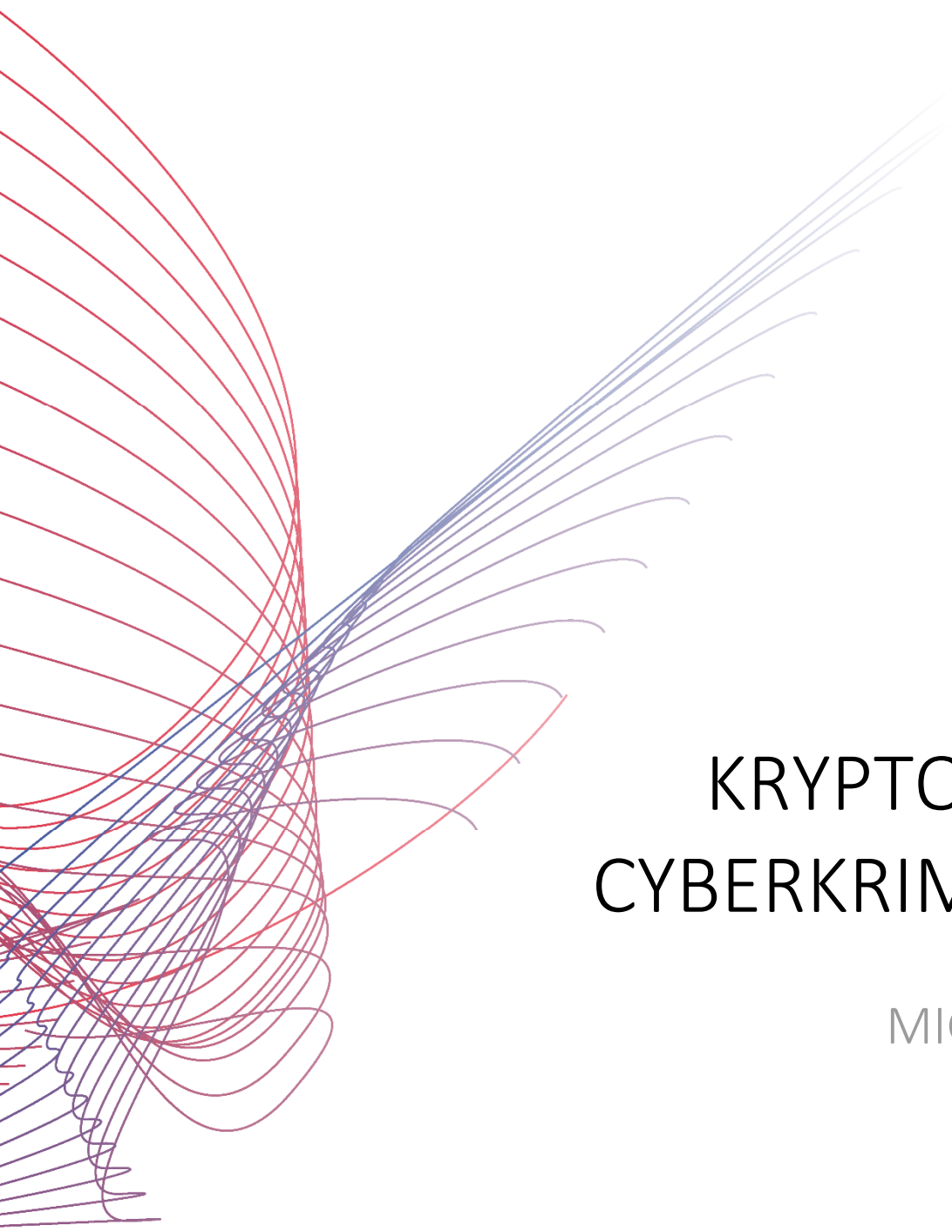
en cs de sk es

TECH pedia



KRYPTOGRAPHIE, CYBERKRIMINALITÄT

MIGUEL SORIANO

Titel der Arbeit: Kryptographie, Cyberkriminalität
Author: Miguel Soriano
Übersetzt (von): Alena Dvořáková
Veröffentlicht (von): České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktadresse: Technicka 2, Prague 6, Czech Republic
Tel.: +420 224352084
Drucken: (nur elektronisch)
Anzahl der Seiten: 40
Ausgabe: 1. Ausgabe, 2017

