



Stephen Pincock · Mark Frary

# Verschlüsselt

Die Geschichte geheimnisvoller Codes  
von den Hieroglyphen bis heute

**Haupt**





Stephen Pincock · Mark Frary

# Verschlüsselt

Die Geschichte geheimnisvoller Codes  
von den Hieroglyphen bis heute

Haupt Verlag

**Rechts:** Der Diskos von Phaistos, entdeckt auf Kreta. Seine kryptischen Zeichen haben ihn zu einem der berühmtesten Rätsel der Archäologie gemacht.

1. Auflage: 2023

ISBN 978-3-258-08339-1

Alle Rechte vorbehalten.

Copyright © 2023 für die deutschsprachige Ausgabe: Haupt Verlag, Bern

Jede Art der Vervielfältigung ohne Genehmigung des Verlages ist unzulässig.

Aus dem Englischen übersetzt von Sebastian Vogel, DE-Kerpen

Lektorat der deutschsprachigen Ausgabe: Heike Werner, DE-München

Satz der deutschsprachigen Ausgabe: Die Werkstatt Medien-Produktion GmbH, DE-Göttingen

Umschlaggestaltung der deutschsprachigen Ausgabe: Tanja Frey, Haupt Verlag, CH-Bern

Umschlagabbildungen:

Vorne links: Everett Collection/Shutterstock.com; oben rechts: Science Photo Library;

Mitte rechts: marekuliasz/Shutterstock.com

Hinten: Fedor Selivanov/shutterstock.com

Die englischsprachige Originalausgabe erschien 2019 unter dem Titel *The Story of Codes* bei Elwin Street Productions Limited, London, UK. Die erste Ausgabe erschien im Jahr 2007 und wurde auf Deutsch unter dem Titel *Geheime Codes: Die berühmtesten Verschlüsselungstechniken und ihre Geschichte* vom Ehrenwirth Verlag veröffentlicht. Teile davon sind in der hier vorliegenden vollständig überarbeiteten und erweiterten Ausgabe enthalten.

Copyright © Elwin Street Productions Limited 2023

Konzipiert und produziert von: Elwin Street Productions, 10 Elwin Street, London E2 7BU, UK

Printed in China

Um lange Transportwege zu vermeiden, hätten wir dieses Buch gerne in Europa gedruckt. Bei Lizenzausgaben wie diesem Buch entscheidet jedoch der Originalverlag über den Druckort. Der Haupt Verlag kompensiert mit einem freiwilligen Beitrag zum Klimaschutz die durch den Transport verursachten CO<sub>2</sub>-Emissionen. Dabei unterstützt der Verlag ein Projekt zur nachhaltigen Forstbewirtschaftung in der Zentralschweiz. Wir verwenden FSC®-zertifiziertes Papier. FSC® sichert die Nutzung der Wälder gemäß sozialen, ökonomischen und ökologischen Kriterien.

Diese Publikation ist in der Deutschen Nationalbibliografie verzeichnet. Mehr Informationen dazu finden Sie unter <http://dnb.dnb.de>.

Der Haupt Verlag wird vom Bundesamt für Kultur für die Jahre 2021–2024 unterstützt.



Sie möchten nichts mehr verpassen?

Folgen Sie uns auf unseren Social-Media-Kanälen und bleiben Sie via Newsletter auf dem neuesten Stand.

[www.haupt.ch/informiert](http://www.haupt.ch/informiert)



Wir verlegen mit Freude und großem Engagement unsere Bücher. Daher freuen wir uns immer über Anregungen zum Programm und schätzen Hinweise auf Fehler im Buch, sollten uns welche unterlaufen sein.

[www.haupt.ch](http://www.haupt.ch)





# Inhalt

Einleitung ..... 8

Kapitel 1: Ursprünge ..... 11

Vom Alten Ägypten über die Codes von Sex und Religion  
bis zur schottischen Königin Maria Stuart.

Einfache Substitution · Transposition · Häufigkeitsanalyse

Kapitel 2: Erfindungsreichtum ... 43

Wie findige Mönche, Diplomaten und Papstberater die  
Kryptologie auf den Kopf stellten. Außerdem: die ersten  
beamten Codeknacker

Kapitel 3: Scharfsinn ..... 63

Die technische Entwicklung führte in der Kryptologie zu  
weiteren Umwälzungen, aber viele Chiffren bleiben ungelöst.  
Morsecode · Playfair-Chiffre · Autokey-Chiffre

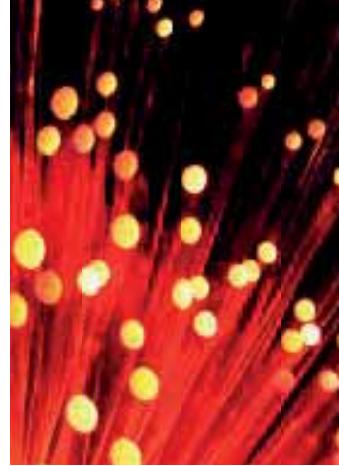
Kapitel 4: Beharrlichkeit ..... 87

Durch pure Hartnäckigkeit wurden die Enigma und auch  
andere militärische Verschlüsselungen geknackt. Zimmermann-  
Depesche · ADFGX-Chiffre · Navajo-Code · die Schlacht der  
Codes im Kalten Krieg



## Kapitel 5: Geschwindigkeit ..... 127

Im Online-Zeitalter schützt leistungsfähige digitale Verschlüsselung die Daten vor Cyberkriminellen. Asymmetrische Verschlüsselung · Faktorisierung · Advanced Encryption Standard



## Kapitel 6: Visionen ..... 147

Die Quantenkryptografie wird als unentschlüsselbar gepriesen. Sind die Codeknacker:innen also am Ende? Kryptografie in Quantenphysik und Chaostheorie

## Kapitel 7: Ausblick ..... 165

Im großen Konflikt des Digitalzeitalters um die widerstreitenden Pole Überwachung und Privatsphäre ist die Kryptografie wichtiger als je zuvor. Edward Snowden · Secure Hash Algorithm · Bitcoin

## Eine Zukunft ohne Verschlüsselung? ..... 184

Glossar .....	186
Register .....	188
Über die Autoren .....	191
Literaturhinweise .....	192
Bildnachweis .....	192



---

# Einleitung

Im 21. Jahrhundert ist digitale Verschlüsselung Teil des Alltags. Jedes Mal, wenn wir mit dem Handy telefonieren, einen Film schauen oder Online-Bankgeschäfte tätigen, bedienen wir uns einer hochentwickelten Form der computergestützten Verschlüsselung und sorgen so dafür, dass die neugierigen Augen und Ohren anderer außen vor bleiben.

