JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schmoranz, Paul W.; Schick, Lukas; Schwickert, Axel

# Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 2 / 2020
ISSN 1613-6667

# Arbeitspapiere WI Nr. 2 / 2020

**Autoren:** Schmoranz, Paul W.; Schick, Lukas; Schwickert, Axel

**Titel:** Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete

**Zitation:** Schmoranz, Paul W.; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, in: Arbeitspapiere WI, Nr. 2/2020, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2020, 66 Seiten, ISSN 1613-6667.

**Kurzfassung:** In dem Arbeitspapier WI „Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete“ (Nr. 02/2020) wird erläutert, was unter Hybrider Verschlüsselung zu verstehen ist und wie diese grundsätzlich funktioniert. Dabei wird zwischen symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren unterschieden und aufgezeigt, welche Vor- und Nachteile die unterschiedlichen Verschlüsselungsverfahren bieten. Des Weiteren wird dargestellt, was der Unterschied zwischen privaten und öffentlichen Schlüsseln ist. Basierend auf den Verfahren hybrider Verschlüsselung werden Anwendungsgebiete dieser näher betrachtet, um deren Verständlichkeit und Anwendungsorientierung zu verdeutlichen. Im vorliegenden Arbeitspapier 02/2020 wird gezeigt, wie eine hybride Verschlüsselung im Web funktioniert und wie sie in alltäglichen Situationen wie Web Shops und Bezahlvorgängen zu Stande kommt.

**Schlüsselwörter:** Verschlüsselung, Web, Signatur, Schlüssel, Schlüsselpaar, öffentlich, privat, symmetrisch, asymmetrisch, hybrid, Public-Key-Infrastruktur, RSA, Diffie-Hellman, TLS, Cipher Suites, Web Sites, Electronic Mail, Web Shops

# Inhaltsverzeichnis

Seite

# Abbildungsverzeichnis

Seite

# Tabellenverzeichnis

Seite

# Abkürzungsverzeichnis

AES ..... Advanced Encryption Standard
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
CA ..... Certification Authorities
CTR ..... Counter-Modus
DES ..... Data Encryption Standard
DHE ..... Diffie-Hellman Ephemeral
DNS ..... Domain Name System
ECDHE ..... Elliptic-Curve Diffie-Hellman Ephemeral
GCM ..... Galois/Counter Mode
HTML ..... Hypertext Markup Language
HTTP ..... Hypertext Transfer Protocol
HTTPS ..... Hypertext Transfer Protocol Secure
IETF ..... Internet Engineering Task Force
IMAP ..... Internet Message Access Protocol
IMTPS ..... Internet Message Access Protocol Secure
MAC ..... Message Authentication Code
MITM ..... Man-in-the-Middle
MS ..... Master Secret
NIST ..... National Institute of Standards and Technology
NSA ..... National Security Agency
OSI ..... Open-Systems-Interconnection-Model
PFS ..... Perfect Forward Secrecy
PGP ..... Pretty Good Privacy
PKI ..... Public-Key-Infrastruktur
PMS ..... Pre-Master Secret
PRNG ..... Pseudorandom Number Generator
RSA ..... Verfahren nach Rivest, Shamir und Adleman
S/MIME ..... Secure/Multipurpose Internet Mail Extensions
SHA ..... Secure Hash Algorithm
SMTP ..... Simple Mail Transport Protocol
SMTPS ..... Simple Mail Transport Protocol Secure
SSL ..... Secure Socket Layer
TCP/IP ..... Transmission Control Protocol/Internet Protocol
TLS ..... Transport Layer Security
UDP ..... User Datagram Protocol
VPN ..... Virtual Private Network
XOR ..... Exklusiv-Oder-Gatter (eXclusive OR gate)

# 1 Problemstellung, Ziel und Aufbau

Das Internet hat unseren analogen Briefkasten längst durch digitale Posteingänge in E-Mail-Programmen und Server-basierten Kommunikationsplattformen ersetzt. In diesen Posteingängen landen unweigerlich sensible Informationen, wovon jedoch die wenigsten in einem digitalen Briefumschlag verschlossen sind. Spätestens seit den Enthüllungen von Edward Snowden ist deutlich geworden, wie gefährlich und allumfassend eine unverschlüsselte Kommunikation im Zeitalter der Digitalisierung sein kann. Jüngste Ereignisse zum Jahreswechsel 2018/2019 aus dem Deutschen Bundestag zeigen jedoch, dass selbst hochrangige Politiker ihre Kommunikation immer noch nicht gründlich verschlüsseln und darüber hinaus grob fahrlässig mit der Verwaltung ihrer Passwörter umgehen. Selbiges trifft auch auf Organisationen aus Wirtschaft und Verwaltung zu.[1]

Unternehmen, Ministerien und andere Organisationen versenden über das Internet Nachrichten und Dokumente, die verschwiegenheitspflichtige Informationen beinhalten. Beispielhaft können an dieser Stelle Geschäfts- und Bankgeheimnisse oder Steuerdokumente und Patientendaten genannt werden. Diese sensiblen Informationen dürfen nur von bestimmten Empfängerkreisen eingesehen werden, ohne dass dabei das Interesse von Außenstehenden geweckt wird oder einer unbefugten Person Einblicke in die geheimen Informationen gewährt werden. Aus diesem Grund sichern kryptografische Verfahren die Privatsphäre und informationelle Selbstbestimmung im Internet. Kryptografie gewährleistet die Vertraulichkeit von Informationen und stellt zusätzlich die Integrität, Authentizität und Verbindlichkeit bei der Internet-basierten Kommunikation von Organisationen und Privatpersonen im Web sicher.[2]

Der technologische Fortschritt von intelligent vernetzten und autonomen IT-Systemen lässt erahnen, welche Relevanz die kryptografischen Verfahren für die Gesellschaft und die Systementwicklung zukünftig haben werden. In unterschiedlichsten Domänen fehlt jedoch immer noch Grundlagenwissen über die verschlüsselte Kommunikation im Web und somit auch die Wertschätzung für kryptografische Verfahren.[3]

1 Vgl. Vgl. Greis, Friedhelm; Ernst, Nico; Thoma, Jörg: Chronologie der Enthüllungen von Edward Snowden, Online im Internet: https://www.golem.de/news/nsa-chronologie-der-enthuellungen-von-edward-snowden-1307-100411.html, 16.07.2013, vgl. Krempl, Stefan: Gehackte Daten: Politiker beklagen schweren Angriff auf die Demokratie, Online im Internet: https://heise.de/-4265847, 04.01.2019 und vgl. Holland, Martin: Facebook: Hunderte Millionen Passwörter im Klartext gespeichert, Online im Internet: https://heise.de/-4342184, 21.03.2019.

2 Vgl. Wewer, Göttrik: Auf dem Weg zum gläsernen Staat Privatsphäre und Geheimnis im digitalen Zeitalter, in: der moderne staat – Zeitschrift für Public Policy, Recht und Management, 2/2012, S. 249 und vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Wiesbaden: Springer Vieweg 2017, S. 10f.

3 Vgl. Schäfer, Günter; Roßberg, Michael: Netzsicherheit – Grundlagen & Protokolle, 2. aktualisierte und erweiterte Auflage, Heidelberg: dpunkt Verlag 2014, S. 7f, 443f.

Das Ziel der vorliegenden Arbeit ist es daher, eine Einführung in die Grundlagen, Verfahren und Anwendungsgebiete der Kryptografie im Web zu geben. Die Bestandteile der hybriden Verschlüsselung sollen durch Abbildungen und Anwendungsbeispiele verdeutlicht werden, um den Mechanismus der verschlüsselten Kommunikation im Web zu veranschaulichen. Dabei werden unter anderem die Netzwerkprotokolle thematisiert, welche den Versand einer E-Mail und den Aufbau einer Web Site ermöglichen.

**Kapitel 2:** Grundlagen der hybriden Verschlüsselung

Das zweite Kapitel befasst sich zunächst mit den relevanten Grundbegriffen der Kryptografie. In diesem Kapitel wird der Ursprung der klassischen Kryptografie gezeigt und die Entwicklung bis zur modernen Kryptografie erläutert. Wichtig ist hier die Begriffsabgrenzung der kryptografischen Verfahren. Die kryptografischen Verfahren beinhalten verschiedene Verschlüsselungsverfahren, Hashfunktionen und digitale Signaturen. Diese Verfahren sichern die Schutzziele der Informationssicherheit. Auch die Netzwerkprotokolle im Web werden thematisiert und werden entlang des TCP/IP-Referenzmodells eingeordnet. Die fiktiven Personen Alice und Bob werden beispielhaft dabei helfen, die Kommunikation im Web zu verdeutlichen.

**Kapitel 3:** Verfahren der der hybriden Verschlüsselung

Das dritte Kapitel erläutert die kryptografischen Verfahren des Grundlagenkapitels. Anhand von Alice und Bob werden die Funktionsprinzipien der kryptografischen Verfahren deutlich. Es wird zwischen den symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren unterschieden. Jeder Abschnitt beschreibt zusätzlich den Schlüsselaustausch, den Schlüsseltransport und die vergängliche Schlüsselvereinbarung.

**Kapitel 4:** Anwendungsgebiete der hybriden Verschlüsselung

Das vierte Kapitel behandelt die Anwendungsgebiete und die alltäglichen Berührungspunkte mit hybrider Verschlüsselung im Web. Das Transport-Layer-Security-Protokoll kombiniert in diesem Zusammenhang sämtliche kryptografische Verfahren. Im weiteren Verlauf wird der Umgang mit hybrider Verschlüsselung am Beispiel eines verschlüsselten Web Shops und dem Versand einer Server- und Client-basierten verschlüsselten E-Mail aufgezeigt.

# 2 Grundlagen der hybriden Verschlüsselung

## 2.1 Systematisierung der Grundlagen

Die Verschlüsselung von Daten und die sichere Kommunikation im Internet stellen ein weitreichendes Teilgebiet der Informatik dar. Dieses Kapitel befasst sich mit dem Ursprung und den Grundbegriffen der Kryptologie. Die Kryptologie lässt sich allgemein in die beiden Teilgebiete der Kryptografie und Kryptoanalyse unterteilen. Die Kryptografie ist die Wissenschaft der Verschlüsselung von Informationen und beschäftigt sich mit der Methodik, Nachrichten, Dokumente und andere digitale Daten durch Verschlüsselung zu schützen. Die Kryptoanalyse prüft die kryptografischen Verfahren auf mögliche Schwachstellen und somit den Aufwand, um die Verschlüsselung zu brechen.[4]

**Kapitel 2.2:** Klassische Kryptografie

Das zweite Grundlagenkapitel zeigt die frühen Formen der klassischen Kryptografie. Schon vor mehreren tausend Jahren wurden analoge Informationen verschlüsselt. Im antiken Griechenland wurden militärische Botschaften unleserlich gemacht, um den Inhalt der Nachricht geheim zu halten und vor Feinden zu schützen. Dies gelang ihnen zum Beispiel durch die sogenannte „Skytale“. Mit zwei weiteren Beispielen, der „Caesar-Chiffre“ des Römischen Reichs und der „Vigenère-Chiffre“ aus der Renaissance, werden die Ursprünge der Kryptografie deutlich. Mit dem Vertauschen von Klartextinformationen mithilfe von einem und mehreren Geheimalphabeten wird die mono- und polyalphabetische Substitution veranschaulicht. Das Kerckhoffs’sche Prinzip verdeutlicht anschließend die Anfälligkeit der klassischen Kryptografie und die Bedeutung der Kryptoanalyse.

**Kapitel 2.3:** Moderne Kryptografie

Das dritte Grundlagenkapitel beschreibt die zentralen Themengebiete der modernen Kryptografie. Hier werden die sogenannten „schweren Berechnungsprobleme“ der Verschlüsselungsalgorithmen thematisiert und anschließend auf die Schlüssel- und Bitlängen eingegangen. Des Weiteren werden die Grundlagen von vier kryptografischen Verfahren vorgestellt: Die symmetrischen Verschlüsselungsverfahren, die asymmetrischen Verschlüsselungsverfahren, Hashfunktionen bzw. Nachrichtenauthentifizierungscodes und digitale Signaturen. Ein Grundlagenwissen über moderne Verschlüsselungsverfahren ist hilfreich, um die Anwendungsgebiete von hybrider Verschlüsselung im Web in den weiteren Kapiteln der Arbeit einordnen zu können.

4 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., Wiesbaden: Springer Spektrum 2015, S. 1f.

**Kapitel 2.4:** Informationssicherheit durch kryptografische Verfahren

Das vierte Grundlagenkapitel verdeutlicht, wie wichtig die richtige Wahl und die einwandfreie Implementierung von kryptografischen Verfahren für die Sicherheit von IT-Systemen ist. Die Prüfung und stetige Weiterentwicklung der Algorithmen und Verfahren ist essentiell, um die Schutzziele der Informationssicherheit – die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit – langfristig gewährleisten zu können. Diese Schutzziele werden durch kryptografische Verfahren erreicht, welche im vorherigen Grundlagenkapitel bereits einleitend erläutert werden.

**Kapitel 2.5:** Netzwerkprotokolle und die Kommunikation im Web

Das fünfte Grundlagenkapitel zeigt, dass die Kommunikation im Internet durch Netzwerkprotokolle zwar systematisiert stattfindet, jedoch nicht automatisch abgesichert ist. Durch das TCP/IP-Referenzmodell werden die verwendeten Netzwerkprotokolle entlang der Architekturschichten des Internets abgebildet und mit der Thematik dieser Arbeit in Bezug gebracht. Die hybride Verschlüsselung wird in unterschiedliche Netzwerkprotokolle des Internets implementiert.

## 2.2 Klassische Kryptografie

Die Kryptografie befasst sich mit der Verschlüsselung und Entschlüsselung von Informationen und somit auch mit der Sicherheit von Nachrichten. Die Herausforderung besteht seit jeher darin, eine Information in Klartext so zu verändern, dass niemand außer dem berechtigten Empfänger den verschlüsselten Geheimtext entziffern kann. Eine einzelne Geheimtextziffer oder der gesamte Geheimtext wird auch als „Chiffre“ bezeichnet. Damit der Empfänger eines Geheimtextes die ursprüngliche Klartextinformation wieder lesbar machen kann, benötigt er eine exklusive Information des Senders – den geheimen Schlüssel. Die Ursprünge der Kryptografie werden durch die nachfolgenden historischen Beispiele deutlich.[5]

Die Spartaner nutzten im antiken Griechenland einen schmalen Leder- oder Pergamentstreifen und einen Zylinder, genannt „Skytale“, um militärische Botschaften geheim zu übertragen. Um die geheime Botschaft zu erstellen, wurde der Streifen zunächst spiralförmig um die Skytale gewickelt. Die Nachricht wurde danach zeilenweise auf den Streifen geschrieben. Abbildung 1 zeigt eine Skytale der Spartaner:[6]

5 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, Berlin Heidelberg: Springer Vieweg 2016, S. 4.

6 Abbildung von Hebisch, Udo: Skytale-Abbildung, Online im Internet: http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/skytale.html, 07.04.2010.

Abb. 1: Skytale der Spartaner

Der abgewickelte Streifen bzw. die darauf untereinander aufgereihten Buchstaben standen anschließend in keinem erkennbaren Zusammenhang mehr. Die Buchstaben waren demnach ohne passende Skytale – um den Steifen wieder um die Zylinder zu wickeln – nicht mehr ohne weiteres lesbar. Der geheime Schlüssel war also der vorab vereinbarte Durchmesser der Skytale, mit deren Hilfe die Nachricht ursprünglich verfasst wurde. Nur mit dem passenden Zylinder konnte der Empfänger die Zeilen der Botschaft in die richtige Stellung verschieben, um die Nachricht entschlüsseln zu können. Die zugrundeliegende Verschlüsselungsmethode der Skytale wird Transposition genannt. Noch heute werden bei der Verschlüsselung Informationen nach bestimmten Mustern transponiert bzw. zerteilt und durch verstreute Buchstaben unleserlich gemacht.[7]

Eine weitere Methode zur Verschlüsselung ist die sogenannte Substitution. Die Ziffer eines Klartextes wird dabei durch eine andere Ziffer eines Schlüsselalphabets ersetzt. Ein prominentes Beispiel mit historischem Bezug ist die sogenannte „Caesar-Chiffre“. Der römische Feldherr hat auf diese Weise Geheimbotschaften an seine Offiziere versandt. Im Gegensatz zur Skytale verwendet die Caesar-Chiffre zur Verschlüsselung keinen physischen Gegenstand. Stattdessen wird jedem Buchstaben eines Klartextes ein anderer eindeutiger Buchstabe systematisch zugeordnet. Caesar soll dafür das Alphabet konstant um drei Stellen verschoben haben. A wird durch D ersetzt, B durch E, und so weiter. Gegen Ende wird der Buchstabe X wieder durch A ersetzt (siehe Abbildung 2):[8]

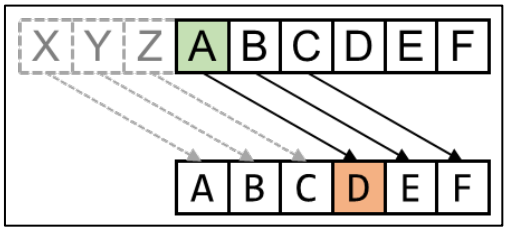



Abb. 2: Die Caesar-Chiffre

7 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O, S. 3f.

8 Vgl. Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: Kryptographie und IT-Sicherheit – Grundlagen und Anwendungen, Wiesbaden: Vieweg und Teubner Verlag 2008, S. 5f.

Durch die konstante Rechtsverschiebung des Alphabets um drei Stellen entsteht ein neues Geheimalphabet. Durch dieses Geheimalphabet wird zum Beispiel der Klartext „ATTACKE“ in den Geheimtext „DWWDFNH“ verschlüsselt (siehe Abbildung 3):[9]

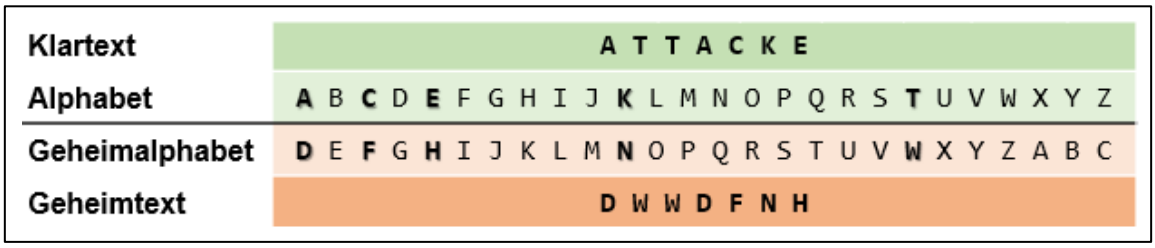



Abb. 3: Das Geheimalphabet der Caesar-Chiffre

Diese Substitutions-Chiffre erfüllte zu Zeiten Caesars ihren Dienst. Damals waren allerdings die meisten Menschen Analphabeten. Heute wäre eine solche Verschlüsselung ohne größeren Aufwand zu brechen. Die Buchstaben eines Alphabets werden in der Regel unterschiedlich häufig verwendet und sind somit ungleich verteilt. In der deutschen Sprache sowie im Lateinischen werden die Buchstaben A und E beispielsweise besonders oft benutzt. Mithilfe einer Häufigkeitsanalyse würde man auf wiederholende Buchstabenfolgen im Geheimtext achten und zunächst mit den am häufigsten verwendeten Buchstaben der Klartextsprache als möglicher Schlüssel arbeiten. Das Testen verschiedener Buchstaben bzw. sämtlicher Schlüsselwerte würde irgendwann ein Muster und schließlich einen sinnvollen Klartext liefern. Dies liegt unter anderem an der Tatsache, dass mit der Caesar-Chiffre nur ein einziges Geheimalphabet – mit 26 Buchstaben und 25 Möglichkeiten der Buchstabenverschiebung – verwendet wird. Man spricht daher von einer monoalphabetischen Substitution. Ist das Prinzip der Caesar-Chiffre einmal durchschaut, würde der geheime Schlüssel schnell offen liegen und die Kommunikation zwischen Caesar und seinen Gefolgsleuten wäre nicht mehr geheim.[10]

Erst im 16. Jahrhundert wurde mit der Vigenère-Verschlüsselung eine polyalphabetische Substitution zur Verschlüsselung von Nachrichten verwendet. Der französische Diplomat Blaise de Vigenère verwendete im Vergleich zur Caesar-Chiffre mehrere Geheimalphabete gleichzeitig und nutzte einen verbesserten geheimen Schlüssel. Statt einer einstelligen Schlüsselziffer wird bei der polyalphabetischen Verschlüsselung ein längeres Schlüsselwort benutzt. Das Schlüsselwort wird dem Klartext über die gesamte Länge des Textes fortlaufend zugeordnet und wiederholt.[11]

9 Eigene Abbildung in Anlehnung an Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., a. a. O., S. 34.

10 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 43f.

11 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., a. a. O., S. 33f.

Wie in der nachfolgenden Abbildung 4 zu sehen ist, wird das Schlüsselwort „HALLO“ fortlaufend unter die Klartextbuchstaben des zu verschlüsselnden Wortes „kryptografie“ geschrieben. Der Geheimtext der Vigenère-Chiffre entsteht durch die Verwendung einer Buchstabenmatrix, dem sogenannten „Vigenère-Quadrat“:[12]

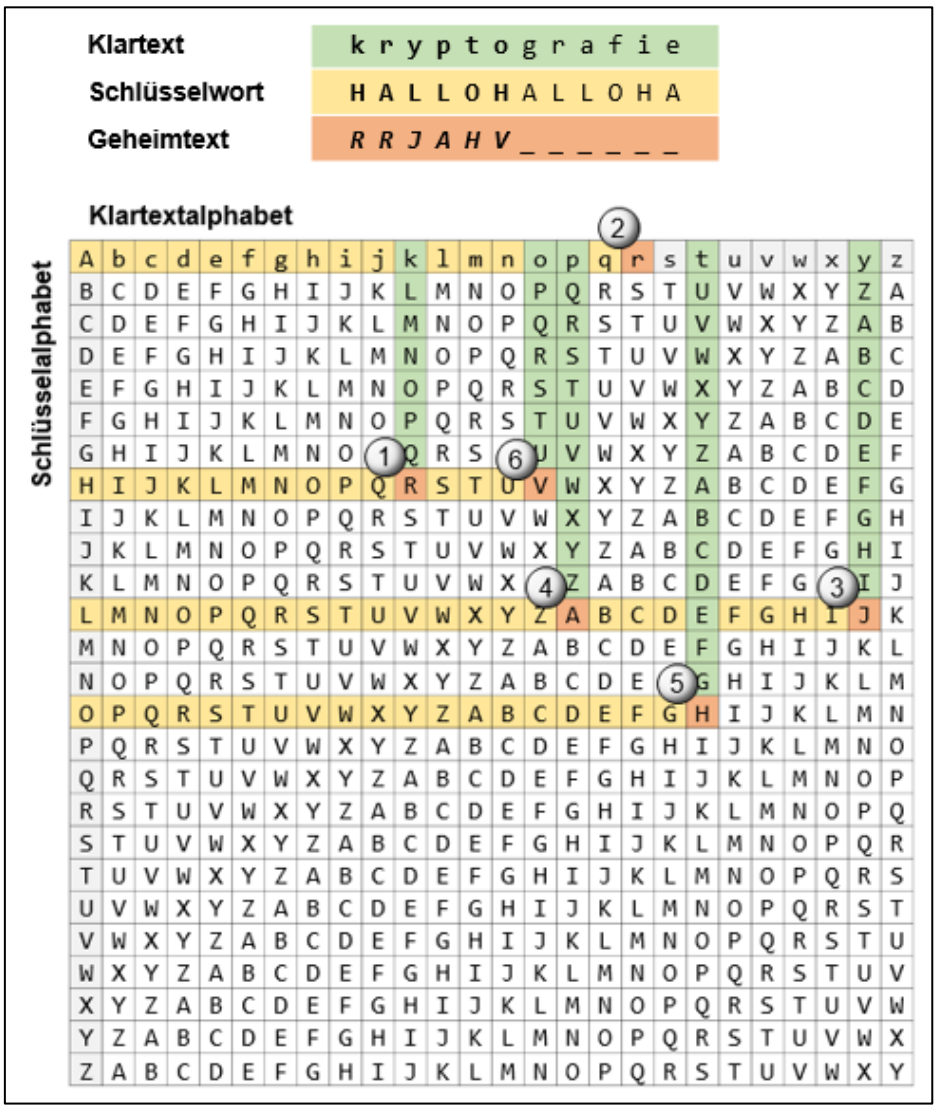



Abb. 4: Die Vigenère-Chiffre und das Vigenère-Quadrat

**Schritt 1:** Unter dem ersten Buchstaben **k** des Klartextes steht ein **H**, also wird das **k** nach dem Geheimalphabet verschlüsselt, welches mit einem **H** beginnt. Innerhalb des Vigenère-Quadrats steht in der **k**-Spalte des Klartextalphabets und in der **H**-Zeile des Schlüsselwortalphabets der Buchstabe ***R***. Der erste Buchstabe ist somit gefunden.

