STUDIENSKRIPT

## Kryptologie

DLMCSEAITSC02

# Lernziele

Die Kryptologie als Lehre und Wissenschaft der vertraulichen Nachrichtenübermittlung umfasst die beiden Teilgebiete Kryptografie und Kryptoanalyse. Kryptografie ist die Wissenschaft der Verschlüsselung von Informationen, so dass diese nur für den vorgesehenen Empfänger entzifferbar sind. Kryptoanalyse dagegen ist die Wissenschaft von der Entschlüsselung von verschlüsseltem Text ohne Kenntnis des Schlüssels. In diesem Studienskript befassen wir uns darüber hinaus auch mit der geheimen Weitergabe von Informationen mit Hilfe der Steganografie, also dem Verbergen einer Nachricht durch deren Einbettung in eine andere Nachricht. Dadurch weiß niemand außer dem beabsichtigten Empfänger überhaupt von der Existenz der Nachricht – im Gegensatz zur Kryptografie, bei der die Nachricht unkenntlich gemacht wird.

Wir werden lernen, dass die Kryptografie Informationen schützt, indem sie Daten so mischt, dass nur mit Hilfe zusätzlicher geheimer Informationen, dem Schlüssel, die ursprünglichen Daten wiederhergestellt werden können. Wenn der zur Ver- und Entschlüsselung einer Nachricht verwendete Schlüssel derselbe ist, wird dies symmetrische oder Ein-Schlüssel-Kryptografie genannt. Indem wir die Rollen der Schlüssel vertauschen und den privaten Schlüssel zum Verschlüsseln und den öffentlichen Schlüssel zum Entschlüsseln verwenden, erhalten wir die Möglichkeit, eine Nachricht digital zu signieren. Bei der asymmetrischen Kryptografie liegt die Sicherheit ihrer Algorithmen für öffentliche Schlüssel in der sehr aufwendigen und ineffizienten Berechnung mathematischer Funktionen mit ganzen Zahlen begründet. Bei symmetrischen kryptografischen Algorithmen basiert die Sicherheit darauf, dass kleine Unterschiede bei der Eingabe und beim Schlüssel zu großen Unterschieden bei der Ausgabe führen.

Wir werden zwischen symmetrischer und asymmetrischer Kryptografie unterscheiden und deren größte Herausforderungen untersuchen. Eine Lösung bieten Public-Key-Infrastrukturen, bei denen private Schlüssel entweder von dritten, hierarchisch aufgebauten Behörden oder durch das Netz des Vertrauens (Web of Trust) zertifiziert werden, wobei das Vertrauen in einem Netz wiederum transitiv übertragen wird. Eine der bekanntesten Einsatzmöglichkeiten für Chiffrierungen sind Hashfunktionen. Eine Hashfunktion ist ein Algorithmus, der aus einer Eingabe mit variabler Größe eine Ausgabe mit fester Größe erzeugt. Die von einer kryptografischen Hashfunktion aus einer beliebig langen Zeichenkette erzeugte Ausgabekette mit fester Länge ist eine Form der unnachahmlichen Signatur.

Wir besprechen die Widerstandsfähigkeit bekannter Kryptografie-Algorithmen wie AES, DES, RSA und ECC gegen gängige Methoden der Kryptoanalyse wie Brute-Force-Angriffe und, im Falle von kryptographischen Hashes, gegen Brute-Force-Angriffe mit Rainbow Tables. Wir werden uns zudem die empfohlenen Schlüsselgrößen ansehen und den Aufwand berechnen, der erforderlich ist, um alle möglichen Schlüssel zu überprüfen.

Schließlich werden wir uns mit Netzwerkverbindungen wie VPN über den OSI-Stack und bekannten Netzwerkprotokollen wie TLS und seinem Vorgänger SSL zur Authentisierung, Geheimhaltung und Authentizität von über TCP gesendeten Daten befassen. Auch rechtliche Aspekte wie die Datenschutz-Grundverordnung und andere Rechtsgrundlagen, die sich auf die Verwendung von Verschlüsselung auswirken, werden zur Sprache kommen.

Als Anwendungsbeispiele für die Kryptografie in verschiedenen Bereichen werden wir das Online-Banking-Protokoll FinTS, die aktuellen Fortschritte bei der Blockchain als einem vertrauenswürdigem Dritten in Form einer Datenbank mit Einträgen und die zu berücksichtigenden Möglichkeiten der Datenverarbeitung mit einem Quantencomputer diskutieren. Die anonyme Datenübertragung im Internet durch das Onion-Routing im Tor-Netzwerk rundet unseren Praxisexkurs ab.


# Lektion 1

## Grundkonzepte der Kryptologie

Lernziele

Nach der Bearbeitung dieser Lektion werden Sie in der Lage sein, …

… Kryptologie, Kryptografie und Kryptoanalyse gegeneinander abzugrenzen.

… die Einsatzmöglichkeiten der Kryptologie hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu benennen.

… zu erläutern, welche kryptografischen Algorithmen es bisher gegeben hat und welche Bedeutung sie bis heute haben.

… das Kerckhoffs‘sche Prinzip wiederzugeben.

… zu beschreiben, wofür Hashfunktionen eingesetzt werden.

# 1. Grundkonzepte der Kryptologie

### Einführung

Kryptografie dient dem Schutz von Informationen durch Verschlüsselung, d. h. durch Umwandlung von verständlichen Daten in nicht mehr entzifferbare Daten, die nur durch eine zusätzliche geheime Information, den Schlüssel, wieder lesbar gemacht werden können (Entschlüsselung oder Dechiffrierung). Verschlüsselte (chiffrierte) Daten können nur durch Kenntnis des Schlüssels entschlüsselt (dechiffriert) werden. Da die ursprünglichen Daten grundsätzlich wiederhergestellt werden können, kann dieses Vorgehen als Verschleierung bezeichnet werden. Da historisch gesehen nur schriftliche Nachrichten verschlüsselt wurden, werden die Ausgangsdaten als Klartext und die verschlüsselten Daten als Geheimtext (Chiffretext) bezeichnet, auch wenn es sich tatsächlich um eine Folge von Einsen (1) und Nullen (0) (wie in der symmetrischen Kryptografie) oder um eine Zahl (wie in der asymmetrischen Kryptografie) handelt.

