Variante werden die Zwischencodes des Polybios-Quadrates fragmentiert, indem diagonal auftretende Ziffern kombiniert werden.[50]

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`DIAGONAL`

Zunächst wird ein Polybios-Quadrat mit dem Schlüssel `DIAGONAL` erstellt.

	1	2	3	4	5
1	D	I	A	G	O
2	N	L	B	C	E
3	F	H	J	K	M
4	P	R	S	T	U
5	V	W	X	Y	Z

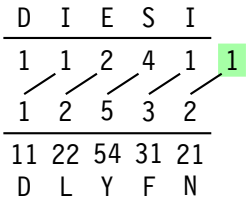
Wie beim normalen Bifid werden mit diesem Polybios-Quadrat die Koordinaten jedes Buchstabens untereinander platziert und in Gruppen einer festgelegten Länge unterteilt.

Klartext	DIESI	STEIN	GEHEI	MERTE	XT
Zeile	11241	44212	12321	32442	54
Spalte	12532	34521	45252	55245	34

Nun werden allerdings die Ziffern in diesen Gruppen unterschiedlich zusammengefasst, um die Fragmentierung zu verstärken. Die erste Ziffer der oberen Teilgruppe wird am Ende noch

[50] Rubin [164] S. 114

einmal eingefügt, während die unteren Ziffern unverändert bleiben, wie am Beispiel der beiden linken Teilgruppen zu erkennen ist. Danach werden jeweils die Diagonalen von einer der unteren Ziffern zu der Ziffer der darüberstehenden Teilgruppe gezogen, die sich eine Position weiter rechts befindet. Die durch die Diagonalen festgelegten Ziffern werden dann abschließend mithilfe des Polybios-Quadrates in Buchstaben umgewandelt.



Insgesamt ergibt sich dann aus diesen Bigrammen der Geheimtext.

diagonal	11	22	54	31	21	34	42	51	22	14	42	53	22	51	21	52	54	24	42	53	34	45
	D	L	Y	F	N	K	R	V	L	G	R	X	L	V	N	W	Y	C	R	X	K	U
Geheimtext	DLYFN KRVLG RXLVN WYCRX KU																					

Frank Rubin erachtet diese Variante als etwas stärker im Vergleich zur normalen Variante und ordnet sie in seinem Bewertungssystem in Stufe 4 ein.

6.1.3 Bifid horizontal

Im Gegensatz zu der diagonalen Variante, werden die Ziffern in den Teilgruppen hier horizontal verändert.[51]

Klartext	Dies ist ein geheimer Text
Schlüssel	HORIZONTAL 3 7

Auch bei dieser Variante wird zunächst ein Polybios-Quadrat mit dem Schlüssel HORIZONTAL erstellt.

	1	2	3	4	5
1	H	O	R	I	Z
2	N	T	A	L	B
3	C	D	E	F	G
4	J	K	M	P	S
5	U	V	W	X	Y

[51] Rubin [164] S. 113

Die Koordinaten jedes Buchstabens des Polybios-Quadrates werden auch bei dieser Variante in Teilgruppen untereinander platziert und in Gruppen einer festgelegten Länge unterteilt.

Klartext	DIESI	STEIN	GEHEI	MERTE	XT
Zeile	31341	42312	33131	43123	52
Spalte	24354	52341	53134	33323	42

Auch der dritte Schritt unterscheidet sich noch nicht vom normalen Bifid, da die oberen und unteren Teilgruppen jeweils zusammengefasst werden. Doch danach folgt eine Maßnahme, die die Fragmentierung der Ziffern verstärkt. Die Ziffern werden innerhalb der soeben gebildeten Gruppen zyklisch nach links verschoben. In diesem Beispiel mit zwei festgelegten Verschiebungszahlen geschieht das immer abwechselnd. Sind dagegen noch mehr Zahlen festgelegt worden, werden die Verschiebungen periodisch vorgenommen.

Gruppe 1 (3)	3134124354	⟶	4124354313
Gruppe 2 (7)	4231252341	⟶	3414231252
Gruppe 3 (3)	3313153134	⟶	3153134331
Gruppe 4 (7)	4312333323	⟶	3234312333
Gruppe 5 (3)	5242	⟶	2524

Aus der so veränderten Ziffernfolge können dann jeweils zwei Ziffern mithilfe des Polybios-Quadrates in Buchstaben umgewandelt werden und bilden den Geheimtext.

	41	24	35	43	13	34	14	23	12	52	31	53	13	43	31	32	34	31	23	33	25	24
	J	L	G	M	R	F	I	A	O	V	C	W	R	M	C	D	F	C	A	E	B	L
Geheimtext	JLGMR		FIAOV		CWRMC		DFCAE		VK													

Diese Variante ist deutlich stärker als die diagonale Variante, sodass Frank Rubin sie in seinem Bewertungssystem in Stufe 6 einordnet.

6.1.4 Bifid mit zwei Tabellen

Um die Stärke einer Verschlüsselung mit Bifid zu erhöhen, können auch zwei Quadrate verwendet werden.[52]

Klartext	Dies ist ein geheimer Text
Schlüssel	ERSTETABELLE ZWEITETABELLE

[52] Rubin [164] S. 105

Jedes der beiden Quadrate sollte dabei mit einem eigenen Schlüssel erstellt werden.

	1	2	3	4	5
1	E	R	S	T	A
2	B	L	C	D	F
3	G	H	I	K	M
4	N	O	P	Q	U
5	V	W	X	Y	Z

	1	2	3	4	5
1	Z	W	E	I	T
2	A	B	L	C	D
3	F	G	H	K	M
4	N	O	P	Q	R
5	S	U	V	X	Y

Für die Verschlüsselung wird der Klartext in Bigramme unterteilt, die mit einem der beiden Polybios-Quadrate verschlüsselt werden. Welches Quadrat dabei benutzt wird, richtet sich nach dem numerischen Schlüssel, der aus den ersten zehn Ziffern des ersten Schlüsselwortes erstellt wird. Ist dieses kürzer, können die fehlenden Ziffern entweder periodisch oder, wie in diesem Beispiel, mit einem fortlaufenden Schlüssel erzeugt werden. Wie häufig bei numerischen Schlüsseln, wird auch hier die Zahl 10 durch die Ziffer 0 repräsentiert.

Schlüssel	E	R	S	T	E	T	A	B	E	L
numerisch	3	7	8	9	4	0	1	2	5	6
fortlaufend	3	7	8	9	4	0	1	2	5	6	0

Um sicherzustellen, dass beide Verschlüsselungen gleich häufig verwendet werden, wird das erste Quadrat benutzt, wenn die zugehörige Ziffer des numerischen Schlüssels kleiner als fünf ist, und sonst das zweite Quadrat. Da Bigramme verschlüsselt werden, kann die Blockgröße nicht wie beim normalen Bifid beliebig gewählt werden, sondern beträgt immer 2.

Klartext	DI	ES	IS	TE	IN	GE	HE	IM	ER	TE	XT
	3	7	8	9	4	0	1	2	5	6	0
Quadrat 1	CP				KG	GE	GB	IM			VK
Quadrat 2		TF	TN	ZV					IM	ZV	

Abschließend müssen die erhaltenen Buchstaben nur noch zum Geheimtext zusammengefügt werden.

Geheimtext	CPTFT	NZVKG	GEGBI	MIMZV	VK

6.2 Kliger

Im Jahr 1980 veröffentlichte der Kryptologe Frank Rubin ein mathematisches Verschlüsselungsverfahren, das von Albert Kliger stammt und ihm zugesandt worden war.[53] Die exakte

[53] Cryptogram [165], Cryptogram [192]

mathematische Zahlentheorie soll nicht im Detail formuliert, sondern nur der zentrale Begriff *Primitivwurzel* verständlich erklärt werden, soweit es für das Verständnis des Verfahrens erforderlich ist. Zusätzlich wird eine weitere Einschränkung vorgenommen, da für das Verfahren nur Primzahlen betrachtet werden.

> Sei p eine Primzahl. Dann heißt $m \in \mathbb{Z}$ *Primitivwurzel* modulo p genau dann, wenn
> $$\left\{m^x \mid x = 1,2,\ldots,p-1\right\} = \left\{1,2,\ldots,p-1\right\}$$

Die zentrale Eigenschaft einer Primitivwurzel m modulo p ist also, dass jedes Element der Menge $\{1,2,\ldots,p-1\}$ als Potenz der Primitivwurzel dargestellt werden kann. Ist m eine Primitivwurzel modulo p, so bezeichnet man für die Zahlen $x \in \{1,2,\ldots,p-1\}$ die eindeutige Lösung der Gleichung $c = m^x \mod p$ mit $x = \log_m c$ als *diskreten Logarithmus*.

Um festzustellen, ob etwa $m = 5$ eine Primitivwurzel von $p = 7$ ist, muss man nacheinander die Potenzen $5^x \mod 7$ für alle Exponenten $\{1,2,3,4,5,6\}$ berechnen.

$5^1 = 5^0 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \equiv 5$	$4^1 = 4^0 \cdot 4 \equiv 1 \cdot 4 \equiv 4 \equiv 4$
$5^2 = 5^1 \cdot 5 \equiv 5 \cdot 5 \equiv 25 \equiv 4$	$4^2 = 4^1 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \equiv 2$
$5^3 = 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6$	$4^3 = 4^2 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1$
$5^4 = 5^3 \cdot 5 \equiv 6 \cdot 5 \equiv 30 \equiv 2$	
$5^5 = 5^4 \cdot 5 \equiv 2 \cdot 5 \equiv 10 \equiv 3$	
$5^6 = 5^5 \cdot 5 \equiv 3 \cdot 5 \equiv 15 \equiv 1$	

Da alle Zahlen $\{1,2,\ldots,p-1\}$ als Ergebnis auftreten, ist 5 eine Primitivwurzeln modulo 7. Ab dem Exponenten 7 wiederholen sich alle Ergebnisse, was an dem letzten Ergebnis $5^6 \equiv 1$ zu erkennen ist. Die Zahl $m = 4$ ist dagegen keine Primitivwurzel modulo 7, da nur drei unterschiedliche Ergebnisse auftreten.

Untersucht man für $p = 7$ alle Zahlen $1 \leq m \leq 6$, erhält man

m^1	m^2	m^3	m^4	m^5	m^6	o(x)
1						1
2	4	1				3
3	2	6	4	5	1	6
4	2	1				3
5	4	6	2	3	1	6
6	1					2

Diese Tabelle zeigt, dass die Ordnung o(x), also die Anzahl der unterschiedlichen Ergebnisse, für $m = 3$ und $m = 5$ gleich $p - 1 = 6$ ist. Daher sind nur diese beiden Zahlen Primitivwurzeln modulo 7.

