Digital Business University
of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Grundlagen Cyber- & IT-Security

Sommersemester 2024

Verschlüsselte Kommunikation: Wie kryptografische Verfahren digitale Sicherheit gewährleisten

Studienarbeit

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
David Lübeck

9. August 2024

Inhaltsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIA	Confidentiality, Integrity, Availability
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMV	Europay International, MasterCard und VISA
FinTS	Financial Transaction Services
GSM	Global System for Mobile Communications
HMAC	Hash-based Message Authentication Code
IPsec	Internet Protocol Security
LTE	Long Term Evolution
MD5	Message-Digest-Algorithm 5
MITM	Man-In-The-Middle
NIST	National Institute of Standards and Technology
OTP	One-Time-Pad
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public-Key-Infrastruktur
RC4	Rivest Cipher 4
RC6	Rivest Cipher 6
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Networking
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

1 Einleitung

Die moderne Welt ist geprägt von einem stetigen Kommunikationsbedürfnis. Mit der Zeit hat sich ein globales Netzwerk entwickelt, das den Austausch unterschiedlichster Informationen ermöglicht, um diesem Bedürfnis nachzukommen. Dabei ist der Gedanke eines global vernetzten Informationssystems nicht neu. Lediglich die Art der Informationen, die über das Netzwerk geteilt werden, hat sich im Laufe der Zeit enorm verändert, wodurch unzählige neue Möglichkeiten geschaffen wurden.

Mit der Entwicklung des Internets wurde es erstmals möglich, Informationen mit nur minimalem zeitlichen Verlust über weit verteilte Netze zu verbreiten. So konnte mit der Zeit fast jedes erdenkbare technische Gerät an ein globales oder lokales Netzwerk angeschlossen werden.

1.1 Problemstellung

Die große Herausforderung bestand nun darin, Kommunikationswege zu finden, mit denen die Sicherheit und Integrität der übertragenen Daten zu jedem Zeitpunkt gewährleistet ist. Daraus hat sich das Feld der *Kryptografie* entwickelt, das anhand unterschiedlicher Verfahren Antworten auf diese Fragen liefern soll. Denn schon häufig sind die Auswirkungen unsicherer Kommunikationskanäle sichtbar geworden. So existieren mittlerweile vielfältige Angriffsmethoden, die in nahezu allen Bereichen des Lebens erhebliche Auswirkungen haben können.

Schnell wurde klar, dass Kryptografie insbesondere in der digitalen Ära essenziell für die Kommunikationssicherheit ist. Gleichzeitig ist es von entscheidender Bedeutung, dass mit der Wahl eines sicheren Kommunikationskanals auch die Frage nach dem Grad der Sicherheit beantwortet werden muss. Denn nicht jedes eingesetzte Verfahren bietet in der Praxis auch höchstmögliche Sicherheit.

In der heutigen vernetzten Welt werden komplexe Anforderungen an eine gute Umsetzung und Auswahl kryptografischer Verfahren gestellt. Denn mit der Zeit entwickeln sich immer komplexere und stärkere Angriffsmethoden, auf die mittels geeigneter Verschlüsselung reagiert werden muss. Nahezu das gesamte öffentliche Leben hängt von sicheren Datenströmen ab. Es stellt sich also die Frage, inwieweit digitale Sicherheit gewährleistet werden kann und welche Möglichkeiten das Gebiet der Kryptografie hierzu eröffnet.

1.2 Inhalte der Arbeit

Diese Arbeit befasst sich mit den unterschiedlichen Formen der Kryptografie und welche Antworten diese auf das mit der Zeit veränderte Bedürfnis nach sicherer Kommunikation liefern.

Hierzu werden in **Kapitel 2** zunächst die **Grundlagen** der Kryptografie erläutert und aufgezeigt, welche Ziele und Herausforderungen an sie gestellt werden. Dies wird vor allem unter dem Aspekt der *Sicherheit* beleuchtet, wobei explizit auf den Sicherheitsaspekt im Bereich der Kryptologie eingegangen wird.

Anschließend werden in **Kapitel 3** zunächst unterschiedliche **klassische Verschlüsselungsverfahren** benannt, die als Basis für heutige moderne Verschlüsselungsverfahren gelten. Dabei werden die unterschiedlichen Arten der Verfahren aufgezeigt und erläutert, welche Vor- und Nachteile sie jeweils charakterisieren. Daran anknüpfend werden in **Kapitel 4** die **modernen Verschlüsselungsverfahren** in ihrer typischen Eigenschaft der symmetrischen und asymmetrischen Techniken behandelt, wobei zusätzlich noch das Feld der hybriden Verfahren beleuchtet wird. **Kapitel 5** behandelt im Anschluss die Nutzung asymmetrischer Verfahren zur Erstellung **digitaler Signaturen**. Hierbei wird außerdem die Funktionalität von Hashfunktionen vorgestellt.

Die Arbeit schließt in **Kapitel 6** mit einer **Zusammenfassung** der vorgestellten Kapitel und geht mit einer kritischen Würdigung erneut auf die ursprüngliche Problemstellung ein. Außerdem wird ein Ausblick auf aktuelle Forschungsfelder und offene Fragestellungen gegeben.

1.3 Abgrenzungen

Der Fokus dieser Arbeit liegt auf der Vorstellung unterschiedlicher Arten kryptografischer Verfahren. Es wird nicht näher auf konkrete Angriffsszenarien eingegangen, da diese häufig ein deutlich tiefgreifenderes Verständnis des Aufbaus von IT-Systemen erfordern. Dies würde den Rahmen dieser Arbeit sprengen und ist in ihrer Tiefe für das Verständnis der vorgestellten kryptografischen Verfahren auch nicht notwendig. Dennoch werden im Laufe der Arbeit einige Angriffsmethoden benannt und passende Abwehrmechanismen in Form kryptografischer Verfahren vorgestellt.

Ebenfalls wird nicht näher auf die sogenannte *Quantenkryptografie* eingegangen, ein Gebiet, das sich mit neueren Verschlüsselungsverfahren befasst, um dem Zuwachs moderner Quantencomputer standzuhalten. Diese Verfahren sind noch relativ neu und dementsprechend nicht sehr weit verbreitet, weshalb sie nicht näher beleuchtet werden. Am Ende der Arbeit wird jedoch ein Ausblick gegeben, inwieweit die Quantenkryptografie zukünftig eingesetzt werden könnte und welche Ideen hierfür existieren.

2 Grundlagen

2.1 Kryptografie

Kryptografie ist die Lehre der Verschlüsselung von Informationen (Hansen et al., 2015). Gemeinsam mit dem Bereich der *Kryptanalyse*, welche sich mit dem Aufbrechen ver-

schlüsselter Nachrichten befasst, gehört sie zum übergeordneten Gebiet der *Kryptologie* (Ertel & Löhmann, 2020).

Innerhalb des Gebiets der Kryptografie existieren kryptografische Verfahren (häufig auch *Verschlüsselungsverfahren* oder *Chiffren* genannt), die sich explizit mit der Ver- und Entschlüsselung von Informationen auseinandersetzen. Die zu verschlüsselnden Informationen werden als *Klartext* bezeichnet; die verschlüsselten Informationen bilden den *Geheimtext* (häufig auch *Chiffrat* genannt). Das Ziel der Kryptografie besteht darin, „Daten so zu verändern, dass nur ein autorisierter Empfänger in der Lage ist, den Klartext zu rekonstruieren“ (Esslinger, 2018, S. 1). Insofern ist der Klartext ein Merkmal, das nur Absender und Empfänger bekannt sein soll, während der Geheimtext auch Dritten zugänglich gemacht werden kann.