#### Verschlüsselung

Auch als Chiffrierung bezeichnet. Daten werden so verschlüsselt, dass sie nur durch zusätzliche geheime Informationen wieder lesbar gemacht werden können. Die Umkehrung dieses Vorgangs wird als Entschlüsselung oder Dechiffrierung bezeichnet.

### Single-Key- und Public-Key-Kryptografie

#### Schlüssel

Dies ist die zusätzliche geheime Information, die für die Entschlüsselung praktisch unerlässlich ist.

Historisch gesehen war der Schlüssel zur Umkehrung der Umwandlung von verständlichen Daten in nicht entzifferbare Daten sowohl zur Entschlüsselung als auch zur Verschlüsselung erforderlich. In früheren Zeiten war der Schlüssel zum Ver- und Entschlüsseln immer derselbe. Symmetrische Kryptografie wurde von den Ägyptern bereits 2000 Jahre v. Chr. verwendet und im Zweiten Weltkrieg bei der Enigma-Maschine eingesetzt. Heute findet er noch immer Anwendung bei der Verschlüsselung von drahtlosen Netzwerken (z. B. durch den AES-Algorithmus).

#### Symmetrische Kryptografie

Kryptografie ist symmetrisch, wenn derselbe Schlüssel zur Ver- und Entschlüsselung verwendet wird.

Die asymmetrische Kryptografie wurde dagegen erst in den 1970er Jahren erfunden. Hier unterscheiden sich der Schlüssel zum Verschlüsseln (der öffentliche Schlüssel) und der Schlüssel zum Entschlüsseln (der geheime oder private Schlüssel) voneinander. Tatsächlich ist nur der Schlüssel zum Entschlüsseln privat, während der Schlüssel zum Verschlüsseln öffentlich und damit allen bekannt ist. Die symmetrische Verschlüsselung vermeidet das Risiko der Offenlegung des Chiffrierschlüssels beim Austausch des Schlüssels mit dem Chiffrierer und beim Besitz des Chiffrierschlüssels (durch den Chiffrierer zusätzlich zum Dechiffrierer).

#### Asymmetrische Kryptografie

Kryptografie ist asymmetrisch, wenn zur Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden. Der Schlüssel für die Verschlüsselung ist öffentlich, und der für die Entschlüsselung ist privat.

Für eine digitale Signatur ist es sinnvoll, wenn die Schlüssel ihre Rollen vertauschen, d. h. der private Schlüssel verschlüsselt und der öffentliche Schlüssel entschlüsselt. Während die verschlüsselte Nachricht nicht mehr geheim ist, kann jeder Besitzer des öffentlichen Schlüssels überprüfen, ob der private Schlüssel die ursprüngliche Nachricht verschlüsselt hat.

Heute sind solche asymmetrischen Kryptografie-Algorithmen im Internet allgegenwärtig. Beispiele hierfür sind RSA, das auf der schwierigen Faktorisierung in Primzahlen beruht, oder ECC, das auf der Schwierigkeit beruht, Punkte in endlichen Kurven zu berechnen. Diese schützen (finanzielle) Transaktionen auf sicheren Websites (durch ein Vorhängeschloss in der Adressleiste des Browsers gekennzeichnet).

### Datenformat

Bis zum Digitalzeitalter konzentrierte sich die Kryptografie auf die Umwandlung von verständlichem Text in nicht entzifferbaren Text. Heutzutage befasst sich die Kryptografie schwerpunktmäßig mit der Umwandlung von verarbeitbaren (digitalen) Daten in nicht entzifferbare (digitale) Daten. Bei den Daten kann es sich z. B. um eine digitale Datei (Text, Bild, Ton, Video usw.) handeln. Dargestellt werden sie als Bitfolge (eine Folge aus 0 und 1) oder Bytefolge (eine Folge von hexadezimalen Paaren 00, 01, ..., FE, FF) oder als Zahl (wie gewohnt in ihrer dezimalen Ausprägung 0, 1, 2, 3 ...). Erinnern wir uns daran, dass jede Bitfolge 1011… eine Zahl n in Binärschreibweise n = 1 + 0 · 2 + 1 · 22 + 1 · 23 + ... ist (und umgekehrt).

In der symmetrischen Kryptografie, deren Algorithmen die Bits z. B. durch Permutation und Substitution umwandeln, wird die Betrachtungsweise als eine Bitfolge (genauer gesagt von hexadezimalen Ziffern, deren sechzehn Symbole 0-9 und A-F einer Gruppe von vier Bits entsprechen) bevorzugt. In der asymmetrischen Kryptografie hingegen wird die Betrachtungsweise als Zahl bevorzugt, die durch Algorithmen mit mathematischen Funktionen wie Potenzierung und Exponentiation bearbeitet wird. Der Schlüssel, die zusätzliche geheime Information, kann dabei verschiedene Formen annehmen. Zwar ist die gewählte Form in erster Linie eine Frage der Zweckmäßigkeit, doch die gängigsten Ausprägungen sind eine Zahl oder eine Buchstabenfolge, z. B. ein Passwort, oder ein geheimer Satz (mit Leerzeichen).

Beim antiken Skytale-Algorithmus, bei dem eine Pergamentrolle um einen Stab gewickelt wird, besteht der Schlüssel aus dem Umfang (in Buchstaben) des Stabes, also einer kleinen Zahl. Heutzutage sind PIN-Codes (Persönliche Identifikationsnummer) oder Passwörter im täglichen Leben allgegenwärtig. Um sich den Code besser einprägen zu können, sollten ganze Geheimsätze oder Passphrasen verwendet werden.

