2. Kryptographische Sicherheitsbestimmungen

»Ist das sicher?« Diese Frage ist früher oder später Teil von Unterhaltungen über (neue) Apps, Programme, Funktionen oder technische Endgeräte, und wurde mir, je länger ich mich mit IT-Sicherheit befasst habe, umso häufiger von Kolleg_innen, Freund_innen und Familienmitgliedern gestellt. Es gibt viele Möglichkeiten, diese Frage zu beantworten: Man könnte sich die AGB und Angaben zum Datenschutz eines jeweiligen Herstellers durchlesen und versuchen, nachzuvollziehen, was mit den Daten passiert, die bei der Benutzung einer App entstehen. Man könnte sich – sofern es sich um eine Open Source-Anwendung handelt – um einen Blick in den Quelltext bemühen, und versuchen zu überprüfen, ob die Anwendung bisher unbemerkte Sicherheitslücken enthält. Man könnte sich darüber informieren, ob eine App, beispielsweise ein Messenger, die bei der Benutzung entstehenden Daten verschlüsselt, und wenn ja, welche Verschlüsselungsmechanismen es gibt, und wie die verwendete Art der Verschlüsselung im Vergleich zu anderen abschneidet. Man könnte ein Gerät auseinander bauen, um sich zu vergewissern, dass die Hardware nicht manipuliert wurde. Man könnte… Diese Liste ist viel zu kurz, um alle Antwortmöglichkeiten zu beinhalten. Darüber hinaus setzen alle bisher angeführten Möglichkeiten auf verschiedenen Ebenen an, und unterschiedliche Kompetenzen voraus, die von dem Verständnis juristischer Texte wie AGBs bis hin zu den technischen Eigenschaften von Soft- und/oder Hardware reichen. Was in diesen Antwortmöglichkeiten nicht explizit angesprochen, aber durch die Auflistung sichtbar wird, ist die implizite Frage nach der Bedeutung des Wortes *sicher.* Denn nicht nur werden in dieser Aufzählung unterschiedliche Kompetenzen vorausgesetzt, sondern mit ihnen wird Sicherheit auch auf unterschiedlichen Ebenen verhandelt: auf rechtlicher Ebene (AGB), auf technischer Ebene (Vergleich von Verschlüsselungsmethoden, Untersuchen der Hardware) und auf der Ebene von Herstellungspraktiken (Open Source). Diese Ebenen sind bei der Herstellung von IT-Sicherheit, um die es im weitesten

Sinne bei der Frage nach Sicherheit in digitalen Medien geht, miteinander verknüpft. Die Annäherung an die Frage, was (IT-)Sicherheit bedeutet, wird im Folgenden zunächst über die Geschichte der Kryptographie vollzogen, da diese in bisherigen medienkulturwissenschaftlichen Betrachtungen von digitalen Phänomenen mit Bezug zu IT-Sicherheit, wie beispielsweise Computerviren, kaum bis gar nicht beachtet wurde,[1] aber grundlegend für das Verständnis von IT-Sicherheit ist. Von besonderem Interesse für die weiteren Ausführungen ist daher auch eine genauere Betrachtung der Intersektion von Kryptographie und Informatik, und der daraus folgenden Übertragung kryptographischer Sicherheitskonzepte in die Informatik, die den Bereich der IT-Sicherheit sowohl in der Industrie als auch als wissenschaftliche Disziplin kennzeichnet.

In diesem Kapitel soll daher zunächst ein wissensgeschichtlicher Überblick über zentrale Konzepte in der Geschichte der Kryptographie gegeben werden, die jeweils im Hinblick auf ihre Medialität sowie das zugrunde liegende Konzept von Sicherheit diskutiert werden. Anschließend wird im folgenden Kapitel eine wissensgeschichtliche Betrachtung dessen, was heute in der IT-Sicherheit unter Sicherheit verstanden werden kann, entfaltet werden. Für diesen Zweischritt ist eine artifizielle Aufteilung der Anwendungsbereiche von Kryptographie in zwei Bereiche notwendig: Erstens die Sicherheit von Kommunikationsinhalten während des Kommunikationsvorgangs und zweitens die Sicherheit von (vernetzten) IT-Systemen abseits von Kommunikationsprozessen menschlicher Akteur_innen.[2] Diese Trennung

1 So findet Kryptographie beispielsweise in Jussi Parikkas (2016) *Digital Contagions. A Media Archaeology of Computer Viruses* keine Erwähnung. Alexander Galloway und Eugene Thacker (2007, 86–87) streifen in *The Exploit. A Theory of Networks* Kryptographie als Eigenschaft sowohl von biologischen Viren als auch von Computerviren, allerdings eher in einem (schiefen) metaphorischen Sinne, da sie das kryptographische Element von Viren daran festmachen, dass diese sich stets veränderten. Während Galloway und Thacker zwar die prozessuale Eigenschaft von Kryptographie erkennen, ist das Ziel von Kryptographie jedoch, wie sich im Folgenden herausstellen wird, eine Remediatisierung mit möglichst geringer Veränderung des Inhaltes. Der Gebrauch des Worts Kryptographie bei Galloway und Thacker folgt also eher einer »occult cryptography« (ebd., 129), die in die Richtung einer Numerologie zeigt.

2 Letzteres betrifft einerseits bereits gespeicherte Daten, sowie andererseits das ungestörte Funktionieren vernetzter Computer. Der Aspekt der Stabilität und Verfügbarkeit durch die regelmäßige Wartung von Systemen wird in diesem Buch nicht thematisiert, da er, mehr als die anderen beiden Aspekte, an konkreten Praktiken im Sinne von Heuristiken und *best practices* orientiert ist, und daher einerseits über eine schlechte wis-

dient ausschließlich der Vermittelbarkeit dieser komplexen Geschichte in zwei Erzählsträngen: Erstens der Geschichte der Kryptographie, die in diesem Kapitel besprochen wird, und der darin liegenden Abgrenzung *moderner* von *klassischer* Kryptographie, sowie zweitens deren Anwendungsfelder in der IT-Sicherheit, die im nachfolgenden Kapitel diskutiert werden. Diese Einteilung wird sich bereits im Verlauf des vorliegenden Kapitels an manchen Stellen als brüchig erweisen, was gleichsam als Nachweis der Künstlichkeit der von mir eingezogenen Trennung verstanden werden kann. Da dies jedoch immer noch eine nur unzureichende Beantwortung der Frage danach ist, was *sicher* in den jeweiligen Fällen und Diskursen bezeichnet, wird außerdem darauf eingegangen, welche Aussagen darüber, wie Sicherheit funktioniert, was sie leisten kann und soll, vom mathematisch-technischen Diskurs unausgesprochen bleiben.

2.1 Zum Status des Wissens über Kryptographie

Die Geschichte der Kryptographie ist, gemessen an ihrer langen Existenz, erst vor kurzem geschrieben worden. David Kahn, der Autor des kanonischen Buchs *The Codebreakers. The Story of Secret Writing*, bemerkt dazu im Vorwort desselben:

> »CODEBREAKING is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments. Yet it has never had a chronicler. It badly needs one.« (Kahn 1967, ix)

Kahns Buch wurde 1967 veröffentlicht, inmitten des Kalten Krieges, und nur wenige Jahre vor Ende des Vietnamkrieges. Wie bereits aus dem kurzen Zitat aus dem Vorwort zu erkennen ist, erzählt Kahn die Geschichte der Kryptographie als Militärgeschichte. Die zahlreichen Beispiele – Kahn (ebd.) legt mit *The Codebreakers* die, in seinen Worten, »entire history of cryptology« vor – befassen sich also mit der Rolle von Kryptographie in Kriegshandlungen, in Konflikten zwischen Staaten, als Werkzeug von Botschaftern und Spionen.

---

senschaftliche Quellenlage verfügt, und andererseits außerhalb dessen liegt, was eine qualitative medienwissenschaftliche Arbeit leisten kann.

Entsprechend beginnt das erste Kapitel in medias res: Mit einer Nachricht zunächst unbekannten Ursprungs an den japanischen Botschafter in den USA, die in den frühen Morgenstunden des 7. Dezember 1941 von der US-amerikanischen Navy abgefangen und entschlüsselt wurde. Die Nachricht wies den japanischen Botschafter an, der US-amerikanischen Regierung einen einige Stunden zuvor in 14 Teilen gesendeten Beschluss der japanischen Regierung mitzuteilen: Dass diese sich außerstande sehe, durch weitere Verhandlungen mit den USA zu einer diplomatischen Lösung des Konflikts der beiden Staaten zu kommen (vgl. ebd., 2). Die Beziehungen von Japan und den USA waren bereits seit längerem konfliktbehaftet, und sollten an diesem Tag in dem Angriff japanischer Soldaten auf Pearl Harbor kulminieren, und das, wie Kahn (ebd., 4) herausstellt, *obwohl* es den USA gelang, die abgefangenen Nachrichten zu dekodieren, was er schließlich darauf zurückführt, dass in der dekodierten Nachricht keine Pläne für einen Angriff enthalten waren. Kahns Erzählungen der Ereignisse lesen sich für einen wissenschaftlichen Text nahezu übermäßig szenisch, fast wie ein Spionage-Thriller, was zweifelsohne dazu dienen soll, jeden Verdacht darauf zu zerstreuen, dass mathematische Entwicklungen eine trockene Materie seien.

In Kahns Tradition steht, sowohl was den Schreibstil als auch die Rahmung von Kryptographiegeschichte als Militärgeschichte angeht, auch Simon Singhs *The Code Book. Science of Secrecy from Ancient Egypt to Quantum Cryptography*, das ungefähr 30 Jahre später, kurz vor der Jahrtausendwende erstmals veröffentlich wurde. »For thousands of years«, so beginnt Singhs (2000, xiii) Einleitung,

> »kings, queens and generals have relied on efficient communication in order to govern their countries and command their armies. At the same time, they have all been aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rival nations and betraying vital information to opposing forces. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.«

Die historisch gewachsene, enge Verknüpfung von Kryptographie und Kriegsführung sowie Spionage soll an dieser Stelle nicht nur als eine mögliche Art der Diskursivierung durch die Autor_innen dieser Geschichte abgetan werden, sondern hat Auswirkungen auf das Wissen, das über Kryptographie gewusst und hergestellt werden kann. Auf diesen Umstand nimmt ein – verglichen mit Kahn und Singh – eher unbekanntes, aber dennoch sehr genaues und

hilfreiches Buch Bezug, das an dieser Stelle ebenfalls erwähnt sein soll: Friedrich Bauers *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Bauers Buch ist vor allem aufgrund seiner Situierung im deutschen akademischen Kontext spannend, innerhalb dessen er zu Beginn der 1980er Jahre die erste öffentliche Vorlesung an einer westdeutschen Hochschule mit dem Titel »Kryptologie« hielt (vgl. Bauer 1997, V). Nach einer scherzhaft erzählten Anekdote darüber, dass Bauer eine Einmischung seitens deutscher Behörden in seinen Unterricht befürchtete, und er eines Tages tatsächlich die »unbekannten Gesichter zweier mittelalterlicher Herren mit Anzügen« (ebd., VI) in seiner Vorlesung erblickte – ein Vorkommnis, das ungeklärt blieb – schreibt Bauer (ebd., VI–VII) in der Einleitung seines Buchs weiter:

> »Ich bin es dem Leser nun doch schuldig, zu erklären, woher mein Interesse an der Kryptologie und meine Vertrautheit mit ihr herrührt. Vorab, mein größter Vorteil ist, daß ich nie Angehöriger eines Dienstes war. Ich stehe also unter keiner irgendwie gearteten Schweigepflicht. […] Trotzdem weiß ich nie, ob ich das, was ich weiß, auch wissen darf.«

Die Verstrickung von Geheimdiensten oder anderen staatlichen Akteur_innen in die Wissensproduktion in der und über die Kryptographie thematisiert auch David Kahn in seinem Vorwort mit einem kurzen Hinweis darauf, dass sein Buch vor Veröffentlichung dem *Department of Defense* zugegangen sei. Dies lässt darauf schließen, dass Kahn sicherstellen musste, keine *classified information* zu veröffentlichen – was allerdings an dieser Stelle eine Spekulation meinerseits (und vermutlich auch anderer Leser_innen) ist, da Kahn sich nicht zum Zweck dieser Vorlage äußert. Auch Singh (2000, xvi) weist auf die Prekarität des Wissens über Kryptographie hin, wenn er schreibt, »I must mention a problem that faces any author who tackles the subject of cryptography: the science of secrecy is largely a secret science.« Im Gegensatz zu Kahn findet bei Singh keine Kontrolle durch staatliche Akteur_innen Erwähnung, allerdings verweist er darauf, für seine Forschung wichtige Daten direkt vom britischen Geheimdienst GCHQ bekommen zu haben, und dass diese erst kurz vorher freigegeben wurden. Doch diese Unterstützung deutet auch darauf hin, so schreibt er weiter, dass Geheimdienste »such as GCHQ and America's National Security Agency continue to conduct classified research into cryptography, which means that their breakthroughs remain secret and the individuals who make them remain anonymous« (ebd., xvii). Eine Geschichte der Kryptographie steht aufgrund ebendieser Geheimhaltungspraktiken notwendigerweise stets unter Verdacht, nicht auf der Höhe

der Zeit zu sein, nicht alle Entwicklungen und Akteur_innen bedacht haben zu können – dies gilt damit ebenso für die vorliegende Publikation. Doch Singh weicht auch in einigen Punkten von dem militärischen Narrativ ab, vor allem in der Darstellung von kryptographischen Entwicklungen der späten 1970er Jahre wie der Public Key-Kryptographie. Weshalb diese Verschiebung in der Erzählweise möglich ist, wird unter anderem Gegenstand dieses Kapitels sein.

2.2 Zur Medialität von Kryptographie

Die bisherigen Überlegungen stützen sich maßgeblich auf Literatur aus dem Feld der Kryptographie selbst, sowie auf Quellen von Historikern. Dies ist zwar eine reichhaltige Materialgrundlage, aber dennoch auch keine zufällige Auswahl: Die Menge geisteswissenschaftlicher Forschung zu Kryptographie ist recht überschaubar, und oft wird Kryptographie nur im Zuge eines anderen Themas begleitend gestreift.[3] Eine nennenswerte Ausnahme ist Quinn DuPonts (2017) unter dem Namen *An Archeology of Cryptography: Rewriting Plaintext, Encryption, and Ciphertext* veröffentlichte Dissertation, die Kryptographie aus medienarchäologischer Perspektive betrachtet. Während sowohl DuPonts Arbeit als auch die vorliegende sich gegen ein instrumentelles Technikverständnis wenden und an diskursiven Möglichkeitsbedingungen von Kryptographie interessiert sind, schlagen sie doch differente Wege ein. DuPont situiert Kryptographie vorrangig in Hinblick auf Notation, d.h. Schrift, Schreiben und dessen Materialität, und fokussiert vor allem die Relation von Kryptographie und Sprache. An den technischen und mathematischen Details kryptographischer Systeme, ebenso wie an der jüngeren Geschichte der Kryptographie ist DuPont im Gegensatz zur vorliegenden Untersuchung jedoch

3 In *What is Media Archaeology?* diskutiert Jussi Parikka (2012, 90–112) kurz das Erstarken der Kryptographie im 19. Jahrhundert und ihren Zusammenfall mit der Telegraphie, wobei es ihm hauptsächlich um das Phänomen *Noise* geht. Friedrich Kittler (1986, 378–379) erwähnt Kryptographie in *Grammophon, Film, Typewriter*, allerdings im Zuge der kulturpessimistischen Diagnose, dass die Kryptographie eine automatisierte Diskursanalyse zur Folge habe. Alexander Galloway und Eugene Thacker (2007) streifen, wie bereits erwähnt, in *The Exploit* Kryptographie als Konzept, um auf Viren einzugehen. Die Performerin und Philosophin Susan Kozel geht in zwei Artikeln, die ihre eigenen Performanceprojekte diskutieren, auf die für die Performances zentrale prozessuale Dimension asymmetrischer Verschlüsselung ein (vgl. Kozel 2017; 2016).

nicht interessiert, weswegen sich die Pfade unserer Betrachtungen im Weiteren kaum kreuzen werden. Den überschaubaren geisteswissenschaftlichen Forschungsstand zu Kryptographie bespricht allerdings auch DuPont (2020) in seinem Aufsatz *Cryptographic Media*: »Despite the phenomenal rise in the use of cryptography, the emergence of a trillion-dollar computer security industry, unprecedented government interest and investment, and daily news stories describing the horrors of an insecure or overly secure Internet«, führt DuPont (ebd., 692) aus, »academic work on cryptographic media has tended to focus on a few important but limited areas of investigation.« Diese Felder seien zumeist, und diese Aussage bestätigte sich in meiner Recherche, Informatik, Ingenieurswissenschaften, und die Kryptographie als Disziplin selbst. Die Forschung in diesen Bereichen bezeichnet DuPont (ebd.) als »massive and well-funded«, sowie in vielen Fällen »cozy with corporate and government sponsors« – dies ist zweifelsohne ein Umstand, der sich darauf auswirkt, welches Wissen gewusst, produziert wird und werden kann.[4] Angesichts dieser Förderungssituation, schreibt DuPont (ebd.) weiter, könne man fälschlicherweise glauben, »cryptographic media« seien ausreichend beforscht und verstanden, doch das Gegenteil sei der Fall. DuPont (ebd., 692–693) macht große Wissenslücken in der Forschung, vor allem auf Seite der Geisteswissenschaften aus:

> »We might wonder, then, why have important questions not yet been *asked*? For instance, what *is* cryptography? Technologists, mathematicians, and engineers have answers, but they are not very satisfying – either doing too little or too much (the common plea that cryptography is just math is so broad that it risks explaining everything and nothing). Either way, these answers lack social and human richness. […] why, given its ubiquity, is encryption not considered one of the fundamental media technologies of the twentieth cen-

4 DuPont geht bis auf diese spitze Bemerkung nicht weiter auf die Förderungssituation mathematisch-naturwissenschaftlicher Fächer ein. Eine der wenigen Stimmen innerhalb der Kryptographie, die diesen Umstand kritisch diskutiert, ist Phillip Rogaway. In seinem Vortrag *The Moral Character of Cryptographic Work* greift Rogaway (2015, 37) die scheinbare Neutralität kryptographischer Forschung, die sich vornehmlich mit Zahlen und Rätseln befasse, angesichts ebendieser Nähe kryptographischer Forschung zu Geheimdiensten, Militär und Industrie an: »The military funding of science invariably redirects it and creates moral hazards. […] No matter what people say, our scientific work does change in response to sponsor's institutional aims.«

> tury (alongside radio, telephone, and television), and how do we explain its emergence and its future?«

DuPonts Artikel liefert einen Überblick über die Auseinandersetzung mit Kryptographie in den Bereichen Medienwissenschaft, Science and Technology Studies und Software Studies, und konstatiert, dass alle bisherigen Auseinandersetzungen unzureichend seien: Es fehle ein »sufficient theoretical framework for cryptography« (ebd., 693). Während DuPont (ebd.) zuzustimmen ist, was die überschaubare Quellenlage angeht, so kann es nur als Polemik aufgefasst werden, wenn er gleich drei Forschungsfeldern die naive Haltung unterstellt, sich bisher nicht mit Kryptographie auseinandergesetzt zu haben, da diese vermutlich glaubten, »that encrypted communication changes nothing, since, after all, encrypted communication is usually decrypted at its terminal location, seemingly returned to its original.« Der von ihm eigeforderten »cryptographic media theory« (ebd.) möchte dieses Buch dennoch nicht entsprechen, da die ersten richtungsweisenden Vorschläge, die DuPont im diskutierten Artikel für eine solche *cryptographic media theory* macht, in die Richtung einer weiteren Spielart kulturtechnischer Betrachtungen zeigen. Das vorliegende Buch wird daher den Blick nicht auf Kryptographie, also Verschlüsselung, *als Medium* (als »one of the fundamental media technologies of the twentieth century (alongside radio, telephone, and television)«) richten, da eine solche Betrachtungsweise Gefahr läuft, die Leistung von Verschlüsselung stillzustellen und damit zu verkennen, sondern fokussiert die prozessuale Dimension, *die Medialität*, von Ver- und Entschlüsselung, von Kryptographie. Was ist damit gewonnen?