Es lässt sich beweisen, dass für jede Primzahl p eine Primitivwurzel modulo p existiert. Ta-

belle 6.1 zeigt die Primitivwurzeln bis 23.

m	Primitivwurzeln modulo m
2	1
3	2
5	2 3
7	3 5
11	2 6 7 8
13	2 6 7 11
17	3 5 6 7 10 11 12 14
19	2 3 10 13 14 15
23	5 7 10 11 14 15 17 19 20 21

Tab. 6.1: Primitivwurzeln für Primzahlen bis 23

Das Verschlüsselungsverfahren von Kliger benutzt Primitivwurzeln für die Codierung der Buchstaben. Da mindestens 26 unterschiedliche Ergebnisse für die Zuordnung zu den Buchstaben auftreten müssen, sind erst Primzahlen ab 29 für die Verschlüsselung geeignet.

m^1	m^2	m^3	m^4	m^5	m^6	m^7	m^8	m^9	m^{10}	m^{11}	m^{12}	m^{13}	m^{14}	m^{15}	m^{16}	m^{17}	m^{18}	m^{19}	m^{20}	m^{21}	m^{22}	m^{23}	m^{24}	m^{25}	m^{26}	m^{27}	m^{28}	o(x)
1																												1
2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21	13	26	23	17	5	10	20	11	22	15	1	**28**
3	9	27	23	11	4	12	7	21	5	15	16	19	28	26	20	2	6	18	25	17	22	8	24	14	13	10	1	**28**
4	16	6	24	9	7	28	25	13	23	5	20	22	1															14
5	25	9	16	22	23	28	24	4	20	13	7	6	1															14
6	7	13	20	4	24	28	23	22	16	9	25	5	1															14
7	20	24	23	16	25	1	7	20	24	23	16	25	1															7
8	6	19	7	27	13	17	20	15	4	3	24	18	28	21	23	10	22	2	16	12	9	14	25	26	5	11	1	**28**
9	23	4	7	5	16	28	20	6	25	22	24	13	1															14
10	13	14	24	8	22	17	25	18	6	2	20	26	28	19	16	15	5	21	7	12	4	11	23	27	9	3	1	**28**
11	5	26	25	14	9	12	16	2	22	10	23	21	28	18	24	3	4	15	20	17	13	27	7	19	6	8	1	**28**
12	28	17	1																									4
13	24	22	25	6	20	28	16	5	7	4	23	9	1															14
14	22	18	20	19	5	12	23	3	13	8	25	2	28	15	7	11	9	10	24	17	6	26	16	21	4	27	1	**28**
15	22	11	20	10	5	17	23	26	13	21	25	27	28	14	7	18	9	19	24	12	6	3	16	8	4	2	1	**28**
16	24	7	25	23	20	1																						7
17	28	12	1																									4
18	5	3	25	15	9	17	16	27	22	19	23	8	28	11	24	26	4	14	20	12	13	2	7	10	6	21	1	**28**
19	13	15	24	21	22	12	25	11	6	27	20	3	28	10	16	14	5	8	7	17	4	18	23	2	9	26	1	**28**
20	23	25	7	24	16	1																						7
21	6	10	7	2	13	12	20	14	4	26	24	11	28	8	23	19	22	27	16	17	9	15	25	3	5	18	1	**28**
22	20	5	23	13	25	28	7	9	24	6	16	4	1															14
23	7	16	20	25	24	1																						7
24	25	20	16	7	23	1																						7
25	16	23	24	20	7	1																						7
26	9	2	23	18	4	17	7	8	5	14	16	10	28	3	20	27	6	11	25	12	22	21	24	15	13	19	1	**28**
27	4	21	16	26	6	17	24	10	9	11	7	15	28	2	25	8	13	3	23	12	5	19	20	18	22	14	1	**28**
28	1																											2

Tab. 6.2: Potenzen m^x für $1 \leq m,x \leq 28$ und $p = 29$

Die Berechnung der Potenzen in Tabelle 6.2 zeigt, dass für $p = 29$ insgesamt zwölf Primitivwurzeln existieren. Tabelle 6.3 gibt für die ersten zehn Primzahlen, die größer als 26 und damit für die Verschlüsselung geeignet sind, die Primitivwurzeln an.

m	Primitivwurzeln modulo m
29	2 3 8 10 11 14 15 18 19 21 26 27
31	3 11 12 13 17 21 22 24
37	32 2 35 5 13 15 17 18 19 20 22 24
41	6 7 11 12 13 15 17 19 22 24 26 28 29 30 34 35
43	33 34 3 5 12 18 19 20 26 28 29 30
47	5 10 11 13 15 19 20 22 23 26 29 30 31 33 35 38 39 40 41 43 44 45
53	2 3 5 8 12 14 18 19 20 21 22 26 27 31 32 33 34 35 39 41 45 48 50 51
59	2 6 8 10 11 13 14 18 23 24 30 31 32 33 34 37 38 39 40 42 43 44 47 50 52 54 55 56
61	2 6 7 10 17 18 26 30 31 35 43 44 51 54 55 59
67	2 7 11 12 13 18 20 28 31 32 34 41 44 46 48 50 51 57 61 63

Tab. 6.3: Primitivwurzeln für die Primzahlen von 29 bis 67

Da sich jede Primzahl mit einer zugehörigen Primitivwurzel als Schlüssel für das Verfahren benutzen lässt, ergibt sich theoretisch eine unendliche Anzahl von Schlüsseln. Sollen aber die Klartextbuchstaben durch zweistellige Zifferncodes verschlüsselt werden, eignen sich nur die Primzahlen bis 100.

Im dargestellten Beispiel werden die kleinste geeignete Primzahl $p = 29$ und die Primitivwurzel $m = 11$ für die Verschlüsselung gewählt.

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`29 11`

Unabhängig von den gewählten Schlüsseln werden den Buchstaben zunächst die Zahlen von 1 bis 26 zugeordnet.

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	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

Danach wird der Klartext durch die festgelegten Zahlencodes umgeformt.

D	I	E	S		I	S		T	E	I	N		G	E	H	E	I	M	E	R		T	E	X	T
4	9	5	19		9	19		20	5	9	14		7	5	8	5	9	13	5	18		20	5	24	20

Die endgültige Verschlüsselung erfolgt über den diskreten Logarithmus, also den Exponenten der Potenz m^x, bei dem der den Buchstaben zugeordnete Zahlencode auftritt. Für $p = 29$ und $m = 11$ ergeben sich die Potenzen aus Tabelle 6.4. Natürlich treten bei den Potenzen auch

Zahlen größer als 26 als Ergebnis auf. Da diese aber nicht als Zahlencodes der Buchstaben auftreten, spielen sie keine Rolle bei der Bestimmung der Geheimtextcodes.

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	27	28
11	5	26	25	14	9	12	16	2	22	10	23	21	28	18	24	3	4	15	20	17	13	27	7	19	6	8	1

Tab. 6.4: Potenzen 11^x für $p = 29$

Der erste Klartextbuchstabe D besitzt den Zahlencode 4, der als Ergebnis der Potenz 11^{18} auftritt. Damit ist 18 der zugehörige Geheimtextcode. Der zweite Buchstabe I mit dem Zahlencode 9 tritt als Ergebnis der Potenz 11^6 auf. Da alle Codes zweistellig sein müssen, lautet dieser 06. Verfährt man so mit allen Buchstaben des Klartextes, ergibt sich der Geheimtext.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
4	9	5	19	9	19	20	5	9	14	7	5	8	5	9	13	5	18	20	5	24	20
18	06	02	25	06	25	20	02	06	05	24	02	27	02	06	22	02	15	20	02	16	20

Tab. 6.5: Verschlüsselung mit dem Verfahren von Kliger

Da der Klartext für Primzahlen kleiner als 100 mit zweistelligen Zahlen verschlüsselt wird, liegt es nahe, für den Geheimtext alle Zahlen $\{01,02,\ldots,99\}$ zu verwenden. Dies ist ohne Probleme möglich, da sich bei Primitivwurzeln die auftretenden Ergebnisse periodisch wiederholen. Für $p = 29$ bedeutet dies, dass für den diskreten Logarithmus der Geheimtextcode unter drei bis vier Codes beliebig gewählt werden kann. Die Differenz der zueinander gehörenden Codes ist immer ein Vielfaches von $p-1$. In diesem Beispiel betragen die Unterschiede jeweils 28 und die Verschlüsselung wird damit homophon.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96	97	98	99													

Tab. 6.6: Gleichwertige Codes für den Geheimtext

Der Geheimtext kann damit auch mit der Zahlenfolge aus Tabelle 6.7 verschlüsselt werden.

D	I	E	S	I	S	T	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T
4	9	5	19	9	19	20	5	9	14	7	5	8	5	9	13	5	18	20	5	24	20
74	90	02	81	90	53	76	86	06	05	24	86	27	30	06	22	02	43	76	58	44	20

Tab. 6.7: Homophone Verschlüsselung mit dem Verfahren von Kliger

Entschlüsselung

Für die Entschlüsselung geht man genau umgekehrt vor, wie an einem Beispiel für $p = 31$ und $m = 21$ dargestellt wird.

Geheimtext	42284 08603 90340 02898 02404 87028 79406 48200 1782
Schlüssel	31 21

Im ersten Schritt müssen für die Primitivwurzel $m = 21$ die 30 unterschiedlichen Ergebnisse der Potenzen m^x bestimmt werden.

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	27	28	29	30
21	7	23	18	6	2	11	14	15	5	12	4	22	28	30	10	24	8	13	25	29	20	17	16	26	19	27	9	3	1

Der Geheimtext wird zunächst in Gruppen von jeweils zwei Ziffern unterteilt und wegen $p = 31$ auf die Basiszahlen $\{1,2,\ldots,30\}$ reduziert. Dazu muss man von den gegebenen Geheimtextzahlen nur solange $p - 1 = 30$ subtrahieren, bis man zu einer Basiszahl gelangt.

Über den diskreten Logarithmus dieser Zahl gelangt man dann zu den zugeordneten Buchstaben.

42	28	40	86	03	90	34	00	28	98	02	40	48	70	28	79	40	64	82	00	17	82							
12	28	10	26	3	30	4	10	28	8	2	10	18	10	28	19	10	4	22	10	17	22							
4	9	5	19	23	1	18	5	9	14	7	5	8	5	9	13	5	18	20	5	24	20							
D	I	E	S	W	A	R	E	I	N	G	E	H	E	I	M	E	R	T	E	X	T							

Damit lautet der entschlüsselte Klartext

Klartext	Dies war ein geheimer Text

6.3 Zahlenschloss

Diese Verschlüsselung wurde 2020 in einer besonderen Ausgabe der *British National Cipher Challenge* vorgestellt und vielfach auch als *Combination-lock Cipher* bezeichnet. Es handelt sich um ein fragmentiertes Verfahren, das an ein Zahlenschloss bei Koffern oder Fahrrädern erinnert.[54]

Klartext	Dies ist ein geheimer Text
Schlüssel	364

[54] Classical Cryptography [104] Unit 165, British National Cipher Challenge [39]

Die Klartextbuchstaben A bis Z werden mit den Zahlen von 1 bis 26 codiert. Die Codes werden dann in das Zahlensystem zur Basis 3 umgewandelt, sodass drei Bits für die Darstellung ausreichen. Da Leerzeichen nicht aus dem Klartext entfernt werden, wird diesem die Zahl 0 zugeordnet. Zur besseren Darstellung werden Leerzeichen durch einen Unterstrich _ dargestellt.