#### Asymmetrischer Schlüssel

-----BEGIN PGP PUBLIC KEY BLOCK -----

iQI2BCABCAAgFiEErZvSGgyHY7r19sbt31JsxV5IVU0FAl7aa3sCHQAACgkQ31Js xV5IVU0E7xAAiy24cTZz2OK+OwcoB2GxDjFC/qYV8sup3aFUqDRCpXRDRee18t+e

/N/pJUzY0CurgsNMl3bRDDMuZNPw/2/jaSYUrSpDsTHwqMI4sDAvqXOB1j6bMEUm S1/ME9EJ+LMdRhtpnmqfsHkptGfnMrrRfHAdzo43Fw5j/xmFx7eb9a8DdQMkBM9m zBtfoxB9d2/ZVqk0yoFwovuUnwVnEaOx0xLtdxdHlxRUWUF6nXJ278IHr6h4wolO JEBtZv9VN8f3rbmnaWDLEplfnOIVwAB2Becch7t1sBYbxy3rzvSU9cEHIpYgWuyQ wX2qy20+vfHEGMkwlv83l2ncacXRDeHXKAtigxhqirrAyUSThWxsAOGNJMmPq6RY aCg8IvgW09rvwU6CqZ2QuBjxXN8K0EtSH+RHH4FVTTP4wtbg3UsV/aXgNCWHF9EO V+bbhaig5bhC6lS/inosVg8ooOhW6+czl2in4G4mHSRrPZ8w74jfcxBm0ubbAdSy

DUrMcNGHJ8ITjGKp23WKYpcnss5vMFYGKBa2eKlOmemPTzb3SHxlzAaHC6nef+GQ

W/wHgP5KgtVG4Y+HXtu+0tJhRCqlOPGzxVaBX0b61CYzN5jurAhZi2CCZ1E+xte+

7wEZ7j7zawT0Ev9oZpT56m00OTUcjfRPDy9tQlehuNLI6XXXLLW0F+M=

=+tEF

-----END PGP PUBLIC KEY BLOCK-----

Dieser asymmetrische Schlüssel wird aufgrund seiner Länge in einer Datei von mehreren Kilobyte Größe gespeichert, die als ASCII Armor bezeichnet wird.

## 1.1 Begriffe

Das Präfix Krypto- stammt vom griechischen *kryptós*: „versteckt, verborgen, geheim“. Dementsprechend ist Kryptografie (vom griechischen *gráphein*: „schreiben“) die Kunst des verborgenen oder geheimen Schreibens, d. h. Informationen werden so verändert, dass sie für alle anderen als den vorgesehenen Empfänger nicht mehr entzifferbar sind. Kryptoanalyse (vom griechischen *analýein*: „Auflösung“) ist die Kunst, die verborgene Schrift ohne den zugehörigen Schlüssel zu entschlüsseln. Zum Entziffern (Brechen) von Chiffrierungen wird die verschlüsselte Information ohne Kenntnis des Schlüssels wiederhergestellt oder gefälscht.

Kryptologie (von griechisch *lógos*: „Wort“, „Vernunft“ , „Lehre“ oder „Bedeutung“) ist die Wissenschaft von der verborgenen, vertrauenswürdigen Nachrichtenübermittlung, die Kryptografie und Kryptoanalyse umfasst. Der allgemeine Begriff ist Kryptologie und wird oft als Synonym für Kryptografie und auch Kryptoanalyse verwendet. Häufig synonym verwendete Adjektive sind in diesem Zusammenhang geheim, privat und vertraulich. Sie alle beschreiben Informationen, die anderen Personen nicht bekannt sind oder die ihnen nicht bekannt sein sollen. Etwas ist

* *geheim*, wenn es nur einer bestimmten Person oder Gruppe bekannt ist,
* *vertraulich*, wenn es geheim gehalten werden, d. h. nicht an andere Personen weitergegeben werden soll,
* *privat*, wenn es geheim bleiben soll, insbesondere wenn es um eine Einzelperson gegenüber dem Staat geht.

Geheimhaltung ist zwar auch heute noch wichtig, aber seit dem Aufkommen der Kryptografie mit öffentlichen Schlüsseln in den 1980er Jahren ist sie nicht mehr der einzige Zweck der Kryptologie. Damit elektronische Geräte das ersetzen können, was früher von Hand gemacht wurde, wurden digitale Signaturen und Authentifizierung eingeführt.

Steganografie (von griechisch *steganos*: „verborgen“) ist die Kunst, eine Nachricht zu verbergen, indem sie in eine andere Nachricht (ein Bild, eine Audio-Datei oder ein binäres Datenformat) eingebettet wird, so dass niemand außer dem vorgesehenen Empfänger überhaupt von der Existenz der Nachricht weiß. Im Gegensatz dazu wird bei der Kryptografie nicht die Existenz der Nachricht selbst verschleiert, sondern nur ihr Inhalt. Allerdings deutet eine Verschlüsselung darauf hin, dass bestimmte – vermutlich wichtige – Informationen absichtlich verborgen werden. Da eine typische Bild- oder Tondatei Hunderte von Kilobyte groß ist, können einige wenige Bytes verändert werden, um eine geheime Botschaft zu übermitteln, ohne dass dies für das unbedarfte Auge oder Ohr erkennbar wäre. (OPTED, o. J.)

#### Kryptografie

Kryptografie wird bereits seit langer Zeit eingesetzt, um beispielsweise militärische Nachrichten vor dem Feind zu verbergen. Inzwischen haben (elektronische binäre) Daten schriftliche Texte ersetzt, und was früher von Boten ausgetauschte oder geheim gehaltene geschriebene Nachrichten waren, sind heute gesicherte Daten, die zwischen Computern übertragen oder auf einem Computer gespeichert werden. Asymmetrische Kryptografie ermöglicht durch digitale Signaturen, dass alle Kommunikationsteilnehmer zweifelsfrei veriﬁziert werden können, was als Non-Repudiation (Nichtabstreitbarkeit, Nachweisbarkeit) bekannt ist. Dies eröffnet zahlreiche Möglichkeiten, insbesondere für den elektronischen Handel.

Alle kryptografischen Verfahren, die wiederum als Kryptosysteme bezeichnet werden, werden in symmetrische und asymmetrische Kryptosysteme eingeteilt. Symmetrische Kryptosysteme werden danach eingeteilt, ob sie mit Bitblöcken von fester Länge, z. B. 128 Bit, (Blockchiffre wie AES oder RSA) oder mit einzelnen Bits (Stromchiffre wie RC4) arbeiten. Stromchiffren sind zwar in der Regel einfacher, schneller und für Echtzeitübertragungen hervorragend geeignet, aber sie sind im Allgemeinen weniger sicher und werden daher seltener verwendet (ein WLAN-Netzwerk wird z. B. üblicherweise durch eine Blockchiffre wie AES gesichert).