Zunächst lässt sich festhalten, dass die »Annahme, es gebe Einzelmedien«, sich mit Sybille Krämer (2003, 85) als »Resultat einer Abstraktion« begreifen lässt, die zu der für die Medientheorie zentralen Frage führt, ob Medien Sinn erzeugen oder vermitteln. Krämer nähert sich dieser Frage in ihrem Aufsatz *Erfüllen Medien eine Konstitutionsleistung? Thesen über die Rolle medientheoretischer Erwägungen beim Philosophieren* davon ausgehend, dass die Bestimmung dessen, was Medien sind, sich weder in den Zeichen, die sie übertragen, noch in den Gegenständen und technischen Apparaten, die ihre Materialität ausmachen, erschöpft (vgl. ebd., 79). Im Verlauf ihres Aufsatzes legt Krämer eine philosophische Reflexion von Medien und Medialität vor, die Medien als konstitutive Elemente für das, was sie vermitteln, und damit auch des Denkens und des Philosophierens wahrnimmt, ohne dabei ein mediales Apriori anzu-

nehmen. Wie eine solche Denkweise von Medien aussehen kann, etabliert sich, wie Krämer (ebd., 80) formuliert,

> »zwischen zwei Polen: Der eine Pol ist die (traditionell geisteswissenschaftliche) Auffassung von der ›Sekundarität des Medialen‹: Ausgehend von der Vehikelfunktion, vom transitorischen, vermittelnden Charakter des Mediums werden Medien mit den materiellen Realisierungsbedingungen symbolischer Formen/Gehalte identifiziert. Medien übertragen etwas, das selbst nicht ›von der Natur eines Mediums‹ ist, sei das nun der Gehalt, die Botschaft, der Sinn oder die Form. Es gibt also ein Außerhalb von Medien. Der andere Pol ist die (eher kulturalistisch inspirierte) Auffassung vom ›Primat des Medialen‹: Medien gelten dann […] als zeitgenössische Fortbildung eines Sprach-, Zeichen- oder Technikapriori. […] Es gibt kein Außerhalb von Medien.«

An diesem Punkt stellt sich die »Gretchenfrage« (ebd.) der Medientheorie: Übermitteln oder erzeugen Medien etwas? Die beiden von Krämer beschriebenen Pole entstehen durch die für Medien charakteristische Eigenschaft, einen Unmittelbarkeitseindruck durch ihren Entzug herzustellen: Gelingt die Vermittlungsleistung, so werden Medien unsichtbar. Nur in ihrer Störung treten Medien an Stelle ihres Inhaltes wieder in Erscheinung (vgl. ebd., 81). Weiterhin unterscheidet Krämer (ebd.) zwischen Medium und Medialität, und setzt dazu im Anschluss an Niklas Luhmann Medien als »Unterscheidungs-Potenziale« ein: »Sie stellen ein Strukturierungsrepertoire bereit, das zur Formbildung dient.« In Absetzung von Luhmanns systemtheoretischer Perspektive sind die medialen Akte der Formgebung für Krämer (ebd.) allerdings keine »Operationen eines Systems«, sondern vielmehr »kulturelle Praktiken« – was sich als Medien beschreiben lässt, ist folglich eine Art geronnener Kultur. Als bedeutsam für diese Sichtweise von Medien führt Krämer zwei Momente an: Erstens, dass die Unterscheidung von Medium und Form nicht statisch sei, sondern stets abhängig von dem Erkenntnisinteresse und der eingenommenen Perspektive auf den analysierten Gegenstand; und zweitens, dass Medien sich nicht nur durch eine Störung, sondern auch dort nicht mehr der Wahrnehmung entziehen, wo sie zur Form werden, die in einem anderen Medium erscheint (vgl. ebd., 82). Eine ähnliche Beobachtung machen auch Jay David Bolter und Richard Grusin (2000) mit dem von ihnen geprägten Begriff der *Remediation*, der im Folgenden verwendet wird, um die Aufnahme eines Mediums in ein anderes Medium zu beschreiben. Bolter und Grusin stellen ebenso wie Krämer fest, dass Medien sich einerseits der Wahrnehmung

entziehen und so eine durch den Eindruck von Unmittelbarkeit gekennzeichnete Erfahrung herstellen, was sie als *immediacy* bezeichnen (vgl. ebd., 70). Gleichzeitig gehe mit der Aufnahme eines Mediums in ein anderes Medium einher, dass man sich – vermittelt über die Differenz zum alten Medium – des Neuen gewahr werde, was sie als *hypermediacy* beschreiben (vgl. ebd., 34). In dieser »double logic of remediation« (ebd., 55) nehmen Medien darüber hinaus stets aufeinander Bezug, ohne dabei zwangsläufig eine zeitlich lineare Genealogie zu bilden: Nicht nur neue Medien können ältere remediatisieren, auch ältere Medien können neuere remediatisieren (vgl. ebd.). Bolters und Grusins Modell der Remediation eignet sich damit nicht für eine historisierende Betrachtung von Medien, stellt aber in der Logik, dass Remediation »*the mediation of mediation*« ist, eine analytische Herangehensweise zur Verfügung, die es erlaubt, Mediatisierungsprozesse in den Blick zu nehmen, und Medien als interdependent zu verstehen: »Each act of mediation depends on other acts of mediation. Media are continually commenting on, reproducing, and replacing each other, and this process is integral to media. Media need each other in order to function as media at all.« (Ebd.) Ein ähnlicher Einsatz findet sich bei Krämer (2003, 85), die konstatiert: »Immer geht dem Medium etwas voraus; doch das, was ihm vorausgeht, ist zwar in einem anderen Medium, nie aber ohne Medium gegeben.« An dieser Stelle benennt Krämer das von ihr vertretene Programm als *Metaphysik der Medialität*, die als Gegenprogramm zu einer von einem Medienapriori ausgehenden Medienontologie fungiere.[5] Die Metaphysik sei keine universale, wie Krämer (ebd., 82) schreibt, da über Medialität nachzudenken auch heiße, über Perspektivität nachzudenken. So lässt sich Krämers Medialitätsbegriff an Haraways Konzept des *Situierten Wissens* anschließen (vgl. Haraway 1991a). Die Fokussierung auf Medialität ermöglicht es Krämer darüber hinaus, über die Performativität von Medien nachzudenken. Diese liege darin begründet, dass Medien Dinge erscheinen lassen, und dabei das, was erscheint, »zugleich transformiert, manchmal

5 Krämer betont, dass eine nicht-essentialistische Sichtweise auf Medien eine Medienontologie ausschließe. Dies scheint auf den ersten Blick ein Widerspruch zu Deuber-Mankowskys Überlegungen zur Medienontologie zu sein. Bei näherer Betrachtung erweisen sich die beiden Ansätze jedoch als demselben Erkenntnisinteresse verschrieben, denn Deuber-Mankowsky (2017a, 166) zufolge zeige sich die Existenz von Medien jenseits eines medialen Apriori »in den Effekten, die sie durch ihre Teilnahme an Werdensprozessen zeitigen.« Medien sind demnach nicht apriorisch ontologisch gesetzt, sondern ihre Existenz lässt sich genau in den Effekten ihrer Medialität in den mediatisierten Dingen erkennen.

auch unterminiert« (Krämer 2003, 83) werde. Die Performativität des Medialen ziele auf eine Beschäftigung mit diesem »Überschuss« (ebd.) ab, der in der medialen Hervorbringung entstehe, und sich damit als Eigenleistung des Mediums konzeptualisieren lässt. Mit Anja Michaelsen (2018, 112) lässt sich an dieser Stelle noch hinzufügen, dass gerade dieser durch die »Betonung des Medienspezifischen und Materiellen« in den Blick rückende »ästhetische[…], sinnliche[…] Überschuss« ein zentrales Anliegen medienwissenschaftlicher Analyse ist, und sich für Fragestellungen aus der Geschlechterforschung produktiv machen lässt. In diesem Sinne soll DuPonts Frage, was Kryptographie eigentlich ist, durch eine Fokussierung der prozessualen Dimension, *der Medialität*, von Ver- und Entschlüsselung diskutiert werden, die sich auch, wie in dieser Untersuchung deutlich werden wird, ausgehend von mathematischen, technischen, und historischen Quellen bestreiten lässt.

2.3 *Klassische* und *moderne* Kryptographie

Es gibt verschiedene Definitionen dessen, was Kryptographie ist, die zwar nicht über denselben Wortlaut verfügen, aber grundsätzlich dasselbe Prinzip beschreiben: Singh (2000, xiv) definiert Kryptographie als »art of secret communication«, und Kahn (1967, xiii) gibt keine direkte Definition, verweist aber darauf, dass »methods of cryptography […] do not conceal the presence of a secret message but render it unintelligible to outsiders«. Aus dem Feld der Kryptographie selbst kommen folgende Definitionen: Neal Koblitz (2007, 979) definiert Kryptographie als »science of transmitting and managing information in the presence of an adversary«. Bauer (1997, 27) schreibt: »Die klassische Aufgabe der Kryptographie ist es, eine Nachricht oder Aufzeichnung für den Unbefugten unverständlich zu machen.« Oded Goldreich (2004, 2, Herv. i.O.) spezifiziert: »The problem of providing *secret communication over insecure media* is the most traditional and basic problem of cryptography.« Whitfield Diffie und Martin Hellman (1976, 645) setzen Kryptographie als »the study of ›mathematical‹ systems for solving two kinds of security problems: privacy and authentication.« Christof Paar und Jan Pelzl (2016, 2, Herv. i.O.) konstatieren in ihrem Lehrbuch *Kryptografie Verständlich*: »Die **Kryptografie** beschäftigt sich mit der *Absicherung* von Daten, z.B. der Verschlüsselung von Nachrichten.« Etymologisch setzt sich das Wort *Kryptographie* aus dem griechischen *κρυπτός* (»kryptós«) für verborgen, heimlich, geheim und *-γραφία* (»-graphia«, von γράφειν, »gráphein«: kerben, (ein)ritzen, schreiben, zeichnen) zusammen

(vgl. Dudenredaktion 2020, 423, 634), und könnte wörtlich etwa als *Geheimschrift* ins Deutsche übertragen werden. Das *Oxford English Dictionary* (2011) definiert *cryptography* als »1. The art or practice of writing in code or cipher; the science of encryption; the branch of cryptology concerned with this (cf. cryptanalysis n.). More generally: the study of codes and ciphers; cryptology«, und »2. Coded writing; a particular code or cipher. Also *figurative*.« Alle diese kurzen Definitionen nennen Teilaspekte dessen, was Kryptographie leistet, die für ein besseres Verständnis an dieser Stelle zusammengezogen werden sollen. Kryptographie ist, soviel geht aus den bereits genannten Definitionen hervor, mit dem Verschlüsseln von Inhalten befasst, die entweder als Nachrichten, Informationen, oder einfach als Kommunikation bezeichnet werden (dazu später mehr). Die Verschlüsselung macht besagte Inhalte für unbefugte Leser_innen unverständlich, verbirgt aber nicht ihre Existenz.

Sowohl Bauer als auch Paar/Pelzl ordnen Kryptographie, ausgehend von ihrem Oberbegriff Kryptologie, mittels eines Baumdiagramms ein. Bauer (1997, 26) unterschiedet an der ersten Verzweigung des Baumes zwischen offenen und gedeckten Geheimschriften: Offene Geheimschriften definiert er als »eigentliche Kryptologie«, verdeckte als »Steganographie«. Aus dieser Differenz erklärt sich Kahns Bemerkung, dass Kryptographie eine Nachricht unlesbar mache, aber ihre Existenz nicht verstecke – letzteres ist die Aufgabe der Steganographie (vgl. ebd., 9).[6] Während Bauer das Baumdiagramm lediglich auf der Seite der Steganographie weiter ausführt, lässt sich für den Bereich der »eigentlichen Kryptologie« mit Paars und Pelzls (2016, 3) Baumdiagramm anschließen, die Kryptographie und Kryptanalyse als erste Verzweigung unter dem Oberbegriff Kryptologie benennen. Mit Bauer (1997, 25) sei an dieser Stelle noch darauf verwiesen, dass der Begriff *Kryptologie*, trotz sporadischer früherer Verwendung, erst durch Kahns *The Codebreakers* als Oberbegriff für *Kryptographie* und *Kryptanalyse* fest etabliert wurde. Die Aufteilung von Kryptologie in zwei komplementäre Bereiche entspricht auch der genau gegensätzlichen Aufgabenverteilung der beiden: Ist Kryptographie mit dem Verschlüsseln von Nachrichten befasst, so geht es in der Kryptanalyse um das »*Brechen* von Kryptosystemen« (Paar/Pelzl 2016, 2, Herv. i.O.). Entgegen der Annahme, dass Kryptanalyse vornehmlich von Kriminellen oder Geheimdiensten praktiziert würde, weisen Paar und Pelzl (ebd., 2–3) darauf hin, dass es sich bei der Kryptanalyse durchaus um eine wissenschaftliche Disziplin

6 Auf Steganographie wird in diesem Buch nicht genauer eingegangen. Für einen ausführlichen Überblick über steganographische Methoden siehe Bauer (1997, 9–25).

handelt, deren Ergebnisse für die Kryptographie unabdingbar seien, und dass die meisten Kryptanalyst_innen Wissenschaftler_innen seien. Der Status von Wissenschaftlichkeit ist tatsächlich, und das mag aus heutiger Perspektive überraschen, auch für die Kryptographie nicht selbstverständlich. Die Kryptographen Jonathan Katz und Yehuda Lindell (2008, 3) gehen auf diesen zweifelhaften Status zu Beginn ihres Buchs *Introduction to Modern Cryptography* genauer ein, in dem sie eine *modern cryptography* von einer *classical cryptography* abgrenzen:

> »The Concise Oxford Dictionary (2006) defines cryptography *as the art of writing or solving codes*. This definition may be historically accurate, but it does not capture the essence of modern cryptography. First, it focuses solely on the problem of secret communication. This is evidenced by the fact that the definition specifies ›codes‹, elsewhere defined as ›a system of pre-arranged signals, especially used to ensure secrecy in transmitting messages‹. Second, the definition refers to cryptography as an art form. Indeed, until the 20th century (and arguably until late in that century), cryptography was an art.«

Obgleich die Definition des *Concise Oxford Dictionary*, gegen die sich Katz und Lindell wenden, im bereits zitierten *Oxford English Dictionary* um den Aspekt der Wissenschaftlichkeit erweitert ist, benennt auch dasselbe Kryptographie zuvorderst als »art or practice of writing in code or cipher«. Katz und Lindell konstatieren, dass das Verständnis von Kryptographie als Kunst bis ins späte 20. Jahrhundert gerechtfertigt sei, da es kaum wissenschaftliche Theoriebildung und damit kein Feld gegeben habe.[7] Dies habe sich jedoch mit dem Aufkommen *moderner Kryptographie*, das Katz und Lindell (ebd., Herv. i.O.) auf die 1980er Jahre datieren, verändert: »A rich theory emerged, enabling the rigorous study of cryptography as a *science*.« Anhand des Worts »rigorous«, das in Katz' und Lindells Buch noch sehr oft in beschreibender Funktion für die Genauigkeit von Methoden Verwendung findet, wird deutlich, dass die beiden Autoren die Wissenschaftlichkeit von Kryptographie nicht nur an

7 Ein ähnliches Argument macht auch Kahn (1967, 72), der darauf hinweist, dass die Entwicklung der Kryptologie in den ersten 3000 Jahren ihrer Geschichte schleppend und nicht linear verlaufen sei: »In its first 3,000 years, it did not grow steadily. Cryptology arose independently in many places, and in most of them it died the deaths of its civilizations. In other places, it survived, embedded in a literature, and from this the next generation could climb to higher levels. But progress was slow and jerky. More was lost than retained. Much of the history of cryptology of this time is a patchwork, a crazy quilt of unrelated items, sprouting, flourishing, withering.«

Theoriebildung, sondern vor allem an der Ausbildung von strengen Definitionen und Methoden festmachen. Kennzeichnend für die *moderne Kryptographie* ist Katz und Lindell folgend darüber hinaus ihr erweitertes Anwendungsgebiet: Moderne Kryptographie ist nun nicht mehr auf die Geheimhaltung von Nachrichten, und damit auf Kommunikationsakte beschränkt, sondern »deals with the problems of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash and more« (ebd.). Diese Entgrenzung, die im Folgenden aus mediengeschichtlicher Sicht als maßgeblich mit der Entstehung des Internets zusammenhängend beschrieben werden kann, bringt auch eine erweiterte Nutzer_innenschaft mit sich und löst die Kryptographie aus ihrer vormals ausschließlich militärisch diskursivierten Geschichte. Gleichsam ist diese Entgrenzung an der Verschmelzung von Kryptographie und Informatik beteiligt, und damit an der Herausbildung von IT-Sicherheit als wissenschaftliche Disziplin. »Without attempting to provide a perfect definition of modern cryptography,« schreiben Katz und Lindell (ebd.), »we would say that it is *the scientific study of techniques for securing digital information, transactions, and distributed computations.*« Im Folgenden sollen die mediengeschichtlichen Entwicklungen betrachtet werden, die diese Verschiebung ermöglichten, sowie anhand konkreter Beispiele auf die Medialität kryptographischer Verfahren eingegangen werden.

2.4 Zwei Schlüsselprobleme der Kryptographie

1976 veröffentlichten Whitfield Diffie und Martin Hellman ein Paper mit dem Titel *New Directions in Cryptography*. Eines der Hauptprobleme, für das Diffie und Hellman (1976, 644) in ihrem Aufsatz eine Lösung anbieten, ist das Problem der Schlüsselverteilung, oder genauer: »the need for secure key distribution channels«. Singh (2000, 251) folgend, gingen Diffie und Hellman damit eines der Grundprobleme der Kryptographie an, denn, so formuliert er pointiert, »[t]he problem of key distribution has plagued cryptographers throughout history.« Der Einfluss des Aufsatzes von Diffie und Hellman auf die Entwicklung der Kryptographie als Forschungsfeld kann kaum überschätzt werden, legt er doch den Grundstein für die sogenannte *asymmetrische*

Kryptographie,[8] die damit von der sogenannten *symmetrischen* Kryptographie abgegrenzt werden kann, und darüber hinaus formativ ist für das, was Katz und Lindell als *moderne Kryptographie* definieren.[9] Wie die Unterscheidung von symmetrischer und asymmetrischer Kryptographie möglich wurde, wird im Folgenden nach einem Überblick über die Grundbegriffe des Feldes anhand von zwei – im doppelten Sinne des Wortes zu verstehenden – Schlüsselproblemen der Kryptographie entfaltet werden: Erstens anhand der Trennung von Schlüssel und Verschlüsselungsverfahren, die als das *Kerckhoffs'sche Prinzip* kanonisch geworden ist, und zweitens anhand der Lösung des Problems der Schlüsselverteilung durch asymmetrische Kryptographie.

2.4.1 Grundbegriffe der Kryptographie

Schematisch betrachtet, besteht ein Verschlüsselungsverfahren aus mehreren Elementen: Einer zu verschlüsselnden Nachricht im Klartext (*Plaintext*), einer Verschlüsselungsmethode, d.h. ein Algorithmus,[10] und einem Schlüssel, der

8 Wie zu Anfang des Kapitels bemerkt, riskiert eine Geschichte der Kryptographie aufgrund der mit ihr verbundenen Geheimhaltungspraktiken, nicht alle Ereignisse und Akteur_innen zu kennen. Ein Beispiel dafür ist die Geschichte der asymmetrischen Kryptographie, die – nach heutigem Kenntnisstand – zweimal erfunden wurde: Das erste Mal Ende der 1960er/Anfang der 1970er Jahre durch James Ellis, Clifford Cocks und Malcolm Williamson. Da die drei zum damaligen Zeitpunkt Angestellte des britischen Geheimdienstes GCHQ waren, blieb ihre Erfindung bis zum Ende des 20. Jahrhunderts geheim. Singh (2000, xvii, 279–280) verweist darauf, dass die entsprechenden Informationen erst kurz vor der Publikation seines Buches freigegeben wurden, und auch seine Wiedergabe der Ereignisse ist gekennzeichnet von weißen Flecken, da noch nicht alle Teile dieser Geschichte für die Öffentlichkeit frei zugänglich sind (vgl. ebd., 284). Ein zweites Mal wurde asymmetrische Kryptographie nur kurze Zeit später von Whitfield Diffie und Martin Hellman erfunden – diesmal im Licht der Öffentlichkeit. Aufgrund der besseren Quellenlage wird im weiteren Verlauf ausschließlich auf Diffie und Hellmans Arbeit Bezug genommen.

9 Aus Gründen der Verständlichkeit wird in der vorliegenden Untersuchung nicht diskutiert, welche Neuerungen auf dem Gebiet symmetrischer Kryptographie für die *moderne Kryptographie* grundlegend sind. Weiterführend dazu siehe Shafi Goldwasser und Silvio Micali (1984; 1982).

10 Ein Algorithmus lässt sich basal als eine präzise definierte Abfolge von Handlungsschritten verstehen. Ein Alltagsbeispiel wäre das Befolgen eines Kochrezepts: Alle Zutaten müssen in der richtigen Menge und zum richtigen Zeitpunkt für die korrekte Dauer in den Topf gegeben werden. Je nachdem, an wen oder was ein Algorithmus sich richtet, sind unterschiedliche Grade an Präzision notwendig: Während Menschen

die Details der Verschlüsselung bestimmt (vgl. Singh 2000, 11). Anhand eines einfachen Beispiels lässt sich dies veranschaulichen: Eine Nachricht soll verschlüsselt werden. Die gewählte Verschlüsselungsmethode ist die Cäsar-Chiffre *(Caesar shift cipher)*,[11] die darin besteht, alle Buchstaben des Plaintext[12] um eine bestimmte Anzahl an Stellen im Alphabet zu verschieben und den Plaintext so in einen verschlüsselten *Ciphertext* zu verwandeln. Der Schlüssel bestimmt die Anzahl der Stellen, um die die Buchstaben verschoben werden, sowie die Richtung der Verschiebung. Bei der Cäsar-Chiffre werden alle Buchstaben des Plaintext um drei Stellen nach hinten verschoben, sodass a durch D, b durch E, c durch F ersetzt wird und so fort. Bolters und Grusins Konzept der Remediatisierung folgend lässt sich an dieser Stelle der Verschlüsselungsvorgang als Remediatisierungsvorgang beschreiben, und ein Ciphertext damit als remediatisierter Plaintext.

Die Cäsar-Chiffre ist verhältnismäßig leicht zu brechen: Wird eine solche verschlüsselte Nachricht abgefangen, und ist das verwendete Verfahren bekannt, so müssen bei einem Alphabet mit 26 Buchstaben maximal 25 Kombinationen ausprobiert werden, bis der Ciphertext wieder in den Plaintext verwandelt werden kann. Eine ähnliche Verschlüsselungsmethode aus dem Bereich der monoalphabetischen Substitutionschiffren, bei der im Unterschied zur *shift cipher* die Reihenfolge des Alphabets nicht gewahrt bleiben muss, und die Buchstaben des Plaintext im Ciphertext durch beliebige andere Buchstaben des Alphabets ersetzt werden (einzige Bedingung: die Ersetzung darf innerhalb eines jeweiligen Textes nicht changieren), ist schon wesentlich schwerer zu entschlüsseln: Selbst wenn bekannt ist, dass es sich um eine Substitutionschiffre handelt, so bedeutet dies bei einem Alphabet mit 26 Buchstaben 26! (lies: »26 Fakultät«) Kombinationsmöglichkeiten –

---

in der Regel mit unpräzisen Algorithmen umgehen können (auch angesichts fehlender Zutaten oder einer etwas zu hohen Temperatur können sie ein Gericht fertigkochen), sind Computer nicht dazu in der Lage, eine ungenau formulierte Handlungsanweisung auszuführen (vgl. Cormen 2013, 1).

11 Tatsächlich ist diese Chiffre nach ihrem prominentesten Nutzer und Erfinder, Julius Cäsar, benannt (vgl. Singh 2000, 9–10) und fällt in die Kategorie der monoalphabetischen Substitutionschiffren. Chiffrieren bezieht sich auf das Austauschen einzelner Buchstaben, während codieren das Austauschen ganzer Wörter bezeichnet (vgl. ebd., 30).

12 Der zu verschlüsselnde Plaintext wird im Folgenden stets klein geschrieben, der verschlüsselte Ciphertext hingegen in Großbuchstaben.

ausgeschrieben sind das über 400.000.000.000.000.000.000.000.000 Kombinationsmöglichkeiten (vgl. ebd.). Nun könnte man darauf schließen, dass daraus zu folgen habe, dass es größeren Schutz vor Entschlüsselung böte, das verwendete Verfahren geheim zu halten, doch dem ist nicht so.[13] Das sture Durchprobieren von Kombinationen scheidet angesichts von 26! Kombinationsmöglichkeiten (vor allem, ohne auf Computer zurückgreifen zu können) zwar als Entschlüsselungsmethode aus, wodurch die monoalphabetische Substitutionschiffre in der westlichen Welt lange für absolut sicher gehalten wurde. Doch zufälliges Ausprobieren von Möglichkeiten ist nicht die einzige Methode der Kryptanalyse, die auf einen Ciphertext anwendbar ist. Der arabische Gelehrte Abū Ya'qūb ibn Ishāq al-Kindī erfand ca. im 9. Jahrhundert[14] ein kryptanalytisches Verfahren, das heute unter dem Namen *Frequenzanalyse* bekannt ist, und dessen Grundprinzip darin besteht, Annahmen über den Plaintext zu treffen, die zu dessen Entschlüsselung dienlich sein könnten. Al-Kindīs Methode besteht darin, die Vorkommnisse der Buchstaben (oder Symbole) eines Ciphertexts zu zählen. Der Buchstabe, der am häufigsten vorkommt, muss dem Buchstaben entsprechen, der in der Sprache des Plaintexts statistisch gesehen am häufigsten verwendet wird (vgl. ebd., 17–19). Ist der Plaintext auf Deutsch verfasst, entspräche dies einem e, das mit ca. 17 % der am häufigsten verwendete Buchstabe des Alphabets ist, gefolgt von dem Buchstaben n mit einer Häufigkeit von ca. 10 % (vgl. Paar/Pelzl 2016, 9). Al-Kindī weist ebenfalls darauf hin, dass Texte auch in ihrem Ausdruck und ihrer Form gewissen Regelhaftigkeiten gehorchen, d.h. dass sie beispielsweise je nach Textgattung mit einer bestimmten Formulierung beginnen, was für die Entschlüsselung hilfreich sein kann (vgl. Mrayati et al. 2003, 82). Je länger ein Ciphertext ist, desto besser funktioniert diese Methode, vorausgesetzt, dass er nicht in verschiedenen Sprachen verfasst ist, die Rechtschreibregeln eingehalten, sowie keine gezielten Maßnahmen ergriffen wurden, um eine Frequenzanalyse zu umgehen, wie beispielsweise Wörter, die den Buchstaben e enthalten, komplett zu vermeiden (vgl. Singh 2000, 19–20).

