Klaus Schmeh

# Codeknacker gegen Codemacher

## Die faszinierende Geschichte der Verschlüsselung

*4. Auflage*

SACHBUCH

Springer

Codeknacker gegen Codemacher

Klaus Schmeh

# Codeknacker gegen Codemacher

## Die faszinierende Geschichte der Verschlüsselung

4. Auflage

Springer

Klaus Schmeh
Gelsenkirchen, Deutschland

ISBN 978-3-658-34188-6 ISBN 978-3-658-34189-3 (eBook)
https://doi.org/10.1007/978-3-658-34189-3

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer


Planung: Petra Steinmüller
Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

# Inhaltsverzeichnis

# 1

# Ein Wettlauf über 3500 Jahre

Kennen Sie das Voynich-Manuskript? Dieses handgeschriebene Buch (Abb. 1.1) aus dem Spätmittelalter ist ein einziges großes Mysterium. Es ist in einer unbekannten Schrift verfasst. Auf den Text, der sich über 230 Seiten erstreckt, konnte sich bisher niemand einen Reim machen. Auch die zahlreichen Illustrationen darin tragen mehr zur Verwirrung bei, als dass sie eine Hilfe wären. So sind die abgebildeten Pflanzen nicht identifizierbar, die Bedeutung der astrologischen Darstellungen ist unbekannt, und warum im Manuskript so viele nackte Frauen abgebildet sind, hat bisher ebenfalls noch niemand ergründet. Nebenbei weiß man auch nicht, wer das Voynich-Manuskript verfasst hat, wo es entstanden ist und welchem Zweck es dienen sollte.

Das Voynich-Manuskript (in Abschn. 2.15 gibt es mehr dazu) ist eines der spektakulärsten und bekanntesten Beispiele für einen (mutmaßlich) verschlüsselten Text. Doch die Verschlüsselungstechnik hat in ihrer mindestens 3500 Jahre langen Geschichte noch viel mehr Interessantes hervorgebracht. So sind zahlreiche weitere verschlüsselte Texte bekannt – einige davon sind gelöst, andere nicht. Darüber hinaus gab und gibt es knifflige Verschlüsselungsverfahren, ausgeklügelte Verschlüsselungsmaschinen, geniale Codeknacker und nicht zuletzt unzählige Pleiten, Dilettanten und Kuriositäten.

Fachleute bezeichnen die Verschlüsselungstechnik als **Kryptologie**. Der Begriff stammt aus dem Griechischen, wo „kryptos“ für „geheim“ und „logos“ für „Lehre“ steht. Die Kryptologie ist also wörtlich genommen die Lehre des Geheimen. Eine ähnliche Bedeutung hat der Begriff **Kryptografie**. Streng genommen bezeichnet man mit Kryptografie nur das Verschlüsseln, während



K. Schmeh, *Codeknacker gegen Codemacher*, https://doi.org/10.1007/978-3-658-34189-3_1

**Abb. 1.1** Das Voynich-Manuskript (hier eine Nachbildung) ist eines der größten Rätsel der Verschlüsselungstechnik. (Klaus Schmeh)

die Kryptologie auch das unbefugte Entschlüsseln einschließt. In der Praxis werden die beiden Bezeichnungen aber nahezu synonym verwendet.

Dieses Buch ist der Geschichte der Kryptologie gewidmet. Meiner Meinung nach gibt es kaum einen Teilbereich der Technikgeschichte, der so spannend und vielschichtig ist wie die Kryptologie-Geschichte. Vielleicht werden Sie es genauso sehen, wenn Sie dieses Buch gelesen haben.

Die Kryptologie hat den Lauf der Geschichte immer wieder beeinflusst und dabei über Schicksale, Schlachten und ganze Kriege entschieden. Den Höhepunkt dieser Entwicklung markierte zweifellos der Zweite Weltkrieg, in dem Verschlüsselungsmaschinen wie die berühmte Enigma für eine bis dahin unerreichte Verschlüsselungssicherheit sorgten. Doch auch die Dechiffrier-Experten lernten in dieser Zeit dazu. Es entstanden ganze Entschlüsselungsfabriken, die ihrerseits erstaunliche Erfolge erzielen konnten.

**Codeknacker gegen Codemacher**

Nicht nur für den Zweiten Weltkrieg gilt: Das Interessanteste an der Geschichte der Kryptologie ist der seit mindestens 3500 Jahren andauernde Wettlauf zwischen den Erfindern von Verschlüsselungsverfahren und ihren Gegenspielern, den Dechiffrierern. Mit anderen Worten: Es geht um den Kampf der Codeknacker gegen die Codemacher. Die Codemacher haben es

im Laufe der Zeit immer wieder geschafft, ihre Verfahren zu verbessern, doch in nahezu allen Fällen konnten die Codeknacker mit verbesserten Analysemethoden nachziehen. Erst vor etwa 70 Jahren, als die verfügbaren Verschlüsselungsmaschinen immer besser wurden und später auch der Computer Einzug hielt, wendete sich das Blatt erstmals zu Gunsten der Verschlüssler.

Trotz ihrer langen und faszinierenden Geschichte ist die Kryptologie erst spät ins Visier der Historiker geraten. Dies liegt vermutlich daran, dass Verschlüsselung traditionell meist im Verborgenen betrieben wird. Da niemand gern über die Methoden redet, mit denen er den Gegner am Mitlesen hindern will, war die Kryptologie Jahrhunderte lang eine Geheimwissenschaft, die an den Höfen der Mächtigen und im Auftrag des Militärs betrieben wurde. Die Auswirkungen, die das Verschlüsseln und Dechiffrieren auf die Geschichte hatten, blieben dadurch lange unerkannt.

Als Vater der Kryptologie-Geschichtsschreibung gilt der Historiker und Journalist David Kahn. Dieser veröffentlichte 1967 sein Buch *The Codebreakers*, in dem er die Geschichte der Verschlüsselung auf über 1000 Seiten erzählte (Kahn, 1996). Dieses Werk, das 1996 neu aufgelegt wurde, gilt heute als der Klassiker überhaupt zum Thema und wird daher auch in diesem Buch mehrfach zitiert.

Die Kryptologie-Geschichte hat seit Kahns Pionierarbeit immer mehr begeisterte Anhänger gefunden. Längst gibt es eine ganze Szene, die sich damit beschäftigt. Mit der *Cryptologia* erscheint seit über 40 Jahren eine Fachzeitschrift, die hauptsächlich der Kryptologie-Geschichte gewidmet ist (zu einem kleineren Teil berichtet sie auch über aktuelle Verschlüsselungstechnik). Als Mekka der historischen Kryptologie gilt das alle zwei Jahre stattfindende *NSA Cryptologic History Symposium* in Fort Meade bei Baltimore (USA). In Europa hat sich die jährlich an wechselnden Orten abgehaltene *HistoCrypt* etabliert. Längst haben auch Museen die Faszination der Verschlüsselungstechnik entdeckt, und so kann man beispielsweise im Paderborner Heinz Nixdorf MuseumsForum oder im Deutschen Museum in München interessante Kryptologie-Sammlungen betrachten.

**Epochen der Kryptologie-Geschichte**

Die Geschichte der Kryptologie kann man in drei Epochen aufteilen. Die erste und längste Epoche ist das Zeitalter der Verschlüsselung von Hand. Sie begann im Altertum und endete um 1920. In diesen knapp dreieinhalb Jahrtausenden verwendeten Menschen nur Schreibwerkzeug, simple Buchstabenscheiben und ähnliche einfache Vorrichtungen zum Verschlüsseln. Um das Zeitalter der Verschlüsselung von Hand geht es im ersten Teil dieses Buchs.

Um 1920 erfanden gleich mehrere Ingenieure mechanisch ausgeklügelte Geräte zum Verschlüsseln von Nachrichten und läuteten damit das Zeitalter der Verschlüsselungsmaschinen ein. Zur Ikone dieser Epoche wurde die bereits erwähnte deutsche Verschlüsselungsmaschine Enigma, die im Zweiten Weltkrieg eine entscheidende Rolle spielte. Es gab jedoch noch zahlreiche weitere Geräte, die zu dieser Zeit eingesetzt wurden und schließlich in den frühen Jahren des Kalten Kriegs den höchsten Stand ihrer Entwicklung erreichten. Das Zeitalter der Verschlüsselungsmaschinen, das im zweiten Teil dieses Buchs behandelt wird, ging um 1970 zu Ende, als die Elektronik und die Computer-Technik für die Ablösung der mechanischen Apparate sorgte.