#### Code

Eine Kodierung ist eine Regel zum Ersetzen einer Information, z. B. eines Buchstabens, durch eine andere, in der Regel, um sie für die Verarbeitung durch einen Computer vorzubereiten. Beispiele:

* Morsecode
* American Standard Code for Information Interchange (ASCII-Code) aus dem Jahr 1963, der auf Computern 128 Zeichen (und Operationen wie Rücktaste und Zeilenvorschub) durch 7-Bit-Zahlen darstellt. In ASCII entspricht ein kleines a der Bitfolge 1100001, ein kleines b der Bitfolge 1100010 usw., ein großes A entspricht der Bitfolge 1000001 und ein großes B wiederum der Bitfolge 1000010.
* UTF-8 (8-bit Unicode Transformation Format). Hierbei handelt es sich um eine von Ken Thompson und Rob Pike entwickelte Zeichenkodierung mit variabler Länge, die jedes universelle Zeichen des Unicode-Standards durch eine Folge von ein bis vier Bytes darstellt und zudem mit ASCII rückwärtskompatibel ist. Dieser Standard bietet die Möglichkeit, bis zu 232 ≈ 4 Milliarden Zeichen abzubilden und enthält u. a. die Alphabete zahlreicher Sprachen, wie Deutsch und Chinesisch, sowie Symbole wie Emoticons.

#### Chiffren

Eine Chiffre ersetzt genau wie eine Kodierung eine Information (die von einem einzelnen Bit bis zu einer ganzen Zeichenfolge reichen kann) durch eine andere, wobei die Ersetzung jedoch nach einer durch einen Schlüssel festgelegten Regel erfolgt, so dass niemand ohne dessen Wissen die Ersetzung umkehren kann.

#### Chiffre

Diese Regel wird verwendet, um Informationen so zu ersetzen, dass deren Umkehrung nur mit Kenntnis des Schlüssels möglich ist.

Heute werden Informationen für die Verarbeitung durch einen Computer kodiert und für einen sinnvollen Grad an Informationssicherheit chiffriert. Informationen, die im Internet zu finden sind, werden zunächst in das ASCII-Format umgewandelt (kodiert), dann in Chiffren verschlüsselt, z. B. mit dem AES-Algorithmus (Advanced Encryption Standard), und schließlich für die Übertragung mit Fehlerkorrekturcodes erneut kodiert. Nach der Übertragung muss der Empfänger dasselbe in umgekehrter Reihenfolge tun (Bellare & Rogaway, 2000).

## 1.2 IT-Sicherheit: Bedrohungen und verbreitete Angriffsmethoden

Ein prägnantes Akronym, das die grundlegenden Ziele der Informationssicherheit zusammenfasst, lautet CIA. Noch umfassender sind die „Fünf Säulen der Informationssicherheit“, zu denen auch die Authentifizierung und die Nichtabstreitbarkeit (Non-Repudiation) gehören (Chen et al., 2019).

#### CIA

In der Informationssicherheit steht CIA für die Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity, Availability) von Informationen.

Mit Hilfe der Kryptografie können wir alle diese Ziele hervorragend realisieren. Eine gute Verschlüsselung, wie sie durch gründlich getestete Standardalgorithmen wie AES oder RSA erreicht wird, ist computertechnisch praktisch nicht zu brechen (entziffern). Stattdessen werden die Schlüssel oder der Klartext in vielen Fällen vor der Verschlüsselung oder nach der Entschlüsselung gestohlen. Zwar bietet die Kryptografie ein hohes Maß an technischer Sicherheit, jedoch ist der größte Schwachpunkt für die Informationssicherheit am Ende menschliches Versagen, z. B. aus Bequemlichkeit oder unangebrachtem Vertrauen.

### Vertraulichkeit

Vertrauliche Informationen sollen geheim gehalten und nicht an andere Personen weitergegeben werden. Dies können beispielsweise Informationen sein, die nur Ihrem Arzt oder Ihrer Bank bekannt sind. In der Rechtswissenschaft bezeichnet der Begriff Vertraulichkeit die Beziehung zwischen einem Mandanten und seinem Anwalt oder Bevollmächtigten und bezieht sich auf das Vertrauen, das der eine dem anderen entgegenbringt. Die Internationale Organisation für Normung (ISO) definiert Vertraulichkeit als die Sicherstellung, dass Informationen nur denjenigen zugänglich sind, die zum Zugriff berechtigt sind (2005). In der IT bedeutet dies, dass die auf Computern gespeicherten sensiblen Informationen nicht an unbefugte Personen, Programme oder Geräte weitergegeben werden. So muss beispielsweise verhindert werden, dass eine beliebige Person mit Zugang zu einem Netzwerk gängige Tools verwendet, um den Datenverkehr abzuhören und wertvolle private Informationen abzufangen.

### Integrität

Bei der (Daten-)Integrität geht es um die zuverlässige, vollständige und fehlerfreie Übertragung und den Empfang oder die Speicherung von Daten. Dies bedeutet, dass die ursprünglichen Daten nicht verändert oder verfälscht wurden; insbesondere entsprechen die Daten den Erwartungen.

Wenn die Daten durch elektronische Beschädigung mittels Software oder durch physische Beschädigung des Datenträgers verändert wurden, werden sie unlesbar. Wenn wir eine Datei herunterladen, überprüfen wir ihre Integrität, indem wir ihren Hash berechnen und ihn mit dem veröffentlichten Hash vergleichen. Ohne diese Prüfung könnte jemand zum Beispiel einen Trojaner in ein Installationsprogramm für Microsoft Windows einschleusen.

### Verfügbarkeit

Auch wenn es nichts mit Kryptologie zu tun hat, geht es bei der Informationssicherheit um die Verfügbarkeit von Informationen gegenüber Bedrohungen wie Angriffen (z. B. DoS (Denial of Service), Störfällen (z. B. Stromausfällen) oder Naturkatastrophen (z. B. Erdbeben). Um dies zu erreichen, ist es am besten, einen Sicherheitsspielraum zu haben und Redundanz einzuplanen, insbesondere die folgenden:

* Parallel redundante Failover-Hardware, wie z. B. einen Server oder ein Netzwerk. Dieses System ist ständig in Betrieb, so dass bei einer festgestellten Störung des Primärsystems die Verarbeitung automatisch umgeschaltet werden kann.
* Verhinderung des Eindringens in das System, indem die Netzverkehrsmuster auf Anomalien überwacht und der Netzverkehr ggf. gesperrt wird.