13 Der Versuch, Sicherheit durch die Geheimhaltung des Verfahrens zu erzielen, wird als *security by obscurity* bezeichnet und generell als untauglich angesehen (vgl. Paar/Pelzl 2016, 12).

14 Al-Kindīs Manuskript wurde erst im Jahr 1987 wiederentdeckt, das genaue Datum der Publikation ist unbekannt (vgl. Singh 2000, 17). 2003 erschien erstmals eine englischsprachige und kommentierte Übersetzung von al-Kindīs Manuskript (vgl. Mrayati et al. 2003).

Europa sollte erst einige Jahrhunderte nach al-Kindīs Erfindung von der Frequenzanalyse erfahren: Im Mittelalter befassten sich hauptsächlich Mönche mit Kryptographie, oder vielmehr mit Kryptanalyse, als sie Teile des Alten Testaments dechiffrierten, die mit der hebräischen Substitutionschiffre *Atbasch*[15] verschlüsselt waren, und auch neue Chiffren erfanden (vgl. ebd., 26). Sukzessive fand die Kryptographie ihren Weg aus den Klöstern hinaus, und wurde im 14. Jahrhundert in Wissenschaft und Alchemie verwendet (vgl. ebd., 27). Im 15. Jahrhundert, beflügelt durch die Wiederbelebung der Künste und Wissenschaften in der Renaissance, sowie dem dazugehörigen politischen Klima, in dem viele unabhängige Stadtstaaten sich gegenseitig Diplomaten sandten, wurde Kryptographie in der westlichen Welt zu einer »burgeoning industry« (ebd.). Gleichzeitig erfuhr auch die Kryptanalyse verstärkte Aufmerksamkeit. Singh (ebd., 27–28) weist darauf hin, dass es zwar möglich sei, dass die Frequenzanalyse in Europa unabhängig von al-Kindīs Methode erfunden wurde, schätzt es aber als ebenso wahrscheinlich ein, dass das Wissen aus der arabischen Kultur übernommen wurde. Während in den folgenden Jahrhunderten zwar immer neue Verschlüsselungsverfahren erfunden wurden (beispielsweise der Nomenklator oder die Vignère-Chiffre), so war doch mit der Brechung der monoalphabetischen Substitutionschiffre durch die Methode der Frequenzanalyse deutlich geworden, dass eine Verschlüsselung auch gebrochen werden kann, ohne dass der Entschlüsselungsalgorithmus einer Umkehrung des Verschlüsselungsalgorithmus folgt, wenn vom Plaintext Rückschlüsse auf den Ciphertext gezogen werden können. Die Unabhängigkeit der Kryptanalyse von den intendierten Verfahren zur Entschlüsselung, sowie ihre generelle Bedeutung für die Erfindung neuer kryptographischer Verfahren sollte sich in den folgenden Jahrhunderten mit weiteren Schwerpunkten fortsetzen.

2.4.2 Erstes Schlüsselproblem: Das Kerckhoffs'sche Prinzip

1883 publizierte der niederländische Linguist Auguste Kerckhoffs den für das Feld der modernen Kryptographie kanonisch gewordenen Text *La Cryptographie Militaire*.[16] Kerckhoffs (1883, 8) stellt sechs Prinzipien vor, denen militäri-

15 Die Atbasch-Chiffre ersetzt den ersten Buchstaben des Alphabets durch den letzten, den zweiten durch den vorletzten etc. (vgl. Singh 2000, 26).

16 Kerckhoffs ist außer für dieses kanonische Werk bekannt für seine Begeisterung für und seine Verdienste um die artifizielle Sprache *Volapük*, und hat nach dem Erscheinen von *La Cryptographie Militaire* extensiv zu dieser publiziert, bis er sich mit Johann Martin Schleyer, dem Erfinder von Volapük, über die Ausrichtung der Kunstsprache

sche Kryptographie zu folgen habe, und leitet diese mit einer Unterscheidung von verschlüsselter brieflicher Kommunikation zwischen Einzelpersonen und verschlüsselter militärischer Kommunikation per Telegraphie, beispielsweise zwischen Befehlshabern einer Armee, ein:

> »Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux.«[17]

Über diesen Satz schreibt Kahn (1967, 234): »This clear recognition of the new order constitutes Kerckhoffs' first great contribution to cryptology.« Was Kahn als »new order« bezeichnet, worauf er aber nicht konkreter eingeht, ist der von Kerckhoffs ebenfalls nur flüchtig erwähnte, aber doch als signifikant bestimmte Medienwechsel vom Brief zur Telegraphie. Ungefähr hundert Jahre vor dem Erschienen von *La Cryptographie Militaire* begann in Frankreich der Ausbau des optischen Telegraphennetzes (vgl. Flichy 1994, 55). Mit diesem neuen Medium veränderte sich die Übertragungsgeschwindigkeit von Nachrichten: Verdoppelte sich gegen Ende des 19. Jahrhunderts bereits durch den Ausbau des Straßennetzes die Transportgeschwindigkeit von Briefen, so amplifizierte die optische Telegraphie diesen Prozess um ein Vielfaches, und die Übertragung einer Nachricht von Paris nach Valenciennes (ca. 190 km Luftlinie) dauerte nur noch ca. 15 Minuten (vgl. ebd.). Doch mit der optischen Telegraphie kam noch eine weitere Neuerung: Die Notwendigkeit, die übertragenen Nachrichten mittels eines standardisierten Verfahrens zu kodieren. Dies sicherte die Geheimhaltung der übermittelten Nachrichten, und beschleunigte darüber hinaus die Nachrichtenübertragung noch weiter (vgl. ebd., 58). In der ersten Hälfte des 19. Jahrhunderts schritt die Entwicklung der elektrischen Telegraphie voran, die abermals eine starke Erhöhung der Übertragungsgeschwindigkeit zur Folge hatte. Im »für die Entstehung des optischen wie auch des elektrischen Telegraphen charakteristische[n]

überwarf: Während Schleyer Volapük zu einer möglichst umfassenden Form bringen wollte, die zugleich ihre Künstlichkeit verschleiern sollte, wollte Kerckhoffs die Sprache verschlanken und vereinfachen (vgl. Kahn 1967, 232; Andreas 2014, 160).

17 »Es sollte zwischen einem Chiffriersystem, das für einen momentanen Briefwechsel zwischen einigen wenigen isolierten Personen gedacht ist, und einer Methode der Kryptographie, die dazu bestimmt ist, auf unbegrenzte Zeit die Korrespondenz verschiedener Heerführer untereinander zu regeln, unterschieden werden.« Übersetzung MS.

Anspruch, ein weltumspannendes Netz zu errichten« (ebd., 72), lag auch die Notwendigkeit für die Standardisierung des Systems, sowie der zu übertragenden Daten, sodass Mitte des 19. Jahrhunderts das Morse-Alphabet für die Chiffrierung[18] der zu übertragenden Nachrichten verwendet wurde. Doch zurück zu Kerckhoffs: Im Falle von telegraphiegestützter militärischer Kommunikation, so bemerkt dieser, gebe es zwei Dinge, die besondere Beachtung finden müssen. Zum einen sei es nicht möglich, die Vereinbarungen der verschlüsselten Kommunikation, d.h. die Verschlüsselungsmethode, spontan nach Belieben zu ändern. (Dies wäre unter Umständen zwischen zwei per Brief kommunizierenden Parteien möglich, jedoch nicht innerhalb eines Systems, in dem eine Person konstant mit vielen anderen kommuniziert.) Zum anderen müsse man damit rechnen, dass Soldaten gefangen genommen würden; daher dürften diese keine Informationen bei sich tragen, die den Feinden das Brechen der verwendeten Verschlüsselung erleichtern könnten (vgl. Kerckhoffs 1883, 8). Basierend auf diesen beiden Einschränkungen formuliert Kerckhoffs (ebd.) sechs Prinzipien militärischer Kryptographie:

1. Ein kryptographisches System sollte, wenn auch nicht theoretisch, dann wenigstens praktisch nicht zu brechen sein;
2. ein kompromittiertes System sollte keine Gefahr für die kommunizierenden Parteien darstellen;
3. der Schlüssel sollte einfach memorierbar sein (spezifisch: ohne dass er notiert werden muss), sowie einfach auszutauschen;
4. die verschlüsselte Nachricht muss telegraphisch übertragbar sein;
5. die Verschlüsselungsmethode sowie die dazugehörigen Dokumente sollten portabel sowie von einer Person allein verwendbar sein;
6. das kryptographische System sollte einfach zu bedienen sein und nicht viel Vorkenntnisse erfordern.

Kahn (1967, 235) evaluiert: »[A]ny modern cryptographer would be very happy if any cipher fulfilled all six. Of course, it has never been possible to do that.« Dies führt Kahn darauf zurück, dass die Forderungen zueinander inkompatibel seien, und schreibt weiter, dass in der Regel die erste Forderung geopfert werde. (Dies wird sich wenige Jahre nach Kahns Publikation verändert haben,

18 Gemeinhin wird von *Morse-Code* gesprochen, doch mit Singhs (2000, 30) Distinktion von Chiffrieren (Austausch einzelner Buchstaben) und Codieren (Austausch ganzer Wörter) muss hier korrekterweise von Morse-Chiffrierung gesprochen werden.

doch dazu später mehr.) Die erste Forderung ist jedoch, so könnte man sagen, der Grundgedanke der Kryptographie: Kerckhoffs beweist an dieser Stelle sein Wissen um die Frequenzanalyse, mittels derer die monoalphabetische Substitutionschiffre, die theoretisch nicht zu brechen schien, praktisch dennoch zu entschlüsseln war – ein Szenario, das sich bestenfalls nicht wiederholen sollte. Die fünfte und sechste Forderung Kerckhoffs nach Portabilität sowie Einfachheit in der Verwendung lassen sich mit heutigem Vokabular als Forderungen nach Usability beschrieben, und zeugen von Kerckhoffs' Umsichtigkeit.[19] Nicht ganz so selbsterklärend sind die zweite bis vierte Forderung, auf die an dieser Stelle genauer eingegangen werden soll.

Die vierte Forderung, dass die verschlüsselte Nachricht telegraphisch übertragbar bleiben muss, ist ein medienspezifisches Argument, das quer zu der Geschichte der Kryptographie verläuft, und ein Umdenken erforderlich macht: Historisch betrachtet war Kryptographie, da sie mit der Verschlüsselung von Plaintext befasst ist, notwendigerweise am Medium Schrift orientiert. Darüber hinaus waren allerdings oftmals auch die jeweiligen Trägermedien einer Nachricht von Bedeutung für das verwendete kryptographische Verfahren. Dies lässt sich anhand der auf das fünfte Jahrhundert v. Chr. datierten *Skytale* verdeutlichen, dem ältesten bekannten Gerät, das für militärische Kryptographie eingesetzt wurde. Die Skytale ist ein hölzerner Stab, der eng mit einem dünnen Streifen Pergament oder Leder umwickelt wurde. Die Nachricht wurde längs auf den umwickelten Stab geschrieben, und anschließend wurde der Lederstreifen abgewickelt und zum_zur Empfänger_in transportiert. Auf dem abgewickelten Lederstreifen ist lediglich eine scheinbar zufällige Aneinanderreihung von Buchstaben sichtbar. Um die Nachricht zu entschlüsseln, muss sie erneut auf einen Stab desselben Durchmessers aufgewickelt werden (vgl. Singh 2000, 8–9). Die Integrität des physischen Trägermediums, also von Stab und Lederstreifen, ist von

19 Ab Mitte der 1970er Jahre formierte sich unter dem Namen *Usable Privacy and Security* ein Teilbereich der IT-Sicherheitsforschung, der sich explizit mit der Usability kryptographischer Anwendungen befasst. Zentrales Anliegen von *Usable Privacy and Security* ist die Vereinfachung der Anwendung kryptographischer Verfahren, sodass User_innen diese tatsächlich verwenden (können), und nicht aus Unkenntnis oder Bequemlichkeit umgehen (vgl. Garfinkel/Lipford 2014). Kennzeichnend für diesen Ansatz ist die Rehabilitierung von User_innen, die nicht mehr als (zusätzliches) Sicherheitsproblem betrachtet werden sollen, und die Verlagerung der Verantwortung für die (korrekte) Anwendung von Sicherheitsmechanismen auf Designer_innen (vgl. Adams/Sasse 1999).

elementarer Bedeutung: Verändert sich der Abstand zwischen den Buchstaben, oder wird ein dickerer oder dünnerer Stab verwendet, so lässt sich die Nachricht nicht mehr entschlüsseln. Obgleich dieses Beispiel sehr alt ist, so waren kryptographische Methoden, die auf den physischen Eigenschaften ihrer Trägermedien basierten, auch noch zu Kerckhoffs' Zeit im Einsatz. Ein Beispiel dafür ist die Fleissner-Scheibe,[20] die, ebenso wie die Skytale, das kryptographische Prinzip der Transposition verwendet, bei der der Plaintext nicht durch die Substitution einzelner Buchstaben, sondern durch deren Anordnung in einen Ciphertext verwandelt wird (vgl. Bauer 1997, 93). Die Fleissner-Scheibe ist eine metallene quadratische Scheibe mit quadratischen Aussparungen, in die jeweils einzelne Buchstaben eines Plaintexts geschrieben werden. Sind alle Felder voll, so wird die Scheibe um 90 Grad gedreht, und erneut wird weitergeschrieben, bis alle Felder ausgefüllt sind. Nach insgesamt vier Durchgängen ist ein quadratisch angeordneter Buchstabenblock entstanden, der am Stück gelesen keinen Sinn ergibt, aber durch die Linse des Drehrasters seine Nachricht offenbart.[21] Auch hier ist die Form/atierung der Nachricht, die kennzeichnend für die Medialität des kryptographischen Verfahrens ist, für die Ver- und Entschlüsselung entscheidend. Ähnlich wie bei dem Transport des Lederriemens der Skytale wird auch die Form des mittels Fleissner-Scheibe verschlüsselten Textblocks während des Transports gewahrt. Erführe die verschlüsselte Nachricht durch den Transport eine Remediatisierung, so müsste für die Entschlüsselung dieser eine Anleitung beiliegen, um den bei dem_der Empfänger_in angekommenen Nachrichteninhalt erneut in die mediale Ausgangsform zu überführen, da diese Teil der Verschlüsselung ist. Dies wäre, vor allem in einer Kriegssituation aufgrund des zeitlichen Mehraufwands und einer erhöhten Fehleranfälligkeit nicht praktikabel. Die Forderung nach telegraphischer Übertragbarkeit, mit der die

20 Bauer (1997, 95) weist darauf hin, dass diese Verschlüsselungsmethode bereits im Jahr 1745 nachgewiesen werden konnte, aber aus Unkenntnis des genauen Ursprungs dem österreichischen Oberst Eduard Fleissner zugeschrieben wird, der diese Methode in seinem 1881 verlegten *Handbuch der Kryptographie* erläutert.

21 An dieser Stelle wird die Nähe der Fleissner-Scheibe zu steganographischen Verfahren deutlich, wie beispielsweise zu der auf den italienischen Philosophen und Mathematiker Gerolamo Cardano zurückgehenden Raster-Methode. Cardanos Methode basierte darauf, eine mittels einer Schablone angeordnete Nachricht mit weiterem Text (beispielsweise einem Gedicht) zu umgeben, um ihre Existenz zu verschleiern. Nur wer eine passgenaue Schablone anlegt, kann die versteckte Nachricht sehen (vgl. Bauer 1997, 23–24).

Trennung von Verschlüsselungsleistung und Form/atierung einhergeht, ist also ein Argument über die Medialität von Kryptographie.

Auch Kerckhoffs zweite Forderung ist voraussetzungsreich: Wie kann ein kompromittiertes System kein Problem für verschlüsselte Kommunikation, also geheimzuhaltende Inhalte sein? Kerckhoffs (1883, 9–10) führt aus:

> »Quant à la nécessité du secret, qui, à mes yeux, constitue le principal défaut de tous nos systèmes de cryptographie, je ferai observer qu'elle restreint en quelque sorte l'emploi de la correspondance chiffrée aux seuls commandants en chef. Et ici j'entends par secret, non la clef proprement dite, mais ce qui constitue la partie matérielle du système : tableaux, dictionnaires ou appareils mécaniques quelconques qui doivent en permettre l'application. En effet, il n'est pas nécessaire de se créer des fantômes imaginaires et de mettre en suspicion l'incorruptibilité des employés ou agents subalternes, pour comprendre que, si un système exigeant le secret se trouvait entre les mains d'un trop grand nombre d'individus, il pourrait être compromis à chaque engagement auquel l'un ou l'autre d'entre eux prendrait part. Rien qu'à ce point de vue il y aurait lieu de condamner l'emploi du dictionnaire chiffré, qui est en usage aujourd'hui dans l'armée.«[22]

Mit dem *système* sind also alle Bestandteile eines kryptographischen Systems gemeint außer dem Schlüssel selbst: Tabellen (wie sie beispielsweise für Substitutionschiffren verwendet werden), Kodierungswörterbücher (gegen die Kerckhoffs sich im Besonderen ausspricht), oder mechanische Geräte (wie beispielsweise die Fleissner-Scheibe). Kerckhoffs ist aus rein praktischer Perspektive beizupflichten: Je mehr Glieder die Kette von Ver- und Entschlüsselung hat, je mehr Materialien geheim zu halten, und je mehr Menschen

22 »Was die Notwendigkeit der Geheimhaltung angeht, die in meinen Augen das größte Manko all unserer kryptographischen Systeme ist, möchte ich darauf hinweisen, dass sie die Verwendung verschlüsselter Korrespondenz in gewisser Weise auf die Oberbefehlshaber beschränkt. Und hier meine ich mit Geheimhaltung nicht den Schlüssel selbst, sondern das, was den materiellen Teil des Systems ausmacht: Tabellen, Wörterbücher oder mechanische Geräte, die die Verwendung des Schlüssels ermöglichen. In der Tat ist es nicht notwendig, imaginäre Geister zu erschaffen und die Unbestechlichkeit untergeordneter Mitarbeiter oder Agenten in Frage zu stellen, um zu verstehen, dass ein System, das Geheimhaltung erfordert, und in den Händen zu vieler Individuen liegt, bei jedem Einsatz, an dem einer von ihnen teilnimmt, kompromittiert werden könnte. Allein unter diesem Gesichtspunkt ist die Verwendung des verschlüsselten Wörterbuchs, wie es heute im Militär im Einsatz ist, zu verurteilen.« Übersetzung MS.

an diesem Prozess beteiligt sind, desto mehr Schwachstellen hat diese Kette auch. Diese Erkenntnis resultiert für Kerckhoffs jedoch nicht darin, alle Materialien und Menschen aus dieser Kette auszuschließen, wobei er schon auf eine Reduktion drängt (siehe Forderung 5), sondern darin, erstmals in der Geschichte der Kryptographie das kryptographische System, die Verschlüsselungsmethode, explizit vom Schlüssel zu trennen (vgl. Kahn 1967, 235), verbunden mit dem Anspruch, dass die Bekanntheit des kryptographischen Verfahrens nicht dazu führen dürfe, dass die Verschlüsselung gebrochen sei. Dies schließt bestimmte kryptographische Verfahren aus, wie beispielsweise Code-Wörterbücher oder auch Fleissner-Scheiben, da die Trennung von Verfahren und Schlüssel bei diesen nicht gegeben ist. Zusammengenommen mit der dritten Forderung danach, dass der Schlüssel so leicht zu merken sein müsse, dass er nicht notiert werden muss (wodurch er erneut Teil des *système* werden würde), bilden diese Forderungen den Kern dessen, was heute als Kerckhoffs'sches Prinzip kanonisch geworden ist, und dessen zeitgenössische Formulierung folgendermaßen lautet:

> »Ein [sic!] kryptografische Lösung muss auch dann noch sicher sein, wenn der Angreifer alle Details des Kryptosystems kennt, mit der Ausnahme des Schlüssels. Insbesondere muss das Verfahren auch dann sicher sein, wenn dem Angreifer der Ver- und Entschlüsselungsalgorithmus bekannt sind.« (Paar/Pelzl 2016, 12)

Die Essenz des Kerckhoffs'schen Prinzips ist damit nichts Geringeres als eine doppelte Modularisierung der Kryptographie: Einerseits durch die Trennung von Verfahren und Schlüssel, andererseits durch die Trennung von Verschlüsselung und Form. Mit Krämer (2003, 82) lässt sich an dieser Stelle von der erkenntnisinteressenabhängigen Unterscheidung von Form und Medium Gebrauch machen: Verschlüsselung als Medium nach Kerckhoffs wird getrennt von einer spezifischen Form, insofern diese Form nicht mehr Teil der Verschlüsselungsleistung sein darf, und zugunsten einer scheinbaren Formlosigkeit vernachlässigt werden muss. Diese beiden Modularisierungen konstituieren sich wechselseitig, da sich nicht argumentieren lässt, welche die jeweils andere bedingt. Die Verwendung einer kryptographischen Methode wie beispielsweise der Transposition, die nah an der Steganographie liegt, und bei der die Form, oder vielmehr die Formatierung des Ciphertexts Teil der Verschlüsselungsleistung und damit der Remediatisierung des Plaintexts ist, fällt damit kategorisch aus. Kerckhoffs' Forderung, die elektronische Telegraphie solle der standardisierte Übertragungsweg militärischer

Kryptographie sein, argumentiert so für grundsätzliche und barrierearme Remediatisierbarkeit verschlüsselter militärischer Kommunikation über den Remediatisierungsvorgang der Verschlüsselung hinaus. Der Medienwechsel – und damit auch Materialitätswechsel – verschlüsselter Kommunikation von Schrift auf Papier zu elektronischen Signalen und wieder zurück soll Teil militärischer Kryptographie werden. Dies kann nur durch eine Regulierung der Medialität von Kryptographie selbst gelingen: Der Vernachlässigung einer spezifischen Anordnung, Form und Materialität des Ciphertexts als Ergebnis der Verschlüsselung zugunsten einer Verschlüsselungsmethode, deren Remediatisierung des Plaintexts sich ausschließlich auf eine basale Variante des Mediums Schrift bezieht und in diesem verbleibt, und deren Ergebnis daher erneut durch die Telegraphie remediatisiert werden kann, ohne an Sicherheit zu verlieren.