**Schritt 2:** Der zweite Buchstabe des Klartextes ist ein **r**, darunter steht ein **A**. Im Vigenère-Quadrat steht in der **r**-Spalte und der **A**-Zeile rein zufällig wieder ein ***R***.

12 Eigene Abbildung in Anlehnung an Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., a. a. O., S. 35.

Für die Klartextbuchstaben „kryptografie“ erhält man so den Geheimtext „*RRJAHVGCLTPE*“. Ein Vorteil der polyalphabetischen Vigenère-Chiffre gegenüber der monoalphabetischen Caesar-Chiffre liegt darin, dass gleiche Klartextbuchstaben in verschiedene Geheimbuchstaben verschlüsselt werden können. Auch umgekehrt werden verschiedene Klartextbuchstaben in gleiche Geheimbuchstaben verschlüsselt:

- Die beiden gleichen Klartextbuchstaben **r** des Wortes „k**r**yptog**r**afie“ werden sowohl erneut durch ***R*** als auch durch ***C*** substituiert (*R**R**JAHVG**C**LTPE).*
- Die beiden Klartextbuchstaben **k** und **r** des Wortes „**kr**yptografie“ werden in die gleichen Geheimbuchstaben ***R*** substituiert (***RR****JAHVGCLTPE).*

An dem Beispiel der Vigenère-Chiffre wird deutlich, dass durch ein längeres Schlüsselwort und ein komplexeres Vorgehen die Verschlüsselung willkürlicher und somit sicherer wird. Der Ansatz der polyalphabetischen Verschlüsselung ist somit ein Prototyp moderner Verschlüsselung. Noch heute wird durch die sogenannten Methoden der „Konfusion“ und „Diffusion“ der Sinnzusammenhang zwischen Klartext, Schlüssel und Geheimtext verzerrt. Ist die zugrundeliegende Systematik des Vigenère-Quadrats jedoch einmal durchschaut, kann durch eine erweiterte Häufigkeitsanalyse auch ohne Kenntnis des geheimen Schlüsselworts auf den Klartext geschlussfolgert werden. Ein Grund dafür ist, dass das Verschlüsselungsverfahren der Vigenère-Verschlüsselung mathematisch nicht komplex genug ist.[13] Außerdem wurden in der Vergangenheit nicht nur die geheimen Schlüssel, sondern auch die gesamte Methodik und der Mechanismus eines Verschlüsselungsverfahrens geheim gehalten und somit der Öffentlichkeit vorenthalten.[14]

Ein prominentes Beispiel für das Versagen eines kryptografischen Systems durch die Geheimhaltung des Verschlüsselungsverfahrens ist Enigma. Enigma war ein mechanisches Verschlüsselungsverfahren und wurde während des Zweiten Weltkriegs von der Deutschen Wehrmacht zur Kommunikation benutzt. Mit mehreren rotierenden Buchstabenwalzen basiert Enigma ebenfalls auf einem Prinzip der polyalphabetischen Substitution und ihre Verschlüsselung galt lange Zeit als unbezwingbar. Allerdings gelang es den Alliierten, das gesamte kryptografische System der Maschine zu entschlüsseln und für ihre Zwecke zu nutzen. Bereits 1927 machten drei polnische Kryptografen dafür den Anfang. Sie besorgten sich ein zu der Zeit noch käuflich zu erwerbendes Exemplar einer ähnlich funktionierenden Verschlüsselungsmaschine. Über die Jahre hinweg konnten sie gemeinsam mit dem Briten Alan Turing die Enigma-Verschlüsselung vollständig rekonstruieren. In dem Dechiffrier-Zentrum von Blechely Park fing Turing in der

13 Vg. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., a. a. O., S. 35f.

14 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O., S. 34 und Buchmann, Johannes: Einführung in die Kryptographie, 6. Aufl., Berlin Heidelberg: Springer Spektrum 2016, S. 112.

Folge gemeinsam mit fast 10.000 Mitarbeitern täglich Botschaften der Wehrmacht ab und entschlüsselte sie. Die Verschlüsselung war nur durch die Geheimhaltung des gesamten kryptografischen Verfahrens möglich (security by obscurity).[15]

Der niederländische Kryptologe und Sprachwissenschaftler Auguste Kerckhoffs beschrieb bereits 1883 die Problematik von Enigma: Ein kryptografisches Verfahren muss auch dann noch sicher sein, wenn ein Angreifer alle Methoden der Verschlüsselung kennt, mit Ausnahme des geheimen Schlüssels. Die Sicherheit einer Verschlüsselung sollte daher ausschließlich auf der Geheimhaltung des Schlüssels sowie einem robusten Design des Verfahrens beruhen (security by design). Bekannt als das Kerckhoffs'sche Prinzip, gilt diese Aussage seither als Grundsatz der modernen Kryptografie.[16]

Das nachfolgende Kapitel thematisiert die Weiterentwicklung der oben vorgestellten historischen Beispiele der Verschlüsselung. Dabei werden verschiedene Begriffe aus der modernen Kryptografie erläutert, welche im Rahmen dieser Arbeit benötigt werden.

## 2.3 Moderne Kryptografie

### 2.3.1 Algorithmen und Berechnungsprobleme

Die Beispiele der klassischen Kryptografie zeigen, dass überwiegend Nachrichten mit militärischer Bedeutung verschlüsselt wurden. Aus diesem Grund entwickelte sich die Wissenschaft der Kryptografie auch in der Zeit des Kalten Krieges und vor allem seit den 1970er Jahren rasant weiter. Der Einsatz von Computern und deren enorme Rechenleistung schafft heutzutage gänzlich neue Möglichkeiten zur Verschlüsselung und Entschlüsselung von Informationen. Der Ausbau von Kommunikationsnetzwerken wie das Internet bietet viele neue Anwendungsgebiete. Die moderne Kryptografie beschäftigt sich daher mit der Verschlüsselung und Entschlüsselung von digitalen Informationen.[17]

Die Verschlüsselung von digitalen Informationen gelingt durch das Ineinandergreifen unterschiedlicher mathematischer Berechnungen. Die formalisierte Beschreibung dieser Berechnungen werden Algorithmen genannt. Algorithmen sollten möglichst effizient Berechnungsprobleme lösen können. Diese Effizienz im Zusammenhang mit kryptografischen Verfahren bedeutet, dass Algorithmen in kurzer Zeit Klartextinformationen in Geheimtextinformationen verschlüsseln und in umgekehrter Reihenfolge wieder entschlüsseln. Bei der Verschlüsselung ei-

15 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 66f.

16 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O., S. 19f und Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 12f.

17 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 12f.

ner Information wird ein kryptografischer Schlüssel in das Berechnungsproblem des Algorithmus mit eingebunden. Das mathematische Problem ist in der Folge nur noch dann zu lösen, wenn der richtige Schlüsselwert für den verwendeten Algorithmus bekannt ist.[18]

Mit der Rechenleistung von modernen Computern können große Datenmengen mit sehr hoher Geschwindigkeit digital verarbeitet werden. Computer können in der Praxis auch mit „roher Gewalt“ nach dem richtigen Schlüsselwert einer Verschlüsselung suchen und den geheimen Schlüssel somit zufällig erraten. Eine solche Trial-and-Error-Methode zur vollständigen Schlüsselsuche nennt man auch einen „Brute-Force-Angriff“. Die Chiffren der klassischen Kryptografie wären bei einem solchen computergestützten Angriff absolut wirkungslos, weil die Berechnungsprobleme für heutige Verhältnisse bei weitem nicht schwer bzw. komplex genug sind.[19]

### 2.3.2 Schlüssel- und Bitlängen

Aus technischer Sicht ist ein Schlüssel eine eigenständige Datei, bestehend aus einer langen Zeichenabfolge in Binärcode. Man spricht auch von der Bitlänge eines kryptografischen Schlüssels. Ein Schlüssel basiert auf einer speziellen mathematischen Funktion, die einen Klartext in Abhängigkeit eines Schlüssels (digitaler Code) in einen Geheimtext umwandelt. Die Dezimalzahl der 25 Schlüsselvarianten der Caesar-Chiffre entsprechen gerade einmal 5 Bit (25 als Binärzahl = 11001). Fortschrittlichere Verschlüsselungsstandards verschlüsseln hingegen mit 256 Bit und mehr. Ein 256-Bit-Schlüssel entspricht einer Zahl mit 78 Stellen statt den zwei Stellen der Caesar-Chiffre und besitzt 115.792.089.237.316.195.423.570.985.008.687.907.853 .269.984.665.640.564.039.457.584.007.913.129.639.936-Schlüsselvarianten statt den 25-Schlüsselvarianten der Caesar-Chiffre. Diese sehr langen Bitfolgen erhöhen den Rechenaufwand, um das Berechnungsproblem der vollständigen Schlüsselsuche eines Verschlüsselungsverfahrens zu lösen, ins Unermessliche. Längere Bitfolgen garantieren jedoch nicht zwangsläufig mehr IT-Sicherheit. Moderne Verschlüsselungsverfahren basieren deswegen zusätzlich auf rechenintensiveren Algorithmen. Dafür werden komplexere mathematische Konzepte und Teilgebiete verwendet, wie zum Beispiel die Primfaktorzerlegung und diskrete Logarithmen. Auch die modernste Computertechnologie kommt hier an ihre Grenzen. Ein Verschlüsselungsverfahren ist dann nur noch in einer sehr unwirtschaftlichen, jahrtausendlangen Zeitspanne zu brechen

18 Vgl. Buchmann, Johannes: Einführung in die Kryptographie, a. a. O., S. 17ff.

19 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 83f.

und gilt somit als sicher. Diese sogenannten schweren Berechnungsprobleme der Algorithmen und Schlüssel sind die Grundlage für die Sicherheit eines kryptografischen Verfahrens.[20]

### 2.3.3 Kryptografische Verfahren

Die Funktionsweisen von modernen kryptografischen Verfahren sind sehr vielfältig, weswegen die Verfahren in der Praxis je nach Anwendungsgebiet entsprechend variabel verwendet werden. Die Verfahren werden benötigt, um die Schutzziele der Informationssicherheit von IT-Systemen gewährleisten zu können. Diese IT-Schutzziele werden im nachfolgenden Kapitel definiert. Im Rahmen dieser Arbeit wird prinzipiell zwischen vier kryptografischen Verfahren bzw. Mechanismen unterschieden:[21]

- Symmetrische Verschlüsselungsverfahren
- Asymmetrische Verschlüsselungsverfahren
- Hashfunktionen und Nachrichtenauthentifizierungscodes
- Digitale Signaturen

Diese verschiedenen kryptografischen Verfahren werden nun vorab erklärt, um sie in den darauffolgenden Kapiteln der Verfahren und Anwendungsgebiete trennscharf aufgreifen und ausführlich erläutern zu können. Mit einer Kombination dieser kryptografischen Verfahren lässt sich die hybride Verschlüsselung im Web hinreichend umsetzen.[22]

**Symmetrische Verschlüsselungsverfahren:**

Ein Verschlüsselungsverfahren basiert auf speziellen mathematischen Funktionen, die einen Klartext in Abhängigkeit eines Schlüssels in einen Geheimtext umwandeln. Bei einem „guten" Verschlüsselungsverfahren sollte es für einen Angreifer unmöglich sein, eine Information ohne Kenntnis des Schlüssels zu entschlüsseln, auch wenn das Verfahren selbst bekannt ist (Kerckhoffs'sche Prinzip). Die Grundbausteine eines Schlüssels werden durch einen Computer zufällig generiert und fließen als Zusatzinformationen in das Verschlüsselungsverfahren mit ein. Ein Verschlüsselungsverfahren beschreibt, wie der Schlüssel auf die zu verschlüsselnde Klartextinformation angewendet werden muss, damit ein verschlüsselter Geheimtext entsteht und umgekehrt.[23]

20 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 180ff und 235.

21 Vgl. Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013, S. 25.

22 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 3f.

23 Vgl. Beutelsbacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter: Moderne Vefahren der Kryptologie – Von RSA zu Zero-Knowledge, 8. Aufl., Wiesbaden: Springer Spektrum 2015, S. 2.

Die Verschlüsselung aus den bereits genannten historischen Beispielen der Kryptografie funktioniert konzeptuell überall ähnlich: Der Zylinderumfang der Skytale muss beim Verfassen und beim Lesen identischen sein, um das Entziffern der Botschaft entlang der Zeilen zu ermöglichen. Auch der Geheimtext der Caesar-Chiffre muss um den identischen Wert des Alphabets zurückverschoben werden, um ihn wieder in Klartext entschlüsseln zu können. Diese Beispiele beruhen auf einer „Schlüssel-Symmetrie“. Sowohl für die Verschlüsselung als auch für die Entschlüsselung einer Information wird das identische Geheimnis bzw. derselbe geheime Schlüssel, engl. secret key, verwendet. Wie bei einem herkömmlichen Türschloss dreht sich der passende Schlüssel nach links und nach rechts. Ein symmetrischer Schlüssel ist folglich in zwei Richtungen zu verwenden und kann sowohl dupliziert, als auch von mehreren Personen verwendet werden.[24] Abbildung 5 stellt das Verfahren einer symmetrischen Verschlüsselung schematisch dar:

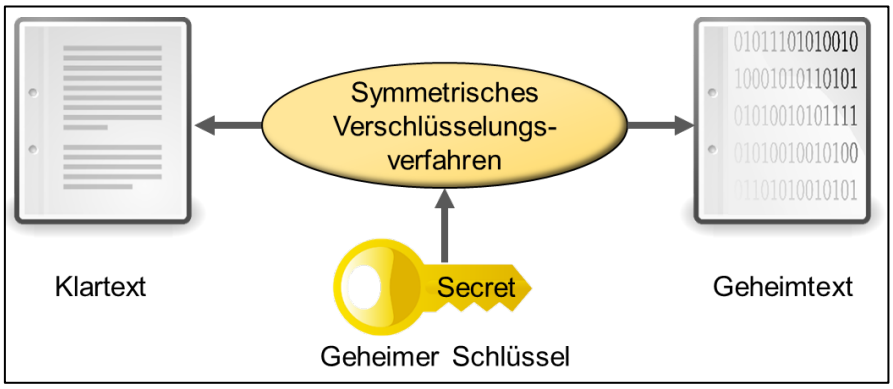



Abb. 5: Verschlüsselung mit einem symmetrischen Schlüssel

**Asymmetrische Verschlüsselungsverfahren:**

Das Gegenstück zu den symmetrischen Verfahren sind die asymmetrischen Verfahren. Bei den asymmetrischen Verschlüsselungsverfahren wird nicht nur ein einziger geheimer Schlüssel verwendet, sondern stattdessen ein Schlüsselpaar, wie in Abbildung 6 zu sehen ist:[25]

24 Vgl. Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter: Moderne Verfahren der Kryptologie – Von RSA zu Zero-Knowledge, a. a. O., S.10.

25 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Theorie und Praxis, 4. Auflage, Wiesbaden: Springer Vieweg 2014, S. 19.

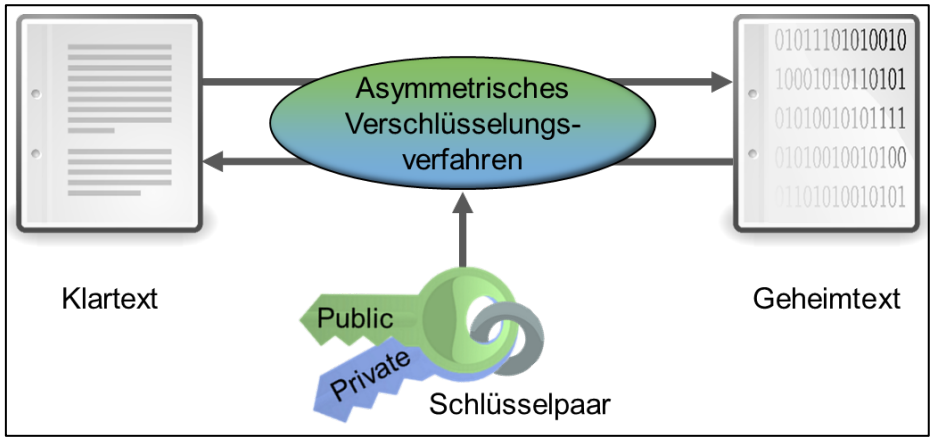



Abb. 6: Verschlüsselung mit einem asymmetrischen Schlüsselpaar

Ein Schlüsselpaar besteht aus einem privaten Schlüssel, engl. private key, und aus einem öffentlichen Schlüssel, engl. public key. Jedes Schlüsselpaar ist einzigartig und ist fest an eine Person gebunden. Die zugrundeliegenden Algorithmen der asymmetrischen Verschlüsselungsverfahren basieren auf sogenannten Einwegfunktionen. Ist der Klartext beispielsweise mit dem öffentlichen Schlüssel verschlüsselt, kann der Geheimtext nur noch mit dem privaten Schlüssel desselben Schlüsselpaars wieder entschlüsselt werden. Ein Schlüssel des Schlüsselpaars kann entweder für die Verschlüsselung oder für die Entschlüsselung einer Information verwendet werden.

Die Erläuterungen zu standardisierten und in der Praxis angewandten symmetrischen und asymmetrischen Algorithmen sowie den Vor- und Nachteilen beider Verschlüsselungsverfahren werden in späteren Kapiteln ausführlich fortgesetzt. Die hybride Verschlüsselung ist eine Kombination der oben angedeuteten Verfahren, bei der unterschiedliche Verschlüsselungsmechanismen ineinandergreifen. Mit Bezug auf die hybride Verschlüsselung sind zwei weitere kryptografische Verfahren relevant: Die Hashfunktionen bzw. Nachrichtenauthentifizierungscodes und die digitalen Signaturen. Sie erweitern die Verschlüsselungsverfahren und bieten zusätzliche Sicherheitsaspekte.

**Hashfunktionen und Nachrichtenauthentifizierungscodes:**

Eine Hashfunktion überträgt eine eingehende Information in einen verstreuten Wert (Streuwertfunktion). Mit dem entstandenen Hashwert kann der Rückweg zur ursprünglichen Information allerdings nicht mehr nachvollzogen werden. Es existiert keine mathematische Funktion, um vom Hashwert zurück zur Klartextinformation zu gelangen. Anders als bei den symmetrischen und asymmetrischen Verschlüsselungsverfahren ist zur Umkehrung des Hashwerts in den ursprünglichen Klartext also kein symmetrischer geheimer Schlüssel und auch kein asymmetrisches Schlüsselpaar vorhanden. Hashfunktionen sind daher Falltürfunktionen.[26]

26 Vgl. Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: Kryptographie und IT-Sicherheit – Grundlagen und Anwendungen, a. a. O., S. 34.

Unabhängig von der Menge oder Größe des Klartexts ist der verstreute Wert einer Hashfunktion immer gleich lang. Ein Beispiel für eine Hashfunktion ist SHA (Secure Hash Algorithm) mit einer Zeichenkette von 40 Dezimalstellen bzw. 160 Bit (SHA-1). Eine weitere Eigenschaft einer Hashfunktion ist, dass selbst die kleinste Änderung eines Klartextes in einem gänzlich neuen Hashwert resultiert, ohne jeglichen Bezug zu einer ähnlichen Information. Beginnt beispielsweise der erste Buchstabe des Worts „Krypto“ mit einem kleinen „k“ verändert sich der Hashwert gravierend:[27]

Klartext: **K**rypto → SHA-1: `c2d1dd21904cea969497f50ec22e86a225233548`

Klartext: **k**rypto → SHA-1: `ea0ebebc190e9f69181c9c2dcac2bc503a9ffc54`

Bei der Eingabe von sensiblen Informationen, wie zum Beispiel der Passwortvergabe bei der Erstellung eines Online Accounts, sollten die Benutzerpasswörter nicht im Klartext auf einem Server abgespeichert werden. Stattdessen können die Passwörter durch Hashfunktionen unleserlich gemacht werden. Bei einem Benutzer-Login wird nur noch der entsprechende Hashwert des Benutzers und nicht mehr das Passwort selbst mit der Datenbank auf dem Web Server abgeglichen. Ein potentieller Angreifer auf einen Online Account müsste folglich nicht nur nach allen erdenklichen Passwörtern in Klartext suchen, sondern diese auch noch in sämtliche Hashwerte umrechnen. Hashwerte sind wie oben bereits erwähnt absolut einzigartig. Bekannte und typische Passwortinformationen und deren Hashwerte werden in Datenbanken und öffentlichen Listen hinterlegt. Für einen Angreifer lohnt es sich einen Blick in diese Listen zu werfen, um zu erst nach den am häufigsten verwendeten Passwörtern zu suchen, um sich Zugang zu einem System zu verschaffen.[28]

Die Hashfunktion SHA-1 mit 160 Bit ist zu kurz und heutzutage nicht mehr sicher. Die Hashfunktion SHA-2 verstreut eine eingeworfene Information in einen Hashwert mit bis zu 512 Bit. Theoretisch ist jede erdenkliche Information der Welt, die in einen Hashwert übertragen wurde, absolut einzigartig. Man spricht von der Kollisionsfreiheit bzw. Kollisionssicherheit einer Hashfunktion, weil ein zufälliger Hashwert einer Information mit keinem Hashwert einer anderen Information kollidieren kann. Durch diese wichtige Eigenschaft sind Hashfunktionen geradezu prädestiniert, die Unversehrtheit und Echtheit einer Information zu überprüfen. Der Hashwert einer Hashfunktion wird dann als Nachrichtenauthentifizierungscode, engl. Message Authentication Code (MAC) bezeichnet und wird in Kombination mit einem symmetrischen

27 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 241f und Gobrecht, Jan: SHA Generator, Online im Internet: https://www.sha-generator.de, zuletzt aufgerufen am 16.01.2019.

28 Vgl. Schirrmacher, Dennis: Zahlenfolge "123456" immer noch beliebtestes Passwort in Deutschland, Online im Internet: https://heise.de/-3927009, 22.12.2017.

Schlüssel verwendet. Durch einen MAC können mögliche Veränderungen bzw. Manipulationen von Informationen erkannt werden. In der Praxis werden Hashfunktionen und MAC regelmäßig in digitalen Signatursystemen verwendet.[29]

**Digitale Signaturen:**

Durch den fehlenden persönlichen Kontakt bei der Kommunikation im Web sind Anwender darauf angewiesen, den digitalen Informationen zu vertrauen. Bei einer digitalen Signatur handelt es sich nicht um einen Scan einer handschriftlich angefertigten Unterschrift. Eine digitale Signatur ist ein Nachrichtenauthentifizierungscode in Verbindung mit einem asymmetrischen Schlüsselpaar. Eine digitale Signatur hat ähnliche Eigenschaften wie eine herkömmliche Unterschrift. Eine Unterschrift ist in der Regel nur sehr schwer zu fälschen und bestätigt deswegen die Identität und Urheberschaft einer Information. Mit digitalen Signaturen im Web wird überprüft, ob die erwarteten Absenderinformationen fehlerfrei vorliegen (peer entity authetication) oder eine Information nachträglich manipuliert wurde (data origin authentication). Digitale Signaturen erzeugen somit Vertrauen und Verbindlichkeit im Internet und prüfen, dass Informationen vom korrekten Versender und keinem anderen stammen.[30]

Dieses Kapitel hat die Berechnungsprobleme von Verschlüsselungsalgorithmen und die Schlüssel- bzw. Bitlängen thematisiert. Anschließend wurde zwischen vier kryptografischen Verfahren unterschieden. Das nächste Kapitel thematisiert die Schutzziele der Informationssicherheit, welche durch die oben genannten kryptografischen Verfahren erreicht werden.[31]

29 Vgl. Microsoft (Hrsg.): MACs, hashes, and signatures, Online im Internet: https://docs.microsoft.com/de-de/windows/uwp/security/macs-hashes-and-signatures, 08.02.2017 und vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 281f.

30 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 215f und 281f und vgl. Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013, S. 25f.

31 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 200.