_	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
0	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
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2
0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2
0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2

Tab. 6.8: Umwandlung in das Dreiersystem

Der Buchstabe E besitzt etwa die Kennzahl 5, die im Dreiersystem $(012)_3$ lautet.

$$5 = (012)_3 = 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0$$

Mit der Zuordnungstabelle 6.8 wird der Klartext verschlüsselt.

D	I	E	S	_	I	S	T	_	E	I	N	_	G	E	H	E	I	M	E	R	_	T	E	X	T
0	1	0	2	0	1	2	2	0	0	1	1	0	0	0	0	0	1	1	0	2	0	2	0	2	2
1	0	1	0	0	0	0	0	0	1	0	1	0	2	1	2	1	0	1	1	0	0	0	1	2	0
1	0	2	1	0	0	1	2	0	2	0	2	0	1	2	2	2	0	1	2	0	0	2	2	0	2

Tab. 6.9: Zugeordnete Ziffern

Nach der Codierung der Klartextbuchstaben mit den Ziffern des Dreiersystems kommt der Schlüssel 364 zur Anwendung. Die drei Ziffern des Schlüssels geben an, um wie viele Positionen die unteren drei horizontalen Ziffernfolgen aus Tabelle 6.9 nach rechts verschoben werden. Diese Verschiebungen werden zyklisch vorgenommen, d.h., die Ziffern am rechten Rand werden dabei nach vorne verschoben. In der oberen der drei Zeilen betrifft dies bei dem gewählten Schlüssel 364 die letzten Ziffern 022, in der mittleren Zeile die Ziffern 000120 und in der unteren Zeile die vier Ziffern 2202.

	D	I	E	S	_	I	S	T	_	E	I	N	_	G	E	H	E	I	M	E	R	_	T	E	X	T
3 ⟶	0	2	2	0	1	0	2	0	1	2	2	0	0	1	1	0	0	0	0	0	1	1	0	2	0	2
6 ⟶	0	0	0	1	2	0	1	0	1	0	0	0	0	0	0	1	0	1	0	2	1	2	1	0	1	1
4 ⟶	2	2	0	2	1	0	2	1	0	0	1	2	0	2	0	2	0	1	2	2	2	0	1	2	0	0

Tab. 6.10: Verschieben der Ziffernfolgen

Durch die drei Verschiebungen werden den Buchstaben des Klartextes neue Ziffern zugeordnet. Der erste Buchstabe D mit der Kennzahl 4 wurde zunächst durch die Ziffern 011 codiert.

Nach den Verschiebungen lauten die neuen Ziffern 002, die den Buchstaben B kennzeichnen.

Abschließend werden die neuen Ziffern aus Tabelle 6.10 wieder in Buchstaben zurückverwandelt.

0	2	2	0	1	0	2	0	1	2	2	0	0	1	1	0	0	0	0	0	1	1	0	2	0	2
0	0	0	1	2	0	1	0	1	0	0	0	0	0	0	1	0	1	0	2	1	2	1	0	1	1
2	2	0	2	1	0	2	1	0	0	1	2	0	2	0	2	0	1	2	2	2	0	1	2	0	0
B	T	R	E	P	_	W	A	L	R	S	B	_	K	I	E	_	D	B	H	N	O	D	T	C	U

Tab. 6.11: Verschlüsselung mit den verschobenen Ziffernfolgen

Damit lautet der Geheimtext

Geheimtext	BTREP _WALR SB_KI E_DBH NODTC U

Variante

Ein Teilnehmer der Challenge schlug eine Variante vor, bei der die Fragmentierung noch ausgeprägter vorgenommen wird.[55]

Hier muss der Klartext eine gerade Anzahl von Buchstaben enthalten, sodass er notfalls mit einem Füllzeichen verlängert wird. Zudem wird ein Schlüsselwort verwendet, das aus sechs Buchstaben besteht.

Klartext	Dies ist ein geheimer Text
Schlüssel	ENIGMA

Im ersten Schritt wird der Klartext in zwei Buchstabenfolgen unterteilt, deren Buchstaben gemäß Tabelle 6.8 codiert werden. Dabei werden die Kennzahlen der Buchstaben in das Dreiersystem umgewandelt und immer abwechselnd der linken und rechten Buchstabenfolge vertikal zugeordnet.

D	E	_	S	_	I	_	E	E	M	R	T	X		I	S	I	T	E	N	G	H	I	E	_	E	T
0	0	0	2	0	1	0	0	0	1	2	2	2		1	2	1	2	0	1	0	0	1	0	0	0	2
1	1	0	0	0	0	0	1	1	1	0	0	2		0	0	0	0	1	1	2	2	0	1	0	1	0
1	2	0	1	0	0	0	2	2	1	0	2	0		0	1	0	2	2	2	1	2	0	2	0	2	2

Tab. 6.12: Zugeordnete Ziffern

[55] Classical Cryptography [104] Unit 165

Zusätzlich werden auch den Buchstaben des Schlüssels die Kennzahlen aus dieser Tabelle zugeordnet.

E	N	I	G	M	A
5	14	9	7	13	1

Den ersten drei Buchstaben ENI des Schlüssels werden die Zahlen 5, 14 und 9, den hinteren Buchstaben die Zahlen 7, 13 und 1 zugeordnet. Diese Zahlen bestimmen die Größe der Verschiebungen der horizontalen Ziffernfolge, die sich aus der Codierung im Dreiersystem ergeben.

	D E _ S _ I _ E E M R T X		I S I T E N G H I E _ E T
5 ⟶	0 1 2 2 2 0 0 0 2 0 1 0 0	7 ⟶	0 0 1 0 0 0 2 1 2 1 2 0 1
14 ⟶	2 1 1 0 0 0 0 0 1 1 1 0 0	13 ⟶	0 0 0 0 1 1 2 2 0 1 0 1 0
9 ⟶	0 0 0 2 2 1 0 2 0 1 2 0 1	1 ⟶	2 0 1 0 2 2 2 1 2 0 2 0 2

Tab. 6.13: Verschieben der Ziffernfolgen

Nach den Verschiebungen werden die neuen Kombinationen von Ziffern aus Tabelle 6.13 wieder in Buchstaben zurückverwandelt.

0 1 2 2 2 0 0 0 2 0 1 0 0	0 0 1 0 0 0 2 1 2 1 2 0 1
2 1 1 0 0 0 0 0 1 1 1 0 0	0 0 0 0 1 1 2 2 0 1 0 1 0
0 0 0 2 2 1 0 2 0 1 2 0 1	2 0 1 0 2 2 2 1 2 0 2 0 2
F L U T T A _ B U D N _ A	B _ J _ E E Z P T L T C K

Tab. 6.14: Verschlüsselung mit den verschobenen Ziffernfolgen

Diese Buchstaben bilden aneinandergereiht zusammen den Geheimtext.

Geheimtext	FLUTT A_BUD N_AB_ J_EEZ PTLTC K

6.4 ASAC

Diese Verschlüsselung wurde auf der Webseite *Mystery Twister* veröffentlicht und stellt laut ihrem Entwickler eine Verbesserung der ADFGVX-Chiffre dar.[56] Sie erfolgt in drei Abschnitten:

1. Verschlüsselung mit einem Polybios-Quadrat

[56] ASAC [75]

2. Addition der Ziffern mit einer pseudozufälligen Ziffernfolge
3. Doppelte Spaltentransposition

Das Verfahren benutzt zwei 10 x 10 - Tabellen und benötigt für die umfangreichen Zwischenschritte mehrere Schlüssel.

Klartext	`Dies ist ein geheimer Text`
Schlüssel	`ASACVERSCHLUESSELUNG`
	`MATHEMATIK SUBTRAHEND SPALTEN TAUSCHEN`

Der erste Schlüssel kann wie in diesem Beispiel aus einem Wort, aber auch aus zwei Worten bestehen, die dann zusammengefasst werden. Die Länge muss genau 20 Buchstaben betragen. Ist der Schlüssel zu kurz, wird er periodisch verlängert. Ist er dagegen zu lang, wird er verkürzt.

Die erste Tabelle wird mit den Ziffern $0,1,\ldots,9$, dem Leerzeichen und den Buchstaben von `A` bis `Z` gefüllt. Um die Häufigkeiten der Vokale zu verschleiern, sind die Vokale `A`, `I`, `O` und `U`, doppelt vertreten, während `E` sogar viermal auftritt. Damit lautet die einzufügende Zeichenfolge

```
0123456789 AABCDEEEEFGHIIJKLMNOOPQRSTUUVWXYZ
```

Diese 44 Zeichen werden der Reihe nach horizontal so oft in die Tabelle eingefügt, bis diese vollständig gefüllt ist. Die zehn Spalten und Zeilen der Tabelle werden jeweils mit den Kennzahlen von 0 bis 9 versehen. Zusätzlich werden die Buchstaben des ersten Schlüsselwortes mit den 20 Buchstaben zuerst waagrecht und dann senkrecht zu den Kennzahlen hinzugefügt.

		0	1	2	3	4	5	6	7	8	9
		A	S	A	C	V	E	R	S	C	H
0	L	0	1	2	3	4	5	6	7	8	9
1	U		A	A	B	C	D	E	E	E	E
2	E	F	G	H	I	I	J	K	L	M	N
3	S	O	O	P	Q	R	S	T	U	U	V
4	S	W	X	Y	Z		A	A	B	C	D
5	E	E	E	E	E	F	G	H	I	I	J
6	L	K	L	M	N	O	O	P	Q	R	S
7	U	T	U	U	V	W	X	Y	Z		A
8	N	A	B	C	D	E	E	E	E	F	G
9	G	H	I	I	J	K	L	M	N	O	O

Abb. 6.1: Ausgangstabelle

Nach dem Einfügen der Buchstaben in die Ausgangstabelle werden die Zeilen und Spalten

in dieser Reihenfolge verschoben, wobei der Kennbuchstabe der Zeilen in den üblichen Zahlencode umgewandelt wird.

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
0	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

Abb. 6.2: Codierung der Buchstaben durch Zahlen

Dieser Zahlencode legt für jede Zeile fest, um wie viele Positionen die Zellen zyklisch nach rechts verschoben werden. Die obere Zeile besitzt den Kennbuchstaben L mit dem Zahlencode 11. Also werden in dieser Zeile alle Zellen um 11 Positionen verschoben, was bei zehn Spalten einer Verschiebung um eine Position entspricht.