Die Geschichte der Kryptologie ist jedoch, wie Mediengeschichte so oft, keine lineare Fortschrittsgeschichte: So wurden die von Kerckhoffs formulierten Forderungen bereits im Zweiten Weltkrieg von den Deutschen nicht konsequent beachtet. Die Verwendung der Chiffriermaschine Enigma war, wie Friedrich Bauer und Dominik Landwehr ausführen, von einigen »Dummheiten der Deutschen« (Bauer 1997, 200), oder anders formuliert: durch »[s]ystematische und wiederholt begangene Fehler auf der Seite Deutschlands und der Achsenmächte« (Landwehr 2008, 49) geprägt, was schlussendlich zu der erfolgreichen Kryptanalyse seitens der Briten führte. Da Landwehr in *Mythos Enigma. Die Chiffriermaschine als Sammler- und Medienobjekt* vor allem auf die Automatisierung von Ver- und Entschlüsselung eingeht und darlegt, wie durch die kryptanalytischen Unternehmungen der Polen und schließlich der Briten in Bletchley Park die Mathematik zur »Königsdisziplin in der Kryptografie, respektive in der Kryptoanalyse« (ebd., 57) avancierte, werde ich an dieser Stelle auf eine detaillierte Wiedergabe dieser Ereignisse verzichten. Stattdessen möchte ich als kurze Ergänzung zu Landwehrs ansonsten sehr ausführlichen Untersuchung einen Aspekt beleuchten, den Landwehr ausgespart hat, und kursorisch darlegen, inwiefern die Verwendung der Chiffriermaschine Enigma den Kerckhoffs'schen Forderungen widersprach. Auf die Ähnlichkeit der Enigma zur Schreibmaschine ist bereits Friedrich Kittler ausführlich eingegangen. Kittler (1986, 364) bemerkt, die Enigma habe mit ihrer »Maschinenmathematik Kryptographen von ihrer Handarbeit« erlöst – und während das für die Kryptograph_innen sicher stimmt, so gilt es nicht für alle am Prozess der Entschlüsselung beteiligten Personen. Die Enigma konnte im Gegensatz zur Schreibmaschine kein Papier bedrucken, was dazu

führte, dass für eine schnelle Verwendung drei Personen notwendig waren, »one to read the incoming text and press the keys, one to call out the letters in a loud voice as they lit up, one to write down the text« (Kahn 1967, 422), womit bereits der fünften Forderung Kerckhoffs widersprochen wurde. Auch die dritte Forderung, der Schlüssel solle einfach memorierbar sein, wurde nicht eingelöst – dies lag auch daran, dass die Deutschen, um die Sicherheit der Verschlüsselung zu erhöhen, drei verschiedene Schlüssel verwendeten, die täglich ausgetauscht wurden, was es notwendig machte, sie in Codebüchern aufzuschreiben (vgl. Singh 2000, 146–147) – so wurden die Schlüssel Teil des *systèmes*. Den Briten gelang es Anfang der 1940er Jahre sowohl einige funktionstüchtige Enigmas sowie Benutzungsvorschriften und das sog. *Kurzsignalhandbuch* aus angegriffenen Schiffen und U-Booten zu bergen, die wichtige Informationen für die Kryptanalyse lieferten (vgl. Bauer 1997, 202–203). So brach die Enigma mit Kerckhoffs' zweiter Forderung, indem das Bekanntwerden des Systems die Verschlüsselung kompromittierte. Die unklare Abgrenzung von Schlüssel und System betraf noch einen weiteren Aspekt: Da die in der Enigma verbauten Walzen nicht ausgetauscht, sondern erst gegen Ende des Zweiten Weltkriegs in manchen militärischen Abteilungen um eine Walze ergänzt wurden, wurden die Walzen praktisch zum Teil des Schlüssels, und die strikte Trennung von Verfahren und Schlüssel war damit in zweifacher Weise nicht mehr gegeben.

2.4.3 Zweites Schlüsselproblem: Asymmetrische Kryptographie

In der Geschichte der Kryptographie lassen sich, so die eingangs formulierte These, im doppelten Sinne des Wortes zwei Schlüsselprobleme ausmachen. Das erste betrifft die Trennung von Verschlüsselungsverfahren und Schlüssel. Obwohl diese Trennung bereits in Kapitel 2.3.1 anhand der monoalphabetischen Substitutionschiffren beispielhaft verdeutlicht werden konnte, woraus hervorgeht, dass die Trennung von Verfahren und Schlüssel in der Geschichte der Kryptographie immer wieder vorkam, wurde diese Trennung erstmals durch Kerckhoffs' *La Cryptographie Militaire* auf der Ebene der Theoriebildung vollzogen. Die Umsetzung des Kerckhoffs'schen Prinzips ist, wie am Beispiel der Enigma deutlich wurde, in der Praxis nicht so leicht wie man vermuten könnte, da sich die Zugehörigkeiten einzelner Elemente zu System oder Schlüssel durch ihren Gebrauch verschieben können.

Das zweite Schlüsselproblem ist das der »key distribution« (Singh 2000, 251), der Schlüsselverteilung. Von einem heutigen Standpunkt aus lassen sich

– zusätzlich zu der durch Katz und Lindell vorgenommenen Einteilung – zwei Grundtypen von Kryptographie ausmachen: »(1) *symmetric* or *secret key* and (2) *asymmetric* or *public key*« (Lloyd/Adams 2011, 683). Ein kryptographisches Verfahren wird als *symmetrisch* bezeichnet, wenn derselbe Schlüssel für die Ver- und Entschlüsselung verwendet wird (vgl. ebd., 683). Ein solches Verfahren setzt voraus, dass Sender_in und Empfänger_in sich auf einen Schlüssel geeinigt haben, und dass beide eine Kopie dieses Schlüssels besitzen müssen (vgl. ebd.). Dem Kerckhoffs'schen Prinzip folgend basiert die Sicherheit eines symmetrischen Verfahrens einzig und allein auf der Geheimhaltung des Schlüssels, weswegen symmetrische Kryptographie auch als *secret key cryptography* bezeichnet wird. Dies bringt in der Praxis ein grundsätzliches Problem mit sich: Da verschlüsselte Kommunikation notwendigerweise medial vermittelt ist, gibt es keine Möglichkeit, sich über den Schlüssel zu verständigen, denn der Übertragungsweg wird grundsätzlich als ein »unsicherer Kanal« (Paar/Pelzl 2016, 5) konzeptualisiert. Als unsicher wird ein Kanal nicht etwa deshalb beschrieben, weil dem Übertragungsmedium gewisse Eigenleistungen zugestanden würden, die über die bloße Vermittlung von Inhalten hinausgehen, sondern weil davon ausgegangen wird, dass eine unbefugte, dritte Partei den Inhalt der Kommunikation während der Übertragung abfangen und/oder manipulieren wollen würde – andernfalls wäre die Verschlüsselung des Kommunikationsinhaltes auch nicht notwendig. Eine Möglichkeit für einen sicheren Schlüsselaustausch ist, dass die beiden kommunizierenden Parteien einen anderen Kanal wählen, von dessen Sicherheit sie ausgehen, oder bei einem Treffen in leiblicher Ko-Präsenz einen Schlüssel vereinbaren.[23] Die Ende der 1970er Jahre durch Whitfield Diffie und Martin Hellman erfundene *public key cryptography*, auch *asymmetrische Kryptographie* genannt, nimmt sich genau dieses Umstands an, der durch eine veränderte Medienlage in besonderer Weise in den Vordergrund kryptographischer Fragestellungen rückt.

ARPANET und der Beginn computergestützter Kommunikation

1958 wurde in den USA die *Advanced Research Projects Agency*, kurz: ARPA gegründet, die dem Verteidigungsministerium unterstellt war, und Forschungen in den Bereichen Verhaltenswissenschaft, Materialwissenschaft und Raketenabwehr durchführte (vgl. Abbate 1999, 36). 1962, als Informatik noch kei-

23 Besteht Grund zur Annahme, dass trotz Sicherheitsvorkehrungen ein neuer Schlüssel vereinbart werden muss, so müssen sich beide Parteien erneut treffen.

ne universitäre Disziplin war, wurde das *Information Processing Techniques Office* (IPTO) als ARPA-Untergruppe gegründet, wodurch ARPA die treibende finanzielle Kraft hinter informatischer Forschung wurde (vgl. ebd.). Durch das IPTO entstanden in den folgenden Jahren mehrere Forschungszentren an Universitäten wie dem MIT, der Carnegie Mellon und der UCLA und einigen weiteren, die durch das ARPANET verbunden werden sollten (vgl. ebd.). Im Fokus der Vernetzungsbemühungen stand zunächst das sog. *time share computing*: Zentralrechner waren teuer, und die begrenzten Kapazitäten sollten über das ARPANET auch anderen universitären Standorten zur Verfügung gestellt werden (vgl. Warnke 2011, 30–31). Am 29.10.1969 wurde schließlich das ARPANET eingeweiht, und der erste Nutzungsversuch endete schneller als geplant mit dem berühmt-berüchtigten ersten Wort des Internets, »LO«, da das System zusammenbrach, bevor das Wort »LOGIN« zu Ende geschrieben werden konnte (vgl. ebd., 33). Die in medienwissenschaftlicher Literatur der letzten Jahre meistbesprochene Erfindung im Zusammenhang mit dem ARPANET ist das *Packet Switching*, das gleichzeitig die Grundlage für das Internet legte,[24] doch auch die E-Mail als neue Form der Kommunikation entstand mit dem ARPANET. Entgegen dem ursprünglich angedachten Verwendungszweck des ARPANET stand das Teilen von Rechenressourcen schnell nicht mehr im Vordergrund, im Gegenteil verringerte sich die Nachfrage nach Fernressourcen. Abbate (1999, 104) bemerkt dazu treffend: »Ironically, however, many sites rich in computing resources seemed to be looking in vain for users.« Verschiedene Faktoren zeichnen für diese Entwicklung verantwortlich: Einerseits waren die wenigen verbundenen Universitäten bereits gut mit Computern ausgestattet, was die Nachfrage nach zusätzlichen Ressourcen schmälerte. Darüber hinaus wurden Programme anderer Standorte eher auf die Computer einer jeweiligen Universität kopiert als per Fernzugriff ausgeführt. Auch die antizipierte Nutzung des »distributed computing«, bei dem eine Rechenaufgabe zwischen verschiedenen vernetzten Computern aufgeteilt wird, wurde kaum in Anspruch genommen, da sie an den administrativen Vorgängen innerhalb der Universitäten scheiterte (vgl. ebd., 104–105). Schlussendlich wurde auch im Verlauf der 1970er Jahre Computerhardware günstiger, und die ehemals verwendeten

24 Die Geschichte des ARPANET ist wesentlich detailreicher und komplizierter, als sie hier dargestellt werden soll, da dies nicht im Fokus dieses Buchs steht. Für einen ausführlichen Überblick siehe unter anderem Abbate (1999), sowie Warnke (2011) und Gießmann (2016); speziell zu *Packet Switching* siehe Sprenger (2015).

Mainframe-Computer an den Universitäten durch Mini- oder Microcomputer ersetzt, wodurch das ursprüngliche Problem, dessen Lösung das ARPANET darstellen sollte, auf anderem Wege gelöst wurde (vgl. ebd., 105). Doch mit dem ARPANET bildete sich auch eine neue Form der Kommunikation aus, und nahm die E-Mail als ein Phänomen digitaler Kulturen unvorhergesehen Fahrt auf.

Zu Beginn der 1960er Jahre hatten Nutzer_innen der Time-Sharing-Computer einen eigenen passwortgeschützten Bereich, auf dem Dateien abgelegt werden konnten. Diese Bereiche und die Schaffung von Zugangsvoraussetzungen durch Passwörter lassen sich mit Paul Ferdinand Siegert (2008, 191) als eine erste Form der Herstellung von Sicherheit als *access control*, also der Kontrolle von Zugangsberechtigungen betrachten. Mit der Zeit etablierte sich das Freigeben von Textdateien sowohl für einzelne Nutzer_innen, die anhand ihres Logins identifizierbar waren, als auch über *Public Domains*, die für alle zugänglich waren, als Methode der Kommunikation der Nutzer_innen des Time-Share-Systems untereinander (vgl. ebd.). 1965 wurde im Zuge der Arbeit am Dateisystem des *Compatible Time Share Systems*, kurz CTSS, ein System-Kommando namens »MAIL« entworfen und in CTSS implementiert. MAIL sollte Systemadministrator_innen dazu befähigen, Nutzer_innen über von Backupmedien wiederhergestellte Daten zu informieren. Die Idee Tom Van Vlecks, eines der Entwickler von MAIL, dass mit dem MAIL-Befehl alle Nutzer_innen allen anderen Nutzer_innen desselben Computers zeitversetzt Nachrichten egal welchen textlichen Inhalts zukommen lassen konnten, setzte sich durch, und so wurde MAIL in seiner erweiterten Funktionalität 1965 fester Bestandteil des CTSS-Dateisystems. MAIL war ab diesem Zeitpunkt ein *Push-Dienst* geworden, was, wie Siegert (ebd., 192) feststellt, integraler Bestandteil dessen werden sollte, was heute als E-Mail bezeichnet wird. Zu diesem Zeitpunkt operierte MAIL nur innerhalb desselben Computers, doch das sollte sich mit der breiteren Einbindung von MAIL in das ARPANET ändern. Dazu waren, wie Siegert (ebd., 198) ausführt, zwei Herausforderungen zu bewältigen: Es musste ein standardisiertes Protokoll für den Nachrichtenaustausch geschaffen werden, um die verschiedenen Mainframe-Computer miteinander zu verbinden, sowie ein computerübergreifendes Adressenschema entwickelt werden, damit die jeweiligen Nutzer_innen direkt adressierbar waren. Bemerkenswert ist die Tatsache, dass die verschiedenen am ARPANET beteiligten Akteur_innen – beispielsweise das Militär, die universitären Forscher_innen und diverse Firmen – unterschiedliche Ansprüche an Nachrichtenaustauschsysteme hatten, und so »Konferenz-Systeme, Chat-Systeme, schwarze Bretter

u.a.« (Ebd.) miteinander konkurrierten. Das erste funktionstüchtige Mail-Programm, das eine Kommunikation zwischen vernetzten Computern desselben Betriebssystems erlaubte, wurde Anfang der 1970er Jahre von Ray Tomlinson für das Betriebssystem TENEX geschrieben (vgl. Abbate 1999, 106). Kurze Zeit später wurde über die Möglichkeiten einer Vereinheitlichung der Mailsysteme von Time-Sharing-Betriebssystemen diskutiert, und wie diese zwischen vernetzten Computern zur Anwendung kommen könnten. Trotz der offensichtlichen Beliebtheit von E-Mail-Diensten im Alltag ihrer Nutzungsgemeinde war die Möglichkeit, Nachrichten zu versenden, auf der Ebene der Planung ein Nebenprodukt des ARPANET und wurde in den Papieren und Präsentationen, die sich an die geldgebenden Institutionen richteten, bis Mitte der 1970er Jahre kaum erwähnt (vgl. Siegert 2008, 212). Mehr noch: »[D]ie Betonung dieses Dienstes«, führt Siegert (ebd., 213) aus, hätte »das ARPANET-Projekt politisch gefährden können.« Dies lag hauptsächlich daran, dass das Versenden einfacher Textnachrichten gemessen an dem zur damaligen Zeit hohen ökonomischen und ressourcentechnischen Aufwand unangemessen verschwenderisch anmutete (vgl. ebd.). Und obgleich es nicht das Ziel des ARPANET war, ein neues Kommunikationsnetzwerk zu erschaffen – Abbate (1999, 108) weist darauf hin, dass die Möglichkeit, sich gegenseitig Nachrichten senden zu können, sogar als unwichtige Funktion eines wissenschaftlichen Netzwerks abgetan wurde – wurde durch eine Untersuchung im Jahr 1973 ermittelt, dass Dreiviertel des Netzwerkverkehrs durch E-Mails verursacht wurde. Damit war der ursprünglich anvisierte Einsatzbereich, das Teilen von Dateien und Rechenleistung, eindeutig in den Hintergrund gerückt (vgl. Siegert 2008, 217), und ein »radical shift in the ARPANET's identity and purpose« (Abbate 1999, 109) eingetreten: »The rationale for building the network had focused on providing access to computers rather than to people« (ebd.). Dieser radikale Shift sollte in den nächsten Jahren mit der Entwicklung des Internets weiter voranschreiten.

Eine Kiste mit zwei Schlössern

Die Nutzugspraktiken des ARPANET, die unverhofft die E-Mail als neue Form der Kommunikation hervorbrachten, waren auch für Diffies und Hellmans Überlegungen ausschlaggebend, die die Ablösung des ARPANET aus dem vornehmlich militärischen und akademischen zugunsten eines privatwirtschaftlichen Kontexts antizipierten. So schreiben sie in der Einleitung von *New Directions In Cryptography*:

> »The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.« (Diffie/Hellman 1976, 644)

Tatsächlich spielte Verschlüsselung in der Entwicklung des ARPANET, und damit auch für die Entstehung der E-Mail keine Rolle,[25] wodurch die Möglichkeit verschlüsselter Kommunikation erst nachträglich durch die Kryptographie beigesteuert wurde. Ein dringlicheres Problem war zunächst die Standardisierung des Adresssystems von E-Mails. Erste Versuche dazu lassen sich auf den Beginn der 70er Jahre zurückdatieren: Eine erste Liste mit 45 Netzwerkadressen und den dazugehörigen Hostnamen war bereits 1971 zum Download verfügbar (vgl. Siegert 2008, 268). Da es schnell umständlich wurde, dieses Dokument zu pflegen, kam der Vorschlag auf, ein solches Dokument in maschinenlesbarer Form online zu pflegen, das neben Adresse und Name des Hostrechners auch die durch ihn unterstützen Dienste anzeigte. Obwohl die Adresskonvention »mailbox@host.domain« erst 1982 verbindlich festgelegt wurde, entstand mit dem »Directory of Electronic Mail« (ebd., 269) Mitte der 1970er Jahre ein Adressbuch, in dem 134 unterschiedliche Netzwerke mit ihren jeweiligen Adressformen verzeichnet waren.[26] Ein solches Adressbuch machte es möglich, per E-Mail mit Personen in Kontakt zu treten, die man nicht bereits persönlich kannte. Obwohl Diffie und Hellman E-Mail nicht

25 Siegert (2008, 151) sieht dies als Beweis dafür, dass das ARPANET in erster Linie für die Forschung, und nicht für militärische Anwendungen konstruiert wurde: »Was hier entstehen sollte, war ein Forschungsnetz. Militärische Erfordernisse eines stabilen Kommunikationssystems unter Kriegsbedingungen, also besonders hohe Ausfallsicherheit, Verschlüsselung oder Prioritätenmanagement, wie sie Baran ausgearbeitete hatte, wurden nicht übernommen. Insofern ist der Schluss, das ARPANET sei ein militärisches Netz, da es von einer militärischen Behörde finanziert und von Baran entsprechend entworfen wurde, nicht haltbar.«

26 Siegert (2008, 269) weist darauf hin, dass zwischen Mailbox und Hostnamen im ARPANET das @-Zeichen verwendet wurde, in anderen Netzwerken aber auch : und ! gebräuchlich waren.

konkret erwähnen, so lässt sich doch darauf schließen, dass die von ihnen bemängelten »severe inconveniences«, die gleichermaßen die Vorteile des neuen Kommunikationsmediums zunichte machen würden, sich auf die Notwendigkeit des Schlüsselaustauschs beziehen, der mit symmetrischer Verschlüsselung *vor* dem Versenden verschlüsselter E-Mails notwendig wäre. Asymmetrische Verschlüsselung erlaube es hingegen, eine verschlüsselte Konversation »between any two individuals regardless of whether they have ever communicated before« (Diffie/Hellman 1976, 644) zu etablieren, ohne dass vorher ein Schlüsselaustausch über einen sicheren Kanal (der nicht leicht zu finden ist) oder während eines persönlichen Treffens stattfinden muss. Wie ist das möglich?

Die Funktionsweise asymmetrischer Kryptographie wird oft anhand des Beispiels einer verschlossenen Kiste erläutert (vgl. Paar/Pelzl 2016, 176; Singh 2000, 258–259): Person A möchte Person B eine Nachricht zukommen lassen, und legt diese in eine Kiste, die mit einem Vorhängeschloss gesichert ist. Bei symmetrischer Kryptographie müssen nun Person A und B über den gleichen Schlüssel verfügen, um die Kiste abzuschließen und zu öffnen. Asymmetrische Kryptographie hingegen funktioniert analog zu einer Kiste mit zwei Schlössern: Person A schließt die Kiste mit ihrem Vorhängeschloss ab und sendet sie an Person B. Person B kann die Kiste nicht öffnen, da sie den Schlüssel zu Vorhängeschloss A nicht hat, und hängt ihrerseits ein Vorhängeschloss B an, zu dem sie den Schlüssel hat, und sendet die Kiste mit zwei Vorhängeschlössern zurück an Person A. Person A wiederum entfernt ihr Vorhängeschloss A und sendet die Kiste mit nur noch dem Vorhängeschloss B zurück an Person B, die die Kiste nun öffnen und die Nachricht lesen kann. Dieser Vorgang erscheint zunächst umständlich, da die Nachricht mehrmals hin und her gesendet werden muss. Nichtsdestotrotz, schreibt Singh (ebd., 259), »[f]or the first time we have a suggestion that key exchange might not be an inevitable part of cryptography.« Dieses Modell hat nur einen Nachteil: Es funktioniert zwar mit Vorhängeschlössern und einer Kiste, die die Nachricht einkapselt, aber nicht mit kryptographischen Verfahren, die die Nachricht remediatisieren. Würden Person A und B denselben Vorgang nicht mit einer Kiste und Vorhängeschlössern, sondern mit einem Text und beispielsweise einer monoalphabetischen Substitutionschiffre durchführen, so wäre das Endergebnis unlesbar: Person A verschlüsselt den Plaintext mit ihrem Schlüssel A und sendet den *Ciphertext A* an Person B. Person B kann *Ciphertext A* nicht entschlüsseln, und verschlüsselt ihn nun erneut mit ihrem Schlüssel B, und sendet dann den *Ciphertext AB* zurück an Person A – so weit,

so gut. Person A kann allerdings den *Ciphertext AB* nicht mit ihrem Schlüssel A entschlüsseln, da die letzte Substitution mit dem Schlüssel B erfolgt ist. Die Anwendung des umgekehrten Verschlüsselungsalgorithmus mit Schlüssel A führt ganz im Gegenteil zu einer weiteren Verschlüsselung, an dessen Ende der *(Ciphertext AB)A* steht, der dann an Person B zurückgesendet werden würde. Person B würde dies durch eine weitere Bearbeitung mit Schlüssel B in *(Ciphertext AB)AB* verwandeln, aber nicht in den Plaintext. Die korrekte Reihenfolge von Ver- und Entschlüsselung muss also der Maxime »last on, first off« (ebd.) gehorchen. Die Lösung dieses Dilemmas liegt unter anderem darin, dass es sich bei den vorangegangenen Schilderungen lediglich um Modelle handelt, und nicht um die Gegenstände selbst, was auch bedeutet, dass die Einschränkungen der Modelle nicht auf die Gegenstände zutreffen müssen. Mit der grundsätzlichen Idee, dass ein Schlüsselaustausch nicht notwendig sei, um verschlüsselte Nachrichten zu versenden, forschten Diffie und Hellman, zu denen inzwischen Ralph Merkle gestoßen war, bis sie in der Verwendung von Einwegfunktionen[27] in Kombination mit modularer Arithmetik[28] eine Möglichkeit für die Umsetzung ihres Vorhabens entdeckten (vgl. ebd., 260–261). Mit dieser Lösung geht auch die Zweiteilung des Schlüssels

27 Eine gegebene Funktion wird als Einwegfunktion bezeichnet, wenn sie in Polynomialzeit berechnet werden kann, ihre Umkehrung allerdings nicht mehr. Bei einer Einwegfunktion, hier beispielhaft als die Funktion $y=f(x)$ dargestellt, geht man davon aus, dass für jedes x genau ein y berechnet werden kann. Die Funktion ist damit *eineindeutig* und kann in *polynomialer Zeit* berechnet werden (vgl. Spitz et al. 2011, 32). Eine solche Funktion wird beispielsweise verwendet, um von einer Datei x eine Hashsumme y zu erzeugen. Möchte man nun von der Hashsumme aus die dazugehörige Datei errechnen, muss der Rechenvorgang umgekehrt durchgeführt werden – dies wird durch die Notation $x= f_1(y)$ dargestellt. Dies ist zwar theoretisch möglich, aber der Rechenaufwand steigt mit jeder Stelle der Hashsumme exponentiell an (vgl. ebd., 33). Aus praktischer Sicht ist ein solches Zurückrechnen unmöglich, da dies je nach Länge der Hashsumme mehrere Jahrzehnte, Jahrhunderte oder sogar Jahrtausende dauern könnte (vgl. Paar/Pelzl 2016, 177–178). Aufgrund der *praktischen* Unumkehrbarkeit der Funktion wird diese als Einwegfunktion bezeichnet.

