Teil I
Kryptographie & Technologie

Die heute genutzte Kryptographie ist zunächst eine *technologische Angelegenheit*. Auf digitale Weise sicher und vertraulich kommunizieren zu können, erfordert zwangsläufig den Einsatz kryptographischer Algorithmen. Schließlich wollen wir, dass eine digitale Finanztransaktion vertraulich ist und dass sie die gewünschte Person erreicht. Gleichzeitig möchten wir, dass beispielsweise unsere digitalen Gesundheitsdaten sicher verwahrt werden, damit sie nicht von jemand anderem mitgelesen werden können. Und nicht weniger wollen wir, dass niemand unsere intimsten Interessen im Internet erfährt. Eine technologisierte Gesellschaft verlässt sich damit auf die Implementierung von kryptographischen Verfahren.

In einer Zeit, in der Kommunikation noch prä-digital stattfand, war die Bedeutung von Kryptographie nicht vergleichbar mit jener, die sie heute hat. *Bedeutung* meint dabei zunächst gar kein quantifizierbares Kriterium. Es geht viel eher um die Frage, *für wen* Kryptographie Bedeutung hatte und hat. Wir werden in den folgenden Kapiteln sehen, dass in dieser Hinsicht ein fundamentaler Wechsel stattgefunden hat. Noch bis in die Mitte des 20. Jahrhunderts hatte die Kryptographie als Werkzeug des Militärs, der Nationalstaaten, der Diplomatie und der Mächtigen der Welt gegolten.[1] Im Laufe des letzten Jahrhunderts wurde die Kryptographie hingegen für *alle Individuen* von Bedeutung.[2]

Die spezifischen Gründe hierfür werden in den folgenden Abschnitten anhand zweier *Paradigmen* veranschaulicht: einerseits des Paradigmas

1 Menezes, Oorschot und Vanstone erkennen dabei: „The predominant practitioners of the art were those associated with the military, the diplomatic service and government in general. Cryptography was used as a tool to protect national secrets and strategies." Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997, S. 1.

2 Siehe Jonathan Katz und Yehuda Lindell. *Introduction to Modern Cryptography*. 2. Aufl. Boca Raton: CRC Press, 2015, S. 1.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

der *Klassischen Kryptographie* (Kapitel 1) und andererseits des Paradigmas der *Modernen Kryptographie* (Kapitel 2).[3] Das Konzept des Paradigmas und der damit zusammenhängende *Paradigmenwechsel* (engl. *paradigm shift* oder *paradigm change*) wurden bereits 1962 von Thomas S. Kuhn in seinem einflussreichen Werk *The Structure of Scientific Revolutions* geprägt.[4] Für Kuhn gibt es zwei Charakteristika, durch die eine bestimmte *Leistung* (engl. *achievement*) zum Paradigma wird: Einerseits sei die Leistung „sufficiently unprecedented to attract an enduring group of adherents away from competing modes of scienific activity"[5]. Andererseits sei sie „sufficiently open-ended to leave all sorts of problems for the redefined group of practitioners to resolve"[6].

Sicherlich ist dieser durchaus unscharfe Begriff in den letzten Jahren inflationär verwendet worden. Gleichwohl könnte er für die Entwicklung der Kryptographie passender kaum sein. Was nämlich das 16. Jahrhundert für das astronomische Weltbild bedeutet hatte, war für die Kryptographie das 20. Jahrhundert: eine neue Art und Weise, über Kryptographie als Wissenschaft nachzudenken, um gerade damit sehr erfolgreich spezifische Problemfelder der Praxis zu lösen.[7] Diese neuartige Denkweise und die Bedeutung der Kryptographie sind allerdings nur verständlich mit dem systematischen Wissen um *beide* Paradigmen – das der Klassischen Kryptographie und das der Modernen Kryptographie.

---

3 Die Unterteilung in eine Klassische Kryptographie und eine Moderne Kryptographie findet sich auch in der Literatur; siehe etwa Katz und Lindell, *Introduction to Modern Cryptography* sowie Craig P. Bauer. *Secret History: The Story of Cryptology*. 2. Aufl. Boca Raton, London und New York: CRC Press, 2021.

4 Siehe Thomas S. Kuhn. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012. Er selbst war gegenüber dem Begriff des Paradigmas später kritisch eingestellt; siehe Ian Hacking. „Introductory Essay". In: Thomas S. Kuhn. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012, S. vii–xxxvii, hier S. xviii.

5 Kuhn, *The Structure of Scientific Revolutions*, S. 10.

6 Ebd., S. 10–11.

7 Im Paradigma der Klassischen Kryptographie galt kryptographische Forschung als Teil der Linguistik. Sie war, wie der kommende Abschnitt deutlich machen wird, dabei eine zumeist militärische Angelegenheit. Erst mit herausragenden Persönlichkeiten des 20. Jahrhunderts wie dem Mathematiker Claude Shannon wurde Kryptographie im Bereich der Mathematik angesiedelt. Diese neue Art und Weise, über Kryptographie nachzudenken, wurde zum fruchtbaren Boden, auf dem sich das zweite Paradigma der *Modernen Kryptographie* entwickeln konnte. Zu dieser neuen Kryptographie kommen nun Algorithmen und Protokolle hinzu, die über das alleinige Schutzziel von Vertraulichkeit hinausgehen.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Diese modellhafte Systematisierung anhand einer historischen Einteilung ist auch für eine Ethik der Kryptographie erforderlich. Zum einen lassen sich dadurch Begrifflichkeiten klären, die im späteren Verlauf diskutiert werden. Zum anderen hat erst die Entwicklung der Modernen Kryptographie jene fundamentalen, gesellschaftlichen Konflikte hervorgebracht: Wer soll kryptographische Forschung betreiben können? Welche Institution soll Algorithmen standardisieren dürfen? Und überhaupt: Kann Kryptographie für die *good guys* zugänglich gemacht werden – und für die *bad guys* nicht? Für all diese Fragen wird Teil I die technologisch-systematischen Grundlagen liefern.[8]

8 Damit handelt es sich bei Teil I nicht um ein in erster Linie historisches Kapitel, sondern vielmehr um eine technologisch-systematische Einteilung und zugleich Einleitung in die Kryptographie.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

1 Klassische Kryptographie

> The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write.
>
> – David Kahn, Autor von *The Codebreakers*[1]

Wenn man bereits mit dem ersten Kapitel in eine wissenschaftliche Auseinandersetzung geraten möchte, dann damit, etwas als *klassisch* zu bezeichnen, sei es in der Musik, Kunst, Mathematik, Politik oder jeglicher anderen Wissenschaft. Für die Kryptographie gilt dies in ähnlicher Weise, denn wer oder was entscheidet schon, was eine klassische Kryptographie sein soll?

Im Kontext dieser Arbeit ist die *Klassische Kryptographie* dialektisch gegenüber einer Art der neuen Kryptographie, der *Modernen Kryptographie*, definiert.[2] Vereinfacht könnte man sagen, dass Klassische Kryptographie in vielerlei Hinsicht das ist, was Moderne Kryptographie nicht ist – und umgekehrt. Diese Dialektik ist zwar nicht willkürlich zu verstehen, doch sagt sie aus: Unsere heutige, Moderne Kryptographie ist nicht verständlich ohne ihren systematisch-historischen Hintergrund. Um diesen Wechsel und seine weitreichenden Auswirkungen auf sowohl die Wissenschaft als auch die Gesellschaft überhaupt nachvollziehen zu können, ist daher das Wissen um das frühere Paradigma notwendig.

Neben diesem dialektischen Ansatz zeichnet sich die Klassische Kryptographie auch dadurch aus, dass sie das beschreibt, was man etymologisch wie auch in der Alltagssprache unter dem Begriff der Kryptographie versteht: Verschlüsselung von Texten, damit Parteien, die die Texte

1 David Kahn. *The Codebreakers: The Story of Secret Writing*. Überarbeitete Version. New York: Scribner, 1996, S. 84; auch zitiert in John F. Dooley. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Cham: Springer, 2018, S. 5.

2 Die Unterscheidung von Klassischer und Moderner Kryptographie wird in der Literatur oft gezogen, so etwa bei Bauer, *Secret History*, sowie Katz und Lindell, *Introduction to Modern Cryptography*. Die zeitlichen und inhaltlichen Grenzen beider Paradigmen unterscheiden sich jedoch teilweise.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

nicht lesen *sollen*, sie auch nicht lesen *können*.[3] Für über zweitausend Jahre erfüllte Kryptographie auch just diese Funktion. Erst die Moderne Kryptographie wird diese Definition erweitern.[4] Um sich dieser Klassischen Kryptographie anzunähern, werden im Folgenden zunächst die Anfänge der Kryptographie und Kryptoanalyse beschreiben (Abschnitt 1.1). Anschließend werden mit deren Mechanisierung die ersten Schritte einer Technologisierung der Kryptographie analysiert (Abschnitt 1.2).

1.1 Die Anfänge von Kryptographie und Kryptoanalyse

Mit *The Codebreakers* gelang es David Kahn im Jahr 1967, die grundlegendste und bis dahin aktuellste Geschichte der Kryptographie zu verfassen.[5] Kahn legte damit aber nicht nur ein fundamentales Geschichtsbuch vor, sondern beeinflusste mit seinem Lebenswerk eine ganze Genera-

3 Der Begriff *Kryptographie* ist abgeleitet vom griechischen κρυπτός (dt. *geheim*) und γράφειν (dt. *schreiben*). Damit ist das Schutzziel der Vertraulichkeit gemeint, das sowohl in der Klassischen als auch in der Modernen Kryptographie vorhanden ist.

4 Charakteristisch ist für die Klassische Kryptographie zudem, dass sie manchmal eher als Kunst definiert wird. Siehe zur Diskussion Katz und Lindell, *Introduction to Modern Cryptography*, S. 3. Joachim von zur Gathen charakterisiert die Kryptographie etwa als „the art of making secure systems"; Joachim von zur Gathen. *CryptoSchool*. Berlin und Heidelberg: Springer, 2015, S. 13.

5 Siehe in der Version von 1996 Kahn, *The Codebreakers*. Für Craig Jarvis handelt es sich bei *The Codebreakers* gar um die „authoritative history of cryptology"; Craig Jarvis. *Crypto Wars: The Fight for Privacy in the Digital Age. A Political History of Digital Encryption*. Boca Raton: CRC Press, 2021, S. 71, weiterführend auch 71–74. Neben Kahn werden im Folgenden weitere Geschichtswerke betrachtet, insbesondere Bauer, *Secret History*; Dooley, *History of Cryptography and Cryptanalysis*; sowie Gathen, *CryptoSchool*. Für eine populärwissenschaftliche Einführung siehe auch Simon Singh. *The Code Book: The Secret History of Codes and Codebreaking*. Taschenbuchausgabe. London: Fourth Estate, 2000. Eine konzise Einführung in die Klassische Kryptographie liefert auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–16. Historisch wurde im Englischen teilweise zwischen *code* und *cipher* unterschieden, wobei bei Ersterem Wörter des Klartextes mit alphabetischen oder numerischen *codes* ausgetauscht wurden; *cipher* hingegen bezieht sich auf Transformationen von kleineren Elementen des Klartextes. Siehe dazu Whitfield Diffie und Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Überarbeitete und erweiterte Version. Cambridge, MA, und London: MIT Press, 2007, S. 13–14. Im Folgenden wird meist von Verschlüsselung im Sinne der *ciphers* gesprochen.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

tion von herausragenden Kryptographinnen und Kryptographen.[6] In der Begründung einer dediziert kryptographischen Geschichtswissenschaft steht *The Codebreakers* metaperspektivisch ganz im Zeichen des Paradigmenwechsels der zweiten Hälfte des 20. Jahrhunderts.[7] Denn seit dessen Veröffentlichung handelt es sich mit jener Forschung zur Geschichte der Kryptographie um ein lebendiges Forschungsfeld. Immer wieder kommen neue, lange Zeit unbekannte Informationen über vergangene kryptographische Methoden ans Licht.[8] Der Zeitpunkt dieser Erkenntnisse ist nun vor allem dadurch bedingt, dass es sich aufgrund des Paradigmenwechsels um ein relativ junges Feld der Geschichtsforschung handelt. Die Kryptographie war über Jahrtausende eine Art Geheimwissenschaft, über deren Fortschritt nur wenig an die Öffentlichkeit oder in Feindeshand gelangen sollte.

Diese längere Zeit der intransparenten und unbekannten Wissenschaft könnte den Eindruck erwecken, dass die Kryptographie selbst eigentlich eine noch sehr junge Disziplin sei.[9] Tatsächlich aber reichen die Ursprünge und die Motivation zum verschlüsselten Kommunizieren historisch weit zurück. David Kahn erkennt sogar eine mögliche Kausalität zwischen dem menschlichen Drang nach Privatsphäre und der Entwicklung der Kryptographie:

6 So z. B. Whitfield Diffie; siehe Steven Levy. *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. New York: Penguin Books, 2002, S. 21–24.

7 Siehe zum Umfeld der 1960er-Jahre und der kryptographischen Geschichtsschreibung auch David Naccache, Peter Y. A. Ryan und Jean-Jacques Quisquater. „Preface". In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. IX–X; sowie Andrew J. Clark. „Foreword". In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. VII–VIII.

8 Vor allem erscheint immer wieder neuere Forschung in der Zeitschrift *Cryptologia*, in der etwa erst 2011 gezeigt wurde, dass das bedeutende *One-Time-Pad* bereits vor Vernam und Mauborgne beschrieben wurde. Siehe Steven M. Bellovin. „Frank Miller: Inventor of the One-Time Pad". In: *Cryptologia* 35.3 (2011), S. 203–222; zu den Hintergründen des Artikels von Bellovin auch Bauer, *Secret History*, S. 102–103.

9 Siehe Charles Berret. „The Cultural Contradictions of Cryptography: A History of Secret Codes in Modern America". Dissertation. New York: Columbia University, 2019. URL: https://academiccommons.columbia.edu/doi/10.7916/d8-3h8z-4t93 (besucht am 15.04.2024), S. 133.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

> It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated.[10]

Solch eine Kryptographie scheint also eng mit zivilisatorischer Entwicklung zusammenzuhängen. Sie ist damit auch immer nicht bloß reine Technologie gewesen, sondern kontextuell eingebunden in politische, soziale, gesellschaftliche und historische Rahmenbedingungen. In ihrer Natur als kommunikatives Werkzeug ist Kryptographie also seit jeher auch eine sozial-gesellschaftliche Sache. Zwar war eine rigorose Verschlüsselung, wie wir sie heute kennen, nicht notwendig, um Informationen geheim zu halten oder verschlüsselt kommunizieren zu können. Lesen und Schreiben war in einer analphabetischen Gesellschaft bereits eine hohe Hürde, sodass weitere Maßnahmen oft nicht erforderlich waren.[11] Manche Texte und Schriften wurden allerdings als eine Art „cosmic top secrets"[12] verstanden und sollten durch weiteren Schutz nur der königlichen Oberschicht zugänglich sein.[13] Nach Kahn begann die (nachgewiesene) Geschichte der Kryptologie vor viertausend Jahren in einem Dorf in der Nähe des Nils:

> On a day nearly 4000 years ago, in a town called Menet Khufu bordering the thin ribbon of the Nile, a master scribe sketched out the hieroglyphs that told the story of his lord's life – and in so doing he opened the recorded history of cryptology.[14]

Natürlich erkennt Kahn auch, dass es sich dabei nicht um ein „system of secret writing"[15] gehandelt hatte, wie es die moderne Welt kenne. Dieser

10 Kahn, *The Codebreakers*, S. 84; zitiert auch in Dooley, *History of Cryptography and Cryptanalysis*, S. 5.

11 Siehe Gathen, *CryptoSchool*, S. 70; sowie Jan Assmann. „Zur Ästhetik des Geheimnisses. Kryptographie als Kalligraphie im alten Ägypten". In: *Zeichen zwischen Klartext und Arabeske. Konferenz des Konstanzer Graduiertenkollegs „Theorie der Literatur". Veranstaltet im Oktober 1992*. Hrsg. von Susi Kotzinger und Gabriele Rippl. Amsterdam und Atlanta: Rodopi, 1994, S. 175–186, hier S. 178.

12 Gathen, *CryptoSchool*, S. 70.

13 Siehe ebd., S. 70; umfassender auch Assmann, „Zur Ästhetik des Geheimnisses".

14 Kahn, *The Codebreakers*, S. 71.

15 Ebd., S. 71.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

anonyme Schreiber führte aber zumindest eine absichtliche Transformation des Textes durch.[16] Kahn bezeichnet die Kryptologie des alten Ägyptens daher auch als „quasi cryptology in contrast to the deadly serious science of today"[17].

Auf ähnliche Weise analysiert der Ägyptologe Jan Assmann die Kryptographie als Kalligraphie im alten Ägypten.[18] Schließlich gelang es Jean-François Champollion erst im Jahr 1822, die Bedeutung der Hieroglyphen zu entschlüsseln. Bis zu diesem geschichtlichen Ereignis hatte man sie Assmann zufolge tatsächlich für Kryptographie gehalten. Dies stellte sich als ein „gründliches Mißverständnis"[19] heraus, wie er schreibt – allerdings um ein „interessantes und produktives Mißverständnis"[20]. Bei den Hieroglyphen handelt es sich nämlich keineswegs um irgendeine Form von „Geheimniskrämerei, Verrätselung, Arcanisierung"[21], was aufgrund von Analphabetismus auch nicht notwendig gewesen wäre.[22] Trotzdem gab es nach Assmann verschiedene Formen einer „Kryptographie im literarischen Sinne"[23].

Mit dieser historischen Einordnung dürfte für Teil I deutlich werden: Der konkrete Beginn dessen, was *heute* als Kryptographie verstanden wird, ist teilweise diffus und nur schwer zu lokalisieren. Das Beispiel ägyptischer Hieroglyphen lässt unterschiedliche Ebenen der Beziehung zur Kryptographie zu, die gar bis zu einer „Verrätselung zum Zwecke der Ästhetisierung"[24] reichen konnten. Der Ursprung kryptographischer Kommunikation liegt eben nicht in einer rigorosen Mathematik. Unterschiedliche Ziele, Motive und Methodiken bedeuten ein facettenreiches Bild der Anfänge der Kryptographie.

Bereits an dieser Stelle ist jedoch eine Faszination für die *Verschlüsselung* zu unterscheiden von einer Faszination für das *Verschlüsselte* selbst.

16 Siehe ebd., S. 71.

17 Ebd., S. 72.

18 Siehe dazu und zum Folgenden Assmann, „Zur Ästhetik des Geheimnisses". Siehe allgemein einführend auch Singh, *The Code Book*, S. 201–217.

19 Assmann, „Zur Ästhetik des Geheimnisses", S. 175.

20 Ebd., S. 175.

21 Ebd., S. 178.

22 Siehe ebd., S. 178.

23 Ebd., S. 178. So lassen sich Beispiele einer sogenannten *Entkonventionalisierung* finden: „Entweder, die vorhandenen Zeichen erhalten eine andere als die konventionelle Bedeutung, oder es werden andere als die konventionellen Zeichen, d. h. neue Zeichen eingeführt"; ebd., S. 180.