So begann schließlich das Zeitalter der Verschlüsselung mit dem Computer, das bis heute andauert. Durch die Nutzung der Informationstechnik erreichte die Kryptologie völlig neue Dimensionen und drang in bis dahin unbekannte Anwendungsbereiche vor. Insbesondere ermöglichte der Computer erstmals auch dem Normalbürger den einfachen Einsatz von starker Verschlüsselung, was interessante Folgen hatte. Um die Höhen und Tiefen der Computer-Verschlüsselung geht es im dritten Teil dieses Buchs.

**Ein paar Fachbegriffe**

Ein Verschlüsselungsverfahren bezeichnet man auch als **Chiffre**. Ein Text, den es zu verschlüsseln gilt, heißt **Klartext**. Das Ergebnis der Verschlüsselung ist der **Geheimtext**. Das unbefugte Entschlüsseln wird als **knacken** oder **dechiffrieren** bezeichnet. Ein Geheimtext, den man dechiffrieren will, heißt **Kryptogramm**. Die einfachste Form der Verschlüsselung ist die **Geheimschrift**. Bei einer solchen gibt es für jeden Buchstaben des Alphabets einen Geheimbuchstaben.

Die bekannteste Geheimschrift ist die Pigpen-Chiffre, die auch als Freimaurer-Chiffre bezeichnet wird (siehe Abb. 1.2). Sie ist seit dem Mittelalter belegt. Es gibt zahlreiche Varianten davon. Zu den bekanntesten Dokumenten, die mit einer Pigpen-Chiffre verschlüsselt sind, gehört die Nachricht, die der Pirat La Buse unmittelbar vor seiner Hinrichtung in die Menge der Schaulustigen geworfen haben soll (siehe Abschn. 2.19). Sie soll die Lage eines Schatzes verraten.

Auch wenn eine Geheimschrift auf den ersten Blick recht geheimnisvoll wirkt, ist sie meist recht einfach zu knacken. Dies liegt daran, dass in allen bekannten Sprachen die verwendeten Buchstaben unterschiedlich oft vorkommen. Im Deutschen ist beispielsweise der Buchstabe E mit 18 Prozent der häufigste, gefolgt vom N mit etwa 10 Prozent (Abb. 1.3). Ein Codeknacker muss daher nur die Buchstaben zählen, um eine Geheimschrift de-

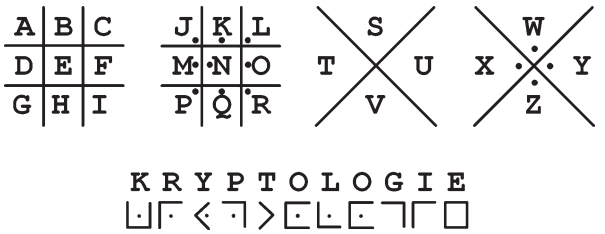


**Abb. 1.2** Die Pigpen-Chiffre ist die bekannteste Geheimschrift. Hier wird als Beispiel das Wort KRYPTOLOGIE damit verschlüsselt. (Klaus Schmeh)

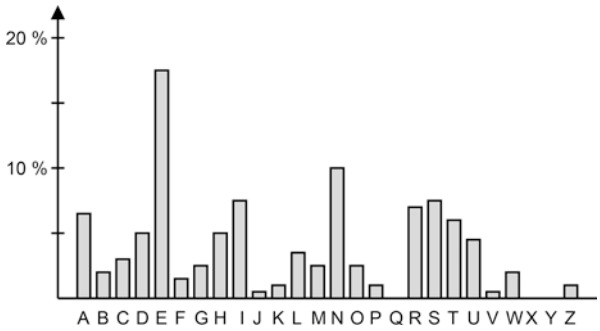


**Abb. 1.3** Die Buchstaben des Alphabets sind in der deutschen Sprache ungleichmäßig verteilt. Das E ist der häufigste Buchstabe. (Klaus Schmeh)

chiffrieren zu können (dies nennt man **Häufigkeitsanalyse**). Schon etwa 40 Buchstaben reichen bei einem deutschsprachigen Text für eine aussagekräftige Häufigkeitsanalyse aus.

Anstatt eine Geheimschrift zu verwenden, kann man Buchstaben auch untereinander ersetzen. Die folgende Tabelle liefert ein Beispiel:

```
Klartext: ...... ABCDEFGHIJKLMNOPQRSTUVWXYZ
Geheimtext: .... ECKHJOQLDRPUVTWSXMNGYFZIBA
```

Das Wort KRYPTOLOGIE verschlüsselt sich damit in PMBSGWUWQDJ. Das bekannteste Verfahren dieser Art ist die Caesar-Chiffre, die Sie in Abschn. 2.1 kennen lernen werden. Das Ersetzen von Buchstaben durch Buchstaben oder Geheimschriftzeichen fasst man unter dem Begriff **einfache Buchstabenersetzung** zusammen. Einfache Buchstabenersetzungen lassen sich mit einer Häufigkeitsanalyse lösen.

In viele Verschlüsselungsverfahren (vor allem in die guten) geht eine Geheiminformation ein, die man als **Schlüssel** bezeichnet. Der Schlüssel kann ein Passwort, aber auch eine bedeutungslose Buchstabenfolge sein. Im

Idealfall kann ein Codeknacker eine Verschlüsselung ohne den Schlüssel nicht knacken – selbst dann nicht, wenn er das Verschlüsselungsverfahren genau kennt. Diese Anforderung bezeichnet man auch als Kerckhoffs'sches Prinzip (siehe Abschn. 2.3).

Zum Schluss dieser Einführung noch eine wichtige Abgrenzung: Die Kryptologie ist nicht mit der **Steganografie** zu verwechseln. Als Steganografie bezeichnet man das Verstecken von Nachrichten. Abb. 1.4 zeigt ein Beispiel aus dem 17. Jahrhundert (Schott, 1665). Im Bild einer Mauer ist das Seneca-Zitat MULTI PERVENIRENT AD SAPIENTIAM NI IAM PUTASSENT SE PERVENISSE versteckt („Viele könnten weise werden, wenn sie nicht meinten, sie wären es schon"). Da die Steganografie ihre eigene, hochinteressante Geschichte hat, habe ich bereits 2008 ein Buch darüber veröffent-

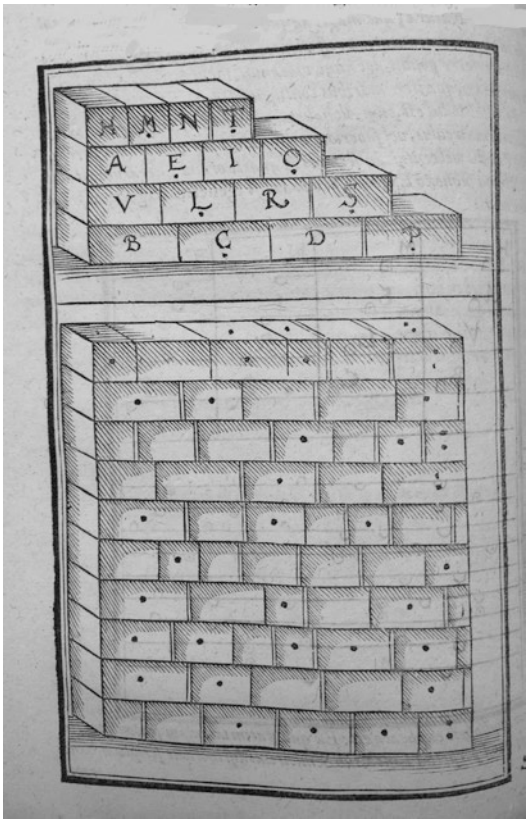


**Abb. 1.4** Ein Beispiel für Steganografie: In der Mauer ist ein Text versteckt. (Caspar Schott: „Schola steganographica" (1680), Wellcome Library, Public Domain, https://wellcomecollection.org/works/tgdms2j8)

licht. Es trägt Titel *Versteckte Botschaften* (Schmeh, 2017). In dem Buch, das Sie gerade lesen, spielt die Steganografie dagegen keine Rolle.

Bevor es losgeht, bleibt mir nur noch eines zu sagen: VPU JHRAF-PUR VUARA IVRY FCNFF ORVZ YRFRA.

## Literatur

Schmeh, K. (2017). *Versteckte Botschaften – Die faszinierende Geschichte der Steganografie.* Heise.
Schott, G. (1665). *Schola Steganographica*. Herbipoli
Kahn, D. (1996). *The Codebreakers.* Scribner.