Aber die heutige Zeit hat kein Monopol auf die geheime Übermittlung von Informationen. Schon seit mindestens zweitausend Jahren spielen Codes und Chiffren eine wichtige und manchmal entscheidende Rolle in der Politik, im blutigen Drama des Krieges, bei Mordanschlägen und bei der Verbrechensbekämpfung. Durch die geheime Weitergabe von Nachrichten wurden Kriege gewonnen und verloren, Imperien aufgebaut und zerstört, Menschenleben gerettet oder vernichtet. Es steht also viel auf dem Spiel – da ist es kein Wunder, dass eine nie endende Schlacht tobt: auf der einen Seite die Kryptografie, deren Ziel es ist, die Bedeutung einer Nachricht hinter einem Code oder einer Chiffre zu verbergen, und auf der anderen Seite die Kryptoanalyse mit erfindungsreichen, schlauen Codeknacker:innen, deren erklärtes Ziel es ist, Codes und Chiffren zu entschlüsseln und verborgene Nachrichten offenzulegen.

Jedes Mal, wenn Kryptograf:innen einen neuen Code oder eine Chiffre erfinden, tappen die Kryptoanalytiker:innen zunächst im Dunkeln. Codierte Nachrichten, die bislang leicht zu entschlüsseln waren, bleiben plötzlich undurchschaubar. Dieser Kampf wird wohl nie ein Ende haben. Mit verbissener Hartnäckigkeit oder einem plötzlichen, erhellenden Geistesblitz finden die Kryptoanalytiker:innen irgendwann eine Schwachstelle, arbeiten sich unermüdlich daran ab, bis die geheimen Nachrichten sich wieder offenbaren.

Die bemerkenswerten Menschen, die Kryptoanalyse zu ihrem Beruf gemacht haben, lassen eine Reihe besonderer Charaktereigenschaften erkennen, die bei dieser schwierigen und oftmals gefährlichen Arbeit besonders hilfreich sind. Zunächst einmal legen sie häufig eine verblüffend originelle Denkweise an den Tag. Alan Turing, einer der größten Kryptoanalytiker aller Zeiten, der im Zweiten Weltkrieg zur Kriegswende beitrug, gehörte zu den originellsten Denkern seiner Zeit. Erfolgreiche Kryptoanalytiker:innen zeichnen sich außerdem durch eine besonders hohe Motivation aus. Nichts vermag den Geist eines Menschen so zu fesseln wie ein Geheimnis. Für manche Codeknacker:innen ist bereits die Herausforderung, ein Geheimnis zu lüften, Motivation

---

genug. Häufig kommen aber andere Motive hinzu: Patriotismus, Rachegefühle, Habgier oder auch reiner Wissensdurst.

Um Codes und Chiffren zu entschlüsseln, braucht man mehr als ein nur beiläufiges Interesse. Die frühe Chiffre zu entschlüsseln, die Julius Caesar bevorzugte, scheint uns heute kinderleicht zu sein, aber zu Caesars Zeit erforderte es große Beharrlichkeit, die codierten Nachrichten lesbar zu machen.

Auch Geschwindigkeit ist beim Knacken von Codes ein wesentlicher Faktor. Viele Codes und Chiffren lassen sich brechen – aber nur dann, wenn man genug Zeit hat, um daran zu arbeiten. Ein klassisches Beispiel ist das RSA-Kryptosystem. Es basiert auf der Besonderheit, dass die Multiplikation von zwei Primzahlen nur wenig Zeit in Anspruch nimmt; aber herauszufinden, welche Primzahlen multipliziert wurden und eine bestimmte Zahl ergeben, kann selbst mit einem Computer ewig dauern.

Codeknacker:innen brauchen auch eine Vision, die sie antreibt. Oft arbeiten sie verdeckt, unter amtlicher oder krimineller Geheimhaltung, und da ihre Tätigkeit so heikel ist, arbeiten sie häufig alleine. Ohne eine feste Zielvorstellung im Kopf ist ihre kryptanalytische Arbeit zum Scheitern verurteilt.

Dieses Buch zeigt, dass sich – allein durch Codes, die geschaffen und entschlüsselt wurden – der Lauf der Geschichte ändern kann. Dass diese unsre Fantasie stark beflügeln, ist eigentlich kein Wunder, und es erklärt sowohl den Erfolg von Romanen, in denen es von Codes nur so wimmelt, als auch die regelmäßigen Auftritte von Codeknacker:innen in Kino- und Fernsehfilmen. Mit der Realität haben solche fiktiven Szenen wenig zu tun, dennoch ist die wahre Geschichte der Kryptologie und insbesondere der Kryptanalyse häufig spannender als alles, was Krimiautor:innen sich je ausdenken könnten. Auf den folgenden Seiten wird davon die Rede sein, wie außergewöhnlich die Menschen, die zu Codeknacker:innen werden, tatsächlich sind. Wir lernen einige der faszinierendsten historischen Figuren kennen und erfahren, welche grundlegenden Fähigkeiten zum mentalen Rüstzeug echter Codeknacker:innen gehören.

## DER DISKOS VON PHAISTOS

---

In den ersten Julitagen des Jahres 1908 war der junge italienische Archäologe Luigi Pernier an der Südküste Kretas mit Ausgrabungen im minoischen Palast von Phaistos beschäftigt.

In der Sommerhitze arbeitete Pernier im Hauptraum eines unterirdischen Tempelmagazins und entdeckte dort eine bemerkenswert gut erhaltene, kalkverkrustete Terrakottascheibe von etwa 15 Zentimetern Durchmesser, die aber nur etwas über einen Zentimeter dick war.

Die Scheibe trug auf beiden Seiten insgesamt 242 rätselhafte, eingravierte Hieroglyphen, die vom äußeren Rand bis zur Mitte eine Spirale bildeten. Von den 45 verschiedenen Zeichen – eingravierten oder eingedrückten symbolischen Figuren – stellten mehrere offensichtlich Dinge aus dem Alltag dar, beispielsweise Menschen, Fische, Insekten, Vögel, ein Boot und so weiter.

Die Symbole mochten leicht zu erkennen sein, aber was sie bedeuten, wurde in den nachfolgenden 100 Jahren hitzig diskutiert.

Manche Amateurarchäolog:innen äußerten die Vermutung, es könne sich um eine Art Gebet handeln, andere hielten es für einen Kalender und wieder andere für einen Ruf zu den Waffen. Weitere Spekulationen gingen davon aus, es könnte sich um ein antikes Brettspiel oder einen geometrischen Lehrsatz handeln.

Erst 2014 entwickelte man eine glaubwürdige Methode, um die Scheibe zu lesen, aber auch sie führte nicht dazu, dass man den Inhalt der Nachricht vollständig verstand.

Einer, der sich schon seit Langem für die Geheimnisse der Scheibe interessiert, ist der Mathematiker Anthony Svoronos aus Kreta.

„Der wichtigste Aspekt des Diskos ist nach meiner Überzeugung die Methode, mit der er geschaffen wurde“, erklärt Svoronos. „Die Scheibe wurde mit mehreren Stempeln bedruckt. Zur Herstellung dieser Stempel waren große Anstrengungen notwendig, und deshalb sollten wir davon ausgehen, dass sie zur Herstellung vieler verschiedener Dokumente verwendet wurden. Und doch ist der Diskos das einzige Dokument, das mit diesen Stempeln erzeugt wurde und bis in unsere Zeit erhalten geblieben ist.“

Noch enttäuschender wird dieser Mangel, weil Archäologen auf der anderen Seite Kretas, an der Ausgrabungsstätte des minoischen Palastes von Knossos, Hunderte von Tafeln entdeckt haben, die mit antiken Schriftzeichen namens Linear A und Linear B verziert sind.