24 Ebd., S. 183.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Erstere ist das, was diese Arbeit als Kryptographie versteht. Letztere dagegen legt den Fokus auf das Verschlüsselte selbst. Dies inkludiert unter anderem die Suche nach Geheimbotschaften, verborgenen Wahrheiten, paranormalen Schriften. Ein prominentes Beispiel ist hierbei die Suche nach solchen versteckten Botschaften, Wahrsagungen und Prophezeiungen in Offenbarungen wie der Bibel.[25] Eine Ethik der Kryptographie, wie sie hier gedacht ist, wird versteckte Prophezeiungen und das Verschlüsselte selbst nicht behandeln. Es geht ihr vielmehr um die Grundlagen von Kryptographie, Technologie und Gesellschaft mit Blick auf die zukünftige Anwendung. Ausschließlich Letzteres ist Untersuchungsgegenstand einer Ethik der Kryptographie.[26]

Eine solche Kryptographie, wie sie im Rahmen dieser Arbeit inkludiert sein könnte, lässt sich aber auch in der hebräischen Bibel finden. Dabei handelt es sich um eine Substitution, die als *atbash*-System bezeichnet wird.[27] Substitutionsmethoden wie im *atbash*-System werden zur sogenannten *symmetrischen* Kryptographie eingesetzt, die für die Zeit der Klassischen Kryptographie charakteristisch ist. *Symmetrisch* meint in diesem Zusammenhang, dass der Schlüssel zum Verschlüsseln (genannt k_e) identisch ist mit dem Schlüssel zum Entschlüsseln (genannt k_d), also $k_e = k_d$.[28] Dies mag auf den ersten Blick sinnvoll oder gar notwendig erscheinen, allerdings wird auch hier der Modernen Kryptographie der

25 Ein Beispiel hierfür ist Drosnins kritisierte Monographie *The Bible Code*. Siehe Michael Drosnin. *The Bible Code*. New York: Simon & Schuster, 1997. Zur berechtigten Kritik an der generell dahinterstehenden Methode der *Equidistant Letter Sequence* siehe Brendan McKay u. a. „Solving the Bible Code Puzzle". In: *Statistical Science* 14.2 (1999), S. 150–173.

26 Noch spezifischer wäre hier das *Verschlüsselte* von der *Methodik* des Verbergens von Nachrichten zu unterscheiden. Bei dieser handelt es sich dann nämlich um eine Form der *Steganographie*. Als Steganographie wird eine Methode bezeichnet, bei der Nachrichten, die geheim gehalten werden sollen, in anderen Nachrichten *verborgen* werden. In gewissem Maße kann die Steganographie als Teil der wissenschaftlichen Kryptographie auch ethisch relevant sein, z. B. im Rahmen des Whistleblowings. Da dies aber eine untergeordnete Rolle spielt, wird es nicht näher diskutiert. Siehe zur Steganographie einführend z. B. Frank Y. Shih. *Digital Watermarking and Steganography: Fundamentals and Techniques*. 2. Aufl. Boca Raton: CRC Press, 2017; sowie Ingemar J. Cox u. a. *Digital Watermarking and Steganography*. Burlington: Morgan Kaufmann, 2008.

27 Siehe Kahn, *The Codebreakers*, S. 77–78; einführend auch Bauer, *Secret History*, S. 19.

28 Üblicherweise werden in der Literatur englische Begriffe verwendet. *k* steht daher für *key*, *e* für *encrypt* und *d* für *decrypt*. Siehe einführend zur symmetrischen Kryptographie z. B. Gathen, *CryptoSchool*, S. 37–38.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Durchbruch gelingen. Einige Forschende werden in den 1970er-Jahren nämlich zeigen, dass k_e nicht zwangsläufig auch k_d sein muss.[29]

Für die symmetrische Kryptographie gibt es zwei grundsätzliche Methodiken zur Ver- und Entschlüsselung: die bereits genannte *Substitution* sowie eine *Transposition*.[30] Bei einer Substitution werden Zeichen eines Alphabets – zum Beispiel Buchstaben – nach einer vorgegebenen Systematik ersetzt. Bei einer Transposition hingegen wird die Anordnung solcher Zeichen vertauscht. Beide Methodiken sind ein wichtiges Bauteil für die symmetrische Verschlüsselung, die in ihrer weiterentwickelten Form bis heute vertrauliche Kommunikation sicherstellen kann.

Die mathematischen Definitionen der beiden Methoden werden an dieser Stelle ausgelassen, jedoch soll die grundsätzliche Idee deutlich gemacht werden: Indem bei einer Transposition (auch Permutation genannt) die *Anordnung* von Zeichen vertauscht wird, könnte beispielsweise aus dem Wort *cryptolove* das Wort *rcpyotolev* werden. Der erste Buchstabe wird dabei mit dem zweiten getauscht, der dritte mit dem vierten usw. Bei der Substitution hingegen werden Zeichen des Klartextes durch Zeichen eines Chiffrentextes *ersetzt*. Mit der Regel, alle *o* durch ein *l* (und umgekehrt) zu ersetzen, würde etwa die Zeichenkette *cryptolove* zu *cryptlolve*. Der womöglich bekannteste Algorithmus einer solchen Substitution ist die sogenannte Caesar-Chiffre.[31] Bei dieser wird jedes Zeichen aus einem geordneten Alphabet des Klartextes zyklisch auf ein Zeichen aus dem geordneten Alphabet des verschlüsselten Textes abgebildet.[32] Mit einem Schlüssel $k = 3$ wird zum Beispiel der Buchstabe a zum Buchstaben d, b zu e, c zu f usw. bis zum Buchstaben z, der zum

29 Die entsprechende Methode wird daher dann auch als *asymmetrische* Kryptographie bezeichnet. Siehe Abschnitt 2.3.

30 Diese heute übliche Teilung wurde bereits im 16. Jahrhundert von Giovanni Battista Porta grob beschrieben; siehe Kahn, *The Codebreakers*, S. 139. Siehe zur folgenden Einführung Katz und Lindell, *Introduction to Modern Cryptography*, S. 10–13; sowie Gathen, *CryptoSchool*, S. 61–69; für den umfassenden historischen Kontext auch Bauer, *Secret History*, S. 3–57 und 107–127.

31 Caesar selbst beschreibt eine Idee der Kryptographie in seinem bekannten Werk *De bello Gallico*. Von der *Caesar-Chiffre* berichtet erstmalig allerdings der römische Geschichtsschreiber Sueton in seinem Werk *De vita Caesarum*. Siehe dazu Kahn, *The Codebreakers*, S. 83–84; sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 13–14. Sie wird häufig in der Didaktik genutzt, um die grundsätzlichen Verfahrensweisen von Kryptographie zu erläutern.

32 Siehe hierzu und zur folgenden Beschreibung einführend Bauer, *Secret History*, S. 7–8. Caesar selbst hatte keine unterschiedlichen Schlüssel verwendet, jedoch ge-

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Buchstaben *c* wird. Ein Klartext *cryptolove* wird damit zu *fubswroryh*. Die Entschlüsselung erfolgt anschließend umgekehrt.

Besonders faszinierend ist die Caesar-Chiffre nicht nur aufgrund ihrer Verständlichkeit im pädagogischen Sinne, sondern vor allem durch ihre Historizität. Suetons Beschreibung der Caesar-Chiffre war nach John F. Dooley die erste schriftliche Beschreibung der modernen monoalphabetischen Substitutionsmethode unter Verwendung eines verschobenen Standardalphabets.[33] Bis heute ist das Grundprinzip der Substitution ein entscheidendes Primitiv für praktisch anwendbare Kryptographie. Mit dem Fall des Römischen Reiches verschwand das Wissen über die Kryptographie allerdings für eine gewisse Zeit.[34] Für Dooley wandelte sich die Kryptographie sogar „from a useful technique for keeping communications secret into a dark art that bordered on magic“[35].

Im Mittelalter war es daher auch im arabischen Raum, wo während des islamischen goldenen Zeitalters eine der einflussreichsten Methoden zum Brechen von Substitutionsmethoden entwickelt wurde: die Häufigkeitsanalyse (engl. *Frequency Analysis*), erstmalig beschrieben durch den islamischen Universalgelehrten al-Kindī.[36] Die revolutionäre Erkenntnis dabei war, dass linguistische Charakteristika durch eine monoalphabetische Substitutionsmethode *nicht* versteckt werden. In der englischen Sprache kommt der Buchstabe *e* beispielsweise häufiger vor als *l*, der Buchstabe *k* wiederum häufiger als *x*.[37] Mit einem entsprechend großen Datensatz bestehend aus Briefen, Büchern oder Notizen können die pro-

nügt folgende Beschreibung zur Darstellung der Funktionsweise. Siehe weiterführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–10.

33 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 14. Nach Beutelspacher begann die Kryptographie sogar mit Caesar, da dieser einerseits keine Geheimzeichen verwendete und andererseits eine Variabilität eingebaut wurde; siehe Albrecht Beutelspacher. *Geheimsprachen und Kryptographie: Geschichte, Techniken, Anwendungen*. 6. Aufl. München: C. H. Beck, 2022, S. 18–19. Letzterer Aspekt zur Variabilität ist jedoch historisch unklar, da Caesar selbst einen fixen Schlüssel verwendet hatte; siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–9.

34 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 15.

35 Ebd., S. 15.

36 Siehe dazu und zur folgenden Beschreibung der Häufigkeitsanalyse ebd., S. 15 und 18. Umfassender zur arabischen Kryptologie auch Gathen, *CryptoSchool*, S. 499–503. Zur Häufigkeitsanalyse siehe einführend Bauer, *Secret History*, S. 17–18.

37 Siehe zur Häufigkeitsverteilung Katz und Lindell, *Introduction to Modern Cryptography*, S. 11.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

zentualen Häufigkeiten für alle Buchstaben eines Alphabets einer bestimmten Sprache angegeben werden.

Mit diesem Wissen erfolgt die Entschlüsselung eines mit einer monoalphabetischen Substitutionsmethode verschlüsselten Textes, indem die Vorkommnisse der einzelnen Buchstaben im verschlüsselten Text gezählt werden.[38] In einem längeren verschlüsselten Text fällt dann vielleicht auf, dass der Buchstabe *g* am häufigsten vorkommt. Der Buchstabe *v* am zweithäufigsten usw. Wir wissen zudem bereits, dass das *e* in englischen Klartexten am häufigsten vorkommt, der Buchstabe *t* am zweithäufigsten usw. Uns fällt schließlich auf: Der Buchstabe *g* ist der zweite Buchstabe nach *e*, und auch der Buchstabe *v* ist der zweite Buchstabe nach *t*. Sofern es sich um eine Caesar-Verschlüsselung handelt, können wir daher vermuten, dass der Text mit dem Schlüssel $k = 2$ verschlüsselt wurde.

Diese Häufigkeitsanalyse ist Teil der *Kryptoanalyse*, des Gegenstücks zur Kryptographie. Während die Klassische Kryptographie als die Verschlüsselung von Texten definiert ist, versucht sich die Kryptoanalyse an der Entschlüsselung von bereits verschlüsselten Texten.[39] Die Oberbezeichnung sowohl für die Kryptoanalyse als auch für die Kryptographie ist die sogenannte *Kryptologie*. Heute allerdings wird der Begriff *Kryptographie* in der Praxis oftmals synonym zu Kryptologie verwendet.[40] Ein Grund hierfür liegt sicherlich darin, dass Kryptographie und Kryptoanalyse untrennbar zusammengehören: Ein Algorithmus, der nicht auf mögliche Angriffe per Kryptoanalyse hin untersucht wurde, kann nicht als sicher eingestuft werden. Daher findet bereits seit jeher eine Wechselwirkung von Kryptographie und Kryptoanalyse statt. Es gab Zeiten, in denen Kryptoanalystinnen und Kryptoanalysten im Vorteil waren. Während anderer Zeiten wiederum sollten Kryptographinnen und Kryptographen die

38 Diese und die folgenden Erläuterungen der Entschlüsselung orientieren sich an ebd., S. 11–12. Siehe umfassender auch Gathen, *CryptoSchool*, S. 87–95.

39 Siehe zur Einführung in diese und die folgenden, üblichen Definitionen etwa Bauer, *Secret History*, S. xix–xxi; sowie Kahn, *The Codebreakers*, S. xv–xviii, für die Kryptoanalyse vor allem S. xviii.

40 Martin Hellman sagte einmal in einem späteren Interview bezogen auf die Begriffe *Cryptology* und *Cryptography*: „Yeah. I use the two interchangeably. David Kahn would tell me I'm wrong, and he's probably right, but 'cryptography' has a nicer ring to it than 'cryptology.'" Interview in Hugh Williams. *An Interview with Martin Hellman. Recipient of the 2015 ACM Turing Award*. Palo Alto, 19. Mai 2017. URL: https://amturing.acm.org/pdf/HellmanTuringTranscript.pdf (besucht am 15.04.2024), S. 13.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Oberhand haben – zum Beispiel mit *polyalphabetischen Substitutionsmethoden*, wie wir gleich sehen werden.[41]

Obschon Kryptographie nach David Kahn in der ein oder anderen Form eine zivilisatorisch-kulturelle Folge ist, war die praktische Auseinandersetzung mit ihr doch lange Zeit auch ein gesellschaftliches Nischen- oder Randthema. Wie im Kontext der Anfänge der Kryptographie deutlich geworden ist, galt dies insbesondere für eine Zeit, in der viele Menschen weder schreiben noch lesen konnten. Allein dieses Faktum erlaubte bereits ein gewisses Maß an Vertraulichkeit der verschriftlichten Kommunikation. Erst im Italien der frühen Renaissance lässt sich dann die erste systematische, gut dokumentierte Nutzung im westlichen Europa erkennen.[42] Die Kryptoanalyse, insbesondere die einfache Häufigkeitsanalyse, war zu diesem Zeitpunkt bereits weiterentwickelt und das Reisen war unsicher, sodass briefliche Kommunikation abgefangen werden konnte.[43] Eine solche Situation ist – analogisch gedacht – beim heutigen Internet nicht viel anders: Nachrichten können mitgelesen, mitgeschnitten, abgehört werden. Ähnlich wie zu damaliger Zeit gibt es kaum direkt in den Kommunikationskanälen implementierte Sicherheiten, die die Angriffe verhindern könnten. Kommunikationskanäle mussten damals wie heute als grundsätzlich unsicher gelten.

Besondere Bedeutung hatte in dieser Zeit daher die Entwicklung jener polyalphabetischen Substitutionsmethode durch Leon Battista Alberti, den Kahn als „Father of Western Cryptology"[44] beschreibt. Mit einer monoalphabetischen Substitutionsmethode wie der Caesar-Chiffre wird ein Buchstabe des Alphabets immer durch einen anderen Buchstaben eines Alphabets ersetzt. Da also ein *e* immer durch den gleichen Buchstaben wie etwa *c* substituiert wird, ist der Buchstabe *c* im verschlüsselten Text genauso häufig vorhanden wie der Buchstabe *e* im unverschlüsselten Ursprungstext. Im Gegensatz dazu ist die Idee der polyalphabetischen Substitutionsmethode nun, *mehrere* Alphabete zur Verschlüsselung zu nutzen.[45]

41 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 37.
42 Siehe Gathen, *CryptoSchool*, S. 79.
43 Siehe ebd., S. 79.
44 Kahn, *The Codebreakers*, S. 125, auch S. 130. Siehe zu Alberti einführend auch Gathen, *CryptoSchool*, S. 80–81.
45 Siehe Kahn, *The Codebreakers*, S. 125.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Alberti legte dafür den Grundstein in der zweiten Hälfte des 15. Jahrhunderts.[46] Trithemius entwickelte die *tabula recta*, während Belaso eine Erweiterung des Systems mit einem einfach zu merkenden Schlüsselwort beschrieb, was entschieden zur Sicherheit des Systems beitragen konnte. Giovanni Batista Porta fügte schließlich die Gedanken der drei Gelehrten zusammen. Eine noch sicherere Version polyalphabetischer Kryptographie entwickelte aber Blaise de Vigenère. Seine Idee war dabei die Verwendung eines *autokey*, mit dem die Nachricht selbst als ihr eigener Schlüssel dient. Die Methode allerdings, die später als *Vigenère-Chiffre* bzw. *le chiffre indéchiffrable* (dt. *die nicht entschlüsselbare Verschlüsselung*) bezeichnet wurde und für die Vigenère bekannt geworden ist, ist lediglich eine vereinfachte Version polyalphabetischer Kryptographie.[47]

Eine reine Häufigkeitsanalyse, die bei monoalphabetischen Substitutionsmethoden sehr erfolgreich sein konnte, ist ohne eine Verbesserung selbst bei der vereinfachten Vigenère-Chiffre kaum vielversprechend. Erst im 19. Jahrhundert entwickelten der Mathematikprofessor Charles Babbage sowie der preußische Major Friedrich Wilhelm Kasiski unabhängig voneinander eine Methode, die eine entscheidende Schwäche der Vigenère-Chiffre ausnutzt: Das Schlüsselwort, mit dem das jeweilige Alphabet zur Verschlüsselung gewählt wurde, wiederholt sich in einem längeren Text mehrfach.[48] Identische Teile des Klartextes (z. B. der im Deutschen häufig vorkommende Artikel *der*) können nämlich in einem langen Text mehrfach mit einem gleichen Teil des Schlüssels verschlüsselt worden sein. Mithilfe dieser Erkenntnis wird zunächst die mögliche Schlüssellänge eingegrenzt. Anschließend kann auf jedes einzelne Alphabet wieder eine Häufigkeitsanalyse angewandt werden. Heute bekannt ist diese Methode als *Kasiski-Test*.[49] Trotz der höheren Sicherheit und der revo-

46 Siehe zu Alberti, Trithemius, Belaso, Porta und Vigenère im Folgenden Dooley, *History of Cryptography and Cryptanalysis*, S. 37–39; sowie Bauer, *Secret History*, S. 61–65. Ausführlicher siehe auch Kahn, *The Codebreakers*, S. 125–148. Kahn lehnt dabei auch die Bezeichnung für Trithemius als „Father of Cryptology" ab; siehe ebd., S. 136–137.

47 Siehe dazu im Speziellen Dooley, *History of Cryptography and Cryptanalysis*, S. 39, und Kahn, *The Codebreakers*, S. 148. Eine erste Version eines *autokey* entwickelte Cardano, die allerdings problembehaftet war; siehe ebd., S. 143–144.

48 Siehe hierzu und zur folgenden Beschreibung ebd., S. 204–213, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 69–71. Für eine eher technische Einführung mit Beispiel siehe Gathen, *CryptoSchool*, S. 241–250.

49 Dabei entdeckte Babbage diese Methode neun Jahre vor Kasiski. Zu den möglichen Gründen für die Benennung sowie als Einführung zu Babbage und Kasiski siehe

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

lutionären Gedanken blieben polyalphabetische Substitutionsmethoden aber lange Zeit wenig genutzt, zumindest verglichen mit sogenannten *Nomenklaturen*.[50] Einerseits waren polyalphabetische Substitutionsmethoden nämlich langsamer als die Nomenklaturen, andererseits wurde ihrer Genauigkeit nicht wirklich vertraut.[51]

Eine andere Person der Kryptographiegeschichte, die einen vielleicht noch größeren Einfluss auf das Verständnis heutiger Verschlüsselungsmethoden hatte, war aber der Niederländer Auguste Kerkhoffs.[52] Im Jahr 1883 veröffentlicht er sein Werk *La Cryptographie militaire*.[53] Für Kahn ist diese Arbeit neben Portas *De Furtivis Literarum Notis* das zweite großartige „outward-looking"[54] Buch. Er beschreibt es gar als „the most concise book on cryptography ever written"[55]. Das große Problem für die Kryptographie zur damaligen Zeit waren angesichts der Möglichkeit telegraphischer Kommunikation nämlich Anwendungsfragen.[56] Kerckhoffs holte die Kryptographie damit aus ihrem eigenen Dunstkreis heraus und führte sie in ein neues Zeitalter der Kommunikation.

Bedeutend ist dabei vor allem, dass Kerckhoffs die Kryptographie in enger Verbindung mit der Kryptoanalyse dachte.[57] Kryptographie und Kryptoanalyse sind auch in der Modernen Kryptographie keine Gegen-

---

Singh, *The Code Book*, S. 78; außerdem Kahn, *The Codebreakers*, S. 207. Eine weitere, scharfsinnige Methode ist der von William Friedman entwickelte *Index of Coincidence* von 1920. Siehe weiterführend Abschnitt 2.1.