# 2

# Das Zeitalter der Verschlüsselung von Hand

## 2.1 Als die Schrift zum Rätsel wurde

Wirtschaftsspionage muss bereits im alten Mesopotamien ein Problem gewesen sein. Anders ist es nicht zu erklären, dass dort um 1500 v. Chr. ein Töpfer beim Notieren einer Keramikglasur auf einer Tontafel einen Trick anwandte: Er nutzte die damals üblichen Keilschriftbuchstaben in einer unüblichen Weise und machte dadurch den Inhalt des Texts für Außenstehende unlesbar (Kahn, 1996, S. 75). Mit anderen Worten: Der mesopotamische Töpfer führte eine Verschlüsselung durch.

### Verschlüsselung im Altertum

Die Tontafel des mesopotamischen Töpfers ist erhalten geblieben und gilt heute als der früheste bekannte verschlüsselte Text der Geschichte. Bedenkt man, dass die Menschheit zu diesem Zeitpunkt bereits seit zwei Jahrtausenden die Schrift kannte, dann kommt man nicht umhin festzustellen: Es dauerte lange, bis die Kryptologie Einzug in die Kultur des Menschen hielt.

Das erste überlieferte Buch, das ein Verschlüsselungsverfahren beschreibt, entstand erst mehr als ein Jahrtausend nach der mesopotamischen Tontafel. Dieses Werk trägt den Namen *Poliorketika* und stammt von dem Griechen Aeneas dem Taktiker, der im vierten vorchristlichen Jahrhundert lebte (Whitehead, 2003). Das Buch behandelt eine damals wichtige Frage: Wie sollen sich die Bewohner einer Stadt verhalten, während diese von feindlichen



K. Schmeh, *Codeknacker gegen Codemacher*, https://doi.org/10.1007/978-3-658-34189-3_2

Truppen belagert wird? Noch heute bezeichnet man die Belagerungstechnik als „Poliorketik“.

Für den Fall, dass in einer belagerten Stadt etwas verschlüsselt werden musste, schlug Aeneas ein Verfahren vor, das heute wohl keinen Experten mehr beeindrucken würde. Auf das heutige Alphabet übertragen funktioniert es so: Das A wird durch einen Punkt ersetzt, das E durch zwei Punkte, das I durch drei, das O durch vier, das U durch fünf sowie das Y durch sechs Punkte. Die Konsonanten bleiben unverschlüsselt.:S:.ST N:.CHT B:S::ND:RS SCHW:.:RIG, D:.:S:S V:RF.HR:N Z::. KN.CK:N.

Etwa zur gleichen Zeit findet sich in einem Text des griechischen Geschichtsschreibers Plutarch eine Beschreibung des ersten bekannten Verschlüsselungswerkzeugs der Geschichte: die Skytale. Eine Skytale (auch als Chiffrierstab bekannt) ist ein rundes Stück Holz, um das der Absender einen Lederstreifen (heute würde man Papier nehmen) wickelte, um den Klartext darauf zu schreiben (siehe Abb. 2.1). Der Empfänger benötigte einen Stab gleichen Durchmessers, um die Nachricht zu entschlüsseln. Der Durchmesser des Stabs ist somit die zum Entschlüsseln benötigte Geheiminformation, also der Schlüssel.

Nach heutigen Maßstäben ist die Skytale nicht besonders sicher. Wer ein paar Stäbe unterschiedlicher Dicke durchprobiert, wird schnell die richtige Lösung finden. Ob die alten Griechen die Skytale wirklich einsetzten, ist nach neueren Erkenntnissen ohnehin fraglich – möglicherweise hat Plutarch in diesem Zusammenhang einige Ereignisse kryptologisch aufgebrauscht, die damals schon Jahrhunderte zurücklagen (Kelly, 1998).

Nicht nur die Griechen, sondern auch die Römer kannten bereits Verschlüsselungstechniken. Nach Überlieferung des römischen Schriftstellers Sueton ging beispielsweise Julius Caesar beim Verschlüsseln wie folgt vor: „…

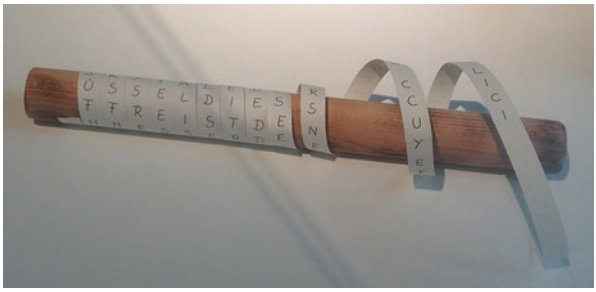

**Abb. 2.1** Die Skytale ist das älteste bekannte Verschlüsselungsgerät. Man schreibt die zu verschlüsselnde Nachricht auf einen Papierstreifen, der um einen runden Stab gewickelt ist. (Klaus Schmeh)

wenn etwas Geheimes zu überbringen war, schrieb er in Zeichen, das heißt, er ordnete die Buchstaben so, dass kein Wort gelesen werden konnte: Um diese zu lesen, tauscht man den vierten Buchstaben, also D für A aus und ebenso mit den restlichen." Mit anderen Worten: Caesar verschob jeden Buchstaben des Alphabets um drei Einheiten (A->D, B->E, C->F usw.). Bis heute spricht man von einer Caesar-Chiffre, wenn jeder Buchstabe im Alphabet um eine bestimme Distanz verschoben wird. Die folgende Tabelle zeigt ein Beispiel:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
UVWXYZABCDEFGHIJKLMNOPQRST
```

Das Wort KRYPTOLOGIE verschlüsselt sich damit in ELSJNIFIACY. Laut dem römischen Schriftsteller Aulus Gellius verwendete Caesar weitere Verschlüsselungsverfahren, über die aber nichts bekannt ist. Eine gewisser Probus soll sogar eine Abhandlung über die Verschlüsselungsverfahren Caesars geschrieben haben, doch leider ist auch diese Arbeit nicht erhalten geblieben. Der erwähnte Sueton berichtet außerdem, dass auch der römische Kaiser Augustus die Caesar-Chiffre nutzte, jedoch mit einer Verschiebung um nur einen Buchstaben. Statt einem X, dem letzten Buchstaben des damaligen lateinischen Alphabets, schrieb Augustus AA.

Es ist leider nicht bekannt, ob die primitiven Verschlüsselungen der Römer ihren Zweck erfüllten. Dies könnte durchaus der Fall gewesen sein, denn die Feinde der Römer waren oftmals Analphabeten, und die wenigen Schriftkundigen dachten möglicherweise, sie hätten es mit einer Fremdsprache zu tun.

Im vierten nachchristlichen Jahrhundert kam erstmals eine wichtige Nutzergruppe der Kryptologie zu ihrem Recht: die Liebenden. Im berühmten indischen Buch *Kama Sutra* werden 64 Künste beschrieben, die eine Frau in Bezug auf die Liebe zu einem Mann beherrschen sollte, darunter Kochen, Massieren, Glücksspiel, der Umgang mit Papageien und die Zubereitung von Parfümen. Nummer 45 auf der Liste ist die „Kunst des verschlüsselten Schreibens und des Schreibens von Wörtern in ungewöhnlicher Form".

Welche Verschlüsselungsverfahren eine Frau verwenden sollte, wird in der *Kama Sutra* jedoch nicht erwähnt. Offensichtlich gab es damals andere Quellen, aus denen sich frau informieren konnte – leider sind sie verloren gegangen. Erst ein Kommentar zur *Kama Sutra* des Gelehrten Yasodhara aus dem 13. Jahrhundert nannte zwei Verschlüsselungsmethoden. Die eine ist eine Buchstabenersetzung, die auf das lateinische Alphabet übertragen etwa so aussieht:

```
KBJHOESNWYCVI
APMRZQGFXDULT
```

Das Wort KAMA SUTRA verschlüsselt sich damit in AKJK GCIHK. Die zweite Verschlüsselungstechnik von Yasodhara sah ebenfalls nur einfache Buchstabenersetzungen vor.

Keine Frage, die Verschlüsselungsmethoden des Altertums waren aus heutiger Sicht ausgesprochen schwach. Ich finde dies durchaus erstaunlich. So waren die alten Griechen bereits in der Lage, den Erdumfang und die Entfernung des Monds von der Erde zu bestimmen, doch in der Kryptologie kamen sie nicht über das heutige Grundschul-Niveau hinaus. Bei den Römern sah es nicht besser aus. Sie eroberten fast die ganze damals bekannte Welt, blieben in der Kryptologie jedoch bei der Caesar-Chiffre stecken. Es gibt aus dem Altertum keine einzige Quelle, die die Verschlüsselungstechnik systematisch behandelt. Anders als später in der frühen Neuzeit ließen die Universalgelehrten des Altertums – von Archimedes bis Cicero – die Kryptologie links liegen.

Die meisten Kulturen des Altertums entwickelten nach heutigem Wissensstand sogar überhaupt keine Verschlüsselungstechnik. Die alten Ägypter beispielsweise, die bekanntlich mit Hieroglyphen schrieben, kamen offensichtlich nicht auf die Idee, diese zu Zwecken der Geheimhaltung durcheinanderzuwürfeln oder abzuändern. Bei den Chinesen verhielt es sich ähnlich. Die chinesischen Schriftzeichen, die für jeden Begriff ein eigenes Zeichen vorsehen, sind für das Verschlüsseln ohnehin denkbar ungeeignet. Auch in der Bibel findet sich nichts Bemerkenswertes zur Kryptologie, wenn man von einigen Tarnnamen (beispielsweise „Babylon“ für „Rom“) absieht.

Warum also kam die Verschlüsselungstechnik in der Menschheitsgeschichte so schwer in die Gänge? Meines Wissens gibt es in der Literatur dazu bisher keine überzeugende Erklärung. Es muss damit zu tun haben, dass damals kein größerer Bedarf für diese Kulturtechnik bestand. Die meisten Menschen konnten noch nicht lesen und schreiben, und ein Postwesen im heutigen Sinne gab es ohnehin noch nicht. Die Bedrohung durch ungebetene Mitleser war daher wohl noch kein ernsthaftes Problem. Vielleicht deshalb fristete die Verschlüsselungstechnik im Altertum nur ein Schattendasein.

## Verschlüsselung im Mittelalter

Die Stadtbibliothek von Trier besitzt ein Buch, das aus mehreren mittelalterlichen Schriften zusammengebunden ist. Eine dieser Schriften stammt vermutlich aus dem 8. oder 9. Jahrhundert (Anonym, 2021a) und gibt einen

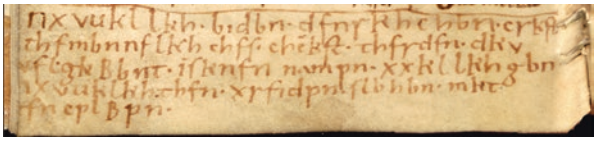

**Abb. 2.2** Der Trierer Teufelsspruch ist ein verschlüsselter Text aus dem Mittelalter. Er sollte vermutlich eine magische Wirkung haben. (©Wissenschaftliche Bibliothek /Stadtarchiv Trier. Foto: Anja Runkel; Ru -Nr. 088 2021. Signatur: © Handschrift 564/806 8°, fol 65 v)

Text des Bischofs Isidor von Sevilla (ca. 560–636) wieder. An eine ursprünglich leere Stelle schrieb jemand – wahrscheinlich noch im 9. Jahrhundert – fünf Textzeilen. Dieser aus 128 Buchstaben bestehende Absatz ist verschlüsselt. Man bezeichnet ihn als den „Trierer Teufelsspruch" (siehe Abb. 2.2).

Der Trierer Teufelsspruch ist nicht schwer zu dechiffrieren. Lediglich die Vokale des Texts sind ersetzt. Der Klartext lautet: „Nu vuillih bidan den rihchan crist, the mannelihches chenist, ther den diuvel gibant. In sinen namon uuillih gan, nu vuilih then ureidon slahan mit ten colbon." In heutiges Deutsch übertragen: „Nun will ich hoffen auf den mächtigen Christ, Rettung jedes Menschen, der den Teufel fesselte: in seinem Namen will ich gehen und den Abtrünnigen mit dem Knüppel erschlagen."

Der Trierer Teufelsspruch ist bei weitem nicht das einzige Kryptogramm aus dem Mittelalter. In den Büchern aus dieser Zeit hat man Hunderte von verschlüsselten Texten und Textpassagen gefunden. Die verwendeten Verschlüsselungsverfahren sind allesamt äußerst schwach. Offensichtlich kannte man im Mittelalter kaum mehr als die einfache Buchstabenersetzung. Oftmals begnügte man sich sogar mit dem Ersetzen der Vokale oder ähnlichen Minimalverschlüsselungen. Der deutsche Kaiser Friedrich III. (1415–1493) verschlüsselte beispielsweise, indem er A durch E, I durch O und B durch C (und jeweils umgekehrt) ersetzte. Dazu verkündete er stolz: „hab ich selbs gedacht" (Chmel, 1840, S. 582).

Interessant ist nun die Frage, warum der Trierer Teufelsspruch überhaupt verschlüsselt wurde. Da vom Teufel die Rede ist, liegt der Verdacht nahe, dass sich der Urheber eine magische Wirkung von der Verschlüsselung versprach. Dies war im Mittealter nicht ungewöhnlich. Die mittelalterliche Gelehrte Hildegard von Bingen (1098–1179) schuf ein Beispiel dafür. Wie viele andere Personen der Kryptologie-Geschichte war auch Hildegard von Bingen vielseitig interessiert. Sie wird heute in der katholischen Kirche als Heilige verehrt, und die Anhänger der Hildegard-Medizin schwören auf die angeblich von ihr entwickelten Heilmethoden. Weniger bekannt ist, dass Hildegard von Bingen mit der „Litterae ignotae" auch eine Geheimschrift entwickelte und verwendete (siehe Abb. 2.3). Vermutlich diente diese nicht in erster Linie der

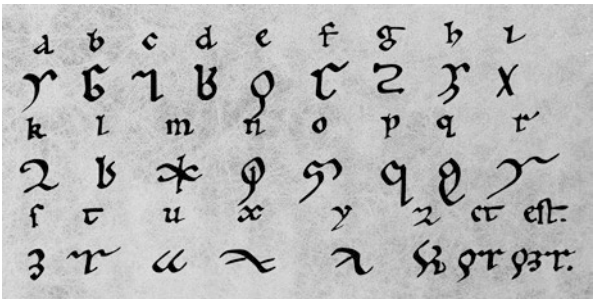

**Abb. 2.3** Auch die Kirchenlehrerin Hildegard von Bingen entwickelte eine Geheimschrift. Ob sie der Geheimhaltung diente, ist unklar. (Klaus Schmeh)

Geheimhaltung, sondern sollte einen magischen Zweck erfüllen (Bausani, 1970, S. 76–78). Leider lässt sich heute nicht mehr sagen, was genau sich Hildegard davon versprach, in dieser Geheimschrift zu schreiben.

Eines der bekanntesten Beispiele für mittelalterliche Verschlüsselungstechnik lieferte der englische Dichter Geoffrey Chaucer. Dieser war nicht nur als Poet, sondern auch als Wissenschaftler aktiv – wir haben es also auch hier mit einem sehr vielseitigen Gelehrten zu tun. Sein Buch *The Equatorie of the Planetis* ist eine Gebrauchsanweisung für ein astronomisches Instrument. In diesem Werk gibt es sechs verschlüsselte Passagen. Diese sind in einer einfachen Geheimschrift verfasst und daher leicht zu lösen. Die verschlüsselten Stellen enthalten einige Tricks für die Bedienung des Instruments, die Chaucer offensichtlich nur Eingeweihten zugänglich machen wollte.

Ein weiteres typisches Kryptogramm aus dem Mittelalter ist das „Astle-Kryptogramm" (siehe Abb. 2.4). Dieses ist erhalten geblieben, weil es in einem Buch von Thomas Astle aus dem 19. Jahrhundert abgebildet ist (Astle, 1976, S. CCLXXVII). Der Autor dieses Werks, ein gewisser Thomas Astle, gab dem Kryptogramm seinen Namen. Es handelt sich um einen in Geheimschrift verfassten Text, den Astle wie folgt beschreibt: „Manuskript auf Pergament in meiner Büchersammlung, geschrieben während der Herrschaft von Heinrich VI." Heinrich VI. regierte von 1422 bis 1461 und von 1470 bis 1471. Mehr ist über das Kryptogramm nicht bekannt.

Der Historiker Albert Leighton veröffentlichte das Astle-Kryptogramm 1977 in der Fachzeitschrift *Cryptologia* (Winkel, 1977). Er konnte es selbst nicht dechiffrieren und bat daher die Leser des Magazins um Hilfe. Gleich zwei davon fanden die Lösung (Winkel, 1978). Einer davon war James Gillogly, von dem in diesem Buch noch mehrfach die Rede sein wird. Die Verschlüsselung entpuppte sich wieder einmal als einfache Buchstabenersetzung. Der Klartext lautet:

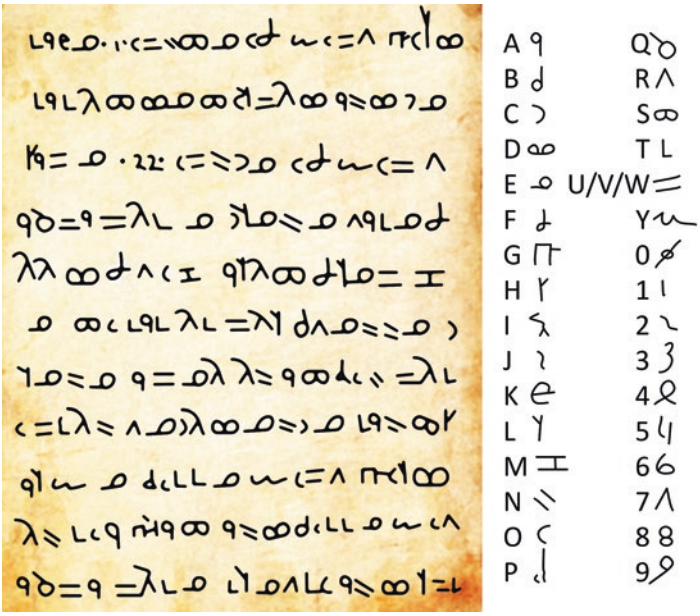


**Abb. 2.4** Das Astle-Kryptogramm stammt aus dem 15. Jahrhundert. Es wurde in den Siebzigerjahren dechiffriert. Die Ersetzungstabelle ist rechts zu sehen. (Klaus Schmeh)

*Take 1 ounce of your gold that is desolved and chave 22 ounce of your aquavitae clean ratified from a lis-fleume so that it will brenne clean away in a spoon without any residue. Then shall ye potte your gold into a glas and botte aquavitae til erto and lut.*

Der Text ist also ein Rezept für eine Mischung aus 22 Unzen Alkohol und einer Unze Gold (eine Unze entspricht heute 28 Gramm). Dies erinnert an „Danziger Goldwasser", einen Gewürzlikör mit darin enthaltenen Goldplättchen. Allerdings: Der Goldanteil im Danziger Goldwasser ist minimal, während das im Astle-Kryptogramm beschriebene Gebräu eine so große Menge enthält, dass man es kaum trinken könnte. Nebenbei wäre ein solches Getränk kaum bezahlbar. Es ist leider völlig unklar, was dieses Rezept bezwecken sollte.