### Authentifizierung

Das Wort authentisch kommt aus dem Griechischen *authentikós* und bedeutet „echt oder unverfälscht“. Authentifizierung ist also der Nachweis von etwas (oder jemandem) als „authentisch“. So könnte es darum gehen, die Identität einer Person oder die Herkunft eines Objekts zu bestätigen. In der IT bedeutet Authentifizierung insbesondere:

* „Nachweis der Identität eines Benutzers oder seiner Berechtigung, auf ein Objekt zuzugreifen“ d. h. einen Computer davon zu überzeugen, dass eine Person diejenige ist, die sie nach der Identifizierung vorgibt zu sein.
* „Nachweis, dass eine Nachricht nicht verändert oder verfälscht wurde“ (IBM, o. J.).

Eine Person weist ihre Identität durch Belege nach (Authentisierung). Es gibt verschiedene Möglichkeiten, diese Belege zu erbringen bzw. abzufragen, insbesondere auf Computern. Die gängigsten Methoden sind PIN (Persönliche Identifikationsnummer bzw. englisch: *Personal Identification Number*) und Passwörter, aber auch Chipkarten oder biometrische Identifizierungsverfahren wie Fingerabdrücke oder Iris-Scans können diese Aufgabe übernehmen.

Ein häufiges Szenario ist der Man-in-the-Middle-Angriff (MITM), bei dem der Angreifer die Identität des anderen Kommunikationsteilnehmers annimmt. Zur Lösung dieses Problems werden Zertiﬁkate, also digitale Signaturen durch Dritte, eingesetzt. Dies kann entweder, wie beim Web of Trust in OpenPGP, durch Signaturen zwischen Personen, die untereinander bekannt sind, oder, wie auf sicheren Seiten in einem Webbrowser, durch eine Signatur einer vorbehaltlos vertrauenswürdigen, zentralen Zertifizierungsstelle realisiert werden.

### Nichtabstreitbarkeit (Non-Repudiation)

Repudiation ist ein juristischer Begriff für die Leugnung einer rechtlichen Bindung (z. B. einer Vereinbarung oder Verpflichtung). Eine Repudiation liegt vor bei einer Person, die a) sich weigert, eine rechtliche Verpflichtung zu akzeptieren oder mit ihr in Verbindung gebracht zu werden, b) sich weigert, die Gültigkeit der rechtlichen Verpflichtung anzuerkennen (z. B. ihre Unterschrift), und c) sich weigert, die rechtliche Verpflichtung zu erfüllen.

Die Non-Repudiation (Nichtabstreitbarkeit) stellt sicher, dass ein Vertrag später von keiner der Parteien bestritten werden kann und dass die Identität des mutmaßlichen Absenders oder Empfängers einer bestimmten Nachricht feststeht. In der Informatik bedeutet dies, dass die Authentifizierung im Nachhinein nicht mehr widerlegt werden kann. Dies wird durch eine digitale Signatur erreicht. So beweist z. B. ein elektronischer Beleg, dass ein bestimmter Nutzer eine Nachricht, z. B. eine Anweisung zum Kauf eines Artikels in einer Online-Auktion, gesendet hat. Wenn in der E-Mail steht, dass Person A sie geschickt hat, kann Person A dies später nicht abstreiten. In der heutigen globalisierten Wirtschaft, in der persönliche Vereinbarungen von Angesicht zu Angesicht oft nicht mehr möglich sind, ist die Nichtabstreitbarkeit für einen sicheren Geschäftsverkehr unerlässlich.

## 1.3 Historischer Überblick

Die Geschichte der Kryptografie reicht mindestens 4000 Jahre zurück. Wir unterscheiden drei Perioden (Davies, 1997):

1. Bis zum zwanzigsten Jahrhundert waren die Methoden klassisch, im Wesentlichen Stift und Papier.
2. Zu Beginn des zwanzigsten Jahrhunderts wurden sie durch effizientere und ausgefeiltere Methoden auf komplexen elektromechanischen Maschinen ersetzt. Dabei handelte es sich hauptsächlich um Rotor-Chiffriermaschinen für die polyalphabetische Substitution, wie z. B. die Enigma, die von den Achsenmächten während des Zweiten Weltkriegs eingesetzt wurde.
3. Seit dem frühen zwanzigsten Jahrhundert hat die Digitalisierung, also die Ablösung analoger Geräte durch digitale Computer, immer komplexere Methoden möglich gemacht. Die meistgetesteten Algorithmen sind DES (bzw. seine dreifache Iteration 3DES) und sein Nachfolger AES für die symmetrische Kryptografie sowie RSA und sein Nachfolger ECC für die asymmetrische Kryptografie.

### Klassische Kryptografie

Von der Antike bis zum Ersten Weltkrieg wurde Kryptografie von Hand ausgeführt und war daher in ihrer Komplexität und Länge auf höchstens ein paar Seiten beschränkt. Obwohl die Grundlagen der Kryptoanalyse bereits damals bekannt waren, wurden sie wegen der fehlenden Automatisierung in der Kryptografie praktisch nicht angewandt. Daher war die Kryptoanalyse bei einer ausreichenden Menge an Geheimtext und entsprechendem Aufwand praktisch immer erfolgreich. Die Araber waren die Ersten, die sich der Kryptoanalyse bedienten. Sie verwendeten sowohl Substitutions- als auch Transpositions-Chiffren und kannten sowohl die Häufigkeitsverteilung der Buchstaben als auch den wahrscheinlichen Klartext bei der Kryptoanalyse.

#### Skytale

Eine Skytale (aus dem Griechischen für „Stock“ oder „Stab“) besteht aus einem mit Pergamentband umwickelten Stab, auf dem eine geheime Botschaft geschrieben steht. Das Pergamentband wird auf den Stab gewickelt und beschrieben. Die Geheimschrift ist nur lesbar, wenn das Pergament um einen Stab mit demselben Durchmesser gewickelt wird. Es handelt sich um eine Transpositions-Chiffre: Sie vermischt (transponiert) die Buchstaben des Klartextes (OPTED, o. J.).