50 Siehe ebd., S. 150–154. Nomenklaturen sind ein System, das einerseits aus Codes und andererseits aus Chiffren besteht. Bestimmte Worte werden bei Nomenklaturen explizit codiert. Siehe zur Definition ebd., S. xvii, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 10.

51 Siehe Kahn, *The Codebreakers*, S. 150.

52 Sein ursprünglicher und voller Name war etwas länger und zeigt unzweifelhaft seine adelige Herkunft aus einer der ältesten flämischen Familien, nämlich Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof. Siehe ebd., S. 230.

53 Siehe Auguste Kerckhoffs. „La Cryptographie Militaire: Première partie". In: *Journal des sciences militaires* IX (Jan. 1883), S. 5–38; sowie Auguste Kerckhoffs. „La Cryptographie Militaire: Seconde Partie". In: *Journal des sciences militaires* IX (Feb. 1883), S. 161–191.

54 Kahn, *The Codebreakers*, S. 230.

55 Ebd., S. 233.

56 Siehe ebd., S. 233.

57 Wie Kahn schreibt: „Kerckhoffs established ordeal by cryptanalysis as the only sure trial for military cryptography. It is the judgement which is still used today"; ebd., S. 235. Siehe einführend zu Kerckhoffs auch Bauer, *Secret History*, S. 157–158.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

sätze, sondern bedingen einander. Ein kryptographisches System kann nicht als sicher bezeichnet werden, wenn nicht ein möglichst großer Aufwand betrieben wurde und wird, es zu brechen. Wir werden später sehen, wie dies im 20. und 21. Jahrhundert an vielen Algorithmen deutlich wird, zum Beispiel im Rahmen von Standardisierungen von kryptographischen Verfahren wie AES.

Bekannt geworden ist Kerckhoffs aber durch die Beschreibung von sechs Voraussetzungen oder Grundsätzen für ein kryptographisches System.[58] Am wichtigsten für die heutige Kryptographie wurde der zweite Grundsatz, der auch als *Kerckhoffs' Prinzip* bezeichnet wird.[59] Heute sagt dieses Prinzip aus, dass die Sicherheit eines Systems *allein* in der Geheimhaltung des Schlüssels liegen darf.[60] Dieses Prinzip ist damit auch die Antwort auf *Security by Obscurity* – eine Methode, bei der nicht allein der Schlüssel geheim gehalten wird, sondern auch die Funktion und die Verfahrensweise des Systems.[61] Kerckhoffs verband mit seiner Arbeit und diesen Grundsätzen die Kryptographie mit der Telegraphie. Aber auch danach war Kryptographie immer abhängig von den aktuellen technologischen und maschinellen Möglichkeiten, wie der nächste Abschnitt zeigen wird.

58 Diese Grundsätze sind: (1) Das System sollte, wenn auch nicht theoretisch, in der Praxis unknackbar sein. (2) Die Kompromittierung der Details des Systems sollte den Korrespondentinnen und Korrespondenten keine Unannehmlichkeiten bereiten. (3) Der Schlüssel sollte ohne Notizen zu merken und leicht zu ändern sein. (4) Das Kryptogramm sollte sich telegrafisch übertragen lassen. (5) Das Verschlüsselungsgerät sollte tragbar und von einer einzigen Person bedienbar sein. (6) Das System sollte einfach sein und weder die Kenntnis einer langen Liste von Regeln noch geistige Anstrengung voraussetzen. Eigene Übersetzung ausgehend von Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 14, sowie Kahn, *The Codebreakers*, S. 235. Siehe im französischen Original Kerckhoffs, „La Cryptographie Militaire", S. 12.

59 Siehe zu einer aktuelleren und ausführlichen Diskussion zu Kerckhoffs' Prinzip Katz und Lindell, *Introduction to Modern Cryptography*, S. 7–8.

60 Siehe Kahn, *The Codebreakers*, S. 236.

61 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 8. Manchmal wird die Methode auch als *Security through Obscurity* bezeichnet; siehe Claudia Eckert. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. 10. Auflage. Berlin und Boston: De Gruyter Oldenbourg, 2018, S. 173.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

1.2 Die Mechanisierung der Kryptographie

Der Erste Weltkrieg markiert den letzten größeren militärischen Konflikt, in dem Geheimdienstoffiziere die Ver- und Entschlüsselung *von Hand* verrichten sollten.[62] Bis dahin waren es denn auch meist Einzelne oder kleinere Gruppen, die an der Ver- und Entschlüsselung arbeiteten. Für Whitfield Diffie und Susan Landau war Kryptographie während des Ersten Weltkriegs daher auch mehr „an esoteric than a secret field"[63]. Und für Dooley gibt es zwei Gründe für das Ende einer Vorstellung, die er beschreibt als „romantic notion of the single, driven cryptanalyst working alone through the night to crack the cryptogram that would bring victory to his side"[64].

Der eine Grund sei die Erfindung des Radios und drahtloser Telegraphie.[65] Nicht mehr nur einige wenige Nachrichten konnten pro Tag per Bote oder Telegramm versendet und empfangen werden. Nun war es möglich, ohne größeren Aufwand mithilfe Tausender solcher Nachrichten zu kommunizieren. Dies führte zu der Problematik, dass eine manuelle Ver- und Entschlüsselung dieser unzähligen Nachrichten kaum mehr praktikabel war. Kommunikation wurde omnipräsent – und mit ihr auch die Notwendigkeit einer automatisierten Verschlüsselung dieser Kommunikation.

Der andere Grund für eine Automatisierung liegt Dooley zufolge in der Idee, Ver- und Entschlüsselung durch Maschinen zu ermöglichen.[66] Während Substitution, Codebücher, Permutationsalgorithmen und Schlüsseladditionen seit bereits mehreren hundert Jahren Verwendung gefunden hatten, blieb die breite Anwendung von Kryptographie mithilfe von elektromechanischen Maschinen und später auch Computern dem 20. Jahrhundert vorbehalten.[67] Für die Patentierung und den

62 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 87. Zur kryptographischen Geschichte des Ersten Weltkriegs siehe Bauer, *Secret History*, S. 163–198; sowie John F. Dooley. *Codes, Ciphers and Spies: Tales of Military Intelligence in World War I*. Cham: Copernicus, 2016.

63 Diffie und Landau, *Privacy on the Line*, S. 58.

64 Dooley, *History of Cryptography and Cryptanalysis*, S. 87.

65 Siehe dazu und zu diesem Absatz ebd., S. 87.

66 Siehe ebd., S. 88.

67 Siehe für eine visuelle Darstellung dieser verhältnismäßig doch kurzen Episode der elektromechanischen Maschinen seit dem 20. Jahrhundert Gathen, *CryptoSchool*, S. 70.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Verkauf solcher Maschinen wurde vor allem die Zeit zwischen den beiden Weltkriegen genutzt.[68]

Man könnte daher auch von einer *Mechanisierung der Kryptographie* sprechen, die zur entscheidenden Bedingung für den späteren Erfolg von Verschlüsselungstechnologie werden sollte.[69] Zwar gab es bereits weitaus früher Ideen, Ver- und Entschlüsselung zu mechanisieren, beispielsweise bei Alberti, Jefferson und Leibniz.[70] Allerdings ermöglichte erst die erste Hälfte des 20. Jahrhunderts die praktische und weitverbreitete Anwendung solcher kryptographischen Maschinen. Die heute bekannteste Maschine dieser Art war *Enigma*, die vorwiegend im Zweiten Weltkrieg genutzt wurde und deren Bezeichnung an das griechische Wort αἴνιγμα (dt. *Rätsel*) angelehnt ist.[71]

Dabei handelt es sich um eine elektromagnetische Chiffriermaschine, die eine Menge an Polyalphabeten zur Ver- und Entschlüsselung erzeugt, wobei dieselbe Einrichtung und Prozedur sowohl für die Ver- als auch für die Entschlüsselung verwendet wird.[72] Entwickelt wurde diese Maschine ursprünglich vom deutschen Unternehmer Arthur Scherbius. Später wurde Enigma über den gesamten Kriegsverlauf von Deutschland als ausgereifte Verschlüsselungsmethode zur militärischen Kommunikation genutzt und dabei immer wieder verbessert. Aber trotz der ausgefeilten Mechanik war es möglich, Enigma zu brechen. In den 1970er-Jahren erfuhr man von der laut David Kahn „greatest codebreaking operation of the Second World War“[73], genannt *Ultra*, die in Bletchley Park (UK)

68 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 88.

69 Auch Diffie und Landau sowie Singh sprechen von einer *Mechanisierung*; siehe Diffie und Landau, *Privacy on the Line*, S. 57–60, und Singh, *The Code Book*, S. 101–142.

70 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 137. Zu Leibniz siehe Nikolas Rescher. „Leibniz's Machina Deciphratoria: A Seventeenth-Century Proto-Enigma“. In: *Cryptologia* 38.2 (2014), S. 103–115.

71 Siehe einführend zu Enigma Bauer, *Secret History*, S. 217–260.

72 Siehe dazu und zur folgenden Beschreibung von Enigma Dooley, *History of Cryptography and Cryptanalysis*, S. 142 und 151–153; sowie Gathen, *CryptoSchool*, S. 719–725. Die Maschine verwendete unter anderem mehrere *Rotoren*, eine sogenannte *Umkehrwalze*, in manchen Versionen ein *Steckerbrett* sowie die Möglichkeit, die Anordnung der Rotoren zu tauschen; als Schlüssel sind ein *Day Key* und ein *Message Key* erforderlich. Siehe zur Einführung in die Funktionsweise Singh, *The Code Book*, S. 127–142, sowie Bauer, *Secret History*, S. 220–224.

73 Kahn, *The Codebreakers*, S. 972, weiterführend S. 972–978; ausführlicher David Kahn. *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943*. Überarbeitete Auflage. London: Frontline Books, 2012.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

durchgeführt worden war. Maßgeblich beteiligt am Erfolg dieser Operation war der Mathematiker Alan Turing, der aufgrund seiner theoretischen Überlegungen als Pionier der Informatik und der Entwicklung des Computers gilt.[74] Turing und sein Team konnten in Bletchley Park auf polnische Vorarbeiten zurückgreifen, die kurz vor Beginn des Zweiten Weltkriegs mit den Alliierten geteilt worden waren.[75] Nach Dooley handelte es sich bei den polnischen Arbeiten gar um „the first analytical break of a cipher machine by mathematicians turned cryptanalysts".[76] Mit der Kryptoanalyse von Enigma sollte die Mathematik sich also als Wissenschaft der Kryptoanalyse bewähren – ein Vorgeschmack auf das Zeitalter Moderner Kryptographie.

Mit den Modifikationen, die Deutschland nach den kryptoanalytischen Erfolgen Polens eingeführt hatte, waren jedoch die rein mathematischen Methoden nicht mehr zielführend.[77] Zu viele Möglichkeiten von Polyalphabeten machten einen neuen Ansatz erforderlich, der an die *Mechanisierung der Kryptographie* auch im Rahmen der Kryptoanalyse anknüpfen sollte. Die Idee, die Alan Turing verfolgte, war eine sogenannte *Probable-Word*-Attacke, die darauf abzielt, wahrscheinliche Wörter im verschlüsselten Text zu identifizieren.[78] Dazu entwickelte er eine Maschine, genannt *bombe*.[79] Diese Maschine reduzierte die Anzahl von möglichen Schlüsseln, die anschließend von Hand getestet werden mussten. Dadurch war es den Alliierten im Verlauf des Zweiten Weltkriegs immer wieder möglich, mit Enigma verschlüsselte Nachrichten zu entschlüsseln. Zu Kriegsende vermochten sie sogar Nachrichten einer noch weiter verbesserten Version von Enigma zu dechiffrieren.

74 Breitere Bekanntheit erlangte Turing auch durch den sogenannten *Turing-Test*; siehe Alan M. Turing. „I.—Computing Machinery and Intelligence". In: *Mind* LIX.236 (1950), S. 433–460.

75 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 156. Zur Einführung in das Brechen von Enigma siehe Singh, *The Code Book*, S. 143–189. Tatsächlich war es den Kryptoanalysten Marian Rejewski, Henryk Zygalski und Jerzy Rozycki gelungen, eine frühere Version von Enigma mit mathematischen Methoden zu brechen. Siehe ausführlicher Bauer, *Secret History*, S. 226–242.

76 Dooley, *History of Cryptography and Cryptanalysis*, S. 151.

77 Siehe ebd., S. 156.

78 Siehe ebd., S. 156. Die *Probable-Word*-Attacke hatte bereits Porta beschrieben. Wenn das Thema des Textes bekannt war, konnten wahrscheinlich vorkommende Wörter ausprobiert werden. Siehe Kahn, *The Codebreakers*, S. 140.

79 Siehe dazu und zur folgenden Beschreibung des Erfolgs gegen Enigma während des Zweiten Weltkriegs Dooley, *History of Cryptography and Cryptanalysis*, S. 157.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Die Bedeutung von Bletchley Park und Enigma lässt sich an der späteren historiographischen Rezeption verdeutlichen. Simon Singh schreibt beispielsweise, dass wohl „[e]inige, wenn auch umstrittene Stimmen behaupteten, die Leistungen von Bletchley Park seien entscheidend für den Sieg der Alliierten gewesen“[80]. Für Kahn half das Wirken in Bletchley Park zumindest die Atlantikschlacht zu gewinnen, jedoch gilt für ihn die Entschlüsselung nicht als allein entscheidend für den Sieg.[81] Er hinterfragt dabei auch zu Recht die grundsätzliche Quantifizierbarkeit des Einflusses dieses Ereignisses. Für Singh ist hingegen sicher, dass das Wirken in Bletchley Park den Krieg wesentlich verkürzt und viele weitere Opfer verhindert hat.[82]

Diese beispielhafte Episode zeigt für die Relevanz einer Ethik der Kryptographie, dass die Kryptographie im letzten Jahrhundert zunehmend Einfluss auf die sozial-gesellschaftliche Umgebung haben konnte. Die Wissenschaft der Verschlüsselung war immer auch eingebunden in komplexe Zusammenhänge aus Wirtschaft, Politik und Militär. Zum einen entwickelte sich über die Jahrhunderte ein Wechselspiel von denen, die Verschlüsselungsmethoden entwickelten, und jenen, die diese Methoden brechen wollten. Die Partei, die dann selbst vertraulich kommunizieren konnte und gleichzeitig die Nachrichten der anderen Partei zu entschlüsseln vermochte, war im entscheidenden Vorteil.

Zum anderen zeigt dieser historische Abriss der Klassischen Kryptographie, dass Verschlüsselung auch stets von den jeweils möglichen

80 Simon Singh. *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets*. 17. Aufl. München: dtv, 2022, S. 230. Siehe außerdem auch Beutelspacher, *Geheimsprachen und Kryptographie*, S. 33. Zur Rezeption siehe zudem Bauer, *Secret History*, S. 253–254.

81 Siehe dazu und zur folgenden Kritik an der Quantifizierbarkeit David Kahn. „The Significance of Codebreaking and Intelligence in Allied Strategy and Tactics“. In: *Cryptologia* 1.3 (1977), S. 209–222, vor allem S. 218–219; sowie Kahn, *The Codebreakers*, S. 978.

82 Siehe Singh, *Geheime Botschaften*, S. 230. Auch in der Medienkultur wurde das Ereignis im Film *The Imitation Game* mit Benedict Cumberbatch als Alan Turing rezipiert, wenn auch historisch teilweise fragwürdig. Chris Christensen kam in seiner Kritik – erschienen in der kryptographisch-historischen Fachzeitschrift *Cryptologia* – zu dem Schluss, dass die künstlerische Freiheit mit Blick auf die historischen Ereignisse doch zu weit gegangen sei; siehe Chris Christensen. „Review of *The Imitation Game*“. In: *Cryptologia* 41.2 (2017), S. 178–181. Der Film war inspiriert durch Andrew Hodges' Biographie über Alan Turing; siehe Andrew Hodges. *Alan Turing: The Enigma*. Princeton und Oxford: Princeton University Press, 2014.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Kommunikationskanälen und Technologien abhing. In einer Zeit, in der die Bevölkerung zum größten Teil weder lesen noch schreiben konnte, war Kryptographie zur Geheimhaltung von verschriftlichter Information kaum notwendig. Mit der Kommunikationsflut infolge der Telegraphie allerdings wurde Information ubiquitär. Keine Partei konnte mehr auf Kryptographie verzichten. Die Methodiken der Verschlüsselung mussten sich daher an die neuen Realitäten der Technologie anpassen. Kerckhoffs und die Mechanisierung der Kryptographie waren darauf die Antwort.

Enigma steht aber auch sinnbildhaft für eines der letzten Großereignisse vor dem Übergang der Klassischen Kryptographie in ein neues Paradigma. Dieses neue Paradigma sollte nämlich erstmals überhaupt eine fundamentale und dezidierte Beschäftigung der Ethik mit Kryptographie notwendig machen. Bis einschließlich der 1940er- und 1950er-Jahre war die Entwicklung der Kryptographie normativ betrachtet schließlich eher eine *dunkle* Geschichte, die dem einzelnen, gewöhnlichen Individuum wenig bis keinen Vorteil zu bringen vermochte. Kryptographie wurde genutzt zur Kriegsführung, zu einer Art Geheimniskrämerei, zum Schutz vor Informationsverbreitung.[83]

Kryptographie war bis dahin also ein geheimnisvolles Mittel der Mächtigen – und *nur* der Mächtigen. Wer mächtig war, konnte Kryptographie nutzen. Und wer Kryptographie nutzte, wurde noch mächtiger. Im kommenden Paradigma der Modernen Kryptographie hingegen muss niemand schon zuvor in irgendeiner Form mächtig, wohlhabend oder einflussreich sein, um Kryptographie nutzen zu können. Kryptographie sollte nun keine Kunst mehr sein, die einige wenige in den Kammern der Herrschenden durchdenken, entwickeln, brechen und einsetzen. Denn die unzensierte Mathematik wird zur Wissenschaft der Kryptographie. Und genauso wie menschliche Kommunikation wird Kryptographie ubiquitär.

83 Andrew J. Clark erkennt daher in seinem Vorwort zur Festschrift zu Kahns 85. Geburtstag auch: „From its first routine adoption by the Spartans in the fifth century BC, cryptography has been the domain of the military, governments, and spies. Governments throughout the ages have strived to control the dissemination of information relating to cryptology […] and its widespread usage." Clark, „Foreword", S. VII.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

2 Moderne Kryptographie

> The universe believes in encryption.
> – Julian Assange, Gründer von *Wikileaks*[1]

In der Klassischen Kryptographie war die Anwendung verschlüsselter Kommunikation in weiten Teilen nur jenen möglich, die Wissen, Macht, Fähigkeiten und die Technik dazu hatten.[2] Die zweite Hälfte des 20. Jahrhunderts markiert jedoch den Anfang des Paradigmas der *Modernen Kryptographie*. Die Entwicklung hin zu dieser neuen Art der Kryptographie fassen Katz und Lindell wie folgt zusammen:

> [C]ryptography has gone from a heuristic set of tools concerned with ensuring secret communication for the military to a science that helps secure systems for ordinary people all across the globe.[3]

Adams erkennt mit Blick auf Katz und Lindell drei entscheidende Neuerungen: (1) Kryptographie als Wissenschaft, (2) die die Sicherheit der Systeme zum Ziel hat und (3) die dies für gewöhnliche Menschen überall auf der Erde ermöglicht.[4] Rigorose Wissenschaft wurde die Kryptographie vor allem durch den Mathematiker Claude Shannon, der dafür die theoretischen Grundlagen lieferte (Abschnitt 2.1). Aber auch die Entwicklungen der kryptographischen Standards (Abschnitt 2.2) und die asymmetrische Kryptographie (Abschnitt 2.3) sind Ausdruck dieses wissenschaftlichen

1 Julian Assange u. a. *Cypherpunks: Freedom and the Future of the Internet*. New York und London: OR Books, 2012, S. 4.

2 Nach Dooley also „an arcane science, known only to a few and jealously guarded by governments, exiled kings and queens, and religious orders." Dooley, *History of Cryptography and Cryptanalysis*, S. vii.