## 2.4 Informationssicherheit durch kryptografische Verfahren

Moderne IT-Systeme nutzen verschiedene kryptographische Verfahren, um den Schutz von digitalen Informationen durch Verschlüsselung zu gewährleisten. Dabei gilt es zu beachten, dass die einzelnen kryptographischen Verfahren die Schutzziele der Informationssicherheit nur teilweise bedienen. Je nach Notwendigkeit und Anwendungsgebiet einer Verschlüsselung verändert sich auch die Anforderung an die Schutzziele und somit an die zu verwendenden kryptografischen Verfahren. Die kryptografischen Verfahren werden daher in IT-Systeme variabel eingesetzt und unterschiedlich implementiert. Die im vorangegangenen Kapitel erläuterten kryptografischen Verfahren werden nun den vier Schutzzielen der Informationssicherheit zugeordnet. Die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit von Informationen. Abbildung 7 stellt die Zusammenhänge zwischen den kryptografischen Verfahren und den Schutzzielen der Informationssicherheit grafisch dar:[32]

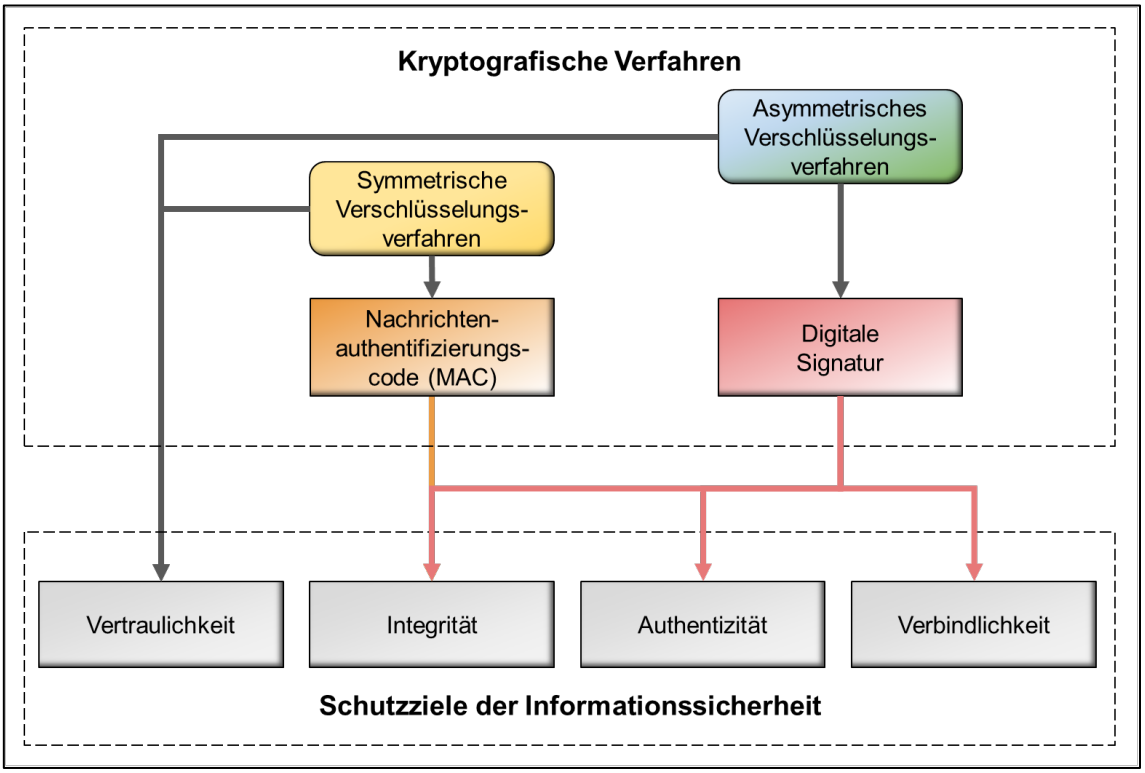



Abb. 7: Kryptografische Verfahren und die Schutzziele der IT-Sicherheit

**Vertraulichkeit:** Das Schutzziel der Vertraulichkeit bedeutet, dass nur ausgewählte Personen Einblicke in Informationen oder Zugang zu einer Kommunikation erhalten. Unbefugte Personen dürfen gespeicherte oder versendete Informationen nicht mitlesen. Mithilfe von symmetrischen und asymmetrischen Verfahren können vertrauliche Information durch Verschlüsselung

32 Eigene Abbildung in Anlehnung an Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013, S. 32.

mit einem geheimen Schlüssel bzw. einem Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, geschützt werden.

**Integrität:** Das Schutzziel der Integrität besagt, dass Informationen vollständig und unversehrt vorliegen müssen. Veränderungen an Informationen dürfen außerdem nicht unerkannt bleiben. Ein Prüfverfahren basierend auf einer Hashfunktion bzw. einem MAC erkennt mögliche Veränderungen und Manipulationen von Informationen. Auch minimale Abweichungen an der ursprünglichen Information erkennt der MAC als Verletzung der Integrität einer Information.[33]

**Authentizität:** Das Schutzziel der Authentizität besagt, dass die Identität eines Kommunikationspartners korrekt ist und eine Information tatsächlich von der angegebenen Quelle stammt. Eine digitale Signatur bestätigt die Identität eines Kommunikationsteilnehmers durch den Besitz eines kryptografischen Schlüssels bzw. die Prüfung eines MAC. Diese Überprüfung gelingt durch die Verwendung eines personengebundenen asymmetrischen Schlüsselpaars.

**Verbindlichkeit:** Das Schutzziel der Verbindlichkeit stellt sicher, dass ein Kommunikationspartner eine Handlung nicht leugnen kann. Dies wird ebenfalls durch digitale Signaturen realisiert. Der Empfänger einer Information erhält durch die digitale Signatur des Senders einen Urhebernachweis, den der Sender anschließend nicht mehr abstreiten kann. Die digitale Signatur ist somit rechtskräftig.[34]

Heutzutage sind viele Geschäftsmodelle digitalisiert und eng mit IT-Systemen verbunden. Die oben genannten kryptografischen Verfahren helfen dabei, die Prinzipien und Schutzziele der IT-Sicherheit zu erfüllen. IT-Systeme werden durch kryptografische Verfahren abgesichert, um die gesetzlichen oder unternehmensinternen Vorgaben und Regularien der IT-Compliance einzuhalten. Nur so kann die Vertraulichkeit in der Kommunikation mit Kunden oder mit Mitarbeitern über Unternehmensinterna gewahrt werden.

Bei der Wahl des passenden kryptografischen Verfahrens ist es von Vorteil, den Ressourcenbedarf für Rechenkapazität und Speicherplatz abzuschätzen. Die ordnungsgemäße Implementierung des kryptografischen Verfahrens durch eine lückenlose Verknüpfung in bereits bestehende IT-Systeme ist ebenfalls sehr bedeutsam. Wird eine Verschlüsselungstechnologie unsauber implementiert, entstehen möglicherweise gravierende Schwachstellen in einem für sicher

33 Vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, a. a. O, S. 10f und vgl. Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, a. a. O., S. 25f.

34 Vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, a. a. O, S. 10f und Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013, S. 25f.

deklarierten IT-System.[35] Ein Angriff auf ein verschlüsseltes IT-System, der schneller oder besser funktioniert als die vollständige Schlüsselsuche eines Brute-Force-Angriffs, weist bereits auf eine signifikante Schwäche der Implementierung des kryptografischen Verfahrens hin.[36]

Die Kryptografie ist ein aktives Forschungsfeld. Es existieren einige staatliche Standardisierungsgremien sowie Gruppierungen von Industrieverbänden und auch Interessenten aus Forschung und Wirtschaft, welche stetig an neuen Verschlüsselungs- und Internetstandards arbeiten. Im Rahmen von Standardisierungswettbewerben werden die kryptografischen Verfahren heutzutage regelmäßig in Bezug auf ihre Sicherheit und Praxistauglichkeit getestet. Dadurch entstehen kontinuierlich fortschrittlichere kryptografische Verfahren mithilfe von verbesserten Algorithmen.[37]

Das National Institute of Standards and Technology (NIST) in den USA hat bereits zahlreiche Verschlüsselungsstandards entwickelt und veröffentlicht. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) ebenfalls an der Entwicklung kryptografischer Standards beteiligt. Das BSI veröffentlicht zudem Empfehlungen zu aktuellen Verschlüsselungsstandards. In diesen „Technischen Richtlinien“ werden Informationen und Hilfestellungen zur praktischen Umsetzung und Implementierung von kryptografischen Verfahren gegeben. Die Technischen Richtlinien haben das Ziel einen angemessenen IT-Sicherheitsstandard in Deutschland zu etablieren.[38]

Die Internet Engineering Task Force (IETF) ist eine wichtige Organisation für die Weiterentwicklung der modernen Kryptografie. Die IETF bildet fortlaufend internationale Arbeitsgruppen zur Entwicklung von Standardvorschlägen, die regelmäßig neue Konzepte für kryptografische Internetstandards beinhalten. Die Vorschläge der IETF werden nach internen sowie öffentlichen Revisionen und Tests als offizielle Verschlüsselungsstandards publiziert. Die publizierten Standards werden RFC genannt (Request for Comment). Im August 2018 veröffentlichte die IETF ein aktualisiertes Protokoll für den verschlüsselten Transport von Informationen im Internet, das Transport-Layer-Security-Protokoll (TLS) in der Version 1.3. Dieses verschlüsselte Netzwerkprotokoll basiert auf hybriden Verfahren, welches im vierten Kapitel detaillierter thematisiert wird.[39]

Das nachfolgende und abschließende Kapitel der Grundlagen skizziert die Verwendung der Netzwerkprotokolle im Web. Dabei werden die in der Literatur häufig verwendeten Stilfiguren

35 Vgl. Buchmann, Johannes: Einführung in die Kryptographie, a. a. O., S. 19.

36 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 113f.

37 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 390.

38 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kryptographische Verfahren – Empfehlungen und Schlüssellängen, in: TR-02102-1, 22.02.2019, S.13.

39 Vgl. Rescorla, Eric: The Transport Layer Security (TLS) Protocol Version 1.3, in: Internet Engineering Task Force (Hrsg.): RFC 8446, August 2018 und vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 391.

Alice und Bob vorgestellt, welche die verschlüsselte Kommunikation im Web zu veranschaulichen.

## 2.5 Netzwerkprotokolle und die Kommunikation im Web

Damit kryptografische Verfahren im Web Anwendung finden können, müssen bestimmte Abläufe und Vorgehensweise durch Netzwerkprotokolle klar definiert werden. Netzwerkprotokolle dienen dem Transport von Daten und legen die „Sprachen" fest, in denen Computer oder Router in einem Netzwerk miteinander kommunizieren. Wie bei einem diplomatischen Protokoll werden bei Netzwerkprotokollen Regeln für einen Kommunikationsverlauf festgehalten. Dabei halten Netzwerkprotokolle fest, schreiben vor oder zeichnen auf, in welcher Reihenfolge oder zu welchem Zeitpunkt ein bestimmter Vorgang der digitalen Kommunikation veranlasst wird. Ein Netzwerkprotokoll ist also eine Menge von Vereinbarungen, in denen geregelt ist, wie Daten und Informationen im Netzwerk ausgetauscht und abgefragt werden. Das Internet ist kein geschlossenes Netzwerk, sondern eine Menge von Computern, die mithilfe von Datenleitungen miteinander verbunden sind. Ein Zusatznutzen für den Benutzer der Netzwerkprotokolle entsteht erst durch verschiedene Internetdienste und Anwendungsprogramme, die ihm basierend auf den Netzwerken zur Verfügung stehen.[40]

Diese Sender- und Empfänger-Kommunikation zwischen Client und Server verläuft beispielsweise über das Netzwerkprotokoll HTTP (Hypertext-Transfer-Protocol). Eine typische Anfrage eines Clients (Web Browser) an einen Server (Web Site) ist beispielsweise: „Zeig mir die Homepage von www.uni-giessen.de". Eine solche Anfrage wird als HTTP-Anfrage (Request) bezeichnet. Im Domain Name System (DNS) wird diese Suchanfrage in eine Internetprotokolladresse (IP-Adresse) aufgelöst. So kann der angefragte Server eindeutig im Internet ausfindig gemacht werden. Der Server stellt dem Client anschließend die angeforderten Informationen in einer HTTP-Antwort bereit (Response). Die Informationen dieser Antwort werden zum Beispiel in der Auszeichnungssprache HTML (Hypertext Markup Language) übertragen, welche auf dem Server zuvor gespeichert wurden.[41]

Ähnlich zu den oben beschriebenen HTTP-Anfragen, wird auch die Kommunikation zwischen zwei Personen über Netzwerkprotokolle abgewickelt. Für den Internetdienst E-Mail sind das beispielsweise SMTP (Simple Mail Transfer Protocol) und IMAP (Internet Message Access Protocol). Die Protokolle der E-Mail-Server verarbeiten und regeln den Empfang, den Versand und die Speicherung der E-Mails.[42]

40 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 427f.

41 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, 2. aktualisierte und erweiterte Auflage, Wiesbaden: Springer Vieweg 2013, S. 272ff.

42 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a. a. O., S. 260f.

Eine Vielzahl von Netzwerkprotokollen sorgt heute für die Darstellung und den Transport von Informationen in Kommunikationssystemen. Die Internationale Organisation für Normung hat in diesem Zusammenhang ein Open Systems Interconnection-Modell entwickelt (OSI-Modell). Dieses Referenzmodell beruht auf den Netzwerkprotokollen von TCP/IP (Transmission Control Protocol/Internet Protocol). Das OSI- und das TCP/IP-Modell sind mit einer Auswahl an Netzwerkprotokollen in Abbildung 8 zu sehen. Durch die nachfolgende Erläuterung entlang der Schichten von TCP/IP entsteht eine Übersicht der Netzwerkprotokolle in den Architekturebenen des Internets:[43]

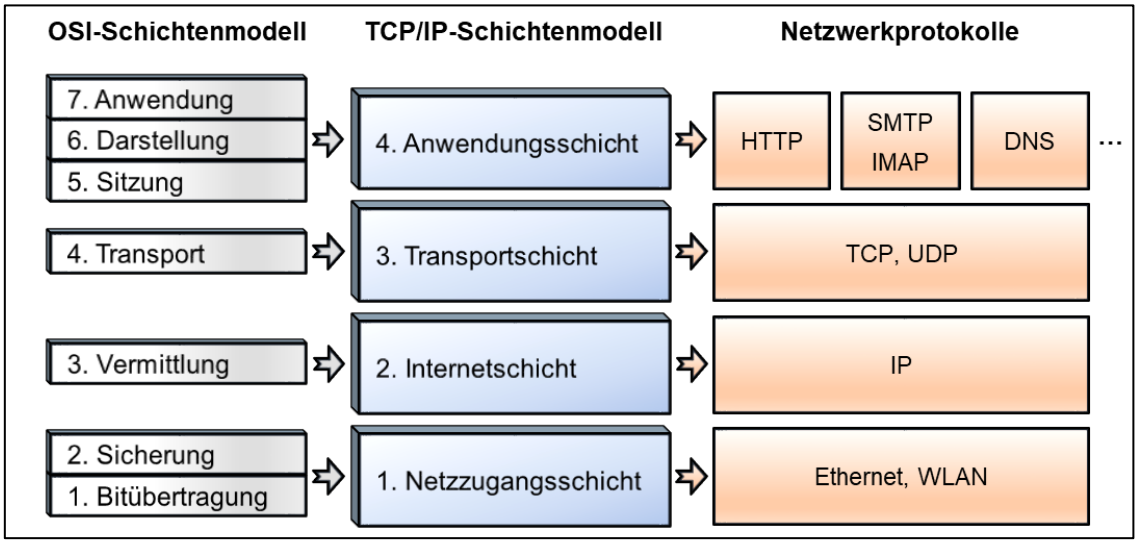



Abb. 8: Das OSI- und TCP/IP-Modell und die Netzwerkprotokolle

**4. Anwendungsschicht:** Die Netzwerkprotokolle der oberen, vierten Schicht des TCP/IP-Modells werden zum Beispiel durch Web Browser wie Mozilla Firefox oder in E-Mail-Programmen wie Microsoft Outlook verwendet. Neben den dafür bereits erwähnten Netzwerkprotokollen HTTP, DNS und SMTP/IMAP werden auch weitere Protokolle für andere Anwendungsgebiete verwendet. In dieser Schicht werden die versendeten Informationen zwischen Sender und Empfänger in ein passendes Format zur einheitlichen Darstellung konvertiert. Die Informationen und Daten der Anwendungsschicht werden dabei gebündelt und einer eindeutigen Sitzung zugeordnet, um sie für den Transport über das Netzwerk vorzubereiten.

**3. Transportschicht:** Die Transportschicht realisiert die Verbindung zwischen dem Sender und Empfänger einer Information durch eine sogenannte Ende-zu-Ende-Verbindung. Die Datenbündel der Anwendungsschicht werden durch die Transportschicht segmentiert und systematisch in kleinere Datenpakete unterteilt. Eine E-Mail kann aus vielen Millionen einzelner Datenpakete bestehen, die eigenständig durch das Internet gesendet werden. Es kommt vor, dass

43 Eigene Abbildung in Anlehnung an Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a. a. O., S. 108f, vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 668f und vgl. Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, a. a. O., S. 13f.

die Datenpakete in der falschen Reihenfolge versendet werden oder nicht auf Anhieb beim Empfänger ankommen. Über das Transmission-Control-Protocol (TCP) kontrolliert die Transportschicht, dass alle Datenpakete einer E-Mail oder HTTP-Antwort verlässlich übertragen werden. Die Transportschicht kann auch einen konstanten, verbindungslosen Strom an Datenpaketen, etwa für Audio- und Video-Streaming-Dienste, mit dem User-Datagram-Protocol (UDP) bereitstellen.

**2. Internetschicht**: Die Internetschicht ist für die eigentliche Vermittlung der Daten zuständig und entscheidet, wohin genau die Pakete weitergeleitet werden sollen. Die Datenpakete wählen über die IP-Adressen der verschiedenen Web Server und Netzknoten ihren Weg vom Sender zum Empfänger. Diese Wegwahl durch das Netz wird als Routing bezeichnet.

**1. Netzzugangsschicht**: In der Netzzugangsschicht werden die Datenpakete über physikalische und technische Netze übertragen, zum Beispiel per Ethernet/Glasfaser oder WLAN/Funk. Die Bitströme werden durch Prüfsummen erneut überprüft, um trotz gelegentlicher Störungen im Netz, eine vollständige Übertragung zu gewährleisten.[44]

Damit der Ablauf der Kommunikation im Internet in den folgenden Kapiteln anschaulich dargestellt werden kann, helfen die Stilfiguren Alice und Bob. Die beiden Figuren werden im weiteren Verlauf der Arbeit verschiedene kryptografische Verfahren verwenden, um möglichst sicher miteinander zu kommunizieren.[45]

Die folgende Abbildung 9 zeigt Alice und Bob, welche entlang der oben beschriebenen Schichten des TCP/IP-Modells über die Netzwerkprotokolle im Internet miteinander kommunizieren:[46]

44 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 668f, vgl. Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi: Sicherheit in Kommunikationsnetzen, a. a. O., S. 13f und vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a. a. O., S. 109f.

45 Alice und Bob wurden 1978 zum ersten Mal von den Kryptografen Rivest, Shamir und Adleman verwendet, um die Kommunikation im Internet zu verdeutlichen. Vgl. Rivest, Ron; Shamir, Adi; Adleman, Leonard: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, in: Communications of the ACM (Hrsg.), Volume 21 Issue 2, 02/1978.

46 Eigene Abbildung in Anlehnung an Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 670.

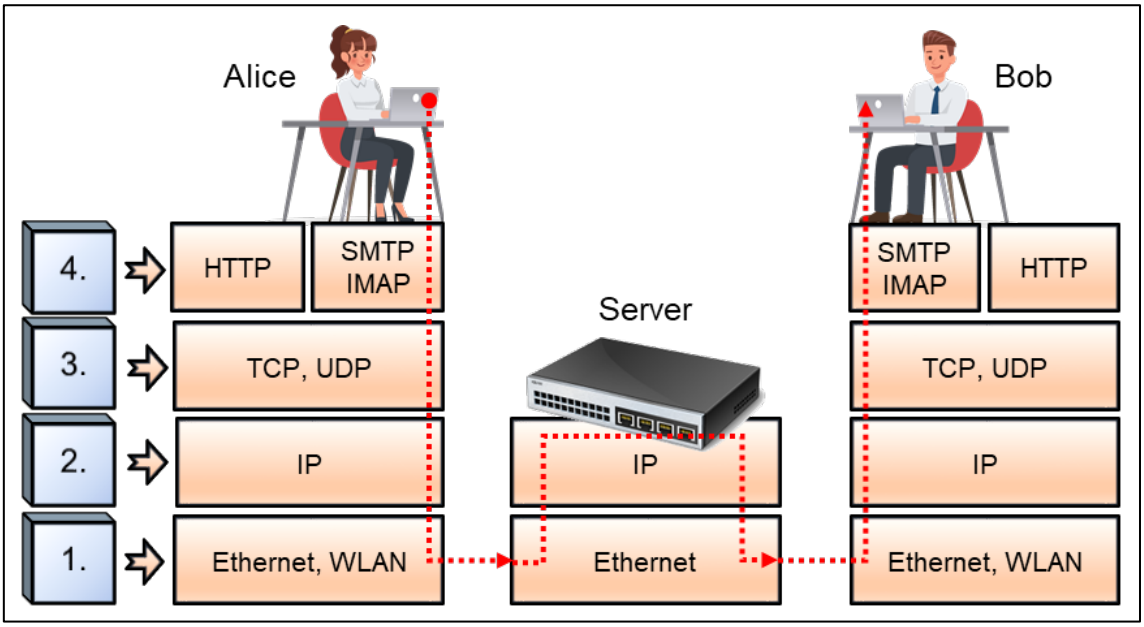



Abb. 9: Die Kommunikation zwischen Alice und Bob im Web

Die oben beschriebenen Netzwerkprotokolle haben zunächst wenig mit den kryptografischen Verfahren des vorherigen Kapitels zu tun und sorgen per se für keine Verschlüsselung der transportierten Informationen. Ihre Hauptaufgabe liegt darin, die Kommunikation innerhalb von globalen Rechnernetzwerken grundlegend zu ermöglichen und ordnungsgemäß abzuwickeln. Eine E-Mail, die von Alice mithilfe der Netzwerkprotokolle SMTP und IMAP an Bob versendet wurde, könnte also theoretisch auf dem Transportweg abgefangen und von einer unbefugten Person gelesen werden.

Der letzte Abschnitt dieser Arbeit wird die oben dargestellten Abbildungen 8 und 9 erneut erläutern und die *verschlüsselten* Netzwerkprotokolle des TCP/IP-Modells thematisieren. Im Rahmen dieser Arbeit sind die Anwendungsschicht und die Transportschicht des TCP/IP-Modells relevant. Die hybride Verschlüsselung im Web knüpft vor allem an der Transportschicht an, um die Netzwerkprotokolle der Anwendungsschicht mit kryptografischen Verfahren zu untermauern.[47]

47 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 671f.

Im nachfolgenden Kapitel drei werden Alice und Bob auf Basis verschiedener Verfahren miteinander kommunizieren. Keine unbefugte Person soll die Möglichkeit haben, ihre Kommunikation zu belauschen oder zu manipulieren. Die Verschlüsselungsverfahren sorgen für verschlüsselte Netzwerkprotokolle und werden nun ausführlich erläutert.

# 3 Verfahren der hybriden Verschlüsselung

## 3.1 Systematisierung der Verfahren

In diesem Kapitel werden die kryptografischen Verfahren des Grundlagenkapitels ausführlich erläutert. Dafür werden die kryptografischen Verfahren in die symmetrischen und asymmetrischen Verschlüsselungsverfahren kategorisiert, welche in Kombination ein hybrides Verschlüsselungsverfahren bilden. Die zugrundeliegenden Algorithmen der Verschlüsselungsverfahren werden konzeptionell verdeutlich. Dabei entsteht kein vollständiger Überblick über sämtliche kryptografische Standards. Die exemplarisch ausgewählten Verschlüsselungsstandards werden in der Praxis jedoch sehr häufig verwendet.

Zu Beginn der nachfolgenden Kapitel werden die Verschlüsselungsverfahren exemplarisch anhand von Alice und Bob und deren Kommunikation per E-Mail veranschaulicht und schrittweise erläutert. Diese Verfahren besitzen spezifische Vor- und Nachteile, welche abschließend zusammengefasst werden.

**Kapitel 3.2:** Symmetrische Verschlüsselungsverfahren und der Schlüsselaustausch

Das zweite Kapitel thematisiert das symmetrische Verschlüsselungsverfahren. Die klassische Kryptografie aus den Grundlagen besitzt einige Parallelen zu modernen symmetrischen Standards. Der geheime manuelle Schlüsselaustausch der symmetrischen Verschlüsselung führt in einem digitalisierten Zeitalter unweigerlich zu Problemen.

**Kapitel 3.3:** Asymmetrische Verschlüsselungsverfahren und der Schlüsseltransport

Das dritte Kapitel thematisiert die asymmetrische Verschlüsselung. Statt einem einzigen geheimen symmetrischen Schlüssel wird ein asymmetrisches Schlüsselpaar verwendet. Das asymmetrische Verfahren behebt das Schlüsselaustauschproblem der symmetrischen Verfahren. Auch die übrigen kryptografischen Verfahren des Grundlagenkapitels werden erneut aufgegriffen. Hashfunktionen und digitale Signaturen sind wichtige Bausteine des asymmetrischen RSA-Verfahrens von Rivest, Shamir und Adleman. In diesem Zusammenhang spielt die Public-Key-Infrastruktur (PKI) eine zentrale Rolle, weil sie für zusätzliches Vertrauen in der Kommunikation im Web sorgt.