Linear A, die ältere der beiden Schriften, ist bis heute nicht entschlüsselt – damit gehört auch sie zu den ungelösten Rätseln der antiken Schriften. Linear B dagegen, die aus dem 14. und 13. Jahrhundert v. u. Z. stammt, wurde in den 1950er-Jahren entschlüsselt: Damals entdeckte der englische Architekt Michael Bentriss, dass auf den Tafeln eine Form des Griechischen stand.

Die Schwierigkeit bei der Entschlüsselung des Diskos von Phaistos ist nach Ansicht der meisten Expert:innen, dass die Scheibe einfach nicht genügend Schriftzeichen enthält, um eine definitive Entzifferung durchzuführen.

Interessant ist auch, dass die auf der Scheibe eingravierten Zeichen sehr scharf und detailliert sind, ganz anders als die viel abstrakteren Formen und Zeichen der Linearschriften.



**Oben:** Die beiden Seiten des Diskos von Phaistos. Die Bedeutung der Zeichen und die Herkunft der Scheibe sind bis heute unklar. Damit bleibt der Fund eines der berühmtesten Rätsel aus Archäologie und Kryptologie.

Aber das alles hielt den Linguisten Dr. Gareth Owens vom Technological Educational Institute in Kreta und John Coleman, Professor für Phonetik an der Universität Oxford, nicht von der Entwicklung einer plausiblen Methode ab, mit der man die Scheibe lesen kann. Mit ihr erhält man faszinierende Anhaltspunkte für den Inhalt.

Die beiden Wissenschaftler erkannten Ähnlichkeiten zwischen der entzifferten Linear B und den Glyphen auf der Scheibe. Mit ihrer Hilfe konnten sie „mehr als 90 Prozent des Diskos von Phaistos lesen“. So hat beispielsweise das Symbol, das Owens als „punk head“ (Punkkopf) bezeichnete, den gleichen phonetischen Laut [l] wie das Symbol 28 im Linear B. Mit dieser und ähnlichen Annahmen sowie mit parallelen, in Linear B geschriebenen Texten identifizierten die beiden die sich wiederholende

Gruppe von Symbolen als IQEKURJA, was so viel wie „schwangere Mutter“ oder „Göttin“ bedeutet. Dies veranlasste sie zu der Vermutung, die Scheibe könnte ein Gebet an eine minoische Göttin enthalten.

Aber solange es keine eindeutige Entschlüsselung gibt – etwa dadurch, dass man die gleichen Zeichen auf anderen Dokumenten entdeckt –, werden wir nicht genau erfahren, ob diese Erklärung stimmt.

بِرَانِ وَاثِنِ تَوَانِدَنِدَ وَأَنِاسِبَ شَفَاعَشَرَدَ وَبَازِعَمَالِخِيرَ وَسَلَخَنِ قَوْشَهَ آخِرَتَ اَزْعَالَتَ كَاهَ اَزَانَ  
كَوْنَدَ شَفَاعَىَ دَهَذَكَهَ مَعَاوَدَتَ صَمَرَتَ بَنَنَدَدَ وَمَنْجَحَكَمَ اِيَنَ مَفَرَّمَاتَ اَزْعَلَمَ طَبَّ بَرَانَغَفَمَهَقَنَدَ



دَنْهَتَ بِرَطَبَ دِينَ صَرَوْفَ كَرَدَانِيدَمَ وَلَهَقَ رَاهَ آنَنَدَلَزَوَنَىَ بَايَانَ يَا فَنَمَ سَلَرَمَخَادَوَهَ مَصَانَوَنَهَ سَهَهَ

## Der Ursprung der Kryptoanalyse

Jahrtausendelang hatte sich die Entwicklung der Kryptografie ohne nennenswerte parallele Bestrebungen bei der Kryptoanalyse und den entsprechenden Entschlüsselungsmethoden vollzogen. Die Techniken der Kryptoanalyse wurden von den Völkern Arabiens erdacht.

Im goldenen Zeitalter der islamischen Kultur nach dem Jahr 750 unserer Zeitrechnung besaßen die Gelehrten tiefe Kenntnisse in Naturwissenschaften, Mathematik, Kunst und Literatur. Wörterbücher, Enzyklopädien und Lehrbücher der Kryptografie erschienen, und die wissenschaftliche Erforschung von Wörtherkunft und Satzstrukturen führte auch in der Kryptoanalyse zum ersten größeren Durchbruch. Muslimische Gelehrte gelangten zu der Erkenntnis, dass Buchstaben in allen Sprachen mit einer bestimmten Häufigkeit auftreten. Sie belegten, dass man Erkenntnisse über solche Häufigkeiten dazu nutzen konnte, Chiffren zu entschlüsseln – ein Verfahren, das als Häufigkeitsanalyse bekannt ist.

Soweit man weiß, stammt die erste schriftlich festgehaltene Erklärung der Kryptoanalyse aus dem 9. Jahrhundert. Sie wurde von dem arabischen Wissenschaftler und Autor Abu Yusuf Yaqub ibn Ishaq al-Sabbah al-Kindi verfasst und steht in seinem Werk *Abhandlung über die Entzifferung kryptografischer Botschaften*.



**Gegenüber:** Das goldene Zeitalter des Islam, das von ungefähr 750 u. Z. bis ins 13. Jahrhundert dauerte, war eine Zeit großer Errungenchaften in Wissenschaft, Kunst und Philosophie. Einer ihrer Vertreter war der große Kryptoanalytiker al-Kindi.

**Links:** Eine Seite aus al-Kindis *Abhandlung über die Entzifferung kryptografischer Botschaften*



## Kapitel 2

---

# Erfindungsreichtum

*Wie findige Mönche, Diplomaten und Papstberater  
die Kryptologie auf den Kopf stellten.  
Außerdem: die ersten beamteten Codeknacker*

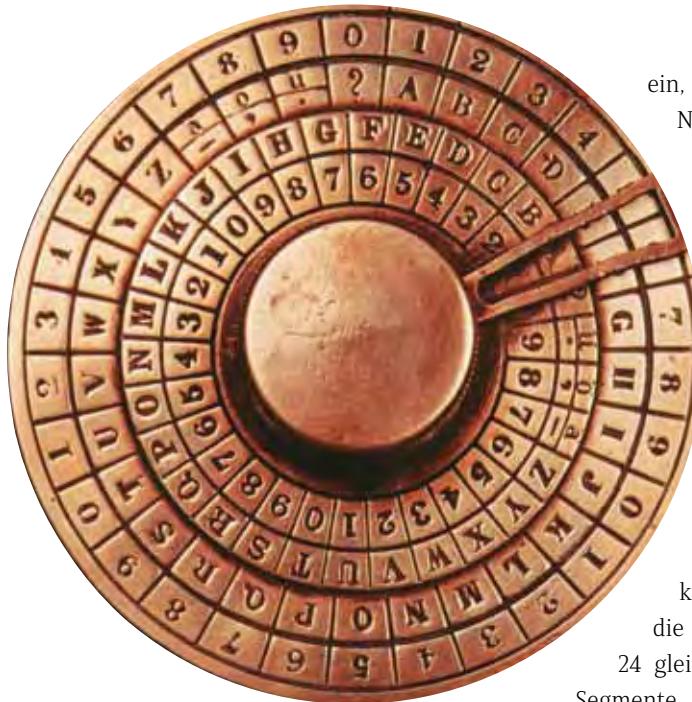
Mit der Häufigkeitsanalyse war die Sicherheit, die einfache Verschlüsselungsmethoden zuvor geboten hatten, dahin. Wer jetzt noch die monoalphabetische Substitution nutzte, musste stets damit rechnen, dass die Nachrichten entschlüsselt und vom Feind gelesen wurden.