Die Veränderung der Daten vom Klartext zum Geheimtext erfolgt im Rahmen der *Verschlüsselung*, bei welcher der Klartext durch den Absender „nach einer bestimmten Methode und unter Einbeziehung eines *Schlüssels* in eine scheinbar sinnlose Zeichenfolge umgewandelt“ wird (Hansen et al., 2015, S. 384). Der Empfänger kann dann den Geheimtext mittels *Entschlüsselung* wieder lesbar zum Klartext umwandeln. Je nach Verschlüsselungsverfahren werden unterschiedliche Schlüssel oder Schlüsselpaare verwendet (siehe Kapitel 3 und Kapitel 4).

2.2 Sicherheit in der Kryptologie

Damit sichere Kommunikation mittels kryptografischer Verfahren gewährleistet ist, muss zunächst definiert werden, wie der Begriff *Sicherheit* konkret eingeordnet werden kann. In der Kryptologie existieren hierzu zwei Hauptnotationen, welche „Sicherheit in Abhängigkeit von den Möglichkeiten des Angreifers“ definieren (Esslinger, 2018, S. 2):

- **Berechenbare oder bedingte Sicherheit**: Wenn ein Verschlüsselungsverfahren (obwohl theoretisch möglich) „selbst mit den besten bekannten Verfahren nicht gebrochen werden kann“ (Esslinger, 2018, S. 2), gilt es als *berechenbar sicher*. Die Fortschritte in der Mathematik und bei Hochleistungsrechnern erfordern jedoch eine ständige Anpassung, um mit diesem Konzept, das auf der Annahme über begrenzte Rechenkraft und aktuellem Stand der Wissenschaft basiert, Stand halten zu können (Esslinger, 2018).

- **Informations-theoretische oder unbedingte Sicherheit**: Hat ein Angreifer theoretisch unbegrenzt viele Ressourcen und kann dennoch ein Verschlüsselungsverfahren nicht brechen, so gilt dieses als *unbedingt sicher*. In diesem Fall ist es auch informations-theoretisch nicht möglich, aus dem Geheimtext sinnvolle Informationen zu gewinnen. (Esslinger, 2018)

2.3 Ziele der Kryptografie

In der IT-Sicherheit werden im Allgemeinen drei übergeordnete Hauptziele betrachtet. Diese werden als *Confidentiality, Integrity, Availability (CIA)-Triade* bezeichnet und setzen sich aus folgenden Kriterien zusammen:

- **Vertraulichkeit** (engl. *confidentiality*): „Bestreben, geheime Information für unberechtigte Dritte unzugänglich zu halten“ (Hansen et al., 2015, S. 374)
- **Integrität** (engl. *integrity*): „Bestreben, die Unverändertheit von Daten (...) nachzuweisen“ (Hansen et al., 2015, S. 375)
- **Verfügbarkeit** (engl. *availability*): „Bestreben, dass Dienste, die einem berechtigten Benutzer (...) angeboten werden, diesem auch stets zur Verfügung stehen“, insbesondere durch Vermeidung einer übermäßigen Beanspruchung eines anderen Benutzers (Hansen et al., 2015, S. 377)

Ein wichtiges Ziel ist außerdem die **Authentifikation** (engl. *authentication*), welche die „nachweisliche Identifikation eines Benutzers oder Kommunikationspartners“ (Hansen et al., 2015, S. 376) beschreibt. Für einige dieser Ziele existieren unterschiedliche kryptografische Verfahren. Dabei werden je nach Anwendungsfall unter anderem folgende Aspekte betrachtet:

- **Schutz vor Datenverlust und -diebstahl**: Besonders schützenswerte Daten wie Kreditkarteninformationen, medizinische Aufzeichnungen, Ausweisdokumente oder Geschäftsgeheimnisse werden durch Verschlüsselung geschützt. Dies ist besonders in Betrachtung der Vertraulichkeit ein wichtiges Ziel der Kryptografie.
- **Sichere Kommunikationskanäle**: Die Kommunikation zwischen Regierungen, Privatpersonen und Unternehmen erfordert kryptografische Verfahren, um sie aktiv gegen Spionage und Abhörversuche zu schützen.
- **Vermeidung von Identitätsdiebstahl**: Insbesondere bei der Übertragung sensibler Daten wie Passwörter oder Kreditkarteninformationen, mit denen Identitätsdiebstahl betrieben werden kann, ist Verschlüsselung ein wichtiges und unerlässliches Hilfsmittel. Verschlüsselung erfüllt hier außerdem das Ziel der Authentifizierung, durch das die korrekte Identität aller Kommunikationspartner gewährleistet wird.
- **Sicherstellung der Integrität von Daten**: Um sicherzustellen, dass Daten bei der Übertragung nicht verändert werden, können ebenfalls kryptografische Verfahren eingesetzt werden. Dadurch wird die Datenintegrität gewährleistet und unerwünschte Manipulationen verhindert. In der Praxis spielt dies vor allem zur Abwehr von Man-In-The-Middle (MITM)-Angriffen eine entscheidende Rolle.

2.4 Anwendungsfälle

Durch die immer stärker wachsende Verlagerung von Informationen und Daten in öffentliche Netze wuchs mit der Zeit auch der Bedarf zur Ausweitung kryptografischer Anwendungen in verschiedene Bereiche der Netzwerkinfrastruktur. So lassen sich mittlerweile eine Vielzahl an Anwendungsfällen auflisten, bei denen kryptografische Verfahren Anwendung finden. Darunter zählen beispielsweise:

- **Datenübertragung**: Der sichere Transfer von Daten ist ein zentrales Einsatzgebiet der Kryptografie. Dabei kommen Verschlüsselungsverfahren zum Einsatz, die vor allem die Vertraulichkeit und Integrität der Daten gewährleisten. Dies wird zumeist durch Protokolle wie Secure Sockets Layer (SSL) und Transport Layer Security (TLS) realisiert.

- **Datenspeicherung**: Neben der Übertragung werden auch bei der Speicherung von Daten kryptografische Verfahren eingesetzt. Dies schützt die Informationen sowohl auf physischen Geräten wie Festplatten als auch Cloud-Speichern und etabliert eine Form der Zugriffskontrolle, da für den Zugriff der entsprechende Geheimschlüssel benötigt wird.

- **Identitätsmanagement**: Zur Authentifizierung und Autorisierung von Benutzern können kryptografische Verfahren verwendet werden. Häufig stehen hierzu geeignete Infrastrukturen zur Verfügung, mit denen zum Beispiel bei asymmetrischen Verschlüsselungsverfahren bestimmte Benutzermerkmale ausgetauscht werden können.

- **Digitale Signatur**: Um die Echtheit digitaler Dokumente oder Transaktionen zu bestätigen, können digitale Signaturen eingesetzt werden, die auf kryptografischen Verfahren aufgebaut sein können.

- **Kommunikationssysteme**: Zur Wahrung der Vertraulichkeit, insbesondere bei der militärischen oder geheimdienstlichen Kommunikation, werden kryptografisch sichere Kommunikationssysteme entwickelt. Dabei wird der gesamte Kommunikationskanal verschlüsselt. Dies wird beispielsweise bei der Mobilfunkkommunikation mittels Global System for Mobile Communications (GSM) oder Long Term Evolution (LTE) realisiert.

3 Klassische Verschlüsselungsverfahren

Alle bis etwa 1950 entwickelten Verfahren werden als *klassische Chiffren* bezeichnet (Ertel & Löhmann, 2020). Die ersten dieser Verfahren entstanden bereits vor über 3000 Jahren und sind beispielsweise für Geheimdienste immer noch sehr populär (Esslinger, 2018). Techniken wie *Transposition* (Vertauschung), *Substitution* (Ersetzung),

Blockbildung und deren Kombination finden sich in fast allen klassischen Verschlüsselungsverfahren wieder (Esslinger, 2018) und bilden auch heute noch die Grundlage für viele moderne Verschlüsselungsverfahren.