**Kapitel 3.4:** Hybride Verschlüsselungsverfahren und die Schlüsselvereinbarung

Das vierte Kapitel verdeutlicht die hybride Verschlüsselung. Durch das asymmetrische RSA-Verfahren wird zunächst ein geheimer Schlüssel transportiert, der wiederum auf symmetrischen AES-Algorithmen basiert. Anschließend wird mit der Diffie-Hellman-Schlüsselvereinbarung ein weitaus robusteres asymmetrisches Verfahren für den Schlüsselaustausch erläutert. In diesem Kapitel wird ersichtlich, dass durch die effiziente Kombination von symmetrischen und asymmetrischen Verfahren, sämtliche Schutzziele der IT-Sicherheit mit einer hybriden Verschlüsselung bedient werden können.

## 3.2 Symmetrische Verschlüsselungsverfahren

### 3.2.1 Symmetrisch verschlüsselte Kommunikation von Alice und Bob

Das symmetrische Verschlüsselungsverfahren wird zunächst erneut exemplarisch an einem Beispiel der Kommunikation per E-Mail veranschaulicht. Abbildung 10 zeigt diese Kommunikation zwischen Alice und Bob auf Basis eines symmetrischen Verfahrens, bei dem der Schlüssel für die Verschlüsselung und Entschlüsselung identisch ist:[48]

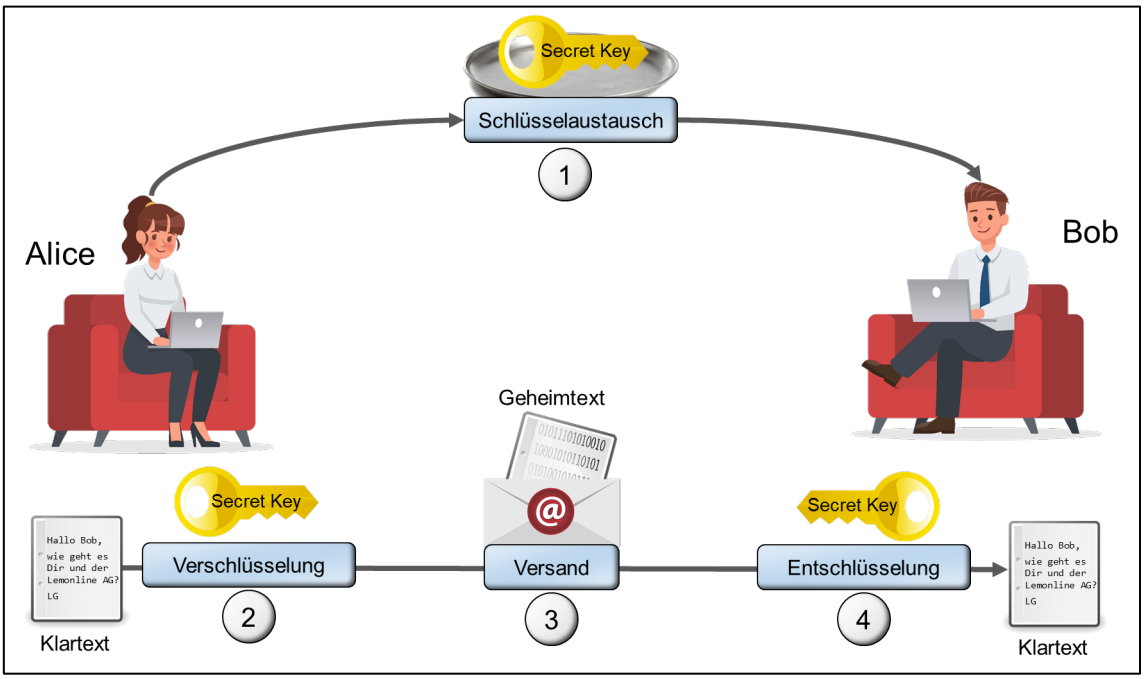



Abb. 10: Die symmetrische Verschlüsselung

48 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 174.

(1) Alice erstellt einen geheimen Schlüssel (Secret Key) und tauscht diesen mit Bob aus.

(2) Alice schreibt ihre Nachricht in Klartext und verschlüsselt diesen0 mit dem geheimen Schlüssel, den Alice und Bob miteinander ausgetauscht haben. Es entsteht eine Nachricht mit dem Geheimtext.

(3) Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Bob kann die Geheimtext-Datei mit dem geheimen Schlüssel, den Alice zuvor mit Bob geteilt hat, wieder in Klartext umwandeln.

### 3.2.2 Verschlüsselungsstandards und das Schlüsselaustauschproblem

Bei einem symmetrischen Verfahren wird derselbe geheime Schlüssel für die Verschlüsselung und Entschlüsselung der Nachricht verwendet. Die symmetrischen Verfahren sind heutzutage deutlich sicherer als die bereits erwähnten Anwendungsbeispiele der klassischen Kryptografie. In den Vereinigten Staaten von Amerika entwickelte Anfang der 1970er Jahre das National Institute of Standards and Technology (NIST) gemeinsam mit anderen staatlichen Sicherheitsbehörden wie der National Security Agency (NSA) standardisierte und sichere Verschlüsselungsverfahren. Durch öffentliche Ausschreibungen wurden Vorschläge von IT- und Beratungsunternehmen wie zum Beispiel IBM eingereicht. So wurden regelmäßig fortschrittlichere kryptografische Verfahren ins Leben gerufen, die – gemäß des Kerckhoffs'schen Prinzips – ausschließlich auf der Geheimhaltung des Schlüssels sowie einem robusten Design des Verschlüsselungsverfahrens beruhen.[49]

1977 deklarierte das NIST einen Verschlüsselungsalgorithmus von IBM als offiziellen Data Encryption Standard (DES). Dieser Verschlüsselungsstandard bot erstmals ein computertaugliches Verfahren, welches frei von Patentrechten weltweit anerkannt wurde. DES war für zwei Jahrzehnte das Mittel der Wahl für die Verschlüsselung von Informationen. Zur Jahrtausendwende wurde das DES-Verfahren durch den Advanced Encryption Standard (AES) als offiziellen Nachfolger abgelöst, der von den belgischen Kryptografen Joan Daemen und Vincent Rijmen 1997 entwickelt wurde.[50] AES findet bis heute in unterschiedlichen IT-Systemen regelmäßig Anwendung und wird sehr vielseitig verwendet, zum Beispiel für die Verschlüsselung von Festplatten, Netzwerkverbindungen oder bei der verschlüsselten Kommunikation im Web.

49 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O., S. 19f und Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 12f.

50 Vgl. Freiermuth, Karin; Hromkovič, Juraj; Keller, Lucia; Steffen, Björn: Einführung in die Kryptologie – Lehrbuch für Unterricht und Selbststudium, 2. überarbeitete Auflage, Wiesbaden: Springer Vieweg 2014, S. 178f.

Neben dem AES-Verfahren werden auch andere symmetrische Verschlüsselungsverfahren verwendet, welche je nach Einsatzgebiet zum Beispiel in Chipkarten oder Mobilfunknetzen implementiert sind.[51]

Die Mechanismen der symmetrischen Verschlüsselungsstandards ähneln im Ansatz den historischen kryptografischen Ursprüngen der mono- und polyalphabetischen Substitution bzw. Transposition. Bei der symmetrischen Verschlüsselung (DES und AES) wird der Klartext in mehrere kleine Blöcke unterteilt. Mit dem DES-Verfahren werden die Blöcke in dem sogenannten Feistelnetzwerk vertauscht (Konfusion durch Substitution) und anschließend gemischt bzw. transponiert (Diffusion durch Permutation). Das Prinzip dieser Blockchiffren wird über mehrere Runden wiederholt.[52] Mit dem modernen AES-Verfahren werden die Blöcke durch sogenannte Exlusiv-Oder-Gatter (engl. eXclusive OR gate, XOR) pseudozufällig miteinander verbunden. Zusätzlich werden mehrere voneinander abhängige Duplikate des ursprünglichen symmetrischen Schlüssels verwendet. In der nachfolgenden Abbildung 11 ist diese „Betriebsart“ des symmetrischen Verfahrens skizziert. Sie zeigt einen Counter-Modus (CTR), der gegenwärtig häufig für das AES-Verfahren verwendet wird:[53]

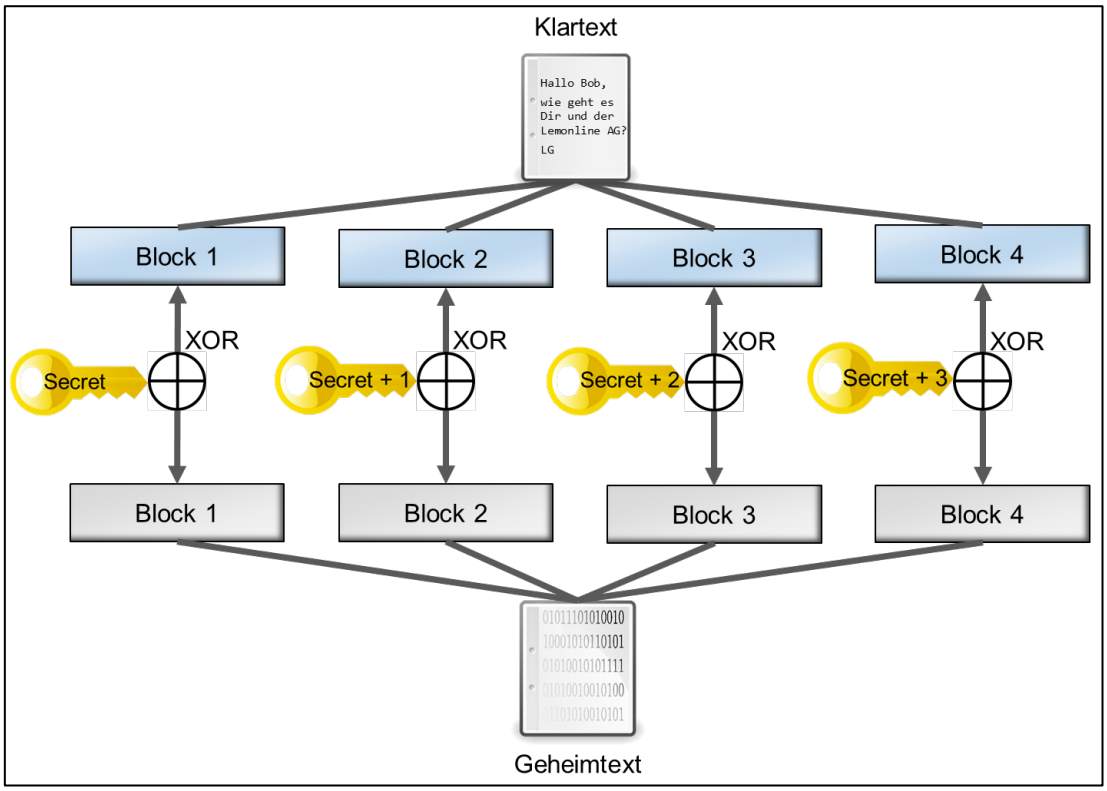



Abb. 11: Eine symmetrische AES-Betriebsart am Beispiel des Counter-Modus

51 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 171ff.

52 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 171ff.

53 Eigene Abbildung in Anlehnung an Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 416f.

Die symmetrischen Algorithmen sind trotz dieser komplexen Betriebsarten in beide Richtungen aufzulösen, sofern der geheime Schlüssel bekannt ist. Es herrscht also – wie in den historischen Beispielen der Caesar- und Vigenère-Chiffre – immer noch „Schlüssel-Symmetrie“.

Moderne symmetrische Verfahren und ihre Betriebsarten sind sehr effizient und benötigen verhältnismäßig wenig Rechenleistung. Die symmetrische Verschlüsselung bietet sich zudem durch besonders hohe Verschlüsselungs- und Entschlüsselungsgeschwindigkeiten an, auch auf unterschiedlichen Plattformen und Betriebssystemen. Die Symmetrische Verschlüsselung sorgt für Vertraulichkeit und verhindert, dass unbefugte Personen Einblicke in verschlüsselte Informationen erlangen. Sofern Alice und Bob ihre Schlüssel geheim halten, sind moderne symmetrische Algorithmen nicht zu knacken und auch in absehbarer Zukunft sicher. Trotzdem birgt das symmetrische Verschlüsselungsverfahren Gefahren und Risiken.[54]

Bei der symmetrischen Verschlüsselung muss sich vorab auf einen geheimen Schlüssel geeinigt und dieser ausgetauscht werden. Ein Versand des Schlüssels per Post oder in derselben E-Mail wäre jedoch zu unsicher und führt das Ziel der Verschlüsselung ad absurdum. Der Schlüssel würde der Öffentlichkeit auf dem Silbertablett serviert werden, wenn sich Alice und Bob über denselben Kanal auf einen geheimen Schlüssel einigen, über den sie später verschlüsselt miteinander kommunizieren möchten. Das Risiko wäre zu hoch, dass der geheime Schlüssel von einer unbefugten Person auf dem Weg abgefangen würde. Verschlüsselte Nachrichten könnten dann mitgelesen oder verändert werden. Um sicher zu sein, müsste der geheime Schlüssel folglich bei einem persönlichen Treffen an Bob übergeben werden. Alice möchte aber nicht nur mit Bob, sondern auch mit anderen Person verschlüsselt im Web kommunizieren. Sie müsste dann für jede Person einen neuen Schlüssel generieren und diesen ebenfalls vorab geheim übergeben. Dieser manuelle Schlüsselaustausch ist bei einem sehr großen und weit entfernten digitalen Empfängerkreis nicht praktikabel. Diese Nachteile des symmetrischen Verfahrens werden zusammenfassend als Schlüsselaustauschproblem bezeichnet. Das Schlüsselaustauschproblem hat zur Folge, dass die Schutzziele der IT-Sicherheit – die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit (vgl. Kapitel 2.4) – erheblich gefährdet sind.[55]

### 3.2.3 Vor- und Nachteile der symmetrischen Verfahren

Im vorherigen Kapitel wurde das Schlüsselaustauschproblem erläutert und festgestellt, dass symmetrische Verschlüsselungsverfahren alleine nicht ausreichen, wenn im Internet zwei Personen miteinander geheim kommunizieren wollen. Das Schlüsselaustauschproblem wird durch

54 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 108f, 148f, 412 und 415f.

55 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 189f.

das asymmetrische Verfahren gelöst. Im nächsten Kapitel wird das asymmetrische Verschlüsselungsverfahren näher skizziert.

Die Vor- und Nachteile des symmetrischen Verfahrens werden in der nachfolgenden Tabelle erneut zusammengefasst, welche zugleich das Kapitel der symmetrischen Verschlüsselungsverfahren schließt:

| **Symmetrische Verschlüsselungsverfahren**   | |
|---|---|
| **Vorteile** | **Nachteile** |
| + Verschlüsselung gewährleistet zwar die Vertraulichkeit der Informationen, allerdings nur wenn der Schlüssel unter allen Umständen geheim bleibt | – Unbefugte Personen könnten während des Schlüsselaustauschs über einen offenen Kanal in die Hände des geheimen Schlüssels kommen |
| + Hohe Arbeitsgeschwindigkeit bei der Verschlüsselung und Entschlüsselung durch effiziente Algorithmen | – Manueller Schlüsselaustausch führt bei einem weltweit entfernten Empfängerkreis zu Problemen |
| + Einfache Implementierung in unterschiedliche Hard- und Softwaresysteme | – Anzahl der Schlüssel wächst mit jedem Kommunikationsteilnehmer quadratisch |
| | – Gewährleistet keine Integrität, Authentizität bzw. Verbindlichkeit der zu verschlüsselten Daten |

Tab. 1: Vor- und Nachteile von symmetrischen Verschlüsselungsverfahren

## 3.3 Asymmetrische Verschlüsselungsverfahren

### 3.3.1 Asymmetrisch verschlüsselte Kommunikation von Alice und Bob

Das asymmetrische Verschlüsselungsverfahren soll nun ebenfalls am Beispiel der Kommunikation zwischen Alice und Bob exemplarisch erläutert werden. Abbildung 12 zeigt die Kommunikation per E-Mail auf Basis des sogenannten RSA-Verfahrens. Bob ist nun Eigentümer eines Schlüsselpaars:[56]

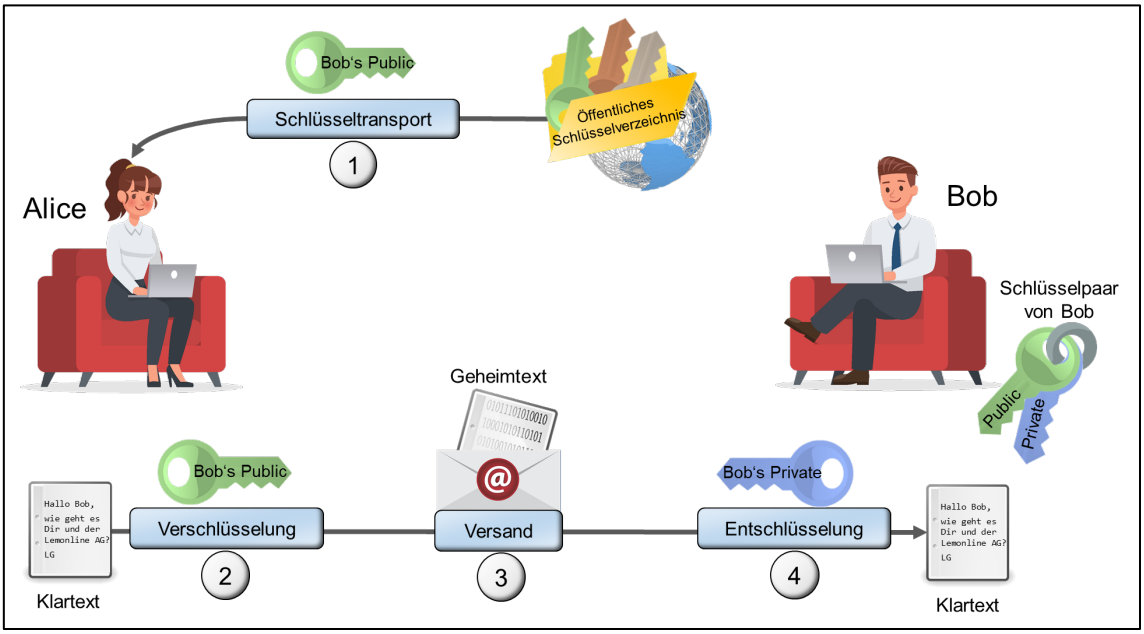



Abb. 12: Die asymmetrische Verschlüsselung auf Basis des RSA-Verfahrens

(1) Bob erstellt ein Schlüsselpaar. Bob hinterlegt seinen öffentlichen Schlüssel in einem öffentlichen Schlüsselverzeichnis. Den privaten Schlüssel behält er für sich.

(2) Alice beschafft sich Bobs öffentlichen Schlüssel aus dem Schlüsselverzeichnis.

(3) Alice schreibt ihre Nachricht in Klartext und verschlüsselt diese mit dem öffentlichen Schlüssel von Bob. Es entsteht eine Nachricht mit dem Geheimtext.

(4) Alice schickt die verschlüsselte Nachricht per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet diese Person nur den unverständlichen Geheimtext.

(5) Nur Bob kann die Geheimtext-Datei mit seinem privaten Schlüssel in Klartext umwandeln, weil die Nachricht zuvor mit dem öffentlichen Schlüssel seines Schlüsselpaars verschlüsselt wurde.

### 3.3.2 Der RSA-Schlüsseltransport und die Public-Key-Infrastruktur

56 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 176.

Die Kryptografen Whitfield Diffie und Martin Hellman hatten bereits im Jahr 1976 eine revolutionäre Idee, um das Schlüsselaustauschproblem der symmetrischen Verfahren mit einem für die Kryptologie gänzlich neuartigen Konzept zu umgehen. Im Folgejahr entwickelten Ronald Rivest, Adi Shamir und Leonard Adleman das erste standardisierte asymmetrische Verschlüsselungsverfahren. Heute ist dieses Verfahren nach den Initialen der Erfinder benannt und als RSA-Verfahren bekannt.[57]

Statt einen einzigen geheimen Schlüssel zur verschlüsselten Kommunikation auszutauschen, können Alice und Bob nun ein Schlüsselpaar verwenden. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel und einem dazugehörigen privaten Schlüssel. Beide Schlüssel sind durch ein mathematisches Verfahren miteinander verbunden und somit voneinander abhängig. Die Schlüsselpaare sind zudem einzigartig und werden individuell erstellt.[58] Anders als das symmetrische AES-Verfahren, welches Informationen mit einem einzigen geheimen Schlüssel sowohl verschlüsselt als auch entschlüsselt, wirkt ein asymmetrischer Schlüssel des RSA-Schlüsselpaars nur in eine Richtung. Ist der Klartext mit dem öffentlichen Schlüssel verschlüsselt worden, kann der Geheimtext nur noch mit dem privaten Schlüssel entschlüsselt werden. Die Algorithmen der asymmetrischen Verschlüsselungsverfahren basieren aus diesem Grund auf sogenannten Einwegfunktionen.[59]

Das RSA-Verfahren beruht zusätzlich auf aufwendigen Berechnungen, wie zum Beispiel der Zerlegung von sehr großen Primzahlen mit Schlüssellängen von 2048-Bit, was einer Dezimalzahl mit 617 Stellen entspricht. Dadurch wird das sogenannte Faktorisierungsproblem erreicht, was für aktuelle Computertechnik ein schweres Berechnungsproblem darstellt. Das asymmetrische RSA-Verfahren ist jedoch, verglichen mit dem symmetrischen AES-Verfahren, um ein Vielfaches rechenintensiver. Asymmetrische Verfahren verschlüsseln Informationen somit langsamer als symmetrische Algorithmen – in etwa um den Faktor 1000. Asymmetrische Verfahren bieten sich deswegen für die Verschlüsselung von sehr kleinen Daten bzw. für Informationen mit geringer Dateigröße an.[60]

Im weiteren Verlauf wird deutlich, dass je nach Einsatzgebiet entweder der öffentliche oder der private Schlüssel zur Verschlüsselung benutzt werden kann. Wenn der öffentliche Schlüssel verschlüsselt und der private Schlüssel entschlüsselt – wie im oben genannten Beispiel der

57 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 178 und vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O., S. 117f.

58 Berechnung eines Schlüsselpaars auf Basis von Primzahlen. Vgl. Popyack; Jeffrey: RSA Calculator, Online im Internet: https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html, zuletzt aufgerufen am 20.02.2019.

59 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Theorie und Praxis, a. a. O., S. 19.

60 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 180, 199 und 235 und vgl. Schmidt, Jürgen: Kryptographie in der IT - Empfehlungen zu Verschlüsselung und Verfahren, Online im Internet: https://heise.de/-3221002, 17.06.2016.

Kommunikation zwischen Alice und Bob – kann nur eine Person, also der Besitzer des privaten Schlüssels, den Geheimtext entschlüsseln.

Wenn jedoch der private Schlüssel verschlüsselt und der öffentliche Schlüssel entschlüsselt, soll eine Vielzahl von Personen Zugang zu einer verschlüsselten Information im Web erhalten. Asymmetrische Verfahren werden in diesem Zusammenhang in Kombination mit digitalen Signaturen verwendet. Abbildung 13 verdeutlicht das Prinzip der digitalen Signatur und ergänzt die asymmetrische Verschlüsselung auf Basis des RSA-Verfahrens (vgl. Abbildung 12) um den rot markierten Bereich und die Schritte A bis F zur Signaturerstellung:[61]

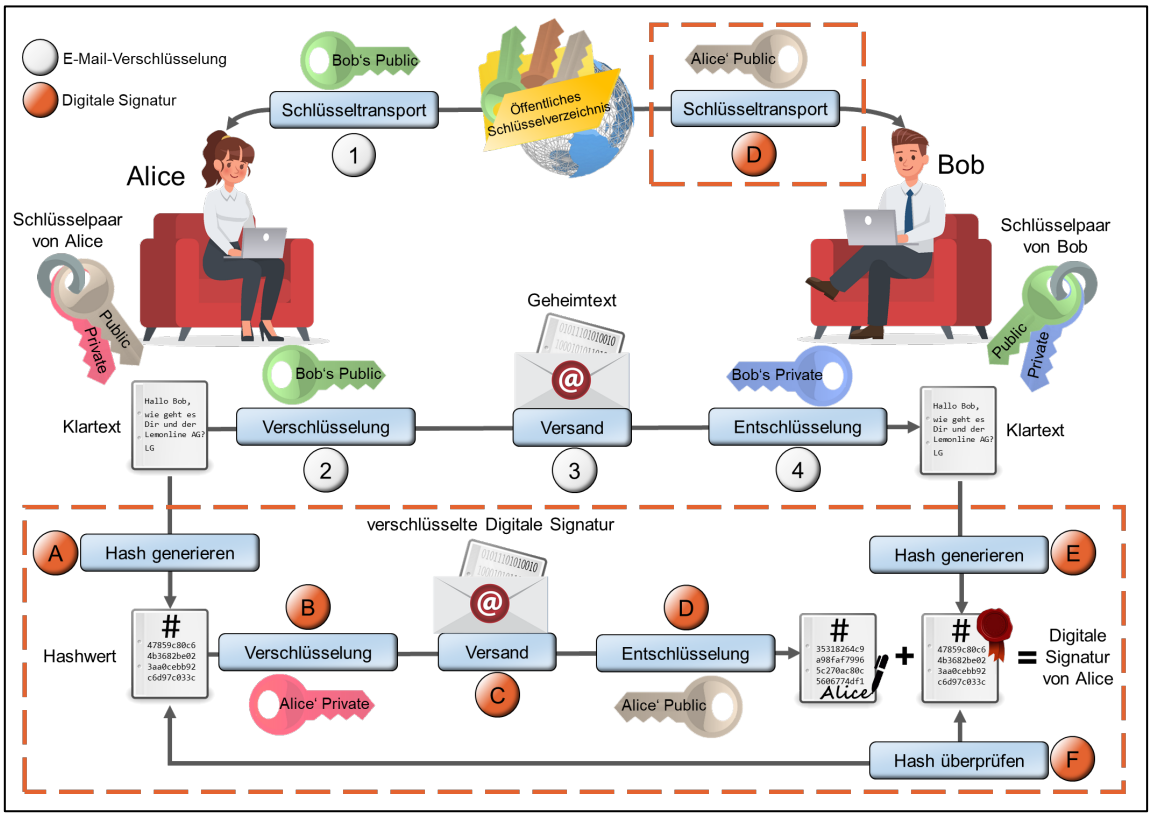



Abb. 13: Das Prinzip der digitalen Signatur auf Basis des RSA-Verfahrens[62]

(A) Alice und Bob erstellen sich jeweils ein Schlüsselpaar. Beide hinterlegen ihre öffentlichen Schlüssel in einem öffentlichen Schlüsselverzeichnis. Die privaten Schlüssel behalten Alice und Bob für sich.