28 Bei Modularer Arithmetik wird innerhalb eines begrenzten Zahlenraumes ›in Kreisen‹ gerechnet. Dies lässt sich am besten anhand eines Alltagsbeispiels für die Anwendung modularer Arithmetik verdeutlichen: der Uhrzeit. Wer um 10 Uhr vormittags eine Aufgabe beginnt, die 8 Stunden dauert, wird um 6 Uhr nachmittags fertig sein. 10 + 8 ergibt innerhalb dieses Systems 6, da ab Erreichen der Zahl 12 am Anfang des Zahlenraumes bei der Zahl 1 weitergezählt wird. Die mathematische Notation lautet: $10 + 8 = 6 \ (mod\ 12)$ (lies: »modulo 12«).

in einen privaten und einen öffentlichen Teil einher, die mathematisch so zusammenhängen, dass der öffentliche Schlüssel mittels des privaten über eine Einwegfunktion generiert wird. Die beiden öffentlichen Schlüssel können über einen unsicheren Kanal ausgetauscht werden. Die Einwegfunktion verhindert, dass der private Schlüssel berechnet werden kann, selbst wenn der öffentliche Schlüssel sowie die verwendete Funktion bekannt sind, wodurch bei diesem Verfahren das Kerckhoffs'sche Prinzip auf elegante Weise gewahrt wird. Zwei miteinander kommunizierende Parteien müssen nun nicht mehr einen symmetrischen Schlüssel austauschen, allerdings wird der herkömmliche Schlüssel*austausch* praktisch durch eine Schlüssel*vereinbarung* ersetzt, da eine Einwegfunktion verabredet werden muss, was entweder in einem (Telefon-)Gespräch oder in einem zeitversetzten Mailwechsel geschehen kann (vgl. ebd., 265–267). Damit ist das Problem des Schlüsselaustausch über einen unsicheren Kanal zwar gelöst, aber dennoch »the spontaneity of e-mail« (ebd., 267) nicht völlig ausgeschöpft, da nach wie vor nicht einfach verschlüsselt drauf los geschrieben werden kann. Dazu gesellte sich ein weiteres Problem: Das von Diffie und Hellman entwickelte Verfahren kann nur zur Generierung von Schlüsseln verwendet werden, aber noch nicht für Ver- und Entschlüsselung von Nachrichten (vgl. Schneier 2015, 513). Nur kurze Zeit später legten Ronald Rivest, Adi Shamir und Leonard Adleman (1978) in ihrem Paper *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* eine Verschlüsselungsmethode vor, die der von Diffie und Hellman beschriebenen Einwegfunktion in ihrer Funktionsweise recht ähnlich ist, und ebenfalls von modularer Arithmetik Gebrauch macht. Die Sicherheit des nach den Anfangsbuchstaben der Nachnamen seiner Erfinder benannten RSA-Verschlüsselungsverfahrens liegt in dem Faktorisierungsproblem großer Zahlen (vgl. ebd., 126): Der Schlüssel ist auch hier in eine öffentliche und eine private Komponente aufgeteilt. Für die private Komponente werden zwei Primzahlen p und q ausgewählt, die miteinander multipliziert die Zahl n ergeben. p und q bleiben privat, n hingegen bildet gemeinsam mit einer weiteren, zufällig gewählten Zahl e den öffentlichen Schlüssel (vgl. ebd., 122–123). Während das Produkt n durch die Multiplikation von p und q schnell berechnet ist, so ist für die Zerlegung von n in p und q bis heute kein effizientes Verfahren bekannt, was die Herstellung von n aus der Multiplikation von p und q (nach aktuellem kryptanalytischen Forschungsstand) zu einer Kandidatin für eine Einwegfunktion macht. Je größer p und q, und damit auch n sind, desto länger dauert im Falle eines Angriffs die Primfaktorzerlegung, und desto sicherer ist

das Verfahren.[29] Singh (2000, 279) bemerkt dazu: »It is now routine to encrypt a message with a sufficiently large value of N so that all the computers on the planet would need longer than the age of the universe to break the cipher.« Mit dem öffentlichen Schlüssel (n, e) kann eine Nachricht m, die kürzer ist als n, verschlüsselt werden. Ist die Nachricht länger, so muss sie in mehrere Teile aufgeteilt werden. Der Ciphertext entsteht in der Rechnung $m_e \bmod n$ (vgl. Schneier 2015, 467).[30]

Digitale Signaturen

Der Austausch verschlüsselter Nachrichten ohne vorherigen Schlüsselaustausch ist nicht die einzige Funktion asymmetrischer Kryptographie. Eine zweite ist die Möglichkeit, digitale Signaturen zu erzeugen – ein Novum in der Verwendung von Kryptographie. Diffie und Hellman (1976, 645) führen diese Funktion am Beispiel von Unterschriften bei Geschäftsvorgängen ein, die in der Zukunft online, und damit papierlos abgewickelt werden sollen:

> »In current business, the validity of contracts is guaranteed by signatures. A signed contract serves as legal evidence of an agreement which the holder can present in court if necessary. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for this paper instrument, each user must be able to produce a message whose authenticity can be checked by anyone, but which could not have been produced by anyone else, even the recipient.«

Auch Rivest, Shamir und Adleman (1978, 120) verweisen auf die Digitalisierung von Briefen als Anwendungsgebiet ihres Verschlüsselungsverfahrens:

> »The era of »electronic mail« may soon be upon us; we must ensure that two important properties of the current »paper mail« system are preserved: (a)

29 In der Praxis ist n meist 1024 Bit lang, wobei bereits 2048 Bit als Länge empfohlen wird (vgl. Paar/Pelzl 2016, 203).

30 Dieses Verfahren wird innerhalb der Kryptographie als *Textbook-RSA* bezeichnet, da es die Funktionsweise von RSA-Verschlüsselung schematisch verständlich macht, aber in der Praxis unsicher ist, da es deterministisch ist (vgl. Katz/Lindell 2008, 356). Mehrfaches Verschlüsseln eines gegebenen Plaintexts führt mit dieser Methode immer zu exakt demselben Ciphertext, was bedeutet, dass Angreifer_innen Informationen über die Kommunikationsinhalte ableiten können, die eigentlich geheim zu halten wären. Weiterführend zu sicheren Anwendungen von RSA siehe Katz/Lindell (ebd., 337–340).

> messages are private, and (b) messages can be signed. We demonstrate in this paper how to build these capabilities into an electronic mail system.«

Konkret geht es also sowohl Diffie und Hellman als auch Rivest, Shamir und Adleman darum, handschriftliche Unterschriften auf Papierdokumenten mittels asymmetrischer Kryptographie zu remediatisieren. Diffie und Hellman (1976, 649, Herv. i.O.) spezifizieren:

> »In order to develop a system capable of replacing the current written contract with some purely electronic form of communication, we must discover a digital phenomenon with the same properties as a written signature. It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it. We will call any such technique *one-way authentication*.«

Rivest, Shamir und Adleman (1978, 121, Herv. i.O.) erweitern diese Forderungen mit Blick auf die medienspezifische Unmöglichkeit »to detect electronic ›cutting and pasting‹« innerhalb digitaler Datenverarbeitung: »An electronic signature must be *message*-dependent, as well as *signer*-dependent.« Zusammengefasst belaufen sich die Eigenschaften, über die digitale Unterschriften verfügen sollten, um handschriftliche Unterschriften auf Papierdokumenten zu ersetzen, auf 1) Authentizität der Signatur, 2) Fälschungssicherheit der Signatur, 3) Dokumentenbindung der Signatur, 4) Unveränderlichkeit des Dokuments nach der Unterschrift, und 5) Nicht-Zurückweisbarkeit der Signatur (vgl. Schneier 2015, 36). Eine digitale Signatur mittels *Textbook-RSA* würde folgendermaßen funktionieren: Person A verschlüsselt ein Dokument mit ihrem privaten Schlüssel und sendet es an Person B. Person B entschlüsselt das Dokument mit dem öffentlichen Schlüssel von Person A, und kann so die Unterschrift verifizieren (vgl. ebd., 37). Die Entschlüsselung des Dokuments verifiziert dabei die Authentizität der Signatur (1): Käme die Unterschrift beispielsweise von Person C, könnte die Entschlüsselung nicht mit dem öffentlichen Schlüssel von Person A durchgeführt werden. Die Fälschungssicherheit (2) der Signatur ist dadurch gegeben, dass sie mit dem privaten Schlüssel erstellt wird, auf den (in diesem Modell) ausschließlich Person A zugreifen kann. Da die Signatur sich mathematisch auf das signierte Dokument bezieht, ist sie dokumentenabhängig (3), und verhindert gleichsam die nachträgliche Veränderung des Dokuments (4), da eine solche die Signatur ungültig machen würde. Schlussendlich ist die Signatur nicht zurückweisbar, da sie unabhängig von der weiteren Mitarbeit der unterschreibenden Person

verifiziert werden kann (vgl. ebd., 37–38). Je nach Größe des unterschriebenen Dokuments ist diese Methode jedoch sehr zeit- und ressourcenaufwändig. Eine mögliche Lösung für dieses Problem besteht darin, nicht das Dokument selbst zu signieren, sondern mit einer Hashfunktion eine Prüfsumme des Dokuments zu erstellen, und diese zu signieren (vgl. ebd., 38–39). Dies hat ebenfalls den Vorteil, dass das Dokument selbst nicht verschlüsselt werden muss, und offen, aber unterschrieben versendet werden kann; oder aber, dass ein Dokument geheim gehalten werden kann, aber mittels der Signatur, die beispielsweise in eine Online-Datenbank hochgeladen wurde, und dadurch einen Zeitstempel erhalten hat, ein zeitkritischer Nachweis über die Autor_innenschaft eines Dokuments erbracht werden kann (vgl. ebd., 39).

Asymmetrische Kryptographie umfasst damit vier sogenannte *Sicherheitsdienste*:[31] Nichtzurückweisbarkeit, Schlüsselaustausch über unsichere Kanäle, Authentisierung/Identifikation und Verschlüsselung (vgl. Paar/Pelzl 2016, 178). Die Neuheiten gegenüber symmetrischer Kryptographie sind der Schlüsselaustausch über unsichere Kanäle, sowie die Möglichkeit *öffentlich*[32] überprüfbarer Signaturen. Darüber hinaus wird mit asymmetrischer Kryptographie, beispielsweise im Fall einer verschlüsselten E-Mail, eine versendete Nachricht mathematisch an den_die Empfänger_in gebunden, und, falls sie signiert wurde, ebenfalls an den_die Sender_in. Es können also sowohl die kommunizierenden Parteien als auch das jeweilige Dokument authentifiziert werden. So wird die Bezugnahme von Plaintext, Ciphertext, Empfänger_in und ggf. Sender_in aufeinander verhärtet.

31 Als *Sicherheitsdienste* werden »Schutzziele, die mit einem Sicherheitsmechanismus erreicht werden können« (Paar/Pelzl 2016, 297) bezeichnet.

32 Es existieren auch Signaturverfahren mit symmetrischer Kryptographie. Diese werden als *message-authentication schemes* bezeichnet. Der Unterschied von *message-authentication schemes* und asymmetrisch erzeugten Signaturen liegt in den Verifizierungsmöglichkeiten der jeweiligen Unterschriften (vgl. Goldreich 2009, 498). Durch die Trennung des öffentlichen und privaten Teils des Schlüssels bei asymmetrischer Kryptographie lassen sich Signaturen öffentlich verifizieren, da nur ein Teil des verwendeten Schlüssels für diesen Vorgang benötigt wird, wohingegen eine öffentliche Verifizierung einer symmetrisch erzeugten Signatur die Fälschungssicherheit und Personenbindung derselben aufheben würde, da der komplette Schlüssel dann bekannt ist.

2.5 Kryptographische Modellbildung

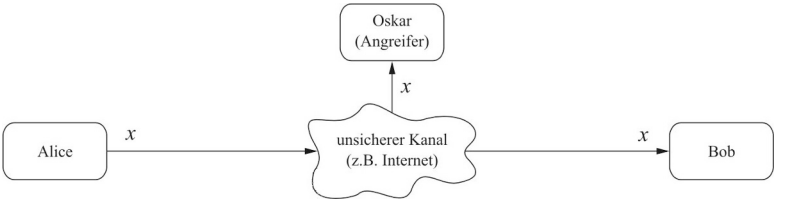
Anhand der bisher geschilderten Funktionsweisen kryptographischer Verfahren sowie der zwei formativen Schlüsselprobleme der Kryptographie ist ein Überblick über einige der wichtigsten Gegenstände sowie Theorieimpulse des Feldes entstanden. Dieser stellt die Grundlage für die weitere Analyse kryptographischer Modellbildung dar, im Zuge derer der Kanal, zwei berüchtigte Figuren und schlussendlich der innerfachlich zugrunde liegende Sicherheitsbegriff diskutiert werden wird. Zusammenfassend lässt sich als Hauptaufgabe der Kryptographie nach den bisherigen Ausführungen die Geheimhaltung einer Nachricht auf ihrem Weg von Sender_in zu Empfänger_in beschreiben. Der durch Verschlüsselung hergestellte Ciphertext ist die Remediatisierung eines Plaintexts, insofern der Vorgang der Verschlüsselung sich als prozessual auffassen lässt. Der Ciphertext wird nun wiederum durch Bot_innen, Telegraphie, das Internet etc. von Sender_in zu Empfänger_in übertragen. Diese jeweiligen Vorgänge, so lässt sich mit Kerckhoffs festhalten, müssen restlos reversibel sein, sodass am Ende der Kommunikationskette erneut die eingangs geschriebene Nachricht, der Plaintext steht. Auch asymmetrische Kryptographie folgt dem Prinzip einer restlosen Reversibilität, und bindet darüber hinaus (Sender_in und) Empfänger_in an die verschlüsselte (und signierte) Nachricht. So werden mit mathematischen Mitteln die Möglichkeiten der Verbreitung einer verschlüsselten Nachricht über den intendierten Weg hinaus beschränkt, und die Anwendungsbereiche von Kryptographie um Nichtzurückweisbarkeit und öffentliche Authentisierung erweitert, sowie eine mathematische Lösung für das Problem des Schlüsselaustauschs über den bisher mehrfach genannten *unsicheren Kanal* bereitgestellt, der im Folgenden genauer betrachtet wird.

2.5.1 Der *unsichere Kanal*

Ein repetitives Muster, das sich durch die Geschichte der Kryptographie zieht, wurde bisher noch nicht besprochen: Sowohl symmetrische als auch asymmetrische Kryptographie geht von einem Szenario aus, das gewissermaßen als Grundstruktur der Kryptographie beschrieben werden kann, in dem zwei räumlich voneinander getrennte Parteien miteinander kommunizieren wollen. Diese Kommunikation erfolgt über einen sogenannten *unsicheren Kanal*, der einer dritten Partei die Möglichkeit bietet, die Kommunikation abzufangen, zu belauschen, zu verändern, oder sich als eine der kommunizierenden

Parteien auszugeben. Paar und Pelzl (2016, 5) stellen diese Struktur schematisch dar:

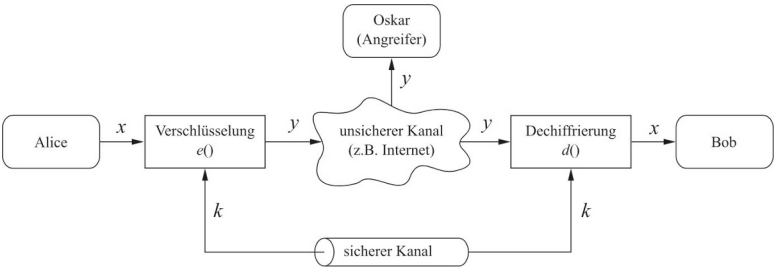
»*Kommunikation über einen unsicheren Kanal mit lauschendem Gegenspieler*«



Quelle: Paar/Pelzl 2016, 5

Bemerkenswert ist an dieser Stelle, dass nicht der Kanal, sondern der Weg der Nachricht »X« in der Grafik durch Pfeile visualisiert wird, wohingegen der unsichere Kanal als ein Zwischenraum dargestellt wird, in den die mit »X« bezeichnete unverschlüsselte Nachricht hineingegeben wird, und der die kommunizierenden Parteien »Alice« und »Bob« voneinander trennt. Eine solche Anordnung entspricht einer Sichtweise von Medien, die Sybille Krämer (2008, 16) als kennzeichnend für das sogenannte *technische Übertragungsmodell* von Kommunikation ausmacht: Medien sind zwischen Sender_in und Empfänger_in platziert, und gleichsam das, was »es überhaupt erst möglich macht, dass der Sender etwas ›aufgeben‹ kann, was dann beim Empfänger auch ankommt. Das Medium […] schafft eine Verbindung trotz und in der Entfernung.« Inwiefern ist dieser Kanal aber unsicher? Dies lässt sich anhand der Antwort der Kryptographie auf das durch die Grafik prägnant visualisierte Problem der als »Oskar« bezeichneten, eingreifenden dritten Partei beantworten. »Oskar« macht sich den unsicheren Kanal zunutze, um die versendete Nachricht abzuhören oder abzufangen – um dies zu verhindern, muss die Nachricht verschlüsselt werden. Dadurch schaffen die kommunizierenden Parteien, Paar und Pelzl (2016, 6) folgend, einen eigenen, *sicheren Kanal*, der an dem_der Angreifer_in vorbei führt:

»Verschlüsselung mit symmetrischer Kryptographie«



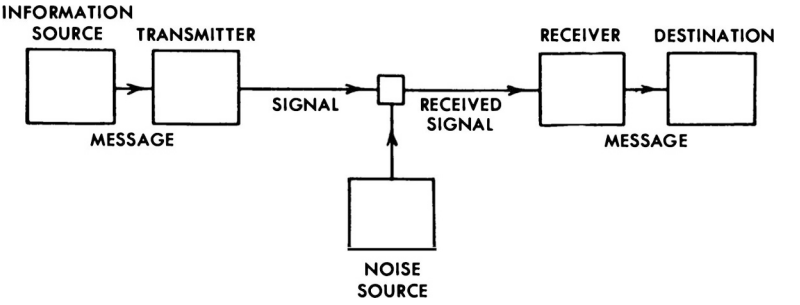
Quelle: Paar/Pelzl 2016, 6

Verschlüsselung macht dieser Darstellung zufolge also einen Kanal sicher. Bevor näher auf den Begriff »un/sicher« eingegangen wird, lohnt es, die Aufmerksamkeit zunächst noch einmal auf den Kanal zu richten. Als Beispiel für einen unsicheren Kanal wird in beiden Grafiken »z.B. Internet« angegeben. »Der leicht abstrakte Begriff ›Kanal‹«, schreiben Paar und Pelzl (ebd., 4) dazu, »bezeichnet lediglich die Kommunikationsstrecke, z.B. das Internet, eine Luftstrecke im Fall von WLAN oder Mobilfunk oder jedes andere Medium, über das sich digitale Daten übertragen lassen.« Die durch das Wort »lediglich« erzeugte Beiläufigkeit, und die scheinbare Beliebigkeit des Mediums lassen vermuten, dass Medien hier keine besondere Rolle zukäme, doch das Gegenteil ist der Fall. An dieser Stelle lässt sich ausführlicher mit Sybille Krämer (2008) anschließen, die sich in ihrem Buch *Medium, Bote, Übertragung. Kleine Metaphysik der Medialität* ausgehend von den Begriffen Kommunikation und Botengang der Übertragung als Medialitätsprinzip widmet. Krämer (ebd., 13) versucht zu Beginn ihrer Untersuchung, der Unschärfe des Begriffs »Kommunikation« beizukommen, indem sie anmerkt, dass der Ausdruck im aktuellen Diskurs ein »begriffliches Doppelleben« führe, das aus »zwei profilierten, jedoch gegenläufig zueinander stehenden Zusammenhängen, die wir hier das ›technische Übertragungsmodell‹ und das ›personale Verständigungsmodell‹ der Kommunikation nennen wollen«, bestehe. Als paradigmatisch für letzteres macht Krämer die Kommunikationstheorie Jürgen Habermas' aus, während für das technische Übertragungsmodell die Informationstheorie Claude Shannons und Warren Weavers grundlegend sei (vgl. ebd.). Das Ausgangsproblem des technischen Übertragungsmodells, so beschreibt es Krämer (ebd.), bestehe in der

> »räumlich/zeitlichen Entfernung zwischen Sender und Empfänger. Beide gelten als Instanzen, die menschlicher oder sächlicher Natur sein können und die Anfangs- und Endpunkte einer *linearen* Kette bilden, in der es unverzichtbare Zwischenglieder gibt, sei es in Gestalt des Mediums (Kanal), sei es in Form einer von außen kommenden ›Störgröße‹.«

In dieser Beschreibung findet sich ebenfalls das *Medium als Kanal*, wie es bereits bei Paar und Pelzl eingeführt wurde. Krämer (ebd., 14) schreibt weiter: »Die technische Verbindung ist dann erfolgreich, wenn es gelingt, in dem Übertragungsgeschehen vom Sender zum Empfänger den ›störenden Dritten‹ fernzuhalten.« Wer oder was der *störende Dritte* ist, ist abhängig davon, worauf der Blick fällt – für die Kryptographie ist es eine dritte Partei, die die Kommunikation zweier anderer abfangen möchte, für die mathematische Kommunikationstheorie von Claude Shannon (1964, 65) ein Nebenprodukt des Kanals, »noise«, Störgeräusche, die die Nachricht in der Übertragung verfremden können:

»*Schematic diagram of a general communication system.*«



Quelle: Shannon 1964, 34

Die strukturelle Gemeinsamkeit des *störenden Dritten* als Gefahr, aber auch der Anordnung im Allgemeinen lässt sich ebenfalls anhand der von Shannon entworfenen schematischen Darstellung des mathematischen Modells von Kommunikation erkennen. Über den Kanal, der als einziges Element der Grafik nicht mit einer Beschriftung ausgezeichnet ist, schreibt Shannon (ebd., 34, Herv. MS): »The channel is *merely* the medium used to transmit the

signal from transmitter to receiver. It may be a pair of wires, a coaxial cable, a band of radio frequencies, a beam of light etc.« Damit lässt sich Paars und Pelzls Beschreibung der Funktionsweise von Kryptographie als explizit an dem Shannonschen Modell orientiert erkennen.[33] Mit seiner Erläuterung des *transmitters*, »which operates on the message in some way to produce a signal suitable for transmission over the channel«, formuliert Shannon (ebd., 33) explizit aus, was bei Kerckhoffs bereits latent in der Forderung, Ciphertexte sollen telegraphisch[34] übertragbar sein, vorhanden ist: dass mit der Übermittlung einer (verschlüsselten) Nachricht ein Mediatisierungsvorgang verbunden ist. Anhand des Kerckhoffs'schen Prinzips und der damit einhergehenden Forderung nach Remediatisierbarkeit von Ciphertexten konnte in Kapitel 2.4.2 bereits gezeigt werden, dass die Telegraphie als Übertragungsmedium durch ihre Materialität und Medialität einen regulierenden Einfluss auf die Medialität, das heißt, auf die Übersetzungsleistung von Verschlüsselung nimmt. Shannon nimmt jedoch eine explizite Trennung zwischen dem Eingang einer Nachricht/Information in ein System an der Stelle des Transmitters, dem die Übersetzungsleistung zufällt, und deren augenscheinlich bloßer Übertragung über einen Kanal vor. Die Gleichsetzung von Medium und Kanal im Zusammenhang mit dieser Trennung erzeugt dabei zwei gegenständliche Medien, von denen eines ausschließlich übersetzt und eines ausschließlich überträgt. Diese Aufteilung verengt den Raum für die Betrachtung der *Medialität des Kanals*, und schließt Fragen nach dem, was als generatives Moment von Medien beschrieben werden kann, an dieser Stelle aus, die jedoch für eine medienwissenschaftliche Betrachtung von Kryptographie von Interesse wären. Anschließend an die bisherige Darstellung von Sybille Krämers medienphilosophischen Überlegungen soll hier daher erneut an die von ihr als zentral für die Medientheorie bestimmte Frage, ob Medien Sinn vermitteln oder erzeugen, angeknüpft werden. Mit Krämer lässt sich anhand des postalischen Prinzips von Medien, das in diesem Fall durch das technische Übertragungsmodell vorliegt, Medialität im Spannungsfeld von *Übertragung*

33 Warren Weaver (1964, 25) bemerkt in seinen Ergänzungen zu Shannons Theorie, dass die geringe Spezifizität des Modells dessen Stärke ausmache, da es auf alle Kommunikationssituationen übertragbar sei. »It is an evidence of this generality«, schreibt er weiter, »that the theory contributes importantly to, and in fact is really the basic theory of cryptography which is, of course, a form of coding.« (Ebd.)