Entsprechend geht man bei den Spalten vor, deren Buchstaben nach unten verschoben werden. Die rechte Spalte besitzt den Kennbuchstaben H mit dem Zahlencode 7. Damit werden alle Buchstaben in dieser Spalte um 7 Positionen nach unten verschoben.

		0	1	2	3	4	5	6	7	8	9
		A	S	A	C	V	E	R	S	C	H
0	L	9	0	1	2	3	4	5	6	7	8
1	U		A	A	B	C	D	E	E	E	E
2	E	K	L	M	N	F	G	H	I	I	J
3	S	P	Q	R	S	T	U	U	V	O	O
4	S	Y	Z		A	A	B	C	D	W	X
5	E	H	I	I	J	E	E	E	E	F	G
6	L	S	K	L	M	N	O	O	P	Q	R
7	U	T	U	U	V	W	X	Y	Z		A
8	N	E	F	G	A	B	C	D	E	E	E
9	G	K	L	M	N	O	O	H	I	I	J

a) Zeilen

		0	1	2	3	4	5	6	7	8	9
		A	S	A	C	V	E	R	S	C	H
0	L	9	L	1	A	O	O	U	I	E	O
1	U		Q	A	N	3	X	C	V	I	X
2	E	K	Z	M	2	C	C	E	D	7	G
3	S	P	I	R	B	F	O	O	E	E	R
4	S	Y	K		N	T	4	Y	P	I	A
5	E	H	U	I	S	A	D	D	Z	O	E
6	L	S	F	L	A	E	G	H	E	W	J
7	U	T	L	U	J	N	U	5	I	F	8
8	N	E	O	G	M	W	B	E	6	Q	E
9	G	K	A	M	V	B	E	H	E		J

b) Spalten

Abb. 6.3: Verschiebungen innerhalb der ersten Tabelle

Nach den Verschiebungen wird der Klartext inklusive der enthaltenen Leerzeichen verschlüsselt. Dazu wird jedem Buchstaben eine seiner möglichen Koordinaten aus Tabelle 3b in der Reihenfolge *Spalte-Zeile* zugeordnet. Da der erste Klartextbuchstabe D dreimal in der Tabelle vertreten ist, kann man zwischen den Koordinaten 55, 65 und 72 wählen. Wählt man etwa 65, beginnt der verschlüsselte Text mit diesen beiden Ziffern.

D	I	E	S		I	S	T		E	I	N	
65	25	73	06	89	81	35	44	24	80	70	34	24
G	E	H	E	I	M	E	R		T	E	X	T
92	98	69	46	81	29	68	23	01	07	62	51	44

Bis hierher handelt es sich prinzipiell um eine Verschlüsselung mit einem Polybios-Quadrat, die leicht modifiziert wurde.

Im zweiten Hauptschritt wird die erhaltene Ziffernfolge mithilfe einer pseudozufälligen Ziffernfolge verändert. Dazu wird eine zweite 10 x 10 - Tabelle erstellt, in deren Zeilen jeweils die Ziffernfolge `0123456789` eingetragen wird. Als Kennbuchstaben der Spalten und Zeilen werden die nächsten beiden Schlüsselworte gewählt, die entweder wie hier jeweils zehn Buchstaben enthalten oder wie bei der ersten Tabelle zu einem einzigen Schlüsselwort mit 20 Buchstaben zusammengefasst werden.

		0	1	2	3	4	5	6	7	8	9
		M	A	T	H	E	M	A	T	I	K
0	S	0	1	2	3	4	5	6	7	8	9
1	U	0	1	2	3	4	5	6	7	8	9
2	B	0	1	2	3	4	5	6	7	8	9
3	T	0	1	2	3	4	5	6	7	8	9
4	R	0	1	2	3	4	5	6	7	8	9
5	A	0	1	2	3	4	5	6	7	8	9
6	H	0	1	2	3	4	5	6	7	8	9
7	E	0	1	2	3	4	5	6	7	8	9
8	N	0	1	2	3	4	5	6	7	8	9
9	D	0	1	2	3	4	5	6	7	8	9

Abb. 6.4: Ausgangstabelle für pseudozufällige Ziffern

Wie bei der ersten Tabelle werden die Zeilen und Spalten verschoben. Dabei legen die Codes der aus den beiden Schlüsselworten erzeugten Kennbuchstaben wieder die Größe der einzelnen Verschiebungen fest.

		0	1	2	3	4	5	6	7	8	9
		M	A	T	H	E	M	A	T	I	K
0	S	2	3	4	5	6	7	8	9	0	1
1	U	0	1	2	3	4	5	6	7	8	9
2	B	9	0	1	2	3	4	5	6	7	8
3	T	1	2	3	4	5	6	7	8	9	0
4	R	3	4	5	6	7	8	9	0	1	2
5	A	0	1	2	3	4	5	6	7	8	9
6	H	3	4	5	6	7	8	9	0	1	2
7	E	6	7	8	9	0	1	2	3	4	5
8	N	7	8	9	0	1	2	3	4	5	6
9	D	7	8	9	0	1	2	3	4	5	6

a) Zeilen

		0	1	2	3	4	5	6	7	8	9
		M	A	T	H	E	M	A	T	I	K
0	S	7	3	2	4	7	2	8	7	7	1
1	U	7	1	1	6	0	2	6	6	9	9
2	B	2	0	3	3	1	7	5	8	1	8
3	T	0	2	5	6	1	5	7	0	8	0
4	R	9	4	2	9	6	4	9	7	1	2
5	A	1	1	5	0	4	6	6	0	4	9
6	H	3	4	8	0	3	8	9	3	5	2
7	E	0	7	9	5	5	5	2	4	5	5
8	N	3	8	9	3	7	8	3	4	0	6
9	D	6	8	4	2	4	1	3	9	8	6

b) Spalten

Abb. 6.5: Verschiebungen innerhalb der zweiten Tabelle

Anschließend werden die Ziffern zeilenweise von links nach rechts notiert und ergeben eine pseudozufällige Ziffernfolge. Diese muss genauso lang sein wie die sich aus der Codierung des Klartextes ergebende Ziffernfolge aus dem ersten Hauptschritt. Ist die neue Ziffernfolge zu lang, wird sie verkürzt. Ist sie dagegen zu kurz, wird sie periodisch verlängert.

Danach werden die Ziffern aus der Polybios-Verschlüsselung und gleich vielen in Abbildung 6.5 erzeugten pseudozufälligen Ziffern ziffernweise ohne Übertrag addiert.

```
   65257 30689 81354 42480 70342 49298 69468 12968 23010 76251 44
 + 73247 28771 71160 26699 20331 75818 02561 57080 94296 49712 11
-------------------------------------------------------------------
   38494 58350 52414 68079 90673 14006 61929 69948 17206 15963 55
```

Abschließend erfolgt der dritte Hauptschritt, bei dem die Ziffern der Summe mit einer doppelten Spaltentransposition noch einmal verändert werden. Für diese Transformation werden zwei Schlüssel verwendet, deren Längen keine gemeinsamen Teiler enthalten. Zusätzlich sollten die beiden Längen jeweils größer als $\sqrt{n}$ sein, wenn n die Länge des zu verschlüsselnden Klartextes ist. Diese beiden Bedingungen sind hier mit den Längen 7 und 8 der beiden Schlüssel SPALTEN und TAUSCHEN erfüllt.

Für die erste Spaltentransposition ist für die 52 Ziffern eine Tabelle der Breite 7 und der Höhe 8 erforderlich. In diese Tabelle werden die Ziffern horizontal eingefügt und spaltenweise in der Reihenfolge des numerischen Schlüssels des ersten Schlüsselwortes wieder ausgelesen. Diese Ziffern werden dann horizontal in die zweite Tabelle eingetragen.

S	P	A	L	T	E	N
6	5	1	3	7	2	4
3	8	4	9	4	5	8
3	5	0	5	2	4	1
4	6	8	0	7	9	9
0	6	7	3	1	4	0
0	6	6	1	9	2	9
6	9	9	4	8	1	7
2	0	6	1	5	9	6
3	5	5				

a) 1. Spaltentransposition

T	A	U	S	C	H	E	N
7	1	8	6	2	4	3	5
4	0	8	7	6	9	6	5
5	4	9	4	2	1	9	9
5	0	3	1	4	1	8	1
9	0	9	7	6	8	5	6
6	6	9	0	5	3	3	4
0	0	6	2	3	4	2	7
1	9	8	5				

b) 2. Spaltentransposition

Abb. 6.6: Doppelte Spaltentransposition

Diese Ziffern werden wieder vertikal in der Reihenfolge des numerischen Schlüssels des zweiten Schlüsselwortes ausgelesen und bilden den Geheimtext.

```
Geheimtext   04006 09624 65369 85329 11834 59164
             77417 02545 59601 89399 68
```

+

7 Spionage-Chiffren

7.1 Spionagering Lucy

Allan Alexander Foote (Deckname Jim) war im Zweiten Weltkrieg ein britischer Agent und gehörte dem erfolgreichen Spionagering *Lucy* an. In seinem Buch *Handbook for Spies* beschrieb er, wie er seine Nachrichten verschlüsselte und sie dann nach Moskau übermittelte.[57]

Klartext	`Eine geheime Nachricht von 007`
Schlüssel	`ZAHLEN`

Mit dem Schlüssel wird ein gemischtes Alphabet erstellt, das in eine Tabelle mit fünf Zeilen und sechs Spalten eingetragen wird. Zusätzlich werden die Zeichen `@` und `.` hinzugefügt. `@` kennzeichnet den Wechsel von Text zu Zahlen und umgekehrt, während das Stoppsignal `.` an beliebigen Stellen eingefügt werden kann, um eine besondere Unterbrechung oder einen Wechsel zu kennzeichnen.

Z	A	H	L	E	N
B	C	D	F	G	I
J	K	M	O	P	Q
R	S	T	U	V	W
X	Y	@	.		

Den Buchstaben und den beiden Sonderzeichen `@` und `.` werden die 40 Codes $(1,2,3,5,6,7,8,9)$, $(00,01,\ldots,09)$ und $(40,41,\ldots,49)$ zugeordnet. Bei den einstelligen Codes ist die Zahl 4 ausgenommen, da es sonst zu Mehrdeutigkeiten mit den Codes ab 40 kommen würde.

Den verbliebenen acht einstelligen Zahlen werden die am häufigsten in der englischen Sprache vorkommenden Buchstaben zugeordnet, die sich leicht mit dem Satz `A SIN TO ERR` einprägen lassen. Diese Buchstaben, ohne das im Satz doppelt vorkommende `R`, werden den Buchstaben des mit dem Schlüssel gebildeten gemischten Alphabets so zugeordnet, wie sie spaltenweise in der Tabelle von links nach rechts vorkommen.