3.1 Transpositionschiffren

Bei *Transpositionschiffren* werden einzelne Buchstaben des Klartexts mittels Permutation (Umstellung) in den Geheimtext umgewandelt. „Die Zeichen bleiben gleich, tauschen aber ihre Plätze“ (Ertel & Löhmann, 2020, S. 32). Daher sind diese Verfahren leicht zu analysieren und gelten nicht mehr als sicher.

Schon die Spartaner nutzten Transpositionschiffren zur sicheren Kommunikation. Sie entwickelten mit der *Skytale* ein zum damaligen Zeitpunkt effektives Verfahren, um sich gegenseitig vor drohenden Gefahren zu warnen und geheime Informationen auszutauschen. Dabei wickelten sie einen Streifen Leder oder Pergament um einen Holzstab, die Skytale, und schrieben die Nachricht der Länge des Stabes nach auf den Streifen, wickelten ihn wieder ab und übergaben ihn an den Empfänger, der die scheinbar sinnlose Zeichenfolge wiederum auf seine Skytale gleicher Länge wickelte und so die Nachricht entschlüsselte. Mit diesem Verfahren konnte Lysander von Sparta im Jahre 404 v. Chr. einen drohenden Angriff des Pharnabasus von Persien abwehren, nachdem ein Bote ihm eine geheime Nachricht übermittelte, die er mithilfe seiner Skytale entschlüsseln konnte (Singh, 2001).

3.2 Substitutionschiffren

Im Gegensatz zu Transpositionschiffren wird bei einer *Substitutionschiffre* „jedes Zeichen eines Klartextes durch ein anderes ersetzt“ (Ertel & Löhmann, 2020, S. 32). Die Position der einzelnen Zeichen bleibt jedoch gleich (Ertel & Löhmann, 2020).

3.2.1 Monoalphabetische Substitutionschiffren

Bei *monoalphabetischen Substitutionschiffren* wird „jedes Klartextzeichen immer auf das gleiche Geheimtextzeichen abgebildet“ (Ertel & Löhmann, 2020, S. 32). Ein klassisches Beispiel hierfür ist die *Caesar-Verschlüsselung*. Sie geht auf den römischen Kaiser und Feldherr Gaius Julius Cäsar zurück, der laut römischen Quellen „für seine Kommunikation so vorgegangen ist, dass er jeden Buchstaben des Alphabets durch den drei Stellen weiter stehenden ersetzt hat“ (Manz, 2019, S. 7).

3.2.2 Polyalphabetische Substitutionschiffren

Demgegenüber haben *polyalphabetische Substitutionschiffren* keine feste Zuordnung zwischen Klartext- und Geheimtextzeichen, sondern diese ist (meist abhängig vom Schlüssel) variabel (Esslinger, 2018).

Die **Vigenère-Chiffre** ist ein populäres Beispiel polyalphabetischer Substitutionschiffren. Sie wurde im 16. Jahrhundert von dem französischen Diplomaten Blaise de Vigenère vorgestellt und wird heute noch als Prototyp für viele in der Praxis eingesetzten Algorithmen verwendet (Beutelspacher, 2014). Grundlage des Verfahrens bietet das sog. *Vigenère-Tableau*, mit dessen Hilfe jedes Klartextzeichen mit einem anderen Geheimtextalphabet, das aus dem entsprechenden Zeichen des Schlüsselwortes entsteht, verschlüsselt wird (Esslinger, 2018).

Eine Vigenère-Chiffre mit bekannter Schlüssel- bzw. Periodenlänge ist die **Enigma-Chiffriermaschine** (Ertel & Löhmann, 2020). Sie wurde von dem deutschen Unternehmer Arthur Scherbius erfunden und 1918 erstmals zum Patent angemeldet. Die Enigma besteht aus raffiniert angeordneten Verschaltungen, einem Steckbrett, mehreren beweglichen Walzen und einer Umkehrwalze. Durch den in den Walzen befindlichen Drehmechanismus erhält sie den Charakter der polyalphabetischen Chiffren (Manz, 2019). Für die deutsche Wehrmacht hat sich die Enigma im zweiten Weltkrieg besonders bewährt gemacht. Sie konnte mit ihrer Hilfe bis Ende 1943 den Nordatlantik beherrschen, indem sie die Positionen aliierter Versorgungskonvois übermittelten (Ertel & Löhmann, 2020). Schlussendlich konnte eine Kommunikation mithilfe der Enigma aber nicht mehr als sicher angesehen werden, da es immer wieder gelang, sie trotz mehrfacher Weiterentwicklungen zu entschlüsseln (Landwehr, 2015).

Eine andere Weiterentwicklung der Vigenère-Chiffre ist das **One-Time-Pad (OTP)**, welches auch als „die perfekte Chiffre“ (Ertel & Löhmann, 2020, S. 52) betitelt wird. Es nutzt ein unendlich langes Schlüsselwort (Ertel & Löhmann, 2020) und gilt damit theoretisch als unbedingt sicheres Verschlüsselungsverfahren (Esslinger, 2018). In der Praxis spielt es aber „außer in geschlossenen Umgebungen, [wie] zum Beispiel beim heißen Draht zwischen Moskau und Washington, kaum eine Rolle“ (Esslinger, 2018, S. 2). Das liegt vor allem am Geheimschlüssel, der nur einmal verwendet werden darf, zufällig gewählt sein muss und mindestens so lang sein muss wie die zu schützende Nachricht (Esslinger, 2018). Dadurch ist der Aufwand für den Schlüsselaustausch in der Praxis schlichtweg zu hoch (Ertel & Löhmann, 2020).

3.3 Kombination aus Transposition und Substitution

Als kryptografisch sicherer als Transpositions- und Substitutionschiffren gelten Kombinationen beider Verfahren (Esslinger, 2018). Erwähnenswert ist hier beispielsweise die *ADFG(V)X*-Verschlüsselung. Sie wurde 1918 in Deutschland im ersten Weltkrieg entwickelt und war dauerhaft für Feldoperationen an der Westfront und für die sichere Kommunikation mit dem Schwarzmeer-Raum im Einsatz. Bei ADFG(V)X findet zunächst eine Ersetzung (Substitution) von Buchstabenpaaren anhand einer 5x5- oder 6x6-Matrix statt. „Abschließend wird auf dem so entstandenen Text eine (Zeilen-)Transposition durchgeführt“ (Esslinger, 2018, S. 42).

4 Moderne Verschlüsselungsverfahren

Die bisher vorgestellten klassischen Verschlüsselungsverfahren zeigen deutlich, dass bereits vor Jahrhunderten Verfahren entwickelt wurden, um sichere Kommunikation zu gewährleisten. Spätestens mit der Entwicklung neuer Verfahren im ersten und zweiten Weltkrieg zeigte sich aber auch, dass mit zunehmendem Stand der Wissenschaft und dem Einsatz erster Computer selbst die komplexeste Variante der polyalphabetischen Chiffren nicht mehr als sicher angesehen werden kann (Singh, 2001). Während Chiffren wie das OTP absolute Sicherheit bieten, gelten etwa klassische monoalphabetische Transpositionschiffren als nicht mehr sicher. Entsprechend mussten neue Verfahren gefunden werden, die „in ihrer Sicherheit (...) irgendwo zwischen der Verschiebechiffre und dem One-Time-Pad“ lagen (Ertel & Löhmann, 2020, S. 57). Man unterteilt diese typischerweise in *symmetrische* und *asymmetrische Verschlüsselungsverfahren*. Eine Kombination beider Technologien wird unter den *hybriden Verschlüsselungssystemen* zusammengefasst (Esslinger, 2018).

