

Holger Danielsson

Manuelle Kryptografie

Mit über 150 Papier- und
Bleistiftverfahren die Welt der Ver- und
Entschlüsselung entdecken



Springer Spektrum

Manuelle Kryptografie

Holger Danielsson

Manuelle Kryptografie

Mit über 150 Papier- und
Bleistiftverfahren die Welt der Ver- und
Entschlüsselung entdecken

Holger Danielsson
Schwerte, Deutschland

ISBN 978-3-662-72570-2 ISBN 978-3-662-72571-9 (eBook)
<https://doi.org/10.1007/978-3-662-72571-9>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <https://portal.dnb.de> abrufbar.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer-Verlag GmbH, DE, ein Teil von Springer Nature 2025

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber*in sind zu beachten.

Der Verlag, die Autor*innen und die Herausgeber*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor*innen oder die Herausgeber*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Iris Ruhmann

Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

Vorwort

Verschlüsselungen begegnen uns überall im alltäglichen Leben. Viele Leute kaufen online über das Internet, führen Banküberweisungen online durch oder heben am Bankautomaten Geld ab. Bei diesen Tätigkeiten ist es offensichtlich, dass die eingegebenen Daten verschlüsselt werden. Dies geschieht aber auch oft unbewusst, wenn man etwa mit dem Handy Nachrichten oder E-Mails verschickt.

Aber bereits seit der Antike wurden Verschlüsselungen benutzt, weil es schon immer wichtig war, dass Nachrichten und Informationen nur an ganz bestimmte Personen gelangen und vor anderen geheim gehalten werden. Nachrichten betrafen den militärischen oder diplomatischen Dienst und wurden mühsam über große Entfernungen transportiert. Viele Kryptologen arbeiteten auch im päpstlichen Dienst.

Eine Nachricht, die von einem Sender A mit einem Schlüssel verschlüsselt und an einen Empfänger B gesendet wird, darf auch nur von diesem gelesen werden können. Sollte die Nachricht bei der Übertragung von A nach B von einer dritten Partei C gelesen werden, so ist diese für diesen wertlos, da er den Inhalt ohne Schlüssel nicht lesen kann.

Die bisher verfügbare Literatur beinhaltet entweder nur wenige allgemein Verfahren, die in vielen Büchern beschrieben werden, oder ist sehr wissenschaftlich gehalten. In diesem Buch sollen dagegen auch Verfahren vorgestellt werden, die eher unbekannt sind, aber trotzdem in vielen Fällen angewendet wurden. Zudem bieten viele der enthaltenen Verfahren auch kryptografisch neue Gesichtspunkte oder Ideen.

Es wird ein umfassender Überblick über Verfahren gegeben, die in den Bereich der *manuellen Kryptografie* fallen. Üblicherweise versteht man hierunter Verschlüsselungsverfahren, die per Hand mit Papier und Bleistift ausgeführt werden können. Hierunter fallen beispielsweise alle Verfahren der *klassischen Kryptografie* seit Beginn der Kryptografie bis zum Zeitraum der modernen Kryptografie, die mit Computern realisiert wird und für deren Analyse Kenntnisse in Mathematik und Programmierung erforderlich sind.

Trotz der Computerdominanz werden bis zum heutigen Tag neue manuelle Verschlüsselungsverfahren entwickelt und die Beschäftigung mit ihnen hat in den letzten Jahren auch zugenommen. Will man sich etwa mit modernen Verschlüsselungen beschäftigen, erfordert dies gewisse Grundkenntnisse, die bei den manuellen Verfahren leichter gewonnen und dann auf moderne Verfahren übertragen werden können. Ein Verständnis der manuellen Verfahren ist also für heutige Verfahren wichtig, da sie in einem einfacheren, nicht so komplexen Kontext auftreten.

Von ganz herausragender Bedeutung ist aber das zunehmende Interesse an Kryptogrammen. Dies sind verschlüsselte Texte, bei denen das benutzte Verschlüsselungsverfahren meist unbekannt ist. Solche Rätsel veröffentlicht beispielsweise alle zwei Monate die *American Cryptogram Association (ACA)* in ihrem Magazin. Daneben existiert eine Vielzahl von Challenges zur Entschlüsselung derartiger Texte. Auch für Historiker sind solche Verfahren von besonderem Interesse. Es gibt viele bis heute nicht entschlüsselte Nachrichten, die eventuell wichtige, bisher nicht bekannte Informationen und neue Sichtweisen vermitteln können.

Durch die stark wachsende Bedeutung der Datensicherheit hat die Kryptografie auch in Schulen Einzug gehalten. Verschlüsselungsverfahren sind heutzutage bereits ab der Mittelstufe ein verpflichtender Teil des Unterrichts. Moderne Verfahren wie AES können erst im Informatikunterricht der gymnasialen Oberstufe behandelt werden. Aber die Betrachtung manueller Verfahren entwickelt ein allgemeines Verständnis für kompliziertere Verfahren. Sie anzuwenden, zu analysieren und zu „knacken“, führt zu einem großen Verständnis für das Thema und baut grundlegende Kompetenzen auf, die zu späteren Zeitpunkten vertieft werden können.

Dabei ist wichtig, dass bei diesem Thema die Kompetenzen der Schülerinnen und Schüler je nach Komplexität des Inhalts, nach Alter und Leistungsvermögen auf einem unterschiedlichen Niveau entwickelt werden können. Handlungsorientiertes Lernen und vielfältige Möglichkeiten, den Unterricht variabel zu gestalten, vermitteln nicht nur Wissen, sondern fördern auch praktische Fähigkeiten und soziale Kompetenzen.

Um die Ideen hinter den dargestellten Verschlüsselungsverfahren herauszuarbeiten, existiert zu jedem Verfahren ein Beispiel, das bisher noch nirgendwo veröffentlicht wurde. Diese werden ausführlich und verständlich in einzelnen nachvollziehbaren Schritten beschrieben. Ausdrucksstarke Grafiken unterstützen das Verständnis.

Eine Beschreibung der Algorithmen zur Entschlüsselung wird dagegen nur bei einzelnen Verfahren gegeben. Die meisten Entschlüsselungen können automatisch nachvollzogen werden und werden daher meist nicht genauer aufgeführt. Nur wenn dazu kompliziertere Schritte erforderlich werden, werden sie mit einem zusätzlichen Beispiel erläutert. Dies geschieht vorzugsweise bei komplexeren Verfahren, bei denen die einzelnen Schritte nicht aus dem Vorgehen bei der Verschlüsselung ersichtlich sind.