61 Vgl. Beutelsbacher, Albrecht: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, a. a. O., S. 111f und vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 176.

62 Eigene Abbildung in Anlehnung an Gramm, Andreas: Integrität einer Nachricht und Authentizität ihres Absenders mit einer digitaler Unterschrift sicherstellen, Online im Internet: http://it-lehren.de/asym/Integritaet-und-Authentizitaet-mit-digitaler-Unterschrift-sicherstellen.html, 2010.

(B) Alice möchte ihrer Nachricht eine digitale Signatur beifügen. Dafür muss sie den Klartext ihrer Nachricht in eine Hashfunktion eingeben. Der entstandene Hashwert ist einzigartig und lässt keinerlei Rückschlüsse auf den Inhalt ihrer Nachricht zu.

(C) Alice verschlüsselt den Hashwert mit ihrem privaten Schlüssel. Dadurch signiert Alice ihre Nachricht und hat ihre digitale Signatur erfolgreich generiert.

(D) Alice sendet die digitale Signatur, wie ihren verschlüsselten Geheimtext (Schritt 3), ebenfalls per E-Mail an Bob. Sie kann ihre Identität durch die digitale Signatur jetzt nicht mehr abstreiten (Verbindlichkeit).

(E) Gelingt es Bob die digitale Signatur von Alice mit ihrem öffentlichen Schlüssel zu entschlüsseln, bestätigt diese Tatsache die Identität von Alice (Authentizität). Bob kann die digitale Signatur ausschließlich mit dem öffentlichen Schlüssel von Alice entschlüsseln, da nur sie die Eigentümerin des Schlüsselpaars ist (Schritt B).

(F) Unmittelbar nachdem Bob die Nachricht von Alice mit seinem privaten Schlüssel entschlüsselt hat (Schritt 4), generiert er aus diesem Klartext erneut einen Hashwert.

(G) Bob vergleicht nun die entschlüsselte digitale Signatur von Alice bzw. den Hashwert der Originalnachricht (Schritt D) mit seinem soeben nachträglich erstellten Hashwert (Schritt E). Sind beide Hashwerte identisch weiß Bob, dass die Nachricht auf dem Transportweg zu ihm nicht verändert wurde (Integrität). Die kleinste Veränderung der ursprünglichen Nachricht während dem Versand (Schritt 3) hätte den Hashwert fundamental verändert. Beide Hashwerte sind identisch. Die digitale Signatur von Alice ist somit vollständig und einwandfrei.

Möchten Alice und Bob ihre E-Mails asymmetrisch verschlüsseln und digital signieren, können sie die dafür benötigten Schlüsselpaare mithilfe frei zugänglicher Verschlüsselungssoftware selbstständig generieren. Sobald sie ihren öffentlichen Schlüssel miteinander ausgetauscht haben und anschließend ordnungsgemäß zur Verschlüsselung nutzen, kann ihre Kommunikation als sicher und vertrauensvoll eingestuft werden. Dieses direkte Vertrauensmodell sieht vor, dass Alice vorab sich selbst und die Echtheit ihres öffentlichen Schlüssels gegenüber Bob bzw. ihrem Empfängerkreis im Netz bestätigt (Web of Trust).[63]

Damit Vertrauen durch asymmetrische Verschlüsselungsverfahren auch beim alltäglichen Surfen im Web gewährleistet werden kann, wird eine Public-Key-Infrastruktur (PKI) benötigt. Die PKI interpretiert das Wort Vertrauen im technischen Sinne so: Autorisierte Zertifizierungsbehörden, engl. Certification Authorities (CA), stellen einerseits die einzigartigen asymmetrischen Schlüsselpaare bereit und bestätigen darüber hinaus die Identität von Personen und Un-

63 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 216f und 565f.

ternehmen bzw. deren Web Server. Eine Analogie einer CA wäre beispielsweise ein Einwohnermeldeamt, welches sowohl Personalausweise ausstellt als auch An, Ab- und Ummeldungen registriert. Die zentralen Aufgaben einer CA werden im deutschsprachigem Raum auch unter dem Pseudoanglizismus Trust Center zusammengefasst. Wird eine Web Site aufgerufen, kann ein Web Browser über das vorliegende Zertifikat der CA die Web Site implizit als vertrauenswürdig einstufen. Möglich wird dies durch Zertifikatslisten, welche direkt in Web Browsern implementiert werden. Durch dieses hierarchische Vertrauensmodell der PKI, kann eine CA für die Echtheit von Organisationen und Individuen garantieren und sorgt mit den Zertifikaten und digitalen Signaturen der Schlüsselpaare für mehr Vertrauen und Verbindlichkeit bei der Kommunikation im Web. Eine CA ist somit als Kontrollorgan für eine funktionierende PKI und zur Wahrung der IT-Sicherheitsziele im Web notwendig (Hierarchical Trust).[64]

### 3.3.3 Vor- und Nachteile der asymmetrischen Verfahren

Asymmetrische Verfahren stellen vor allem sicher, dass ein Teil des Schlüsselpaars öffentlich transportiert werden kann, wodurch das seit Jahrtausenden bestehende Schlüsselaustauschproblem behoben wird. Alice und Bob können nun ihre öffentlichen Schlüssel über einen unverschlüsselten Kanal schicken oder sie in einem öffentlichen Schlüsselverzeichnis ablegen. Der andere Schlüssel des Paars muss stets privat bleiben und sollte deswegen geheim gehalten werden.

Asymmetrische Verschlüsselungsverfahren werden selten verwendet, um gesamte Nachrichten oder große Datenmengen zu verschlüsseln. Stattdessen spielen sie eine zentrale Rolle für den sicheren Schlüsselaustausch in der PKI. In der Praxis werden asymmetrische Verfahren wie RSA häufig zusammen mit einem symmetrischen Verfahren wie AES verwendet. RSA regelt den Schlüsselaustausch und die Verifizierung einer digitalen Signatur, wohingegen AES die eigentliche Verschlüsselung der Daten mit einem zusätzlichen geheimen Schlüssel übernimmt. Es entsteht ein hybrides Verschlüsselungsverfahren, welches im nächsten Kapitel erläutert wird.

64 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Theorie und Praxis, a. a. O., S. 193, vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 575 und 579 und vgl. Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: Kryptographie und IT-Sicherheit – Grundlagen und Anwendungen, a. a. O., S. 166.

Die Vor- und Nachteile der asymmetrischen Verfahren werden in der nachfolgenden Tabelle erneut zusammengefasst und schließen zugleich das Kapitel der asymmetrischen Verschlüsselungsverfahren:[65]

| **Asymmetrische Verschlüsselungsverfahren** | |
|---|---|
|  | |
| **Vorteile** | **Nachteile** |
| + Der Schlüsseltransport des öffentlichen Schlüssels kann über einen unsicheren Kanal erfolgen<br>+ Ein einzigartiges asymmetrisches Schlüsselpaar pro Kommunikationsteilnehmer erleichtert das Schlüsselmanagement gegenüber dem symmetrischen Verfahren enorm<br>+ Das RSA-Verfahren und die Public-Key-Infrastruktur gewährleisten die Integrität, Authentizität und Verbindlichkeit durch Zertifikate und digitale Signaturen | – Sehr rechenintensiv und um ein Vielfaches langsamer als symmetrische Verfahren (ca. um den Faktor 1000) |

Tab. 2: Vor- und Nachteile von asymmetrischen Verschlüsselungsverfahren

[65] Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 178.

## 3.4 Hybride Verschlüsselungsverfahren

### 3.4.1 Hybrid verschlüsselte Kommunikation von Alice und Bob

Die Kombination von symmetrischen und asymmetrischen Verfahren sind die hybriden Verschlüsselungsverfahren. Sie bedienen sich aus sämtlichen Teilgebieten der Kryptografie. Abbildung 14 zeigt das hybride Verschlüsselungsverfahren exemplarisch am Beispiel von Alice und Bob:

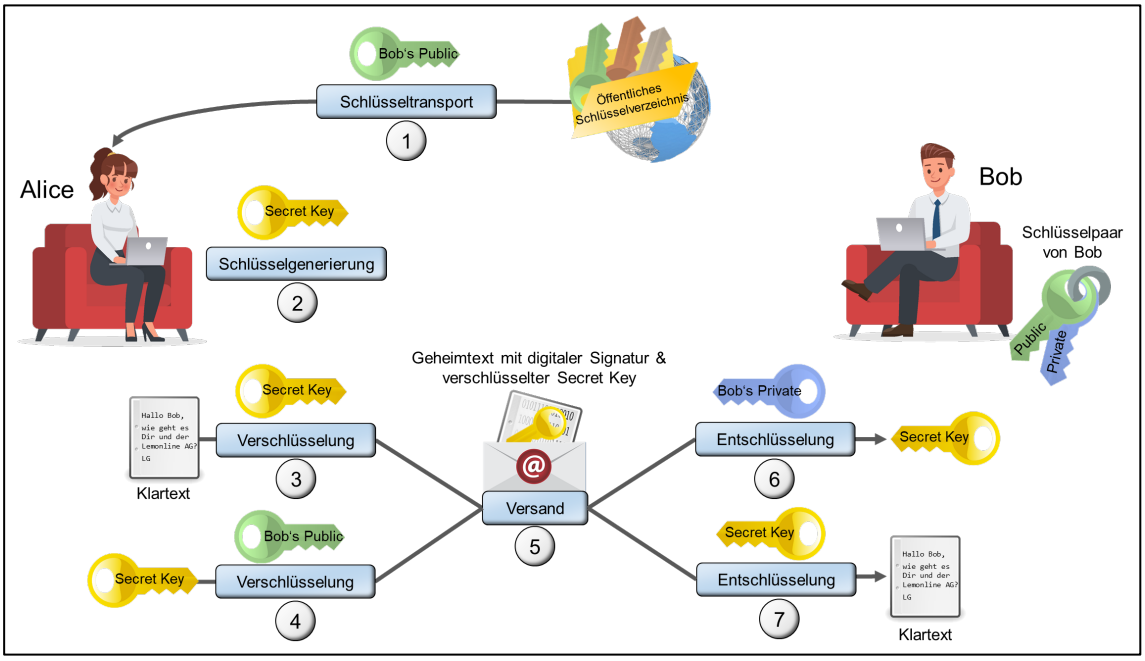



Abb. 14: Hybrides Verschlüsselungsverfahren

(1) Alice beschafft sich den öffentlichen asymmetrischen Schlüssel von Bob aus einem öffentlichen Schlüsselverzeichnis.

(2) Alice generiert einen geheimen symmetrischen Schlüssel für die zukünftige Kommunikation mit Bob.

(3) Alice schreibt eine Nachricht in Klartext. Sie erstellt auch ihre digitale Signatur (vgl. Abbildung 13). Alice verschlüsselt die Nachricht mit dem generierten geheimen Schlüssel. Die Nachricht wird in Geheimtext umgewandelt.

(4) Alice verschlüsselt den geheimen Schlüssel mit dem öffentlichen Schlüssel von Bob.

(5) Alice versendet die verschlüsselte Nachricht zusammen mit ihrer digitalen Signatur und dem verschlüsselten geheimen Schlüssel per E-Mail an Bob.

(6) Bob entschlüsselt den geheimen Schlüssel mit seinem privaten Schlüssel. Bob überprüft auch die digitale Signatur von Alice (siehe Abbildung 13).

(7) Danach entschlüsselt Bob die Nachricht von Alice mit dem geheimen Schlüssel.

Das hybride Verfahren sorgt dafür, dass Alice und Bob einen symmetrischen AES-Schlüssel für ihre verschlüsselte Kommunikation verwenden können. Mithilfe des asymmetrischen RSA-Verfahrens kann der symmetrische Schlüssel, mit dem die Nachricht verschlüsselt wurde, von Alice zu Bob transportiert werden. Das RSA-Verfahren hat jedoch einen Nachteil. Alice und Bob sind zwar theoretisch Eigentümer der privaten Schlüssel, jedoch praktisch nicht die Besitzer des RSA-Schlüsselpaars. Das gesamte RSA-Schlüsselpaar ist häufig in der Hand von externen Dienstleistern im Web. Die privaten Schlüssel könnten von unbefugten Personen oder von Angreifern entnommen werden. Wenn eine Person den privaten Schlüssel von Alice oder Bob in die Hände bekommen sollte, würde er damit den geheimen AES-Schlüssel entschlüsseln. In diesem Fall wäre die Vertraulichkeit der Kommunikation rückwirkend und zukünftig erheblich bedroht. Aus diesem Grund werden einmalig erstellte RSA-Schlüsselpaare für den Transport des geheimen symmetrischen AES-Schlüssels nicht mehr empfohlen.[66]

Das Verfahren von Diffie und Hellman – den beiden Pionieren der asymmetrischen Kryptografie – ergänzt daher das RSA-Verfahren mit einer notwendigen Methode, vergängliche Schlüssel für den Transport zu vereinbaren und keine starren RSA-Schlüsselpaare zu verwenden. Der RSA-Schlüsseltransport bleibt jedoch weiterhin ein solides Prüfverfahren für digitale Signaturen (vgl. Abbildung 13). Das Repertoire der hybriden Verfahren wird durch die Diffie-Hellman-Schlüsselvereinbarung lediglich komplementiert.[67]

### 3.4.2 Die vergängliche Diffie-Hellman-Schlüsselvereinbarung

Die Diffie-Hellman-Schlüsselvereinbarung unterscheidet sich zu den oben genannten starren Schlüsselpaaren des RSA-Verfahrens dahingehend, dass lediglich das Zwischenergebnis einer Rechenoperation ausgetauscht wird und nicht der geheime Schlüssel selbst. Was bei RSA die personengebundenen starren Schlüsselpaare waren, sind bei Diffie-Hellman also sehr komplexe aber flexible Rechenoperationen. Auf Basis dieser komplexen Berechnungen einigen sich Alice und Bob auf einen geheimen symmetrischen Sitzungsschlüssel, engl. session key.[68] Dieser Sitzungsschlüssel gilt nur für „eine“ Interaktion zwischen Client und Server und verfällt nach Beendigung einer Kommunikation. Der Verlust eines geheimen Sitzungsschlüssels würde keine schwerwiegenderen Folgen nach sich ziehen, da nur ein Bruchteil der Kommunikation offen

66 Vgl. Ronen, Eyal; Gillham, Robert; Genkin, Daniel; Shamir, Adi; Wong, David; Yarom, Yuval: The 9 Lives of Bleichenbacher's CAT – New Cache ATtacks on TLS Implementations, in: IEEE Symposium on Security & Privacy, 2019.

67 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 235 und vgl. Ristić, Ivan: Bulletproof SSL and TLS – Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, London: Feisty Duck 2015, S. 38.

68 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 200f.

läge. Diese Folgenlosigkeit bzw. perfekte Vorwärtssicherheit, engl. Perfect Forward Secrecy (PFS), dieses Verfahrens wird Diffie-Hellman Ephemeral (DHE) genannt.[69]

Das DHE-Verfahren ist in Abbildung 15 dargestellt. Die mathematischen Grundlagen sind bewusst vereinfacht und durch Farben ersetzt worden, jedoch bleibt das Grundprinzip von DHE unverändert. Alice und Bob mischen sich ihre Farben entsprechend einer definierten Vorgabe, um eine gemeinsame Farbe (den Sitzungsschlüssel) zu erhalten:[70]

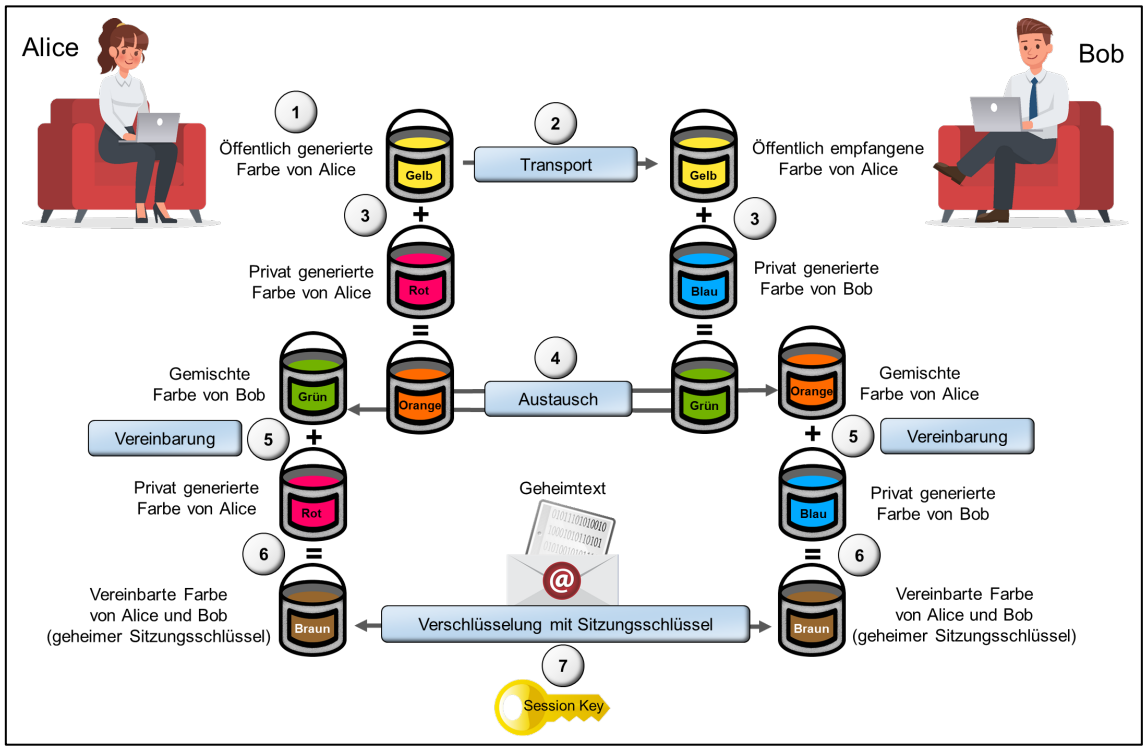



Abb. 15: Die vergängliche Diffie-Hellman-Schlüsselvereinbarung

(1) Alice generiert eine neue zufällige Farbe. Diese Farbe ist Gelb.

(2) Alice teilt die Farbe Gelb über einen öffentlichen Transportweg mit Bob.

(3) Alice und Bob generieren daraufhin jeweils eine persönliche Farbe. Die Farbe von Alice ist Rot, die von Bob ist Blau. Diese Farben bleiben privat, werden jedoch von beiden mit der öffentlichen Farbe Gelb vermischt.

(4) Alice mischt ihre Farbe Rot mit der Farbe Gelb und erhält Orange. Bob mischt seine Farbe Blau mit der Farbe Gelb und erhält Grün. Beide tauschen ihre gemischten Farben anschließend öffentlich miteinander aus.

69 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 389.

70 Eigene Abbildung in Anlehnung an Chapple, Mike: CISSP Cert Prep: 3 Security Architecture and Engineering, Online im Internet: https://www.linkedin.com/learning/cissp-cert-prep-3-security-architecture-and-engineering/diffie-hellman, 08.03.2018.

(5) Alice und Bob vereinbaren, dass sie die getauschte Farbe mit der eigenen privaten Farbe vermischen werden. Alice und Bob wissen dadurch implizit, dass sie gemäß ihrer Vereinbarung beide dieselbe Farbe mischen werden.

(6) Alice mischt daher die erhaltene Farbe Grün mit ihrer privaten Farbe Rot. Auch Bob mischt die erhaltene Farbe Orange mit seiner privaten Farbe Blau. Sowohl Alice als auch Bob haben sich an die Abmachung gehalten. Beide erhalten die vereinbarte Farbe Braun. Diese geheime Farbe ist für einen Außenstehenden (mathematisch) nicht nachzuvollziehen. Dieser hat nur den öffentlichen Transport von Gelb, Orange und Grün mitbekommen, kennt aber nicht die von Alice und Bob privat generierten Farben (Schritt 3).

(7) Aus diesem Grund benutzen Alice und Bob nun ihre gemeinsame Farbe Braun als geheime Farbe (geheimen Sitzungsschlüssel) für ihre Kommunikation.

Die oben beschriebene Abbildung wirkt unter Berücksichtigung der Farbenlehre stark vereinfacht und fehleranfällig. Für einen Außenstehenden wäre es ein Leichtes, bei Kenntnis der öffentlichen Ausgangsfarbe Gelb sowie den getauschten Farben Orange und Grün, durch das Gesetz der Farbmischung auf die privaten Farben Rot und Blau zu schlussfolgern. In der Praxis ist das durch Einweg- und Falltürfunktionen unmöglich.[71]

Sowohl RSA als auch DHE sind asymmetrische Verfahren. Die Verfahren unterscheiden sich in ihrem methodischen Ansatz und in ihren unterschiedlichen Algorithmen und Rechenoperationen. Wohingegen RSA sein schweres Berechnungsproblem durch die Faktorisierung von großen Primzahlen erzeugt, nutzt DHE Potenzen bzw. die daraus schwer zu berechnenden diskreten Logarithmen. Auch elliptische Kurven und die Addition von Schnittpunkten können verwendet werden, um sich auf einen gemeinsamen Sitzungsschlüssel für die Verschlüsselung von Daten zu einigen (Elliptic-Curve Diffie-Hellman Ephemeral, ECDHE).[72]

Die in Abbildung 15 generierte Ausgangsfarbe Gelb wird in der Realität zufällig über einen sogenannten Pseudorandom Number Generator (PRNG) erstellt und Pre-Master Secret (PMS) genannt. Ist die Kommunikation zwischen Alice und Bob durch das PMS auf Basis des asymmetrischen DHE-Verfahrens eröffnet, wird im weiteren Verlauf der Kommunikation der vereinbarte symmetrische Schlüssel zur eigentlichen Verschlüsselung der Informationen verwendet. Dieser geheime Schlüssel ist der Sitzungsschlüssel und wird auch Master Secret (MS) genannt. Mit jedem Verbindungsaufbau im Web wird durch ein PRNG ein anderes PMS generiert und so ein einzigartiges MS erzeugt. Alice und Bob einigen sich somit bei jedem Kommunikationsaufbau auf einen neuen vergänglichen geheimen symmetrischen Sitzungsschlüssel. Wenn

71 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 199.