Danach folgen die zweiziffrigen Codes, die der Reihe nach ebenfalls vertikal den restlichen

[57] Foote [79] S. 206 – 210, Read - Fisher [160]

Buchstaben und den zwei Sonderzeichen zugeordnet werden.

	2 A			7 E	8 N
					9 I
			6 O		
1 R	3 S	5 T			

00 Z	2 A	07 H	41 L	7 E	8 N
01 B	04 C	08 D	42 F	45 G	9 I
02 J	05 K	09 M	6 O	46 P	48 Q
1 R	3 S	5 T	43 U	47 V	49 W
03 X	06 Y	40 @	44 .		

Für die Übermittlung muss die zu übertragende Nachricht zunächst aufbereitet werden, da der Wechsel von den Buchstaben zu den Ziffern besonders gekennzeichnet werden muss. Neben dem Wechselzeichen `@` werden auch Stoppsignale eingefügt. Weiterhin ist zu beachten, dass jede vorkommende Ziffer dreifach notiert wird.

Zusätzlich begannen alle Meldungen, die Foote versendet hat, mit den Buchstaben `JIM` und alle Meldungen, die er aus Moskau empfangen hat, mit `DIRECTOR`, jeweils gefolgt von einem Stoppsignal. Darauf sei aber hier verzichtet.

E	I	N	E		G	E	H	E	I	M	E		N	A	C	H	R	I	C	H	T
7	9	8	7		45	7	07	7	9	09	7		8	2	04	07	1	9	04	07	5
V	O	N	.	@		0		0		7		@	.								
47	6	8	44	40		000		000		777		40	44								

Tab. 7.1: Verschlüsselung

Anschließend wird die sich ergebende Ziffernfolge in Gruppen von jeweils fünf Ziffern notiert. da diese Anordnung für die weitere Verschlüsselung wichtig ist. Sollte die letzte Gruppe aus weniger Ziffern bestehen, wird sie mit Nullen aufgefüllt.

79874	57077	90978	20407	19040	75476	84440	00000	07774	04400

Diese Zifferngruppen werden jeweils zu anderen Zifferngruppen addiert, die er bis 1943 aus dem *Statistical Handbook of Foreign Trade* für 1938 und danach aus dem *Swiss Handbook of Trade Statistics* für 1939 entnommen hat. Alle Zifferngruppen wurden natürlich nur einmal verwendet und der Beginn mit der Angabe der Seite, Zeile und Spalte wurde besonders verschlüsselt mit übertragen.

Die in diesem Beispiel verwendeten Ziffern sind allerdings aus keinem dieser Bücher und

wurden zufällig erzeugt. Die Addition geschieht dann ziffernweise ohne Übertrag.

```
  79874 57077 90978 20407 19040 75476 84440 00000 07774 04400
+ 23184 10933 97673 84323 71173 58813 23184 10933 97673 84323
-----------------------------------------------------------------
  92958 67900 87541 04720 80113 23289 07524 10933 94347 88723
```

Jetzt werden noch zwei besondere Zifferngruppen benötigt, die unterschiedliche Merkmale enthalten.

- *Code-Book-Group:* Mit dieser Kennung wird dem Empfänger mitgeteilt, wo sich die für die Addition benötigte Ziffernfolge befindet. Für Seite 77, Zeile 14 und Spalte 4 aus dem verwendeten Handbuch mit den Statistiken ergibt sich der Code 77144.
- *Fixed-Group:* Der feste Code 69696 für Foote. Dieser wurde von Moskau vorgegeben und kann auch nur dort geändert werden.
- *Message-Group:* Für die erste der beiden Zifferngruppen wird immer der fünfte Block der aktuellen Nachricht gewählt, in diesem Beispiel also 80113. Für die zweite Zifferngruppe dagegen der fünfte Block vom Ende der Nachricht aus gesehen, also 23289.

Diese drei Ziffernfolgen werden jeweils wieder ohne Übertrag addiert. Dabei ist zu beachten, dass sie sich nur in einer Zifferngruppe unterscheiden.

```
  77144          77144
+ 69696        + 69696
+ 80113        + 23289
----------     ----------
  16843          59919
```

Die Ergebnisse der beiden Additionen werden abschließend als dritte Zifferngruppe von vorne und hinten eingefügt. Mit diesen Schritten ist der zu übertragende Geheimtext fertiggestellt.

```
92958 67900       87541 04720 80113 23289 07524 10933       94347 88723
92958 67900 16843 87541 04720 80113 23289 07524 10933 59919 94347 88723
```

Literatur

[1] Abeles, Francine F. *Corrigendum to "Lewis Carroll's ciphers - The literary connections"*. In: *Advances in Applied Mathematics* Vol. 37. Nr. 1 (2006). S. 1.

[2] Abeles, Francine F. *Lewis Carroll's ciphers - The literary connections*. In: *Advances in Applied Mathematics* Vol. 34. Nr. 4 (2005). S. 697–708.

[3] Agency, National Security. *A History of U.S. Communications Security (Volumes I and II)*. National Security Agency, 2008.

[4] AQUILA. *The Fracfair Cipher*. In: *The Cryptogram* Vol. 33. Nr. 6 (1967). S. 129–130.

[5] Association, American Cryptogram. *The ACA and You - A Handbook for the Members of the American Cryptogram Association*. American Cryptogram Association, 2024.

[6] Bauer, Craig P. *Secret History - The Story of Cryptology*. CRC Press, 2013.

[7] Bauer, Friedrich L. *Entzifferte Geheimnisse*. 3. erw. Berlin, Heidelberg, New York: Springer Verlag, 2000.

[8] Bazeries, E. *Les Chiffres secrets dévoilés*. Paris: Librairies Charpentier et Fasquelle, 1901.

[9] Beaufort, Francis. *Cryptography, a system of secret writing by the late Admiral Sir Francis Beaufort*. Web-published document, URL: https://repository.duke.edu/dc/broadsides/bdseg19048 (letzter Zugriff: 26.9.2025).

[10] Becher, A. B. *Sir Francis Beaufort's Plan for Secret Correspondence*. In: *The Nautical Magazine* (1855). S. 431–433.

[11] Bellaso, Giovan Battista. *La cifra del sig. Giouan Battista Belaso, gentil'huomo bresciano*. Venetia, 1553.

[12] Bellaso, Giovan Battista. *Noui et singolari modi di cifrare de l'eccellente dottore di legge messer Giouan Battista Bellaso nobile bresciano*. Brescia, 1555.

[13] BELTESHAZZAR. *The Auto Dinomic Cipher*. In: *The Cryptogram* Vol. 66. Nr. 6 (2000). S. 8–9.

[14] Beutelspacher, Albrecht. *Kryptologie*. 10 akt. Wiesbaden: Springer Spektrum, 2015.

[15] BION. *The Numbered Key Cipher*. In: *The Cryptogram* Vol. 76. Nr. 3 (2010). S. 4–5.

[16] Bonavoglia, Paolo. *Bellaso + Vernam = DIANA*. Web-published document, URL: http://www.crittologia.eu/en/critto/cifraDIANA.html (letzter Zugriff: 26.9.2025).

[17] Bonavoglia, Paolo. *Bellaso's 1552 cipher recovered in Venice*. In: *Cryptologia* Vol. 43. Nr. 6 (2019). S. 459–465.

[18] Bonavoglia, Paolo. *Cifra Bellaso del 1553*. Web-published document, URL: http://www.crittologia.eu/critto/tavolaBellaso.html (letzter Zugriff: 26.9.2025).

[19] Bonavoglia, Paolo. *Cifra Orchema del Tritemio (1507)*. Web-published document, URL: http://www.crittologia.eu/critto/orchemaTritemio.html (letzter Zugriff: 26.9.2025).

[20] Bonavoglia, Paolo. *Cifrario di Vigenere disordinato*. Web-published document, URL: www.crittologia.eu/critto/vigenere_disordinato.phtml (letzter Zugriff: 26.9.2025).

[21] Bonavoglia, Paolo. *Il disco cifrante di Leon Battista Alberti*. Web-published document, URL: http://www.crittologia.eu/critto/alberti.phtml (letzter Zugriff: 26.9.2025).

[22] Bonavoglia, Paolo. *La cifra zero di G. B. Bellaso (1552)*. Web-published document, URL: http://www.crittologia.eu/critto/tavolaBellaso1552.html (letzter Zugriff: 26.9.2025).

[23] Bonavoglia, Paolo. *La tavola di Vigenère*. Web-published document, URL: http://www.crittologia.eu/critto/vigenere.html (letzter Zugriff: 26.9.2025).

[24] Bonavoglia, Paolo. *Le cifre di G. B. Bellaso*. Web-published document, URL: http://www.crittologia.eu/critto/bellaso.html (letzter Zugriff: 26.9.2025).

[25] Bonavoglia, Paolo. *Tavola Bellaso (1555)*. Web-published document, URL: http://www.crittologia.eu/critto/tavolaBellaso1555.html (letzter Zugriff: 26.9.2025).

[26] Bonavoglia, Paolo. *Tavola Della Porta*. Web-published document, URL: http://www.crittologia.eu/critto/tavolaDellaPorta.html (letzter Zugriff: 26.9.2025).

[27] Bonavoglia, Paolo. *The straddling checkerboard cipher*. Web-published document, URL: http://www.crittologia.eu/en/critto/straddle.html (letzter Zugriff: 26.9.2025).

[28] Bonavoglia, Paolo. *Trithemius, Bellaso, Vigenère - Origins of the Polyalphabetic Ciphers*. In: *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*. 2020, S. 46–51.

[29] Bowers, William Maxwell. *Digraphic substitution - The Playfair cipher, the four square cipher*. Practical Cryptanalysis; vol. 1. Greenfield, MA, USA: American Cryptogram Association, 1959.

[30] Bowers, William Maxwell. *The Bifid cipher*. Practical Cryptanalysis; vol. 2. Greenfield, MA, USA: American Cryptogram Association, 1960.

[31] Bowers, William Maxwell. *The Trifid cipher*. Practical Cryptanalysis; vol. 3. Greenfield, MA, USA: American Cryptogram Association, 1960.

[32] Bryan, William G. *Cryptographic ABC's - Periodic Ciphers Miscellaneous*. Practical cryptanalysis; vol. 5. Greenfield, MA, USA: American Cryptogram Association, 1967.

[33] Bryan, William G. *Cryptographic ABC's - Substitution and Transposition Ciphers*. Practical cryptanalysis; vol. 4. Greenfield, MA, USA: American Cryptogram Association, 1967.

[34] Bud, Nip N. *The Cadenus - A Lesson in Practical Cryptography*. In: *The Cryptogram* Vol. 24. Nr. 5 (1955). S. 71–74.

[35] Buonafalce, Augusto. *Bellaso's Reciprocal Ciphers*. In: *Cryptologia* Vol. 30. Nr. 1 (2006). S. 39–51.