Nicht behandelt werden Verschlüsselungen mit Nomenklaturen (Codebücher), symbolbasierte Alphabete, verborgene Speicherungen mittels Steganografie sowie Verschlüsselungen mit Maschinen. Diese Teilgebiete sind so vielfältig und komplex, dass eine Behandlung den Rahmen dieses Buches sprengen würde.

Schwerte,
September 2025

Holger Danielsson

Interessenkonflikt Der/die Autor*in hat keine für den Inhalt dieses Manuskripts relevanten Interessenkonflikte.

Inhaltsverzeichnis

- 1 Manuelle Kryptografie 1**
 - 1.1 Grundlegende Begriffe und Aufbau des Buches 1
 - 1.2 Modulare Arithmetik 2
- 2 Monoalphabetische Substitution 5**
 - 2.1 Historische Verfahren 6
 - 2.1.1 Atbash 6
 - 2.1.2 Albam 7
 - 2.1.3 Atbah 8
 - 2.1.4 Caesar 9
 - 2.1.5 Augustus 10
 - 2.1.6 ROT13 11
 - 2.1.7 Kamasutra 12
 - 2.1.8 Wolseley 13
 - 2.2 Allgemeine Verfahren 15
 - 2.2.1 Affine Substitution 15
 - 2.2.2 Aristocrat – Patristocrat 17
- 3 Polyalphabetische Substitution 21**
 - 3.1 Entwicklung der polyalphabetische Substitution 23
 - 3.1.1 Alberti 23
 - 3.1.2 Trithemius 28
 - 3.1.3 Bellaso 33
 - 3.1.4 Porta 41
 - 3.2 Vigenère und verwandte Verschlüsselungen 43
 - 3.2.1 Vigenère 43
 - 3.2.2 Beaufort 45
 - 3.2.3 Variante Beaufort 47
 - 3.2.4 Rozier 49
 - 3.2.5 Vigenère (ungeordnet) 51

3.2.6	Saint-Cyr Schieber	53
3.2.7	Gronsfeld	55
3.2.8	Italienische Taschenschiffre	56
3.2.9	Wilhelm (Fuer God)	57
3.2.10	Key-Vowel	60
3.2.11	Auvray	61
3.3	Besondere Schlüssel	63
3.3.1	Autokey	63
3.3.2	Progressive Key	65
3.3.3	Interrupted Key	66
3.3.4	Running Key	67
3.3.5	Quagmire	67
3.3.6	Ragbaby	71
3.4	One-Time-Pad	72
3.4.1	Was ist ein One-Time-Pad?	72
3.4.2	Diana	73
4	Homophone Verschlüsselungen	77
4.1	Argenti	78
4.2	Chiffrierscheibe der mexikanischen Armee	81
4.3	Spanish Strip Cipher	83
4.4	Verschleierung der Häufigkeiten	84
5	Checkerboard	87
5.1	Historische Chiffren	87
5.1.1	Polybios	87
5.1.2	Weitere Tabellenvarianten	90
5.1.3	Polybios mit Buchstaben	91
5.1.4	Vier Polybios-Quadrate	92
5.1.5	Givierge	94
5.1.6	Sidewinder	95
5.1.7	Polybios (fragmentiert)	96
5.2	Modernere Tabellen	97
5.2.1	Chase	97
5.2.2	Matrix	99
5.2.3	Syllabary	101
5.2.4	Hocheck	103
5.2.5	Checkerway	105
5.3	Homophone Checkerboards	107
5.3.1	Homophone Polybios-Quadrate	107

5.3.2	Grandpré	110
5.3.3	Sacco	112
6	Straddling Checkerboard	115
6.1	Argenti	115
6.2	Moderne Form (Meurling)	117
6.3	Monome-Dinome	118
6.4	Ché Guevara	120
6.5	Spionage-Chiffren	121
6.5.1	DEINSTAR	122
6.5.2	EISTRAND	123
6.5.3	STEINRAD	124
6.5.4	Karten-Kosak	125
6.5.5	AEIOU	126
7	Transposition	127
7.1	Einfache Transpositionen	128
7.1.1	Skytale	128
7.1.2	Skytale (abgewandelt)	130
7.2	Geometrische Muster	131
7.2.1	Railfence	131
7.2.2	Redefence	134
7.2.3	Routen	134
7.2.4	Kreuz-Transposition	138
7.2.5	Fleißner-Schablone	139
7.2.6	Dreiecks-Transposition	140
7.2.7	Dreieck mit Diagonalen	143
7.2.8	Trapez-Transposition	146
7.2.9	Rechteck mit Diagonalen	146
7.3	Spaltentranspositionen	148
7.3.1	Einfache Spaltentransposition	148
7.3.2	Zeilen-Spalten-Transposition	151
7.3.3	Nihilisten-Transposition	152
7.3.4	Doppelte Spaltentransposition	153
7.3.5	Doppelwürfel	154
7.4	Amadi	156
7.5	Unvollständig gefüllte Zeilen	158
7.6	Auto-Transposition	159
7.7	Permutationen	160

7.8	Sequence Transposition	161
7.9	Listenmethode von Roche	163
7.10	Tabellenmethode von Roche	165
7.11	Magisches Quadrat	167
7.12	Myszkowski	170
7.13	AMSCO	171
7.14	Swagman	173
7.15	Cadenus	175
7.16	Binärer Baum	177
8	Fragmentierte Verfahren	181
8.1	Verfahren von Delastelle	181
8.1.1	Bifid	182
8.1.2	Bifid-Bigramme	185
8.1.3	CM-Bifid	187
8.1.4	Trifid	188
8.2	Hermann	190
8.3	ADFGX	192
8.4	ADFGVX	193
8.5	Collon	197
8.6	Compressocrat	199
8.7	Verschlüsselung mit Morsezeichen	202
8.7.1	Pollux	202
8.7.2	Morbit	203
8.7.3	Morfid	205
8.7.4	Fragmentierter Morsecode	206
9	Polygrafische Verfahren	209
9.1	Playfair-Verfahren	209
9.1.1	Playfair	210
9.1.2	Seriated Playfair	213
9.2	Verwandte Verfahren	215
9.2.1	Doppelkasten	215
9.2.2	Four Square	220
9.2.3	Two Square	222
9.2.4	Tri Square	224
9.2.5	Digrafid	226