3 Katz und Lindell, *Introduction to Modern Cryptography*, S. 3; auch zitiert in Carlisle Adams. *Introduction to Privacy Enhancing Technologies: A Classification-Based Approach to Understanding PETs*. Cham: Springer, 2021, S. 242. Für Katz und Lindell zeichnet sich die Moderne Kryptographie auch durch eine zentrale Rolle von Definitionen, die Wichtigkeit von formalen und präzisen Annahmen sowie die Möglichkeit rigoroser Beweise von Security aus. Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv–xvi sowie 16–23.

4 Siehe Adams, *Introduction to Privacy Enhancing Technologies*, S. 242.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Charakters. Insofern Kryptographie nun außerdem mehr als nur Vertraulichkeit der Kommunikation zum Ziel hatte, wurde sie zu einem bedeutenden Teil ganzheitlicher Informationssicherheit (Abschnitt 2.4). In all diesen Kontexten relevant ist heute auch das Verhältnis von Quantum Computing und Verschlüsselung (Abschnitt 2.5).

Die Folge dieses wissenschaftlichen Fokus auf die digitale Sicherheit ist der ubiquitäre und globale Anspruch einer Modernen Kryptographie. Eine Kryptographie nämlich, die nicht ubiquitär wäre, würde eine Asymmetrie von Staat und Individuum schaffen. Und eine Kryptographie, die nicht global wäre, wäre nicht auf diese Weise im weltweiten Internet nutzbar. Mit der Modernen Kryptographie findet Verschlüsselung heute also Anwendung im World Wide Web, im Online-Banking, in der Telefonie, in Smartcards und vielem mehr. Die allermeisten Menschen sind bewusst oder unbewusst auf Verschlüsselungstechnologien angewiesen. Mit dieser Ubiquität könnte man auch sagen: Die Gesellschaft des 21. Jahrhunderts erlebt – tagtäglich und global – die Auswirkungen dieses Paradigmenwechsels.

Dieser Paradigmenwechsel zeigt einerseits die Notwendigkeit und Relevanz einer *Ethik der Kryptographie*. Ohne eine weitverbreitete und ubiquitäre Kryptographie wäre ein solches soziales, politisches und ökonomisches Leben, wie wir es heute kennen, im digitalen Zeitalter kaum möglich. Zugleich beschreibt dieser Paradigmenwechsel aber auch grundlegende strukturelle Veränderungen einer Gesellschaft, in der Kryptographie eben *in der Mitte* der Gesellschaft angekommen ist – und nicht mehr nur der Diplomatie, dem Militär oder Geheimdiensten zur Verfügung stehen sollte. Erst mit einem Wissen um diese fundamentalen Entwicklungen im 20. Jahrhundert wird die Relevanz der Beziehung von Staat und privater Kommunikation, von Cypherpunks und Crypto-Anarchie, von einer Unterdrückung der Verschlüsselung und dem Verhältnis von Internet, Kryptographie und Regulierbarkeit verständlich.

2.1 Ein neues Paradigma durch die Mathematik

Neben jener *Mechanisierung* von Verschlüsselung, wie sie das letzte Kapitel diskutiert hat, liegt der Modernen Kryptographie vor allem ein Wechsel der Disziplin zugrunde: Bis zum Beginn des 20. Jahrhunderts war die Kryptographie insbesondere Teil der *Linguistik*, die zumeist von einigen wenigen händisch durchgeführt wurde. In der Praxis basierten beispiels-

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

weise die Caesar-Verschlüsselung und die Vigenère-Chiffre auf einem natürlichsprachlichen Alphabet.

Mit veränderten Kommunikationsformen wie der Telegraphie und später dem Internet musste Kryptographie aber nicht nur sicher und vertraulich sein, sondern eben auch praktikabel und performant: Die Mathematik begann, die Linguistik als Disziplin der Kryptographie abzulösen. Nach Katz und Lindell verfolgt die Moderne Kryptographie im Unterschied zur Klassischen Kryptographie nämlich keinen Ad-hoc- oder informellen Ansatz mehr – sie hat nun vielmehr einen *rigorosen* Anspruch.[5] Dieser zeichnet sich aus durch eine zentrale Rolle von Definitionen, die Wichtigkeit von formalen und präzisen Annahmen sowie die Möglichkeit rigoroser Beweise von Sicherheit.[6] Es steht daher weniger die (oftmals durchaus systematische) Knobelei im Zentrum kryptographischer Ver- und Entschlüsselung, sondern die Rigorosität von mathematischer Beweisführung und Orientierung an logischen und probabilistischen Prinzipien.

Auch Diffie und Helmann schreiben 1976 in ihrem einflussreichen Artikel *New Directions in Cryptography*, dass erst die theoretischen Entwicklungen in der Informationstheorie und Informatik beweisbar sichere kryptographische Systeme ermöglicht hatten.[7] Erst dadurch hätte sich „this ancient art into a science"[8] gewandelt.[9] Und für Dooley basiert die Moderne Kryptologie auf den Arbeiten von drei Männern mit seltenem Talent, die die Kryptologie „from an esoteric, mystical, strictly linguistic

5 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv und 22.

6 Siehe ebd., S. xv–xvi und 16–23.

7 Siehe Whitfield Diffie und Martin E. Hellman. „New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), S. 644–654, hier S. 644.

8 Ebd., S. 644.

9 Im Folgenden soll deutlich werden, dass es tatsächlich Claude Shannon und die von ihm entwickelte Informationstheorie waren, die die späteren Kryptographinnen und Kryptographen beeinflusst hatten. Neben Diffie beeinflusste Shannon z. B. auch Horst Feistel, den Entwickler des einflussreichen symmetrischen Kryptosystems *Lucifer*; siehe Levy, *Crypto*, S. 44–45. Für Katz und Lindell ist die *Moderne* Kryptographie jene Kryptographie, die nach den 1980er-Jahren existiert; siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv. Abgeschlossen war der Paradigmenwechsel sicherlich erst in den 1980er-Jahren – begonnen hatte das neue Paradigma mit Blick auf Shannon allerdings bereits einige Jahrzehnte zuvor.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

realm into the world of mathematics and statistics“[10] bewegten: William F. Friedman, Lester S. Hill und Claude E. Shannon.[11]

Willian F. Friedman entwickelte mit seiner bekanntesten Schrift *The Index of Coincidence and Its Application to Cryptography* aus dem Jahr 1920 eine Möglichkeit, die Länge des Schlüssels bei einer polyalphabetischen Substitutionsmethode zu schätzen.[12] Zwar hatten bereits zuvor Babbage und Kasiski Methoden beschrieben, wie eine Vigenère-Chiffre gebrochen werden kann. Das Besondere an Friedmans Methode war allerdings, dass sie noch weitaus mehr auf den Grundlagen einer rigorosen Statistik fußte. Um es mit den Worten Kahns auszudrücken: „Friedman led cryptology out of this lonely wilderness and into the broad rich domain of statistics. He connected cryptology to mathematics.“[13]

Lester S. Hill verband wenige Jahre später Kryptographie und Algebra mit seinem Artikel *Cryptography in an Algebraic Alphabet*.[14] Diese Publikation war die erste einer solchen Art, die die abstrakte Algebra mit Kryptographie verknüpfte.[15] Dabei entwickelte er ein neues System polygraphischer Ver- und Entschlüsselung – später als *Hill Cipher* bezeichnet –, das auf invertierbaren quadratischen Matrizen als Schlüsselelement basiert.[16] Der praktische Nutzen dieser Methode war zwar eher gering, allerdings verstärkte Hill den neuen Einfluss der Mathematik auf die Kryptographie.[17]

Die größte Bedeutung für die Moderne Kryptographie dürfte aber zweifelsfrei jener schüchterne, aber doch vielseitig interessierte US-Ame-

10 Dooley, *History of Cryptography and Cryptanalysis*, S. 167.

11 Siehe ebd., S. 167.

12 Siehe Bauer, *Secret History*, S. 66–75, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 124. Siehe im Original William F. Friedman. *The Index of Coincidence and Its Application to Cryptography*. Riverbank Publications 22. Paris: L. Fournier, 1922.

13 Kahn, *The Codebreakers*, S. 383–384; auch zitiert in Dooley, *History of Cryptography and Cryptanalysis*, S. 125.

14 Siehe Lester S. Hill. „Cryptography in an Algebraic Alphabet“. In: *The American Mathematical Monthly* 36.6 (1929), S. 306–312. Zur Einführung Kahn, *The Codebreakers*, S. 404–410. Gewöhnlicherweise wird die sogenannte Matrixverschlüsselung Hill zugeschrieben. Tatsächlich allerdings war ihm aus historischer Sicht Levine in weiten Teilen zuvorgekommen. Siehe zu den Hintergründen Bauer, *Secret History*, S. 199–201.

15 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 167.

16 Siehe ebd., S. 167.

17 Siehe ausführlicher Kahn, *The Codebreakers*, S. 408–410.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

rikaner gehabt haben: Claude Elwood Shannon.[18] Zunächst begründete Shannon mit der Arbeit *A Mathematical Theory of Communication* im Jahr 1948 die Informationstheorie.[19] Ein Jahr später veröffentlichte er sein zweites wichtiges Werk: *Communication Theory of Secrecy Systems*.[20] Dabei formulierte er die formalen und sprachlichen Grundlagen für die heutige Kryptographie. Zahlreiche Begriffe, die bis heute standardmäßig die Sprache der Modernen Kryptographie prägen, wurden durch Shannon definiert.[21] Für Dooley vollendete Shannon daher, was Friedman begonnen und Hill fortgeführt hatte.[22]

Shannons theoretische Brillanz lässt sich beispielhaft an seiner Analyse des *One-Time-Pad* (OTP) zeigen, das bereits einige Jahrzehnte zuvor entwickelt worden war.[23] Das OTP funktioniert wie folgt: Wenn wir einen Klartext (in Bits) in einen verschlüsselten Text (in Bits) chiffrieren wollen, benötigen wir einen zufälligen Schlüssel (in Bits).[24] Dieser muss die gleiche Länge haben wie die zu verschlüsselnde Nachricht. Dann wird eine XOR-Operation mit dem ersten Bit des Klartextes und dem ersten Bit des Schlüssels durchgeführt, anschließend für das zweite Bit, das dritte Bit usw. Das Ergebnis dieser Operationen ist schließlich der verschlüs-

18 Interessiert war er beispielsweise an Schach, Jazz oder Science-Fiction, wobei diese Hobbys wohl durchaus oft wechseln konnten. Siehe ebd., S. 744; teilweise auch genannt in Levy, *Crypto*, S. 17–18, der hier allerdings keine direkte Quellenangabe aufführt. Zur kurzen Biographie von Shannon siehe Ioan James. „Obituary: Claude Elwood Shannon 1916–2001". In: *Bulletin of the London Mathematical Society* 46.2 (2014), S. 435–440; umfassender auch Bauer, *Secret History*, S. 327–343.

19 Siehe Claude E. Shannon. „A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (1948), S. 379–423.

20 Siehe Claude E. Shannon. „Communication Theory of Secrecy Systems". In: *The Bell System Technical Journal* 28.4 (1949), S. 656–715.

21 Beispiele wären *diffusion*, *confusion* oder *redundancy*. Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 168.

22 Siehe ebd., S. 168.

23 Eine Einführung zum OTP findet sich etwa bei Gathen, *CryptoSchool*, S. 375–377, sowie im historischen Kontext bei Bauer, *Secret History*, S. 92–96. Gewöhnlich wird Gilbert S. Vernam Anerkennung für diese Entdeckung während des Ersten Weltkrieges gezollt. Tatsächlich allerdings hatte der Bankier Frank Miller ein solches System bereits 35 Jahre zuvor beschrieben, wie Bellovin zeigen konnte. Siehe dazu Bellovin, „Frank Miller". Nach Bellovin ist es allerdings unklar, wem Anerkennung „with *effectively* inventing the one-time pad" zugesprochen werden sollte; ebd., S. 204, kursiv im Original. Bauer berichtet über die Hintergründe dieses Artikels; siehe Bauer, *Secret History*, S. 102–103.

24 Siehe dazu und zur folgenden Beschreibung beispielsweise Gathen, *CryptoSchool*, S. 375–377.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

selte Text. Der Schlüssel wird, da es sich um ein symmetrisches Protokoll handelt, sowohl zur Ver- als auch zur Entschlüsselung verwendet.

Das Besondere an diesem Algorithmus ist nun, dass Shannon beweisen konnte, dass das One-Time-Pad tatsächlich *perfect secrecy* ermöglicht.[25] Vereinfacht ausgedrückt meint dies, dass eine Kenntnis des verschlüsselten Textes *keine* Information über den Klartext liefert. Wenn böswillige Angreifende den verschlüsselten Text erhalten, gibt es für sie ohne den Schlüssel keine Möglichkeit, an Informationen des Klartextes zu gelangen, denn der verschlüsselte Text enthält schlicht keine Information über den Klartext. Für das OTP gilt daher auch die Eigenschaft, dass ein böswilliger Akteur oder eine böswillige Akteurin auch mit unbegrenzter Rechenkapazität die Nachricht nicht entschlüsseln könnte. Damit ist das OTP also *information-theoretic secure*. Sind kryptographische Verfahren hingegen lediglich *computationally secure*, dann bedeutet dies, dass bei jedem Angriff eine winzige Chance des Erfolgs besteht.

Warum aber wird dann das OTP nicht öfter eingesetzt, zum Beispiel in der täglichen Internetkommunikation? *Perfect secrecy* respektive *information-theoretic security* erreicht das OTP nur, wenn einige entscheidende Eigenschaften erfüllt sind.[26] Erstens muss der Schlüssel des OTP wie bereits erwähnt so lang sein wie die Nachricht selbst. Zweitens muss er tatsächlich *zufällig* sein. Und drittens darf er auch nur einmal verwendet werden.[27] Diese Bedingungen sind oftmals nur schwer zu erreichen oder zumindest wenig praktikabel. In der Praxis handelt es sich also stets um einen Trade-off von Schnelligkeit, Praktikabilität und Sicherheit. Wenn gewisse Informationen strikt geheim gehalten werden mussten, dann wurde das OTP historisch in sehr spezifischen Fällen allerdings bereits angewandt.[28]

---

25 Siehe dazu und zu diesem Absatz die Beschreibung bei Katz und Lindell, *Introduction to Modern Cryptography*, S. 29, 32–34 und 43; ebenso Dietmar Wätjen. *Kryptographie: Grundlagen, Algorithmen, Protokolle.* Wiesbaden: Springer Vieweg, 2018, S. 4–11.

26 Siehe dazu und zu den bekannten Eigenschaften beispielsweise Paul C. van Oorschot. *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*. Cham: Springer, 2021, S. 32–33.

27 Beispielsweise verwendete die Sowjetunion Schlüssel mehrmals, wodurch die USA Nachrichten im Rahmen des *Venona-Projekts* entschlüsseln konnten. Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 34.

28 Beispielsweise war die Kommunikationsverbindung des US-amerikanischen Präsidenten zum russischen Präsidenten (auch der *heiße Draht* genannt) über ein OTP verschlüsselt. Siehe Singh, *The Code Book*, S. 124. Allgemeiner zu den Einsatzmög-

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Die meisten Algorithmen, die in den folgenden Abschnitten besprochen werden und die in der Praxis üblich sind, erfüllen daher das Kriterium einer *perfect secrecy* nicht und sind lediglich *computationally secure*. Sie gelten trotzdem praktisch betrachtet als sicher, weil ein Angriff mit den heute verfügbaren Rechenressourcen mehrere Jahrmillionen oder mehr zur Entschlüsselung dauern würde. Prinzipiell allerdings gilt für diese Algorithmen, dass der verschlüsselte Text Informationen über den Klartext enthält. Dies ist allein schon dadurch der Fall, dass der Schlüssel bei diesen Algorithmen kürzer ist als der zu verschlüsselnde Text.[29]

Ungeachtet dieser Einschränkungen lässt sich mit Shannon der Beginn eines neuen Paradigmas der Kryptographie verorten – vor allem aufgrund der qualitativen Neuausrichtung an rigoroser Mathematik, Statistik und Informationstheorie, ohne die die Moderne Kryptographie nicht in der heutigen Form existieren würde. Shannons Werk wurde damit zur notwendigen Bedingung für die Moderne Kryptographie. Für Gesellschaft und Ethik ist aber auch wichtig: Wir sehen den Anfang eines grundlegenden Wechsels hinsichtlich der Autorität, die über die Kryptographie bestimmt. Seit 2500 Jahren war kryptographisches Denken – manchmal mehr, manchmal weniger – eine wenig transparente Arbeit, auf die Herrschende, Militärs sowie Diplomatinnen und Diplomaten autoritativen Einfluss üben konnten. Nach Shannon allerdings gelang es der Kryptographie, sich zu emanzipieren und in die Mitte des wissenschaftlichen Diskurses zu gelangen. Man könnte daher wohl auch sagen: Shannons Theorie vollzog für die Kryptographie die Transition vom Mythos zum Logos.

Nicht weniger bedeutsam war Shannons Theorie auch für den eher *klassischen* Bereich der Kryptographie, der allerdings uneingeschränkt bis heute Verwendung findet: die *symmetrische Kryptographie*. Das Paradigma Moderner Kryptographie machte in Kombination mit Digitalisierung und Kommerzialisierung auch davor keinen Halt und forderte gar das Selbstverständnis kryptographischer Forschung neu heraus. Retrospektiv lässt sich fragen: Wer würde es nach Shannon überhaupt wagen, Kryptographie nicht allein der Mathematik zu überlassen?

---

lichkeiten auch Mariusz Borowski und Marek Leśniewicz. „Modern usage of 'old' one-time pad". In: *2012 Military Communications and Information Systems Conference. Gdansk, Poland*. 2012, S. 1–5; im historischen Kontext auch Bauer, *Secret History*, S. 94–96.

29 Siehe zu einem Beweis und einer kurzen Diskussion Katz und Lindell, *Introduction to Modern Cryptography*, S. 35.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

2.2 Der Data Encryption Standard (DES)

Die *National Security Agency* (NSA) ging aus der *Armed Forces Security Agency* (AFSA) hervor und wurde am 4. November 1952 durch eine Direktive des damaligen US-Präsidenten Harry S. Truman gegründet.[30] Zwei Missionsziele soll die Organisation verfolgen: „exploiting foreign communications, also known as Signals Intelligence (SIGINT), and protecting U.S. information systems, also called Information Assurance (IA)"[31]. Als Geheimdienstorganisation engagiert sich die NSA bis heute im Bereich der Überwachung, der Spionage und vor allem der Kryptographie.[32]

Insbesondere im Jahr 2013 rückte das Handeln der NSA auch in den internationalen öffentlichen Fokus, nachdem der US-amerikanische Whistleblower Edward Snowden Geheimdokumente veröffentlichen ließ.[33] Unter anderem ist dabei die systematische und umfassende Überwachung von US-Bürgerinnen und -Bürgern, ausländischen Personen, politischen Verbündeten und ganzen Onlinediensten dokumentiert.[34] Bereits fünfzig Jahre zuvor sah die NSA sich selbst, wie Steven Levy es nennt, als „the sole repository of cryptographic information in the country – not just that used by civilian government and all the armed forces, as the law dictated, but that used by the private sector as well"[35]. Mit Blick auf das vorherige Kapitel wird der Konflikt um Autorität und Mathematik deutlich: Die NSA „acted as if it actually owned mathematical truths"[36].

Sicherlich war die NSA zunächst tatsächlich lange Zeit alleiniger Hort für kryptographische Forschung. Der einstige Direktor der NSA, Bobby Inman, ging zum Beispiel davon aus, dass die NSA ein „monopoly on ta-

30 Siehe Kahn, *The Codebreakers*, S. 675; einführend im kryptographischen Kontext auch Bauer, *Secret History*, S. 345–378.