34 Die Beliebigkeit des Mediums schränken auch Paar und Pelzl teilweise mit dem Hinweis auf digitale Datenübertragung ein.

und *Inkorporation* begreifen. Übertragung schließt hier an die Übertragung eines Mediums als Form in ein anderes Medium an, oder mit Bolters und Grusins Term: an die Remediatisierung. Diese Übertragung bestimmt Krämer (2003, 84) zugleich als eine schöpferische Geste, die nicht aus dem Nichts schafft, sondern durch die in der Übertragung geschehende Herstellung neuer Zusammenhänge, ähnlich wie dies bei der Bildung von Metaphern der Fall sei. Als Inkorporation definiert Krämer die Aktualisierung eines Musters, Schemas, einer Struktur, in der diese gleichsam eine Veränderung erfahre, die also über eine bloße »Fleischwerdung« (ebd.) hinausgehe, und den Raum der Betrachtung für die Performativität der Medialität öffnet. Wenn also »Medien im Akt der Übertragung dasjenige, was sie übertragen, zugleich mitbedingen und prägen«, kann »›Übertragung‹ als ›Konstitution‹« verstanden werden (ebd., 84–85). Shannons Trennung von Übersetzungsleistung und Medium, die Aufteilung von Medium und Mediatisierungsvorgang, sowie die Annahme, es gebe Einzelmedien, die sich mit Krämer (ebd., 85) als das »Resultat einer Abstraktion« begreifen lässt, ist eine wiederkehrende Figur technisch-mathematischer Diskurse, die nicht an der Reflexion von Medialität interessiert sind, sondern sich auf die technischen Apparate konzentrieren, die mit Krämer als Teil dessen, was Medien sind, verstanden werden können, in denen sich die Eigenschaften von Medien jedoch nicht erschöpfend zeigen. Diese Trennung ist historisch gewachsen, und erfüllt mehrere Funktionen: Die Verbindung und Interoperabilität zwischen verschiedenen Hard- und Softwarebestandteilen, die Möglichkeit, einzelne Elemente auszutauschen, was sowohl im Falle einer Störung als auch einer Aktualisierung einzelner Komponenten von Vorteil ist, sowie eine Vereinfachung der Fehlersuche, die gleichzeitig für die Ausfallsicherheit eines Systems eine große Rolle spielt. Infolgedessen erscheint der Kanal als neutrales Übertragungsmedium und die Herstellung von Sicherheit wird ebenfalls modularisiert: Sicherheit in der Informationstechnik und der Kodierungstheorie ist bezogen auf den Kanal und bedeutet Sicherheit einer Information vor *noise*. Darauf aufbauend befasst sich die Herstellung von Sicherheit in der Kryptographie damit, dass eine Nachricht auf dem Transportweg vor böswilligen Akteur_innen geschützt ist. Dies ist die Grundlage, auf der die innerfachlichen Diskurse von Kryptographie und IT-Sicherheit basieren.

2.5.2 Alice und Bob

> »Alice and Bob have a storied history. They send each other secrets, they get locked in jail, they get married, they get divorced, they're trying to date each other. I mean, anything two people might want to do securely, Alice and Bob have done it, somewhere in the cryptographic literature.« (Bruce Schneier [RSA Conference 2010, TC 1:04-1:17])

Die Bezeichnungen »Alice« und »Bob« für die beiden kommunizierenden Parteien in den Grafiken von Paar und Pelzl tauchen an dieser Stelle zum ersten Mal in der vorliegenden Untersuchung auf. Dies ist jedoch nicht repräsentativ für ihre Verwendung innerhalb der Fachliteratur der Kryptologie und IT-Sicherheit, in der Alice und Bob nahezu omnipräsent sind. Auch innerhalb popkultureller Kontexte erfreuen sich die beiden Figuren großer Beliebtheit, sind sie doch Teil dessen, was als »geek lore« (DuPont/Cattapan 2017, 1) bezeichnet werden kann: Alice und Bob haben einen eigenen Eintrag im *Jargon File* (vgl. The Jargon File 0.J.a), tauchen hin und wieder im Webcomic *xkcd* auf (vgl. Munroe 2014; 2006), und es gibt eine Menge (unautorisiertes) Merchandise von ihnen zu kaufen. »More than just the world's most famous cryptographic couple«, schreiben Quinn DuPont und Alana Cattapan (2017, 1), »Alice and Bob have become an archetype of digital exchange, and a lens through which to view broader digital culture.« Im Folgenden soll der Blick nicht nur *durch*, sondern vor allem *auf* die Linse gerichtet werden: Wer und was sind Alice und Bob? Welche Rolle spielen sie für die Kryptographie?

Ein Großteil kryptologischer Fachliteratur behandelt, wie bereits herausgestellt, einen dem technisch-postalischen Übertragungsmodell folgenden Kommunikationsvorgang zweier Entitäten, seien es Personen oder Maschinen. Diese wurden gemeinhin als *A* und *B* unterschieden. Mit Ronald Rivests, Adi Shamirs und Leonard Adlemans bereits diskutiertem Paper *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* bekamen A und B die Namen, die sie bis heute behalten haben: »For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem« (Rivest et al. 1978, 121). Trotz dieser eher nüchtern-beiläufigen Einführung, aber vermutlich aufgrund der Praktikabilität der Namen, mit denen sich mathematische Beweisführungen, die zum größten Teil ausschließlich aus (mit Buchstaben bezeichneten) Variablen bestehen, übersichtlicher gestalten lassen, gewannen die Namen Alice und Bob innerhalb der wissenschaftlichen

Community an Popularität.[35] Mit den Namen zieht auch zum ersten Mal explizit die Geschlechterdifferenz in die kryptographische Modellbildung ein,[36] und macht Geschlecht über die Differenz adressierbar: Anhand von DuPonts und Cattapans (2017, 4) Bemerkung, dass A und B, bevor sie als Alice und Bob benannt wurden, »largely featureless« gewesen seien, was sie als »presumptively male, symbolic, and abstract« definieren, wird Androzentrismus als stille Norm sichtbar. Dies wird durch Ronald Rivests Aussage bestätigt: Die Geschlechter*differenz* sei mit der Absicht eingezogen worden, die kommunizierenden Parteien auch dann noch einfach unterscheiden zu können, wenn sie mit Personalpronomen bezeichnet werden – statt der zwei unmarkiert-männlichen Kommunizierenden A und B gibt es nun Alice, »she« und Bob, »he« (vgl. ebd., 7). DuPont und Cattapan (ebd., 9) verweisen darauf, dass auch Alice und Bob dennoch für einige Jahre, abgesehen von der Geschlechterdifferenz, zunächst ebenfalls als »featureless symbols – little more than named abstractions« verwendet worden seien. Dies sollte sich drei Jahre nach ihrem ersten Auftritt im Feld mit Manuel Blums Paper *Coin Flipping By Telephone. A Protocol For Solving Impossible Problems* ändern, das folgendermaßen beginnt:

> »Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice HEADS and hear Alice (at the other end of the line) say »Here goes… I'm flipping the coin …. You lost!« (Blum 1983, 23)

DuPont und Cattapan (2017, 9) resümieren: »Blum's report is the first in what would become a tradition: literature that invents their situational context and backstory. […] From this point on, Alice and Bob have a history and, soon, will start to acquire personalities, and eventually friends.« Von diesem Moment an sind Alice und Bob manchmal verheiratet, manchmal geschieden, und manchmal einfach nur zwei Personen, die nur aufgrund einer gegebenen Situation miteinander in Kontakt treten: In der Phantasie der Forscher_innen, die ihre Geschichten schreiben, entwickeln sie eine Art Eigenleben. Einen Überblick

35 Die Bedeutung und Bekanntheit der ersten nach dem Prinzip der asymmetrischen Kryptographie funktionierenden Verschlüsselungsmethode, die Rivest, Shamir und Adleman entwarfen, wird sicher ihren Teil zur Popularität von Alice und Bob beigetragen haben.

36 In den Computern, die für die kryptographischen Berechnungen und die Übermittlung verschlüsselter Nachrichten verwendet werden, ist die Geschlechterdifferenz bereits mit dem Turing-Test eingezogen (vgl. Bergermann 2018, 339–340; Draude 2017, 190–194).

über die vielfältigen Situationen, in die Alice und Bob hineingeschrieben wurden, liefert nur ein Jahr nach Blum die anekdotisch gehaltene *After Dinner-Speech* des Kodierungstheoretikers John Gordon. Und tatsächlich haben Alice und Bob ein bewegtes Leben, das sich auch nicht mehr nur auf die Kryptologie beschränkt, sondern sich sukzessive auf weitere Disziplinen ausweitet: »Over the years Alice and Bob have tried to defraud insurance companies, they've played poker for high stakes by mail, and they've exchanged secret messages over tapped telephones« (Gordon 2007, 344). Gordon (ebd.) merkt scherzhaft an, sein Vortrag »may be the first time a definitive biography of Alice and Bob has been given« – tatsächlich liefert er allerdings nicht nur eine Biographie, sondern gleichsam einen Überblick über die verschiedenen Funktionalitäten, die Kryptographie in sich vereint. Ein fiktives Szenario sticht dabei besonders hervor, da es mit Katz und Lindell (2008, 3) exemplarisch für das erweiterte Anwendungsgebiet moderner Kryptographie steht, zu dem »problems of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash and more« zählen:

> »So you see Alice has a whole bunch of problems to face. Oh yes, and there is one more thing I forgot to say – Alice doesn't trust Bob. We don't know why she doesn't trust him, but at some time in the past there has been an incident. Now most people in Alice's position would give up. Not Alice. She has courage which can only be described as awesome. Against all odds, over a noisy telephone line, tapped by the tax authorities and the secret police, Alice will happily attempt, with someone she doesn't trust, whom she cannot hear clearly, and who is probably someone else, to fiddle her tax returns and to organize a coup d'etat, while at the same time minimizing the cost of the phone call.« (Gordon 2007, 345)

Da der Kodierungstheoretiker Gordon seinen Vortrag mit dem Satz »A coding theorist is someone who doesn't think Alice is crazy« (ebd.) schließt, folgern DuPont und Cattapan, dass auch Gordon Alice und Bob letztlich nur »for their typical purpose: as means to an explanatory end« (DuPont/Cattapan 2017, 10) gebrauche. Die Geschichten von und mit Alice und Bob lediglich als ein (pädagogisches) Mittel zum Zweck zu verstehen, wäre jedoch zu kurz gegriffen, denn, wie Haraway (1997, 125) bemerkt: »Stories are not ›merely‹ anything.« DuPont und Cattapan benennen Alice und Bob zwar ebenfalls als »tropes of cryptology research«, dennoch suggeriert die Kritik, die sie an Gordon üben, ein flacheres Verständnis von *tropes*, als an dieser Stelle produktiv wäre. Die

Geschichten von Alice und Bob, mit denen Paper wie auch Lehrbücher beginnen, stellen einen Bezug her zwischen Kryptographie und dem (eigenen) Alltag. Damit qualifizieren sich Alice und Bob für pädagogische Zwecke – doch sie dienen dort nicht nur als Mittel zum Zweck, sondern arbeiten an den Modellen mit, indem mit ihren Geschichten eine konkrete Situation mit den dazugehörigen Regeln, Einschränkungen, und Zielen erläutert und verkörpert werden kann. Ulrike Bergermann (2016, 280) schreibt in ihrer Untersuchung der Gründungsdiskurse von Kybernetik und Medienwissenschaft, die Rolle von Modellen liege in »der Verminderung der Komplexität von Theorie«. Modelle

> »[…] vermitteln zwischen Spekulationen und Experimenten, sie verzahnen Natur mit Theorie, und ihr Bau findet in einem Zwischenraum zwischen Phänomenen und Theoriebildung statt, in einer Darstellung, die dem menschlichen Denken und Wahrnehmen angepasst ist, auch wenn ein Fachvokabular noch gar nicht existiert.« (Ebd.)

Modelle schaffen ein Verständnis für einen konkreten Fall, aber auch die Gesetzmäßigkeiten, in die er eingebettet ist, ohne dass, wie Bergermann herausstellt, bereits ein Fachvokabular vorhanden sein muss. Dies ist möglich, da die erzählte modellhafte Geschichte die Gesetzmäßigkeiten einer problematisierten Situation so verkörpert, dass diese in den jeweiligen kryptologischen Schriften aus ihr abgeleitet werden können.[37] Im Fall der Kryptographie, ließe sich hier einwenden, gehe es jedoch weniger darum, »Natur« mit »Theorie« zu verzahnen, schließlich könne nicht behauptet werden, dass diese – wie beispielsweise Physik oder Biologie – Bezug auf ein in der Welt vorhandenes Material nehme, um dieses mit wissenschaftlicher Theoriebildung zu einem Gegenstand zu verschmelzen, kurz: es könne nicht behauptet werden,

37 Bei Blum ergeben sich also aus der eingangs geschilderten Situation, dass Alice und Bob sich nach einer Scheidung telefonisch per Münzwurf darauf einigen wollen, wer das Auto bekommt, bereits folgende Gesetzmäßigkeiten: 1.) Alice und Bob vertrauen sich nicht (mehr), weswegen das entwickelte Verfahren so aufgebaut sein muss, dass keine Partei die andere hintergehen kann; 2.) sie leben in verschiedenen Städten und können (oder wollen) sich daher nicht treffen, was die Notwendigkeit der Entwicklung eines komplexen Verfahrens bedingt – ansonsten hätten sie einfach bei einem gemeinsamen Treffen in leiblicher Ko-Präsenz eine Münze werfen können – wodurch auch das Erkenntnisinteresse des Aufsatzes plausibilisiert wird. Bemerkenswert ist an dieser Stelle auch, in welcher Weise klischeehaft-heteronormative Erzählstrategien an den Gesetzmäßigkeiten und ihrer Plausibilisierung mitarbeiten.

dass Mathematik ebenfalls situiertes Wissen produziere.[38] Mit Donna Haraway lässt sich dieser Einwand entkräften: Anhand eines von Helen Watson-Verran und David Turnbull durchgeführten Vergleichs europäischer Praktiken formaler Logik mit denen der Yolngu, eines indigenen australischen Volksstammes, bemerkt Haraway (2018, 140), dass die Praktiken zwar ähnlich seien, der konstituierende Prozess der Kategorienbildung sich jedoch signifikant unterscheide. Daraus folgt für Haraway (ebd.):

> »Full of tropes, mathematics is specific material-semiotic practice at every level of its being, without ceasing to be of fundamental interest in terms of processes of cognition and products of formal knowledge. Mathematical knowledge is situated knowledge.«

Was Haraway hier für die Mathematik konstatiert, gilt auch für die neuere Kryptographie, deren elementarer Kern aus Mathematik besteht. Auch die Kryptographie erzeugt situiertes, also materiell-semiotisches Wissen, das gebunden ist an Mathematik, Medialität und, nicht zuletzt, an Alice und Bob als *Trope*. »In Greek«, führt Haraway (1997, 125) aus, »*tropos* means a turning; and the verb *trepein* means to swerve, to not get directly somewhere. Words (not to mention sentences) trip us, make us swerve, turn us around; and we have no other options.« Es gibt folglich kein *eigentliches Sprechen*, keine Alternative »to going through the medium of thinking and communicating, no alternative to swerving, materially« (ebd.). *Tropism* ist für Haraway nicht nur mit Metaphern verbunden, sondern auch mit Modellen. Letztere sind, so schreibt sie, ob konzeptuelle oder physische, *uneigentliches Sprechen* »in the sense of instruments built to be engaged, inhabited, lived« (Haraway 2018, 135). Mit den Jahren sind verschiedene Figuren entstanden, die mit Alice und Bob die Modell-Geschichten bewohnen. Spätestens mit Bruce Schneiers (Lehr-)Buch *Applied Cryptography*, das 1994 zum ersten Mal erschien, wurden diese Figuren im Feld kanonisiert: In einer mit »Dramatis Personae« betitelten Tabelle listet Schneier (2015, 23) außer Alice und Bob noch Carol (»Participant in the three- and four-party protocols«), Dave (»Participant in the four-party protocols«), Eve (»Eavesdropper«), Mallory (»Malicious active attacker«), Trent (»Trusted arbitrator«), Walter (»Warden; he'll be guarding Alice and Bob in

38 Dies kann durchaus als das Erbe der im Europa des 19. Jahrhunderts herausgebildeten *formalistischen Mathematik* aufgefasst werden, innerhalb derer die Mathematik als ein in sich geschlossenes System ohne Bezug auf etwas, das ihr äußerlich sei, konzeptualisiert wurde (vgl. Heintz 1993, 16).

some protocols«), Peggy (»Prover«), und Victor (»Verifier«) auf. Mit »Dramatis Personae« werden in der Regel vor Beginn des Dramentexts die handelnden Personen eines Bühnenstücks und deren Rolle in demselben eingeführt – bei Schneier sind es die Protagonist_innen kryptographischer Protokolle, also festgelegter, sich wiederholender Abläufe. Die Wiederholung der Charaktere in Geschichten, die oftmals heterosexuelle Paarbeziehungen durch Heirat, Scheidung oder Dating von Alice und Bob thematisieren, arbeiten auf mehreren Ebenen: Sie bringen einerseits das Geschlecht der Figuren hervor, insofern Geschlechtsidentität wie Judith Butler (2002, 302, Herv. i.O.) formuliert, »durch eine *stilisierte Wiederholung von Akten* zustande kommt«, und entwerfen darüber hinaus eine heteronormative Ordnung. Weiterhin lassen sich durch die Wiederholung der Charaktere, die durch ihre Rollen sinnbildlich für spezifische kryptographisch relevante Aktionen stehen, die geschilderten Alltagssituationen nicht nur in ein Modell übersetzen, sondern werden die Alltagssituationen als kryptographische Systeme *formalisiert*, und gewinnen damit nicht nur einen deskriptiven, sondern auch einen präskriptiven Charakter. Alice und Bob sind damit in Haraways Sinne *Figuren*, sind *Tropen*, die nicht nur ins Denken bringen, sondern dieses Denken mitgestalten. Mit Alice und Bob sind die Geschichten, die Modelle, aber auch die mathematischen Beweisführungen und Ergebnisse der Kryptographie »tropic to the core and *therefore* part of knowledge practices« (Haraway 2018, 141, Herv. i.O.), die die mit ihnen eingeleiteten kryptographischen Verfahren an zeitgenössische gesellschaftliche Fragen und Begehren rückbinden.

Ent/Politisierungen

»In den computertechnischen Schriften«, formuliert Ulrike Bergermann (2018, 339) in *biodrag. Turing-Test, KI-Kino und Testosteron*, »kommen Kultur und Gesellschaft in der Regel nicht vor – nur in den Beispielen zu den Regeln schlendern sie wieder hinein; für die Wissenschaft erschienen sie ausgegliedert, in die Kultur, die Fiktionen, in Filme.« So entsteht der Eindruck von Selbstgenügsamkeit eines scheinbar in sich geschlossenen Systems, obwohl bereits in Alan Turings *Imitationsspiel* Gender »grundlegend in die Modellierung eingetragen« war, was jedoch, wie Bergermann (ebd., 340) ausführt, »durch die Folgemodellierer, die Computergeschichte schreiben, ostentativ ausgeblendet« worden war. Mit Alice und Bob schlendern, wie gezeigt wurde, Kultur und Gesellschaft, sowie »Lust, Liebe, Begehren« (ebd., 339) im Feld der Kryptographie allerdings nicht nur in den Beispielen zu den Regeln, sondern auch in die Expositionen der Probleme und in die Modellbildung hinein.

So halten mit diesen Geschichten, die mal absurde, mal verhältnismäßig realistische (Alltags-)Situationen schildern, im Vergleich zu ihrer ca. 4000 Jahre alten, überwiegend militärischen Geschichte eine Vielzahl an gesellschaftlichen Zusammenhängen und Begehren in das Feld der Kryptographie Einzug.