So wurde im Mittelalter zwar viel verschlüsselt, doch eine systematisch betriebene Kryptologie gab es noch nicht. Zu den wenigen, die nicht einfach nur verschlüsselten, sondern sich auch etwas dabei dachten, gehörte der Franziskaner-Mönch Roger Bacon (1214–1292 oder 1294). Bacon war, wie so viele frühe Kryptologen, ein Universalgelehrter, für den die Kryptologie nur ein Nebenschauplatz bedeutete. Er beschäftigte sich mit Mathematik, Optik, Alchemie, Astronomie, Physik und vielem mehr. Zugleich soll er

Erfindungen wie das Mikroskop, das Teleskop, fliegende Maschinen und Dampfschiffe vorhergesagt haben. Mit seiner rationalen Denkweise war Bacon seiner Zeit weit voraus. Daher halten ihn viele für den bedeutendsten Denker des Mittelalters überhaupt.

In einer Abhandlung schrieb Bacon: „Ein Mensch, der ein Geheimnis nicht in einer anderen Weise aufschreibt als die, die es vor der Öffentlichkeit verbirgt, ist verrückt." Anschließend zählte er sieben Methoden auf, die sich seiner Meinung nach zum Verschlüsseln eignen (Goldstone & Goldstone, 2008, S. 106–107):

- *Nachrichten unter Buchstaben und Symbolen verstecken*: Damit sind wohl Buchstabenersetzungen und die Ersetzung ganzer Wörter gemeint.
- *Enigmatische und bildliche Ausdrücke verwenden*: Das Verwenden unüblicher Ausdrücke zum Verschleiern wird heute noch verwendet, auch wenn man dies nicht zur Kryptologie zählt.
- *Schreiben nur mit Konsonanten*: Diese Verschlüsselungsmethode konnte sich nicht durchsetzen.
- *Unterschiedliche Buchstaben vermischen*: Damit könnte eine Geheimschrift mit Blendern gemeint sein.
- *Spezielle Buchstaben verwenden*: Dies entspricht einer Geheimschrift.
- *Kurzschrift verwenden*: Mit Kurzschrift kann man besonders schnell schreiben. Wie Sie beispielsweise in Abschn. 2.8 erfahren werden, lässt sich eine Kurzschrift auch zum (wenn auch nicht sehr sicheren) Verschlüsseln nutzen.

Keine Frage, diese erste Abhandlung über Kryptologie im abendländischen Kulturkreis wirkt heute mehr als dürftig. Aber immerhin: Eineinhalb Jahrhunderte lang war dies das Beste, was es an Kryptologie-Literatur in Europa gab. Ausführlichere Aufsätze und Bücher über zu diesem Thema erschienen in Europa erst, als die Renaissance das Mittelalter abgelöst hatte.

## Die Araber erfinden die Kryptologie

Ich möchte Ihnen an dieser Stelle ein Kryptologiebuch vorstellen, in dem sowohl Ersetzungsverfahren als auch Umordnungsverfahren in mehreren Varianten beschrieben werden. Außerdem geht das Buch ausführlich darauf ein, wie man eine Verschlüsselung knackt: über die Analyse von Buchstabenhäufigkeiten, das Raten häufiger Wörter und das Zählen von Buchstabenpaaren. Eine Liste der häufigsten Buchstaben und Buchstabenpaare schließen das Buch ab.

Was sich anhört wie ein Werk aus dem 20. Jahrhundert, ist in Wirklichkeit über 1100 Jahre alt. Es stammt von dem arabischen Gelehrten Al-Kindi, der im 9. Jahrhundert lebte (Mrayati & Meer Alam, 2002). Al-Kindi war, wie so viele wichtige Persönlichkeiten der Kryptologie-Geschichte, vielseitig interessiert. Zu seinen Interessensgebieten zählten unter anderem Philosophie, Medizin und Musik. Al-Kindis Kryptografie-Buch ist daher nur eine von vielen Veröffentlichungen des genialen Arabers. Dennoch ragt es in vielerlei Hinsicht aus seinem Werk heraus. Es ist das älteste Kryptologie-Buch, das erhalten geblieben ist. Es ist die erste Quelle, die das Knacken von Kryptogrammen behandelt. Und nebenbei belegt es, dass die Araber den Europäern in Sachen Kryptologie um Jahrhunderte voraus waren. Verglichen mit Al-Kindis Buch wirken die Gedanken von Roger Bacon zu diesem Thema wie die eines Grundschülers.

Man kann daher mit Fug und Recht behaupten: Die Araber haben die Kryptologie erfunden. Sie waren die ersten, die nicht einfach nur verschlüsselten, sondern die auch eine Wissenschaft daraus machten. Diese Tatsache ist den Historikern jedoch erst in den letzten Jahrzehnten klar geworden. Die Geschichtsschreibung ist nun einmal traditionell eine europäische Angelegenheit, und so dauerte es bis in die Sechzigerjahre, bis David Kahn in seinem Buch *The Codebreakers* den Blick erstmals auf Arabien lenkte. „Die Kryptologie wurde bei den Arabern geboren", schrieb Kahn (1996). Dabei kannte Kahn Al-Kindi damals noch gar nicht. Erst 1987 entdeckte man im Istanbuler Süleiman-Osman-Archiv Al-Kindis Buch und weckte es damit aus einem 1100 Jahre währenden Dornröschen-Schlaf.

Al-Kindis Buch erweckt den Eindruck, dass der Autor keine Neuigkeiten verkündet, sondern lediglich Bekanntes zusammenfasst. Vermutlich war also das kryptologische Wissen, das Al-Kindi vermittelte, zur damaligen Zeit bereits verbreitet. Es gab sogar ein noch früheres Buch, das sich ausschließlich der Kryptologie widmete. Geschrieben wurde es von einem gewissen Al-Khalil (718–786). Leider ist dieses Buch verschollen und über den Inhalt kaum etwas bekannt.

## 2.2 In der frühen Neuzeit

Im Februar 2013 nahm ich im thüringischen Gotha an der Tagung „Geheime Post" teil. Etwa zwei Dutzend Experten tauschten sich dort über die Verschlüsselungstechniken der europäischen Adelshäuser in der frühen Neuzeit aus (Dworschak, 2013). Es gab einiges zu besprechen: Quer durch das zerstrittene Europa schmiedete der damalige Adel Allianzen, entsandte Diplo-

maten und arrangierte Ehen. Für die Briefe, die man dabei austauschte, war Verschlüsselung Pflicht, denn das Postgeheimnis war damals noch ziemlich löchrig. Viele Adelshöfe betrieben in ihren Poststationen so genannte Schwarze Kammern, in denen sie Briefe mitlesen und auswerten ließen. Zum Fachpersonal einer Schwarzen Kammer gehörten neben Brieföffnungsspezialisten und Siegelfälschern vor allem auch Dechiffrier-Experten.

## Kryptologie in der Renaissance

Der Wettlauf zwischen Codemachern und Codeknackern war in der frühen Neuzeit also bereits in vollem Gange und erfasste nahezu ganz Europa. So gab es in Gotha Vorträge über die Verschlüsselungen der Habsburger und der Wettiner, genauso wie über die kryptologischen Aktivitäten an den französischen, italienischen und schwedischen Adelshöfen. Viele der Vortragenden waren bei ihren Forschungsarbeiten auf ganze Stapel verschlüsselter Briefe gestoßen. Dies lässt vermuten, dass noch Zehntausende verschlüsselter Schreiben in den europäischen Archiven zu finden sind.

Viele der in Gotha vorgestellten Verschlüsselungen aus der der frühen Neuzeit waren einfache Buchstaben-Ersetzungen. Deren Schwächen sprachen sich jedoch schon damals herum, und so stellten viele Adlige auf Nomenklatoren (siehe Abschn. 2.8) oder ähnliche Verfahren um.

### Die polyalphabetische Verschlüsselung

Mit dem Beginnn der Neuzeit war auch das Zeitalter der Renaissance angebrochen und löste das Mittelalter ab. Die Wissenschaften erlebten nun einen enormen Aufschwung, der auch die Kryptologie mitriss. Auf einmal traten geniale Kryptologen auf den Plan, die neue Verschlüsselungsmethoden entwickelten und faszinierende Bücher schrieben. Inspiriert durch die Araber wurde die Kryptologie nun auch in Europa zur Wissenschaft. Viele der neuen kryptologischen Ideen setzten sich zwar erst Jahrhunderte später in der Praxis durch, doch der Grundstein war gelegt.

Zu den wichtigsten kryptologischen Neuentwicklungen der Renaissance gehörte die polyalphabetische Verschlüsselung. Polyalphabetisch ist ein Verschlüsselungsverfahren, wenn es mehrere Ersetzungstabellen vorsieht, zwischen denen beim Verschlüsseln abgewechselt wird. Ein polyalphabetisches Verfahren hat den Vorteil, dass die typischen Buchstabenhäufigkeiten eines Texts verloren gehen, was das Dechiffrieren deutlich erschwert.

Das bekannteste und wichtigste polyalphabetische Verschlüsselungsverfahren der Vor-Computer-Ära ist die „Vigenère-Chiffre“. Um diese zu erklären, verschlüsseln wir den Klartext ICH BIN EIN BERLINER mit dem Schlüsselwort HAUS. Dazu schreiben wir zunächst den Klartext in eine Zeile und dann darunter wiederholt das Schlüs selwort.