Die Codeknacker – seinerzeit waren praktisch ausschließlich Männer in diesem Metier tätig – hatten nun also einen Vorteil, aber der währte nicht lange. In Europa hatten mehrere scharfsinnige Amateure bereits die nächste Entwicklung in Gang gesetzt und eine Form der Verschlüsselung geschaffen, die den Methoden zur Zählung der Buchstabenhäufigkeit weitaus größeren Widerstand entgegengesetzte.

### **Päpstliche Verschlüsselung**

Diese neue Form der Verschlüsselung lässt sich auf den Vatikan zurückführen. Sie entsprang dem außergewöhnlichen Geist von Leon Battista Alberti, illegitimer Sohn eines reichen Florentiners. Alberti war ein wahrer Renaissancemensch: Seine Begabungen umfassten Architektur, Kunst, Wissenschaft und Justiz. Außerdem war er allen Berichten folge ein hochbegabter Codeknacker. Eines Tages ging Alberti mit seinem Freund, dem Papstsekretär Leonardo Dati, in den vatikanischen Gärten spazieren, und dabei kamen sie auf Chiffren zu sprechen. Dati räumte

**Gegenüber:** Der Renaissancemensch Leon Battista Alberti, ein begabter Codeknacker und Erfinder der Chiffrierscheibe.



**Oben:** Eine Chiffrierscheibe aus dem 19. Jahrhundert, aufgebaut nach Albertis Entwurfskonzept.

ein, der Vatikan müsse verschlüsselte Nachrichten verschicken – und Alberti versprach, dabei zu helfen. Aus diesem Anlass, so scheint es, schrieb er im oder um das Jahr 1467 einen Aufsatz, der die Grundlagen für eine ganz neue Verschlüsselungsschrift legte. Er erklärte darin sehr eindeutig die Häufigschaftsanalyse und nannte verschiedene Methoden der Entschlüsselung. Außerdem beschrieb er ein Verschlüsselungssystem mit zwei konzentrischen Metallscheiben, die jeweils entlang ihres Umfangs in 24 gleiche Segmente geteilt waren. Die Segmente der äußeren Scheibe enthielten die Buchstaben des Alphabets und die Zahlen 1 bis

4 (**h**, **k** und **y** ließ er weg, und **j**, **u** und **w** kamen im damals verwendeten lateinischen Alphabet ohnehin nicht vor). Die Abschnitte des inneren Kreises enthielten die 24 Buchstaben des lateinischen Alphabets (ohne **U**, **W** und **J**, aber zusätzlich mit **et** = und) in zufälliger Reihenfolge. Wenn man einen verschlüsselten Brief verschicken wollte, las man die Buchstaben oder Zahlen des Klartextes auf der äußeren Platte ab und ersetze sie dann durch die entsprechenden Buchstaben der inneren Platte. Absender:in und Empfänger:in mussten identische Scheiben besitzen und sich darüber einigen, welche Anfangsposition die beiden Scheiben relativ zueinander einnahmen.

Bis zu diesem Schritt handelt es sich einfach um eine monoalphabetische Substitution. In seinem nächsten Absatz vollzog Alberti aber einen genialen weiteren Schritt: „Wenn ich drei oder vier Wörter geschrieben habe“, schrieb er, „ändere ich die Position des Index in unserer Formel, indem ich an dem Kreis drehe.“ Das mag sich nicht nach etwas Besonderem anhören, aber es hat wichtige Folgen. Für die ersten Buchstaben könnte beispielsweise der Schlüsseltext **k** auf dem inneren Kreis einem **f** im Klartext entsprechen, aber wenn man die Scheiben gegeneinander verdreht, steht das **k** des Schlüsseltextes plötzlich für **t** oder einen beliebigen anderen Buchstaben.

Diese Methode macht es Codeknacker:innen bedeutend schwerer. Jede neue Position der Scheiben erzeugt neue Beziehungen zwischen Schlüssel- und Klartext, das heißt (um ein Beispiel aus der englischen Sprache zu nehmen), das Wort *cat* wird in einem Fall zu **gdi** und in einem anderen zu **alx**. Damit war die Häufigkeitsanalyse weit weniger erfolgreich anzuwenden.

Zusätzlich nutzte Alberti die Zahlen auf dem äußeren Ring als eine Art chiffrierten Code. Bevor er den Klartext verschlüsselte, ersetzte er bestimmte Formulierungen nach einem kleinen Codebuch durch Kombinationen der Zahlen von 1 bis 4. Diese Zahlen wurden dann zusammen mit der übrigen Nachricht verschlüsselt. Albertis bemerkenswerte Leistungen brachten ihm den Titel „Vater der abendländischen Kryptologie“ ein. Aber die Evolution der Kryptografie war auch damit nicht zu Ende; der nächste Entwicklungsschritt polyalphabetischer Systeme entsprang der Feder einer ebenso herausragenden Geistesgröße.

### Die Tabelle des Trithemius

Der Abt Johannes Trithemius (Johannes von Trittenheim) verfasste das weltweit erste gedruckte Buch über Kryptografie. Er war, gelinde gesagt, eine umstrittene Gestalt, denn er interessierte sich für Okkultismus, was in seinem Freundeskreis zu Bestürzung und bei anderen zu Empörung führte. Seine *Polygraphia*, ein Mammutwerk über das Handwerk der Kryptografie, erschien Anfang des 16. Jahrhunderts, nach seinem Tod, als sechsbändige Reihe. Seine Arbeit formulierte erstmals die heutige Standardmethode zur Erstellung polyalphabetischer Substitutionssysteme, die „quadratische Tafel“ oder *Tabula recta* (siehe Seite 48–49).

In den nachfolgenden Jahrzehnten des 16. Jahrhunderts machten die Ideen, die hinter der polyalphabetischen Substitution standen, eine weitere Verfeinerung durch; der Mann, dessen Name dauerhaft mit der quadratischen Tabelle als Form der Verschlüsselung in Verbindung gebracht wurde, war der 1523 geborene Franzose Blaise de Vigenère.

