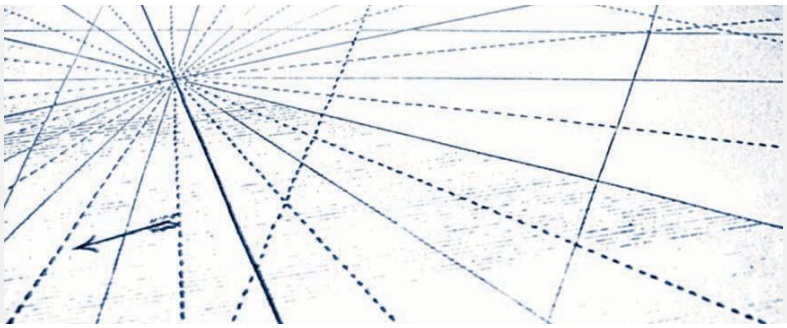
STUDIENSKRIPT

Kryptologie

DLMCSEAITSC02

iubh INTERNATIONALE HOCHSCHULE

Übergeordnete 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 hinausgehend auch mit der geheimen Weitergabe von Informationen mit Hilfe der Steganografie, also dem Verbergen einer Nachricht durch deren Einbettung in eine andere Nachricht, so dass niemand außer dem beabsichtigten Empfänger überhaupt von der Existenz der Nachricht weiß, im Gegensatz zur Kryptografie, bei der die Nachricht unkenntlich gemacht wird.

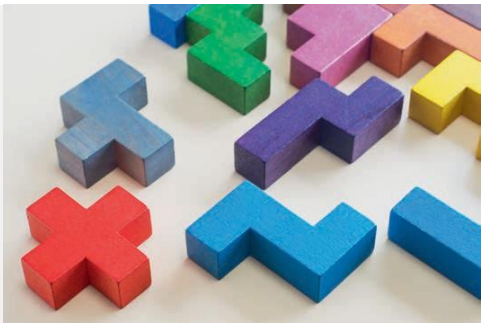
Wir werden lernen, dass die Kryptografie Informationen schützt, indem sie Daten so mischt, dass nur zusätzliche geheime Informationen, der Schlüssel, die ursprünglichen Daten wiederherstellen können. Wenn der zur Ver- und Entschlüsselung einer Nachricht verwendete Schlüssel derselbe ist, spricht man von symmetrischer oder Ein-Schlüssel-Kryptografie. 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 ineffizienten Berechnung von mathematischen Funktionen auf ganzen Zahlen begründet. Bei symmetrischen kryptografischen Algorithmen basiert die Sicherheit darauf, dass kleine Unterschiede in der Eingabe und im Schlüssel zu großen Unterschieden in der Ausgabe führen.

Wir werden zwischen symmetrischer und asymmetrischer Kryptografie unterscheiden und deren größte Herausforderungen diskutieren. 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 Hash-Funktionen. Eine Hash-Funktion ist ein Algorithmus, der aus einer Eingabe mit variabler Größe eine Ausgabe mit fester Größe erzeugt. Die von einer kryptografischen Hash-Funktion aus einer beliebig langen Zeichenkette erzeugte Ausgabekette mit fester Länge ist eine Form der eindeutigen Signatur.

Für bekannte Kryptografie-Algorithmen wie AES, DES, RSA und ECC besprechen wir deren Widerstandsfähigkeit gegen gängige Methoden der Kryptoanalyse wie Brute-Force-Angriffe und, im Falle von kryptographischen Hashes, 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 Authentifizierung, Geheimhaltung und Authentifizierung 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 vertrauenswürdiger Dritter in Form einer Datenbank mit Einträgen und die Möglichkeiten des Quantencomputings diskutieren, die es zu bedenken gilt. 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 wissen, …

… was Kryptologie, Kryptografie und Kryptoanalyse auszeichnet.

… welche Einsatzmöglichkeiten es für die Kryptologie hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit gibt.

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

… was Kerckhoffs‘ Maxime besagt.

… wozu Hash-Funktionen eingesetzt werden.

1. Grundkonzepte der Kryptologie

Einführung

wenn zum Verschlüsseln und Entschlüsseln unterschiedliche Schlüssel verwendet werden. Der Schlüssel zum Verschlüsseln ist öffentlich und der Schlüssel zum Entschlüsseln ist privat.

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

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

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

Asymmetrische Kryptographie Kryptographie ist asymmetrisch,

Kommentiert [JL1]: Please recreate all side notes as text boxes in the translated document. Please check that the term in the main text that coordinates with the side note is put into bold.