9.3	Octafair	230
9.4	Trigrafisches Playfair	233
9.5	Slidefair	236
9.6	Trifair	238
9.7	Hill	240
10	Substitution und Transposition	247
10.1	ABC	247
10.2	Bazeries	249
10.3	Nicodemus	250
10.4	Gromark	253
10.5	Gromark (periodisch)	255
10.6	Portax	258
10.7	Nihilisten-Substitution	261
10.8	Josse	263
10.9	CONDI	266
10.10	Phillips	267
11	Spionage-Chiffren	271
11.1	Granit E 160	271
11.2	VIC	274
11.3	Spionagering Sorge	281
12	Moderne manuelle Verfahren	285
12.1	Hutton	285
12.2	ElsieFour	287
12.3	Solitaire	292
12.4	Chao	296
12.5	SECOM	302
	Glossar	309
	Literatur	319
	Index	329



1

Manuelle Kryptografie

1.1 Grundlegende Begriffe und Aufbau des Buches

Die Wissenschaft von der Verschlüsselung und Entschlüsselung von Informationen nennt man *Kryptografie*. Sie spielt eine zentrale Rolle in der digitalen Welt, da sie Informationen durch Verschlüsselung sichert und vor unbefugtem Zugriff schützt. Der Name stammt aus dem Griechischen und setzt sich aus den Wörtern *kryptós* (versteckt, verborgen, geheim) und *gráphein* (schreiben) zusammen. Heutzutage umfasst dieser Begriff etwas allgemeiner das Thema *Informationssicherheit*.

Ursprünglich aus alten Verschlüsselungstechniken wie ägyptischen Hieroglyphen entstanden, hat sich Kryptografie zu einem unverzichtbaren Bestandteil in der modernen Nachrichtenübertragung entwickelt. Älteste Spuren von Verschlüsselungen lassen sich bis ca. 2000 v. Chr. in Ägypten nachweisen, wo in Schriften unübliche Hieroglyphen verwendet werden.

Allerdings gibt es seit jeher geschickte Methoden, auch ohne den Schlüssel an den Inhalt der Nachricht zu gelangen. Mit solchen Methoden beschäftigt sich die *Kryptoanalyse*. Heutzutage wird mit diesem Begriff eher die Analyse kryptografischer Verfahren verstanden, um ihre Sicherheit und ihre Stärken zu bestimmen. Trotzdem spielt das unbefugte Entziffern geheimer Nachrichten ohne Kenntnis des Schlüssels immer noch eine zentrale Rolle. Beide Teilgebiete zusammen nennt man *Kryptologie*.

Unter dem Begriff der *manuellen Kryptografie*, oft auch Papier- und Bleistiftverfahren genannt, lassen sich alle Verfahren zusammenfassen, die Menschen per Hand anwenden können, um Nachrichten zu ver- und entschlüsseln. Streng genommen existieren unter den manuellen Verfahren der Kryptografie aber nur drei grundlegend unterschiedliche Arten:

- Substitution
- Transposition
- Kombination von Substitution und Transposition

Eine Unterteilung des Buches in nur drei Kapitel würde den über 150 behandelten Verschlüsselungsverfahren aber nicht gerecht, da sie viel zu unübersichtlich werden würde.

Daher wird in diesem Buch eine differenziertere Einteilung in Kategorien vorgenommen. Dies führt zwar auch zu Problemen, da z. B. die ADFGVX-Chiffre sowohl eine Checkerboard-Verschlüsselung als auch eine fragmentierte Verschlüsselung ist. In solchen mehrdeutigen Fällen wurden die Verfahren dann immer der Kategorie derjenigen Verschlüsselungsstrategie zugeordnet, der allgemein eine größere Gewichtung attestiert wird. Bei der ADFGVX-Chiffre ist dies dann die Fragmentierung, da das Checkerboard nur im ersten Teilschritt benutzt wird.

Trotzdem lässt sich dieses Vorgehen nicht in allen Fällen eindeutig durchführen. Insbesondere bei kombinierten Verfahren, die aus einer Substitution und einer Transposition bestehen, lässt sich oft keine eindeutige Zuordnung treffen. Dies führt dann bei der Einteilung in Kategorien zu einer subjektiven Entscheidung.

Deshalb ist das Inhaltsverzeichnis klar gegliedert und liefert einen detaillierten Überblick aller dargestellten Verfahren. Bei der Suche nach bestimmten Verfahren oder Fachbegriffen kann auch das strukturierte Stichwortverzeichnis von Vorteil sein.

Da nicht bei jedem der vielen beschriebenen Verfahren alle wichtigen Fachbegriffe verständlich beschrieben werden können, leistet das Glossar in solchen Fällen eine gute Hilfe.

1.2 Modulare Arithmetik

Für die dargestellten Verschlüsselungen wird häufig *modulare Arithmetik* verwendet.¹ Ohne jetzt die mathematische Zahlentheorie tiefgreifend und exakt zu beschreiben, müssen wenigstens die beiden Begriffe *Äquivalenzrelationen* und *Äquivalenzklassen* verständlich erklärt werden.

Es sei $n \in \mathbb{N}$. Dann gilt für die Relation *kongruent modulo n*

$$a \equiv b \pmod{n} \iff n \mid a - b$$

Anschaulich bedeutet dies, dass zwei Zahlen kongruent modulo n sind, wenn ihre Differenz durch n teilbar ist. So gilt etwa

¹ Gomez [78] S. 27–33

33 mod 5 = 3 18 mod 5 = 3 3 mod 5 = 3 − 2 mod 5 = 3

Im letzten Beispiel folgt $3 - (-2) = 5$ und das Ergebnis ist durch 5 teilbar. Dagegen gilt $-3 \bmod 5 \neq 3$, denn $3 - (-3) = 6$ ist nicht durch 5 teilbar.

Die *Äquivalenzklasse* modulo n einer Zahl a ist die Menge aller ganzen Zahlen der Form

$a + k n$

wobei k eine beliebige ganze Zahl ist. Sie wird auch als *Restklasse modulo n* bezeichnet und mit $a \bmod n$ geschrieben. Meistens wird die kleinste nichtnegative Zahl der Äquivalenzklasse als Standardrepräsentant aller Zahlen dieser Klasse gewählt.

Das Rechnen mit den Zahlen einer Äquivalenzklasse nennt man *modulare Arithmetik*. Addition, Subtraktion und Multiplikation werden ganz normal durchgeführt, und anschließend die modulo-Operation ausgeführt. Bei der Subtraktion kann das Zwischenergebnis durchaus eine negative Zahl sein. Nun gilt aber

$a \bmod n \equiv (a + k n) \bmod n$

sodass die negative Zahl wieder als Standardrepräsentant aus der Zahlenmenge $\{0, 1, 2, \dots, n - 1\}$ geschrieben werden kann. In Abbildung 1.1 sind die Verknüpfungstabellen für Rechnungen modulo 5 angegeben.