Vigenère war ein französischer Diplomat. Mit der Kryptografie kam er erstmals 1549 im Alter von 26 Jahren in Kontakt, als er sich auf einer zweijährigen Mission in Rom befand. In dieser Zeit las er die Werke von Alberti, Trithemius und anderen wichtigen Autoren, und vielleicht lernte er im Vatikan auch einige Entschlüsselungsexperten kennen. Ungefähr 20 Jahre später zog sich Vigenère vom Leben bei Hofe zurück und begann zu schreiben. Eines seiner mehr als 20 Bücher ist die berühmte, 1586 erstmals erschienene *Traicté des chiffres*.

---

# Codeanalyse Transpositionschiffren

Das nachfolgende Beispiel für die Funktionsweise des Systems basiert auf einer Nachricht, die Abraham Lincoln Mitte 1863 verschickte. Der Klartext lautete:

*For Colonel Ludlow.*

*Richardson and Brown, correspondents of the Tribune, captured at Vicksburg, are detained at Richmond. Please ascertain why they are detained and get them off if you can. The President. 4.30 p.m. (Für Colonel Ludlow. Richardson und Brown, Korrespondenten der Tribune, die in Vicksburg gefangen genommen wurden, werden in Richmond festgehalten. Bitte stellen Sie den Grund dafür fest, und befreien Sie sie, wenn Sie können. Der Präsident. 16.30 Uhr.)*

In dem zu jener Zeit verwendeten Codesystem stand VENUS für *colonel*, WAYLAND für *captured* (gefangen genommen), ODOR für *Vicksburg*, NEPTUNE für *Richmond*, ADAM für *the President* und NELLY für *4.30 p.m.* Tauscht man die Wörter entsprechend aus, wird die Nachricht zu:

*For VENUS Ludlow*

*Richardson and Brown, Correspondents of the Tribune, WAYLAND at ODOR, are detained at NEPTUNE. Please ascertain why they are detained and get them off if you can. ADAM, NELLY*

Um die Nachricht zu verschlüsseln, wählte der Chiffrierbeamte eine Route. In diesem Fall entschied er sich für eine Route namens GUARD, die erforderte, dass die Nachricht in sieben Zeilen zu je fünf Worten geschrieben wurde, wobei „Nullen“, also sinnlose Wörter, hinzugefügt wurden, um das Rechteck zu vervollständigen. In der nächsten Tabelle sind die Codewörter komplett in Großbuchstaben geschrieben.

---

For	VENUS	Ludlow	Richardson	And
Brown	Correspondents	Of	The	Tribune
Wayland	At	ODOR	Are	Detained
At	NEPTUNE	Please	Ascertain	Why
They	Are	Detained	And	Get
Them	Off	If	You	Can
ADAM	NELLY	THIS	FILLS	UP

Das erste Wort des chiffrierten Textes gibt die verwendete Route an: GUARD; anschließend liest man zum Verschlüsseln die erste Spalte aufwärts, die zweite abwärts, die fünfte aufwärts, die vierte abwärts und schließlich die dritte wieder aufwärts. Um die Sicherheit zu erhöhen, wurde am Ende jeder Spalte ein sinnloses „Nullwort“ hinzugefügt:

GUARD ADAM THEM THEY AT WAYLAND BROWN FOR	KISSING
VENUS CORRESPONDENTS AT NEPTUNE ARE OFF NELLY	TURNING
UP CAN GET WHY DETAINED TRIBUNE AND	TIMES
RICHARDSON THE ARE ASCERTAIN AND YOU FILLS	BELLY
THIS IF DETAINED PLEASE ODOR OF LUDLOW	COMMISSIONER

Damit lautet die fertige Nachricht:

*GUARD ADAM THEM THEY AT WAYLAND BROWN FOR KISSING VENUS CORRESPONDENTS AT NEPTUNE ARE OFF NELLY TURNING UP CAN GET WHY DETAINED TRIBUNE AND TIMES RICHARDSON THE ARE ASCERTAIN AND YOU FILLS BELLY THIS IF DETAINED PLEASE ODOR OF LUDLOW COMMISSIONER*

Anfangs waren nur drei Buchstabenpaare gesteckert, aber später steigerten die Deutschen diese Zahl auf zehn Paare, und nun entwickelte Zygalski eine andere Methode mit Lochblättern.

Die Herstellung der „Zygalski-Lochblätter“ war sehr zeitaufwendig, denn man brauchte eine große Zahl solcher Blätter, und die Löcher – oft bis zu 1000 in einem Blatt – wurden von Hand mit Rasierklingen durchgestoßen.

Man erstellte 26 Lochblätter, von denen jedes eine mögliche Ausgangsposition des linken Rotors in der Enigma-Maschine repräsentierte. Auf jedem Blatt war ein Gitternetz von  $26 \times 26$  Feldern auf der linken Seite von oben nach unten und oben quer jeweils mit den Buchstaben A bis Z gekennzeichnet. Die Buchstaben auf der linken Seite stellten die Ausgangsposition des mittleren Rotors dar, und die in der obersten Zeile entsprachen den Ausgangspositionen des rechten Rotors.

Dass die Nachricht, die mit AXN EYMEHY beginnt, ein „female“ enthält, wissen wir, denn der erste und der vierte Buchstabe für die Einstellungen sind gleich. Demnach muss auf

dem Zygalski-Lochblatt, das den Buchstaben **A** in der Position des linken Rotors repräsentiert, ein Loch in dem Gitternetz an der Stelle angebracht werden, wo das **X** auf der linken Spalte und das **N** aus der obersten Zeile zusammentreffen.

Wenn am gleichen Tag noch andere Nachrichten von derselben verschlüsselnden Person verschickt werden und ebenfalls „females“ in den Nachrichteneinstellungen enthalten, legen wir die Lochblätter so übereinander, dass die Gitternetze genau deckungsgleich sind. Hält man diesen Blätterstapel gegen das Licht, sind nur die Einstellungen, an denen die Löcher an der gleichen Stelle liegen – sodass das Licht hindurchscheint –, mögliche Einstellungen des jeweiligen Tages. Jedes Blatt, das zu dem Stapel hinzukommt, verringert die Zahl der potenziellen Anfangseinstellungen weiter. Hat man eine ausreichende Zahl von Nachrichten im richtigen Format, kann man letztlich die Anfangseinstellungen ableiten.

**Unten:** Alan Turing (1912–1954) entwickelte mehrere Methoden, um die deutsche Verschlüsselung zu brechen, darunter die „Bombe“, mit der man die Einstellungen der Enigma-Maschine finden konnte.





Im Dezember 1938 konnte man jedoch auch diese Methode nicht mehr anwenden, denn jetzt nahmen die Deutschen an dem System eine neue Verfeinerung vor. Statt drei Rotoren in allen beliebigen Kombinationen zu benutzen, konnten die verschlüsselnden Stationen jetzt drei von fünf Rotoren beliebig auswählen. Damit stieg die Zahl der möglichen Rotoreinstellungen nochmals um das Zehnfache, und die Herstellung der dazu nötigen Lochblätter überstieg die damaligen Möglichkeiten.