4.1 Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass sowohl für die Verschlüsselung als auch für die Entschlüsselung der gleiche Geheimschlüssel verwendet wird. Das Prinzip der symmetrischen Verschlüsselung ist allerdings nicht neu, denn auch „alle klassischen Chiffren sind vom Typ symmetrisch“ (Esslinger, 2018, S. 6). Viele der modernen Verschlüsselungsverfahren nutzen ebenfalls die bekannten Methoden klassischer Verfahren wie Transposition und Substitution, allerdings in einer weitaus komplexeren und umfangreicheren Form. Häufig kommen umfangreiche sog. *S-Boxen* zum Einsatz, die in Kombination mit Permutation tief in die Algorithmen einzelner Verschlüsselungsverfahren eingebettet sind. Die einzelnen Verfahren können grob in *Bitstrom-* und *Bitblock-Chiffren* unterteilt werden (Esslinger, 2018).

4.1.1 Bitstrom-Chiffren

Bei Bitstrom-Chiffren „wird der Reihe nach jedes einzelne Bit einer Bitkette nach einer anderen Vorschrift verschlüsselt, entweder unverändert gelassen oder negiert“ (Esslinger, 2018, S. 336). Dabei wird häufig die XOR-Verschlüsselung angewendet, bei der sowohl der Klartext als auch der Schlüssel (der sog. *Schlüsselstrom*) als Folge von Bits aufgefasst wird. Die eigentliche Verschlüsselung erfolgt dann durch binäre Addition des „jeweils nächste[n] Bit[s] des Klartexts mit dem nächsten Bit des Schlüsselstroms“ (Esslinger, 2018, S. 336). Ein Beispiel aus den klassischen Chiffren ist das OTP. In der modernen Kryptografie wurden unter anderem folgende Bitstrom-Chiffren populär:

- **Rivest Cipher 4 (RC4)**: Ronald Rivest entwickelte dieses Verfahren im Jahr 1987 (Manz, 2019), das unter anderem auch heute noch im SSL-Protokoll ver-

wendet wird, um die Client-Server-Kommunikation im Internet abzusichern (Esslinger, 2018).

- **A5**: Unterschiedliche Versionen dieses Verfahrens werden in diversen Mobilfunkstandards verbaut, unter anderem GSM und LTE, um den Funkverkehr zu verschlüsseln. Bei den neueren Version *A5/3* und *A5/4* handelt es sich um Bitstrom-Chiffren (Manz, 2019).

- **E0**: Diese Bitstrom-Chiffre wurde früher für die Bluetooth-Datenverschlüsselung verwendet. Mittlerweile werden allerdings modernere Verfahren eingesetzt (Manz, 2019).

Ein Vorteil von Bitstrom-Chiffren ist, „dass man zeichenweise dechiffrieren kann und nicht immer einen ganzen Chiffretextblock abwarten muss“ (Manz, 2019, S. 29), wie dies bei Bitblock-Chiffren der Fall ist. Dadurch ist das Verfahren sehr schnell und bietet bei gut gewähltem Schlüsselstrom eine sehr hohe Sicherheit (Esslinger, 2018). Auf der anderen Seite sind Bitstrom-Chiffren „anfällig gegen bekannten Klartext; jedes erratene Klartextbit ergibt ein Schlüsselbit“ (Esslinger, 2018, S. 337). Ein Angreifer kann so „bei bekanntem Klartextstück das entsprechende Schlüsselstück ermitteln und dann diesen Klartext beliebig austauschen“ (Esslinger, 2018, S. 337) – kurzum: „die Integrität der Nachricht ist unzureichend geschützt“ (Esslinger, 2018, S. 337).

4.1.2 Bitblock-Chiffren

Bei Bitblock-Chiffren erfolgt die Verschlüsselung durch Unterteilung der Nachricht in einzelne Blöcke, wobei jeder Block einzeln nacheinander mit dem selben Verfahren verschlüsselt wird (Ertel & Löhmann, 2020; Manz, 2019).

Ein relevantes Maß für die Sicherheit von Bitblock-Chiffren ist die Wahl der Schlüssellänge. Es gilt das Kriterium: „Sie soll so groß sein, dass eine Exhaustion des Schlüsselraums, also eine ‚Brute-Force-Attacke‘, aussichtslos ist“ (Esslinger, 2018, S. 289). In der Regel gilt hierbei eine Schlüssellänge von 128 Bit als ausreichend (Esslinger, 2018). Ebenso relevant ist die Wahl der Blocklänge. Sie „soll groß genug sein, um Muster- und Häufungsanalysen unmöglich zu machen; noch besser ist es, jede Art von Informationspreisgabe über den Klartext (...) im Geheimtext zu vermeiden“ (Esslinger, 2018, S. 290). Die häufig gewählte Blocklänge von 64 Bit wird zumeist schon als bedenklich angesehen, weshalb viele Verfahren mittlerweile eine Blocklänge von 128 Bit verwenden (Esslinger, 2018).

Zusätzlich stellen die beiden Gütekriterien *Konfusion* und *Diffusion* wichtige Anforderungen an die Implementierung einer sicheren Bitblock-Chiffre (Manz, 2019). Konfusion besagt, dass „zwischen Klar- und Chiffretext (...) möglichst keine Beziehung erkennbar sein [soll], die für einen Angriff ausgenutzt werden könnte“ (Manz, 2019, S. 30). Ergänzend soll durch Diffusion sichergestellt werden, dass „alle Zeichen des Klartextes

und des Schlüssels (...) möglichst viele Zeichen des Chiffretextes beeinflussen“ (Manz, 2019, S. 30).

So sind mit der Zeit eine Fülle an Bitblock-Chiffren in der modernen Kryptografie populär geworden, unter anderem:

- **Data Encryption Standard (DES)**: Basierend auf einem von Horst Feistel entwickelten Algorithmus (*LUCIFER*) wurde im Jahr 1977 der DES veröffentlicht. Seinem Ursprung entsprechend wird er – wie viele andere Bitblock-Chiffren – auch als *Feistel-Chiffre* bezeichnet. Die Schlüssellänge beträgt 64 Bit, wobei effektiv nur 56 Bit verwendet werden (die restlichen 8 Bit werden zur Fehlererkennung verwendet) (Manz, 2019). Wie viele klassische Verschlüsselungsverfahren verwendet auch das moderne Verfahren DES Methoden zur Transposition (mittels Permutation) und Substitution (Ertel & Löhmann, 2020). Während das Verschlüsselungsverfahren lange Zeit als sicher galt, wurde es schließlich im Frühjahr 1999 „durch eine vollständige Schlüsselsuche gebrochen“ (Beutelspacher, 2014, S. 23). Es stellte sich heraus, dass die Schlüssellänge von 56 Bit schlichtweg zu kurz war, sodass sich mittels Brute-Force-Angriff nach nur kurzer Zeit ein sinnvoller Klartext ergab (Beutelspacher, 2014). In der Konsequenz gilt das Verfahren nicht mehr als sicher und sollte als solches grundsätzlich nicht mehr verwendet werden.