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

Single-Key- und Public-Key-Kryptografie

Historisch gesehen war der Schlüssel zur Umkehrung der Umwandlung von verständlichen Daten in unentzifferbare 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, im Zweiten Weltkrieg bei der Enigma-Maschine eingesetzt und findet auch heute noch Anwendung bei der Verschlüsselung eines drahtlosen Netzwerks (z. B. durch den AES-Algorithmus).

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 (allen bekannt) ist. Die symmetrische Verschlüsselung vermeidet das Risiko der Kompromittierung des Chiffrierschlüssels beim Austausch des Schlüssels mit dem Chiffrierer und beim Besitz des Chiffrierschlüssels (durch den Chiffrierer zusätzlich zum Dechiffrierer).

Außerdem ist es für eine digitale Signatur 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 von Primzahlen beruht, oder ECC, das auf der Schwierigkeit beruht, Punkte in endlichen Kurven zu berechnen. Diese schützen (finanzielle) Transaktionen auf sicheren Websites (die durch ein Vorhängeschloss in der Adressleiste des Browsers gekennzeichnet sind).

Datenformat

Bis zum Digitalzeitalter konzentrierte sich die Kryptografie auf die Umwandlung von verständlichem Text in unentzifferbaren Text. Heutzutage befasst sich die Kryptografie schwerpunktmäßig mit der Umwandlung von verarbeitbaren (digitalen) Daten in unentzifferbare (digitale) Daten. Bei den Daten kann es sich z. B. um eine digitale Datei (Text, Bild, Ton, Video usw.) handeln. Sie werden als Bitfolge (angegeben durch eine

Folge von 0en und 1en) oder Bytefolge (angegeben durch eine Folge von hexadezimalen Paaren 00, 01, ..., FE, FF) oder als Zahl (angegeben wie gewohnt durch ihre dezimale Ausprägung 0, 1, 2, 3 ...) bezeichnet. Erinnern wir uns daran, dass jede Bitfolge $1011\ldots$ eine Zahl n in Binärschreibweise $n = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + \ldots$ 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. Die Betrachtungsweise als Zahl wird in der asymmetrischen Kryptografie bevorzugt, deren Algorithmen sie mit mathematischen Funktionen wie der Potenzierung bearbeiten. 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 eine geheime Phrase (mit Leerzeichen).

Bei dem 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. Damit Sie sich den Code besser einprägen können, sollten Sie vollständige geheime Sätze oder Passphrasen verwenden.

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+0tJhRCqlOPGzxVaBX0b61CYzN5jurAhZi2CCZlE+xte+
```

Kommentiert [JL2]: Please maintain the use of code in the translated document as given in the original document.

```
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 so zu verändern, dass sie für alle anderen als den vorgesehenen Empfänger unentzifferbar sind. Kryptoanalyse (vom griechischen *analýein*: „Auflösung“) oder Codeknacken ist die Kunst, die verborgene Schrift ohne den zugehörigen Schlüssel zu entschlüsseln. Zum Knacken 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 allgemeinste 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 man sie in eine andere Nachricht einbettet (in ein Bild, eine Audio-Datei oder ein binäres Datenformat), so dass niemand außer dem vorgesehenen Empfänger von der Existenz der Nachricht überhaupt 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 geheimgehaltene 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 Teilnehmer an einer Kommunikation zweifelsfrei verifiziert werden können, was als Non-Repudiation (Nachweisbarkeit) bekannt ist. Dies eröffnet zahlreiche Möglichkeiten, insbesondere für den elektronischen Handel.

Alle kryptografischen Verfahren, die 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 eines Informationsbits, z. B. eines Buchstabens, durch ein anderes, in der Regel, um es 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 $2^{32} \approx 4$ Milliarden Zeichen abzubilden und enthält u.a. die Alphabete zahlreicher Sprachen, wie Deutsch und Chinesisch, sowie bedeutungsvolle 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. Die Ersetzung erfolgt jedoch nach einer durch einen Schlüssel festgelegten Regel, so dass niemand ohne dessen Wissen die Ersetzung umkehren kann.

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, dann in Chiffren verschlüsselt, z. B. mit dem AES-Algorithmus (Advanced Encryption

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

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

CIA

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

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

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 knacken. Stattdessen werden die Schlüssel oder der Klartext in vielen Fällen vor der Verschlüsselung oder nach der Entschlüsselung gestohlen. Die Kryptografie bietet also ein hohes Maß an technischer Sicherheit, doch menschliches Versagen, z. B. aus Bequemlichkeit oder unangebrachtem Vertrauen, ist der größte Schwachpunkt der Informationssicherheit.

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, sind die Daten 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 einbauen.

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

- 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 und ein
- Eindringen in das System verhindert wird, 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

- „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, und
- „Nachweis, dass eine Nachricht nicht verändert oder verfälscht wurde“ (IBM, o. J.).