Schon bald wurden die Polen von den Ereignissen überrollt. Als die Invasion in ihrem Land bevorstand, erkannten sie, dass sie ihre Erkenntnisse mit anderen teilen mussten. Während Deutschland sich auf den Überfall vorbereitete, gaben die Polen nachgebaute militärische Enigma-Maschinen an die GC&CS und den französischen Geheimdienst.

### Die Enigma wird geknackt

Um eine Nachricht zu entschlüsseln, musste die Empfangsstation – und alle, die mithörten – wissen, welche drei Rotoren man bei der Verschlüsselung ausgewählt hatte, welche Positionen sie in der Maschine hatten, wie die drehbaren Kerben eingestellt waren, welche Ausgangs-

**Oben:** Die „Bombe“, mit der die Enigma-Einstellungen entschlüsselt wurden.

---

# Eine Zukunft ohne Verschlüsselung?

*Werden Verschlüsselungsmethoden immer mehr an Bedeutung verlieren, weil Unternehmen zunehmend Zugriff auf unsere Online-Daten haben? Wie können wir unsere Privatsphäre zurückgewinnen?*

Sollen wir uns Sorgen darüber machen, ob Behörden wie NSA, GCHQ und ihre Pendants in anderen Teilen der Welt wissen, wie sie die asymmetrische Verschlüsselung und andere kryptografische Methoden knacken können? Solche Institutionen verfügen sicher über gewaltige Rechenleistungen und können sie sicherlich einsetzen, um eine Verschlüsselung mit kurzem Schlüssel zu brechen. Das schaffen aber auch alle, deren Prozessor nur lange genug läuft.

Haben diese Behörden einen Weg gefunden, um große Primzahlen zu faktorisieren? Das ist möglich, aber unwahrscheinlich. Eines aber haben sie: Zugriff auf die Hintertüren vieler beliebter Cloud-Dienste. Erinnern wir uns noch an das peinliche Bild, das wir damals bei einem Online-Fotoservice gespeichert hatten? Angenommen, es ergibt sich eine Situation, in der sie herausfinden wollen, welche Nachrichten wir gesendet haben: Können wir davon ausgehen, dass sie nicht darauf zugreifen und es nicht zur Erpressung nutzen? Ebenso lassen sich Sprachassistenten und Smartphones bekanntermaßen mit speziellen Tools in Lauschvorrichtungen verwandeln. Wer braucht da noch eine Verschlüsselung zu knacken?

Wir verzichten in zunehmendem Maß auf unsere Privatsphäre. Spätestens seit dem Skandal um Cambridge Analytica und durch den Aufschwung der zielgerichteten, personalisierten Werbung im Netz wissen wir nur allzu gut, was wir Google, Amazon, Facebook (heute Meta Platforms Inc.), Apple (GAFA bzw. GAMA) und ihresgleichen alles anvertrauen, wenn wir etwas posten oder eine Suchmaschine im Internet nutzen. Die große Frage lautet: Sind unsere persönlichen Vorlieben und Abneigungen so stark mit dem Netz verflochten, dass wir sie nicht mehr davon trennen können? Haben



wir den Schlüssel zu unserem eigenen Ich weggegeben, bevor uns überhaupt klar war, was da geschieht? Ist nichts mehr übrig, was irgendjemand noch enthüllen müsste?

Vielleicht spielt es keine Rolle mehr, ob wir mit Ende-zu-Ende-Verschlüsselung kommunizieren, weil die genannten Unternehmen ohnehin praktisch alles über uns wissen. Das führt zwar dazu, dass wir uns unter anderem mit aufdringlicher Werbung herumschlagen müssen, es bedeutet aber auch, dass man Menschen mit finsternen Absichten herauspicken kann, insbesondere wenn noch ein Hauch von künstlicher Intelligenz in die Datenmischung einfließt.

Eine Ahnung von der Zukunft gab uns vielleicht Sir Tim Berners-Lee, der Erfinder des World Wide Web: Er gab 2018 in seinem Artikel „*One Small Step for the Web...*“ auf [www.medium.com](http://www.medium.com) die Gründung von *Solid* bekannt, einer neuen Initiative zum Schutz privater Daten. Diese überträgt die Kontrolle der Daten von Unternehmen auf die individuelle Person und schafft die Möglichkeit, dass wir den Zugriff auf unsere persönlichen Daten und alles, was wir im Netz posten, selbst unter Kontrolle behalten.

Berners-Lee schrieb dazu: „Ich habe immer geglaubt, dass das Netz für alle da ist. Deshalb kämpfen ich und andere so energisch dafür, es zu schützen. Die Veränderungen, die wir zuwege gebracht haben, haben eine bessere und stärker vernetzte Welt geschaffen. Aber bei allem Guten, was wir erreicht haben, hat sich das Netz auch in einen Motor der Ungleichheit und Spaltung verwandelt, und angetrieben wird er von mächtigen Kräften, die es für ihre eigenen Ziele benutzen. Ich glaube, dass wir heute einen entscheidenden Kipppunkt erreicht haben und dass eine kraftvolle Veränderung zum Besseren möglich und auch notwendig ist.“

**Oben:** Die Logos von Google, Amazon, Facebook und Apple (GAFA)

---

## REGISTER

Kursive Seitenzahlen verweisen auf Abbildungen.

### A

Addison, Joseph 136  
ADFGVX-Chiffre 90, 93  
ADFGX-Chiffre 90, 92–93  
Adeleman, Leonard 129–30  
Advanced Encryption Standard (AES) 139–40  
Aineas der Taktiker 111  
Alberti, Leon Battista 42, 43–45, 48  
Algorithmen 13, 139, 152, 174  
Amerikanischer Bürgerkrieg 78–82  
Anagramme 18–19  
Analytische Maschine 68, 69  
Apple 167, 184–85  
Architektur 46–47  
Arisue, Seizo 121  
Assange, Julian 179  
Assyrien 12  
asymmetrische Chiffren 129  
Atbasch-Chiffre 27, 28–29, 29, 30–31  
Autokey-Chiffre 70–75

### B

Babbage, Charles 68–69  
Babington, Anthony 34–37  
Babylonien 12  
Bacon, Roger 52  
Baphomet 30, 30–31  
Baresch, Georg 50  
Bates, David Homer 82  
Bax, Stephen 53  
Bazeries, Étienne 57, 61  
Beale papers 84–85  
Bell Laboratories 152  
Bennett, Charles 147, 149, 158  
Bentris, Michael 20  
Berners-Lee, Tim 185  
Bibelanalyse 29, 29–30  
Binärkode 111

Bitcoin 164, 176–83, 180  
Bletchley Park 86, 95, 95, 98–99, 108–09, 112, 114–15, 118  
Blockchain 176, 181  
Blockchiffre 139  
Bomben (Enigma) 87, 105, 107, 108, 115  
Boniface 109  
Born, Max 149  
Brassard, Gilles 147, 149, 158  
Brown, Dan  
– *Sakrileg* 28, 145  
– *Diabolus* 144–45  
Broza, Gil 136–37  
Bulonde, Vivien L'Abbé, Seigneur du 61  
Bureau du Chiffre 90, 92  
Burger, Ernest 110, 111