$\begin{array}{c c} \backslash & b \\ a & \end{array}$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(a + b) \bmod n$

$\begin{array}{c c} \backslash & b \\ a & \end{array}$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

$(a - b) \bmod n$

$\begin{array}{c c} \backslash & b \\ a & \end{array}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$(a \cdot b) \bmod n$

Abb. 1.1 Verknüpfungstabellen modulo $n = 5$

In der Kryptografie wird die modulare Arithmetik bei vielen Verschlüsselungsverfahren benutzt. Hierzu werden zunächst alle Buchstaben des Alphabets durch die Zahlen von 0 bis 25 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

Abb. 1.2 Codierung der Buchstaben durch Zahlen

Abhängig vom gewählten Verfahren kommt die modulare Arithmetik mit diesen Zahlen zum Einsatz. Bei einem Standardalphabet mit 26 Buchstaben werden dann alle Rechnungen modulo $n = 26$ ausgeführt.²

² Gomez [78] S. 32–35



2

Monoalphabetische Substitution

Monoalphabetische Substitutionen sind eine der einfachsten Verschlüsselungsarten, bei denen nach einem festgelegten Schema jedes Zeichen des Klartextes stets durch ein anderes, ihm zugeordnetes Zeichen ersetzt wird. Daher kann man bei diesen Verfahren zu dem benutzten Alphabet immer das gewählte Tauschalphabet direkt darunterschreiben. So sind diese Chiffren besonders leicht durchzuführen.

Sie bieten neben der Einfachheit eine beeindruckende Anzahl verschiedener möglicher Zuordnungen.

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$$

Diese große Anzahl vermittelte lange eine Sicherheit, die aber gar nicht vorhanden war. Zudem reduziert sich die Anzahl der Zuordnungen bei vielen Verfahren auf einige wenige Möglichkeiten.

Die Einfachheit und die große Anzahl möglicher Schlüssel der Substitutionen führten dazu, dass solche Verfahren jahrhundertlang benutzt wurden, obwohl im arabischen Raum *Al-Kindi* bereits etwa 850 n. Chr. Angriffe auf verschlüsselte Nachrichten mit der Häufigkeitsanalyse beschrieben hat. Von ihm stammt auch die erste Abhandlung über Kryptoanalyse.¹

Die Häufigkeit der in einem Text auftretenden Buchstaben ist für jede natürliche Sprache charakteristisch. Für die deutsche Sprache ist sie in Tabelle 2.1 angegeben.² Dabei werden die Umlaute ä, ö und ü, ß, wie in der klassischen Kryptografie üblich, als ae, oe, ue und ss gezählt.³

¹ Gomez [78] S. 38–39, Pincock [127] S. 13, Mrayati [117]

² Gomez [78] S. 39

³ Gomez [78] S. 38–41, Kippenhahn [97] S. 146–149, Pincock [127] S. 23–26, 37–38, 146–147

A	6,51 %	G	3,01 %	L	3,44 %	Q	0,02 %	V	0,67 %
B	1,89 %	H	4,76 %	M	2,53 %	R	7,00 %	W	1,89 %
C	3,06 %	I	7,55 %	N	9,78 %	S	7,89 %	X	0,03 %
D	5,08 %	J	0,27 %	O	2,51 %	T	6,15 %	Y	0,04 %
E	17,41 %	K	1,21 %	P	0,79 %	U	4,35 %	Z	1,13 %
F	1,66 %								

Tab. 2.1 Häufigkeitsverteilung der Buchstaben in der deutschen Sprache

Die Prozentangaben der Häufigkeitsverteilung bleiben bei monoalphabetischen Substitutionen auch nach dem Verschlüsseln erhalten, da die Buchstaben nur untereinander ausgetauscht werden. So ist das E in der deutschen Sprache mit einer Häufigkeit von etwa 17,41 % der meistverwendete Buchstabe. Der Buchstabe, der im zu entschlüsselnden Geheimtext die größte Häufigkeit aufweist, entspricht daher mit hoher Wahrscheinlichkeit dem E.

Monoalphabetische Chiffren sind seit vielen Jahrhunderten für eine sichere Kommunikation überholt. Trotz ihrer Einfachheit und der einfachen Entschlüsselung ist die monoalphabetische Substitution aber bemerkenswert, da sie das Konzept der Substitution in die Kryptografie einführt und grundlegende Konzepte vermittelt.

Einerseits treten Substitutionen sehr häufig bei später genutzten Verfahren auf und sind andererseits auch gut geeignet, Verständnis für komplexere Verfahren zu vermitteln.

2.1 Historische Verfahren

Monoalphabetische Verschlüsselungen waren wegen ihrer Einfachheit in der Antike weit verbreitet. Sie sind leicht zu verstehen und erfordern für die Vertauschungen der Buchstaben nur ein grundlegendes Verständnis. Da sie für die Entwicklung der Kryptografie einen wichtigen Beitrag geleistet haben, sollen sie hier in ihrem geschichtlichen Ablauf dargestellt werden.

2.1.1 Atbash

Atbash ist eine monoalphabetische Substitutionschiffre, die ab ca. 500 v. Chr. in Palästina ursprünglich zur Verschlüsselung des 22 Buchstaben umfassenden hebräischen Alphabets verwendet wurde.⁴

⁴ Kahn [90] S. 77–79, Pincock [127] S. 17–18, Wrixon [165] S. 19–20, Bauer [6] S. 49

Der Name *Atbash* leitet sich von den beiden ersten und letzten Buchstaben des hebräischen Schriftsystems (A-T-B-Sch) ab. Er illustriert zugleich das Vorgehen, bei dem der erste Buchstabe (Alef) mit dem letzten Buchstaben (Tav) vertauscht wird, der zweite Buchstabe (Bet) mit dem vorletzten Buchstaben (Sin/Schin) usw.

Modifiziert man dieses Prinzip für das lateinische Alphabet mit 26 Buchstaben, ergibt sich das Tauschalphabet aus Abbildung 2.1

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

Abb. 2.1 Tauschalphabet für das Atbash-Verfahren

Mit diesem Tauschalphabet lässt sich dann leicht der Geheimtext bestimmen.

Klartext	Dies ist ein geheimer Text										
Geheimtext	WRVH	RHG	VRM	TVSV	RNVI	GVCG					

Abb. 2.2 Verschlüsselung mit der Atbash-Chiffre

Eine Besonderheit dieses Verfahrens ist, dass es umkehrbar ist, also Verschlüsselungs- und Entschlüsselungsmethode identisch sind. Daher genügt es, die Atbash-Substitution ein zweites Mal auf den Geheimtext anzuwenden, um wieder den Ausgangstext zu erhalten.