#### Caesar-Chiffre

Die Caesar-Chiffre ist eine der einfachsten und bekanntesten Verschlüsselungen, benannt nach Julius Caesar, der sie zur Nachrichtenübermittlung mit seinen Generälen verwendete. Bei dieser Substitutions-Chiffre wird jeder Buchstabe des Klartextes durch einen festen anderen Buchstaben ersetzt. Jeder Buchstabe des Klartextes wird um die gleiche Anzahl von Positionen im Alphabet verschoben, d. h. jeder Buchstabe des Klartextes wird durch einen Buchstaben ersetzt, der eine bestimmte Anzahl von Positionen weiter hinten im Alphabet steht (Bauer, 2000).

#### Bacon-Chiffre

Francis Bacons Chiffre aus dem Jahr 1605 ist eine Anordnung der Buchstaben a und b in Fünfergruppen (von denen es 25 = 32 gibt), die wiederum jeweils einen Buchstaben des englischen Alphabets darstellen (26). Heute würden wir dies als Code bezeichnen, aber damals illustrierte dies den bedeutenden Grundsatz, dass nur zwei verschiedene Zeichen ausreichen, um eine Information zu übermitteln (Tudhope, 1993).

#### Alberti-Scheibe

Im Jahr 1470 beschrieb Leon Battista Alberti die erste Chiffrierscheibe, welche die Buchstaben des Alphabets zyklisch verschiebt. Er empfahl, die Verschiebung nach jeweils drei oder vier Wörtern zu ändern und so eine polyalphabetische Chiffre zu konzipieren, bei der die gleichen Buchstaben durch andere ersetzt werden. Mehr als vier Jahrhunderte später setzte die US-Armee im Ersten Weltkrieg das gleiche Gerät ein (de Leeuw & Bergstra, 2007).

#### ADFGVX-Chiffre

Die berühmteste Chiffre des Ersten Weltkriegs war die deutsche Fraktionierungschiffre ADFGVX, die am 5. März 1918, also gegen Ende des Ersten Weltkriegs, eingeführt wurde. Fritz Nebel, ein Nachrichtenoffizier des Heeres, entwickelte die vermeintlich unknackbare ADFGVX-Chiffre für den Einsatz durch mobile militärische Einheiten. Sie ersetzte die 26 Buchstaben und 10 Ziffern durch eine 6 x 6-Matrix mit Paaren aus den Buchstaben A, D, F, G, V und X. Der resultierende Text wurde dann in Form eines Rechtecks geschrieben, und die Spalten wurden in der durch den Schlüssel angegebenen Reihenfolge gelesen (Dooley, 2013, Kapitel 5).

### Elektromechanische Kryptografie mit Rotor-Chiffriermaschinen

Die ersten Erfolge bei der Mechanisierung der Kryptografie stellten sich kurz nach dem Ersten Weltkrieg ein. Nachdem sich Telegrafie und Radio in den 1920er Jahren durchgesetzt hatten, entstand ein Bedarf an Kryptografie, und die Entwicklung von Rotor-Chiffriermaschinen nahm an Fahrt auf. Dieser Automatisierungsschritt ermöglichte schnellere Abläufe mit höherer Komplexität und geringeren Fehlerquoten als bei der manuellen Verschlüsselung (Dooley, 2013, Kapitel 5).

Bei der Enigma-Maschine sind die Rotoren übereinander angeordnet. Die Drehung eines Rotors bewirkt, dass sich der nächste um 1/26 einer vollen Umdrehung dreht. Während des Betriebs gibt es einen elektrischen Pfad durch alle Rotoren. Durch Schließen des Tastenkontakts des Klartextbuchstabens auf einer schreibmaschinenähnlichen Tastatur wird ein Strom an einen der Kontakte des Startrotors abgegeben. Der Strom fließt dann durch die Kabel der gestapelten Rotoren (abhängig von der Drehlage) und endet an einer Anzeige, wo er die Lampe des Geheimtextbuchstabens zum Leuchten bringt.

### Digitale Kryptografie

Die weitere Entwicklung der Verschlüsselungsmaschinen führte zu noch schnelleren Rotor-Chiffriermaschinen mit elektronischer Ersetzung ihrer Rotoren, aber das Konzept blieb dasselbe: verschobene monoalphabetische Substitutionen führten zu einer polyalphabetischen Substitution. Mit dem Aufkommen des Digitalcomputers in den 1980er Jahren änderte sich an der Entwicklung nichts mehr. Allerdings sind solche buchstabenweisen Substitutionen immer noch „linear über die Buchstaben“, so dass der aus einem Klartext gewonnene Geheimtext verrät, wie alle Buchstaben eines Klartextes von (höchstens) gleicher Länge entschlüsselt werden können. Eine buchstabenweise Substitution hat also eine geringe Verteilung (Diffusion) zur Folge und bewirkt kaum Veränderungen. Eine optimale Diffusion ist immer dann erreicht, wenn die Änderung eines einzigen Buchstabens des Klartextes die Änderung der Hälfte der Buchstaben des Geheimtextes bewirkt. Wenn der Angreifer Zugang zu den Geheimtexten vieler Klartexte hat, die er möglicherweise selbst ausgewählt hat, kann er den Schlüssel aus den Geheimtexten von zwei Klartexten ermitteln, die sich in einer einzigen Position unterscheiden.

#### DES

Der Computer ermöglichte demgegenüber eine wesentlich bessere Diffusion. Computer ermöglichten zudem die Kombination von Substitutionen (z. B. Caesar-Chiffre) mit Transpositionen (z. B. Skytale), wodurch eine wesentlich bessere Streuung erreicht wurde. Dies führte 1976 zur Entwicklung einer der am häufigsten verwendeten Verschlüsselungen der Geschichte, dem Data Encryption Standard oder DES (Davies, 1997).

#### AES

Im Januar 1997 kündigte das US National Institute of Standards and Technology (NIST) einen öffentlichen Wettbewerb für einen Nachfolger des veralteten DES an, den Advanced Encryption Standard (AES). Im Oktober 2000 wurde Rijndael, das von Joan Daemen und Vincent Rijmen entwickelt wurde, ausgewählt und damit zum AES (NIST, 2000).