### C

Cabinet Noir 57  
Caesar, Gaius Julius 9, 12, 16  
Caesar-Chiffre 16, 39  
– Tabelle 48  
Cambridge Analytica 184  
Cardan-Gitter 66–67  
Cardano, Girolamo 67  
Carter, Frank 102  
Chandler, Albert B. 82  
Chaostheorie 159–61  
Chaucer, Geoffrey 27  
Chiffren 13  
– asymmetrische 129  
– Dorabella 96–97, 97  
– dreiteilige 132–33  
– Große 57, 61  
– hebräische 28–31  
– literarische 66–67  
– Substitution *siehe* Substitutionschiffre  
– symmetrische 129  
– Transposition *siehe* Transpositionschiffre  
Chiffrierscheiben 44, 44–45  
Churchill, Winston 98

Cocks, Clifford 129  
Coleman, John 21  
Colossus-Maschine 114, 115, 115  
Connor, Howard 121  
Cox, Brian 149  
Curle, Gilbert 37  
Cypherpunks 178–79

### D

Daemen, Joan 139  
Dasch, George John 111  
Data Encryption Standard (DES) 139  
Dati, Leonardo 43  
Deep Crack 139  
Deutsch, David 149, 151, 152  
Differenzmaschine 68  
Diffie, Whitfield 129  
Diffie-Hellman-Verschlüsselung 129  
Digitale Signaturen 129, 174, 176  
Doctorow, Cory 168–69  
Doppelpaltparallel 154  
Dorabella-Chiffre 96–97, 97  
Doyle, Arthur Conan 142, 143  
dreiteilige Chiffre 132–33  
Driscoll, Agnes Meyer 94  
Drosnin, Michael, *Der Bibel-Code* 29–30  
Dumas, Alexandre 61  
D-Wave 152

### E

Eckardt, Heinrich von 88  
Einstein, Albert 148–49  
Ekert, Artur 158  
Electronic Frontier Foundation (EFF) 139  
Elgar, Edward 96–97  
Elisabeth I., Königin von England 34–37, 35  
Elliptische Kurven 167, 173  
Ellis, James 129  
Enigma 95–115, 98, 101, 103  
Exklusives Oder (XOR) 113, 139

- 
- F**
- Facebook 167, 184–85  
 Faktoren 138, 173  
 Fibonacci-Folge 145  
 Finney, Hal 178, 182, 183  
 Flamsteed, John 68  
 Flowers, Tommy 115  
 Follett, Ken 144  
 Freimaurerei 46  
 Friedman, William F. 50, 79, 117  
 Frisby, Dominic 182–83
- G**
- Gallehawk, John 102  
 Gardner, Meredith 122  
 Gematrie 29  
 Gifford, Gilbert 34, 37  
 Gilmore, John 179  
 Government Code and Cypher School (GC&CS) 88, 94  
 Government Communications Headquarters (GCHQ) 128, 129, 171  
 Grabeel, Gene 122  
 Greenberg, Andy 182  
 Greenglass, David 124, 125  
 Greenwald, Glenn 172  
 Griechenland 12–15, 111  
 Große Chiffre 57, 61  
 Grover, Lov 152  
 Gruppentheorie 100, 105, 173
- H**
- Habsburgerreich 58  
 Hallock, Richard 122  
 Hanyecz, Laszlo 179  
 Harden, Donald 132–33  
 Hashing 176  
 Häufigkeitsanalyse 24–25, 38–39  
 Heath Robinson 114  
 heiliger Gral 46–47  
 Hellman, Martin 129  
 Henrietta Maria, Königin 68  
 Herodot von Halikarnassos 14, 14  
 Hieroglyphen 10, 11, 20
- Hirams Schlüssel 46  
 Hitler, Adolf 112  
 Holland, Tom, *Rubicon* 39  
 Hughes, Eric 178–79
- I**
- IBM 139, 152, 166  
 Internetsicherheit 140–41, 165–72;  
     siehe auch Verschlüsselung  
 Islam, goldenes Zeitalter 23
- J**
- Johnston, Philip 119  
 Jones, J.E. 119  
 Joyce, Herbert, *The History of the Post Office* 59
- K**
- Kahn, David, *The Codebreakers* 41, 83  
 Kalter Krieg 122–25  
*Kamasutra* 40, 41  
 Kaminsky, Dan 182  
 Kartenspiel 111  
 Kasiski, Friedrich, *Geheimschriften und die Dechiffrier-Kunst* 69  
 Kasiski-Test 71  
*kautiliyam* 41  
 Keilschrift 12  
 Kerckhoffs, Auguste 82–83  
 Kerckhoffs'sches Prinzip 83  
 KGB 122–24  
 Kindi, Abu Yusuf Yaqub ibn Ishaq, al- 23, 23  
 Kircher, Athanasius 50  
 Knox, Dilly 98, 103  
 Kryptowährungen 176–81
- L**
- Laser 160–61  
 Leonardo da Vinci 46, 145  
 Lévi, Éliphas 30  
 Linear A und B 20–21  
 Literatur, Codes in der 142–45  
 Lorenz SZ40 112–13, 115
- Lorenz, Edward 160  
 Lorenz-Attraktor 160  
 Ludwig XIII., König von Frankreich 56, 56  
 Ludwig XIV., König von Frankreich 56, 61
- M**
- Madame X 94  
 Mann mit der eisernen Maske 60, 61  
 Mantua, Herzogtum 32  
 Maria Stuart, Königin der Schotten 34–37, 35  
 Maria Theresia, Kaiserin 58  
 Massachusetts Institute of Technology (MIT) 129, 131  
 Mastering the Internet (MTI) 171  
 May, Timothy C. 179  
 McClellan, George B. 78  
 McNealy, Scott 165  
 Melville, Herman, *Moby Dick* 30  
 Mesopotamien 11  
 Metadaten 171  
 Mikropunkte 111  
 Milhon, Jude 179  
 Mitchell, Stuart 47  
 mittelalterliche Kryptografie 27  
 Modulus 134–35  
 Molay, Jacques de 30  
 Morse, Samuel 62, 63–64, 78  
 Morsecode 63–65, 64, 65, 90, 102  
 Mozart, Wolfgang Amadeus 46  
*muladeviya* 41  
 Musik 46–47
- N**
- Nakamoto, Dorian Prentice Satoshi 182, 183  
 Nakamoto, Satoshi 176, 178–79, 182–83  
 National Bureau of Standards (NBS) 139  
 National Security Agency (NSA) 125, 125, 140–41, 171–72, 174, 175

---

Navajo-Code 118, 118–22, 121  
Nebel, Fritz 90  
Newton, Isaac 154  
Nomenklator 27, 37, 56, 65  
Null 37, 80–81