Die Atbash-Chiffre kann als Sonderfall der *Affinen Substitution* angesehen werden. Dort werden die n Zahlen $0, 1, \dots, n - 1$ einem Alphabet zugeordnet. Das hebräische Alphabet hat $n = 22$ und das lateinische Standardalphabet $n = 26$ Buchstaben. Sie kann also mit der Verschlüsselungsfunktion für eine affine Substitution verschlüsselt und entschlüsselt werden, indem $a = b = n - 1$ gesetzt werden. Für die Verschlüsselung und Entschlüsselung ergibt sich

$$G = (n - 1) - K \bmod n \qquad \text{und} \qquad K = (n - 1) - G \bmod n$$

2.1.2 Albam

Albam ist eine dem Atbash ähnliche Verschlüsselungsmethode.⁵ Das aus 22 Zeichen bestehende hebräische Alphabet wird in zwei Hälften zu je elf Buchstaben unterteilt, die einander direkt zugeordnet werden. Der Name *Albam* rührt von den

⁵ Kahn [90] S. 78–79, Bauer [6] S. 49

beiden ersten zu vertauschenden Buchstabenpaaren her: Alef mit Lamed, Bet mit Mem.

Diese Verschlüsselung basiert auf demselben Prinzip, das auch beim lateinischen Alphabet bei der ROT13-Chiffre angewendet wird. Durch die Verschiebung der Zeichen um die halbe Länge des Alphabets sind Verschlüsselung und Entschlüsselung identisch.

Überträgt man Albam ohne Anpassungen auf das lateinische Alphabet mit 26 Buchstaben, ergibt sich eine Verschiebung von 11 Zeichen, was dasselbe Ergebnis liefert wie eine Verschlüsselung mit ROT11 und ROT15 beim Entschlüsseln, also Verschiebungen um 11 und 15 Zeichen.

Alphabet	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
Tauschalphabet	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

Mit diesem Tauschalphabet ergibt sich bei der Albam-Verschlüsselung der Geheimtext aus Abbildung 2.3.

Klartext	Dies ist ein geheimer Text
Geheimtext	OTPD TDE PTY RPSPTXPC EPIE

Abb. 2.3 Verschlüsselung mit der *Albam*-Chiffre

2.1.3 Atbah

Auch die *Atbah*-Verschlüsselung ist eine Chiffre, die von den Hebräern verwendet wurde.⁶ Die ersten neun Buchstaben des hebräischen Alphabets wurden verschlüsselt, indem die Buchstaben von 1 bis 9 nummeriert und durch ein Zeichen ersetzt wurden, dessen Ordnungszahl dem Komplement der Zahl bis 10 entspricht.

Der erste Buchstabe des hebräischen Alphabets, Alef, wird durch den Buchstaben Tet ersetzt, der an neunter Stelle steht, und umgekehrt. Der zweite Buchstabe Bet wird durch den Buchstaben Het ersetzt, der an achter Stelle steht.

Die nächsten 9 Buchstaben werden auf die gleiche Weise substituiert. Jedoch wird der mittlere Buchstabe dieser Buchstabengruppe mit dem mittleren Buchstaben der ersten Gruppe ersetzt und umgekehrt. Wie die weiteren Zeichen substituiert wurden, ist nicht bekannt.

⁶ Kahn [90] S. 79, Fronczak [69]

Die mit dieser unvollständigen Regel für hebräische Zeichen erstellte Umwandlungstabelle für das lateinische Alphabet sieht für die ersten 18 Buchstaben folgendermaßen aus:

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
I	H	G	F	N	D	C	B	A	R	Q	P	O	E	M	L	K	J								

Abb. 2.4 Unvollständiges Tauschalphabet

Für nicht verwendete Zeichen wird üblicherweise ein Zusatz verwendet, der den gegenseitigen Austausch der Zeichen bewahrt.

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

Abb. 2.5 Unvollständiges Tauschalphabet

Da diese Verschlüsselung umkehrbar ist, kann die modifizierte Umwandlungstabelle auch in abgekürzter Form geschrieben werden:

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

Abb. 2.6 Modifiziertes Tauschalphabet

Mit diesem Tauschalphabet ergibt sich der Geheimtext aus Abbildung 2.7.

Klartext	Dies ist ein geheimer Text
Geheimtext	FANZ AZY NAE CNBNAONJ YNUY

Abb. 2.7 Verschlüsselung mit der *Atbah*-Chiffre

2.1.4 Caesar

Die *Caesar*-Verschlüsselung ist eines der frühesten und einfachsten Verschlüsselungsverfahren. Der römische Historiker Gaius Suetonius Tranquillus (ca. 70 - 135 n. Chr.) beschrieb in einem seiner Bücher, dass Julius Caesar (100 - 44 v. Chr.) dieses Verfahren zum Austausch privater und militärischer Nachrichten verwendete.⁷

⁷ Suetonius [151] S. 97

Bei diesem Verfahren wird jeder Buchstabe durch den Buchstaben ersetzt, der sich zyklisch gesehen drei Positionen weiter im Alphabet befindet.⁸ Mit dem Buchstaben X beginnt man damit wieder bei A vorn im Alphabet. Bei einem lateinischen Alphabet mit 26 Buchstaben ergibt sich folgendes Tauschalphabet.

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

Also wird der Buchstabe A durch ein D ersetzt, ein B durch ein E, und so weiter. Führt man diese Verschiebung für jeden Buchstaben durch, erhält man den Geheimtext.

Klartext	Dies ist ein geheimer Text									
Geheimtext	GLHV	LVW	HLQ	JHKHL	PHU	WHAW				

Abb. 2.8 Verschlüsselung mit der *Caesar*-Chiffre

Es existiert eine Reihe von Verfahren, die sich nur durch die Größe der Verschiebung von der Caesar-Verschlüsselung unterscheiden. Sie sind aber alle nur ein Spezialfall der *Affinen Substitution*.

Mathematisch lässt sich die Caesar-Verschlüsselung leicht mithilfe der modularen Arithmetik modulo 26 beschreiben. Die Verschlüsselung eines Klartextbuchstabens K durch den Geheimtextbuchstaben G wird durch die Gleichung

$$G = (K + 3) \bmod 26$$

definiert. Entsprechend lautet die Gleichung für die Entschlüsselung

$$K = (G - 3) \bmod 26$$

Mit diesen beiden Gleichungen lassen sich die beiden Verschiebungen mathematisch eindeutig darstellen.