Dies drückt sich auch in den Visualisierungen von Alice und Bob aus, die nicht lange auf sich warten ließen. Wurden in Schneiers *Applied Cryptography* in einer direkt auf die tabellarische Übersicht der »Dramatis Personae« folgenden Grafik, die verschiedene kryptographische Protokolle veranschaulicht, Alice, Bob und Trent noch nicht als Personen, sondern als Häuser dargestellt (vgl. Schneier 2015, 24), so sollte sich dies in den darauf folgenden Jahren mit dem Zusammenwachsen von Kryptologie und Informatik im Bereich der IT-Sicherheit verändern, nicht zuletzt durch die Popularisierung von computergestützten Präsentationen und Clip-Art: »[F]aculty began to portray Alice and Bob in a classroom setting using clip art and other images that personified Alice and Bob (usually in white, heteronormative,[39] and gendered ways) […].« Als Gegenprogramm zu der scheinbar selbstverständlichen *Whiteness* von Alice und Bob in diesen Darstellungen schlug der indische Kryptograph Srini Parthasarathy (2012, 4) vor, Alice und Bob durch *Sita* und *Rama* zu ersetzen. Parthasarathy (ebd., 2) sieht zwei Vorteile in dieser Ersetzung: Zum einen, dass Sita und Ramas Anfangsbuchstaben mit den Anfangsbuchstaben von *sender* und *receiver* übereinstimmen. Zum anderen, dass eine Szene aus der Geschichte von Sita und Rama in der hinduistischen Mythologie, genauer im *Sundara Kanda*, dem fünften Buch des *Ramayana*, dem technisch-postalischen Übertragungsmodell, und damit der initialen Situation der Kryptographie bereits sehr ähnlich ist: Sita wurde von Ravana entführt und in einem Wald gefangen gehalten. Sie wird von Hanuman aufgesucht, einer hinduistischen Gottheit in Gestalt eines Affen, der von Rama geschickt wurde, was er durch einen Ring Ramas nachweisen kann. Sita gibt Hanuman eine Nachricht, die er an Rama übermitteln soll. Als Nachweis, dass die Nachricht wirklich von ihr ist, gibt Sita Hanuman ein Schmuckstück von ihr mit. Parthasarathy (ebd., 2–3) folgend entspräche Hanuman dem Medium oder Kanal, und Ravana, der die Nachricht abfangen möchte, dem *störenden Dritten*. Diese Geschichte kann, wie Parthasarathy

39 DuPont und Cattapan (2017, 11–12) führen dazu die Entwicklung von Eve (eavesdropper) von einer lauschenden Partei ohne spezifischem Interesse an, das sich mit der Zeit zum Bild von Eve als verlassener Frau wandelte, die die Kommunikation ihres Ex-Partners Bob mit dessen neuer Partnerin Alice belauscht.

ausführt, modellhaft sowohl für Verschlüsselung als auch für digitale Signaturen verwendet werden. Parthasarathys Vorschlag stieß jedoch, wie er anmerkt, nicht auf viel Zustimmung: »Some people […] seemed to have issues with using Hindu names, adding a religious and xenophobic flavour to the conversation« (ebd., 4), was sich als Zeichen sowohl der *Whiteness* von Alice und Bob als auch des innerfachlichen Diskurses der Kryptographie und der IT-Sicherheit sowie der rassistischen Exklusionsmechanismen akademischer Institutionen der westlichen Welt lesen lässt.

Die (Clip-Art-)Darstellungen von Alice und Bob sind darüber hinaus auch Bestandteil der Kritik des US-amerikanischen Kryptographen Phillip Rogaway an der Ausrichtung der Kryptographie als akademischer Disziplin. In seinem Vortrag mit dem Titel *The Moral Character of Cryptographic Work* ermahnt Rogaway seine eigene wissenschaftliche Community, nicht zu vergessen, dass Kryptographie in Machtverhältnisse eingebettet ist, und auch an diesen mitarbeitet. Dieser Umstand werde innerhalb des Fachs selbst nicht oft thematisiert, wie er zugespitzt formuliert:

> »Most academic cryptographers seem to think that our field is a fun, deep, and politically neutral game – a set of puzzles involving communicating parties and notional adversaries. This vision of who we are animates a field whose work is intellectually impressive and rapidly produced, but also quite inbred and divorced from real-world concerns.« (Rogaway 2015, 1)

Diese Art des Denkens wird von Rogaway (ebd., 16) heftig kritisiert: »Some might think that a community's focus is mostly determined by the technical character of the topic it aims to study. It is not. It is extra-scientific considerations that shape what gets treated where.« Einen Teil dieser außerhalb der Wissenschaft stehenden Überlegungen machen für Rogaway die zur Zeit des Vortrags erst zwei Jahre alten Enthüllungen des Whistleblowers Edward Snowden aus, die eine noch nicht da gewesene Form der Massenüberwachung von Bürger_innen der ganzen Welt durch Geheimdienste offenbarten. In seinem Vortrag macht Rogaway seinem Unmut darüber Luft, dass die akademische kryptographische Community nach den Snowden-Enthüllungen scheinbar keinen Handlungsbedarf sehe, und legt anhand eines Exkurses dar, dass es keine unpolitische Wissenschaft geben könne, lediglich eine (falsche) Leugnung der eigenen Verantwortung als Wissenschaftler_in. Das in der Einleitung seines Arguments aufgerufene Bild des Puzzles hat wissenschaftsgeschichtlich durchaus Tradition: Der Wissenschaftshistoriker

Thomas Kuhn, dessen Buch *The Structure of Scientific Revolutions*[40] sich mit der Rolle von wissenschaftlichen Paradigmen, Paradigmenwechseln und der Konzeptionalisierung von wissenschaftlichem Fortschritt befasst, geht ausführlich auf das Lösen von Puzzles als Teil der Herstellung von Wissen der sogenannten »normal science«[41] (dt.: *normale Wissenschaft*) ein. Eine der bemerkenswertesten Eigenschaften der Forschungsfragen *normaler Wissenschaft* sei laut Kuhn (1996, 35), »how little they aim to produce major novelties, conceptual or phenomenal.« Sie würden dennoch gestellt und bearbeitet, da sie dazu beitragen, das zu einem gegenwärtigen wissenschaftlichen Paradigma gehörende Wissen zu verfeinern und zu erweitern (vgl. ebd., 36). Was die beteiligten Wissenschaftler_innen motiviere, sich solchen Forschungsfragen zu widmen, deren Ergebnisse bereits zu antizipieren seien, erklärt sich für Kuhn durch die motivierende Wirkung des Puzzle-Lösens, und damit durch die höhere Bewertung des Weges als des Ergebnisses: »Bringing a normal research problem to a conclusion is achieving the anticipated in a new way, and it requires the solution of all sorts of complex instrumental, conceptual, and mathematical puzzles« (ebd.).[42] Ebendiese Puzzles stellen Kuhn zufolge eine eigene Kategorie wissenschaftlicher Probleme dar, für die Einfallsreichtum und Fähigkeit in der Bearbeitung eher im Vordergrund stünden als dass das Problem eine interessante oder wichtige Lösung habe

40 Kuhns Überlegungen zum Paradigma in der Wissenschaft waren grundlegend für Donna Haraways Diskussion der Metapher, wie sie in *Crystals, Fabrics, and Fields. Metaphors of Organicism in Twentieth-Century Developmental Biology* darlegt (vgl. Haraway 1976, 1–32). Aus diesen Überlegungen entstand sukzessive Haraways erweiterter Begriff der *Trope*.

41 Als *normale Wissenschaft* definiert Kuhn (1996, 10) »research firmly based upon one or more past scientific achievements, achievements that some particular scientific community acknowledges for a time as supplying the foundations for its further practice.« Moderne Kryptographie lässt sich damit im Sinne Kuhns als *normale Wissenschaft* klassifizieren.

42 Kuhn (1996, 36) zieht explizit Parallelen zwischen Puzzles als wissenschaftlicher Problemkategorie und Puzzles und Kreuzworträtseln (englisch: crossword *puzzles*) als Alltagsgegenständen, und geht darauf ein, dass das Lösen eines Puzzles einen Forschungsanreiz darstelle: »The man who succeeds proves himself an expert puzzle-solver, and the challenge of the puzzle is an important part of what usually drives him on.« Was an dieser Stelle spannend wäre, aber leider zu weit führen würde, wäre anhand des vom britischen Geheimdienst GCHQ herausgegebenen *GCHQ Puzzle Book* (vgl. MacAskill 2018) genauer über den Status wissenschaftlicher Puzzles als Spiele nachzudenken.

(vgl. ebd., 36–37) – das *wie* ist in diesem Fall also bedeutsamer als das *was*.[43] Der bisher dargelegte repetitive Charakter kryptographischer Forschung, der sich sowohl für *klassische*, und später für *moderne* Kryptographie im zugrunde liegenden technisch-postalischen Übertragungsmodell zeigt, hat größtenteils Forschungsfragen hervorgebracht, die sich mit Kuhn als ebendieser Kategorie von Puzzles zugehörig beschreiben lassen. Alice und Bob haben dabei, wie bereits dargelegt wurde, ihren illustrativen Charakter hinter sich gelassen, und sind mit Haraway als Trope zu verstehen: Die von ihnen ausgehend erzählten Geschichten, ihre Probleme, die es zu lösen gilt, bringen Forscher_innen ins Denken. Allerdings, und dies ist der Ansatzpunkt von Rogaways Kritik, in ein entpolitisiertes Denken, das durch die Darstellungskonventionen der Charaktere hervorgerufen werde:

> »There is a long tradition of cutesiness in our field. People spin fun and fanciful stories. Protocol participants are a caricatured Alice and Bob. Adversaries are little devils, complete with horns and a pitchfork. Some crypto talks are so packed with clip-art you can hardly find the content. I have never liked this, but, after the Snowden revelations, it started to vex me like never before.« (Rogaway 2015, 41)

Rogaway fordert eine Bereinigung der Kryptographie von ihrer lieb gewonnenen Trope, die sich nahezu memetisch durch Präsentationen, Paper und das Denken der Community zieht. Einerseits, da diese Figuren seiner Wahrnehmung nach überhandnehmen, und anstatt Sachverhalte verständlicher zu gestalten, einen »layer of obfuscation« erzeugten, »that must be peeled away to understand what has actually been done« (ebd., 41). Andererseits, da die Geschichten und Probleme der fiktiven Charaktere von den eigentlichen Gegenspielern ablenkten, was Konsequenzen für die Forschung habe:

> »Worse, the cartoon-heavy cryptography can reshape our internal vision of our role. The adversary as a $53-billion-a-year military-industrial-surveillance complex and the adversary as a red-devil-with-horns induce entirely different thought processes. If we see adversaries in one of these ways, we will actually see at a different set of problems to work on than if we see things in the other.« (Ebd., 41–42)

43 Kuhn (1996, 37–38) konstatiert, dass solche Puzzles eine motivierende Anziehungskraft auf »the proper sort of addict« (ebd., 38) – also auf Wissenschaftler_innen – ausüben würden, die in einer Vielzahl an Möglichkeiten begründet liegen könne, aufgrund derer eine Person sich dazu entschließen könne, zu forschen.

Diese Entpolitisierung, die Rogaway, wie er mehrfach betont, vor allem nach den Snowden-Enthüllungen untragbar erscheint, verstelle den Blick auf den titelgebenden *moral character* der eigenen Arbeit: Sie lenke von der Frage ab, welche Probleme aus Sicht der Geheimdienste, die er als die eigentlichen Gegenspieler identifiziert, von der Wissenschaft lieber *nicht* gelöst werden sollten (ebd., 42). Rogaway kritisiert darüber hinaus die monetäre Verstrickung der Universitäten mit Geheimdiensten, und macht sich daran, die innerfachlich diskursiv entpolitisierte Kryptographie wieder aktiv zu politisieren:

> »I have heard it said that if you think cryptography is your solution, you don't understand your problem. If this quip is true, then our field has gone seriously astray. But we can correct it. We need to make cryptography the solution to the problem: ›how do you make surveillance more expensive?‹« (Ebd., 46)

Ist das also das Ende von Alice und Bob? Rogaways Kritik war vermutlich weniger einflussreich, als er gehofft haben dürfte. Alice und Bob sind wohlauf, und ihr Einfluss auf das Feld scheinbar ungebrochen. Es dürfte sich darüber hinaus als unmöglich erweisen, sich einer Trope vorsätzlich gänzlich entledigen zu wollen, denn schließlich sind Tropen an der Herstellung von Wissen beteiligt und daher mit diesem verwoben. Sich der Frage zu widmen, wie Massenüberwachung teurer – und damit erschwert oder verhindert werden könne – ist erfreulicher Weise dennoch zum Problem zeitgenössischer Kryptographie geworden (vgl. exemplarisch Auerbach et al. 2018; Bellare et al. 2014; Degabriele et al. 2015). Umformuliert könnte Rogaways Frage lauten: Wie kann man vor Massenüberwachung sicher sein? Dies führt zum letzten Teil dieses Kapitels, in dem abschließend darauf eingegangen wird, wie innerhalb der Kryptographie definiert wird, was *Sicherheit* ist.

2.5.3 Sicherheit in der Kryptographie

In den bisherigen Ausführungen ist deutlich geworden, dass klassische, aber auch moderne Kryptographie sich hauptsächlich damit befasst, eine Nachricht, die über einen als *unsicher* definierten Kanal gesendet wird, auf dem Transportweg vor einem *störenden Dritten* zu schützen – gelingt dies, so wurde entsprechend Sicherheit geschaffen. Mit dem Übergang von klassischer zu moderner Kryptographie und der Herausbildung von Kryptologie als Wissenschaft wurde auch innerhalb der noch vergleichsweise jungen Disziplin Sicherheit definiert, allerdings stets basierend auf dem technisch-postalischen Übertragungsmodell. Diese Definitionen befassen sich entsprechend

mit der Frage, welche Anforderungen an kryptographische Mechanismen gestellt werden müssen, damit ein System als sicher gilt. Ein Alternative zum technisch-postalischen Übertragungsmodell wird dabei jedoch nicht gesucht, und dementsprechend auch nicht über die Eigenschaften (und daraus resultierenden Beschränkungen) des zugrunde liegenden Sicherheitsbegriffs nachgedacht. Im Folgenden soll daher anhand eines Teilbereichs der Kryptographie namens *Beweisbare Sicherheit* (eng.: provable security, vgl. Koblitz 2007, 976) dargelegt werden, wie Sicherheit innerhalb der Disziplin Kryptographie weitergehend definiert wird. In einem zweiten Schritt soll diese Definition in einem größeren Kontext situiert werden.

Rigorose Definitionen

Moderne Kryptographie zeichnet sich im Vergleich zu klassischer Kryptographie wie bereits mehrfach bemerkt vor allem dadurch aus, dass Kryptographie von einer Kunst zu einer Wissenschaft geworden ist. Dieser Übergang ist verbunden mit der Formulierung einer rigorosen, also strengen Methodologie, sowie der Explizierung ansonsten unausgesprochen bleibender Vorannahmen, um Fortschritt herstellen und beurteilen zu können, sowie eine generelle Vergleichbarkeit der erfundenen Verfahren zu gewährleisten. Eines der Hauptkriterien dafür ist, dem Kryptographen Oded Goldreich (2004, 21) folgend, ein »rigorous treatment«, oder Jonathan Katz und Yehuda Lindell (2008, 18) folgend, eine »rigorous and precise definition of security«. Was Goldreich 2004 in *Foundations of Cryptography* über die Methode und die Notwendigkeit einer festen Definition von Sicherheit darlegt, nämlich die Notwendigkeit, ein kryptographisches System auf »firm foundations« (Goldreich 2004, 21) und nicht auf Heuristiken oder Intuitionen aufzubauen, sowie seine Überlegungen zur Wichtigkeit unbewiesener Annahmen darüber, was in welcher Zeit mit Computern berechnet werden kann (vgl. ebd., 22), lässt sich als Kernelement dessen beschreiben, was Katz und Lindell vier Jahre später als die drei Prinzipien moderner Kryptographie ausmachen. Das erste Prinzip besagt, dass für das Lösen eines kryptographischen Problems die bereits genannte Formulierung einer »rigorous and precise definition of security« (Katz/Lindell 2008, 18) notwendig sei. Diese sei aus verschiedenen Gründen wichtig: Erstens, um sicherzustellen, dass für ein gegebenes Sicherheitsproblem eine adäquate kryptographische Lösung designt wird, und das Design nicht erst nach Fertigstellung auf die notwendigen Funktionen hin überprüft wird; zweitens, da eine solche Definition eine Vergleichbarkeit verschiedener kryptographischer Systeme im Hinblick auf ihre Sicherheitsdienste und Effizienz

ermöglicht, und so eine Auswahl für ein konkretes Problem getroffen werden kann; und drittens, um eine generelle Vergleichbarkeit hinsichtlich mehr Faktoren als Effizienz und Sicherheitsdienste verschiedener kryptographischer Systeme herstellen zu können (vgl. ebd., 19). Nicht zuletzt ist es auch eine rigorose Sicherheitsdefinition, die es erlaubt, einen *rigorosen Beweis* für die Sicherheit eines gegebenen Systems zu geben (vgl. ebd., 20), denn nur wenn die Ansprüche an ein System klar definiert worden sind, kann eine Aussage darüber getroffen werden, ob sie eingehalten wurden. Darüber hinaus wenden sich Katz und Lindell (ebd., 20) explizit gegen die Annahme, eine formale Definition von Sicherheit sei nicht notwendig, da intuitiv klar sei, was *sicher* bedeute – selbst ein und dieselbe Person könne kontextabhängig unterschiedliche Vorstellungen dazu haben. Nach einigen beispielhaften Annäherungen stellen Katz und Lindell (ebd., 22) basierend auf dem ersten Prinzip moderner Kryptographie eine grundsätzliche Sicherheitsdefinition für moderne Kryptographie auf: »A cryptographic scheme for a given task is secure if no adversary of a specified power can achieve a specified break.« Durch die exponierte Position des zu verhindernden Brechens eines kryptographischen Systems schließt diese Definition auch an die von Kerckhoffs formulierte Wichtigkeit der Kryptanalyse für die Evaluierung kryptographischer Methoden an (vgl. Kahn 1967, 234–235). Der_die Angreifer_in bleibt bei Katz und Lindell dabei an einer entscheidenden Stelle absichtlich unterdeterminiert: Die vorgelegte Definition trifft zwar Aussagen über die Fähigkeiten des_der Angreifer_in, aber keine Aussagen über die gewählte Methode des Angriffs. Dies bezeichnen sie als »arbitrary adversary principle« (Katz/Lindell 2008, 22).[44] Auch Goldreich (2004, 21) geht darauf ein, dass es nutzlos sei, die Strategie des_der Gegner_in vorauszuplanen, da diese_r sich per se nicht an die Spielregeln halte: »the adversary will try to take actions other than the ones the designer has envisioned.« Annahmen über die Ressourcen der angreifenden Partei seien hingegen gerechtfertigt und notwendig (vgl. ebd.).

Das zweite Prinzip moderner Kryptographie besagt, dass wenn die Sicherheit eines kryptographischen Verfahrens auf einer unbewiesenen Annahme

44 Die Unterdeterminiertheit der angreifenden Partei zeigt sich auch in den Figuren, die den Angreifer_innen zugewiesen werden: Schneiers (2015, 23) »Dramatis Personae« beinhalten *Eve* und *Mallory*, die sich lediglich dadurch unterschieden, dass *Eve* (»eavesdropper«) passiv lauscht, und *Mallory* (»malicious active attacker«) aktiv angreift – wie genau dies durchgeführt wird, wird nicht beschrieben. Paar und Pelzls (2016, 4) *Oskar* (vermutlich abgeleitet von »Opponent«) ist ebenfalls nicht näher bestimmt.

basiert, diese so präzise und reduziert wie möglich zu definieren sei (vgl. Katz/Lindell 2008, 18). Katz und Lindell (ebd., 25) führen die schwere Lösbarkeit bestimmter mathematischer Probleme als Beispiel einer solchen unbewiesenen Annahme ein. Dieser Fall ist gar nicht so selten: Spätestens seit dem Aufkommen moderner Kryptographie basiert die Sicherheit kryptographischer Verfahren zu einem Großteil auf Einwegfunktionen, die deshalb als sicher gelten, weil ihre Umkehrung nicht in Polynomialzeit berechnet werden kann – jedenfalls bisher. Goldreich (2004, 22, Herv. i.O.) formuliert dazu pointiert: »Unfortunately, *making assertions about what can or cannot be efficiently computed is exactly what cryptography is all about*.« Die präzise und reduzierte Formulierung solcher Annahmen sind Katz und Lindell (2008, 24–25) zufolge sowohl für die Annahme selbst wichtig (je öfter diese durch ihre Anwendung getestet werde, ohne falsifiziert zu werden, desto vertrauenswürdiger werde sie), als auch für die Vergleichbarkeit kryptographischer Verfahren, wobei ein Verfahren, das auf einer vertrauenswürdigeren Annahme basiert, Vorzug zu gewähren sei. Darüber hinaus erleichtere eine klar definierte Annahme den Sicherheitsbeweis eines kryptographischen Verfahrens, indem sie eine klare Abhängigkeitskette schaffe: Ein Verfahren, das auf Annahme X basiert, ist sicher, wenn Annahme X stimmt. An dieser Stelle wird erneut das Prinzip der Modularisierung und dessen Rolle bei der Herstellung von Sicherheit sichtbar: Basiert ein kryptographisches Verfahren auf einer falsifizierten Annahme, so kann diese gegebenenfalls ausgetauscht werden, ohne das komplette Verfahren zu verändern.

Das dritte Prinzip moderner Kryptographie nach Katz und Lindell (ebd., 18) besagt schließlich, dass kryptographische Systeme über einen »rigorous proof of security« verfügen müssen. Die beiden vorherigen Prinzipien schaffen die Voraussetzungen für die Möglichkeit, einen solchen Nachweis zu erbringen (vgl. ebd., 26): Die Grundlage bildet das erste Prinzip durch die Definition dessen, was erreicht werden muss, damit ein System als sicher gilt. Das zweite Prinzip stellt eine genaue Abgrenzung der nicht-beweisbaren Anteile einer solchen Definition bereit. Ein Sicherheitsnachweis folgt daher in den meisten Fällen einem sog. »reductionist approach« gemäß der Formulierung »Given that Assumption X is true, Construction Y is secure according to the given definition« (ebd., 26).