## O

O'Reilly, Henry 78  
One-Time-Pads 122, 147  
Owens, Gareth 21

## P

Painvin, Geogres-Jean 92, 92–93  
päpstliche Verschlüsselung 43–45  
Pearl Harbor 116–17  
Penny, Dora 96–97  
Pernier, Luigi 20  
Phaistos, Diskos von 20–21, 21  
Phelippes, Thomas 34–37  
Philip IV. von Frankreich 30–31  
Phillips, Cecil 122  
Playfair, Lyon 66, 76–77, 77  
Playfair-Chiffre 76–77  
Plutarch 15  
Poe, Edgar Allan 136–37  
– *Der Goldkäfer* 142–43  
Polarisation 156–58  
Polybios 14  
Polybios-Quadrat 90–91  
Post 58–59  
Pretty Good Privacy (PGP) 140–41  
Primzahlen 129–30, 134, 167–68  
Privatsphäre 165–72, 184  
Purple 116, 117

## Q

Quantencomputer 149–52  
Quantenkryptografie 147, 154–63,  
155  
Quantenmechanik 148–49  
Quantenschlüssel 158–59  
Quantensuperposition 150–51, 155  
Qubits 151–52, 159

## R

Rejewski, Marian 104  
Renza, Louis 136  
Rijmen, Vincent 139  
Rips, Eliyahu 29  
Rivest, Ronald 129–30  
Roberts, Jeff John 183  
Rosen, Leo 117  
Rosenberg, Ethel 124–25  
Rosenberg, Julius 124, 124–25  
Rosenheim, Shawn 136  
Rossignol, Antoine 56–57  
Rossignol, Bonaventure 57  
Rosslyn Chapel 46, 46–47, 47  
Rowlett, Frank 117, 119  
Rózycki, Jerzy 104  
RSA 9, 130–31, 152

## S

Schachbrettmethode 14–16  
Scherbius, Arthur 102  
Schlüsselwechsel 127–29  
Schmetterlingseffekt 159–61  
Schneier, Bruce 166, 166, 172  
Schonfield, Hugh 31  
Schriftrollen vom Toten Meer 31  
Schrödinger, Erwin 150, 151  
Schrödingers Katze 150  
Schwarze Kammern 56–59, 94  
Secure Hash Algorithm (SHA)  
174–75  
Secure Sockets Layer (SSL) 141, 174  
SecurID 130  
Seleukeia, Tafel von 11–12  
Shamir, Adi 129–30  
Shields, Andrew 158  
Shor, Peter 152  
Shor-Algorithmus 152–53  
Shore, Alan 160–61  
Siebenjähriger Krieg 58, 59  
SIGABA-Maschine 119  
Signaturen, digitale 129, 168, 174,  
176

Snowden, Edward 140, 167, 170–72  
Solid 185  
Spionage 110–11  
Stager, Anson 78  
Steckern 100  
Steganografie 13–14, 66, 111, 161  
Stephenson, Neal, *Cryptonomicon*  
144

Stix, Gary 159  
Substitutionschiffre 16–17  
– Atbasch-Chiffre 27–31  
– Caesar-Verschiebung 16, 39  
– digrafische 76  
– homofone 32–33  
– monoalphabetische 27, 32, 43, 44,  
136  
– polyalphabetische 45, 54–56, 59,  
65, 69, 136  
Sueton 12–13  
Superposition, quantenmechanische  
149–51, 155  
Svoronos, Anthony 20  
Svozil, Karl 162  
symmetrische Chiffren 129  
Szabo, Nick 182–83, 183

## T

Telegrafie 63–66, 76–78, 82  
– Zimmermann-Depesche 88–89, 89  
Thackeray, William Makepeace 66  
Thora 28, 29, 30  
Tinker, Charles A. 82  
Toshiba 158  
Transport Layer Security (TLS) 141, 174  
Transpositionschiffre 18–19, 80–81  
Trithemius, Johannes 45, 48–49  
Truman, Harry 125  
Turing, Alan 98, 106, 108, 114

## U

Überwachung 165–66, 168–69  
Unabhängigkeitserklärung der USA  
85, 85

## V

- Venona 122–25  
Verschlüsselung  
– Advanced Encryption Standard (AES) 139–40  
– asymmetrische (Public-Key-Verschlüsselung) 128–31, 134–35, 140  
– Data Encryption Standard (DES) 139  
– doppelte 122  
– Ende-zu-Ende 167, 185  
– päpstliche 43–45  
– Secure Hash Algorithm (SHA) 174–75  
Verschränkung 151, 158  
Vertrauensnetz 168–69, 169

- Vigenère, Blaise de 45, 54, 54, 65, 70, 74, 82  
Voltaire 61  
Voynich-Manuskript 50–53, 50–53

## W

- Walsingham, Francis 34–37  
Ward, J. B. 84–85  
Web of Trust 168–69, 169  
Welchman, Gordon 98, 108  
Weltkrieg, Erster 88–93  
Weltkrieg, Zweiter 95–122, 109, 123  
Whalen, Terence 136  
Wheatstone, Charles 66, 76–77  
Willes, Edward 58  
Williamson, Malcolm 129  
Wright, Craig Steven 183, 183

## X

- XOR (exklusives Oder) 113, 139

## Y

- Yasodhara, Jayamangala 41

## Z

- Zandbergen, René 52  
Zimmermann, Arthur 88  
Zimmermann, Philip R. 140  
Zimmermann-Depesche 88–89, 89  
Zodiac-Killer 132–33, 132–33  
Zygalski, Henryk 104, 106  
Zygalski-Lochblätter 105, 106  
Zykrometer 104

## ÜBER DIE AUTOREN

**Stephen Pincock** ist ein preisgekrönter Wissenschaftsjournalist und Redakteur bei *Springer Nature*. Er hat zahlreiche Artikel über die Geschichte und Entwicklung der Kryptologie und anderen Technologien geschrieben und ist der Autor verschiedener Sachbücher.

**Mark Frary** ist ein Wissenschaftsautor, dessen Artikel unter anderem in *The Times* veröffentlicht wurden. Bevor er mit dem Schreiben begann, studierte er Astrophysik und erforschte die Ursprünge des Universums am CERN in Genf. Sein lebenslanges Interesse gilt jedoch der Kryptografie, insbesondere den Anwendungen der Quantenkryptografie.



Im 21. Jahrhundert sind digital verschlüsselte Daten ein fester Bestandteil unseres Alltags.

Aber die heutige Zeit hat kein Monopol auf die geheime Übermittlung von Informationen. Schon seit mehr als 2000 Jahren spielen Codes und Chiffren in Kultur, Politik und Spionage eine bedeutende Rolle.

Stephen Pincock und Mark Frary zeichnen diese faszinierende Geschichte nach und spannen dabei den Bogen vom Diskos von Phaistos bis hin zur Quantenkryptografie. Auf dieser Reise durch die Zeit führen sie unter anderem in das geheimnisvolle Voynich-Manuskript ein, schildern, auf welchem Weg die Chiffriermaschine Enigma geknackt wurde, und beleuchten die Entwicklung der Kryptografie im Digitalzeitalter.

Anhand von zahlreichen nachvollziehbaren Beispielen zeigen sie, welche Prinzipien hinter den jeweiligen Verschlüsselungssystemen stehen und wie man manche Codes auch selbst knacken kann.



 **Haupt**