- **Triple-DES**: Eine Erweiterung zum unsicheren DES stellt Triple-DES dar. Dabei wird DES drei Mal hintereinander mit zwei verschiedenen Schlüsseln angewendet (Ertel & Löhmann, 2020) und hat somit eine effektive Schlüssellänge von 112 Bit (Manz, 2019). Eingesetzt wird Triple-DES unter anderem für Pretty Good Privacy (PGP). Aber auch im Bereich der Finanzdienstleistungen kam Triple-DES vermehrt zum Einsatz. So wurde es beispielsweise bis Version 3.0 der Financial Transaction Services (FinTS) als symmetrisches Verfahren zur Verschlüsselung von Überweisungsdaten akzeptiert. Außerdem bevorzugte die von der Europay International, MasterCard und VISA (EMV) herausgegebene Spezifikation zur Verschlüsselung von Kreditkartenzahlungen Triple-DES als Verschlüsselungsverfahren. Und auch im elektronischen Reisepass (ePass) wird Triple-DES zur Verschlüsselung der Datenübertragung eingesetzt (Manz, 2019).

- **Advanced Encryption Standard (AES)**: Der AES ist mittlerweile der Standard unter den symmetrischen Verschlüsselungsverfahren (Esslinger, 2018) und gilt als „das derzeit mit Abstand wichtigste symmetrische Chiffrierverfahren“ (Manz, 2019, S. 46). Der dazugehörige Rijndael-Algorithmus wurde im Jahr 2000 vorgestellt und zum Nachfolger des DES-Verfahrens gekürt (Esslinger, 2018). Auch er verwendet Verfahren zur Substitution (mittels sog. *S-Boxen*) und Transposition (etwa mittels `ShiftRow`-Transformation). Er setzte sich in einer Ausschreibung des National Institute of Standards and Technology (NIST) unter

anderem gegen die Feistel-Chiffren *Rivest Cipher 6 (RC6)* und *Twofish* durch, womöglich vor allem wegen seines Geschwindigkeitsvorteils (Manz, 2019). In seiner standardisierten Form hat er „eine Blocklänge von 128 Bit und ermöglicht Schlüssellängen von 128, 192 oder 256 Bit“ (Manz, 2019, S. 47). AES ist „gegen alle bis heute bekannten Angriffe sicher“ (Manz, 2019, S. 51) und bewirkt eine hohe Konfusion und Diffusion (Manz, 2019). Nicht verwunderlich ist daher sein vielfältiges Einsatzgebiet, das nach Manz (2019) unter anderem folgende Bereiche umfasst:

- Datenübertragung in Kombination mit asymmetrischen Verschlüsselungsverfahren (siehe Abschnitt 4.2), z. B. mittels TLS
- Festplattenverschlüsselung & Verschlüsselung von ZIP-Archiven
- Datenverschlüsselung im Wireless Local Area Network (WLAN) mittels Wi-Fi Protected Access 2 (WPA2)
- Bluetooth-Datenverschlüsselung
- E-Mail-Kommunikation mittels PGP
- Verschlüsselung von Überweisungsdaten bei FinTS, ebenfalls in Kombination mit asymmetrischen Verfahren
- Sicheres Bezahlen mit Kreditkarten gemäß EMV-Spezifikation

4.1.3 Vor- und Nachteile

Ein großer Vorteil symmetrischer Verschlüsselungsverfahren ist „die hohe Geschwindigkeit, mit denen Daten ver- und entschlüsselt werden können“ (Esslinger, 2018, S. 7). Aus diesem Grund findet zum Beispiel AES heute noch breite Anwendung. Häufig werden symmetrische Verfahren allerdings mit asymmetrischen Verfahren kombiniert, denn diese lösen ein entscheidendes Problem symmetrischer Verfahren – das Schlüsselmanagement. „Um miteinander vertraulich kommunizieren zu können, müssen Sender und Empfänger vor Beginn der eigentlichen Kommunikation über einen sicheren Kanal einen Schlüssel ausgetauscht haben“ (Esslinger, 2018, S. 7). Können sie dies nicht, gilt die gesamte Kommunikation nicht mehr als sicher, da ein Angreifer den Schlüssel abgreifen und damit die verschlüsselten Informationen entschlüsseln kann. Dieses Problem sollte mit der Erfindung asymmetrischer Verschlüsselungsverfahren gelöst werden.

4.2 Asymmetrische Verschlüsselung

Bei asymmetrischen Verschlüsselungsverfahren (auch *Public-Key-Verschlüsselung* genannt) „hat jeder Teilnehmer ein persönliches Schlüsselpaar, das aus einem *geheimen* und einem *öffentlichen* Schlüssel besteht“ (Esslinger, 2018, S. 14). Für die Verschlüsselung verwendet der Absender stets den öffentlichen Schlüssel des Empfängers, während

dieser zur Entschlüsselung der Nachricht seinen geheimen Schlüssel nutzt (Ertel & Löhmann, 2020).

Im Unterschied zur symmetrischen Verschlüsselung existieren immer nur teilnehmergebundene Schlüsselpaare anstelle eines gemeinsam genutzten geheimen Schlüssels. Dabei müssen die öffentlichen Schlüssel nicht geheim gehalten werden, sondern können problemlos – auch auf einem unsicheren Kanal – ausgetauscht werden (Ertel & Löhmann, 2020). Häufig werden *Public-Key-Infrastrukturen (PKIs)* für die Erzeugung, Authentifizierung, Verteilung und Überprüfung von öffentlichen Schlüsseln verwendet (Ertel & Löhmann, 2020). Asymmetrische Verschlüsselung nutzt häufig teils komplexe mathematische Verfahren wie Primfaktorzerlegung, den diskreten Logarithmus, das wiederholte Quadrieren oder den (erweiterten) euklidischen Algorithmus (Manz, 2019).

4.2.1 Rivest–Shamir–Adleman (RSA)

Das mit Abstand bekannteste asymmetrische Verfahren ist die *RSA*-Chiffre, welche ebenfalls eine Vielzahl solcher mathematischer Berechnungen verwendet. Benannt ist sie nach den drei Entwicklern Ronald Rivest, Adi Shamir und Leonard Adleman, die den Algorithmus im Jahr 1978 veröffentlichten (Esslinger, 2018). Sie entwickelten das Verfahren auf Basis der „Schwierigkeit, große natürliche Zahlen in Faktoren zu zerlegen“ (Manz, 2019, S. VI). Dabei kommen vor allem Primzahlen und Modulo-Rechnung zum Einsatz, durch die eine Nachricht mit einem öffentlichen Schlüssel verschlüsselt und mit dem zugehörigen privaten Schlüssel wieder entschlüsselt werden kann (Manz, 2019).

Die Sicherheit von RSA ist nach derzeitigem Kenntnisstand gewährleistet, wenn man der Richtlinie *BSI TR-02102-1* des Bundesamt für Sicherheit in der Informationstechnik (BSI) folgt und eine Schlüssellänge von mindestens 3000 Bit wählt (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2024). Das hat allerdings zur Folge, dass „die RSA-Chiffre (...) sehr langsam ist, jedenfalls viel mehr Rechenzeit als symmetrische Chiffren benötigt“ (Manz, 2019, S. 61), weshalb in der Praxis „für die eigentliche Informationsübertragung die viel schnellere symmetrische Chiffre“ (Manz, 2019, S. 61) verwendet wird. Nur der zugehörige Schlüssel wird dann mittels RSA übertragen (sog. *Schlüsselaustausch*) (Manz, 2019).