[36] Bury, Jan. *From the Archives: The U.S. and West German Agent Radio Ciphers*. In: *Cryptologia* Vol. 31. Nr. 4 (2007). S. 343–357.

[37] Byrne, John F. *Silent Years - An Autobiography with Memoirs of James Joyce and Our Ireland . New York : Farrar, Straus, and Young*. (Kapitel 21, S. 264–307). New York: Farrar, Straus und Young, 1953, S. 307.

[38] Calof, Jeff, Hill, Jeff und Rubin, Moshe. *Chaocipher Exhibit 5 - History, Analysis, and Solution of Cryptologia's 1990 Challenge*. In: *Cryptologia* Vol. 38. Nr. 1 (2014). S. 1–25.

[39] Challenge, National Cipher. *2020 Special Edition - ELITE Cipher Challenge*. Web-published document, URL: https://github.com/themaddoctor/BritishNationalCipherChallenge/tree/master/2020%20special%20edition (letzter Zugriff: 26.9.2025).

[40] Challenge, National Cipher. *Challenge 2011 - 7B*. Web-published document, URL: https://github.com/themaddoctor/BritishNationalCipherChallenge/blob/master/2011/7B/solution.pdf (letzter Zugriff: 26.9.2025).

[41] Challenge, National Cipher. *Challenge 2024 - 8B*. Web-published document, URL: https://github.com/themaddoctor/BritishNationalCipherChallenge/blob/master/2024/8B-solution.txt (letzter Zugriff: 26.9.2025).

[42] Chase, Pliny Earl. *MMathematical Holocryptic Cyphers*. In: *The Mathematical Monthly* Vol. 1. Nr. March (1859). S. 194–196.

[43] Childs, James R. *German Military Ciphers from February to November 1918*. 1918. Web-published document, URL: https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_268/41784789082381.pdf (letzter Zugriff: 26.9.2025).

[44] Colavito, Cosmo und Cappellano, Filippo. *The Secret War on the Italian Front in WWI (1915 - 1918)*. 3rd ed. Roma: Italian Ministry of Defence, 2021.

[45] Collon, Auguste. *Étude sur la Cryptographie, son emploi à la guerre et dans la diplomatie (Vol. 1)*. (Extrait de la *Revue de l'Armée Belge* (24e année)). Bruxelles: Librairie Falk Fils, 1900.

[46] Collon, Auguste. *Étude sur la Cryptographie, son emploi à la guerre et dans la diplomatie (Vol. 2)*. (Extrait de la *Revue de l'Armée Belge* (25e-26e année)). Bruxelles: Librairie Falk Fils, 1902.

[47] Collon, Auguste. *Étude sur la Cryptographie, son emploi à la guerre et dans la diplomatie (Vol. 3)*. (Extrait de la *Revue de l'Armée Belge* (27e-29e année)). Direction & Administration Liége, 1905.

[48] CONDOR, EL. *Field Codes - Tri-Square Irregular*. In: *The Cryptogram* Vol. 66. Nr. 1 (2000). S. 6.

[49] Cowan, Michael J. *Rasterschlüssel 44 - The Epitome of Hand Field Ciphers*. In: *Cryptologia* Vol. 28. Nr. 2 (2004). S. 115–148.

[50] CROTALUS. *The Sidewinder Cipher*. In: *The Cryptogram* Vol. 57. Nr. 5 (1992). S. 6–7.

[51] Crowley, Paul. *Mirdek: a card cipher inspired by Solitaire*. Web-published document, URL: https://www.ciphergoth.org/crypto/mirdek/ (letzter Zugriff: 26.9.2025).

[52] D'Agapeyeff, Alexander. *Codes and ciphers*. (republished 1974). London: Oxford University Press, 1939.

[53] Danielsson, Holger. *Magische Quadrate und ihre Konstruktion*. Berlin, Heidelberg: Springer Spektrum, 2024. DOI: 10.1007/978-3-662-70448-6.

[54] Danielsson, Holger. *Manuelle Kryptografie*. Berlin, Heidelberg: Springer Spektrum, 2025. DOI: 10.1007/978-3-662-72571-9.

[55] Danielsson, Holger. *Spezielle magische Quadrate und ihre Konstruktion*. Berlin, Heidelberg: Springer Spektrum, 2024. DOI: 10.1007/978-3-662-70708-1.

[56] David, Charles. *A World War II German Army Field Cipher and How We Broke It*. In: *Cryptologia* Vol. 20. Nr. 1 (1996). S. 31–50.

[57] Delatelle, Félix. *Traité de Cryptographie*. Paris: Gauthier-Villars, 1902.

[58] DELEC. *The Nicodemus Cipher*. In: *The Cryptogram* Vol. 18. Nr. 4 (1949). S. 74–78.

[59] Diepenbroek, Martine. *The Spartan Scytale and Developments in Ancient and Modern Cryptography*. London: Bloomsbury Academic, 2024.

[60] Dooley, John F. *Codes, Ciphers and Spies*. New York: Springer Nature, 2016.

[61] Dooley, John F. *History of Cryptography and Cryptanalysis - Codes, Ciphers, and Their Algorithms*. 2nd. Cham: Springer Nature, 2024.

[62] Drobick, Jörg. *Doppelwürfel / Granit – Teil 1*. Web-published document, URL: https://mysterytwister.org/media/challenges/pdf/mtc3-drobick-01-doppelwuerfel-01-de.pdf (letzter Zugriff: 26.9.2025).

[63] Drobick, Jörg. *Manuelle Chiffrierverfahren*. Web-published document, URL: https://scz.bplaced.net/m.html (letzter Zugriff: 26.9.2025).

[64] Drobick, Jörg. *Manuelle Chiffrierverfahren - Gebrauchsanweisung für das Chiffrierverfahren GRANIT*. Web-published document, URL: https://scz.bplaced.net/m.html#granit (letzter Zugriff: 26.9.2025).

[65] Drobick, Jörg. *Manuelle Chiffrierverfahren - verwendet von Richard Sorge und Max Christiansen-Clausen*. Web-published document, URL: https://scz.bplaced.net/m.html#h (letzter Zugriff: 26.9.2025).

[66] Drobick, Jörg. *Manuelle Chiffrierverfahren - VIC*. Web-published document, URL: https://scz.bplaced.net/m.html#vic1 (letzter Zugriff: 26.9.2025).

[67] DUMBO. *A periodic Gromark*. In: *The Cryptogram* Vol. 39. Nr. 2 (1973). S. 27.

[68] DUMBO. *The Gromark Cipher - Part 1*. In: *The Cryptogram* Vol. 35. Nr. 2 (1969). S. 25.

[69] DUMBO. *The Gromark Cipher - Part 2*. In: *The Cryptogram* Vol. 35. Nr. 4 (1969). S. 79–80.

[70] ENDEAVOUR. *Cipher Inspired by Kryptos*. In: *The Cryptogram* Vol. 75. Nr. 5 (2009). S. 4–5.

[71] Ertel, Wolfgang und Löhmann, Ekkehard. *Angewandte Kryptographie*. 6. München: Hanser Verlag, 2020.

[72] Esslinger, Bernhard. *Learning and Experiencing Cryptography with Cryptool and Sagemath*. Boston: Artech House, 2024.

[73] EUREKA. *The Morbit Cipher*. In: *The Cryptogram* Vol. 31. Nr. 3 (1964). S. 60–61.

[74] Falconer, John. *Cryptomenysis Patefacta - The Art of Secret Information*. London, 1685.

[75] Fendt, Stefan. *ASAC – Eine Stärkere ADFGVX-Chiffre*. Web-published document, URL: https://mysterytwister.org/media/challenges/pdf/mtc3-fendt-01-asac-01-de.pdf (letzter Zugriff: 26.9.2025).

[76] FIDDLE. *A Morse Code Fractionating Cipher*. In: *The Cryptogram* Vol. 19. Nr. 2 (1950). S. 25, 32–34.

[77] Figl, Andreas. *Systeme des Chiffrierens*. Graz: Verlag von Ulr. Mosers Buchhandlung, 1926.

[78] Fleissner v. Wostrowitz, Eduard B. *Handbuch der Kryptographie: Anleitung zum Chiffriren und Dechiffriren von Geheimschriften*. Wien: L. W. Seidel und Sohn, 1881.

[79] Foote, Alexander. *Handbook for Spies*. London: Museum Press Limited, 1949.

[80] Friedman, William F. und Callimahos, Lambros D. *Military Cryptanalysis, Part I*. Washington D. C.: National Security Agency, 1956.

[81] Friedman, William F. und Callimahos, Lambros D. *Militarycrypt Analytics, Part II, First Section*. Washington D. C.: National Security Agency, 1955.

[82] FRINKUS. *The Redefence Cipher*. In: *The Cryptogram* Vol. 32. Nr. 6 (1965). S. 123 und 141.

[83] Fronczak, M. *Atbah-Type Ciphers in the Christian Orient and Numerical Rules in the Construction of Christian Substitution Ciphers*. In: *Cryptologia* Vol. 37. Nr. 4 (2013). S. 338–344.

[84] Fuensanta, José Ramón Soler und Javier, López-Brea Espiau Francisco. *The Strip Cipher - The Spanish Official Method*. In: *Cryptologia* Vol. 31. Nr. 1 (2007). S. 46–56.

[85] G4EGG. *The CONDI Cipher*. In: *The Cryptogram* Vol. 77. Nr. 5 (2011). S. 7.

[86] Gaines, Helen Fouche. *Cryptanalysis - a study of ciphers and their solution*. 5th printing 1956. New York: Dover Publications, 1939.

[87] GALUPOLY. *A Numerical Four-Square Cipher (Part 1)*. In: *The Cryptogram* Vol. 29. Nr. 4 (1962). S. 77–80.

[88] GALUPOLY. *A Numerical Four-Square Cipher (Part 2)*. In: *The Cryptogram* Vol. 29. Nr. 5 (1962). S. 99–103.

[89] Gardner, Martin. *Codes, Ciphers and Secret Writing*. New York: Dover Publications, 1972.

[90] GEMINATOR. *The Checkerway Cipher*. In: *The Cryptogram* Vol. 56. Nr. 1 (1990). S. 3.

[91] GEMINATOR. *The Homophonic Checkerboard*. In: *The Cryptogram* Vol. 56. Nr. 2 (1990). S. 6.

[92] Géraud-Stewart, Rémi und Naccache, David. *A French cipher from the late 19th century*. In: *Cryptologia* Vol. 45. Nr. 4 (2021). S. 342–370.

[93] Givierge, Marcel. *Course in Cryptography*. (Translated from „Cours de Cryptographie"). Washington, D.C.: US Government Printing Office, 1934.

[94] Gómez, Joan. *Geheimsprachen und Decodierung*. Kerkdriel: Librero Verlag, 2017.

[95] Grandpré, A. de. *Cryptographie pratique*. Paris: Librairie Boyveau et Chevillet, 1905.