31 National Security Agency. *Transition 2001*. Dez. 2000. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3700340/National-Security-Agency-Transition-2001.pdf (besucht am 15.04.2024), S. 1.

32 Eine konzise Einführung im Kontext der Überwachung liefert hier Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. Aufl. Indianapolis: Wiley, 2020, S. 922–925.

33 Siehe Edward Snowden. *Permanent Record*. London: Pan Books, 2019.

34 Zum Whistleblowing und Edward Snowden siehe Kapitel 7; dazu und zum Hintergrund insbesondere Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books, 2014.

35 Levy, *Crypto*, S. 15.

36 Ebd., S. 13.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

lent“[37] gehabt habe. Die politische Macht der NSA bestand allerdings vor allem darin, Patentanfragen zu kontrollieren und jene Patente, die nicht in öffentliche Hände gelangen sollten, zu klassifizieren.[38] US-amerikanische Forschung zur Kryptographie war bis in die 1960er-Jahre also das, was sie historisch betrachtet meistens war: autoritativ kontrolliert, häufig einer bestimmten Organisation unterstellt – und die Forschungsleistungen sollten möglichst geheim bleiben.

Konnte eine solche Kryptographie dauerhaft erfolgversprechend sein? Gerade mit dem Beginn der Digitalisierung und einem globalen Internet? In einer Zeit, in der Kryptographie zudem nicht mehr nur eine militärische Angelegenheit war, sondern zunehmend auch eine ökonomisch-kommerzielle? Kerckhoffs hatte bereits im vorherigen Jahrhundert beschrieben, dass eine Veröffentlichung des kryptographischen Systems die Sicherheit des Systems nicht kompromittieren darf.[39] Heute auch als *Kerckhoffs' Prinzip* bezeichnet, meint dies, dass die Sicherheit des Systems lediglich auf der Geheimhaltung des Schlüssels beruhen darf. Jede Geheimdienstorganisation, die das Wissen, die Algorithmen, die Verfahren und die Anwendungen von Kryptographie unter Verschluss halten will, widerspricht daher diesem Prinzip.

Daher mag es wenig überraschend sein, dass diese menschengemachte Autorität über kryptographische Forschung und Nutzung in den kommenden Jahren sukzessive auf die Probe gestellt werden sollte. Kapitel 3 und Kapitel 4 werden näher auf die Zusammenhänge von Gesellschaft, Wissenschaft und Regulierung eingehen, bei denen letztlich auch ethische Konflikte zutage treten.[40] Für diesen Teil der Arbeit ist allerdings wichtig: Deskriptiv betrachtet war aufgrund von rasch fortschreitender Entwicklung des Computers sowie einer Kommerzialisierung von Kommunikation auch eine Weiterentwicklung von kryptographischen Verfahren für zivile Behörden und Unternehmen erforderlich. Die Probleme für die NSA begannen damit, dass ein kommerzieller Standard gefun-

37 Zitiert in ebd., S. 115.

38 Siehe ebd., S. 15.

39 Siehe dazu die Ausführungen in Abschnitt 1.1.

40 Gemeint ist hierbei z. B. das Motiv einer *Privacy-vs.-Sicherheit*-Dichotomie, die oftmals als Begründung für eine Art *notwendiger* Beschränkung von Kryptographie angesehen wird. Im späteren Verlauf wird allerdings argumentiert, dass eine solche Dichotomie weder der Realität noch einer ethischen Notwendigkeit entspricht; siehe Abschnitt 6.2.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

den werden sollte, der eine solche Vertraulichkeit der Kommunikation gewährleisten sollte: der sogenannte *Data Encryption Standard* (DES).[41]

DES wurde als symmetrischer Verschlüsselungsalgorithmus am 15. Januar 1977 durch das *National Bureau of Standards* (NBS), den Vorgänger des heutigen *National Institute of Standards and Technology* (NIST), als *Federal Information Processing Standard 46* (FIPS 46) herausgegeben.[42] Dabei basiert der Algorithmus auf dem Verschlüsselungssystem *Lucifer*, das in den 1970er-Jahren durch den Kryptologen Horst Feistel bei IBM entwickelt worden war.[43] Auch bei Feistels Entwicklung wird deutlich, welchen Einfluss Claude Shannons Werk auf die Moderne Kryptographie hatte. Auf die Frage, woher Feistel die Ideen für sein Verschlüsselungssystem nahm, antwortete er: „The Shannon paper reveals it all."[44]

Lucifer war bereits auf dem US-amerikanischen Markt vertrieben worden, in einer geschwächten Version sogar weltweit.[45] Wie Lucifer ist DES eine sogenannte *Block Cipher*.[46] Dabei wird der Klartext in Blöcke unterteilt, die jeweils einzeln verschlüsselt werden. Auch die Entschlüsselung wird blockweise durchgeführt.[47] Entsprechend der fortschreitenden Digitalisierung nutzt DES auch kein natürlichsprachiges Alphabet mehr, sondern operiert nun auf Bits – genauer gesagt auf 64-Bit-Blöcken. Zur Verschlüsselung wird ein 56-Bit-Schlüssel verwendet, der insgesamt 16 Mal (in sogenannten *Runden*) auf den 64-Bit-Block angewandt wird. Dabei wird, ähnlich wie bei Shannon beschrieben, ein Netzwerk aus Substitution und Permutation verwendet. Wenn nun aber Shannons Theorie umfassend berücksichtigt wurde, wie konnte Lucifer beziehungsweise DES eine Kontroverse zur Sicherheit des Systems und zum Handeln der NSA auslösen?

41 Siehe zur historischen Einführung insbesondere Bauer, *Secret History*, S. 379–411.

42 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 169, allgemeiner auch S. 169–175; umfassender zur Geschichte auch Jarvis, *Crypto Wars*, S. 78–104.

43 Siehe ebd., S. 77–78 und 81.

44 Zitiert in Levy, *Crypto*, S. 45, siehe auch ebd., S. 44.

45 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 169.

46 Siehe dazu und zur folgenden Beschreibung von DES Katz und Lindell, *Introduction to Modern Cryptography*, S. 213–216. Siehe auch Dooley, *History of Cryptography and Cryptanalysis*, S. 169–173.

47 Die andere Art symmetrischer Verschlüsselung ist die *Stream Cipher*, bei der Ver- und Entschlüsselung kontinuierlich erfolgt und die an dieser Stelle nur der Vollständigkeit wegen genannt sein soll. Siehe weiterführend Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 20–21.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Im Fokus stand dabei zum einen die als zu kurz empfundene Schlüssellänge von nur 56 Bits, zumal Lucifer einen 128-Bit-Schlüssel verwendet hatte.[48] Um die Bedeutung der Schlüssellänge zu verstehen, hilft folgende Einordnung: Die Anzahl möglicher Schlüssel verdoppelt sich mit jedem weiteren Bit. Für einen 56 Bit langen Schlüssel gibt es insgesamt 2^{56} Möglichkeiten. Ein 128-Bit-Schlüssel allerdings lässt 2^{128} Möglichkeiten zu, also $2^{56} \cdot 2^{72}$. Schon damals gab es daher Stimmen, die den DES-Schlüssel als zu kurz empfanden.[49] Beispielsweise beschreibt Whitfield Diffie die Schlüssellänge bereits im Jahr 1975 als „at best barely adequate“[50]. Warum aber kam es trotzdem zu einem 56-Bit-Schlüssel? Eine mögliche Theorie war, dass die NSA auf IBM und das NBS eingewirkt hatte, da sie 56-Bit-Schlüssel brechen konnte.[51] Laut Dooley konnte dies allerdings nicht bewiesen werden.[52] Einige innerhalb von IBM sowie Forschende wie Diffie und Hellman sahen jedoch bereits damals eine Beeinflussung durch die NSA.[53] Später wurde bestätigt, dass IBM tatsächlich von der NSA überzeugt worden war, dass eine solche Schlüssellänge ausreichend sei.[54] Ob die Verkürzung der Schlüssellänge allerdings aus opportunistischen Gründen empfohlen wurde oder aber aus Performance- und Speichergründen, kann nicht mit abschließender Sicherheit festgestellt werden.

Die andere Kritik am Design von DES betraf die sogenannten *Substitutionsboxen*, auch *S-Boxen* genannt.[55] Die Analyse und die Prinzipien des Designs waren nicht veröffentlicht worden, und es wurde spekuliert, ob

48 Siehe Jarvis, *Crypto Wars*, S. 81–84; einführend auch Bauer, *Secret History*, S. 390–393.

49 Siehe Jarvis, *Crypto Wars*, S. 83–84, sowie Levy, *Crypto*, S. 37–39.

50 Whitfield Diffie. *Preliminary Remarks on the National Bureau of Standars Proposal Standard Encryption Algorithm for Data Protection*. Mai 1975. URL: https://stacks.stanford.edu/file/druid:wg115cn5068/1975%200522%20ltr%20to%20NBS.pdf (besucht am 15.04.2024), S. 3; auch zitiert in Jarvis, *Crypto Wars*, S. 84.

51 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 174.

52 Siehe ebd., S. 174.

53 Siehe Levy, *Crypto*, S. 59.

54 Siehe United States Senate. *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*. Staff Report of the Senate Selected Committee on Intelligence. Washington: U.S. Government Printing Office, Apr. 1978. URL: https://www.intelligence.senate.gov/sites/default/files/publications/95nsa.pdf (besucht am 15.04.2024), S. 4; sowie Levy, *Crypto*, S. 63. Gleichzeitig stellt der Report fest, die NSA habe zertifiziert, dass DES nach ihrem besten Wissen frei von statistischen und mathematischen Schwächen sei.

55 Siehe einführend Bauer, *Secret History*, S. 393–395.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

sich die NSA dadurch eine Hintertür (eine sog. *Backdoor*) für einen möglichen Zugriff auf die Kommunikation offen gelassen hatte.[56] Später jedoch wurden die tatsächlichen Gründe bekannt, warum die NSA Interesse an jener Geheimhaltung gehabt hatte: Die S-Boxen von DES verhindern eine bestimmte Art der Kryptoanalyse, die sogenannte *Differentielle Kryptoanalyse*.[57] Zum Zeitpunkt der Entwicklung von DES war die Differentielle Kryptoanalyse allerdings *nur* der NSA bzw. IBM bekannt. Dieses Wissen um eine neue Angriffsmethode wollte die Geheimdienstorganisation nicht mit den Überlegungen des Designs von DES veröffentlichen; gleichzeitig sollte DES gegen diese Differentielle Kryptoanalyse sicher sein – und daher entschied sich die NSA zur Geheimhaltung.[58] Es scheint plausibel, dass es sich tatsächlich nicht um eine Backdoor gehandelt hatte.

Egal, ob das Wirken der NSA nun rückblickend positiv, nachvollziehbar oder kritisch betrachtet wird: In jeglicher Hinsicht zeigt die Causa um DES auf, dass sich die Kryptographie im Umbruch befand. Eine Geheimhaltung von Designentscheidungen wurde nicht mehr ohne Weiteres von der wissenschaftlichen Forschung oder der Öffentlichkeit hingenommen. Die Intransparenz um die S-Boxen verringerte das Vertrauen in die Institution, und die Frage nach der Schlüssellänge war allenfalls kommunikativ undurchsichtig. Es handelte sich bei DES daher womöglich um den letzten größeren und gleichzeitig einigermaßen erfolgreichen Versuch der NSA, auf eine weit verbreitete Standardisierung von Kryptographie Einfluss zu nehmen. Für Levy steht fest: „DES was the NSA's first lesson that the new age of computer security was going to complicate its life considerably – perhaps even to the point of shaking the entire institution."[59]

An DES wird aber auch deutlich, dass die Zukunft der Standardisierung nicht mehr nur militärisch oder geheimdienstlich ausgerichtet war, sondern in zunehmendem Maße zivil und kommerziell.[60] So kam es, dass bereits 25 Jahre später und nach einigen prominenten DES-Entschlüsselungen kein Zweifel mehr daran bestand, dass DES durch einen Nachfol-

56 Siehe Jarvis, *Crypto Wars*, S. 83.

57 Siehe dazu und zum Folgenden Don Coppersmith. „The Data Encryption Standard (DES) and its strength against attacks". In: *IBM Journal of Research and Development* 38.3 (1994), S. 243–250.

58 Siehe Levy, *Crypto*, S. 55–56.

59 Ebd., S. 65.

60 Beispielhaft wird dies daran deutlich, dass die kommerziellen Interessen von IBM denen der NSA teilweise widersprachen, insbesondere was die Exportbeschränkungen betraf. Siehe Jarvis, *Crypto Wars*, S. 82–83.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

ger abgelöst werden musste.[61] Dieses Mal allerdings sollte es nicht mehr die NSA sein, die weitreichend bei der Standardisierung mitwirkte, sondern allein das *National Institute of Standards and Technology* (NIST) – kein Geheimdienst also, sondern eine zivile US-Bundesbehörde.[62] Die Standardisierung der kryptographischen Forschung emanzipierte sich vom Einfluss des Geheimdienstes.

Der Ausschreibungsprozess für diesen neuen kryptographischen Standard verdeutlicht ein solches neuartiges Selbstverständnis der Modernen Kryptographie: Die Prinzipien und Überlegungen des Designs mussten vollständig veröffentlicht werden und die Schlüssellänge musste mindestens 128 Bits betragen.[63] Hinzu kam, dass zahlreiche Gruppen nicht aus den USA stammten, womit auch das *globale* Element der Modernen Kryptographie ans Tageslicht trat.[64] Schließlich wurde zum neuen Jahrtausend der von belgischen Wissenschaftlern entwickelte Algorithmus *Rijndael* als *Advanced Encryption Standard* (AES) auserkoren.[65]

Während DES noch mit stark technischen Methoden und Begriffen beschrieben worden war, erfolgte dies bei AES primär in mathematischen Formeln und Erklärungen.[66] Kryptographie steht seither auf dem Fundament der Mathematik. Allerspätestens mit AES war also der Paradigmenwechsel, zumindest im Bereich der symmetrischen Verschlüsselung, abgeschlossen. Die Bedeutung für militärische Akteure blieb zwar vorhanden, allerdings kam nun eben auch immer mehr die Bedeutung für kommerzielle und zivile Zwecke hinzu. Die autoritative Beeinflussung der Standardisierung musste daher reduziert werden.[67] Dass dies notwendig

61 Siehe zur Einführung in unterschiedliche Attacken auf DES Diffie und Landau, *Privacy on the Line*, S. 28–29. Siehe außerdem zum Wirken der Cypherpunks Jarvis, *Crypto Wars*, S. 92–99.

62 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 175; außerdem einführend Diffie und Landau, *Privacy on the Line*, S. 249–251.

63 Siehe Levy, *Crypto*, S. 310. In der Praxis werden heute auch Schlüssel zur symmetrischen Verschlüsselung mit einer Länge von 256 Bit eingesetzt, die entsprechend 2^{256} verschiedene Schlüssel ermöglichen. Erfolgreiche Brute-Force-Attacken werden dadurch in der Praxis verhindert.

64 Siehe ebd., S. 310. Zumal es von den US-amerikanischen Teams lediglich eines gab, das nicht auch aus ausländischen Forschenden bestand; siehe Diffie und Landau, *Privacy on the Line*, S. 249.

65 Siehe ebd., S. 249–251.

66 Siehe ebd., S. 250.

67 Deutlich wird dies auch an späteren Ausschreibungsprozessen zur Standardisierung von Kryptographie, etwa bei dem Prozess zur Standardisierung von Post-Quanten-Kryptographie. Siehe Abschnitt 2.5.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

und sinnvoll war, zeigt der Erfolg von AES: Auch zwanzig Jahre nach der Standardisierung ist keine Attacke bekannt, die AES hätte brechen können.

2.3 *Diffie-Hellman und RSA*

Mit AES konnte also ein symmetrisches Verschlüsselungsprotokoll entwickelt werden, das es zwei Parteien ermöglicht, durch einen gemeinsamen Schlüssel auch im digitalen Zeitalter sicher und vertraulich zu kommunizieren. Eine Problematik allerdings galt es noch zu lösen: Wie kann der *gemeinsame* Schlüssel von einem Kommunikationspartner zum anderen gelangen?[68] Wenn der Schlüssel über das Internet übertragen wird, müsste man davon ausgehen, dass er abgefangen werden kann. Böswillige Angreifende könnten damit die gesamte mit dem betreffenden Schlüssel verschlüsselte Kommunikation entschlüsseln. Man müsste somit diesen Schlüssel über einen zweiten, sicheren Kanal übertragen – allerdings ist dies im Internet wenig praktikabel. Alternativ könnte man sogenannte *Key Distribution Centers* oder *Trusted Third Parties* (TTP) nutzen, die jedoch in einem solch interdependenten Netzwerk unzählige Schlüssel zu verwalten hätten.[69]

Dieses Problem bezieht sich also auf die *Key Distribution* und den *Key Exchange*.[70] Die Herausforderung der Verwaltung von Schlüssels wird daher auch als *Key Management Problem* bezeichnet.[71] Seit Beginn der symmetrischen Verschlüsselung – von der Caesar-Chiffre über die Vigenère-Chiffre bis hin zu Enigma – waren diese Probleme weitgehend ungelöst.[72] Intuitiv betrachtet erscheint diese Situation womöglich auch

68 Siehe dazu und zum Folgenden Katz und Lindell, *Introduction to Modern Cryptography*, S. 359–360.

69 Siehe einführend zu möglichen Lösungen mithilfe von symmetrischen Verfahren Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 36–37. Siehe zu *Key Distribution Centers* Katz und Lindell, *Introduction to Modern Cryptography*, S. 361–363. Es wäre etwa aus ethischer Perspektive zu fragen, wer die Verantwortung für diese zentrale Instanz übernehmen sollte und wie sie kontrolliert werden könnte.

70 Siehe ebd., S. 359–360; außerdem Dooley, *History of Cryptography and Cryptanalysis*, S. 185–186.

71 Siehe Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 36.

72 Ausgenommen sind die oben genannten Alternativen, die jedoch wenig praktikabel sind.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

ausweglos, denn irgendein Schlüssel *muss* ja übertragen werden – zumal seit Kerckhoffs feststeht, dass die Sicherheit des Systems ja gerade in der Geheimhaltung der Schlüssel liegen muss. Auch die US-amerikanischen Kryptographen Whitfield Diffie und Martin Hellman machten sich Gedanken über diese Fragen und Probleme.

In den 1970er-Jahren gelang ihnen schließlich die vielleicht bislang größte Revolution innerhalb der Kryptographie.[73] Ihre entscheidende Idee dabei war, mathematische Asymmetrien und eine sogenannte *Trapdoor-Einwegfunktion* (engl. *trapdoor one-way function*) im Bereich der Kryptographie zu nutzen.[74] Eine solche Trapdoor-Einwegfunktion basiert auf einem mathematischen Problem, im Fall von Diffie und Hellman auf dem *Problem des Diskreten Logarithmus*.[75] In einfachen Worten ausgedrückt kann eine Einwegfunktion in die eine Richtung *effizient* berechnet werden, in die andere Richtung allerdings nicht.[76] Mit der Trapdoor (dt. *Falltüre*) gibt es zusätzlich eine geheime Information, mit der die Einwegfunktion doch effizient umgekehrt werden kann.[77] Diffie und Hellman waren nun historisch die ersten, die eine Methode publiziert hatten, die dieses Wissen auf die Kryptographie anwendet.[78] Ihren Artikel *New Directions in Cryptography* leiteten sie 1976 daher auch mit einigem paradigmatischem Pathos ein: „We stand today on the brink of a revolution in cryptography."[79]

Was aber veränderte dieser Schlüsselaustausch ganz *prinzipiell*? Das Entscheidende ist, dass sich mit diesem Algorithmus zwei Parteien auch über einen unsicheren Kanal auf einen gemeinsamen Schlüssel einigen können. Dies gelingt also auch für den Fall, in dem eine böswillige Partei

73 Siehe einführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 363–370, und Gathen, *CryptoSchool*, S. 42–48.

74 Siehe Diffie und Hellman, „New Directions in Cryptography", insbesondere S. 650. Siehe auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 364, zu Einwegfunktionen zudem S. 332; sowie Beutelspacher, *Geheimsprachen und Kryptographie*, S. 52.