Reduktionen

Der Vorgang der Reduktion taucht im Zusammenhang mit dem Erbringen von Nachweisen für die Sicherheit eines kryptographischen Systems mehrfach

auf, und ist auch Gegenstand der Kritik an »provable security« als Teilbereich der Kryptographie. Bereits eingeführt wurde der »reductionist approach« bei Katz und Lindell in Bezug auf die Erbringung eines Sicherheitsnachweises für kryptographische Systeme. Katz und Lindell (ebd., vi) merken im Vorwort ihres Buches an, dass sie keinen Unterschied zwischen Anwendung von und Theoriebildung für Kryptographie machen, und daher »do not separate ›applied cryptography‹ from ›provable security‹; rather, we present practical and widely-used constructions along with precise statements (and, most of the time, a proof) of what definition of security is achieved.« Der Kryptograph Neal Koblitz (2007, 976) beschreibt das Prinzip *Beweisbarer Sicherheit* folgendermaßen:

> »The idea of ›provable security‹ is to give a mathematically rigorous proof of a type of conditional guarantee of the security of a cryptographic protocol. It is *conditional* in that it typically has the form ›our protocol is immune from an attack of type X provided that the mathematical problem Y is computationally hard.‹«

Die an dieser Stelle modellhaft gegebene Sicherheitsdefinition entspricht der von Katz und Lindell. Eine gelungene Sicherheitsdefinition, führen diese an späterer Stelle weiter aus, »essentially provides a mathematical formulation of a real-world problem. If the mathematical definition does not appropriately model the real world, then the definition may be useless« (Katz/Lindell 2008, 22). Die Schwierigkeit, ein mathematisches Modell für die »real world« zu schaffen, die sich oft als widerständiger erweist als den Modellen zuträglich wäre, diskutieren Katz und Lindell (ebd., 23) anhand von zwei Szenarien. Einerseits könne die Implementierung eines mathematisch beweisbar sicheren Verfahrens in ein größeres System (z.B. in Software) andere Wege bereitstellen, mit denen das System dennoch erfolgreich angegriffen werden könne.[45] Darüber hinaus hänge im Fall von IT-Sicherheit ein mathematischer Sicherheitsbeweis davon ab, dass ein Computer ein bestimmtes Problem nicht lösen könne. »The problem is«, schreiben sie weiter, »that computation is a real-world process, and there are many different ways of computing« (ebd.,

45 Katz und Lindell (2008, 22–23) geben hier sog. *smart-cards* als Beispiel, also Plastikkarten, die beispielsweise als Zimmerschlüssel in Hotels verwendet werden. Diese bieten durch ihre physischen Eigenschaften eine Möglichkeit, wie der Schlüssel dennoch ausgelesen werden kann, nämlich durch die Messung der Veränderung der elektrischen Ladung der Karte bei ihrer Verwendung.

23). Daher müsse sichergestellt werden, dass die mathematische Definition von *Computation* dem entspreche, was *Computation tatsächlich* sei. Ein solcher Zugang erscheint in vielerlei Hinsicht als problematisch: Nutzungspraktiken sind vielfältig und können stark von der Designintention divergieren. Auf konkrete Anwendungsfälle hinarbeitende Antworten auf die Frage, was *Computation* sei, schreiben damit einen essentialistischen sowie instrumentellen Technikbegriff in die Überlegung ein. Katz und Lindell weiten ihre Überlegung jedoch noch weiter aus, wenn sie in diesem Zusammenhang die Überlegungen Alan Turings in seinem Aufsatz *On computable numbers, with an application to the Entscheidungsproblem* anführen, und konstatieren, dass Turing ein mathematisches Modell von *Computation* entwickelt habe, ähnlich wie es nun die Aufgabe von Kryptograph_innen sei, ein mathematisches Modell *der Welt* zu entwerfen (vgl. ebd., 23–24).

Kritik an diesem Ansatz wird auch innerhalb der kryptographischen Community geübt, wenn auch aus anderen Gründen: Neal Koblitz und Alfred Menezes haben in einigen gemeinsamen Aufsätzen die Grundannahmen *Beweisbarer Sicherheit* kritisch diskutiert (vgl. Koblitz/Menezes 2006; 2007a; 2007b). In seinem Aufsatz *The Uneasy Relationship Between Mathematics and Cryptography* fasst Koblitz die Kritik, die er gemeinsam mit Alfred Menezes an *Beweisbarer Sicherheit* geübt hat, knapp zusammen.[46] Hauptsächlich interessiert sich Koblitz dabei für die Rolle der Reduktion, allerdings mit einem anderen Schwerpunkt als Katz und Lindell: Während letztere sich hauptsächlich auf Reduktion im Sinne der Herstellung einer logischen Kette für die Erbringung eines

46 Koblitz beschreibt ebenfalls, dass seine und Menezes' Haltung innerhalb der kryptographischen Community auf reichlich Widerstand gestoßen ist. Bereits die erste Veröffentlichung der beiden zu dem Thema (vgl. Koblitz/Menezes 2007b) im *Journal of Cryptology* wurde nach einer heftigen Auseinandersetzung der Mitglieder des Herausgeber_innenteams von einer *Editor's Note* begleitet, in der die Publikation von Koblitz' und Menezes' Aufsatz gerechtfertigt wurde (vgl. Maurer 2007). Oded Goldreich, der ebenfalls Teil des Herausgeber_innenteams war, und die Publikation verhindern wollte, reagierte mit der Veröffentlichung eines Aufsatzes namens *On Post-Modern Cryptography* auf einem eprint-Server. In diesem Aufsatz, der sich besser als Schmähschrift in wissenschaftlicher Form bezeichnen lässt, kritisiert Goldreich (2012, 2) den Ansatz von Koblitz und Menezes als postmodern, denn, so formuliert er, »both post-modernism and the ›critique of rigorous analysis in Modern Cryptography‹ are reactionary (i.e., they play to the hands of the opponents of progress).« Im Verlauf des Artikels wird mehr als deutlich, dass Goldreichs Verständnis des Wortes postmodern derselbe Fehler eingeschrieben ist, der auch schon für die Science Wars kennzeichnend war: die Verkennung von Relationalismus als Relativismus.

Sicherheitsnachweises konzentrieren, und nur kurz auf die Schwierigkeit eingehen, die Welt auf ein mathematisches Modell zu reduzieren, setzt Koblitz' Kritik genau an dieser Stelle an. *Beweisbare Sicherheit*, formuliert Koblitz sein Unbehagen mit dem Term, schaffe eine Illusion von Sicherheit: Ein Aspekt dieser Illusion sei, dass (mathematisch) *Beweisbare Sicherheit* die Möglichkeit eines erfolgreichen Angriffs auf einen mathematisch-kryptographischen reduziere, was bedeute, dass jeder erfolgreiche Angriff das zugrunde liegende mathematische Problem gelöst haben müsse, wodurch ebenfalls eine Reihe weiterer Verfahren gebrochen seien. Andere Formen von Angriffen würden kategorisch ausgeschlossen (vgl. Koblitz 2007, 976–977).[47] Katz und Lindell (2008, 23) adressieren andere Formen von Angriffen nur implizit, und ihre Lösung besteht stets darin, das Modell zu verbessern. Koblitz' Kritik geht über den Ausschluss weiterer Angriffsmöglichkeiten hinaus und problematisiert auch die durch die Reduktion entstehende Kompartimentierung: Die Reduktion eines Sicherheitsproblems aus der echten Welt auf ein mathematisches Problem, und die Reduktion der Sicherheit eines kryptographischen Verfahrens auf die Bedingung, eine (bisher) unbewiesene Annahme sei korrekt, stellt für Koblitz eine Konditionalkette her. Der Begriff *provable security* sei für ein solches Verfahren »very misleading« (Koblitz 2007, 977), denn eine solche Konditionalkette sei nicht im selben Maße beweisbar wie beispielsweise der Satz des Pythagoras (der mathematisch restlos bewiesen ist), und werde oft dafür genutzt, Lai_innen zu beeindrucken und in falscher Sicherheit zu wiegen (vgl. ebd.).

Die Frage nach der Sicherheit, so lässt sich mit Koblitz' Kritik sagen, wird innerhalb der *provable security* als Teilbereich der Kryptologie mittels Reduktion entstehender Konditionalketten auf immer kleiner werdende Bereiche verschoben, aber nie zufriedenstellend geklärt. Dies ist ein Effekt der Reduktion selbst: Angriffe, die außerhalb von den modellhaft durch die Kette beschriebenen Fällen stehen, werden in den Modellen nicht mitgedacht. Darüber hinaus bauen die Glieder der Konditionalketten nicht so engmaschig logisch aufeinander auf, wie es den Anschein macht, da bei jeder Reduktion auf ein Modell

47 Dieser Einwand lässt sich als eine erneute Stärkung des Kerckhoffs'schen Prinzips begreifen, nach dem ein kryptographisches System nicht (nur) mathematisch, sondern auch praktisch nicht zu brechen sein sollte. Polemisch ließe sich Alfred North Whiteheads (1978, 39) wohl bekanntestem Zitat, »The safest general characterization of the European philosophical tradition is that it consists of a series of footnotes to Plato« folgend behaupten, die sicherste allgemeine Charakterisierung der kryptographischen Tradition Europas laute, dass sie aus einer Reihe von Fußnoten zu Kerckhoffs bestehe.

wichtige Aspekte und Widerständigkeiten der jeweils reduzierten Ebene verloren gehen. Während Katz und Lindell die mathematische Modellierung der Welt affirmieren, und davon ausgehen, dass der Hauptgrund für ein gescheitertes Sicherheitsverfahren eine ungenaue Abbildung der Welt durch das Modell sei, lässt sich das Verhältnis von Modell und Welt weitergehend problematisieren. Die oft geübte Kritik, Kryptographie und IT-Sicherheit würden versuchen, technische Lösungen für soziale Probleme zu finden, muss, um nicht erneut affirmativ mit einer noch genaueren Modellierung beantwortet zu werden, den zugrunde liegenden Sicherheitsbegriff problematisieren, dem sich bisher hauptsächlich in nachvollziehender Weise aus der Perspektive der Kryptologie genähert wurde.

Negative Sicherheit

Ob ein Verfahren, eine App, ein Programm sicher ist, um damit zur Ausgangsfrage dieses Kapitels zurückzukommen, kann also mit ja beantwortet werden, falls diese(s) eine bestimmte Leistung erfüllt: Die Einhaltung der zuvor gemachten Angaben, was wie lange und wie stark wovor geschützt werden soll. Was Sicherheit ist, wird innerhalb der Kryptologie also relational auf eine zuvor bestimmte Gefahr hin konzipiert, die in den Ausführungen zum unsicheren Kanal mit Sybille Krämer als das *störende Dritte* des technisch-postalischen Übertragungsmodells von Kommunikation bestimmt wurde. Die folgenden Überlegungen beziehen sich der Klarheit halber ausschließlich auf diese Form der verschlüsselten Kommunikation, und lassen die weiteren Anwendungsgebiete und Funktionen von Kryptographie außen vor.[48]

In der Sicherheitsforschung der letzten Jahre hat sich eine Unterscheidung verschiedener Sicherheitsbegriffe etabliert, die bisher in der vorliegenden Untersuchung nicht thematisiert wurde. Dass diese Unterscheidung nicht ganz augenfällig ist, mag auch an einer sprachlichen Ungenauigkeit liegen: Im Englischen gibt es mehrere Wörter – *security*, *safety* und *certainty* – die dem deutschen Wort *Sicherheit* entsprechen, aber unterschiedlich konnotiert

48 Weiterhin sollen die an dieser Stelle getätigten Aussagen über die strukturelle Verfasstheit kryptographischer Sicherheit nicht als großes Argument über die grundsätzliche Funktionsweise von Sicherheit in der Kryptographie im Sinne einer *strong theory*, die ungenau (genug) ist, um ein großes Feld zu organisieren, verstanden werden, denn die Sicherheitsdienste kryptographischer Verfahren sind, wie in diesem Kapitel bereits etabliert, vielfältig und nicht nur auf den Vorgang des Austauschs verschlüsselter Nachrichten zwischen zwei Parteien beschränkt.

sind und auf verschiedene Sicherheitsbegriffe verweisen. Während *certainty* ebenfalls als Gewissheit übersetzt werden kann und daher an dieser Stelle vernachlässigbar ist, soll der für die vorliegende Untersuchung relevante Unterschied von *security* und *safety* genauer betrachtet werden. Die Differenz der beiden Begriffe fällt darüber hinaus auch je nachdem, ob man technisch-naturwissenschaftlichen oder sozial- und geisteswissenschaftlichen Diskursen folgt, erneut unterschiedlich aus.

Sowohl die IT-Sicherheit, die im Englischen *IT security* heißt, als auch die Kryptologie behandelt in ihren englischsprachigen Aufsätzen zumeist *security*. Weiterhin wird in diesen, ebenso wie in anderen naturwissenschaftlich-technischen Fächern, die mit der Konstruktion und dem Erhalt von Infrastrukturen befasst sind, wenn auch nicht immer ganz trennscharf, zwischen *security* und *safety* unterschieden (vgl. Pièrre-Cambacédès/Chaudet 2010). Unter dem Begriff *security* werden dabei in der Regel »malicious risks« verhandelt, wohingegen *safety* im Zusammenhang mit »purely accidental risks« verwendet wird (ebd., 59) – *security* bezeichnet das Sichern eines Systems *vor* absichtlichen Störungen, *safety* bezeichnet das Sichern des Systems *für* die Nutzer_innen oder auch die Umwelt, die durch das System nicht zu Schaden kommen sollen.[49] Angesichts dieser Unterscheidung ist es verständlich, dass sich Kryptologie, aber auch IT-Sicherheit, mit dem Ausschluss eines *störenden Dritten*, mit *security* befasst.

Sozial- und geisteswissenschaftliche Unterscheidungen von *safety* und *security* sind an verschiedenen Modi von Sicherheit interessiert, die sie auf ihre Praktiken und Rollen in gesellschaftlichen Kontexten hin untersuchen.[50] In seinem Aufsatz *Das Grundgefühl der Ordnung, das alle haben. Für einen queeren*

49 Ein Beispiel für die Diskussion von *safety* wäre die Sicherheit teilautomatisierter Herstellungsprozesse, in denen Menschen in Fabriken mit großen Industrierobotern auf engem Raum zusammenarbeiten. Damit die Sicherheit (*safety*) der menschlichen Arbeiter_innen garantiert werden kann, müssen die maschinischen Arbeiter_innen speziellen Sicherheitsprotokollen folgen, wie beispielsweise sich im Fall eines außerplanmäßigen Zwischenfalls abzuschalten.

50 Einen Überblick der Diskussion innerhalb der Sicherheitsforschung geben beispielsweise Folkers (2020) und Roe (2014). Da dieses Buch weniger an einer allgemeinen Diskussion von Sicherheitsbegriffen interessiert ist als an einer queeren Lesart von Sicherheit, werde ich diese Untersuchungen weitestgehend ausklammern, und stattdessen hauptsächlich mit Texten arbeiten, die ebenfalls Anschlusspunkte an die Queer Theory beinhalten.

Begriff von Sicherheit[51] nimmt der Philosoph und Sozialwissenschaftler Daniel Loick unter anderem eine historisierende und vergleichende Analyse negativer und positiver Sicherheit vor. Für diese Unterscheidung bezieht sich Loick auf Melanie Brazzells Arbeit zu *intersektionaler transformativer Gerechtigkeit*, einem in aktivistischen Räumen entwickelten Konzept geteilter Verantwortungsübernahme für Gewalt(-prävention). In den USA unter dem Namen *transformative justice* entwickelt, soll dieser dem Abolitionismus zugehörige Ansatz Communities dazu befähigen, Gerechtigkeit für von Gewalt betroffene marginalisierte Personen[52] zu schaffen, die von staatlichen Strukturen diskriminiert werden und sich daher nicht auf die staatliche Rechtsprechung verlassen, oder diese gar nicht erst in Anspruch nehmen können oder wollen.[53] Brazzell (2019, 19) unterscheidet in *Was macht uns wirklich sicher? Ein Toolkit zu intersektionaler transformativer Gerechtigkeit jenseits von Gefängnis und Polizei* zwischen einer liberalen Vorstellung von Sicherheit, und einer Konzeptionalisierung von Sicherheit im Sinne transformativer Gerechtigkeit. Die liberale Vorstellung von Sicherheit bestimme diese negativ, insofern sie auf die Abwesenheit konkreter Gewalttaten fokussiert sei, dadurch jedoch strukturelle Gewalt nicht in den Blick nehmen könne. Eine Konzeptionalisierung von Sicherheit im Sinne transformativer Gerechtigkeit sei positiv bestimmt, da sie keinen Schutz durch eine externe Autorität suche, sondern die Mitglieder einer Gemeinschaft selbstbestimmt ein soziales Konzept von Sicherheit für ihre Community entwerfen und umsetzen können. Brazzells Gegenüberstellung aufnehmend, unterscheidet auch Loick (2021, 267–268) zwischen *negativen* und *positiven* Konzeptionen von Sicherheit, um schließlich einen *queeren* Sicherheitsbegriff entwickeln zu können.[54] Negative Sicherheit definiert Loick als Sicherheit *vor*, und weist ihr die englische Entsprechung *security* zu, während positive Sicherheit von ihm als Sicherheit *zu* beschrieben

51 An dieser Stelle möchte ich mich bei Daniel Loick dafür bedanken, dass er mir seinen Aufsatz *Das Grundgefühl der Ordnung, das alle haben. Für einen queeren Begriff von Sicherheit* schon vor dessen Veröffentlichung zur Verfügung gestellt hat.

52 Brazzell (2019, 158) nennt unter dem Akronym QTIBPOC »Queer Trans* Inter* Black und People of Color«.

53 Brazzell (2019, 17) weist darauf hin, dass auch manche feministische Strömungen Gefahr laufen, sich kompliz_innenhaft mit einem strafenden Staat zu verhalten, und so rassistische und nationalistische Diskurse zu stärken.

54 Letzterer wird für die Analyse von Backdoors noch eine größere Rolle spielen und daher auch erst an späterer Stelle ausführlich erläutert. Auf positive Sicherheit werde ich nur am Rande eingehen, da dieses Konzept für die weiteren Ausführungen irrelevant ist.

wird, die dem englischen Wort *safety* näher stehe (vgl. ebd., 267). Loick merkt an, dass sowohl negative als auch positive Sicherheit sich zunächst als Sicherheitskritiken herausgebildet haben (vgl. ebd.), was er im weiteren Verlauf seines Aufsatzes erläutert. Negative Sicherheit sei aus einem negativen Verständnis von Freiheit entstanden, das verknüpft sei mit dem Liberalismus, der sich im 18. Jahrhundert als eine Gegenbewegung zum von Foucault beschriebenen *Sicherheitsdispositiv* entwickelte (vgl. ebd., 268–270). Der Liberalismus definierte Freiheit als den größtmöglichen Handlungsspielraum einzelner Individuen, und richtete sich damit explizit gegen die »absolutistischen Kontrollansprüche des Staates« (ebd., 267), was sich vor allem in der Formation der Wirtschaft als privatem Bereich niedergeschlagen habe (vgl. ebd., 270). Freiheit, führt Loick (ebd.) weiter aus, »wird vom Liberalismus als eine Schranke definiert, die den Bürgern die Möglichkeit verschafft, ihre privaten Interessen vom Staat und den anderen Bürgern ungestört verfolgen zu können.« Die »Schranke« ist eine treffende Formulierung, da die Rolle des Staates, wie Loick konstatiert, in Bezug auf Sicherheit nicht komplett negiert, sondern vielmehr umgedeutet werde: »Sicherheit bedeutet nicht mehr die vollständige Überwachung des gesellschaftlichen Lebens, sondern die Aufrechterhaltung der Grenzen zwischen den voneinander isolierten individuellen Handlungssphären« (ebd., 267). Die Aufgabe der Grenzsicherung komme dem Staat zu: Sicherheit bedeute in diesem Kontext, dass die eigenen, privaten Interessen mit dem staatlichen Gewaltmonopol koexistieren konnten, indem »staatliche Gewalthandlungen zu Durchsetzungsinstrumenten privater Interessen umdefiniert« (ebd., 270) wurden.[55] Basierend auf Karl Marx' Reflektionen zu Sicherheit, die dieser als Versicherung des bürgerlichen Egoismus definiert, konstatiert Loick (ebd., 271, Herv. i.O.):

> »Weil sich die Gesellschaft [als] eine Summe unverbundener Individuen darstellt, die solipsistisch ihre je eigenen Interessen verfolgen, erscheint die Andere für mich immer nur potentiell als Bedrohung meiner Freiheit (daher Sicherheit *vor*). Die xenophobe Fortifizierungslogik, die das liberale Sicherheitsdenken bis heute kennzeichnet, entspringt also einem spezifischen sozialen »Grundgefühl«, welches eine wohlgeordnete Gesellschaft als Trennung, Nichteinmischung oder Nichtansteckung imaginiert.«

55 Aus diesem Zusammenhang erklärt sich auch die historische Hauptaufgabe der Polizei als »Verteidigung der kapitalistischen Wirtschaftsordnung gegen subversive Elemente, wozu sowohl die Gefahr von Landstreicherei als auch von Arbeiteraufständen gezählt wurde« (Loick 2021, 270).

Strukturell betrachtet kann es also als Ziel eines negativen Sicherheitsbegriffs angesehen werden, eine von außen kommende Bedrohung zu verhindern, wodurch auch die Figur des *störenden Dritten* wieder auf den Plan tritt, was den negativen Sicherheitsbegriff anschlussfähig an das Sicherheitskonzept der Kryptologie macht. Dass über die 4000jährige Geschichte der Kryptologie hinweg die Rolle des Staats stets im Wandel begriffen war, tut dieser Analogie keinen Abbruch, da diesem innerhalb kryptographischer Verfahren ohnehin keine feste Rolle zukommt – vielmehr geht es um die grundsätzliche Eigenschaft der Grenzziehung, die zentral am Konzept des un/sicheren Kanals verhandelt wird, der Ein- und Ausschlüsse herstellt.[56] Um die Anschlussstelle expliziter zu formulieren: Der Sicherheitsbegriff der innerhalb des technisch-postalischen Übertragungsmodells operierenden Kryptologie lässt sich strukturell als negativer Sicherheitsbegriff bestimmen, insofern er mit Grenzregulierung und dem Ausschluss des *störenden Dritten* befasst ist. Der von Loick diagnostizierten »xenophobe[n] Fortifizierungslogik«, und dem Aspekt der »Nichtansteckung«, oder vielmehr: den Politiken der Ansteckung, wird im nun folgenden Kapitel mit einer Diskussion des Sicherheitskonzepts der IT-Sicherheit anhand von aktuellen Schadsoftware-Fallbeispielen, sowie ihrer Entstehungsgeschichte in den 1980er Jahren nachgegangen.

56 Darüber hinaus zieht dies nicht automatisch nach sich, dass mit kryptographischen Mitteln zu operieren immer bedeuten müsse, einem negativen Sicherheits- oder Freiheitsbegriff zu folgen: Kryptographische Mittel können in den Händen von Akteur_innen unterschiedlichster Interessen liegen und verwendet werden. So kann ein Staat mittels Kryptographie seine eigenen Interessen schützen, oder Whistleblower_innen mittels Kryptographie ihr Wissen einer Öffentlichkeit zugänglich machen und auf eine Veränderung der von ihnen angeprangerten Lage drängen. Die jeweiligen Einsatzbereiche und Taktiken, in die kryptographische Verfahren in der Praxis eingebettet sind, können die beschriebene Funktionsweise kryptographischer Sicherheit politisch rekontextualisieren, sodass mit diesen Methoden gesamtgesellschaftlich eine andere Form von Sicherheit eingefordert und hergestellt werden kann. Dennoch lässt sich anmerken, dass vor allem die deutschsprachige Diskussion um Privatheit und Datenschutz, die unmittelbar mit Kryptographie verbunden ist, stark von einem negativen Freiheitsbegriff ausgeht, was sich im Konzept des *Selbstdatenschutz* niederschlägt. Internationaler, aber von ähnlichen Grundgedanken ausgehend ist die *Cypherpunk*-Bewegung (vgl. Hughes 1993), auf die auch Rogaway (2015, 46–47) im Zuge seiner Forderung nach einer Repolitisierung der Kryptographie affirmativ rekurriert. All diesen Ansätzen ist gemein, dass sie, um Privatheit einfordern zu können, Daten als Eigentum bestimmen. Für eine Kritik dieses Konzepts siehe exemplarisch Ochs (2015) und Sevignani (2012).