[96] Gylden, Yves. *Le chiffre particulier de Louis XVI et Marie-Antoinette lors de la fuite Varennes*. In: *Revue internationale de criminalistique* Vol. 3 (1931). S. 248–256.

[97] Hermann, A. *Méthode pour Chiffrer et Déchiffrer les Dépèches Secrètes*. Paris: Librairie Scientifique A. Hermann, 1892.

[98] Hermann, A. *Nouvelle méthode cryptographique*. In: *Revue Scientifique* Vol. 51 (1893). S. 594–595.

[99] Hutton, Eric Bond. *Die Hutton-Chiffre*. Web-published document, URL: `https://mysterytwister.org/media/challenges/pdf/mtc3-hutton-01-hutton-01-de.pdf` (letzter Zugriff: 26.9.2025).

[100] Janeczko, Paul B. *Top secret - A Handbook of Codes, Ciphers, and Secret Writing*. Somerville: Candlewick Press, 2004.

[101] Josse, H. *La cryptographie et ses applications à l'art militaire*. In: *Revue Maritime et Coloniale* Vol. 84 (1885).

[102] Al-Kadi, Ibrahim A. *Origins of Cryptology - The Arab Contributions*. In: *Cryptologia* Vol. 16. Nr. 2 (1992). S. 97–126.

[103] Kaeding, Thomas. *A Book on Classical Cryptography*. (Version 1). 2020. Web-published document, URL: https://github.com/themaddoctor/classical_crypto_book (letzter Zugriff: 26.9.2025).

[104] Kaeding, Thomas. *A Modern View of Classical Cryptography*. (Version 2). 2024. Web-published document, URL: https://github.com/themaddoctor/classical_crypto_book (letzter Zugriff: 26.9.2025).

[105] Kaeding, Thomas. *Breaking the Hutton 2 challenge*. 2023. Web-published document, URL: https://eprint.iacr.org/2023/1113 (letzter Zugriff: 26.9.2025).

[106] Kaeding, Thomas. *Quagmire ciphers and group theory - What is a Porta cipher?* 2022. Web-published document, URL: https://eprint.iacr.org/2022/1677 (letzter Zugriff: 26.9.2025).

[107] Kahn, David. *The Codebreakers - The Story of Secret Writing*. revised. New York: Scribner, 1996.

[108] Kaminsky, Alan. *ElsieFour - A Low-Tech Authenticated Encryption Algorithm For Human-to-Human Communication*. 2017. Web-published document, URL: https://eprint.iacr.org/2017/339 (letzter Zugriff: 26.9.2025).

[109] Kasiski, Friedrich Wilhelm. *Die Geheimschriften und die Dechiffrir-Kunst*. Berlin: Mittler & Sohn Verlag, 1863.

[110] Kelly, Thomas. *The Myth of the Skytale*. In: *Cryptologia* Vol. 22. Nr. 43 (1998). S. 244–260.

[111] Kerckhoffs, Auguste. *La Cryptographie Militaire*. Paris: Librairie Militaire de L. Baudoin, 1883.

[112] Kerckhoffs, Auguste. *La Cryptographie Militaire*. In: *Journal des Sciences Militaires* Vol. 9. Nr. Jan 1883 (1883). S. 5–39.

[113] Kerckhoffs, Auguste. *La Cryptographie Militaire*. In: *Journal des Sciences Militaires* Vol. 9. Nr. Feb 1883 (1883). S. 161–191.

[114] Kippenhahn, Rudolf. *Verschlüsselte Botschaften*. Hamburg: Rowohlt Taschenbuch Verlag, 2012.

[115] Kircher, Athanasius. *Polygraphia nova et universalis ex combinatoria arte detecta, etc*. 1663.

[116] Klüber, Johann Ludwig. *Kryptographik - Lehrbuch der Geheimschreibekunst*. Tübingen: Cottasche Buchhandlung, 1809.

[117] Knight, H. Gary. *Cryptanalysts' Corner*. In: *Cryptologia* Vol. 2. Nr. 3 (1978). S. 239–240. (Problem 11).

[118] KNUTE. *The Digrafid Cipher*. In: *The Cryptogram* Vol. 28. Nr. 1 (1960). S. 8–9.

[119] Kruskal, Joseph R. *A Trigraph Cipher With A Short Key For Hand Use*. In: *Cryptologia* Vol. 9. Nr. 3 (1985). S. 202–222.

[120] Kullback, Solomon. *General Solution for the Double Transposition Cipher*. Washington, D.C.: United States Government Printing Office, 1934.

[121] Laffin, John. *Codes and ciphers - secret writing through the ages*. London: Abelard-Schuman, 1964.

[122] Lange, André und Soudart, E.A. *Traité de cryptographie*. Paris: Librairie Félix Alcan, 1925.

[123] Larrabee, Charles S. *Larrabee's Cipher and Secret Letter and Telegraph Code*. 2nd ed. New York: van Nostrand Publisher, 1884.

[124] Lasry, George. *Analysis of a late 19th century french cipher created by Major Josse*. In: *Cryptologia* Vol. 47. Nr. 1 (2023). S. 48–62.

[125] Lasry, George, Kopal, Nils und Wacker, Arno. *Cryptanalysis of columnar transposition cipher with long keys*. In: *Cryptologia* Vol. 40. Nr. 4 (2016). S. 374–398.

[126] Lasry, George, Kopal, Nils und Wacker, Arno. *Solving the Double Transposition Challenge with a Divide-and-Conquer Approach*. In: *Cryptologia* Vol. 38. Nr. 3 (2014). S. 197–214.

[127] Lasry, George, Niebel, Ingo, Kopal, Nils u. a. *Deciphering ADFGVX messages from the Eastern Front of World War I*. In: *Cryptologia* Vol. 41. Nr. 2 (2017). S. 101–136.

[128] LEDGE. *The Ragbaby*. In: *The Cryptogram* Vol. 38. Nr. 6 (1972). S. 154–155.

[129] Lipson, Stanley H. und Abeles, Francine. *The Key-Vowel Cipher of Charles L. Dodgson*. In: *Cryptologia* Vol. 15. Nr. 1 (1991). S. 18–24.

[130] Lipson, Stanley H. und Abeles, Francine. *The Matrix Cipher of Charles L. Dodgson*. In: *Cryptologia* Vol. 14. Nr. 1 (1990). S. 28–35.

[131] MACHIAVELLI. *The Two-Square Cipher*. In: *The Cryptogram* Vol. 38. Nr. 6 (1972). S. 152–153.

[132] Mader, Julius, Stuchlik, Gerhard und Pehnert, Horst. *Dr. Sorge funkt aus Tokyo*. 3. Berlin: Militärverlag der DDR, 1973.

[133] Masterton, R. *A Five-Square Special*. In: *The Cryptogram* Vol. 60. Nr. 5 (1994). S. 4.

[134] Masterton, R. *The Monome-Dinome problem*. In: *The Cryptogram* Vol. 62. Nr. 5 (1996). S. 8–9.

[135] Meer, Hans van der. *An old challenge*. 2010. Web-published document, URL: `https://staff.fnwi.uva.nl/h.vandermeer/pubs/fuergod.pdf` (letzter Zugriff: 26.9.2025).

[136] Meier, Lena. *Biber-Code*. Web-published document, URL: `https://mysterytwister.org/media/challenges/pdf/mtc3-meier-04-biber-de.pdf` (letzter Zugriff: 26.9.2025).

[137] Meister, Aloys. *Die Geheimschrift - Im Dienste der päpstlichen Kurie*. Paderborn: Schöningh Verlag, 1906.

[138] MINIMAX. *The Principle of Double Duty or a Trigraphic Playfair*. In: *The Cryptogram* Vol. 28. Nr. 3 (1961). S. 54–56.

[139] Mitchell, Douglas W. *Rubik's Cube as a Transposition Device*. In: *Cryptologia* Vol. 16. Nr. 3 (1992). S. 250–256.

[140] Mrayati, M., Meer Alam, Y. und at-Tayyan, M.H. *Al-Kindi's Treatise on Cryptanalysis*. Arabic Origins of Cryptology Vol. 1. Kfcris & Kacst, 2003.

[141] MSCREP. *The Morfid - A Morse Based Bifid Type Cipher*. In: *The Cryptogram* Vol. 69. Nr. 6 (2003). S. 6–7.

[142] MSCREP. *The Relativist Substitution Cipher*. In: *The Cryptogram* Vol. 69. Nr. 3 (2003). S. 4–5.

[143] MSCREP. *The Sequence Transposition Cipher*. In: *The Cryptogram* Vol. 81. Nr. 6 (2015). S. 7.

[144] MSCREP. *The SudC - A Sudoku Based Transposition Cipher*. In: *The Cryptogram* Vol. 86. Nr. 5 (2020). S. 4.

[145] Müller, Didier. *Les codes secrets décryptés*. 2025. Web-published document, URL: https://www.apprendre-en-ligne.net/crypto/csd/index.html (letzter Zugriff: 26.9.2025).

[146] Myszkowski, E. *Cryptographie indéchiffrable*. Paris: Société Française d'Imprimerie et de Librairie, 1902.

[147] Nachef, Valerie und Patarin, Jacques. *I shall love you up to the death*. Cryptology ePrint Archive, Paper 2009/166. 2009. Web-published document, URL: https://eprint.iacr.org/2009/166 (letzter Zugriff: 26.9.2025).

[148] NATURAL, B. *The Ragbaby*. In: *The Cryptogram* Vol. 26. Nr. 5 (1959). S. 97, 99–100.

[149] Nichols, Randall K. *Classical Cryptography Course*. Vol. 1. (Pseudonym: Lanaki). Laguna Hills: Aegean Park Press, 1996.

[150] Nichols, Randall K. *Classical Cryptography Course*. Vol. 2. Laguna Hills: Aegean Park Press, 1996.

[151] Office, British War. *Manual of Cryptography*. Laguna Hills: Aegean Park Press, 1914.

[152] Ohaver, M. E. *Solving Cipher Secrets: A Collection of Weekly Articles and Problems Concerning Codes and Ciphers*. (Collection of Flynn's Weekly between March 5, 1927 and Sept. 22, 1928). Aegean Park Press, 1982.

[153] Pincock, Stephen und Frary, Mark. *Geheime Codes*. Bergisch Gladbach: Ehrenwirth Verlag, 2006.

[154] Porta, Giovan Battista. *De furtivis literarum notis*. Neapoli, 1563, S. 229.

[155] Pratt, Fletcher. *Secret and Urgent - The Story of Codes and Ciphers*. Bristol: Robert Hale Ltd., 1939.

[156] QUATERNION. *A Straddling Checkerboard*. In: *The Cryptogram* Vol. 42. Nr. 2 (1976). S. 25.

[157] RASER, RED E. *The Portax Cipher*. In: *The Cryptogram* Vol. 17. Nr. 5 (1948). S. 104–105.