75 Siehe einführend Anderson, *Security Engineering*, S. 188–193.

76 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 332.

77 Siehe Beutelspacher, *Geheimsprachen und Kryptographie*, S. 52.

78 Historisch wurden bereits wenige Jahre zuvor die Methoden am *Government Communications Headquarters* (GCHQ) entwickelt, jedoch nicht veröffentlicht; siehe dazu ausführlicher weiter unten. Außerdem wirkte auch Ralph Merkle in der Gruppe von Diffie und Hellman mit; siehe Singh, *The Code Book*, S. 256 und 270–272.

79 Diffie und Hellman, „New Directions in Cryptography", S. 644.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

den Kanal passiv abhört.[80] Man benötigte damit keine zentrale Instanz mehr, die sich um das Management und die Verwaltung aller Schlüssel hätte kümmern müssen. Nun konnten zwei Parteien, zwei Individuen, vertraulich kommunizieren, ohne sich auf eine dritte Partei zu verlassen. Dieses revolutionäre Verfahren wird heute als *Diffie-Hellman-Schlüsselaustausch* (DH-Schlüsselaustausch) bezeichnet.

Das Key-Exchange-Problem schien damit zunächst gelöst.[81] Tatsächlich kann aber eine solche Kryptographie, die auch als *asymmetrische Kryptographie* oder *Public-Key-Kryptographie* bezeichnet wird, noch mehr erreichen: zum einen ein asymmetrisches System zur Ver- und Entschlüsselung;[82] zum anderen aber auch die Gewährleistung von Authentizität.[83] Für beides legten Diffie und Hellman die grundsätzlichen Ideen dar. Eine Public-Key-Kryptographie basiert darauf, dass $k_e \neq k_d$ ist.[84] Das bedeutet, der Schlüssel zur Verschlüsselung ist nicht identisch mit dem Schlüssel der Entschlüsselung. Entscheidend ist hierbei, dass es nicht möglich ist, k_d durch die Kenntnis von k_e zu ermitteln. Der Schlüssel k_d muss immer geheim bleiben, weshalb er auch *private key* genannt wird. k_e allerdings darf (und soll sogar) veröffentlicht werden – schließlich spielt es keine Rolle, ob auch andere Parteien Nachrichten mit diesem Schlüssel verschlüsseln können. Deswegen wird er auch als *public key* bezeichnet.[85]

80 Aktive Angriffe und sogenannte *man-in-the-middle attacks* sind jedoch möglich. Siehe weiterführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 369–370.

81 Wie Peter Shor knapp zwanzig Jahre später zeigen konnte, gibt es einen Algorithmus, der den DH-Schlüsselaustausch (und einige andere asymmetrische Verfahren) bricht. Dieser benötigt allerdings einen Quantencomputer. Siehe Peter W. Shor. „Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *IEEE Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, S. 124–134; dazu auch Abschnitt 2.5.

82 Siehe Diffie und Hellman, „New Directions in Cryptography", S. 644. *Asymmetrisch* deswegen, weil der Schlüssel zur Verschlüsselung ein anderer ist als der zur Entschlüsselung.

83 Siehe ebd., S. 644–645. Siehe auch Dooley, *History of Cryptography and Cryptanalysis*, S. 189–191.

84 Der Schlüssel k_e dient zur Verschlüsselung, der Schlüssel k_d zur Entschlüsselung. Siehe zur Public-Key-Kryptographie im Folgenden einführend ebd., S. 189–191.

85 Der DH-Schlüsselaustausch wird also zur Einigung eines gemeinsamen Schlüssels verwendet, die Public-Key-Kryptographie zur Ver- und Entschlüsselung. Die sprachliche Unterscheidung ist allerdings unscharf.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Widerspricht dies nun Kerckhoffs' Prinzip, nach dem die Sicherheit des Systems nur darauf basiert, dass der Schlüssel geheim gehalten wird?[86] Tatsächlich lässt sich diese Frage nicht beantworten, denn Kerckhoffs' Ideen waren schließlich aus der Perspektive der symmetrischen Kryptographie entstanden. Eine Kryptographie, bei der *zwei* Schlüssel existieren, war für Kerckhoffs sicher nicht vorstellbar. Diese radikale Idee war in dem Sinne wohl auch eine Art „cryptographic heresy"[87]. Die asymmetrische Kryptographie eröffnet hier ein vollkommen neues Feld, das – wie für ein neues Paradigma üblich – auch nicht mit den Werkzeugen, Methoden und Hilfsmitteln des alten Paradigmas gedacht werden kann.

Das Problem der Authentizität war ebenfalls Teil dieses neuen Paradigmas. Über Jahrtausende war Kryptographie eine Frage vertraulicher Kommunikation. Nur jene Parteien können den Inhalt der Nachricht entschlüsseln, die es auch *sollen*. Mit dem Ziel der Authentizität dagegen soll nachgewiesen werden, dass die Nachricht wirklich von der Partei stammt, die der Absender zu sein vorgibt. Auch wenn Diffie und Hellman sowohl die Frage der Authentizität als auch die grundsätzlichen Ideen zur Public-Key-Kryptographie aufzeigten, lieferten sie dazu keinen konkreten Algorithmus. Dies gelang kurze Zeit später allerdings einer anderen Gruppe von Forschern: Ron L. Rivest, Adi Shamir und Leonard Adleman.[88]

Ihren Algorithmus, den sie in *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* darlegten, sahen sie als direkte Antwort auf den Artikel von Diffie und Hellman. Letztere hätten zwar, wie oben bereits erläutert, das Konzept vorgestellt, jedoch keine praktische Implementierung.[89] Die grundlegende Notwendigkeit für solch ein System sahen sie im Aufkommen der E-Mail, die ähnliche Eigenschaften wie Papierpost erfüllen muss: Einerseits müssen Nachrichten *vertraulich* sein, andererseits müssen sie *signiert* werden können.[90] Ähnlich wie der

86 Horst Feistel, Entwickler von *Lucifer*, erklärte in einem eiligen Moment, dass ein öffentlicher Schlüssel Kerckhoffs' zweitem Grundsatz widersprechen würde. Siehe Levy, *Crypto*, S. 75.

87 Jarvis, *Crypto Wars*, S. xvi.

88 Siehe Ron L. Rivest, Adi Shamir und Leonard Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2 (1978), S. 120–126.

89 Siehe ebd., S. 120.

90 Siehe ebd., S. 120. Diffie und Hellman nennen Ersteres *privacy problem* und Letzteres *authentication problem*. Siehe Whitfield Diffie und Martin E. Hellman. „Privacy and

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

DH-Schlüsselaustausch basiert auch der Algorithmus von Rivest, Shamir und Adleman, der gemäß den Initialen als *RSA* abgekürzt wird, auf einer Einwegfunktion.

Das mathematische Problem ist bei RSA jedoch das sogenannte *Faktorisierungsproblem*.[91] Um dies an einem einfachen Beispiel zu beschreiben: Ein klassischer Computer kann die Berechnung $7 * 3 = 21$ effizient ausführen; für die Faktorisierung der zwei Primzahlen 7 und 3 ausgehend von der Zahl 21 ist jedoch ein proportional deutlich größerer Rechen- und Zeitaufwand notwendig.[92] Für den genauen Algorithmus sei auf die zahlreiche Standardliteratur verwiesen, schematisch funktioniert RSA jedoch folgendermaßen: Wenn Alice (Partei A) eine Nachricht an Bob (Partei B) schicken möchte, dann generiert Bob zunächst ein Schlüsselpaar, das aus einem *private key* k_d^{Bob} und einem *public key* k_e^{Bob} besteht. Der *public key* k_e^{Bob} wird daraufhin veröffentlicht, beispielsweise über ein Repository im Internet. Alice nutzt nun Bobs *public key* k_e^{Bob} und verschlüsselt damit ihre Nachricht. Die verschlüsselte Nachricht kann Alice anschließend an Bob senden. Dies kann auch über einen unsicheren Kanal geschehen, denn ausschließlich Bob kann nun die Nachricht mit seinem geheim gehaltenen *private key* k_d^{Bob} entschlüsseln.[93]

Mit diesem Verfahren kann auch das Authentizitäts-Problem gelöst werden.[94] Gehen wir davon aus, dass nun Bob eine signierte Nachricht an Alice senden möchte.[95] Dazu nutzt Bob seinen *private key* k_d^{Bob}, signiert damit die Nachricht und sendet sie anschließend an Alice. Alice kann nun mit Bobs *public key* k_e^{Bob} überprüfen, ob die Nachricht wirklich von Bob stammt, denn niemand anderes hätte die Nachricht mit Bobs *private key* k_d^{Bob} signieren können. Alice kann dann also sicher sein, dass die

Authentication: An Introduction to Cryptography". In: *Proceedings of the IEEE* 67.3 (1979), S. 397–427, hier S. 398.

91 Siehe Rivest, Shamir und Adleman, „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"; weiterführend auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 410–433; historisch Dooley, *History of Cryptography and Cryptanalysis*, S. 192–193.

92 In der Praxis sind die Zahlen sehr viel größer. Siehe zum Faktorisierungsproblem Anderson, *Security Engineering*, S. 185–188.

93 Vorausgesetzt ist hierbei natürlich, dass Bob seinen *private key* k_d^{Bob} auch wirklich geheim hält.

94 Siehe dazu und zu digitalen Signaturen umfassend Katz und Lindell, *Introduction to Modern Cryptography*, S. 439–486.

95 Zur Vereinfachung gehen wir davon aus, dass dies dieses Mal unverschlüsselt stattfinden soll.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Nachricht nicht von einer böswilligen Partei stammt.[96] Man spricht daher von *digitalen Signaturen*. Auch hier funktioniert dieses Verfahren nur aufgrund des mathematischen Faktorisierungsproblems sowie der Beziehung von *private key* k_d und *public key* k_e.[97]

Sowohl der DH-Schlüsselaustausch als auch RSA waren wahrliche Meilensteine der Kryptographiegeschichte – sowohl aus theoretischer als auch aus praktischer Perspektive.[98] Bis heute spüren wir tagtäglich und ubiquitär die Folgen dieser Entwicklung. Reg Whitaker bezeichnet die Public-Key-Kryptographie gar als „the end of the state's monopoly and the democratization of encryption"[99]. Und für Craig Jarvis war die Public-Key-Kryptographie zusammenfassend mehr eine Entdeckung als eine Erfindung:

> For it was a discovery, rather than an invention. Diffie und Hellman's public key cryptography was to computer science as Newton's theory of universal gravitation was to physics, as Pasteur's germ theory had been to medicine, and as Darwin's theory of evolution was to biology.[100]

Die asymmetrische Kryptographie kann damit zu Recht als ein Pfeiler des Paradigmenwechsels von der Klassischen Kryptographie hin zu einer Modernen Kryptographie gelten. Auch Naccache, Ryan und Quisquater kommen zu einer solchen Rezeption – denn das Revolutionäre ist ja gerade, dass die Fähigkeit zum *Verschlüsseln* nun nicht mehr gleichzeitig auch die Fähigkeit zum *Entschlüsseln* bedeuten muss:

> The discovery in the 1970s of public key cryptography revolutionized the subject and brought it out of the shadows. The realization that the ability to encrypt does

96 Wieder angenommen, nur Bob hat Zugriff auf seinen *private key*.

97 Siehe einführend auch Anderson, *Security Engineering*, S. 185–188.

98 Einer breiteren Öffentlichkeit bekannt wurde diese Art der Kryptographie bereits 1977 durch Martin Gardners Artikel in *Scientific American*; siehe Martin Gardner. „Mathematical Games: A new kind of cipher that would take millions of years to break". In: *Scientific American* (Aug. 1977), S. 120–124. Auch einige der späteren Cryptoaktivistinnen und -aktivisten sind gerade durch diesen Artikel auf die Bedeutung der asymmetrischen Kryptographie aufmerksam geworden. Siehe Thomas Rid. *Rise of the Machines: The Lost History of Cybernetics*. Melbourne und London: Scribe, 2016, S. 252–253 und 262.

99 Reg Whitaker. *The End of Privacy: How Total Surveillance Is Becoming Reality*. New York: The New Press, 1999, S. 108.

100 Jarvis, *Crypto Wars*, S. xvi.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

> not necessarily entail the ability to decrypt overturned (implicit) assumptions that had held sway for centuries. Arguably this insight is comparable in its impact on cryptography as that of Einstein's Theory of Relativity, with the realization that space is not absolute, on physics.[101]

Und obwohl Diffie und Hellman sowie Rivest, Shamir und Adleman am meisten Anerkennung für diese Entdeckungen erhalten, weiß man heute, dass diese grundsätzlichen Algorithmen bereits wenige Jahre zuvor auch auf der anderen Seite des Globus entdeckt wurden.[102] Am *Government Communications Headquarters* (GCHQ), dem UK-Pendant zur US-amerikanischen NSA, hatten zunächst James Ellis, dann Clifford Cocks und schließlich Malcolm Williamson solche Lösungen entwickelt. Trotzdem sind es nicht Ellis, Cocks und Williamson, nach denen die Public-Key-Kryptographie benannt wurde. Der Grund dafür ist simpel: Ihnen wurde verboten, darüber zu sprechen. Erst im Dezember 1997 durfte Cocks öffentlich zum ersten Mal davon berichten. Und Ellis, Cocks und Williamson erfuhren rückblickend Anerkennung für ihr Wirken als die eigentlich ersten Entdecker der Public-Key-Kryptographie.[103]

2.4 Kryptographie und Informationssicherheit

In der Klassischen Kryptographie war das Ziel der Kryptographie maßgeblich die Verschlüsselung von Kommunikation. Nachrichten sollten nur von denen entschlüsselt werden können, die dazu auch autorisiert sind. Im Paradigma der Modernen Kryptographie kommen nun weitere Ziele hinzu. So wird etwa die asymmetrische Kryptographie für die Verschlüsselung *und* für die Gewährleistung von Authentizität genutzt. Und auch die asymmetrische Kryptographie wird in der Praxis oft zusammen mit symmetrischen Verschlüsselungsverfahren und sogenannten Hash-Algorithmen verwendet, wodurch Vertraulichkeit und Integrität einer Nachricht sichergestellt werden soll. Mit all diesen Verfahren wer-

101 Naccache, Ryan und Quisquater, „Preface".

102 Siehe dazu und zu diesem Absatz Dooley, *History of Cryptography and Cryptanalysis*, S. 190–191; ausführlicher auch Levy, *Crypto*, S. 313–330, sowie Rid, *Rise of the Machines*, S. 248–250.

103 Siehe umfassender Singh, *The Code Book*, S. 279–292.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

den sogenannte *Schutzziele* der Informationssicherheit verfolgt.[104] Solche Schutzziele „sind Sicherheitsanforderungen, die an ein System gestellt werden und die durch die Sicherheitseigenschaften des Systems schlussendlich zu gewährleisten sind"[105]. Unterteilt werden diese Schutzziele meist in *Vertraulichkeit* (engl. *confidentiality*), *Integrität* (engl. *integrity*) und *Verfügbarkeit* (engl. *availability*), sodass sie im Englischen mit *CIA* abgekürzt werden.[106] Hinzu kommen weitere Schutzziele wie *Rechtsverbindlichkeit/Nicht-Abstreitbarkeit* (engl. *non-repudiation*) und *Zurechenbarkeit* (engl. *accountability*).[107] Für die Kryptographie ist insbesondere auch das Schutzziel der *Authentizität* (engl. *authenticity*) von Bedeutung.[108] Letzteres ist aus ethischer Sicht primär im Fall von Identifikation und Identifizierbarkeit relevant, wie Abschnitt 7.3 zeigen wird.

Wenn also Moderne Kryptographie heute mehr zum Ziel hat als nur vertrauliche Kommunikation, dann sollte auch eine *Ethik der Kryptographie* diese anderen Facetten und Anwendungen nicht außer Acht lassen.[109] Eine Systematisierung anhand von Schutzzielen hilft dabei einer ethischen Analyse, Zielkonflikte zu identifizieren und Rahmenbedingungen für eine ganzheitliche Informationssicherheit zu etablieren. Beispielsweise muss eine Bank sicherstellen, dass Transaktionen vertraulich und privat sind. Gleichzeitig muss sie sich aber auch auf die Authentizität der Nachrichten und der Nutzenden verlassen können, damit die Transaktion die intendierte Partei erreicht. Damit die Transaktion zudem

104 Über das Verhältnis der Kryptographie zu Schutzzielen siehe Yvo Desmedt. „What is the Future of Cryptography?" In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. 109–122.

105 Eckert, *IT-Sicherheit*, S. 2. Siehe zu den folgenden Schutzzielen auch Oorschot, *Computer Security and the Internet*, S. 2–3.

106 Siehe Eckert, *IT-Sicherheit*, S. 9–12; aus rechtlicher Perspektive auch Marcus Heinemann. *Grundrechtlicher Schutz informationstechnischer Systeme: Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Berlin: Duncker & Humblot, 2015, S. 73–75.

107 Siehe Eckert, *IT-Sicherheit*, S. 12–13, sowie Armin Lunkeit und Wolf Zimmer. *Security by Design: Security Engineering informationstechnischer Systeme*. Berlin und Heidelberg: Springer Vieweg, 2021, S. 89; aus rechtlicher Perspektive auch Heinemann, *Grundrechtlicher Schutz informationstechnischer Systeme*, S. 76–78.

108 Siehe Eckert, *IT-Sicherheit*, S. 9.

109 Siehe beispielsweise Konstantinos Limniotis. „Cryptography as the Means to Protect Fundamental Human Rights". In: *Cryptography* 5.4 (2021).

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

integer bleibt, darf der Betrag der Transaktion nicht verändert werden. All dies sind zunächst grundsätzliche Fragen der Informationssicherheit. Die Kryptographie allerdings ist das Werkzeug, mit dem diese Schutzziele der Informationssicherheit erreicht werden können. Im Folgenden soll auf die einzelnen Schutzziele eingegangen und deren Verhältnis zur Kryptographie bestimmt werden.

Vertraulichkeit

Mit dem Schutzziel der Vertraulichkeit ist beschrieben, dass nicht-öffentliche Informationen nur autorisierten Parteien zugänglich sein sollen.[110] Autorisierung meint hierbei, dass diese Partei Zugriffsrechte auf die betreffenden Informationen besitzt.[111] Dieses Schutzziel deckt sich also mit dem, was bereits die Klassische Kryptographie zum Ziel hatte: Nur jene Personen oder Systeme sollen die Möglichkeit haben, die Informationen unverschlüsselt zu lesen, die dazu auch autorisiert sind.[112] Systematisch unterschieden werden bei der Vertraulichkeit zwei Anwendungsebenen: einerseits eine *zeitliche* Ebene und andererseits eine *räumliche* Ebene.[113] *Zeitlich* meint, dass Informationen und Daten über einen gewissen Zeitraum zu schützen sind, etwa auf einer lokalen Festplatte oder bei ausgedruckten Dokumenten. Die *räumliche* Ebene bezieht sich dagegen auf die technologische Kommunikation. Wenn Alice in Paris mit Bob in Hongkong kommuniziert, dann möchten beide Parteien, dass keine dritte Partei von den Inhalten Kenntnis erlangen kann.[114]

110 Siehe einführend Oorschot, *Computer Security and the Internet*, S. 3. Für eine rechtliche Perspektive zur Vertraulichkeit siehe Heinemann, *Grundrechtlicher Schutz informationstechnischer Systeme*, insbesondere S. 74–75 und 79.

111 Siehe zu Autorisierung Eckert, *IT-Sicherheit*, S. 5. Zu unterscheiden ist hierbei die *Authentifizierung*, dazu weiter unten. Auf andere Art formuliert meint Autorisierung die Bindung einer Identität an eine Menge zulässiger Aktionen; siehe Lunkeit und Zimmer, *Security by Design*, S. 44.