2.1.5 Augustus

Der Nachfolger von Caesar, Kaiser Augustus (63 v. Chr. - 14 n. Chr.), hielt die Verschlüsselung von Caesar für zu schwer und wandte eine noch einfachere Verschiebung an. Er ersetzte bis auf eine Ausnahme jeden Buchstaben durch den nächsten im Alphabet. Bis auf den letzten Buchstaben im römischen Alphabet: Das X ersetzte er durch den Doppelbuchstaben AA.⁹

⁸ Kippenhahn [97] S. 97 – 107, Pincock [127] S. 17 – 18, Gomez [78] S. 32 – 35, Kahn [90] S. 83 – 84

⁹ Das römische Alphabet umfasste zu der Zeit nur 21 Buchstaben.

Auf das heutige lateinische Alphabet mit 26 Buchstaben angewendet ergibt sich folgendes Tauschalphabet:¹⁰

Alphabet	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
Tauschalphabet	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	AA

Mit diesem Tauschalphabet wird ein Klartext wie in Abbildung 2.9 verschlüsselt.

Klartext	Dies ist ein geheimer Text
Geheimtext	EJFT JTU FJO HFIFJNFS UFYU

Abb. 2.9 Verschlüsselung mit der *Augustus*-Chiffre

2.1.6 ROT13

Überraschenderweise wurde eine einfache Verschiebung wie die von Caesar zu den Anfangszeiten des Internets wiederentdeckt. ROT13 (Abkürzung für Rotation 13) ist die Bezeichnung für eine sehr einfache monoalphabetische Substitutionschiffre mit einem festen Schlüssel. Sie ersetzt jeden Buchstaben aus dem lateinischen Alphabet mit 26 Buchstaben durch den Buchstaben, der sich zyklisch gesehen 13 Buchstaben weiter im Alphabet befindet.

Allerdings geht es bei ROT13 eigentlich nicht um die Verschlüsselung von Nachrichten, die versendet werden. Sondern es soll sichergestellt werden, dass die Nachricht nicht unbeabsichtigt gelesen werden kann, etwa wenn sie die Handlung eines Films verrät oder die Lösung eines Rätsels liefert.

Die ROT13-Chiffre wird gerne zum Verstecken von Inhalten verwendet, da sie leicht rückgängig gemacht werden kann. Wenn sie nämlich zweimal angewendet wird, erscheint die ursprüngliche Nachricht wieder.

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

Der sich ergebende Geheimtext einer Verschlüsselung ist leicht zu erstellen und ein Beispiel ist in Abbildung 2.10 dargestellt.

Klartext	Dies ist ein geheimer Text
Geheimtext	QVRF VFG RVA TRURVZRE GRKG

Abb. 2.10 Verschlüsselung mit der *ROT13*-Chiffre

¹⁰ Suetonius [151] S. 289, Bauer [6] S. 51, Kahn [90] S. 84

Mathematisch lässt sich ROT13 mit der modularen Arithmetik modulo 26 beschreiben. Die Verschlüsselung und Entschlüsselung eines Klartextbuchstabens K durch den Geheimtextbuchstaben G wird durch zwei Gleichungen beschrieben.

$$G = (K + 13) \bmod 26 \quad \text{und} \quad K = (G + 13) \bmod 26$$

Zu ROT13 gibt es beispielsweise mit ROT5 und ROT11 verwandte Verschiebungen, bei denen sich die Größe der Verschiebung aus dem jeweiligen Namen ergibt. Dabei kann eine Verschiebung um x Buchstaben immer durch eine weitere Verschiebung von $y = 26 - x$ Buchstaben wieder rückgängig gemacht werden. Alle diese Verschlüsselungen sind wie die Caesar-Verschlüsselung nur Spezialfälle der *Affinen Substitution*.

2.1.7 Kamasutra

Die *Kamasutra*-Chiffre ist eine der ältesten monoalphabetischen Substitutionschiffren und wurde vom Philosophen Vatsyayana vermutlich im vierten Jahrhundert n. Chr. geschrieben. Es basiert allerdings auf Manuskripten, die bereits im vierten Jahrhundert v. Chr. verfasst wurden.¹¹ Neben Ratschlägen zur Lebensführung, Verhaltensweisen, Kochen, Kleidung, Erotik und sonstigen Dingen, die eine Frau nach damaliger Ansicht wissen sollte, wurden ihnen auch Tipps gegeben, wie sie geheime Botschaften vor neugierigen Blicken verbergen können.

Der Schlüssel ist eine zufällige Permutation des Alphabets, das beim heutigen Alphabet in zwei Hälften mit jeweils 13 Buchstaben geteilt wird. Die Hälften werden untereinander geschrieben, um die Buchstaben zu paaren.

Mit diesem Vorgehen entsteht ein symmetrisches Muster. Wenn ein A durch ein J ersetzt wird, wird ein J durch ein A ersetzt. Dies führt zu einer umkehrbaren Chiffre, bei der Verschlüsselungs- und Entschlüsselungsmethoden identisch sind.

Alternativ lässt sich diese Tauschtablelle auch für ein geordnetes Alphabet darstellen.

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

Um die Nachricht mit dem dargestellten Tauschalphabet zu verschlüsseln, beginnt man mit dem ersten Klartextbuchstaben D und ersetzt ihn durch den Partnerbuchstaben F. Das I wird so zu einem C, E wird durch Z ersetzt und so weiter für jeden Buchstaben.

¹¹ Kahn [90] S. 74, Wrixon [165] S. 18–19, Pincock [127] S. 39

Klartext	Dies ist ein geheimer Text					
Schlüssel	VOZLYBAMWCXSDPTEQGNJHUIRKF					
Geheimtext	FCZK	CK0	ZCB	YZMZCHZX	OZRO	

Abb. 2.11 Verschlüsselung mit der *Kamasutra*-Chiffre

2.1.8 Wolseley

Die *Wolseley*-Verschlüsselung ist eine umkehrbare Substitutions-Chiffre, deren Tauschalphabet auf einem Schlüssel basiert und es somit ermöglicht, ein gemischtes Alphabet zu erzeugen.¹² Es ist nicht gesichert, dass dieses Verfahren auch wirklich von Lord Garnet Joseph Wolseley, dem Oberbefehlshaber der britischen Armee, stammt. Auf alle Fälle hat er es jedoch im 19. Jahrhundert häufiger benutzt.