Eine Person weist ihre Identität durch einen Beleg nach. Es gibt verschiedene Möglichkeiten, diesen Beleg abzufragen, insbesondere auf Computern. Die gängigsten Methoden sind PIN-Nummern 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, digitale Signaturen von Dritten, eingesetzt. Dies kann entweder, wie beim Web of Trust in OpenPGP, durch Signaturen zwischen Personen, die sich untereinander bekannt sind, oder, wie auf sicheren Seiten in einem Webbrowser, durch eine Signatur einer vorbehaltlos vertrauenswürdigen, zentralen Zertifizierungsstelle realisiert werden.

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. seine 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 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 Thomas sie geschickt hat, kann Thomas dies 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 ganz 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 bekannt waren, wurden sie wegen der fehlenden Automatisierung in der Kryptografie nicht wirklich 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 Transpositionschiffren 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 Stab, der mit einem Pergamentband umwickelt ist, 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 Transpositionschiffre: Sie

vermischt oder transponiert die Buchstaben des Klartextes (OPTED, o. J.).

Caesar-Chiffre

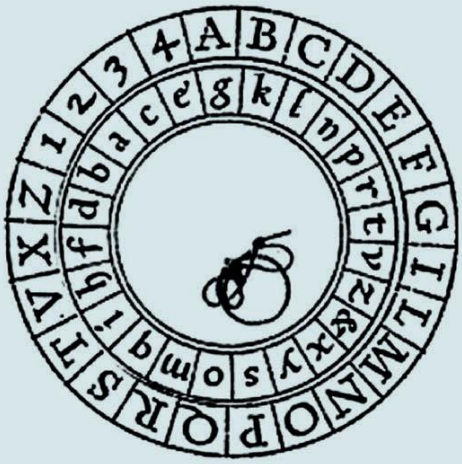
Die Cäsar-Chiffre ist eine der einfachsten und bekanntesten Verschlüsselungen, benannt nach Julius Cäsar, der sie zur Nachrichtenübermittlung mit seinen Generälen verwendete. Bei dieser Substitutionschiffre wird jeder Buchstabe des Klartextes durch einen festen anderen Buchstaben ersetzt. Jeder Buchstabe

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 $2^5 = 32$ 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, die 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).

The Alberti Substitution Disk

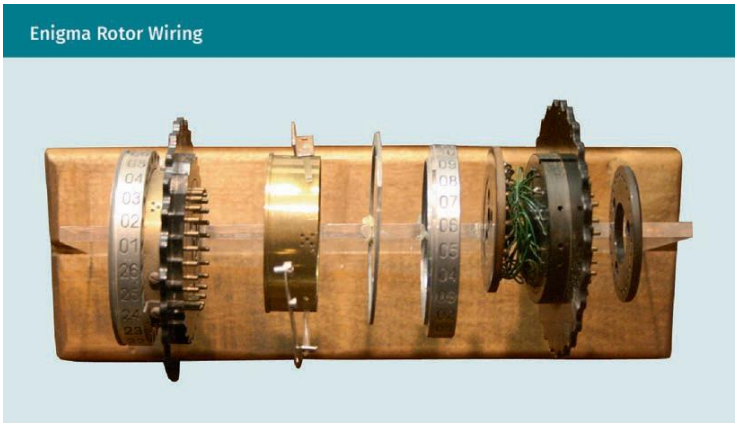


ADFGVX-Chiffre
Die berühmteste Chiffre des Ersten Weltkriegs war die deutsche Fraktionierungschiffre ADFGVX, die am 5. März 1918, also gegen Ende des Ersten Weltkriegs, eingeführt wurde. Fritz Nebel, ein Nachrichtenoffizier der Armee, entwickelte die vermeintlich unknackbare ADFGVX-Chiffre für den Einsatz

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 man alle Buchstaben eines

Lekti

Klartextes von (höchstens) gleicher Länge entschlüsseln

kann. Eine buchstabenweise Substitution streut also wenig und bewirkt kaum Veränderungen. Eine optimale Streuung 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 Streuung. Computer ermöglichten zudem die Kombination von Substitutionen (z. B. Cäsar-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 (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 nicht nur als immun gegen die ausgeklügeltsten bekannten Angriffe, wie z. B. differentielle Kryptoanalyse, und als elegantes und einfaches Design, sondern war auch so klein, dass es auf Chipkarten implementiert werden konnte (mit weniger als 10.000 Byte Code) und 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 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 sie nur ein Verfahren zum Austausch eines geheimen Schlüssels über einen unsicheren Kanal geschaffen. Der kryptografische RSA-Algorithmus (Rivest et al., 1978) oder der Elgamal-Algorithmus (Elgamal, 1985) wendeten dieses Konzept erstmals an. 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.