[158] RASER, RED E. *The Portax Cipher (part II)*. In: *The Cryptogram* Vol. 17. Nr. 6 (1949). S. 125–127.

[159] RAT, THE. *The Octafair Cipher*. In: *The Cryptogram* Vol. 57. Nr. 2 (1991). S. 8–12.

[160] Read, Anthony und Fisher, David. *Operation Lucy*. New York: Coward, McCann & Geoghegan, 1981.

[161] Rijmenants, Dirk. *German Rasterschlüssel 44 Field Cipher*. Web-published document, URL: https://www.ciphermachinesandcryptology.com/en/rasterschlussel44.htm (letzter Zugriff: 26.9.2025).

[162] Rijmenants, Dirk. *The SECOM Cipher*. Web-published document, URL: https://www.ciphermachinesandcryptology.com/en/secom.htm (letzter Zugriff: 26.9.2025).

[163] ROGUE. *More on the periodic Gromark*. In: *The Cryptogram* Vol. 39. Nr. 5 (1973). S. 105–106.

[164] Rubin, Frank. *Secret Key Cryptography*. Shelter Island, NY: Manning Publications Co., 2022.

[165] Rubin, Frank. *The Kliger Residue Cipher*. In: *The Cryptogram* Vol. 46. Nr. 3 (1980). S. 52–53. (Pseudonym: FIRE-O).

[166] Rubin, Moshe. *John F. Byrne's Chaocipher Revealed - An Historical and Technical Appraisal*. In: *Cryptologia* Vol. 35. Nr. 4 (2011). S. 328–379.

[167] S-TUCK. *The Interrupted-Key Cipher*. In: *The Cryptogram* Vol. 15. Nr. 1 (1946). S. 5–9.

[168] Sacco, Luigi. *Manual of Cryptography*. (Original: Manuale di Crittografia). Aegean Park Press, 1977.

[169] Salomon, David. *Data Privacy and Security*. New York: Springer Verlag, 2003.

[170] Sanguino, Luis Alberto Benthin. *Spanish Strip Cipher*. Web-published document, URL: https://mysterytwister.org/media/challenges/pdf/mtc3-sanguino-01-SSC-01-de.pdf (letzter Zugriff: 26.9.2025).

[171] Sanguino, Luis Alberto Benthin u.a. *Analyzing the Spanish Strip Cipher by Combining Combinatorial and Statistical Methods*. In: *Cryptologia* Vol. 40. Nr. 3 (2016). S. 261–284.

[172] Savard, John. *A Cryptographic Compendium - Two Trigraphic Ciphers*. Web-published document, URL: http://www.quadibloc.com/crypto/pp1325.htm (letzter Zugriff: 26.9.2025).

[173] Scheers, D.P.J.A. *The Venetian Ciphers of Agostino Amadi: Volume 3 (English Version)*. Amazon Digital Services, 2024.

[174] Schmeh, Klaus. *Codeknacker gegen Codemacher*. 4. Springer Nature, 2022.

[175] Schneickert, Hans. *Moderne Geheimschriften*. Mannheim: Dr. Haas'che Druckerei, 1900.

[176] Schneier, Bruce. *The Solitaire Encryption Algorithm*. Web-published document, URL: https://www.schneier.com/academic/solitaire/ (letzter Zugriff: 26.9.2025).

[177] Schott, Gaspar. *Schola steganographica, in classes octo distributa*. 1665.

[178] Schwartz, Kathryn A. *Charting Arabic Cryptology's Evolution*. In: *Cryptologia* Vol. 33. Nr. 4 (2009). S. 297–304.

[179] Scotus, Dun. *The Richelieu Number Cipher*. In: *The Cryptogram* Vol. 30. Nr. 5 (1963). S. 105, 109.

[180] Sestri, Giovanni. *Metodo Brevissimo & assoluto per scrivere occulto in tutto le lingue*. Roma: Nella stamperia del Bernabò, 1710.

[181] SHERLAC. *Ragbaby Cipher*. In: *The Cryptogram* Vol. 24. Nr. 4 (1955). S. 54–55.

[182] Shiu, Daniel. *Analysis of Solitaire*. arXiv: 1909.06300. Web-published document, URL: https://arxiv.org/abs/1909.06300 (2019, letzter Zugriff: 26.9.2025).

[183] SHMOO. *Compressocrat - Compression for 26—letter*. In: *The Cryptogram* Vol. 49. Nr. 3 (1983). S. 4–5.

[184] SHMOO. *The Asymmetrical Playfair Cipher*. In: *The Cryptogram* Vol. 54. Nr. 3 (1988). S. 7.

[185] Shulman, David. *A Sherlockian Cryptogram*. In: *Cryptologia* Vol. 3. Nr. 1 (1979). S. 54–55.

[186] SI, SI. *Cryptanalysis Of The Penney Tramp Cipher*. In: *The Cryptogram* Vol. 46. Nr. 1 (1980). S. 4–5.

[187] SI, SI. *More About The Swagman*. In: *The Cryptogram* Vol. 45. Nr. 2 (1979). S. 48.

[188] SI, SI. *The Hocheck Cipher Examined*. In: *The Cryptogram* Vol. 56. Nr. 4 (1990). S. 6.

[189] SI, SI. *The Lazy Swagman*. In: *The Cryptogram* Vol. 44. Nr. 2 (1978). S. 27, 45.

[190] SI, SI. *The Swagman*. In: *The Cryptogram* Vol. 62. Nr. 2 (1996). S. 8, 10.

[191] Singh, Simon. *Geheime Botschaften*. 2. München: Hanser Verlag, 2002.

[192] SOUPY. *Some Observations on the Kliger Cipher*. In: *The Cryptogram* Vol. 46. Nr. 5 (1980). S. 97, 100.

[193] STRUSE, AB. *A Penney Tramp*. In: *The Cryptogram* Vol. 45. Nr. 5 (1979). S. 87. (Pseudonym von David Shulman).

[194] Suetonius Tranquillus, Gaius. *Die Kaiserviten - De vita Caesarum*. (Herausgegeben und übersetzt: Hans Martinet). Berlin: Akademie Verlag GmbH, 2014.

[195] TATTERS. *The Skipping Tramp*. In: *The Cryptogram* Vol. 46. Nr. 1 (1980). S. 3.

[196] THALES. *The Tri-Square Cipher*. In: *The Cryptogram* Vol. 27. Nr. 1 (1959). S. 6–7.

[197] Tiltman, John H. *A Cryptologic Fairy Tale*. In: *MSA Technical Journal* Vol. 7. Nr. 2 (1961). S. 21–39. (Freigegebenes Dokument mit entfernten Grafiken). Web-published document, URL: https://media.defense.gov/2021/Jul/02/2002755809/-1/-1/0/cryptologic-fairy-tale.pdf (letzter Zugriff: 26.9.2025).

[198] Tomokiyo, S. *Ciphers of Marie-Antoinette and Axel von Fersen*. Web-published document, URL: https://cryptiana.web.fc2.com/code/fersen.htm (letzter Zugriff: 26.9.2025).

[199] Tomokiyo, S. *Did Beaufort Really Use the Beaufort Cipher?* Web-published document, URL: https://cryptiana.web.fc2.com/code/beaufort.htm (letzter Zugriff: 26.9.2025).

[200] Tomokiyo, S. *Lovell' Cipher*. Web-published document, URL: https://cryptiana.web.fc2.com/code/lovell.htm (letzter Zugriff: 26.9.2025).

[201] Tomokiyo, Satoshi. *Who Made tthe Vigenère Cipheräs Known Today?* 2021. Web-published document, URL: https://www.academia.edu/62511944/Who_Made_the_Vigen%C3%A8re_Cipher_as_Known_Today (letzter Zugriff: 26.9.2025).

[202] TRANSITION, DD. *The Vimark Cipher*. In: *The Cryptogram* Vol. 37. Nr. 4 (1971). S. 124.

[203] Trithemius, Johannes. *Polygraphiae Libri Sex*. 1518.

[204] Türkel, Siegfried. *Chiffrieren mit Geräten und Maschinen*. Graz: Verlag von Ulr. Mosers Buchhandlung, 1927.

[205] UBET. *The Auto-Transposition Cipher*. In: *The Cryptogram* Vol. 30. Nr. 1 (1962). S. 1, 6–8.

[206] US Army, Department of the. *Basic Cryptography*. (Technical Manual TM32-220). Washington, D.C.: US Government Printing Office, 1950.

[207] Valerio, P. *De la Cryptographie - Essai sur les Méthodes de Déchiffrement*. Paris: Librairie Militaire de L. Baudoin, 1893.

[208] Van der Vieren, Daniel R. *The Rubik's Crypto-Cube - a Trans-Composite Cipher*. Web-published document, URL: https://scispace.com/pdf/the-rubik-s-crypto-cube-a-trans-composite-cipher-3jbzrro8mf.pdf (letzter Zugriff: 26.9.2025).

[209] Vigenère, Blaise de. *Traicté des chiffres ou secrètes manières d'escrire*. Paris: Abel L'Angelier, 1587.

[210] Vogel, Donald S. *Inside a KGB Cipher*. In: *Cryptologia* Vol. 14. Nr. 1 (1990). S. 37–52.

[211] Weierud, Frode. *Schlüsselanleitung zum Rasterschlüssel 44*. (Ausgabe vom 27. März 1944). Web-published document, URL: https://cryptocellar.org/wmc/schluesselanleitung-zum-rs44.pdf (letzter Zugriff: 26.9.2025).

[212] Weierud, Frode. *Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel*. Web-published document, URL: https://cryptocellar.org/wmc/schluesselanleitung-dk-1941.pdf (letzter Zugriff: 26.9.2025).

[213] WHITE, SELLWYN. *The Interrupted Key Cipher*. In: *The Cryptogram* Vol. 21. Nr. 1 (1952). S. 12–15.

[214] Wikipedia. *Hutton Cipher*. Web-published document, URL: https://en.wikipedia.org/w/index.php?title=User:Eric_Bond_Hutton&oldid=840686562 (letzter Zugriff: 26.9.2025).

[215] Wobst, Reinhard. *Abenteuer Kryptologie*. Bonn: Addison-Wesley-Verlag, 1998.

[216] Wrixon, Fred B. *Codes, Chiffren & andere Geheimsprachen*. Köln: Könemann Verlagsgesellschaft, 2000.

[217] YIP, BUN. *The Swagman Transposition Cipher*. In: *The Cryptogram* Vol. 43. Nr. 5 (1977). S. 93, 96.

[218] ZENITH. *The Trifair Cipher*. In: *The Cryptogram* Vol. 49. Nr. 2 (1983). S. 3–5, 8.

[219] ZENITH. *Trifair Variations and Extensions*. In: *The Cryptogram* Vol. 49. Nr. 3 (1983). S. 5.