Klartext	Dies ist ein geheimer Text					
Schlüssel	WOLSELEY					

In der Originalversion hat das Alphabet nur 25 Buchstaben ohne J, die mit einem Schlüssel wie WOLSELEY in eine 5 × 5 - Tabelle eingetragen werden. Zusätzlich werden die Buchstaben in der Tabelle von vorn und von hinten mit den Zahlen 1 bis 12 nummeriert. Somit liegen der Klartext- und der Geheimtextbuchstabe diame-
tral entgegengesetzt. Der mittlere Buchstabe H wird dabei ausgelassen.

1	2	3	4	5
W	O	L	S	E
6	7	8	9	10
Y	A	B	C	D
11	12		12	11
F	G	H	I	K
10	9	8	7	6
M	N	P	Q	R
5	4	3	2	1
T	U	V	X	Z

Die Verschlüsselung besteht darin, zu jedem Buchstaben die zugehörige Kennzahl zu bestimmen und durch den Buchstaben zu ersetzen, der dieselbe Kennzahl

¹² Laffin [101] S. 85–87, D’Agapeyeff [43] S. 108–111, British War Office [125] S. 30–31

besitzt. Der Buchstabe D besitzt die Kennzahl 10 und wird daher durch den Buchstaben M ersetzt. Entsprechend wird I mit der Kennzahl 12 durch G ersetzt. Der Buchstabe H besitzt keine Kennzahl und wird unverändert übernommen. Mit diesen Ersetzungen lässt sich der Geheimtext schnell erzeugen.

Geheimtext	MGTUG UETGC ITHTG DTYET OE
------------	----------------------------

Wolseley mit 26 Buchstaben

Bei einem lateinischen Alphabet mit 26 Buchstaben lässt sich das Vorgehen durch eine andere Tabellenform besser darstellen. Mit dem Schlüssel WOLSELEYGEHEIM bestimmt man zunächst das gemischte Alphabet und ordnet den Buchstaben die Kennzahlen zu.

Schlüssel	WOLSELEYGEHEIM
Alphabet	W O L S E Y G H I M A B C D F J K N P Q R T U V X Z
Kennzahlen	1 2 3 4 5 6 7 8 9 10 11 12 13 13 12 11 10 9 8 7 6 5 4 3 2 1

Diese Tabelle kann aber auch direkt als Tauschalphabet angegeben werden, aus dem direkt die zugeordneten Buchstaben abgelesen werden können. Um diese deutlich einfachere Darstellung benutzen zu können, muss das gemischte Alphabet einfach nur umgekehrt werden.

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

Mit diesem Tauschalphabet ergibt sich die Verschlüsselung aus Abbildung 2.12.

Klartext	Dies ist ein geheimer Text
Schlüssel	WOLSELEYGEHEIM
Geheimtext	CNTUN UETNI QTPTN KTYET OE

Abb. 2.12 Verschlüsselung mit der Wolseley-Chiffre

Auch diese Variante ist umkehrbar, sodass die doppelte Ausführung der Verschlüsselung wieder zum Ausgangstext führt. An dem Tauschalphabet erkennt man auch, dass die Wolseley-Chiffre ohne Schlüsselwort identisch mit der Atbash-Chiffre ist.

2.2 Allgemeine Verfahren

Viele der historischen Verfahren können heutzutage allgemeiner formuliert und katalogisiert werden. So gehören beispielsweise alle Verschiebungsschiffren wie Caesar zu der Gruppe der *affinen Substitution*. Weiterhin können auch die verschiedenen Möglichkeiten, Verschlüsselungen durch unterschiedliche Benutzung von Schlüsseln, mit den Festlegungen von *Aristocrat* und *Patristocrat* sauber definiert werden.

2.2.1 Affine Substitution

Die *Affine Substitution* (oder auch *lineare Substitution*) ist eine monoalphabetische Substitutionschiffre, d. h. jeder Buchstabe des Klartextes wird durch einen anderen, eindeutig definierten Buchstaben ersetzt, um den Geheimtext zu bilden. Sie kombiniert mit der *additiven* und der *multiplikativen* Chiffre zwei grundlegende Verschlüsselungen und benötigt zwei Zahlen a und b aus dem Bereich $1 \dots 25$ als Schlüssel.¹³

Klartext	Dies ist ein geheimer Text
Schlüssel	$a=5 \ b=17$

Für die mathematischen Berechnungen werden die Klartextbuchstaben zunächst in Zahlen umgewandelt.

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

Für jeden Klartextbuchstaben K wird der zugehörige Geheimtextbuchstabe G mit der nachfolgenden Formel berechnet:

$$G = (a \cdot K + b) \bmod 26$$

Ist $a = 0$ handelt es sich um eine *additive Substitution*, d.h. der Klartextbuchstabe wird zyklisch gesehen durch den Buchstaben ersetzt, der sich b Positionen weiter rechts im Alphabet befindet. Mit $b = 3$ wäre das dann einfach die Caesar-Verschlüsselung und mit $b = 13$ das ROT13-Verfahren.

Ist dagegen $b = 0$ handelt es sich um eine *multiplikative Substitution*, weil der Code eines Klartextbuchstaben mit a multipliziert wird. Damit der Geheimtext auch wieder entschlüsselt werden kann, muss der Faktor a relativ prim zu der

¹³ Gomez [78] S. 32–35

Länge 26 des Alphabets sein. Diese Zahlen besitzen eine inverse Zahl a^{-1} mit der Eigenschaft, dass ihr Produkt mit a modulo 26 die Zahl 1 ergibt.

$$a \cdot a^{-1} \equiv 1 \pmod{26}$$

Daher kommen nur bei einem lateinischen Alphabet mit 26 Buchstaben ausschließlich die Zahlen aus Tabelle 2.2 infrage.

Faktor	1	3	5	7	9	11	15	17	19	21	23	25
inverse Zahl	1	9	21	15	3	19	7	23	11	5	17	25
Produkt	1	1	1	1	1	1	1	1	1	1	1	1

Tab. 2.2 Erlaubte Faktoren a und ihre inversen Zahlen a^{-1}

Mit den beiden Schlüssel $a = 5$ und $b = 17$ ergibt sich für den Klartextbuchstaben D mit dem Code 3 die Berechnung

$$5 \cdot 3 + 17 = 15 + 17 = 32 \equiv 6 \pmod{26}$$

Der Geheimtextbuchstabe ist damit G mit der Kennzahl 6. In Tabelle 2.3 ist für alle Klartextbuchstaben K die Berechnung der Geheimtextbuchstaben G dargestellt.