```
Klartext:.     ..ICH BIN EIN BERLINER
Schlüsselwort:..HAU SHA USH AUSHAUSH
Geheimtext:.      PCB TPN YAU BYJSIHWY
```

Zum Verschlüsseln wird jeweils ein Buchstabe des Klartexts zum darunter stehenden Buchstaben des Schlüsselworts gezählt (in diesem Fall gilt A = 0, B = 1, C = 2 usw., manchmal wird auch bei A = 1 angefangen zu zählen). Ist das Additionsergebnis größer als Z, dann fängt man bei A wieder an. Das Ergebnis der Verschlüsselung lautet in unserem Beispiel: PCB TPN YAU BYJSIHWY. Wie man sich leicht klar macht, könnte man das Hinzuzählen eines Buchstabens auch mit einer Ersetzungstabelle erledigen. In unserem Beispiel wird also abwechselnd von vier Ersetzungstabellen Gebrauch gemacht. Die Vigenère-Chiffre ist daher eine polyalphabetische Chiffre.

David Kahn, der bedeutendste Experte für Kryptologie-Geschichte, erkannte als erster, dass die Entwicklung der polyalphabetischen Verschlüsselung bis hin zum Vigènere-Verfahren in mehreren Schritten erfolgte (Kahn, 1996). Jeder dieser Schritte wurde von einem bedeutenden Renaissance-Kryptologen vollzogen.

**Schritt 1: Alberti und die Chiffrierscheibe**

Der Italiener Leon Battista Alberti (1404–1472) gilt als Vater der europäischen Kryptologie. Alberti war, wie so viele Größen der Kryptologie-Geschichte, äußerst vielseitig. Er beschäftigte sich nahezu mit allem, was das geistige Leben seiner Zeit hergab. Er schrieb Dramen und Gedichte, malte, komponierte, spielte Orgel und arbeitete als Architekt. Bleibenden Eindruck hinterließen vor allem seine Sachbücher, in denen er sich unter anderem mit Mathematik, Architektur, Tierhaltung und Philosophie auseinandersetzte. Alberti war bereits über 60 Jahre alt, als er sein erstes und einziges Werk zur Kryptologie verfasste: *De Componendis Cifris*. Dieses um 1466 erschienene Werk ist das älteste bekannte Kryptologiebuch Europas.

Alberti hatte erkannt, dass die Häufigkeiten der Buchstaben und Buchstabenkombinationen einen wichtigen Ansatzpunkt für das Lösen einer Buchstabenersetzung darstellten. In seinem Buch *De Componendis Cifris* schlug er als Gegenmaßnahme vor, die zur Verschlüsselung verwendete Tabelle

jeweils nach drei oder vier Wörtern zu wechseln – damit hatte er die polyalphabetischen Verschlüsselung erfunden. Alberti kam außerdem auf die Idee, Ersetzungstabellen mit Hilfe zweier konzentrischer Scheiben zu realisieren (siehe Abb. 2.5), die sich gegeneinander verschieben ließen – die Chiffrierscheibe war geboren (siehe Abschn. 2.10). Dreht man eine Chiffrierscheibe dann erhält man eine neue Ersetzungstabelle.

Alberti hielt sein Verfahren sogar für unknackbar, was allerdings stark übertrieben war. Er ging außerdem noch nicht so weit, dass er eine Änderung der Tabelle nach jedem Buchstaben verlangte – vermutlich erschien im das zu umständlich. Aber immerhin, der Anfang war gemacht.

**Schritt 2: Trithemius und die quadratischen Tafeln**

Ab etwa 1500 machte sich die Renaissance auch nördlich der Alpen bemerkbar. Einen enormen Schub brachte hier der Buchdruck, der zu einer Flut von wissenschaftlichen Veröffentlichungen führte. Der nach Alberti zweite große Kryptologie-Autor dieser Epoche wirkte in Deutschland: Johannes Trithemius (1462–1516). Wie Alberti war auch er ein Universalgelehrter. Trithemius galt als eine der vielseitigsten und bedeutendsten Gelehrtenpersönlichkeiten seiner Zeit, obwohl er nie eine Universität besucht hatte. Neben seiner regen Vortragstätigkeit war er ein begehrter Lehrer und Ratgeber in intellektuellen und höfischen Kreisen. Trithemius verfasste über 90 Bücher. Er be-

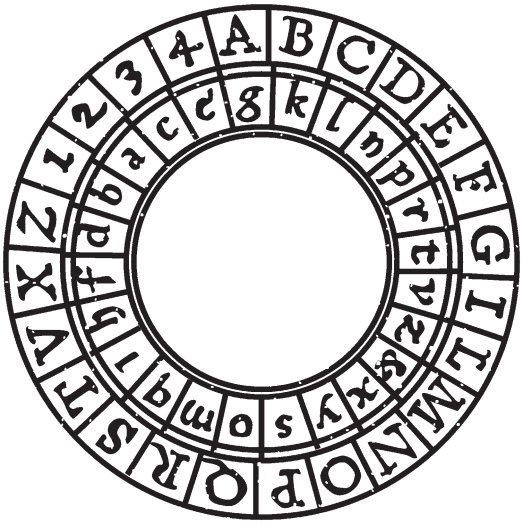

**Abb. 2.5** Leon Battista Alberti entwickelte die erste Chiffrierscheibe. Er schlug vor, diese beim Verschlüsseln jeweils nach ein paar Wörtern zu verdrehen. (Klaus Schmeh)

gann mit Werken über Theologie und Ordensreformen. Später weitete er sein Schaffen auf Heiligendarstellungen, Wunderberichte, Stammes- und Klosterchroniken sowie viel beachtete Kataloge und Nachschlagewerke aus.