Da es aufgrund der verbesserten Rechenleistung möglich war, den feststehenden 56-Bit-DES-Schlüssel durch eine vollständige Schlüsselsuche zu finden, verlangten die NIST-Spezifikationen für den AES eine höhere Schlüssellänge, sofern dies erforderlich werden sollte. Rijndael erwies sich als immun gegen die ausgeklügeltsten bekannten Angriffe, wie z. B. differentielle Kryptoanalyse. Außerdem hatte es ein elegantes und einfaches Design, war so klein, dass es auf Chipkarten implementiert werden konnte (mit weniger als 10.000 Byte Code) und war gleichzeitig ausreichend flexibel für höhere Schlüssellängen (Daemen & Rijmen, 1999; 2002).

#### Public-Key-Kryptografie

Seit den 1980er Jahren hat das Aufkommen der Public-Key-Kryptografie im Informationszeitalter digitale Signaturen und Authentifizierungen ermöglicht und damit Möglichkeiten geschaffen, durch elektronische Informationen das zu ersetzen, was früher durch physische Dokumente erreicht wurde. Difﬁe und Hellman (1976) waren die Ersten, die öffentlich eine asymmetrische Verschlüsselung vorschlugen. Konzeptionell beruht sie auf einer Falltürfunktion (genauer gesagt, der modularen Exponentiation oder diskreten Exponentialfunktion). Diese invertierbare Funktion ist leicht zu berechnen, doch ihre Umkehrung ist kaum zu berechnen, wenn keine zusätzlichen Informationen vorliegen: der geheime Schlüssel (Difﬁe & Hellman, 1976).

Zum Verschlüsseln wird die Funktion angewendet. Zum Entschlüsseln wird die Umkehrung mit dem geheimen Schlüssel verwendet. Im Konzept von Difﬁe und Hellman (1976) zum Beispiel ist diese Funktion die Exponentialfunktion, allerdings in einem anderen Definitionsbereich als dem der reellen Zahlen, den wir gewohnt sind. Tatsächlich haben die beiden Begründer nur ein Verfahren zum Austausch eines geheimen Schlüssels über einen unsicheren Kanal geschaffen. Im kryptografischen RSA-Algorithmus (Rivest et al., 1978) und im Elgamal-Algorithmus (Elgamal, 1985) wurde dieses Konzept erstmals verwendet. Diese Algorithmen ermöglichten nicht nur die Chiffrierung mit einem öffentlichen Schlüssel, wodurch das Problem der geheimen Kommunikation gelöst wurde, sondern machten auch digitale Signaturen mit dem privaten Schlüssel zur Chiffrierung möglich, was wohl den kommerziellen Durchbruch einleitete. Diese Algorithmen haben immer noch Bestand, aber andere, wie ECC, gelten heute als effizienter und ebenso sicher.

## 1.4 Sicherheitskriterien

#### Kerckhoffs‘ Prinzip

Der Geheimtext muss auch dann sicher sein, wenn mit Ausnahme des Schlüssels alles über ihn allgemein bekannt ist.

Das Kerckhoffs‘sche Prinzip postuliert die Unabhängigkeit der Sicherheit eines Kryptoalgorithmus von dessen Geheimhaltung. Die Kenntnis des Schlüssels gefährdet eine einzelne Verschlüsselung, während die Kenntnis des Algorithmus alle jemals durchgeführten Verschlüsselungen gefährdet. Ein öffentlich bekannter Algorithmus garantiert, dass die Schwierigkeit der Entschlüsselung nur von der Kenntnis des Schlüssels, nicht aber vom Algorithmus abhängt. Je häufiger er verwendet wird, desto wahrscheinlicher wird es, dass der Algorithmus irgendwann bekannt wird. Damit der Algorithmus brauchbar ist, muss er also sicher sein, auch wenn er öffentlich bekannt ist.

### Shannons Kriterien

#### Ideale Diffusion

Das Shannonsche Ideal besagt, dass sich die Hälfte der Bits im Geheimtext ändert, wenn sich ein Bit im Klartext oder Schlüssel ändert.

Shannons Prinzipien der Konfusion und der Diffusion geben Kriterien für eine nicht ableitbare Beziehung zwischen dem Geheimtext und dem Schlüssel in Bezug auf den Klartext vor. Während die Ausgabe der Chiffrierung, der Geheimtext, deterministisch von der Eingabe, dem Klartext, und dem Schlüssel abhängt, zielt der Algorithmus darauf ab, diese Beziehung zu verschleiern, um sie so kompliziert, verflochten und verworren wie möglich zu machen. Jeder Buchstabe der Ausgabe (Geheimtext) hängt von jedem Buchstaben der Eingabe (Klartext) und des Schlüssels ab.

Shannon (1949) formulierte es so: „Der Feind kennt das System“, was heute als Shannons Maxime bekannt ist. Das Gegenbeispiel wäre, sich auf einen potenziell schwachen, aber unbekannten Algorithmus zu verlassen: „Sicherheit durch Dunkelheit“. Es gibt zahlreiche historische Beweise für die Vergeblichkeit eines solchen Vorhabens (z. B. die ADFGVX-Chiffre).

#### Hashfunktion

Ein Algorithmus, der aus einer Eingabe mit variabler Größe eine Ausgabe mit fester Größe erzeugt, wird als Hashfunktion bezeichnet.

## 1.5 Hashfunktionen

Eine Hashfunktion (Streuwertfunktion) ist ein Algorithmus, der aus einer Eingabe variabler Größe (z. B. einer Textdatei, einer Bilddatei oder einem komprimierten Archiv) eine Ausgabe fester (Byte-)Größe, in der Regel 16 bis 64 Byte, erzeugt. Aus einer Eingabe variabler Größe berechnet eine Hashfunktion eine Ausgabe fester Größe, die als Hashwert oder, je nach Verwendung, auch als (Nachrichten-)Digest, digitaler Fingerabdruck oder Prüfsumme bezeichnet wird. Der md5-Hash (Größe von 16 Bytes) des Wortes „Schlüssel“ lautet beispielsweise 0f511d362346c2f658bb594d5b04224e in hexadezimaler Kodierung.

#### Prüfsummenfunktion

Ein Algorithmus, der schnell und ohne Kollisionen aus einer Eingabe mit variabler Größe eine Ausgabe mit fester Größe erzeugt, wird als Prüfsummenfunktion bezeichnet.