112 Selbst Kahn definiert die Kryptographie noch wie folgt: „The methods of cryptography […] render [a message] unintelligible to outsiders by various transformations of the plaintext." Kahn, *The Codebreakers*, S. xv.

113 Siehe dazu und zum Folgenden Katz und Lindell, *Introduction to Modern Cryptography*, S. 5–6. Katz und Lindell beschreiben diese zwei Anwendungen im Rahmen einer, wie sie es nennen, *Private-Key-Kryptographie*, die allerdings deckungsgleich ist mit einer symmetrischen Kryptographie.

114 Eine weitere Frage wäre hier, ob bereits das Wissen, dass Alice mit Bob kommuniziert, unter das Schutzziel der Vertraulichkeit fallen sollte. Diese Differenzierung

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Die Maßnahmen zur Wahrung von Vertraulichkeit sind abhängig von der konkreten Nutzungssituation. In der brieflichen Kommunikation soll die Vertraulichkeit des Inhalts beispielsweise durch das Briefgeheimnis oder einen Briefumschlag gewahrt werden. Digitalisiert spielen kryptographische Systeme eine entscheidende Rolle.[115] Kryptographische Verfahren können beispielsweise im Kontext von Festplattenverschlüsselung Vertraulichkeit gewährleisten, wenn symmetrische Algorithmen wie AES verwendet werden.[116] Eine vertrauliche räumliche Kommunikation kann durch ein asymmetrisches Verfahren wie den DH-Schlüsselaustausch erreicht werden. Sobald beide Parteien einen gemeinsamen Schlüssel haben, kann dieser für eine symmetrische Verschlüsselung genutzt werden.[117]

Integrität

Mit dem Schutzziel der Integrität sollen Daten unverändert bleiben, außer wenn die Änderungen autorisiert sind.[118] Dazu werden zum einen Methodiken der Fehlererkennung und Fehlerbehebung genutzt, zum anderen auch Zugangskontrollen sowie kryptographische Prüfsummen.[119] Für Zugangskontrollen sind vor allem Rechte wie Schreib- und Leserechte festzulegen.[120] Kryptographische Prüfsummen (engl. *cryptographic checksums*) hingegen erlauben eine Erkennung von veränderten Daten *a posteriori*, wobei in der Praxis sogenannte Hashfunktionen verwendet werden.[121] Sowohl bösartige Angriffe als auch unbeabsichtigte Fälle von

zeigt den Unterschied von *Inhaltsdaten* und *Metadaten*, worauf an späterer Stelle noch eingegangen wird.

115 Darüber hinausgehend wären z. B. auch Möglichkeiten der Zugriffskontrolle zu nennen; siehe Oorschot, *Computer Security and the Internet*, S. 3.

116 Die Schlüssel dürfen dabei natürlich nur den autorisierten Personen zugänglich sein.

117 In der Praxis ist eine möglichst nachweisbare Gewährleistung einer kryptographischen Implementierung komplexer. So sind unter anderem Implementierungsdetails zu berücksichtigen, die beispielsweise *Seitenkanal-Angriffe* (engl. *side-channel attacks*) verhindern sollen. Desmedt fragt daher auch, inwieweit wir Implementierungen vertrauen können; siehe Desmedt, „What is the Future of Cryptography?", S. 113, zur Einführung S. 113–114.

118 Siehe einführend Oorschot, *Computer Security and the Internet*, S. 3.

119 Siehe ebd., S. 3.

120 Siehe Eckert, *IT-Sicherheit*, S. 9.

121 Siehe ebd., S. 9–10. Einführend zu Hashfunktionen auch Anderson, *Security Engineering*, S. 152–154, 157–161 und 181–185, und Bauer, *Secret History*, S. 498–504.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

beispielsweise Übertragungsfehlern sollen dadurch identifiziert und korrigiert werden können. In der brieflichen Kommunikation wird Integrität hingegen durch eine Versiegelung der Nachricht erreicht. Eine Veränderung der Nachricht kann also angenommen werden, wenn das Siegel gebrochen wurde.

Die Entwicklung der grundsätzlichen Prinzipien solcher Hashfunktionen reicht weit über das digitale Zeitalter zurück. So sahen sich in der Mitte des 19. Jahrhunderts Banken vor die Herausforderung gestellt, Authentizität und Integrität trotz telegraphischer Kommunikation zu wahren.[122] Dafür wurden *test codes* entwickelt, wodurch eine Veränderung der übermittelten Nachricht detektiert, gleichzeitig aber nichts über den Inhalt der Nachricht verraten wurde. Es handelte sich damals wie heute um die Idee einer *Einwegfunktion* (engl. *one-way function*).[123]

Auch wenn die Anwendungsidee von Prüfsummen und Hash-Algorithmen bereits historisch einige Zeit zurückliegt, lässt sich auch hier das Paradigma der Modernen Kryptographie erkennen: Hash-Algorithmen sind heute Teil der Mathematik und Informatik. Daher werden, ähnlich wie bei der symmetrischen Verschlüsselung, standardisierte Verfahren verwendet, die ein deutlich höheres Maß an Sicherheit gewährleisten können. Als Beispiel kann der *Secure Hash Algorithm 3* (SHA-3) genannt werden.[124]

Verfügbarkeit

Mit dem Schutzziel der Verfügbarkeit ist beschrieben, dass Informationen, Dienste und Ressourcen für autorisierte Zugriffe zugreifbar bleiben.[125] Bösartige Parteien, die gegen dieses Schutzziel handeln, führen sogenannte *Denial-of-Service*-(DoS-) bzw. *Distributed-Denial-of-Service*-(DDoS-)Angriffe durch.[126] Solche Angriffe sollen etwa einen Webserver durch eine massive

122 Siehe dazu und zur folgenden Historie Anderson, *Security Engineering*, S. 152–154.
123 Bereits 1678 war eine solche Einwegfunktion entwickelt worden; siehe ebd., S. 153.
124 Siehe einführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 235–236.
125 Siehe Oorschot, *Computer Security and the Internet*, S. 3. In komplexen Systemen kann eine Verzögerung bis zu einem gewissen Grad erwartbar sein. Wie Eckert daher erkennt, ist für das Schutzziel der Verfügbarkeit die Trennlinie von autorisierten und unautorisierten Aktionen ungenau; siehe Eckert, *IT-Sicherheit*, S. 12.
126 Siehe Oorschot, *Computer Security and the Internet*, S. 3.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Flut von Anfragen zur Abschaltung zwingen. Das Erreichen des Schutzziels der Verfügbarkeit kann aber auch durch sogenannte *Ransomware*-Attacken verhindert werden. Zusammengesetzt aus den Begriffen *ransom* (dt. *Lösegeld*) und *software* bezeichnet der Begriff Programme, die sich in den Computersystemen der Angegriffenen einnisten und diese verschlüsseln. Als kryptographische Verfahren werden oft RSA in Kombination mit AES genutzt.[127] Die Opfer werden im Anschluss mit einer Lösegeldforderung konfrontiert, um die Systeme wieder entschlüsseln zu können. Eine Garantie, dass eine Entschlüsselung anschließend auch tatsächlich stattfindet, haben die Angegriffenen jedoch nicht.

Einer breiten Öffentlichkeit bekannt wurde Ransomware durch den Wurm *WannaCry* im Jahr 2017.[128] So wurden etwa auch Krankenhäuser und Teile der kritischen Infrastruktur Opfer dieser Attacken.[129] Mit der Nachricht *Oops, your files have been encrypted!* wurden Nutzende aufgefordert, innerhalb von drei Tagen 300 US-Dollar in der Kryptowährung *Bitcoin* als Lösegeld zu bezahlen. Wer diese erste Forderung nicht erfüllte, dessen Lösegeldforderung wurde verdoppelt. Nach sieben Tagen sollten die verschlüsselten Dateien endgültig gelöscht werden. Betroffen waren hierbei innerhalb weniger Tage über 300.000 Nutzende weltweit.[130]

Das Verhältnis zur Kryptographie ist hier aber komplexer, als auf den ersten Eindruck angenommen werden könnte. Denn für all diese Angriffe können nicht allein die Kryptographie respektive die Möglichkeiten, die sich durch die Kryptographie ergeben, verantwortlich gemacht werden. Zum einen liegen die Ursachen für den Erfolg von Ransomware an anderer Stelle, zum Beispiel an fehlenden Sicherheitskopien, ungeschützten Netzwerken oder veralteter Software. Zum anderen kann die Kryptographie auch bei Ransomware Vertraulichkeit sicherstellen. Eine Drohung

127 Siehe Aaron Zimba und Mumbi Chishimba. „On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems". In: *European Journal for Security Research* 4.1 (2019), S. 3–31, hier S. 27.

128 Siehe Maria F. Prevezianou. „WannaCry as a Creeping Crisis". In: *Understanding the Creeping Crisis*. Hrsg. von Arjen Boin, Magnus Ekengren und Mark Rhinard. Cham: Palgrave Macmillan, 2021, S. 37–50. Siehe zur Ökonomie hinter Ransomware Zimba und Chishimba, „On the Economic Impact of Crypto-ransomware Attacks". Ein anderes Beispiel für Ransomware ist der sogenannte *Gpcode*, der sich ab 2006 verbreitete; siehe Eckert, *IT-Sicherheit*, S. 23–24.

129 Siehe dazu und zum Folgenden Prevezianou, „WannaCry as a Creeping Crisis", S. 38.

130 Siehe Zimba und Chishimba, „On the Economic Impact of Crypto-ransomware Attacks", S. 15.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

mit der Veröffentlichung von gestohlenen Daten läuft ins Leere, wenn die betreffenden Daten bereits zuvor sicher und vertraulich verschlüsselt worden sind.

Authentizität

Authentizität ist „die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist“[131]. Der Prozess der Überprüfung nennt sich Authentifikation.[132] In der brieflichen Kommunikation wird Authentizität etwa durch eine Unterschrift ermöglicht, die mit vorher signierten Unterlagen verglichen werden kann. In der digitalen Welt dagegen lässt sich das Schutzziel der Authentizität insbesondere mit *Public-Key Infrastructures* (PKI) lösen. Dabei werden digitale Signaturen genutzt, die die Nachrichten eindeutig einem Subjekt zuordnen. In der Praxis nutzt Alice ihren *private key* zur Signierung einer Nachricht. Bob kann anschließend die Signatur mit dem *public key* von Alice überprüfen. Im engeren Sinne ist die Authentizität von der *Identifizierung* zu unterscheiden. Die Identifizierung ermittelt eine Identität aus den verfügbaren Informationen, ohne dass zuvor eine ausdrückliche Identität beteuert worden ist.[133] Gleichwohl können in der Konsequenz Authentifizierung und Identifizierung zusammenhängen. Damit verbunden ist selbstverständlich auch die Frage nach der Rechtsverbindlichkeit und der Zurechenbarkeit.

Rechtsverbindlichkeit & Zurechenbarkeit

Die Schutzziele Rechtsverbindlichkeit und Zurechenbarkeit sind dann gegeben, wenn es unmöglich ist, im Nachhinein die Durchführung einer Aktion abzustreiten, und wenn damit eine Entität für eine vergangene

131 Eckert, *IT-Sicherheit*, S. 8.

132 Siehe ebd., S. 8. Nach Lunkeit und Zimmer wird im deutschen Sprachraum zwischen Authentifikation und Authentifizierung unterschieden; siehe Lunkeit und Zimmer, *Security by Design*, S. 44. Im Deutschen kommt zudem der Begriff *Authentisierung* hinzu. Eine ausführliche Analyse der deutschen Begrifflichkeiten würde an dieser Stelle zu weit gehen und ist nicht im Sinne der Arbeit. Zur Vereinfachung orientiert sich die Diskussion daher am englischen Begriff der *authentication*.

133 Siehe Oorschot, *Computer Security and the Internet*, S. 56.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Aktion verantwortlich gemacht werden kann.[134] In der Praxis wird dies neben digitalen Signaturen auch durch Logging oder Transaktionsbeweise erreicht.[135] Insbesondere in Handels- und Rechtssituationen spielt dieser Aspekt eine hervorgehobene Rolle.[136] Allerdings sind diese Schutzziele nicht immer erstrebenswert. So steht *Anonymität* der Zurechenbarkeit entgegen.[137] Differenzierung ist hierbei jedoch insofern erforderlich, als es sich bei den meisten Diskussionen um Anonymität um die ungewollte Zurechnung zur *personellen* und *öffentlichen* Identität handelt. Ein Maß an *technischer* Zurechenbarkeit ist auch in Netzwerken, die eine solche Form der Anonymität wahren möchten, für einen Kommunikationsaustausch notwendig und gewollt.[138]

Jedes einzelne Schutzziel beschreibt somit wünschenswerte und ggf. erforderliche Rahmenbedingungen von sicheren Systemen. Trotzdem können sich Schutzziele auch widersprechen. Wenn ein Backup eines Systems offline gespeichert wird, erhöht dies die Vertraulichkeit. Niemand kann, ohne vor Ort zu sein, auf das Backup zugreifen. Physische Barrieren wie ein Tresor können die Vertraulichkeit weiter erhöhen. All dies senkt aber auch die Verfügbarkeit, denn auf das Backup kann es keinen Fernzugriff per Internet mehr geben. Andere Schutzziele hingegen können situativ komplementär und in Kombination umgesetzt werden, etwa Integrität in Verbindung mit Authentizität. Dies kann erreicht werden, indem der Hashwert einer Nachricht mit einem *private key* signiert wird.

Einer der bedeutendsten Anwendungsfälle der Informationssicherheit und mit ihr der Kryptographie ist heute das Internet und das World Wide Web. In Kapitel 4 wird dediziert das regulatorische Verhältnis von

134 Siehe ebd., S. 4, sowie Eckert, *IT-Sicherheit*, S. 12.

135 Siehe Oorschot, *Computer Security and the Internet*, S. 4.

136 Siehe Eckert, *IT-Sicherheit*, S. 12.

137 Anonymität ist definiert als „the property that one's actions or involvement are not linkable to a public identity"; Oorschot, *Computer Security and the Internet*, S. 4. Im Deutschen: „Unter der Anonymisierung versteht man das Verändern personenbezogener Daten der Art, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"; Eckert, *IT-Sicherheit*, S. 13.

138 Beispielsweise verschleiern anonyme Netzwerken wie *Tor* die Verbindung von digitalen Identitäten zu öffentlichen Identitäten. Aus technischer Perspektive ist jedoch auch hier ein Maß an Zurechenbarkeit und Verbindlichkeit für den Kommunikationsaustausch selbst notwendig.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Kryptographie und Internet analysiert werden, weswegen wir uns hier auf eine rein technologische Sicht beschränken können. Im Internet wird Sicherheit und Verschlüsselung nämlich nicht direkt durch die physische Infrastruktur erreicht, sondern durch eine Protokollentwicklung auf Transport- und Anwendungsebene.[139] Einer der dabei wichtigsten Standards ist *HTTPS* – das *Hypertext Transfer Protocol Secure*.[140] HTTPS baut dabei grundsätzlich auf HTTP auf, verwendet jedoch zusätzlich das *SSL*- bzw. *TLS*-Verfahren.[141] Mit einer Kombination unterschiedlicher kryptographischer Verfahren können mit HTTPS die Schutzziele der Vertraulichkeit, Integrität und Authentizität auch im World Wide Web erreicht werden. Ohne solche Protokollentwicklungen, die auf der Modernen Kryptographie basieren, wäre das Internet ein unsicheres Kommunikationsnetzwerk.

Ein anderer, immer relevanter werdender Fall ist das *Internet-of-Things* (IoT), bei dem Endgeräte mit dem Internet verbunden sind und miteinander kommunizieren können. Ein IoT-Gerät ist zum Beispiel eine Smartwatch, die mit dem Internet sowie mit dem Mobiltelefon verbunden ist. Auch wenn solche Geräte das alltägliche Leben an vielen Stellen bereichern, können sie für entscheidende Sicherheitsprobleme sorgen.[142] Dies ist unter anderem deswegen relevant, weil sie ob ihrer Natur oftmals in privaten und intimen Bereichen eingesetzt werden – zum Beispiel eine Kamera, die spielende Kinder im Garten filmt, ein Kühlschrank, der die Essgewohnheiten von Personen dokumentiert und auswertet, sowie ein im Schlafzimmer stehender *smarter* Lautsprecher,

139 In Kapitel 4 wird das zugrundeliegende *End-to-End Principle* näher diskutiert werden.

140 Siehe dazu und zum Folgenden einführend Oorschot, *Computer Security and the Internet*, S. 252–254; zu TLS auch Anderson, *Security Engineering*, S. 195–197.

141 SSL bedeutet *Secure Sockets Layer*, der Nachfolger TLS ist die Abkürzung für *Transport Layer Security*.

142 Siehe im Kontext von Cyber Threats beispielsweise Richard A. Clarke und Robert K. Knake. *The Fith Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019, S. 265–280; im Kontext des *Going Dark*-Problems, das Kapitel 6 diskutieren wird, siehe zudem Urs Gasser u. a. *Don't Panic: Making Progress on the "Going Dark" Debate*. Berkman Center for Internet & Society at Harvard University, 1. Feb. 2016. URL: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (besucht am 15.04.2024).

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

der sowohl das Schnarchen als auch alle anderen Tätigkeiten mithören wird.[143]

Zusammenfassend zeigt sich im Kontext von Informationssicherheit und Kryptographie, dass die Verschlüsselung hinsichtlich der Vertraulichkeit *ein* bedeutendes Schutzziel darstellt. Vertraulichkeit und Geheimhaltung von Informationen sind das, was eine systematische Kryptographie seit jeher zum Ziel hatte. Die folgenden Kapitel werden sich daher maßgeblich mit Fragen der *Verschlüsselung* auseinandersetzen. Ethische Fragen, die dabei auftreten, sind zum Beispiel: Wer oder was soll vertraulich kommunizieren dürfen? Welche Eingriffsrechte sollten staatliche Strafverfolgungsbehörden erhalten? Welche Konsequenzen sind zu befürchten, wenn Unternehmen das Ziel der Vertraulichkeit ungenügend umsetzen? Wie verhält sich das Konzept von Privacy zur Vertraulichkeit der Kommunikation?

Wie diese mehrdimensionale Komplexität der Schutzziele aber auch zeigt, kann Moderne Kryptographie rein technologisch nicht mehr *nur* als Mittel zur Vertraulichkeit betrachtet werden. Mit Blick auf die unterschiedlichen Schutzziele können wir auch andere, etwas subtilere Fragen des Verhältnisses von Kryptographie und Ethik analysieren: Sollte anonyme Kommunikation in Demokratien technisch möglich sein? Ist eine Authentifizierungspflicht in gewissen Situationen ethisch geboten? Kann mit Kryptographie eine Totalidentifikation des Menschen entstehen, wenn biologische Merkmale mit digitalen Zertifikaten und Signaturen verbunden werden? Unter welchen Umständen sollte eine solche Zurechenbarkeit nicht möglich sein?

All diese Fragen erfordern eine Verbindung von einer ethischen Analyse einerseits mit den technologischen Möglichkeiten Moderner Kryptographie andererseits. Kryptographische Verfahren sind dabei nämlich einem stetigen Wandel unterzogen, wie die vorangehenden Abschnitte gezeigt haben. Seit Jahrhunderten ist die Kryptographie geprägt durch das an vielen Stellen implizit beschriebene Katz-und-Maus-Spiel, bei dem

143 Gasser et al. erkennen hierbei auch Folgen für die Möglichkeiten der Überwachung: „Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel"; ebd., S. 3.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

die *Codemaker* (Kryptographie) gegen die *Codebreaker* (Kryptoanalyse) antreten. RSA und AES sowie die meisten in der Praxis angewandten Verfahren sind lediglich *computationally secure* – das heißt, sie sind mit der *heutigen* Rechenleistung und dem *heutigen* Wissen nicht zu brechen. Das nächste Kapitel soll daher einen Ausblick auf die Zukunft der Kryptographie wagen. Insbesondere soll uns dabei die Frage beschäftigen, welche Auswirkung das Quantum Computing auf die (asymmetrische) Kryptographie hat und haben wird.