Seine Überlegungen zum Thema Kryptologie schrieb Trithemius in seinem Buch *Polygraphiae* (1508) nieder. Er entwickelte die polyalphabetische Verschlüsselung weiter, indem er vorschlug, mit jedem Buchstaben (und nicht erst nach mehreren Wörtern) eine neue Ersetzungstabelle zu nutzen. Im Gegensatz zu Alberti verwendete er jedoch keine Chiffrierscheibe, sondern eine quadratische Tabelle („tabula recta") mit den 24 Buchstaben des lateinischen Alphabets (siehe Abb. 2.6). Der erste Buchstabe eines Texts wurde mit der ersten Zeile, der zweite mit der zweiten Zeile usw. verschlüsselt. Dass Trithemius mit jedem Buchstaben eine neue Tabelle nutzte, war ein Fortschritt.

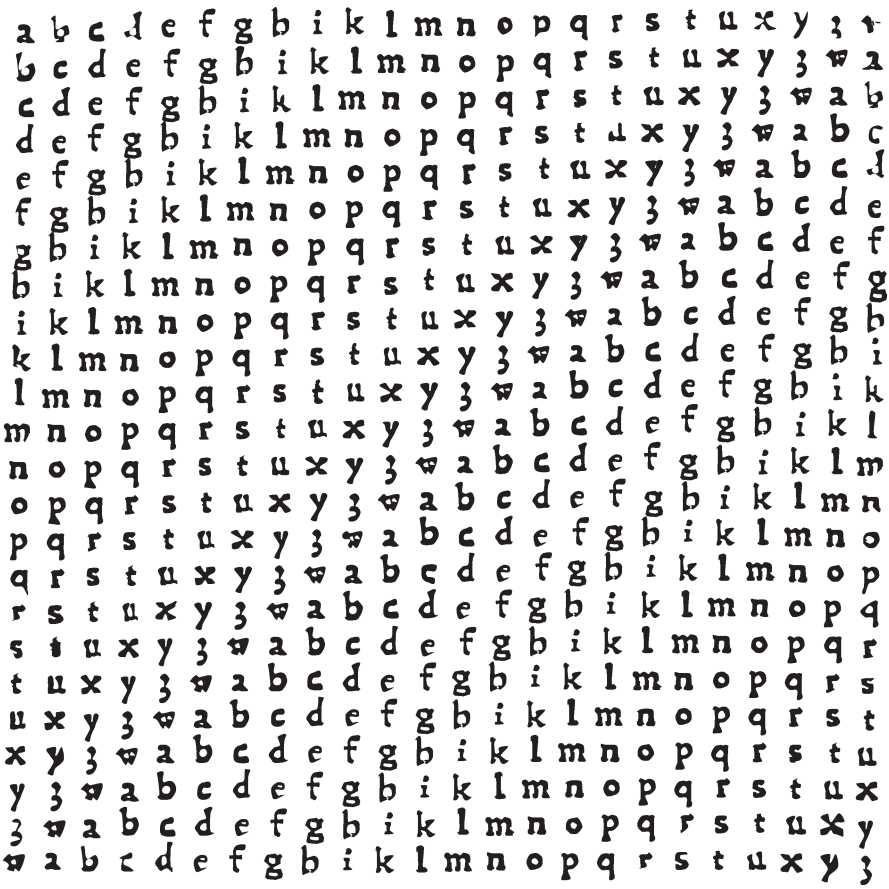

**Abb. 2.6** Die Tabula recta von Johannes Trithemius sieht so viele Ersetzungstabellen vor, wie es Buchstaben im Alphabet gibt. (Klaus Schmeh)

Allerdings folgte der Übergang von einer Tabelle zur nächsten einer einfachen Regel, was das Dechiffrieren erleichterte.

**Schritt 3: Bellasos Tabellen**

Für den nächsten Schritt zur Vigenère-Chiffre sorgte ein im Vergleich zu Alberti und Trithemius deutlich weniger bekannter Mann: Giovan Battista Bellaso. Der Italiener veröffentlichte 1553 sein Buch *La cifra del Sig. Giovan Battista Bellaso*. Darin beschrieb er Tabellen, wie sie in Abb. 2.7 zu sehen sind. Der Verschlüssler wählt zuerst ein Passwort, zum Beispiel ALT. Der erste Buchstabe eines Texts wird nun mit derjenigen Tabelle verschlüsselt, der ein A vorangestellt ist. Der zweite Buchstabe wird entsprechend mit der L-Tabelle und der dritte mit der T-Tabelle verschlüsselt. Danach geht es wieder von vorne los.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AB | a | b | c | d | e | f | g | h | i | l | m |
| | n | o | p | q | r | s | t | u | x | y | z |
| CD | a | b | c | d | e | f | g | h | i | l | m |
| | t | u | x | y | z | n | o | p | q | r | s |
| EF | a | b | c | d | e | f | g | h | i | l | m |
| | z | n | o | p | q | r | s | t | u | x | y |
| GH | a | b | c | d | e | f | g | h | i | l | m |
| | s | t | u | x | y | z | n | o | p | q | r |
| IL | a | b | c | d | e | f | g | h | i | l | m |
| | y | z | n | o | p | q | r | s | t | u | x |
| MN | a | b | c | d | e | f | g | h | i | l | m |
| | r | s | t | u | x | y | z | n | o | p | q |
| OP | a | b | c | d | e | f | g | h | i | l | m |
| | x | y | z | n | o | p | q | r | s | t | u |
| QR | a | b | c | d | e | f | g | h | i | l | m |
| | q | r | s | t | u | x | y | z | n | o | p |
| ST | a | b | c | d | e | f | g | h | i | l | m |
| | p | q | r | s | t | u | x | y | z | n | o |
| VX | a | b | c | d | e | f | g | h | i | l | m |
| | u | x | y | z | n | o | p | q | r | s | t |
| YZ | a | b | c | d | e | f | g | h | i | l | m |
| | o | p | q | r | s | t | u | x | y | z | n |

**Abb. 2.7** Das Verfahren von Bellaso sieht mehrere Verschlüsselungstabellen vor, zwischen denen man hin und her springen muss. (Klaus Schmeh)

Das von Bellaso beschriebene Verfahren kommt der Vigenère-Chiffre schon recht nahe – so nahe, dass Bellaso häufig sogar als ihr Erfinder bezeichnet wird. Das Verfahren hat jedoch gegenüber der Vigenère-Chiffre noch zwei Mängel: Zum einen gibt es für jeweils zwei Buchstaben nur eine Tabelle. Zum anderen muss man zum Verschlüsseln stets die Tabellen zur Hand haben.

**Schritt 4: Portas Neuerungen**

Als das beste Kryptologie-Buch der Renaissance bezeichnen viele Experten *De Furtivis Literarum Notis* von Giambattista della Porta (1535–1616). Porta war – wie könnte es anders sein – ein Universalgelehrter. Er betätigte sich als Mediziner, Naturwissenschaftler, Erfinder, Sammler, Museumsbetreiber und Dramatiker – um nur die wichtigsten seiner Aktivitäten zu nennen.

Nebenbei beschäftigte sich Porta auch mit der Kryptologie und veröffentlichte 1563 das besagte Buch. Darin greift Porta das Verfahren von Bellaso auf. Auch er vollzog jedoch den Sprung zur Vigenère-Chiffre noch nicht. Er machte dafür Angaben zur Wahl sicherer Schlüsselwörter. Außerdem war er der erste, der schrieb, dass auch eine polyalphabetische Chiffre zu knacken ist. Ein weiterer kleiner Schritt war gemacht.