4.2.2 Diffie-Hellman-Schlüsselaustausch

Die Idee der Public-Key-Verfahren wurde schon zwei Jahre vor RSA, im Jahr 1976, von Whitfield Diffie und Martin Hellman publiziert. Sie entwickelten mit dem *Diffie-Hellman-Schlüsselaustausch* ein Verfahren, das die sichere Übertragung eines Geheimschlüssels mittels asymmetrischer Verschlüsselung ermöglicht. Das Verfahren beruht stark auf dem diskreten Logarithmus, der bei Auswahl möglichst hoher Primzahlen das sukzessive Ausprobieren zum Berechnen einzelner Variablen deutlich erschwert (Manz, 2019). Damit der Diffie-Hellman-Schlüsselaustausch als sicher angesehen werden kann,

empfiehlt das BSI, Primzahlen ab einer Länge von 3000 Bit zu wählen (BSI, 2024). Das Diffie-Hellman-Verfahren ist mittlerweile weit verbreitet und ist beispielsweise im Internet ein gängiges Verfahren zum Schlüsselaustausch als Teil des TLS-Protokolls (Manz, 2019).

Angriffe auf den Diffie-Hellman-Schlüsselaustausch sind insbesondere in Form von MITM möglich. Wenn ein Angreifer in den Schlüsselaustausch eingreift und mit den Kommunikationspartnern jeweils eigene Schlüssel vereinbart, kann er jegliche Kommunikation entschlüsseln und verändert weiterleiten (Manz, 2019). Daher ist es ratsam, „dass sich die beiden Kommunikationspartner zuvor eindeutig gegenseitig [...] authentifizieren“ (Manz, 2019, S. 94).

4.2.3 Elliptische Kurven

Obwohl asymmetrische Verschlüsselungsverfahren wie RSA mit einer großen Schlüssellänge aktuell als praktisch sicher gelten, sind sie gerade deshalb in vielen Fällen eher ineffizient. Denn die meisten Chips, beispielsweise auf Smartcards, sind gar nicht in der Lage, „längere Schlüssel als z.B. 2000 Bit zu verarbeiten“ (Esslinger, 2018, S. 246). Eine Ergänzung stellen daher *elliptische Kurven* dar, die schon mit erheblich kürzeren Schlüssellängen als sicher gelten (Esslinger, 2018).

Elliptische Kurven sind mathematisch sehr komplex, lassen sich aber grob gesagt auf viele Public-Key-Chiffren anwenden, die mit dem diskreten Logarithmus arbeiten. So ist der Einsatz von RSA mit elliptischen Kurven bei einem 160 Bit langen Schlüssel „etwa gleich sicher wie RSA ohne elliptische Kurven mit einem 1024 Bit langen Schlüssel“ (Ertel & Löhmann, 2020, S. 94). Bei Kombination mit dem Diffie-Hellman-Schlüsselaustausch (sog. *Elliptic Curve Diffie-Hellman (ECDH)*) empfiehlt das BSI eine Schlüssellänge von mindestens 250 Bit (BSI, 2024).

4.2.4 Vor- und Nachteile

Im Vergleich zu symmetrischen Verfahren bieten asymmetrische Verfahren den klaren Vorteil des einfacheren Schlüsselmanagements. Der zur Verschlüsselung benötigte öffentliche Schlüssel des Empfängers kann einfach – auch über einen unsicheren Kommunikationskanal – übertragen bzw. abgerufen werden. Es ist lediglich auf die Integrität und Authentizität des öffentlichen Schlüssels zu achten. Allerdings sind reine asymmetrische Verschlüsselungsverfahren um ein Vielfaches langsamer als symmetrische Verfahren (Esslinger, 2018).

4.3 Hybride Verfahren

Die Vor- und Nachteile symmetrischer und asymmetrischer Verschlüsselungsverfahren werden durch *hybriden Verfahren* miteinander kombiniert, um einerseits das Schlüsse-

laustauschproblem zu lösen und auf der anderen Seite langsame Algorithmen auszugleichen (Ertel & Löhmann, 2020).

Hybride Verfahren funktionieren wie folgt: „Will Alice eine geheime Nachricht an Bob schicken, so generiert sie (...) zuerst einen zufälligen Sitzungsschlüssel k. Dann verschlüsselt sie mit einem symmetrischen Verfahren die Nachricht M und danach verschlüsselt sie mit Bobs Public-Key den Sitzungsschlüssel k. Beide Chiffretexte schickt sie nun an Bob, der sie nacheinander dechiffriert“ (Ertel & Löhmann, 2020, S. 124).

Populäre Anwendungsfälle hybrider Verfahren sind nach Ertel und Löhmann (2020) und Manz (2019) unter anderem:

- **E-Mail-Versand**: PGP und die Secure Multipurpose Internet Mail Extension (S/MIME) (gemeinsam mit dem *X.509*-Protokoll)
- **Entfernte Rechnerverwaltung**: Secure Shell (SSH)
- **Datenübertragung**: SSL und TLS
- **Kommunikationsnetze**: Virtual Private Networking (VPN) (mittels Internet Protocol Security (IPsec)) und WPA2 (in WLAN-Netzwerken)

5 Digitale Signaturen

Die vorgestellten Verschlüsselungsverfahren adressieren in der bisher vorgetragenem Form den Schutz der Vertraulichkeit im Kontext der CIA-Triade. Potenzielle Angreifer können allerdings nicht nur durch (passives) Abhören der Kommunikation übermittelte Nachrichten abgreifen. Mindestens genauso wichtig ist die Absicherung des (aktiven) Eingreifens in den Kommunikationskanal. Häufig erfolgt dies in Form von MITM-Attacken, bei denen „sich ein Angreifer (...) in eine möglicherweise wechselseitige Kommunikation (...) [einklinkt] und (...) dabei X gegenüber die Rolle von Y und Y gegenüber die Rolle von X“ spielt (Manz, 2019, S. 91). Die Integrität der übermittelten Daten ist dann nicht mehr sichergestellt. Daher wird „bei den meisten heutigen Anwendungen der Kryptologie die Authentizität der Daten gefordert und nicht ihre Geheimhaltung“ (Beutelspacher, 2014, S. 77–78). Um dieses Problem zu beheben, kommen bei der Übertragung von Daten zusätzlich digitale Signaturen zum Einsatz.

5.1 Ziele

Mit digitalen Signaturen sollen sowohl *Benutzerauthentizität* als auch *Nachrichtenintegrität* gewährleistet werden. Damit ist sichergestellt, dass eine Nachricht tatsächlich von einer bestimmten Person stammt, und es kann überprüft werden, ob sie unterwegs verändert wurde (Esslinger, 2018). Dies kommt in der Praxis hauptsächlich beim Übersenden von Dokumenten zum Einsatz.

5.2 Eigenschaften

Folgende Anforderungen werden nach Schneier (2006) an eine gute digitale Signatur gestellt:

1. Sie ist **authentisch**, zeigt also auf, dass der Unterzeichner nach freiem Willen unterschrieben hat.
2. Sie ist **fälschungssicher** und beweist somit, dass nur der Unterzeichner und kein anderer das Dokument unterschrieben hat.
3. Sie ist **nicht wiederverwendbar**, kann also nicht auf ein anderes Dokument kopiert werden.
4. Das unterzeichnete Dokument ist **unveränderbar**, kann also nicht nachträglich geändert werden.
5. Die Unterschrift ist **bindend**, wodurch der Unterzeichner die Signatur im Nachhinein nicht leugnen kann.

Im Gegensatz zu Unterschriften mit Tinte auf Papier erfüllen digitale Signaturen fast alle der Aussagen mit sehr hoher Sicherheit. Allerdings kann „die erste Aussage (...) prinzipiell nicht garantiert werden“ (Ertel & Löhmann, 2020, S. 106).