#### Prüfsumme

Eine (einfache) Hashfunktion oder Prüfsummenfunktion sollte die folgenden Merkmale erfüllen:

* schnelle Berechnung eines Hashwertes für beliebige Daten und
* geringe Wahrscheinlichkeit, dass zwei (nur leicht) unterschiedliche Nachrichten denselben Hashwert ergeben.

Eine Hashfunktion sollte sich daher wie eine Zufallsfunktion verhalten, gleichzeitig aber deterministisch und schnell zu berechnen sein.

So wäre zum Beispiel die simpelste Prüfsumme die Summe der Bits in der Eingabe, die auf die feste Ausgabegröße abgeschnitten wird. Hierbei handelt es sich fast um eine Hashfunktion: sie ist schnell und es ist in der Tat unwahrscheinlich, dass zwei verschiedene Nachrichten denselben Hashwert ergeben. Allerdings können leicht zwei fast identische Nachrichten mit dem gleichen Hashwert gefunden werden. Winzige Änderungen könnten so unentdeckt bleiben.

#### Kryptografische Hashfunktion

Die Ausgabezeichenkette mit fester Länge, die eine kryptografische Hashfunktion aus einer Zeichenkette beliebiger Länge (z. B. einer wichtigen Nachricht) erzeugt, ist also eine Art unnachahmlicher Signatur. Eine Person, die den Hashwert kennt, kann die ursprüngliche Nachricht nicht daraus ableiten; nur die Person, die die ursprüngliche Nachricht kennt, kann nachweisen, dass der „Hashwert“ aus dieser Nachricht erzeugt wurde. Heer (2008) beschreibt es so: „Eine Hashfunktion ist schwach kollisionsresistent, wenn das Auffinden eines Urbildes rechnerisch nicht praktikabel ist“, d. h. aus einer gegebenen Ausgabe eine (noch unbekannte) entsprechende Eingabe zu finden. Starke Kollisionsresistenz beschreibt somit eine Hashfunktion, für die „das Auffinden einer Kollision rechnerisch nicht praktikabel ist“ (Heer, 2008), d. h. zwei Eingaben mit der gleichen Ausgabe zu finden. Andernfalls könnte ein Angreifer eine autorisierte Nachricht durch eine unautorisierte ersetzen.

### Anwendungsfälle

Hashfunktionen werden für die Abfrage von Datenbankeinträgen, zur Fehlererkennung und -korrektur (z. B. für Datenintegritätsprüfungen) und in der Kryptografie zur Identifizierung von Daten bei Verschleierung ihres Inhalts für Datenauthentizitätsprüfungen und Authentifizierung (z. B. zum Speichern von Passwörtern, digitalen Signaturen) verwendet.

In der Praxis sind die meisten Hashfunktionen, selbst bei Prüfsummen, kryptografisch. Sie sind zwar langsamer, aber auf den meisten Geräten immer noch schnell genug. Manchmal – z. B. bei der Speicherung von Passwörtern – sind sie absichtlich langsam, damit die Passwörter nicht durch eine erschöpfende Suche unter den wahrscheinlichen Kandidaten anhand ihrer Hashwerte schnell gefunden werden können. Die am häufigsten eingesetzte kryptografische Hashfunktion war MD5, üblicherweise mit einer Ausgabelänge von 128 Bit, erfunden von Ron Rivest vom Massachusetts Institute of Technology im Jahr 1991.

#### SHA

Die Secure Hash Algorithms (SHA) sind kryptografische Hashfunktionen, die von der National Security Agency (NSA) und dem NIST bereitgestellt werden. SHA-1 ist der Nachfolger von MD5 mit einer Hashgröße von 160 Bit. MD5 war eine frühere, weit verbreitete Hashfunktion, die immer mehr Sicherheitsmängeln zum Opfer fiel (sie wurde aber nicht geknackt, d. h. es ist kein rechnerisch praktikabler Weg bekannt, eine Eingabe aus einer bestimmten Hashfunktion zu erzeugen). SHA-1 wurde im Digital Signature Algorithm (DSA) verwendet, wie er im Digital Signature Standard (DSS) der Internet Engineering Task Force vorgeschrieben ist.

Zwischenzeitlich gab es die drei SHA-Algorithmen SHA-1, SHA-2 und SHA-3 (veröffentlicht 2015) mit zunehmender Sicherheit, welche die Unzulänglichkeiten der jeweiligen Vorgänger abschwächten. „SHA-2“ erlaubt Hashes mit unterschiedlichen Bitgrößen. Die Bitanzahl wird an das Präﬁx „SHA“ angehängt, z. B. „SHA-224“, „SHA-256“, „SHA-384“ und „SHA-512“.

Zusammenfassung

Mit Hilfe der Kryptografie werden Informationen geschützt, indem Daten so gemischt werden, dass nur über zusätzliche geheime Informationen, den Schlüssel, die ursprünglichen Daten wiederhergestellt werden können. Bis Ende der 1970er Jahre war die symmetrische oder Ein-Schlüssel-Kryptografie üblich. Danach folgte die asymmetrische Kryptografie.

Die Sicherheit asymmetrischer kryptografischer Algorithmen, auch Public-Key-Algorithmen genannt, beruht auf der ineffizienten Berechnung mathematischer Funktionen mit ganzen Zahlen. Die Sicherheit symmetrischer kryptografischer Algorithmen basiert darauf, dass kleine Unterschiede in der Eingabe und im Schlüssel zu großen Unterschieden in der Ausgabe führen. Eine gute Verschlüsselung, wie sie durch Standardalgorithmen wie AES oder RSA erreicht wird, ist computertechnisch praktisch nicht zu brechen.

Eine Hashfunktion ist ein Algorithmus, der aus einer Eingabe mit variabler Größe eine Ausgabe mit fester Größe erzeugt. Wir unterscheiden zwischen kryptografischen Hashfunktionen (oder Einweg-Hashfunktionen) und Prüfsummen-Hashfunktionen (oder nicht-kryptografischen Hashfunktionen). Für kryptografische Hashfunktionen haben wir zudem die schwache und die starke Kollisionsresistenz definiert, die davon abhängen, ob es praktisch unmöglich ist, eine unbekannte Nachricht aus einem bestimmten Hashwert zurückzugewinnen und ob es praktisch unmöglich ist, zwei Nachrichten mit demselben Hashwert zu finden.