**Schritt 5: Vigenères „Chiffre indéchiffrable“**

Der Franzose Blaise de Vigenère brachte die polyalphabetische Verschlüsselung schließlich zur vorläufigen Vollendung. Deshalb ist das bekannteste Verfahren dieser Art nach ihm benannt. Auch Vigenère war – Sie ahnen es – vielseitig interessiert. Er beschäftigte sich nicht nur mit Kryptologie, sondern auch mit Alchemie, Astronomie, der Bibel und anderen Dingen. In seinem Kryptologie-Buch *Traicté des Chiffres* zeigt er Tabellen, die der Tabula recta von Bellaso ähneln. Allerdings werden die Zeilen dieser Spalten nicht regelmäßig durchlaufen, sondern mit Hilfe eines Passworts ausgewählt. So entstand die Vigenère-Chiffre, wie ich sie einige Seiten zuvor erklärt habe. Vigenère ging sogar noch einen Schritt weiter. Er zählte jeweils das Ergebnis der Verschlüsselung eines Buchstabens zum nächsten Buchstaben dazu. Diese Variante ist. noch sicherer als die eigentliche Vigenère-Chiffre und wurde sogar als „Chiffre indéchiffrable“ bezeichnet.

Erst im 19. Jahrhundert fand man eine Methode zum Knacken der Vigenère-Chiffre (siehe Abschn. 2.3). Und noch heute ist dieses Verschlüsselungsverfahren für Überraschungen gut: So stellte der Kryptologie-Experte Tobias Schrödel 2008 eine neue Methode vor, die (mit Computer-Unterstützung) selbst sehr kurze Vigenère-Kryptogramme zuverlässig löst (Schrödel, 2008).

## Weitere Renaissance-Neuerungen

Die polyalphabetische Verschlüsselung war bei weitem nicht die einzige kryptologische Innovation der Renaissance. Für das Jahr 1401 ist eine weitere Neuerung dokumentiert: Ein unbekannter Chiffriermeister im norditalienischen Mantua verwendete eine Verschlüsselungstabelle, in der jeder Vokal mehrere Entsprechungen hatte – die Homohone waren geboren (Kahn, 1996, S. 107). Von Homophonen spricht man, wenn mehrere Geheimtext-Buchstaben dieselbe Bedeutung haben. Homofone haben vor allem den Zweck, das Knacken einer Verschlüsselung durch eine Häufigkeitsanalyse zu verhindern. Die italienischen Kryptologen dürften also die Häufigkeitsanalyse zu diesem frühen Zeitpunkt bereits gekannt haben.

Weitere Neuerfindungen finden sich in den zahlreichen Kryptologie-Büchern der Renaissance. Der bereits erwähnte Giambattista della Porta beschrieb in seinem viel gelobten Werk *De Furtivis Literarum Notis* erstmals eine bedeutende Form des Chiffrierens: die „Bigramm-Verschlüsselung". Ein Bigramm ist ein Buchstabenpaar. Wie man leicht nachrechnet, gibt es in unseren Alphabet 26 × 26 = 676 Bigramme. Porta arbeitete nur mit 20 Buchstaben und kam so auf 400 Paare. Für jedes Bigramm dachte er sich ein Geheimzeichen aus. Das Ergebnis ist die in Abb. 2.8 dargestellte Tabelle.

Spätere Kryptologen verzichteten darauf, Hunderte von Zeichen zu erfinden und ersetzten lieber Buchstabenpaare durch Buchstabenpaare. Die Häufigkeitsanalyse ist bei einer Bigramm-Verschlüsselung deutlich weniger aussagekräftig als bei einer gewöhnlichen Buchstabenersetzung. Heutige Verschlüsselungsverfahren, die mit dem Computer ausgeführt werden, ersetzen sogar meist 16 Buchstaben (Bytes) auf einmal – mit dem Ziel, eine Häufigkeitsanalyse nutzlos zu machen.

Ein weiterer Kryptologie-Buchautor der Renaissance war Gerolamo Cardano. Dieser unterschied sich von anderen vielseitig interessierten Gelehrten vor allem dadurch, dass er noch vielseitiger interessiert war. Nicht weniger als 230 Bücher schrieb er im Laufe seines Lebens. Zwei davon behandeln die Kryptologie. Seine bekannteste Entwicklung in diesem Zusammenhang ist das „Cardan-Gitter". Dies ist eine Schablone, die auf einen Text gelegt wird, wodurch nur noch bestimmte Buchstaben oder Wörter zu sehen sind – diese bilden eine geheime Nachricht. Das Cardan-Gitter gehört jedoch nicht in die Kryptologie, sondern in die Steganografie.

Cardano war außerdem der erste Kryptologe, der mit großen Zahlen hantierte (Kahn, 1996, S. 145). Er beschrieb ein Alphabet bestehend aus 27 Zeichen und behauptete, es gäbe eine 28-stellige Zahl an Möglichkeiten, dieses

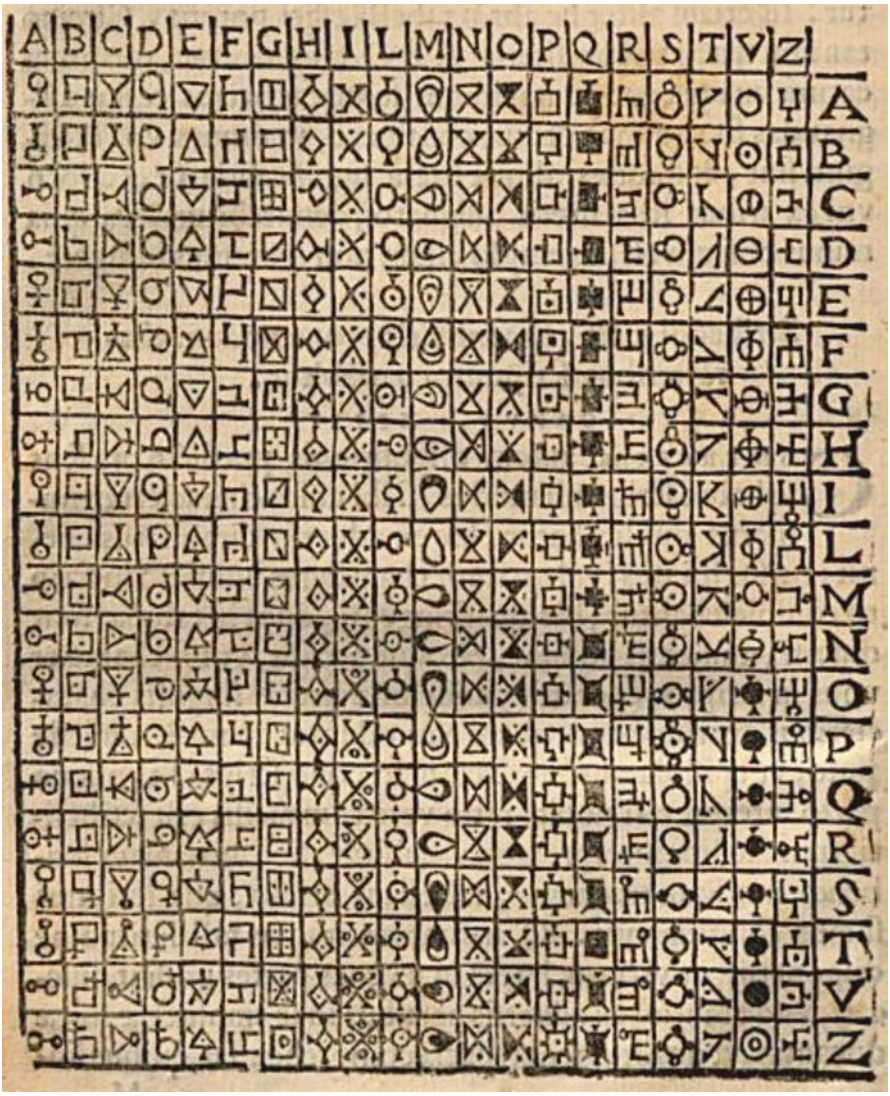


**Abb. 2.8** Diese Tabelle von Giovanni Batista Porta sieht für jedes Buchstabenpaar (Bigramm) ein eigenes Zeichen vor. Es gibt auch weniger umständliche Bigramm-Verschlüsselungen. (Aus dem Buch „De furtivis literarum notis" (1563) von Giambatista della Porta (Google Books))

auf sich selbst abzubilden. In Wirklichkeit ist es sogar eine 29-stellige Zahl, und zwar die Fakultät von 27. Heute gehört es für Kryptologen zum Alltag, mit großen Zahlen um sich zu schmeißen. Moderne Verschlüsselungsverfahren bieten so viele Kombinationen, dass die Zeit vom Urknall bis heute bei weitem nicht ausreichen würde, um sie alle durchzuprobieren.