72 Vgl. Ristić, Ivan: Bulletproof SSL and TLS – Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, a. a. O., S. S. 40.

eine unbefugte Person den geheimen Sitzungsschlüssel zufällig in die Hände bekommen sollte, kann nur der Inhalt der letzten Sitzung entschlüsselt werden.[73]

Dieser Zufall kann allerdings durch einen menschlichen Fehler bzw. eine fehlerhafte Implementierung der Verschlüsselung begünstigt werden. Schwachstellen in für sicher deklarierten IT-Systemen und Anwendungen können dazu führen, dass vertrauliche Informationen abgehört und Kommunikationsverläufe mitgelesen werden (passiver Angriff). Ein Angreifer kann den Schlüsselaustausch und somit das gesamte hybride Verfahren aber auch vorsätzlich manipulieren (aktiver Angriff). Bei einer sogenannten Man-in-the-Middle-Attacke (MITM-Attacke) würde ein Angreifer den öffentlichen Schlüsselaustausch (die Farben Gelb, Orange und Grün in Abbildung 15) abfangen und dieses PMS durch ein eigenes ersetzen. Ein Angreifer vereinbart dann praktisch mit sich selbst einen geheimen Sitzungsschlüssel und lässt Alice und Bob im Irrglauben, dass sie sich ungestört auf einen gemeinsamen Sitzungsschlüssel geeinigt hätten. Eine MITM-Attacke kann ein hybrides Verschlüsselungsverfahren also so weit manipulieren, dass sich Alice und Bob gar nicht erst auf ein Verschlüsselungsverfahren einigen können (Downgrade-Attacke). Ihre Kommunikation im Web verläuft dann gezwungenermaßen nur schwach oder gar nicht verschlüsselt.[74]

In der Praxis werden MITM-Attacken auf die Schlüsselvereinbarung des oben gezeigten DHE-Verfahrens durch die Verknüpfung mit dem RSA-Signatursystem zwar erschwert, sind aber nicht gänzlich auszuschließen. Diese „Schwachstelle“ ist typisch für asymmetrische Verfahren, ist jedoch im direkten Vergleich bei weitem nicht so drastisch wie das Schlüsselaustauschproblem der symmetrischen Verschlüsselungsverfahren.[75]

### 3.4.3 Vor- und Nachteile der hybriden Verschlüsselung

Bei der Betrachtung der vorherigen Kapitel wird deutlich, dass die symmetrischen und asymmetrischen Algorithmen spezifische Vor- und Nachteile bieten. Um das Beste aus beiden Verfahren nutzen zu können, werden in der Praxis hybride Verschlüsselungsverfahren verwendet, um die Vorzüge aller kryptografischen Verfahren zu kombinieren.

Asymmetrische Verfahren werden eingesetzt, um einen vergänglichen Sitzungsschlüssel zu vereinbaren (DHE) und unterstützen die Kommunikation im Web zusätzlich mit digitalen Signaturen (RSA). Die symmetrischen Sitzungsschlüssel (AES) werden für die Verschlüsslung des

73 Vgl. Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: Kryptographie und IT-Sicherheit – Grundlagen und Anwendungen, a. a. O., S. 178.

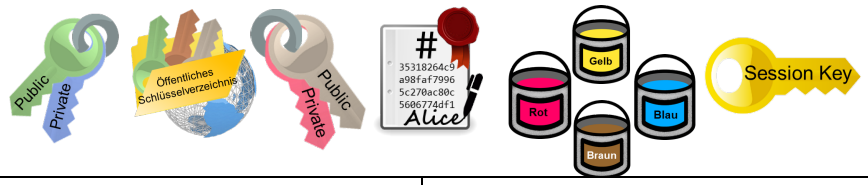
74 Vgl. Schäfer, Günter; Roßberg, Michael: Netzsicherheit – Grundlagen & Protokolle, a. a. O., S. 10f und vgl. Ristić, Ivan: Bulletproof SSL and TLS – Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, a. a. O., S. 40.

75 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, a. a. O., S. 390f.

vertraulichen Inhalts einer Kommunikation genutzt, beispielsweise für E-Mails und andere elektronische Informationen. Die Verschlüsselung von größeren Datenmengen mit dem rechenintensiven asymmetrischen Verfahren wird dadurch umgangen. Asymmetrische Verfahren werden also dafür genutzt, um Informationen von überschaubarer Dateigröße zu verschlüsseln. Die Schlüsselpaare und die digitalen Signaturen sind hinsichtlich ihrer Dateigröße perfekt geeignet, um sie asymmetrisch zu verschlüsseln bzw. zu signieren und transportieren zu können.

In Kombination bildet das symmetrische Verfahren AES, die Hashfunktionen für digitale Signaturen, die asymmetrischen Verfahren RSA und DHE ein solides Konglomerat an kryptografischen Verfahren, welche gebündelt in moderne Netzwerkprotokolle eingebettet werden können. Das nächste Kapitel beschreibt diese Anwendungsgebiete im Web.

Die Vor- und Nachteile der hybriden Verschlüsselungsverfahren werden in der nachfolgenden Tabelle erneut zusammengefasst und schließen zugleich das Kapitel der Verfahren der hybriden Verschlüsselung:

| **Hybride Verschlüsselungsverfahren** | |
|---|---|
|  | |
| **Vorteile** | **Nachteile** |
| + Die DHE-Schlüsselvereinbarung erzeugt einen geheimen symmetrischen Sitzungsschlüssel und bietet Perfect Forward Secrecy (Vertraulichkeit)<br><br>+ Das RSA-Signatursystem bestätigt die Identität von Personen (Authentizität) und prüft Informationen auf Unversehrtheit (Integrität) und macht sie zudem rechtsgültig (Verbindlichkeit)<br><br>+ Hohe Geschwindigkeit bei der Ver- und Entschlüsselung des Sitzungsschlüssels durch das effizienten symmetrische AES-Verfahren | – Die Bedrohung durch potentielle Man-in-the-Middle-Attacken werden durch digitale Signaturen zwar erschwert, sind jedoch nicht immer zu vermeiden<br><br>– In der Praxis möglicherweise anfällig für Anwendungs- und Implementierungsfehler durch die Komplexität der hybriden Verschlüsselungsverfahren |

Tab. 3: Vor- und Nachteile von hybriden Verschlüsselungsverfahren

# 4 Anwendungsgebiete der hybriden Verschlüsselung

## 4.1 Systematisierung der Anwendungsgebiete

Das Grundlagenkapitel hat bereits skizziert, dass die Kommunikation im Internet durch Netzwerkprotokolle zwar systematisiert stattfindet, jedoch nicht automatisch durch Verschlüsselung abgesichert ist. In den vorangegangenen Kapiteln der Verschlüsselungsverfahren wurde deutlich, dass eine Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren und digitalen Signaturen das Mittel der Wahl ist. Dieses Kapitel nimmt daher Bezug auf die zentralen Anwendungsgebiete der hybriden Verschlüsselungsverfahren im Web. Der Fokus liegt dabei auf den Netzwerkprotokollen der oberen vierten und dritten Schicht des TCP/IP-Referenzmodells. Die unverschlüsselten Architekturschichten des Modells sind erneut in Abbildung 16 zu sehen:

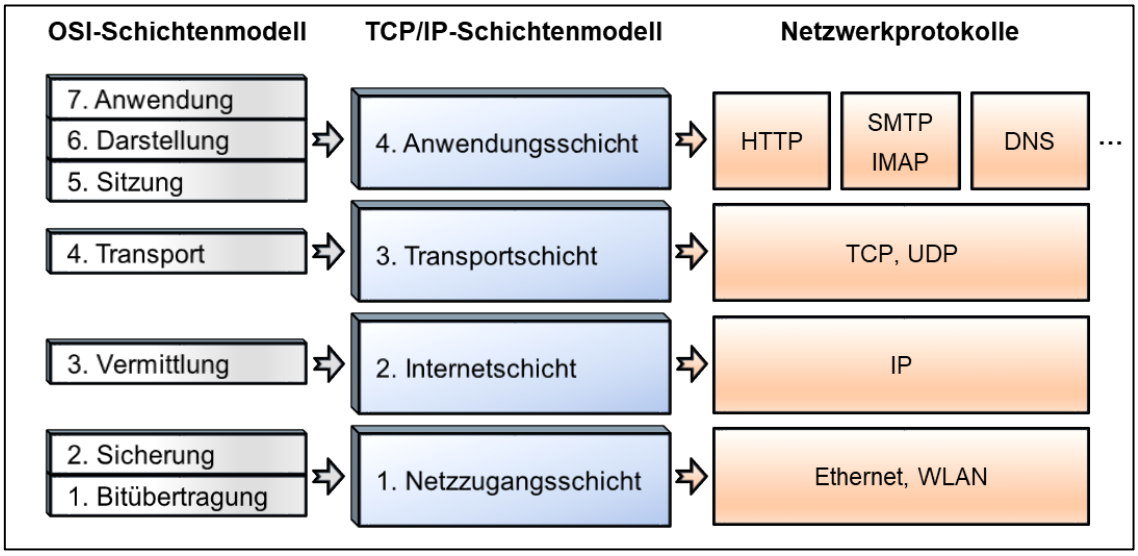



Abb. 16: Das OSI- und TCP/IP-Modell und die Netzwerkprotokolle

**Kapitel 4.2:** Verschlüsselte Netzwerkprotokolle und Cipher Suites im Web

Das zweite Unterkapitel greift die vierte Anwendungsschicht und die dritte Transportschicht des TCP/IP-Modell auf und ergänzt bzw. verknüpft diese Schichten mit dem Verschlüsselungsprotokoll TLS. Die im Rahmen dieser Arbeit vorgestellten hybriden Verschlüsselungsverfahren finden in diesem Verschlüsselungsprotokoll Anwendung. Sogenannte Cipher Suites definieren die Zusammenstellung der verwendeten kryptografischen Verfahren von verschlüsselten Netzwerkprotokollen. Cipher Suites standardisieren den Einsatz der hybriden Verschlüsselungsverfahren bereits bei dem Verbindungsaufbau einer Kommunikation zwischen Client und Server.

**Kapitel 4.3:** Der Transport Layer Security Handshake zwischen Alice und Bob

Das dritte Unterkapitel beschreibt den Aufbau des TLS-Protokolls der Version 1.2. Dabei wird das TLS-Handshake-Protokoll schrittweise erläutert. Dieser Prozess kann erneut durch die Figuren Alice und Bob veranschaulicht werden. Dieses Mal sendet Alice keine Nachricht per E-Mail, sondern ruft mit ihrem Web Browser den verschlüsselten Web Shop der Lemonline AG von Bob auf.

**Kapitel 4.4:** Anwendungsbeispiel: Verbindung einer verschlüsselten Web Site

Das vierte Kapitel bebildert einen alltäglichen Berührungspunkt mit hybrider Verschlüsselung: Das „Browsen“ im Web. Dabei wird auf die Zertifikate von Web Sites und die Verbindungen von Web Browsern mithilfe des TLS- bzw. HTTPS-Protokolls eingegangen. Beispielhaft wird der verschlüsselte Einkauf in einem Web Shop skizziert.

**Kapitel 4.5:** Anwendungsbeispiel: Versand einer verschlüsselten E-Mail

Das fünfte Kapitel zeigt, dass E-Mails zwar mithilfe des TLS-Protokolls „automatisch“ verschlüsselt werden, jedoch nur auf dem Transportweg. Deswegen wird zwischen der Server-basierten und der Client-basierten E-Mail-Verschlüsselung unterschieden. In diesem Zusammenhang werden auch die Ende-zu-Ende-Verschlüsselung, und die Konfiguration eines E-Mail-Clients erläutert. Mit dem hybriden E-Mail-Standard PGP (Pretty Good Privacy) kann Alice ihre E-Mails „eigenhändig“ hybrid verschlüsseln.

## 4.2 Verschlüsselte Netzwerkprotokolle und Cipher Suites im Web

Verschlüsselungsverfahren definieren unter anderem den Schlüsselaustausch oder -transport bzw. die Schlüsselvereinbarung der symmetrischen, asymmetrischen und hybriden Verschlüsselung. Sie stellen zudem die mathematischen Operatoren und Algorithmen für die Schlüsselerstellung und Verschlüsselung und Entschlüsselung der Informationen bereit. Kryptografische Netzwerkprotokolle sorgen für die hybrid verschlüsselte Übertragung von digitalen Informationen. Im Optimalfall gewährleistet ein hybrides Verschlüsselungsprotokoll – wie auch schon das zugrundeliegende hybride Verschlüsselungsverfahren – alle Schutzziele der IT-Sicherheit: Die Vertraulichkeit, Authentizität, Integrität und die Verbindlichkeit der übertragenen Daten (vgl. Kapitel 2.4). Verschlüsselte Netzwerkprotokolle ermöglichen somit eine sichere Kommunikation zwischen zwei Teilnehmern im Web.

Ein regelmäßig im Web verwendetes hybrides Verschlüsselungsprotokoll ist TLS. Das TLS-Protokoll ist landläufig auch unter seiner Vorgängerversion mit dem Namen SSL (Secure Socket Layer) bekannt. Die Begriffe werden häufig synonym verwendet. In den 1990er Jahren wurde das SSL-Protokoll von der Firma Netscape Communications mit dem primären Ziel entworfen, die HTTP-Sitzungen des unternehmenseigenen Web Browser zu sichern. Seit 1996

wird SSL von allen Web-Browser-Anbietern als Standardprotokoll zur Sicherung des HTTP-Verkehrs im Web eingesetzt. Obwohl SSL in seiner Entstehungsgeschichte als Sicherheitsprotokoll für HTTP gilt, kann es zur Sicherung aller Protokolle der Anwendungsschicht dienen, welche die Netzwerkprotokolle TCP und UDP der Transportschicht nutzen. Die Organisation IETF entschied deswegen zukünftige SSL-Versionen mit dem Namen *Transport Layer* Security (TLS) zu veröffentlichen. TLS 1.0 erschien 1999 und die Versionen 1.1 und 1.2 wurden im Jahr 2006 und 2008 veröffentlicht. Ende 2018 publizierte die IETF das TLS-Protokoll in der Version 1.3. Neben HTTP werden auch andere Netzwerkprotokolle der obersten Anwendungsschicht durch TLS verschlüsselt, zum Beispiel die E-Mail-Protokolle SMTP und IMAP für das sichere Versenden und Empfangen von E-Mails. Eine sichere Verbindung wird häufig durch das Kürzel „**S**“ für **Secure** im Protokollnamen gekennzeichnet (HTTP**S**, SMTP**S** und IMAP**S**). Auch der Internetdienst DNS, der die Web Browser Anfragen in IP-Adressen auflöst, kann mit TLS verschlüsselt werden (DNS over TLS).[76]

Abbildung 17 zeigt, wie sich das TLS-Protokoll zwischen die Anwendungsschicht und die darunterliegende Transportschicht des TCP/IP-Modells eingliedert. TLS bildet einen sicheren Bezugspunkt für die Protokolle der Transportschicht. TCP wird in TLS und UDP zu DTLS (Datagram Transport Layer Security) überführt.[77] TLS untermauert zudem die Protokolle der Anwendungsschicht mit hybriden Verschlüsselungsverfahren. Das TLS-Protokoll ist geschichtet aufgebaut und die einzelnen Bestandteile – das Record-, Alert-, Change-Cipher-Spec- und Handshake-Protokoll – werden nachfolgend erläutert:[78]

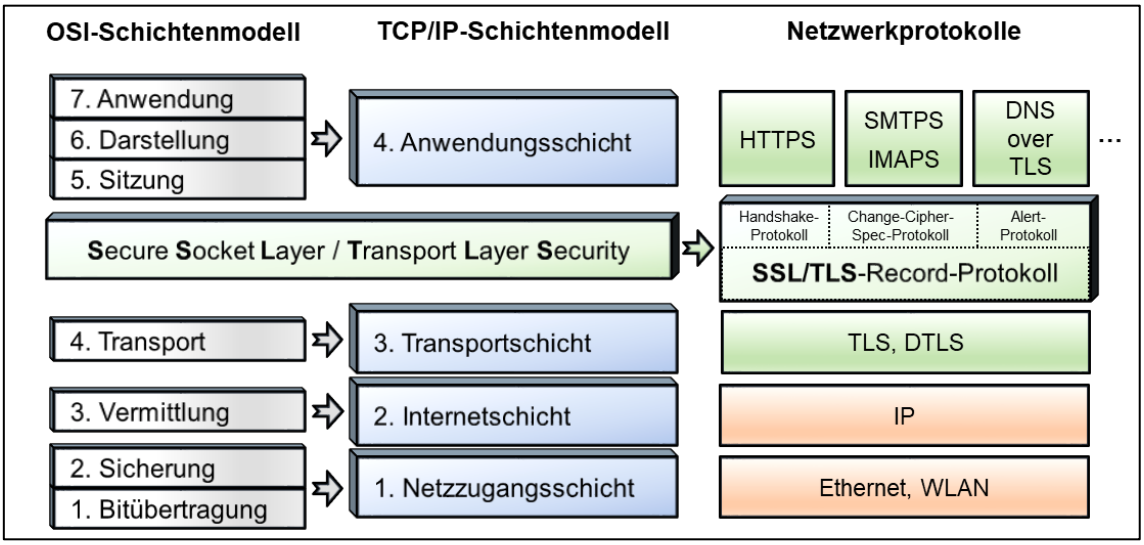



Abb. 17: Das Transport-Layer-Security-Protokoll im OSI- und TCP/IP-Modell

76 Vgl. Schäfer, Günter; Roßberg, Michael: Netzsicherheit – Grundlagen & Protokolle, a. a. O., S. 342.

77 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Theorie und Praxis, a. a. O., S. 145f.

78 Eigene Abbildung in Anlehnung an Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 671f und 720f.

Das TLS-Record-Protokoll bereitet die zu verschlüsselnden Informationen systematisch in Klartextblöcke auf, um die Daten der Anwendungsschicht geordnet an die Netzwerkprotokolle der Transportschicht übergeben zu können. Das TLS-Alert-Protokoll wird benötigt, um während einer HTTPS-Verbindung Regelverstöße oder Verbindungsabbrüche erfassen bzw. dokumentieren zu können und entsprechende Maßnahmen einzuleiten.

Eine sogenannte Cipher Suite bestimmt über die Zusammenstellung der verwendeten kryptografischen Verfahren und standardisiert deren Einsatz zwischen Client und Server. Die Kommunikationspartner einigen sich während dem HTTPS-Verbindungsaufbau bzw. während dem TLS-Handshake auf eine Cipher Suite. Die gewählte Cipher Suite wird über das Change-Cipher-Spec-Protokoll kommuniziert. Auf Basis der Cipher Suite werden Klartextinformationen verschlüsselt und anschließend im Web transportiert.[79]

Abbildung 18 zeigt ein Beispiel einer Cipher Suite des TLS-Protokolls, welche durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Kommunikation mit Perfect Forward Secrecy (PFS) empfohlen wird.[80] Die Abbildung beinhaltet alle bereits thematisierten kryptografischen Verfahren aus den vorherigen Kapiteln. Die Cipher Suite ist von links nach rechts wie folgt zu interpretieren:[81]

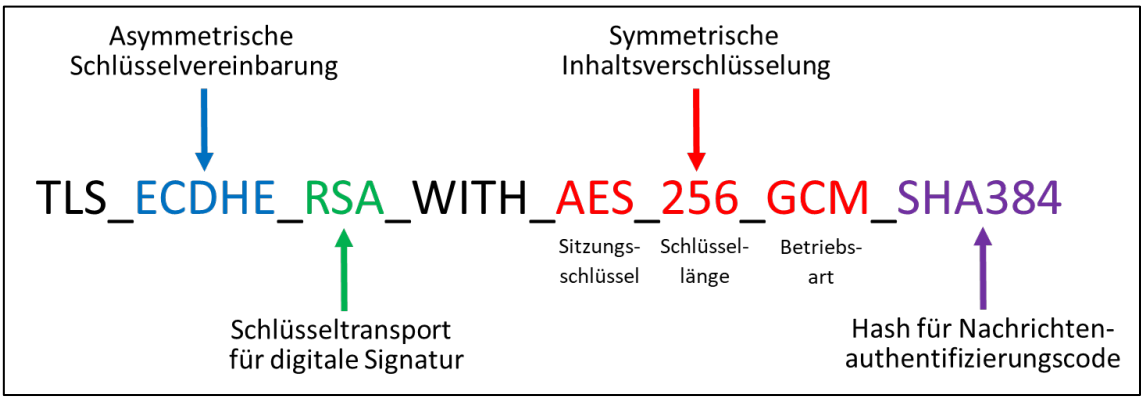



Abb. 18: Eine Cipher Suite aus dem Transport-Layer-Security-Protokoll

- Die Schlüsselvereinbarung wird mit dem vergänglichen Diffie-Hellman-Verfahren auf Basis elliptischer Kurven durchgeführt (ECDHE).
- Der Transport der asymmetrischen Schlüssel zur Überprüfung der digitalen Signatur wird mit dem RSA-Verfahren abgewickelt.

79 Vgl. Schäfer, Günter; Roßberg, Michael: Netzsicherheit – Grundlagen & Protokolle, a. a. O., S. 344f und vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 720f.

80 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Verwendung von Transport Layer Security (TLS), in: TR-02102-2, 22.02.2019, S. 8f.

81 Vgl. Ristić, Ivan: Bulletproof SSL and TLS – Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, a. a. O., S. 50f.

- Die Informationen werden durch einen symmetrischen AES-Schlüssel mit einer Länge von 256-Bit in der Betriebsart GCM (Galois/Counter Mode) verschlüsselt.
- Der Nachrichtenauthentifizierungscode für die digitale Signatur wird mit dem Hash-Algorithmus SHA-2 mit einer Zeichenlänge von 384-Bit erstellt.

Das Netzwerkprotokoll TLS und die darin enthaltenen kryptografischen Verfahren sind modular erweiterbar und die Versionen von TLS sind bis zu einem gewissen Grad abwärtskompatibel. Die Bestandteile der TLS-Zertifikate und die daran gekoppelten Cipher Suites variieren daher je nach Web Site. So wird gewährleistet, dass ein aktueller Web Browser auch mit älteren TLS-Zertifikaten einer Web Site eine verschlüsselte HTTPS-Verbindung aufbauen kann. Bei jedem HTTPS-Verbindungsaufbau vereinbart das TLS-Protokoll die exakte Zusammensetzung einer Cipher Suite und den darin enthaltenen kryptografischen Verfahren.

Das TLS-Handshake-Protokoll handelt den verschlüsselten Transport von Informationen aus. Während dem TLS-Handshake zwischen Client und Server werden die hybriden Verschlüsselungsverfahren besonders deutlich. Der TLS-Handshake wird im nachfolgenden Kapitel am Beispiel von Alice und Bob ausführlich erläutert. Alice ruft dafür den Web Shop der Lemonline AG von Bob auf. Die HTTP-Anfrage ihres Web Browsers durchläuft dabei das TCP/IP-Modell und erwartet die Antwort von Bobs Web Server (siehe Abbildung 19). Während einer HTTP-Anfrage einigen sich Client und Server auf eine Cipher Suite. Die Anfrage mündet in einer sicheren HTTPS-Sitzung.[82]

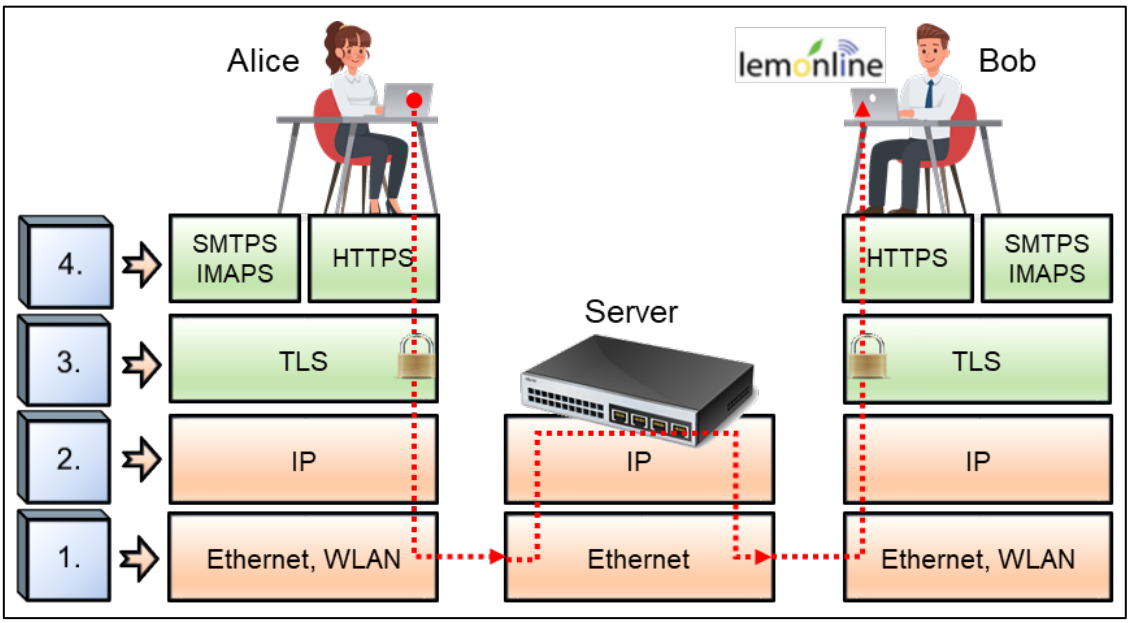



Abb. 19: Die verschlüsselte Kommunikation zwischen Alice und Bob im Web

82 Eigene Abbildung in Anlehnung an Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 720f.

## 4.3 Der TLS-Handshake zwischen Alice und Bob

Abbildung 20 zeigt den Protokollablauf des TLS-Handshakes zwischen Alice und dem Web Shop der Lemonline AG von Bob. Zur besseren Darstellung wird das TLS-Protokoll in vier Phasen unterteilt, welche nachfolgend schrittweise erläutert werden:[83]

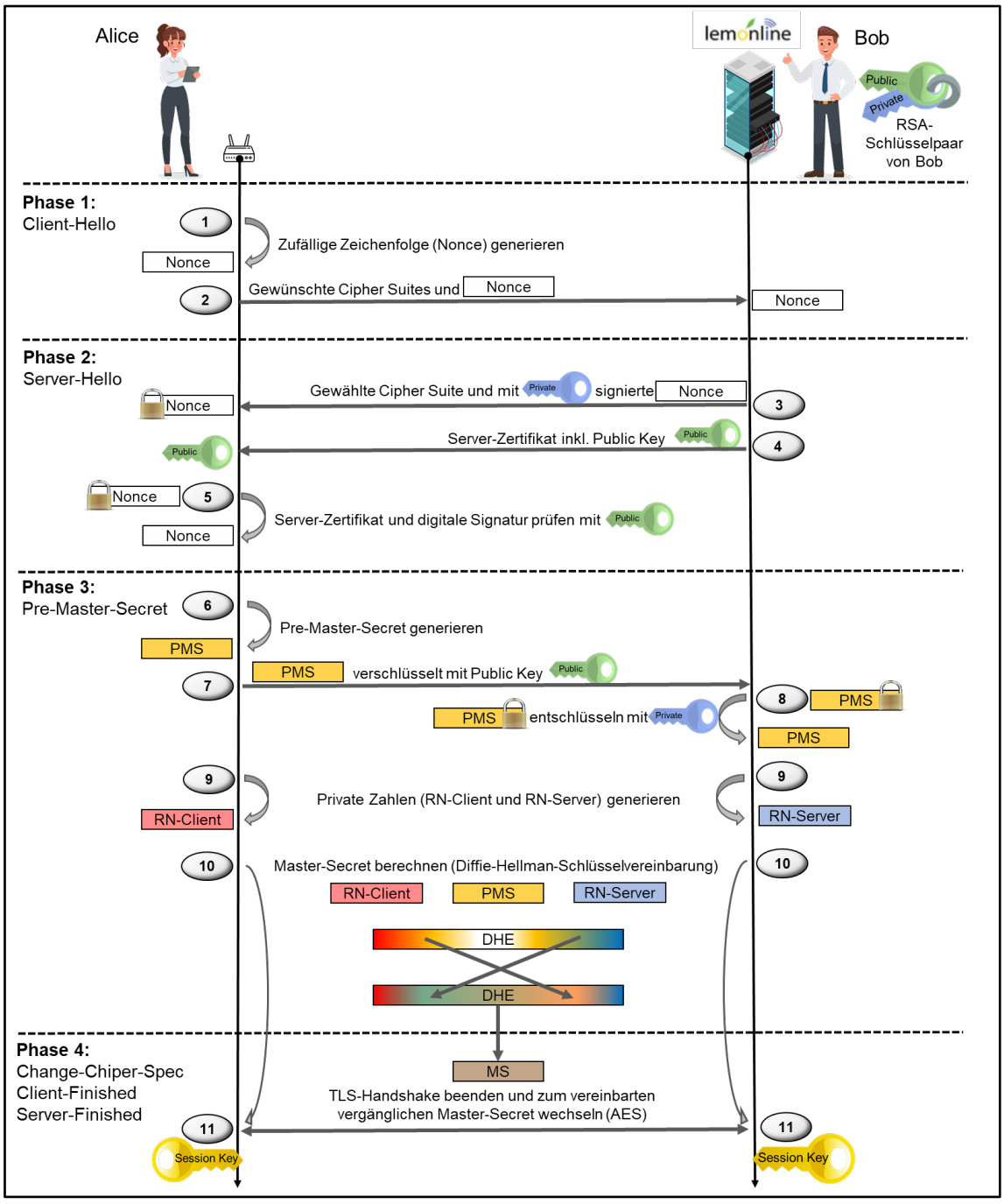



Abb. 20: TLS-Handshake zwischen Alice und dem Web Shop von Bob

83 Eigene Abbildung in Anlehnung an Martins, Filipe; Kobylinska, Anna: Supersicher – Die Neuerungen in TLS 1.3, in: iX Magazin für professionelle Informationstechnik, 08/2018, S. 112f.