K	Code	Multiplikation	Addition	Modulo	G
D	3	15	32	6	G
I	8	40	57	5	F
E	4	20	37	11	L
S	18	90	107	3	D
I	8	40	57	5	F
S	18	90	107	3	D
T	19	95	112	8	I
E	4	20	37	11	L
I	8	40	57	5	F
N	13	65	82	4	E
G	6	30	47	21	V
E	4	20	37	11	L
H	7	35	52	0	A
E	4	20	37	11	L
I	8	40	57	5	F
M	12	60	77	25	Z
E	4	20	37	11	L
R	17	85	102	24	Y
T	19	95	112	8	I
E	4	20	37	11	L
X	23	115	132	2	C
T	19	95	112	8	I

Tab. 2.3 Berechnung mit den Parametern $a = 5$ und $b = 17$

Mit den Berechnungen für alle Buchstaben ergibt sich folgendes Tauschalphabet:

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

Mit diesem Tauschalphabet kann abschließend der Geheimtext erstellt werden.

Geheimtext	GFLD FDI LFE VLALFZLY ILCI
------------	----------------------------

Entschlüsselung

Für die Entschlüsselung werden einfach nur die inversen Zahlen für die beiden Schlüssel a und b bezüglich der Multiplikation und der Addition benutzt. Die inverse Zahl a^{-1} ergibt sich aus Tabelle 2.2, während die inverse Zahl b^{-1} bezüglich der Addition einfach nur $-b$ ist.

$$K = (G - b) \cdot a^{-1} \mod 26$$

Für die Verschlüsselung mit $a = 7$ und $b = 11$ lautet die inverse Zahl $a^{-1} = 15$ und es ergibt sich beispielsweise die Entschlüsselung aus Abbildung 2.13.

Geheimtext	GPNHJ LANPY BNINP RNAON QO
Schlüssel	a=7 b=11
Klartext	DIESW AREIN GEHEI MERTE XT

Abb. 2.13 Entschlüsselung einer *affinen Substitution*

2.2.2 Aristocrat – Patristocrat

Einige der ältesten Verschlüsselungen waren wegen ihrer Einfachheit monoalphabetische Substitutionen, bei denen jeder Buchstabe des Alphabets nach einem festen Schema durch einen anderen Buchstaben ersetzt wurde. Um die Komplexität etwas zu erhöhen, verwenden spätere Versionen ein mit einem Schlüsselwort erstelltes Schlüsselalphabet, das für das Klartextalphabet, das Geheimtextalphabet oder beides verwendet werden kann.

Die *American Cryptogram Association* (ACA) bezeichnet derartige Verschlüsselungen als *Aristocrat*-Chiffren. Sehr eng verwandt mit diesen sind die *Patristocrat*-Chiffren, die die gleiche Methode verwenden, aber Zwischenräume der Worte vorher entfernen.¹⁴

¹⁴ Gaines [72], ACA [4]

Eine zusätzliche Regel besagt, dass sich jeder Klartextbuchstabe von dem zugehörigen Geheimtextbuchstaben unterscheiden muss. Daher können die Schlüsselalphabete verschoben werden, um eine solche Übereinstimmung zu vermeiden. Es werden vier Arten K1, K2, K3 und K4 von Substitutionen verwendet, die sich im Gebrauch der Schlüsselalphabete unterscheiden.

In allen vier Fällen werden Alphabete untereinander geschrieben und dienen als Übersetzungstabelle. Dazu wird für jeden Klartextbuchstaben der darunterstehende Geheimtextbuchstabe zur Verschlüsselung verwendet.

Um Übereinstimmungen von Buchstaben in den beiden Alphabeten zu vermeiden, wird das Schlüsselalphabet für die Geheimtextbuchstaben verschoben. Dies kann beispielsweise durch die Angabe einer Verschiebungszahl geschehen. Eine andere Möglichkeit besteht darin, einen Klartext- und einen Geheimtextbuchstaben anzugeben, an denen die beiden Schlüsselalphabete ausgerichtet werden.

In allen Beispielen wird die Patristocrat-Verschlüsselung gewählt, da in fast allen hier aufgeführten Verschlüsselungen grundsätzlich alle Leerzeichen entfernt werden.

K1

Als Alphabet für die Klartextbuchstaben wird ein gemischtes Alphabet verwendet, für die Geheimtextbuchstaben das normale Alphabet. Dieses Alphabet wird dabei, wie im zweiten Schlüssel angegeben, um acht Positionen verschoben.

Schlüssel	PATRISTOCRAT 8
Klartextalphabet	PATRISOCBDEFGHJKLMNQUVWXYZ
Geheimtextalphabet	STUVWXYZABCDEFGHIJKLMNOPQR

Mit diesen beiden Alphabeten ergibt sich die Verschlüsselung aus Abbildung 2.14.

Klartext	Dies ist ein geheimer Text
Geheimtext	BWCXW XUCWK ECFCW JCVUC PU

Abb. 2.14 Verschlüsselung mit Aristocrat/Patristocrat K1

K2

Hier wird genau umgekehrt vorgegangen und für die Klartextbuchstaben das normale Alphabet verwendet sowie ein gemischtes Alphabet für die Geheimtextbuchstaben.

Schlüssel	PATRISTOCRAT 12
Klartextalphabet	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
Geheimtextalphabet	J K L M N Q U V W X Y Z P A T R I S O C B D E F G H

Abbildung 2.15 zeigt den Klartext und den Geheimtext bei der Verschlüsselung mit diesen beiden Alphabeten.

Klartext	Dies ist ein geheimer Text
Geheimtext	MWNOW OCNWA UNVNW PNSCN FC

Abb. 2.15 Verschlüsselung mit Aristocrat/Patristocrat K2

K3

Für beide Schlüsselalphabete wird das gleiche gemischte Alphabet verwendet.

Schlüssel	PATRISTOCRAT 16
Klartextalphabet	P A T R I S O C B D E F G H J K L M N Q U V W X Y Z
Geheimtextalphabet	E F G H J K L M N Q U V W X Y Z P A T R I S O C B D

Wenn man diese beiden Alphabete für die Verschlüsselung des Standardsatzes benutzt, erhält man den Geheimtext aus Abbildung 2.16.

Klartext	Dies ist ein geheimer Text
Geheimtext	QJUKJ KGUJT WUXUJ AUHGU CG

Abb. 2.16 Verschlüsselung mit Aristocrat/Patristocrat K3

K4

Bei dieser Variante werden zwei Schlüsselworte benutzt, mit denen unterschiedliche gemischte Alphabete erstellt werden.

Schlüssel	ZWEI SCHLUESSEL 6
Klartextalphabet	Z W E I A B C D F G H J K L M N O P Q R S T U V X Y
Geheimtextalphabet	T V W X Y Z S C H L U E A B D F G I J K M N O P Q R