5.3 Algorithmen

Für digitale Signaturen werden grundsätzlich asymmetrische Verfahren verwendet. Naheliegend ist der Einsatz einer *RSA-Signatur*, denn diese nutzt „exakt dieselben Rechenvorschriften wie die RSA-Chiffre selbst“ (Manz, 2019, S. 95), nur in umgekehrter Reihenfolge (Esslinger, 2018). Ebenfalls bekannt ist die *ElGamal-Signatur*, welche auf dem gleichnamigen *ElGamal-Verschlüsselungsverfahren* basiert und im Jahr 1984 von dem ägyptischen Kryptologen Taher ElGamal publiziert wurde (Manz, 2019).

Es existieren jedoch auch Algorithmen, die ausschließlich für den Zweck der digitalen Signatur entwickelt wurden. Beispielsweise steht der *Digital Signature Algorithm (DSA)*, welcher im Jahr 1991 vom NIST vorgestellt wurde, „in keiner direkten Verbindung zu einem entsprechenden Verschlüsselungsverfahren“ (Esslinger, 2018, S. 241). DSA wird beispielsweise für digitale Signaturen mittels PGP eingesetzt, häufig auch in einer Variante mit elliptischen Kurven (sog. *Elliptic Curve Digital Signature Algorithm (ECDSA)*) (Manz, 2019).

5.4 Funktionsweise

Der Prozess der digitalen Signatur besteht aus dem **Signieren** einer Nachricht (Absender) und dem **Verifizieren** der übermittelten Signatur (Empfänger) (Manz, 2019). Im

Unterschied zur Verschlüsselung werden bei digitalen Signaturen andere Schlüsselpaare verwendet: „Ein Teilnehmer (...) benutzt seinen geheimen Schlüssel, um Signaturen zu erzeugen, und der Empfänger benutzt den öffentlichen Schlüssel des Absenders, um die Richtigkeit der Signatur zu überprüfen“ (Esslinger, 2018, S. 238). Hierbei hängt die digitale Signatur stets vom unterschriebenen Dokument ab. „Die Unterschriften ein und desselben Teilnehmers sind verschieden, sofern die unterzeichneten Dokumente nicht vollkommen übereinstimmen“ (Esslinger, 2018, S. 239). In der Praxis wird aus Performance-Gründen jedoch nicht das gesamte Dokument signiert, da die Signatur sonst ähnlich lang wie das eigentliche Dokument wäre. Stattdessen wendet man vor dem Signieren eine kryptografische Hashfunktion auf das Dokument an und signiert nur deren Output (Esslinger, 2018).

5.5 Hashfunktionen

„Eine *Hashfunktion* bildet eine Nachricht beliebiger Länge auf eine Zeichenfolge mit konstanter Größe, den Hashwert, ab“ (Esslinger, 2018, S. 239). Der Hashwert wird dabei auch als *kryptografischer Fingerabdruck* bezeichnet (Ertel & Löhmann, 2020). Wichtig bei der Generierung des Hashwertes ist die sog. *Berechenbarkeit*, also die effiziente Durchführung der Hashfunktion in angemessener Zeit, unabhängig von der Länge der Nachricht. Spricht man von *kryptografischen Hashfunktionen*, müssen zusätzlich folgende Eigenschaften erfüllt sein (Beutelspacher, 2014; Manz, 2019):

- **Kollisionsresistenz**: Für zwei verschiedene Nachrichten darf nicht der gleiche Hashwert berechnet werden können.
- **Einwegeigenschaft**: Zu einem berechneten Hashwert darf mit vertretbarem Aufwand keine passende Nachricht gefunden werden können. Man spricht dann auch von *Einweg-Hashfunktionen*, also Funktionen, „die sich leicht berechnen lassen, deren Umkehrfunktion (...) jedoch nicht oder nur sehr schwer (...) zu berechnen ist“ (Ertel & Löhmann, 2020, S. 99).

5.5.1 Algorithmen

Die in der Praxis am häufigsten genutzten Algorithmen kryptografischer Hashfunktionen sind die der sog. *Secure Hash Algorithm (SHA)*-Familie:

- **SHA-1**: Mit einer Länge von 160 Bit und einem eigens entwickelten Verschlüsselungsverfahren gilt SHA-1 heute nicht mehr als sicher. „Bis zum Jahr 2004 gab es mehrere erfolgreiche Angriffe gegen SHA-1“ (Manz, 2019, S. 102).
- **SHA-2**: Die zweite Generation mit den Varianten *SHA-2-224*, *SHA-2-256*, *SHA-2-384* und *SHA-2-512* (die angefügte Zahl gibt jeweils die Länge des Hashwertes in Bit an) stellt eine sicherere Alternative zu SHA-1 dar. Das NIST empfiehlt

daher den Übergang zu SHA-2, wobei die kleinste Variante SHA-2-224 nicht unbedingt als sicher anzusehen ist. SHA-2 hat sich damit zum De-facto-Standard entwickelt. Bisher gibt es darauf keine praxisrelevanten Angriffe (Manz, 2019).

- **SHA-3**: 2015 wurden die von Grund auf neu entwickelten Varianten *SHA-3-224*, *SHA-3-256*, *SHA-3-384* und *SHA-3-512* als SHA-3 standardisiert (Manz, 2019).

Eine andere, weit verbreitete kryptografische Hashfunktion ist der *Message-Digest-Algorithm 5 (MD5)*. Er wurde im Jahr 1991 von Ronald Rivest entwickelt. Aufgrund der kurzen Länge des Hashwertes von nur 128 Bit gilt MD5 heute allerdings nicht mehr als sehr sicher (Manz, 2019).

5.5.2 Anwendungsfälle

Hashfunktionen werden vor allem für die **Benutzerauthentifizierung** eingesetzt. Eine häufig genutzte Methode ist hierbei die Authentifizierung mittels Passwort oder Personal Identification Number (PIN). Die Charakteristik der Einweg-Hashfunktionen ermöglicht, dass Passwort oder PIN nicht im Klartext gespeichert werden müssen, was sicherheitstechnisch sehr problematisch wäre. Für zusätzliche Sicherheit wird häufig noch ein sog. *Salting* verwendet. „Bei jeder Passworteingabe werden dann nämlich automatisch einige möglichst sinnlose Zeichen ergänzt, also etwa `&7T?a$`“ (Manz, 2019, S. 123).

Für die **Authentifikation von Nachrichten** werden spezielle Hashfunktionen verwendet, die einen sogenannten *Hash-based Message Authentication Code (HMAC)* generieren. Dieser wird als Prüfsumme an den Nachrichtentext angehängt, der gesamte Text verschlüsselt und versandt. Der Empfänger kann den Text dann entschlüsseln und mittels des angehängten HMAC authentifizieren, indem er den HMAC für den Nachrichtentext erneut generiert und beide Werte miteinander vergleicht (Manz, 2019).

6 Zusammenfassung

Schon im alten Rom wurden Maßnahmen ergriffen, um Bedrohungen gegen das eigene Volk möglichst zu vermeiden, indem Methoden zur sicheren Kommunikation entwickelt wurden. Mit der Zeit wurde die Bedrohungslage immer größer und somit nahm auch die Entwicklung geeigneter Abwehr- und Präventionsmaßnahmen stetig zu. Es hat sich gezeigt, dass mittlerweile in nahezu allen Bereichen des Lebens durch den permanenten Datenfluss Risiken bei der Übermittlung von Daten und Informationen entstehen, die häufig gar nicht gänzlich bekannt sind. Kryptografische Verfahren bieten hierfür einen umfangreichen „Werkzeugkoffer“, um eine mögliche Bedrohungslage abzuwenden oder gar nicht erst entstehen zu lassen. Denn vor allem in der heutigen vernetzten Zeit werden immer mehr schützenswerte Güter zu Angriffszielen erklärt.