**Phase 1:** Client-Hello

(1) Alice generiert eine zufällige Zeichenfolge (Nonce).

(2) Alice sendet eine „Hallo"-Nachricht an Bobs Server der Lemonline AG. Darin sind ihre gewünschten Cipher Suites enthalten. Sie fügt der Nachricht auch ihre Nonce hinzu, mit der Absicht, dass Bobs Server die Nonce digital signiert zurücksendet.

**Phase 2:** Server-Hello

(3) Bobs Server wählt eine Cipher Suite aus, die auf seinem Web Server implementiert ist. Bobs Server fügt der Nonce von Alice seine digitale Signatur mit seinem privaten Schlüssel hinzu und sendet sie in einer „Hallo"-Nachricht zurück an Alice.

(4) In der „Hallo"-Nachricht schickt Bobs Server auch das Zertifikat seines Web Servers an Alice und übermittelt ihr zusätzlich seinen öffentlichen Schlüssel.

(5) Alice überprüft zunächst, ob das Zertifikat von Bobs Server in der Zertifikatsliste ihres Web Browsers zu finden ist. Anschließend prüft Alice die digitale Signatur der Nonce mit dem öffentlichen Schlüssel von Bobs Server (vgl. Kapitel 3.3.2 Abbildung 13).

**Phase 3:** Pre-Master Secret

(6) Alice generiert ein Pre-Master Secret, um sich mit Bobs Server nachfolgend auf ein Master Secret zu einigen.

(7) Alice verschlüsselt das Pre-Master Secret zusätzlich mit dem öffentlichen Schlüssel von Bobs Server und sendet es anschließend an ihn.

(8) Bobs Server entschlüsselt das Pre-Master Secret von Alice mit seinem privaten Schlüssel.

(9) Alice und Bobs Server generieren pseudozufällige Zahlen (RN-Client und RN-Server) in Abhängigkeit des Pre-Master Secrets. Sie behalten diese Zahlen für sich, um damit ein gemeinsames Master Secret zu vereinbaren.

(10) Alice und Bobs Server berechnen das Master Secret aus dem Pre-Master Secret und ihren privaten Zufallszahlen RN-Client und RN-Server auf Basis der vergänglichen Diffie-Hellman-Schlüsselvereinbarung (vgl. Kapitel 3.4.2, Abbildung 15).

**Phase 4:** Change-Cipher-Spec, Client-Finished, Server-Finished

(11) Nachdem Alice und Bob unabhängig voneinander das Master Secret errechnet haben, einigen sie sich nun auf den gemeinsamen Sitzungsschlüssel. Mit diesem symmetrischen Sitzungsschlüssel wird von nun an der Austausch von Daten, Informationen und sonstigen Inhalten sicher verschlüsselt. Der TLS-Handshake ist nach der erfolgreicheren Vereinbarung zwischen Alice und Bob abgeschlossen.

Der oben gezeigte TLS-Handshake der Version 1.2 ist ein Paradebeispiel für den Ablauf eines hybrid verschlüsselten Netzwerkprotokolls. Der Aufbau des TLS-Handshake-Protokolls erscheint zwar sehr langwierig, wird jedoch in Realität innerhalb weniger Millisekunden abgearbeitet. Die TLS-Version 1.3 verkürzt den Handshake-Protokollablauf, um noch performantere HTTPS-Verbindungen zu erzeugen und die Angriffsfläche für potentielle MITM-Attacken zu minimieren.[84]

Das nächste Kapitel beschreibt das Anwendungsbeispiel der Verbindung eines Clients zu einer verschlüsselten Web Site. Der Web Browser nimmt Alice letztendlich die gesamte Arbeit ab und stellt selbstständig eine verschlüsselte Verbindung her. Zuerst werden jedoch die dafür notwendigen Zertifikate und Cipher Suites gezeigt, welche die verschlüsselte Verbindung erst ermöglichen.

## 4.4 Anwendungsbeispiel: Verbindung einer verschlüsselten Web Site

Die digitalen Zertifikate der CA spielen ein zentrales Element für den verschlüsselten HTTPS-Verbindungsaufbau. Web-Site-Betreiber beantragen die dafür notwendigen TLS-Zertifikate und implementieren sie auf ihrem Web Server. Bei einem Web-Site-Verbindungsaufbau gleicht der Web Browser des Clients die Zertifikate des Servers mit der Zertifikatsliste ab. Die Zertifikatslisten sind bei Installation der Web Browser bereits enthalten. In der Benutzeroberfläche der Web Browser werden die Zertifikate wie folgt gelistet (siehe Abbildung 21):

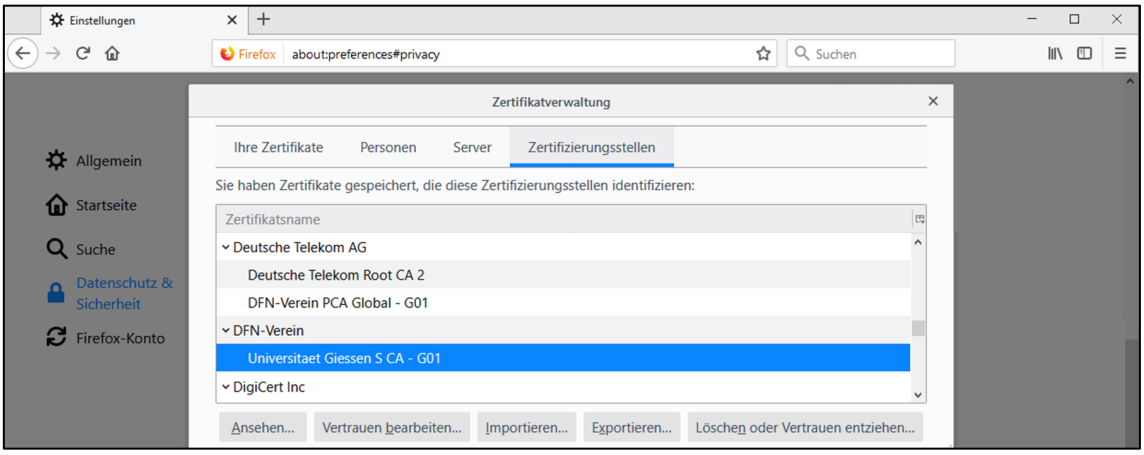



Abb. 21: Zertifikatverwaltung in Firefox

Nach Aufruf einer verschlüsselten Web Site sind die Details der verwendeten hybriden Verschlüsselung und andere Seiteninformationen über die Schaltfläche links neben der Adressleiste einzusehen. Die Seiteninformationen beinhalten den öffentlichen Schlüssel, die digitale Signatur und die Inhaberinformationen der Web Site. Auch die Gültigkeitsdauer und die Austeller-

84 Vgl. Martins, Filipe; Kobylinska, Anna: Supersicher – Die Neuerungen in TLS 1.3, a. a. O., S. 110.

informationen des TLS-Zertifikats sowie die zur Verschlüsslung verwendete Cipher Suite werden angezeigt. Die nachfolgende Abbildung 22 zeigt die Web Site des Fachbereichs für Wirtschaftswissenschaften der Justus-Liebig-Universität in Gießen, welche mit einem TLS-Zertifikat in der Version 1.2 ausgestattet ist:

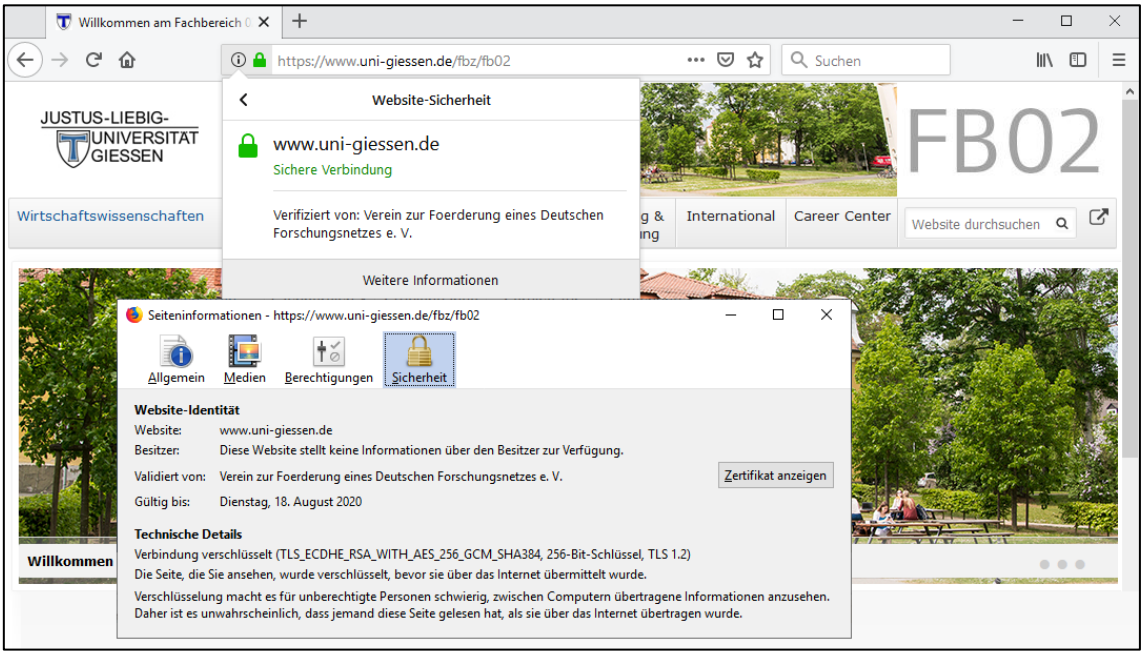


Abb. 22: Sicherheitsinformationen einer Web Site in Firefox

Durch die Zertifizierung und Konfiguration mit TLS beginnt die Internetadresse von Bobs Web Shop mit dem Kürzel HTTP**S** für Hypertext Transfer Protocol **Secure**. Alice wird zusätzlich ein grünes Schloss neben der Adressleiste angezeigt, wodurch sie erkennt, dass die Verbindung zum Web Shop der Lemonline AG von Bob verschlüsselt ist (siehe Abbildung 23):

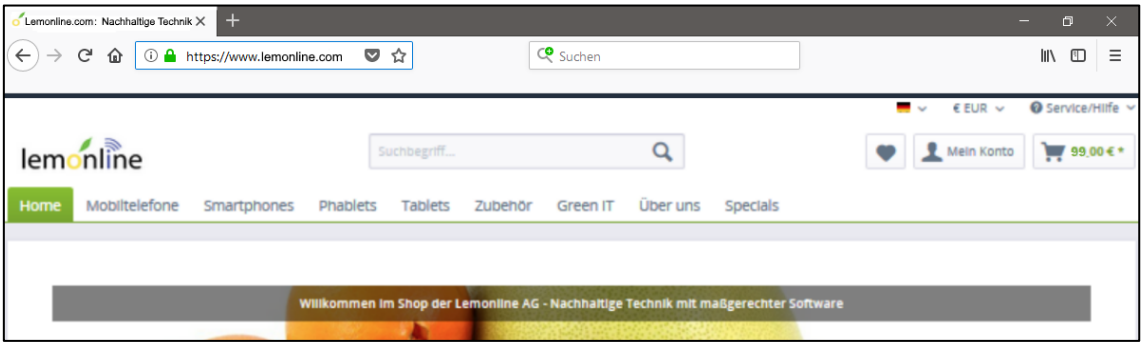


Abb. 23: Hybrid verschlüsselter Web Shop am Beispiel der Lemonline AG

Ruft Alice mit ihrem Web Browser eine Web Site auf, geschieht dies über einen HTTP-GET-Request. Allerdings können auch (Benutzer-) Informationen über Dialogfelder bzw. Formulare eingegeben oder ganze Dateien im Web hochgeladen werden. Statt Informationen abzufragen, werden die Informationen dann über sogenannte POST- und PUT-Requests zu einem Web Server geschickt. Sensible Informationen wie zum Beispiel Bankdaten, Adressen, Passwörter und andere Personendaten werden dabei mit HTTPS verschlüsselt transportiert.[85] Eine unbefugte Person kann die verschlüsselten Informationen von Alice auf dem Transportweg zu dem Web Shop von Bob und zurück nicht mitlesen. Da Bobs Web Shop mit TLS zertifiziert ist, kann Alice ohne größere Bedenken ihre Kreditkarteninformationen als Zahlungsart und andere Informationen hinterlegen. Alice bevorzugt jedoch PayPal als Zahlungsmethode und navigiert zur Kasse. In Abbildung 24 ist zu sehen, wie Alice auf eine andere Web Site weitergeleitet wird. Die TLS-Verbindung wird erneut geprüft:

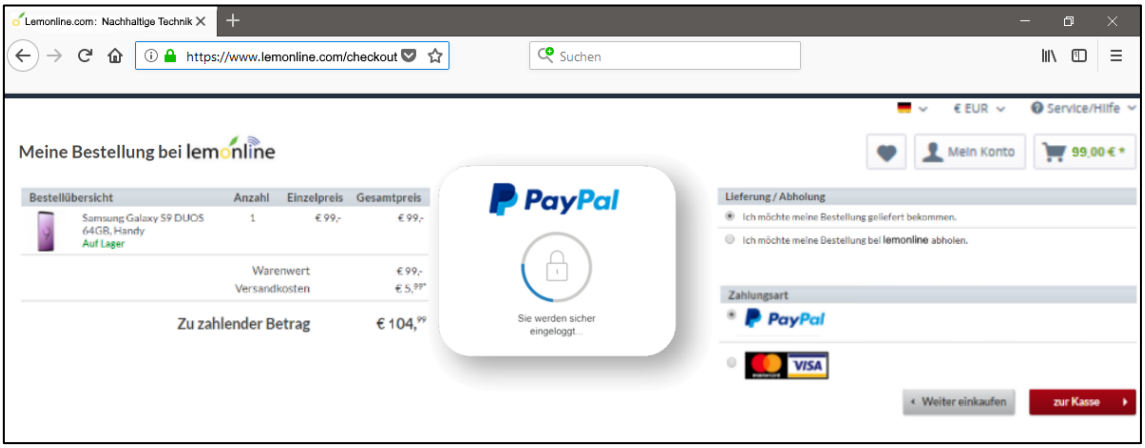



Abb. 24: Web-Site-Weiterleitung und die Zahlungsabwicklung mit PayPal

Der Web Browser von Alice verbindet sich automatisch mit dem Web Server von PayPal, welcher ebenfalls durch TLS verschlüsselt ist. Im Optimalfall bleibt die HTTPS-Verbindung über den gesamten Zeitraum der Benutzung eines Web Shops hinweg bestehen und sorgt jederzeit für einen sicheren Transportweg der Informationen durch die mehrfache Wiederholung des TLS-Handshakes.

Das nächste Kapitel beschreibt das Anwendungsbeispiel einer verschlüsselten E-Mail. Das TLS-Protokoll bietet auch hier Schutz durch Verschlüsselung. Es besitzt allerdings in Bezug auf E-Mails einige Schwachstellen, wie nachfolgend erläutert wird.

85 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a. a. O., S. 274f.

## 4.5 Anwendungsbeispiel: Versand einer verschlüsselten E-Mail

Mit einem vorhandenen und konfigurierten TLS-Zertifikat ist für Alice der Besuch des Web Shops der Lemonline AG von Bob praktisch automatisch hybrid verschlüsselt. Jedoch ist eine ganzheitliche E-Mail-Verschlüsselung nicht so selbstverständlich, wie das alltägliche HTTPS-Surfen mit einem Web Browser. Nicht immer erfüllen E-Mails alle Schutzziele der Informationssicherheit, weil sich E-Mails „unterschiedlich sicher“ hybrid verschlüsseln lassen.

Damit die Unterschiede der hybriden E-Mail-Verschlüsselung deutlich werden, wird dieses Kapitel in vier Sinnabschnitte unterteilt. Jeder Abschnitt erhöht den Grad der Sicherheit der hybriden E-Mail-Verschlüsselung. Bei Grad 0 werden die Nachrichten nicht verschlüsselt und die E-Mails ungesichert transportiert. Mit dem Grad 1, 2 und 3 sind die E-Mails mit unterschiedlichen hybriden Verschlüsselungsverfahren versehen, welche entweder Server-basiert oder Client-basiert umgesetzt werden.[86] Nur Grad 3 erreicht den maximalen Sicherheitsgrad der E-Mail-Verschlüsselung und erfüllt somit ohne Zweifel alle Schutzziele der Informationssicherheit: Die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit.

**Grad 0:** E-Mail ohne Verschlüsselung (SMTP/IMAP)

E-Mails ohne Verschlüsselung benutzten beispielsweise die Netzwerkprotokolle SMTP und IMAP. Sie sind notwendig um E-Mails von Alice zu Bob zu transportieren. Diese Netzwerkprotokolle sind jedoch nicht verschlüsselt.

**Grad 1:** E-Mail mit einer Server-basierten hybriden Verschlüsselung (TLS)

Damit E-Mails auf dem Transportweg geschützt werden, verschlüsseln viele E-Mail-Provider die Verbindungen zwischen dem E-Mail-Server des Senders und dem E-Mail-Server des Empfängers. Dies gelingt über das TLS-Protokoll wie bei HTTPS „automatisch“, da heutzutage die E-Mail-Provider in der Regel ihre E-Mail-Server mit TLS verschlüsseln. Ohne längeres Überlegen verlässt sich Alice auf ihren E-Mail-Provider und nutzt die transportgesicherten Protokolle SMTPS und IMAPS für ihre E-Mails.

Alice verfasst eine Nachricht an Bob. Ihr E-Mail-Client übergibt die Nachricht an den E-Mail-Provider von Alice, der die Nachricht an Bob schicken soll. Der E-Mail-Server von Alice verschlüsselt ihre Nachricht und verschickt den Geheimtext an Bob. Der E-Mail-Server von Bob wandelt den verschlüsselten Geheimtext dann wieder in Klartext um. Diese automatische Transportsicherung für E-Mails von Alice funktioniert zwar, allerdings nur, wenn auch alle anderen E-Mail-Server ihres Empfängerkreises korrekt konfiguriert sind und die verwendeten Verschlüsselungsverfahren fehlerfrei verstehen. Die „Verschlüsselungs-Kompatibilität“ der verschiedenen E-Mail-Provider ist jedoch nicht immer garantiert. Auch wenn die E-Mail-Provider von Alice und Bob kompatible Verschlüsselungsprotokolle verwenden sollten, werden

86 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 733f.

ihre E-Mails nur auf dem „Transportweg“ verschlüsselt. Der E-Mail-Provider von Bob muss die Transportverschlüsselung der Nachricht von Alice zunächst entschlüsseln, um sie auf Bobs Endgeräten in Klartext anzeigen zu können. Ob und in welchem Umfang die E-Mail-Provider dabei ihre eigenen Mail Server gegen Missbräuche schützen, ist hingegen unklar. Eine E-Mail liegt im allerhäufigsten Fall wie eine offen beschriebene Postkarte auf einem Mail Server.

Alice sollte nicht bedenkenlos davon ausgehen, dass ihr E-Mail-Provider den Versand der Nachrichten sicher bewerkstelligt bzw. die eigenen E-Mail-Archive gegen einen externen oder internen Angriff ausreichend schützt. Hinzu kommen mögliche MITM-Attacken, welche die für sicher geglaubten TLS-Verbindungen umgehen oder manipulieren können. Durch einen MITM-Downgrade-Angriff kann das transportgesicherte E-Mail-Protokoll SMTPS auf das unverschlüsselte Protokoll SMTP herabgestuft werden. Diese Problematik einer TLS-„verschlüsselten“ E-Mail-Kommunikation zwischen Alice und Bob ist in dem folgenden Worst-Case-Szenario in Abbildung 25 zu sehen:

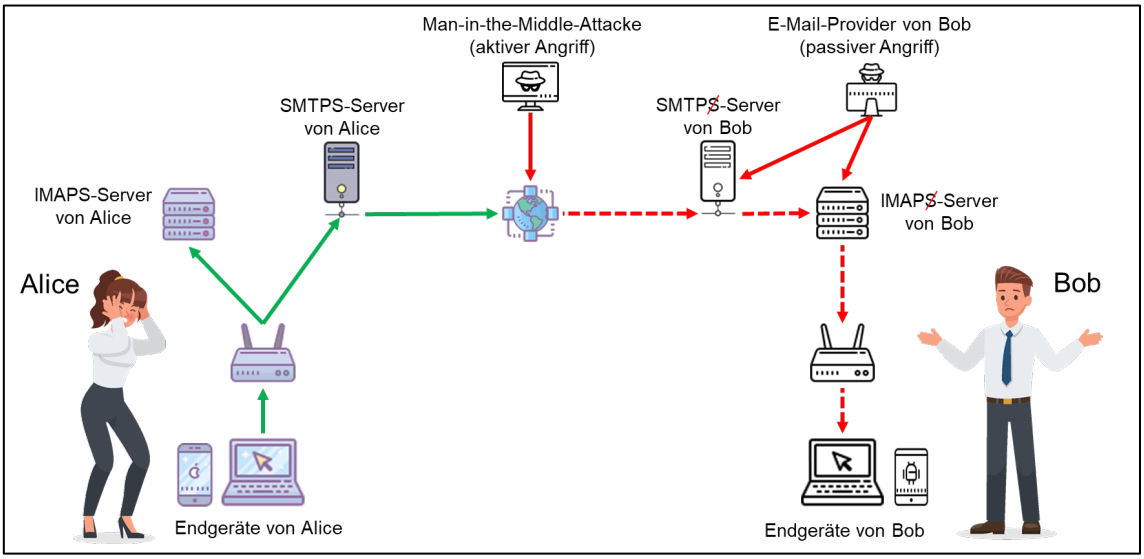



Abb. 25: Unsicherer Versand einer E-Mail von Alice an Bob trotz TLS-Protokoll

**Grad 2:** E-Mail mit einer Server-basierten hybriden Verschlüsselung (PGP und S/MIME)

Damit der Inhalt von E-Mails auch auf E-Mail-Servern und an allen anderen Knotenpunkten während dem Transportweg im Web sicher ist, wird ein asymmetrisches Schlüsselpaar benötigt. Bereits 1991 entwickelte Phil Zimmermann die erste Software für Privatanwender, um Schlüsselpaare zu erstellen und den Inhalt von E-Mails hybrid zu verschlüsseln. Die Software des gleichnamigen Standards nennt sich PGP. Noch heute werden E-Mails mit PGP hybrid verschlüsselt. Ein anderer Standard für die verschlüsselte E-Mail-Kommunikation ist S/MIME (Secure/Multipurpose Internet Mail Extension). Die Standards PGP und S/MIME werden für die Inhaltsverschlüsselung von E-Mails und für digitale Signaturen verwendet.[87] Viele E-Mail-

87 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 737 und 828.