2.5 Quantum Computing und Verschlüsselung

Im Jahr 1994 veröffentlicht Peter Shor einen Algorithmus, der das wahr werden ließ, wovor sich Kryptographinnen und Kryptographen lange Zeit nur fürchten konnten: eine Methode, mit der das Faktorisierungsproblem (relevant für RSA) und das Problem des Diskreten Logarithmus (relevant für den DH-Schlüsselaustausch) in polynomieller Laufzeit gelöst werden kann.[144] Das für die asymmetrische Kryptographie bislang Beruhigende allerdings ist, dass dieser Algorithmus in der Realisierung einen sogenannten *Quantencomputer* benötigt, da an einer entscheidenden Stelle eine Quanten-Fouriertransformation durchgeführt wird. Ein Quantenrechner, der groß genug wäre, um heute verwendete RSA-Verschlüsselungen zu brechen, existiert bislang nicht.[145]

Daher findet RSA weiter breite Anwendung, ohne dass man sich zumindest kurzfristig Sorgen um die Vertraulichkeit und Authentizität von

144 Siehe Shor, „Algorithms for Quantum Computation"; einführend auch Chris J. Hoofnagle und Simson J. Garfinkel. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press, 2022, S. 166–167 und 199–203.

145 Für diese und die folgenden Ausführungen zum Quantum Computing siehe die Standardliteratur, insbesondere LaPierre Ray. *Introduction to Quantum Computing*. Cham: Springer, 2021; Matthias Homeister. *Quantum Computing verstehen: Grundlagen – Anwendungen – Perspektiven*. 6. Aufl. Wiesbaden: Springer Vieweg, 2022; Sean Hallgren und Ulrich Vollmer. „Quantum computing". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 15–34. Zur Post-Quanten-Kryptographie siehe Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen, Hrsg. *Post-Quantum Cryptography*. Berlin und Heidelberg: Springer, 2009; Daniel J. Bernstein. „Introduction to post-quantum cryptography". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 1–14. Zur Einführung in das Quantum Computing im Kontext von Cyber Threats siehe Clarke und Knake, *The Fith Domain*, S. 253–264.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

Kommunikation machen müsste. Zu betonen ist auch, dass für symmetrische Verfahren wie AES sowie für heute genutzte Hashfunktionen kein Algorithmus bekannt ist, der ein solch *fundamentales* Problem wie bei der asymmetrischen Kryptographie darstellen würde. Der Grover-Algorithmus ermöglicht zwar schnellere Brute-Force-Attacken auf AES, allerdings gilt AES mit einer Schlüssellänge von 256 Bit als weiterhin sicher.[146]

Trotz der aktuellen Sicherheit der bekannten asymmetrischen Verfahren gibt es mindestens drei Gründe, die dafür sprechen, die genannten Fragen auch in einer ethischen Diskussion zu berücksichtigen: (1) Dem Quantum Computing *könnte* in wenigen Jahrzehnten der Durchbruch gelingen, sodass bisher verwendete Verfahren nutzlos wären. (2) Der Prozess und die Dauer einer Migration zu einer sogenannten *Post-Quanten-Kryptographie* (engl. *Post-Quantum Cryptography*, abgekürzt PQC) ist schwer abzuschätzen. (3) Eine ganz grundsätzliche Frage praktikabler Kryptographie ist, *wie lange* die heutige Kommunikation und Information erfolgreich verschlüsselt sein soll.[147] Abschnitt 8.3 wird sich daher explizit mit ethischen Fragen zum Quantum Computing und zur Kryptographie auseinandersetzen. Um diese Fragen aber beantworten zu können, betrachten wir in diesem Kapitel zunächst die technischen Grundlagen.

Bisherige, klassische Computer arbeiten mit digitalen Schaltungen und Transistoren, die auf binäre Weise mit Nullen und Einsen Berechnungen durchführen. Dies gilt für Personal Computer (PC), mobile Endgeräte, Smartwatches, Hochleistungsrechner und IoT-Geräte. Das Quantum Computing dagegen stellt ein gänzlich neues Paradigma der Berechnung dar. Ein Quantenrechner macht sich nämlich quantenmechanische Phänomene aus der Physik zunutze, von denen ein algorithmischer Rechenvorteil gegenüber klassischen Rechnern erhofft wird. Algorithmischer Rechenvorteil bedeutet hier, dass ein Quantenalgorithmus gefunden wird, der bekanntermaßen einen Vorteil gegenüber einem klassischen Algorithmus aufweist. Der *Algorithmus von Deutsch* und der *Deutsch-Jozsa-Algo-*

146 Siehe Daniel J. Bernstein und Tanja Lange. „Post-quantum cryptography". In: *Nature* 549 (2017), S. 188–194, hier S. 189.

147 Letzteres meint vor allem Fragen zur *Vorratsdatenspeicherung* (engl. *data retention*). Siehe allgemein einführend Diffie und Landau, *Privacy on the Line*, S. 291–294. Wie in den vorherigen Abschnitten deutlich geworden ist, sind die meisten Algorithmen lediglich *computationally secure*. Ein Angriff mit unbeschränkter Rechenleistung würde daher Nachrichten, die mit solchen Algorithmen verschlüsselt wurden, brechen können.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

rithmus waren die ersten Algorithmen, bei denen solche Vorteile gezeigt werden konnten.[148]

Um einen solchen Quantenvorteil zu erreichen, arbeiten Quantenrechner mit sogenannten *Qubits* – im Gegensatz zu jenen klassischen *Bits*, die entweder 0 oder 1 repräsentieren. Damit hängen wichtige quantenmechanische Phänomene zusammen, primär die sogenannte *Superposition* und die *Verschränkung*. Es würde an dieser Stelle zu weit gehen, neben den kryptographischen Aspekten auch noch jene der Quantenphysik und des Quantum Computings zu erläutern. Für weitere Ausführungen sei daher auf die umfassende Literatur verwiesen.[149] Für die Kryptographie aber ist wichtig: Sollte ein entsprechend großer und nutzbarer Quantenrechner entwickelt werden, werden die meisten der eingesetzten asymmetrischen Verschlüsselungsverfahren unbrauchbar – mit allen sozialen, ökonomischen und gesellschaftlichen Folgen. Wie weit ist die Welt davon aber entfernt?[150]

Für die Marketingabteilungen der großen Hersteller jedenfalls jagt ein Meilenstein den nächsten, der einen Quantenrechner mit immer mehr Qubits ermöglicht.[151] Allerdings spielt die Anzahl an Qubits nicht die alleinige Rolle für die Nutzbarmachung von Quantencomputern, weshalb

148 Siehe David Deutsch. „Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), S. 97–117; sowie David Deutsch und Richard Jozsa. „Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 439.1907 (1992), S. 553–558. Siehe zur Einführung auch Ray, *Introduction to Quantum Computing*, S. 149–161.

149 Für eine aktuelle, aber verständliche Einführung siehe z. B. Homeister, *Quantum Computing verstehen*, sowie umfassend Ray, *Introduction to Quantum Computing*. Auch die Unterscheidung verschiedener Ansätze im Quantum Computing, etwa des sogenannten *adiabatischen Quantum Computing*, sind hier aufgrund der gebotenen Kürze auszuklammern. Siehe im Kontext der Kryptographie einführend Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 204–206.

150 Siehe zu einer aktuelleren Einschätzung im Kontext der Kryptographie ebd., S. 203–206.

151 Für IBM war dies etwa der *IBM Eagle*, dessen Vorstellung von seinem Hersteller werbend kommentiert und tituliert wurde mit „IBM Quantum breaks the 100-qubit processor barrier". Jerry Chow, Oliver Dial und Jay Gambetta. „IBM Quantum breaks the 100-qubit processor barrier". In: *IBM Blog* (16. Nov. 2022). URL: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (besucht am 15.04.2024). Zum Risiko des Hypes siehe auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 17–18.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

werbende Aussagen eher von Hybris zeugen als zu einer realistischen Einschätzung der Technologie führen.[152] Eine wohlwollende Skepsis ist auch vor dem Hintergrund des ständigen Wissenszuwachses durch die Physik und der rapiden Entwicklungen in der informatischen Anwendung angebracht.[153] Denn wie in zahlreichen Bereichen der Wissenschaft gibt es auch im Bereich des Quantum Computings eine Art immanenter *Unsicherheit* – nur mit dem Unterschied, dass jene *Unsicherheit* gerade in diesem Bereich der Wissenschaft einige unangenehme und negative Folgen mit sich bringen könnte. Man kann schlichtweg nicht sagen, wann, ob oder wie dem Quantum Computing der *praktische* Durchbruch gelingen wird. Der Physiker John Preskill hat diese Situation des Quantum Computings bereits im Jahr 2018 auf den Punkt gebracht:

> While this uncertainty fuels optimism, our optimism should be tempered with caution. We may feel confident that quantum technology will have a substantial impact on society in the decades ahead, but we cannot be nearly so confident about the commercial potential of quantum technology in the near term, say the next five to ten years.[154]

Um trotzdem den Versuch einer zeitlichen Systematisierung vornehmen zu können, bietet sich das *Mosca-Theorem* an.[155] Dieses Theorem lässt sich einfach durch $X + Y > Z$ beschreiben.[156] Dabei meint X die Dauer, wie lange kryptographische Schlüssel sicher sein sollten.[157] Nachrichten können durchaus hohe Anforderungen an eine solche Dauer haben, etwa

152 Eine aktuell wichtige Thematik ist hier die Fehlerkorrektur; siehe einführend Ray, *Introduction to Quantum Computing*, S. 341–345.

153 Kritische Argumente zur generellen Realisierbarkeit von Quantencomputern finden sich beispielsweise beim israelischen Mathematiker Gil Kalai. Siehe etwa Gil Kalai. *Three Puzzles on Mathematics, Computation, and Games*. 2018. arXiv: 1801.02602v1. URL: http://arxiv.org/pdf/1801.02602v1 (besucht am 15.04.2024); sowie Gil Kalai. *The Quantum Computer Puzzle (Expanded Version)*. 2016. arXiv: 1605.00992v1. URL: http://arxiv.org/pdf/1605.00992v1 (besucht am 15.04.2024).

154 John Preskill. „Quantum Computing in the NISQ era and beyond". In: *Quantum* 2 (2018), Art. Nr. 79, S. 1. An solch einer Einschätzung hat sich bis heute wenig geändert.

155 Siehe Michele Mosca. „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" In: *IEEE Security and Privacy* 16.5 (2018), S. 38–41.

156 Siehe ebd., S. 38.

157 Siehe ebd., S. 38. Dies ist sowohl auf das Schutzziel der Vertraulichkeit als auch auf jenes der Authentizität anwendbar.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

streng vertrauliche Dokumente zur Identität von Undercover-Agenten oder zu militärischen Operationen.[158] Aber auch persönliche und intime Nachrichten möchte man sicherlich länger als nur wenige Jahre verschlüsselt wissen. Besondere Bedeutung erlangt dieser Aspekt vor dem Hintergrund der Bemühungen von Strafverfolgungsbehörden und Geheimdiensten um eine *Vorratsdatenspeicherung* (engl. *data retention*): Bereits heute kann ein substantieller Teil der Internet-Kommunikation aufgezeichnet und gespeichert werden, und man könnte spekulieren, dass dies mit der Intention geschieht, diese Kommunikation nach dem Tag X auch entschlüsseln zu können.[159]

Leider genügt es aber nicht, wenn X klein ist, zumal X primär eine Business- und Policy-Entscheidung ist.[160] Genauso bedeutend ist Y: Wie lange dauert es, quantensichere Systeme zu entwickeln und einzusetzen?[161] Vorwiegend relevant ist dabei die Migration zu einer PQC. An einer solchen PQC, die einerseits resistent gegenüber Quantenalgorithmen und andererseits auf digitalen Rechnern berechenbar ist, wird bereits seit vielen Jahren geforscht.[162] Trotzdem sind die Integration und die Migration neuer kryptographischer Verfahren in ein bestehendes System aufwendig und komplex, und eine Schätzung, wie lange es dauern könnte, gestaltet sich schwierig.

Z schließlich beschreibt die Dauer der Entwicklung eines ausreichend großen Quantenrechners, der unsere heutigen asymmetrischen Verfahren brechen kann.[163] Auch hier ist eine Schätzung kaum möglich. Im Sinne einer funktionalen Kryptographie ist Z tendenziell jedoch eher kürzer als länger einzuschätzen. Die Folgen wären technologisch und gesellschaftlich potentiell gravierend, wenn von einer falschen und zu großzügigen Dauer ausgegangen wird. Zusammenfassend ist X daher zwar

158 Als Beispiel kann hier die sowjetische Kommunikation dienen, die noch viele Jahre später im Rahmen des Venona-Projekts entschlüsselt werden sollte. Siehe Diffie und Landau, *Privacy on the Line*, S. 29–30; einführend zur Dauer auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 427–428.

159 Siehe im Kontext der NSA James Bamford. „The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". In: *Wired* (12. März 2015). URL: https://www.wired.com/2012/03/ff-nsadatacenter/ (besucht am 15.04.2024); ebenso Diffie und Landau, *Privacy on the Line*, S. 292, allgemeiner siehe S. 291–294.

160 Siehe Mosca, „Cybersecurity in an Era with Quantum Computers", S. 38.

161 Siehe ebd., S. 38–39.

162 Siehe Bernstein, „Introduction to post-quantum cryptography".

163 Siehe Mosca, „Cybersecurity in an Era with Quantum Computers", S. 39.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

a priori einzuschätzen und festzulegen, wird als primäre Policy-Entscheidung jedoch oft nur ungern verändert. *Y* und *Z* dagegen sind zwar bis zu einem gewissen Grad durch die entsprechende Forschung und praktische Maßnahmen zu beeinflussen, allerdings ist eine apriorische Einschätzung nicht möglich.

Neben jener bereits beschriebenen PQC, die für *Y* relevant ist, ist auch die sogenannte *Quantenkryptographie* zu nennen. Während die PQC eine quantenresistente Verschlüsselung mithilfe digitaler Rechner zum Ziel hat, nutzt die Quantenkryptographie selbst quantenmechanische Phänomene. Bedeutend ist hier vor allem der sogenannte *Quantenschlüsselaustausch* (engl. *Quantum Key Distribution*, abgekürzt QKD).[164] Erstmalig veröffentlicht wurde ein solches Verfahren 1984 von Charles H. Bennett und Gilles Brassard (daher abgekürzt mit *BB84*).[165] Benötigt wird allerdings spezielle Hardware zur Quantenkommunikation.[166] Auch hier ist damit unklar, bis wann mit einem breitflächigen und praktischen Einsatz gerechnet werden könnte.[167] Sollte es jedoch dazu kommen, wäre algorithmische *information-theoretic security* in der Kommunikation realisierbar.[168]

Die Thematik um das Quantum Computing, die PQC und die QKD ist damit nicht nur für die Physik, die Informatik und die Ingenieurwissenschaften von Interesse. Das Quantum Computing wird auch zur theoretischen Herausforderung für die Ethik, die Soziologie, die Philosophie, die Theologie und alle weiteren Humanwissenschaften werden – egal ob

164 Siehe zur Sicherheit der QKD Renato Renner. „Security of Quantum Key Distribution". Dissertation No. 16242. Zürich: ETH Zürich, 2005; einführend Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 276–293.

165 Siehe Charles H. Bennett und Gilles Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Proceedings of the International Conference on Computers, Systems and Signal Processing. Bangalore, India*. 1984, S. 175–179; einführend auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 277–293.

166 Siehe zur Einführung in die Quantenkommunikation ebd., S. 257–260.

167 Siehe umfassender zur Quantenkryptographie und BB84 auch Ramona Wolf. *Quantum Key Distribution: An Introduction with Exercises*. Cham: Springer, 2021; sowie Federico Grasselli. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Cham: Springer, 2021; im Deutschen auch Homeister, *Quantum Computing verstehen*, S. 167–189.

168 Siehe Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 257. Allerdings könnten z. B. Fehler in der Implementierung dieses Ziel auch dann noch verhindern.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

und wann ein Durchbruch gelingen mag. Gerade *wegen* der Unsicherheiten von Prognosen und Einschätzungen sind die Geisteswissenschaften im Allgemeinen und die Ethik im Speziellen gefragt, einen Zugang zum Quantum Computing zu entwickeln. Einerseits geht es darum, sich auf die möglicherweise kommenden disruptiven Veränderungen vorzubereiten, sie zu analysieren und schließlich Lösungsansätze für drängende Probleme und den Einsatz von Quantencomputern zu diskutieren. Andererseits gilt es aber auch, das binäre Bild, das unsere digitale Welt über fünfzig Jahre lang in Nullen und Einsen geprägt hat, zu überdenken. Für die Kryptographie wird Abschnitt 8.3 einen solchen Zugang der Ethik entwickeln.

Kommen wir im Kontext dieser Aussichten und zum Abschluss von Teil I noch einmal auf David Kahns *The Codebreakers* zurück. Nach einer Diskussion um DES, den DH-Schlüsselaustausch und RSA schreibt er in der überarbeiteten Ausgabe seines Werkes aus dem Jahr 1996:

> The war of cryptographer against cryptanalyst has been won by the cryptographers. The only way properly encrypted messages can be read nowadays is by theft or betrayal – that is, noncryptologic means. [...] Does this mean that the story of secret writing has ended? In the long term, yes.[169]

Kahn hat ohne jeglichen Zweifel eine beeindruckende Geschichte über das *secret writing* verfasst, die sich stark am Ziel der Vertraulichkeit orientiert hat. In einem rein theoretischen Sinn hat er etwa mit Blick auf das One-Time-Pad also recht. Moderne Kryptographie ist heute jedoch mehr als bloß das. Für Kahn dürfte dies in der ersten Auflage von 1967 noch nicht klar gewesen sein, und selbst in der zweiten Auflage aus dem Jahr 1996 war die Kryptographie in weiten Teilen noch ein reines Werkzeug zum Zwecke der Vertraulichkeit.

Das Paradigma der Klassischen Kryptographie war spätestens mit dem 20. Jahrhundert beendet. Das aber, was danach kam, jene Moderne Kryptographie, steht heute erst am Anfang. Der Algorithmus von Shor, die Standardisierung von PQC und eine neue Art des Schlüsselaustausches durch die QKD zeigen ganz praktisch, dass die Diskussion um sichere Kryptographie noch einen weiten Weg vor sich hat. Auch viele

169 Kahn, *The Codebreakers*, S. 984.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

andere zukünftige Themen der Kryptographie wie beispielsweise die homomorphe Kryptographie, Physical Unclonable Functions (PUF) oder Zero-Knowledge-Proofs konnten in diesem Rahmen nicht einmal ansatzweise diskutiert werden.[170]

Dieses neue Paradigma war und ist aber nicht nur technologischer Natur. Wenige Jahre nach Shannon, Diffie und Hellman erreichte die Moderne Kryptographie zunehmend auch den gesellschaftlichen Diskurs. Wenn Kommunikation schließlich immer mehr digital stattfinden sollte, dann wird sich natürlich auch jeder Einzelne und jede Einzelne fragen müssen: Wie kann meine Kommunikation sicher, vertraulich und integer sein? Der zweite Teil wird zeigen, dass diese Frage einige weitreichende gesellschaftliche Diskussionen zur Folge haben musste.

170 Der Kryptograph Yvo Desmedt meint zur Zukunft der Kryptographie sogar, dass „cryptography as a science is in its infancy." Desmedt, „What is the Future of Cryptography?", S. 113.

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.5771/9783748955009-15 - am 07.02.2026, 00:52:30. https://www.inlibra.com/de/agb - Open Access -