So wurden starke Verschlüsselungsverfahren entwickelt, um die **Vertraulichkeit** übermittelter Daten zu gewährleisten. Von klassischen Verfahren wie Transpositions- und Substitutionschiffren bis hin zu modernen Techniken der symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren existieren eine Reihe an nützlichen Technologien, die sich mit der Zeit teils mehr, teils weniger etabliert haben. Populär sind heute vor allem hybride Verfahren, wie zum Beispiel die Kombination von AES für das Schlüsselmanagement und RSA für die Datenübertragung. Häufig erfolgt die Anwendung dieser Verfahren mit elliptischen Kurven und auf Basis des Diffie-Hellman-Schlüsselaustausches.

Auch für die **Integrität** der übermittelten (verschlüsselten) Daten wurden geeignete technische Umsetzungen gefunden. Der Einsatz digitaler Signaturen ermöglicht das Signieren und Verifizieren von Nachrichten mittels asymmetrischer Verfahren. Hierbei kommen zudem verschiedene Hashfunktionen zum Einsatz, die in vielerlei Hinsicht ein großes Hilfsmittel bei der Verarbeitung und Speicherung von Daten sind.

Das dritte Hauptziel der CIA-Triade, die **Verfügbarkeit**, wird eher implizit durch den Einsatz kryptografischer Verfahren gelöst. Man stelle sich vor, ein Angreifer erhält Zugriff auf ein System, weil der Authentifizierungsprozess eines System-Administrators nicht mittels geeigneter Verschlüsselungsverfahren abgesichert ist. Er kann die Authentifizierungsdaten abgreifen und so selbst Zugriff auf das System erhalten, um es dann beispielsweise zu manipulieren. Die Verfügbarkeit des Systems ist dann nicht mehr gewährleistet.

6.1 Herausforderungen

Man kann also zusammenfassend sagen, dass Kryptografie Lösungswege auf der Suche nach sicheren Kommunikationskanälen aufzeigt. Das hat sich schon zu früheren Zeiten bemerkbar gemacht: Die Spartaner konnten einen drohenden Angriff abwehren, weil sie ein kryptografisches Verfahren einsetzten. Und vor allem in der heutigen Zeit gewährleisten sie digitale Sicherheit und Schutz.

Es gibt Verfahren wie das OTP, das als absolut sicher gilt, oder Algorithmen auf Basis der Faktorisierung sehr hoher Primzahlen, die nach aktuellem technischen Stand nicht gebrochen werden können. Dennoch kann nur in den seltensten Fällen eine hundertprozentige Sicherheit beim Einsatz kryptografischer Verfahren gewährleistet werden. Es existieren eine Vielzahl an Herausforderungen und offensichtlicher Sicherheitslücken, unter anderem (nach Ertel und Löhmann (2020)):

- Programmier- und Softwarefehler
- Unsichere Schlüsselaufbewahrung
- Wahl schlechter Zufallszahlen in den Algorithmen

- Unzureichende Passwortstärke
- Angriffe aufgrund von Seiteneffekten, beispielsweise bei Chipkarten
- Trojanische Pferde
- Gefälschte öffentliche Schlüssel

All diese und weitere Herausforderungen gilt es, bei der stetigen Weiterentwicklung von IT-Systemen und den dort eingesetzten kryptografischen Verfahren im Blick zu behalten.

6.2 Ausblick

Damit Kryptografie weiterhin ein wirksames Mittel für Vertraulichkeit, Integrität und Verfügbarkeit darstellt, wird permanent an der Weiterentwicklung bestehender und Entwicklung neuer Verfahren gearbeitet. So gilt beispielsweise RSA mit entsprechender Konfiguration derzeit als sicher, aber „brillante mathematische Ideen könnten jederzeit dazu führen, dass das Lösen des Faktorisierungsproblems leicht und RSA damit generell unbrauchbar wird“ (Esslinger, 2018, S. 436). Daher werden mittlerweile Quantencomputer – „ein neuer Computertyp, der die Gesetze der Quantenmechanik ausnutzt“ (Esslinger, 2018, S. 436) – eingesetzt, mit denen vor allem die Berechnung des diskreten Logarithmus in angemessener Zeit durchführbar werden soll. Dadurch würden viele kryptografische Verfahren nicht mehr als sicher gelten (Esslinger, 2018). Manch einer wagt die These und sagt: „Sorgfältig konzipierte und implementierte kryptographische Verfahren haben eine Lebensdauer von 5 bis 20 Jahren“ (Esslinger, 2018, S. 436).

Neue mathematische Problemstellungen werden momentan erforscht, beispielsweise die Verschlüsselung auf Basis des *Dekodierproblems* (auch *codebasierte Verschlüsselung* genannt). Dabei werden bei der Verschlüsselung gezielt Fehler addiert, die bei der Entschlüsselung mittels einer geeigneter Methode wieder entfernt werden, wobei eben diese Methode als Geheimschlüssel anzusehen ist (Esslinger, 2018).

Außerdem werden neue Signaturverfahren erarbeitet, wie beispielsweise die von Ralph Merkle vorgeschlagene Konstruktion der *Einmal-Signaturen*. Diese charakterisiert sich dadurch, dass für jede Signatur ein neuer Signier- und Verifikationsschlüssel benötigt wird, wobei letzterer mithilfe eines Hash-Baums auf die Gültigkeit eines einzelnen Schlüssels zurückzuführen sein soll (Esslinger, 2018).

Insgesamt steckt sehr viel Potenzial in der Weiterentwicklung kryptografischer Verfahren. Mit zunehmendem technischem Fortschritt können sicherlich noch viele Verfahren gefunden werden, die auch in Zukunft digitale Sicherheit gewährleisten – sei es durch verschlüsselte Kommunikation oder durch womöglich völlig neu entwickelte Methoden.

Literaturverzeichnis

Beutelspacher, A. (2014). *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen* (10. Aufl.). Springer Fachmedien.

Bundesamt für Sicherheit in der Informationstechnik. (2024). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* (Technische Richtlinie Nr. BSI TR-02102-1) (Version 2024-01). Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

Ertel, W., & Löhmann, E. (2020). *Angewandte Kryptographie* (6. Aufl.). Carl Hanser.

Esslinger, B. (Hrsg.). (2018). *Das CrypTool-Buch: Kryptographie lernen und anwenden mit CrypTool und SageMath* (12. Aufl.). CrypTool-Projekt.

Hansen, H. R., Mendling, J., & Neumann, G. (2015). *Wirtschaftsinformatik* (11. Aufl.). Walter de Gruyter GmbH.

Landwehr, D. (2015). *Mythos Enigma: Die Chiffriermaschine als Sammler- und Medienobjekt* (1. Aufl.). transcript Verlag.

Manz, O. (2019). *Verschlüsseln, Signieren, Angreifen: Eine kompakte Einführung in die Kryptografie*. Springer Spektrum.

Schneier, B. (2006). *Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C* [Aus dem Englischen übersetzt]. Pearson Studium.

Singh, S. (2001). *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. dtv.

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Studienarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der Übersicht verwendeter (gen)KI-Tools habe ich sämtliche eingesetzte (gen)KI-Tools, deren Einsatzform sowie die jeweils betroffenen Teile der Arbeit einzeln aufgeführt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Übersicht verwendeter (gen)KI-Tools

Die (gen)KI-Tools habe ich, wie im Folgenden dargestellt, eingesetzt.

(gen)KI-Tool	**Einsatzform**	**Betroffene Teile der Arbeit**
ChatGPT	Generierung von ersten Ideen für eine geeignete Gliederung	Gesamte Arbeit

Münster, 9. August 2024

Elias Häußler