Provider bieten heutzutage sogenannte E-Mail-Gateways an, um den Inhalt einer Nachricht vor dem Verlassen des eigenen E-Mail-Servers zusätzlich mit PGP oder S/MIME zu verschlüsseln.

Als Senderin verschlüsselt Alice ihre Nachricht also zunächst an ihrem „Ende". Am anderen „Ende" wird die Nachricht dann durch Bob entschlüsselt. Diese Ende-zu-Ende-Verschlüsselung stellt sicher, dass die Nachrichten an jeder Stelle des gesamten Transportwegs verschlüsselt sind.[88] Bei der Server-basierten hybriden Verschlüsselung werden die personengebundenen Schlüsselpaare allerdings auf dem Server eines E-Mail-Providers gespeichert. Theoretisch ist Alice zwar die Eigentümerin ihres Schlüsselpaars, allerdings ist sie praktisch nicht die Besitzerin bzw. die Herrin ihres privaten Schlüssels. Dadurch verliert ihre digitale Signatur an Wert, weil die Verbindlichkeit ihrer Signatur, die nicht sie, sondern ihr E-Mail-Provider mit dem privaten Schlüssel von Alice angefertigt hat, nicht besonders hoch ist.[89]

**Grad 3:** E-Mail mit einer Client-basierten hybriden Verschlüsselung (Bspw. OpenPGP)

Damit nur Alice und die von ihr gewünschten Empfänger die Nachrichten lesen können, muss Alice ihre Nachrichten zunächst in Eigenregie auf ihrem Endgerät verschlüsseln und ihre digitale Signatur selbstständig hinzufügen (vgl. Kapitel 3.3.2, Abbildung 12). Erst dann übergibt Alice ihre verschlüsselte Nachricht an ihren E-Mail-Provider, der den verschlüsselten Text zum E-Mail-Server von Bob transportiert. Bob holt sich die verschlüsselte Nachricht bei seinem E-Mail-Provider ab und entschlüsselt sie danach auf seinem eigenen Rechner (vgl. Kapitel 3.4.1, Abbildung 14).

Damit Alice und Bob den Inhalt der E-Mails in ihrem E-Mail-Client zum Beispiel mit dem frei zugänglichen Verschlüsselungsstandard OpenPGP selbstständig verschlüsseln und entschlüsseln können, benötigen die beiden eine Verschlüsselungs-Software.

- Unter Microsoft Windows für Office Outlook wird beispielsweise die Software „Gpg4win" benötigt, die das Tool „Kleopatra" und das Plugin „GpgOL" beinhaltet.
- Unter MacOS für Apple Mail werden beispielsweise die Software „GPGSuite" und das Plugin „GPG Mail" benötigt.

Mit dieser Software generieren sie sich die asymmetrischen Schlüsselpaare, die sie anschließend speichern und für die hybride Verschlüsselung ihrer E-Mails verwenden. Alice und Bob verwenden beide Microsoft Windows als Betriebssystem und Microsoft Outlook als E-Mail-Client und erstellen sich nach der Installation von Gpg4win mit dem Tool Kleopatra jeweils ein eigenes OpenPGP-Schlüsselpaar. Beide erhalten einen privaten und einen öffentlichen Schlüssel. Abbildung 26 zeigt einen Ausschnitt der Schlüsselerstellung von Alice mit der Software

88 Vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, a. a. O., S. 97f.

89 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 735.

Kleopatra. Im Hintergrund ist bereits der Kontakt von Bob zu sehen. Seinen öffentlichen Schlüssel hat Alice bereits erhalten (vgl. Web of Trust, Kapitel 3.2.2):

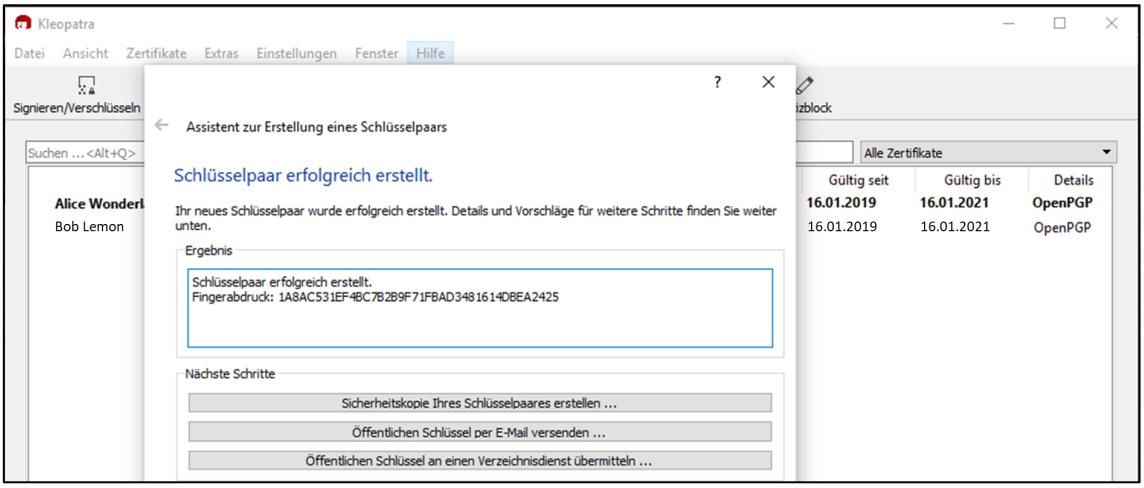



Abb. 26: Erstellung eines asymmetrischen Schlüsselpaars für Alice

Nachdem auch Alice ihr persönliches Schlüsselpaar erstellt und ihren öffentlichen Schlüssel anschließend an Bob verschickt hat, können beide verschlüsselt miteinander kommunizieren. Wenn Alice eine neue E-Mail mit ihrem Outlook Client verfassen möchte, erscheint das Plugin GpgOL am oberen rechten Bildrand. Über diese Schaltfläche kann sie ihre E-Mail digital signieren und verschlüsseln (siehe Abbildung 27):

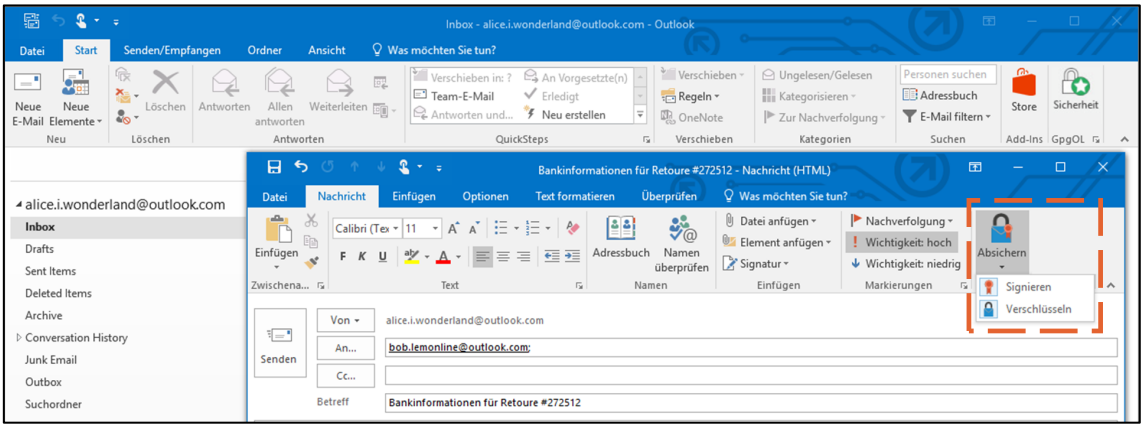



Abb. 27: Versand einer hybrid verschlüsselten E-Mail an von Alice an Bob

Verglichen mit den Methoden der Server-basierten hybriden Verschlüsselung bedeutet die oben gezeigte Client-basierte hybride E-Mail-Verschlüsselung mit OpenPGP einen Mehraufwand für Alice und Bob. Neben diesem Zusatzaufwand und die für den „Otto Normalverbraucher“ möglicherweise umständliche Konfiguration des E-Mail-Clients, besitzt die Client-basierte E-Mail-Verschlüsselung einen weiteren Nachteil: Möchte Alice ihre E-Mails unterwegs oder von einem anderen Endgerät aus verschlüsseln, muss dort ebenfalls eine passende Verschlüsse-

lungs-Software installiert und ihr Schlüsselpaar vorhanden sein. Ohne ein Client-basiertes hybrides Verschlüsselungsverfahren wären die E-Mails von Alice an Bob allerdings nicht ganzheitlich Ende-zu-Ende verschlüsselt.[90]

# 5 Ausblick

In den letzten Jahren findet eine zunehmende Vernetzung von IT-Systemen sowie Multimedia- und Haushaltsgeräten in unserer Umwelt statt. Die IT-Sicherheit ist somit längst ein Querschnittsthema geworden und das Prinzip der Verschlüsselung wird auch zukünftig das Mittel der Wahl sein, um Daten zu schützen.[91]

Kryptoanalyse-Forscher und Hacker finden jedoch immer wieder Lücken und bekannte Schwachstellen in den eingesetzten kryptografischen Verfahren.[92] Ohne die gewissenhafte Weiterentwicklung der vorhandenen Verfahren und eine fehlerfreie Implementierung in moderne IT-Systeme versagen die im Rahmen dieser Arbeit vorgestellten Verschlüsselungsstandards in der Praxis. Auch das asymmetrische Verfahren der vergänglichen Diffie-Hellman-Schlüsselvereinbarung, die für Perfect Forward Secrecy sorgen soll, besitzt Schwachstellen.[93] Es gilt zukünftig konzeptuelle Schwächen bzw. Probleme, die durch neue Technologien (Stichwort: Quantencomputer) aber auch durch fehlerhaftes Anwenderverhalten (Stichwort Schlüssel- und Passwortmanagement) entstehen, zu minimieren. Ein wichtiger Schritt wäre ein höher ausgeprägtes Bewusstsein und Kenntnis für neuartige Bedrohungslagen und anwenderfreundlichere Möglichkeiten der Verschlüsselung.

Die Initiative Let’s Encrypt wurde unter anderem ins Leben gerufen, um kostenlose TLS-Zertifikate für die Masse bereitzustellen. Durch automatisierte Prozesse bei der Verifizierung und Implementierung der Zertifikate von Let’s Encrypt wird es auch Nutzern ohne technische Vorkenntnisse leicht gemacht, ihre Web Sites zu verschlüsseln. Seit Ende 2015 tragen die Community-basierten Zertifizierungsstellen dazu bei, den Transportweg über das World Wide Web mit HTTPS flächendeckend zu etablieren. Heute deckt Let’s Encrypt bereits über 50% des Marktanteils ab und stellt seine Mitbewerber in den Schatten.[94] Der Erfolg von Let’s Encrypt

90 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 744f.

91 Vgl. Abolhassan, Ferri: Security Einfach Machen IT-Sicherheit als Sprungbrett für die Digita-lisierung, Wiesbaden: Springer Gabler 2017, S. 117f und 121.

92 Vgl. Ronen, Eyal; Gillham, Robert; Genkin, Daniel; Shamir, Adi; Wong, David; Yarom, Yuval: The 9 Lives of Bleichenbacher's CAT – New Cache ATtacks on TLS Implementations, a. a. O., 2019.

93 Vgl. Adrian, David; Bhargavan, Karthikeyan; Durumeric, Zakir; Gaudry, Pierrick; Green, Matthew; Halderman, J. Alex; Heninger, Nadia; Springall, Drew; Thomé, Emmanuel; Valenta, Luke; VanderSloot, Benjamin; Wustrow, Eric; Zanella-Béguelin, Santiago; Zimmermann, Paul: Imperfect Forward Secrecy – How Diffie-Hellman Fails in Practice, in: Communications of the Association for Computing Machinery, 01/2019, S. 106.

94 Vgl. Scherschel, Fabian: Let's Encrypt stellt jetzt mehr als die Hälfte aller SSL-Zertifikate aus, Online im Internet: https://heise.de/-4029922, 23.04.2018.

zeigt, dass sich die Akzeptanz des Nutzers nach der Zugänglichkeit der Verschlüsselungstechnologie richtet.

TLS-Zertifikate garantieren nicht für die ganzheitliche Verschlüsselung der Kommunikation. Zwar wird mithilfe von HTTPS ein sicherer Transportweg der Inhaltsdaten zwischen Browser und Server gewährleistet, allerdings sind die so genannten Metadaten noch weitestgehend ungeschützt. Diese entstehen bereits ab der ersten Verbindungsanfrage zu einer Web Site. Metadaten geben unter anderem Auskunft über den Zeitpunkt oder den Ort der Kommunikationspartner. Eine Verschlüsselung des Domain Name System der obersten Anwendungsschicht des TCP/IP-Modells (DNS over TLS) könnte auch diese „Verkehrsflussanalyse“ stoppen, welche konstant an den Nutzern im Web durchgeführt wird.[95]

Die Verschlüsselung der Netzzugangsschicht (erste und unterste Schicht des TCP/IP-Modells) bedeutet, dass sämtliche Daten einer Anwendung inklusive Transport- und Internetprotokoll der Ebenen 4, 3 und 2 mitverschlüsselt würden. Ein Server bzw. Knotenpunkt im Web wüsste nicht mehr, an wen er die verschlüsselten Informationen weiterleiten soll. Ohne neuartige Konzepte für technische oder physische Netze aus der Forschung würden die Informationen schlicht und ergreifend im Web verloren gehen.[96]

Der NSA-Skandal hat seit den Snowden-Enthüllungen für Sensibilisierung und Bewusstsein für das Thema Verschlüsselung und E-Mail-Absicherung gesorgt. Trotzdem verschlüsseln lediglich 13,5% der deutschen Internetnutzer ihre E-Mails Server-basiert Ende-zu-Ende.[97] Die regelmäßig verwendeten Instant Messenger von Facebook werben ebenfalls mit einer Ende-zu-Ende-Verschlüsselung. Die Smartphone Applikation WhatsApp verspricht seinen Anwendern immerhin: „At no time does the WhatsApp server have access to any of the client’s private keys”.[98] Doch auch hier liegt der private Schlüssel auf dem Server eines anderen Unternehmens und der Benutzer der Applikation ist zwar Eigentümer, aber nicht Besitzer seines Schlüssels. Client-basierte Instant Messenger mit einer ganzheitlichen Ende-zu-Ende-Verschlüsselung, wie zum Beispiel Threema, sind gemessen an den aktiven Benutzer-Accounts lediglich eine Ni-

95 Vgl. Ermert, Monika: Mehr Privacy über verschlüsselten DNS-Transport, Online im Internet: https://heise.de/-3779283, 08.12.2013, vgl. Grüner, Sebastian: DNS über HTTPS ist für Endnutzer, Online im Internet: https://www.golem.de/news/daniel-stenberg-dns-ueber-https-ist-fuer-endnutzer-1902-139148.html, 03.02.2019 und vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, a. a. O., S. 47f.

96 Vgl. Raghatwan; Jyoti; Taur; Alka: Physical-Layer Cryptography through Massive MIMO, in: International Journal of Innovative Research in Computer and Communication Engineering (Hrsg.), Vol. 5, Issue 12, 12/2017.

97 Vgl. Statista (Hrsg.); Brand, Mathias: Nur eine Minderheit verschlüsselt E-Mails, Online im Internet: https://de.statista.com/infografik/9522/nutzung-von-ende-zu-ende-verschluesselung/, 26.09.2019.

98 WhatsApp (Hrsg): Whatsapp encryption overview – Technical white paper, 12.19.2017, S.4.

schenerscheinung. Es ist also zu befürchten, dass die Client-basierte Ende-zu-Ende-Verschlüsselung, sowohl für die Nachrichten der Instant-Messenger-Applikationen als auch für die E-Mail-Dienste, noch lange ein Sorgenkind bleibt.[99]

99 Vgl. Schmeh, Klaus: Kryptografie – Verfahren, Protokolle, Infrastrukturen, a. a. O., S. 744f.

## Literaturverzeichnis


1. **Abolhassan, Ferri:** Security Einfach Machen IT-Sicherheit als Sprungbrett für die Digita-lisierung, Wiesbaden: Springer Gabler 2017.
2. **Adrian, David; Bhargavan, Karthikeyan; Durumeric, Zakir; Gaudry, Pierrick; Green, Matthew; Halderman, J. Alex; Heninger, Nadia; Springall, Drew; Thomé, Emmanuel; Valenta, Luke; VanderSloot, Benjamin; Wustrow, Eric; Zanella-Béguelin, Santiago; Zimmermann, Paul:** Imperfect Forward Secrecy – How Diffie-Hellman Fails in Practice, in: Communications of the Association for Computing Machinery, Vol. 62 Issue 1, 01/2019.
3. **Beutelspacher, Albrecht**: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 10. Aufl., Wiesbaden: Springer Spektrum 2015.
4. **Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter**: Moderne Verfahren der Kryptologie – Von RSA zu Zero-Knowledge, 8. Aufl., Wiesbaden: Springer Spektrum 2015.
5. **Buchmann, Johannes**: Einführung in die Kryptographie, 6. Aufl., Berlin Heidelberg: Springer Spektrum 2016.
6. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** Kryptographische Verfahren – Empfehlungen und Schlüssellängen, in: TR-02102-1, 22.02.2019.
7. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):** Verwendung von Transport Layer Security (TLS), in: TR-02102-2, 22.02.2019.
8. **Chapple, Mike:** CISSP Cert Prep: 3 Security Architecture and Engineering, Online im Internet: https://www.linkedin.com/learning/cissp-cert-prep-3-security-architecture-and-engineering/diffie-hellman, 08.03.2018.
9. **Ermert, Monika:** IETF 99: Mehr Privacy über verschlüsselten DNS-Transport, Online im Internet: https://heise.de/-3779283, 08.12.2013.
10. **Freiermuth, Karin; Hromkovič, Juraj; Keller, Lucia; Steffen, Björn:** Einführung in die Kryptologie – Lehrbuch für Unterricht und Selbststudium, 2. überarbeitete Auflage, Wiesbaden: Springer Vieweg 2014.
11. **Gobrecht, Jan:** SHA Generator, Online im Internet: https://www.sha-generator.de, zuletzt aufgerufen am 16.01.2019.

12. **Gramm, Andreas:** Integrität einer Nachricht und Authentizität ihres Absenders mit einer digitaler Unterschrift sicherstellen, Online im Internet: http://it-lehren.de/asym/Integritaet-und-Authentizitaet-mit-digitaler-Unterschrift-sicherstellen.html, 2010.

13. **Greis, Friedhelm; Ernst, Nico; Thoma, Jörg:** Chronologie der Enthüllungen von Edward Snowden, Online im Internet: https://www.golem.de/news/nsa-chronologie-der-enthuellungen-von-edward-snowden-1307-100411.html, 16.07.2013.

14. **Grüner, Sebastian:** DNS über HTTPS ist für Endnutzer, Online im Internet: https://www.golem.de/news/daniel-stenberg-dns-ueber-https-ist-fuer-endnutzer-1902-139148.html, 03.02.2019.

15. **Holland, Martin:** Facebook: Hunderte Millionen Passwörter im Klartext gespeichert, Online im Internet: https://heise.de/-4342184, 21.03.2019.

16. **Kappes, Martin:** Netzwerk- und Datensicherheit – Eine praktische Einführung, 2. aktualisierte und erweiterte Auflage, Wiesbaden: Springer Vieweg 2013.

17. **Krempl, Stefan:** Gehackte Daten: Politiker beklagen schweren Angriff auf die Demokratie, Online im Internet: https://heise.de/-4265847, 04.01.2019.

18. **Martins, Filipe; Kobylinska, Anna**: Supersicher – Die Neurungen in TLS 1.3, in: iX – Magazin für professionelle Informationstechnik, 08/2018.

19. **Microsoft (Hrsg.):** MACs, hashes, and signatures, Online im Internet: https://docs.microsoft.com/de-de/windows/uwp/security/macs-hashes-and-signatures, 08.02.2017.

20. **Paar, Christof; Pelzl, Jan**: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, Berlin Heidelberg: Springer Vieweg 2016.

21. **Petrlic, Ronald; Sorge, Christoph**: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Wiesbaden: Springer Vieweg 2017.

22. **Popyack; Jeffrey**: RSA Calculator, Online im Internet: https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html, zuletzt aufgerufen am 20.02.2019.

23. **Raghatwan; Jyoti; Taur; Alka:** Physical-Layer Cryptography through Massive MIMO, in: International Journal of Innovative Research in Computer and Communication Engineering (Hrsg.), Vol. 5, Issue 12, 12/2017.

24. **Rescorla, Eric:** The Transport Layer Security (TLS) Protocol Version 1.3, in: Internet Engineering Task Force (Hrsg.): RFC 8446, 08/ 2018.

25. **Ristić, Ivan:** Bulletproof SSL and TLS – Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, London: Feisty Duck 2015.

26. **Rivest, Ron; Shamir, Adi; Adleman, Leonard:** A Method for Obtaining Digital Signatures and Public-key Cryptosystems, in: Communications of the ACM (Hrsg.), Volume 21 Issue 2, 02/1978.

27. **Ronen, Eyal; Gillham, Robert; Genkin, Daniel; Shamir, Adi; Wong, David; Yarom, Yuval:** The 9 Lives of Bleichenbacher's CAT – New Cache ATtacks on TLS Implementations, in: IEEE Symposium on Security & Privacy, 2019.

28. **Schäfer, Günter; Roßberg, Michael**: Netzsicherheit, 2. aktualisierte und erweiterte Auflage, Heidelberg: dpunkt Verlag 2014.

29. **Scherschel, Fabian:** Let's Encrypt stellt jetzt mehr als die Hälfte aller SSL-Zertifikate aus, Online im Internet: https://heise.de/-4029922, 23.04.2018.

30. **Schirrmacher, Dennis:** Zahlenfolge "123456" immer noch beliebtestes Passwort in Deutschland, Online im Internet: https://heise.de/-3927009, 22.12.2017.

31. **Schmeh, Klaus**: Kryptografie – Verfahren, Protokolle, Infrastrukturen, 6. Auflage, Heidelberg: dpunkt Verlag 2016.

32. **Schmidt, Jürgen:** Kryptographie in der IT - Empfehlungen zu Verschlüsselung und Verfahren, Online im Internet: https://heise.de/-3221002, 17.06.2016.

33. **Schwenk, Jörg**: Sicherheit und Kryptographie im Internet – Theorie und Praxis, 4. Auflage, Wiesbaden: Springer Vieweg 2014.

34. **Sorge, Christoph; Gruschka, Nils; Lo lacona, Luigi**: Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013.

35. **Statista (Hrsg.); Brand, Mathias:** Nur eine Minderheit verschlüsselt E-Mails, Online im Internet: https://de.statista.com/infografik/9522/nutzung-von-ende-zu-ende-verschluesselung/, 26.09.2019.

36. **Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael**: Kryptographie und IT-Sicherheit – Grundlagen und Anwendungen, Wiesbaden: Vieweg und Teubner Verlag 2008.

37. **Wewer, Göttrik**: Auf dem Weg zum gläsernen Staat? Privatsphäre und Geheimnis im digitalen Zeitalter, in: dms - Zeitschrift für Public Policy, Recht und Management, 2/2012, S. 247-262.

38. **WhatsApp (Hrsg):** Whatsapp encryption overview – Technical white paper, 12.19.2

# Impressum

**Reihe:** **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

**Bezug:** http://wiwi.uni-giessen.de/home/Schwickert/arbeitspapiere/

**Herausgeber:** Prof. Dr. Axel C. Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

**Ziele:** Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

**Zielgruppen:** Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

**Quellen:** Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

**Hinweise:** Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wiwi.uni-giessen.de/home/ Schwickert/arbeitspapiere/.