ISBN 978-80-01-06203-6

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG

	Definition(en)
	Interessantheit (Interessantes)
	Bemerkung
	Beispiel
	Zusammenfassung
	Vorteile
	Nachteile

ZUSAMMENFASSUNG

Dieses Modul gibt eine grundlegende Orientierung im Bereich der Kryptographie und Cyberkriminalität.

ZIELE

Dieses Modul bietet grundlegende Informationen zu den Themen Kryptographie und Cyberkriminalität. Im ersten Teil des Kurses werden die Möglichkeiten der Kryptographie zur Informationssicherheit vorgestellt. Es werden Kryptographie und Algorithmen mit öffentlichen und geheimen Schlüsseln erklärt. Der zweite Teil widmet sich der Einführung des Konzeptes der Cyberkriminalität und der Klassifizierung der Cyberangriffe. Abschließend werden Hinweise zur Vorbeugung von Cyberangriffen gegeben.

LITERATUR

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security Fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Goodrich, Roberto Tamassia: Introduction to Computer Security, 2010

[6] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[7] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Inhaltsverzeichnis

1 Grundlagen der Kryptographie

Kryptographie ist ein wirksames mathematisches Instrument zum Schutz von Informationen in Computersystemen. Daher verwenden viele Sicherheitsanwendungen kryptographische Verfahren für die Ver- und Entschlüsselung von Daten. Dank der Kryptographie werden sensible Daten über Telekommunikationsnetze auf sichere Weise übertragen, ohne dass sie durch das Abhören und die nachfolgende Beeinträchtigung gefährdet werden. Die Verschlüsselung kann als der Prozess definiert werden, bei dem Informationen nicht entzifferbar und zwecklos gemacht werden, bis sie zum richtigen Empfänger gelangen. Die Entschlüsselung ist die Umwandlung der verschlüsselten Daten in die ursprüngliche, lesbare Form.

Diese Technik wird im Alltagshandeln eingesetzt, wie Telefonieren mit einem Handy, Bezahlen mit einer Kredit- oder Debitkarte, Geldheben von einem Geldautomat, Einloggen in einen Computer mit einem Passwort usw. Die Kryptographie erlaubt die Speicherung von empfindlichen Informationen oder ihre Übertragung über ungesicherte Netzwerke (wie das Internet), so dass sie nur vom geplanten Empfänger gelesen werden können. Die Kryptographie wurde zu einem Industriestandard für die Sicherstellung der Informationssicherheit und -vertraulichkeit, Zugriffskontrolle auf Ressourcen und elektronische Transaktionen. Sie kann jedoch nicht allein alle Bedrohungen der Informationssicherheit behandeln.

Ein kryptographischer Algorithmus (auch als Chiffre bezeichnet) ist eine Sequenz von entsprechenden Ver- und Entschlüsselungsprozessen. Es handelt sich um eine mathematische Formel, die speziell für das Verdecken des Dateninhaltes entworfen wurde. Die wirksamsten Verschlüsselungsalgorithmen arbeiten mit einem oder mehreren Schlüsseln zusammen. Der gleiche Klartext kann mit Hilfe von unterschiedlichen Schlüsseln in unterschiedliche Geheimtexte verschlüsselt werden. Ein zuverlässiger kryptographischer Algorithmus muss garantieren, dass keine Möglichkeit besteht, den ursprünglichen Klartext zu entdecken, ohne dass man den Schlüssel kennt. Selbstverständlich gibt es auch Brute-Force-Methoden, die versuchen, alle möglichen Schlüssel auszuprobieren, bis der richtige gefunden wird. Die Sicherheit der verschlüsselten Daten hängt von zwei Faktoren ab: der Stärke des kryptographischen Algorithmus und der Geheimhaltung des Schlüssels.

Die Anzahl möglicher Schlüssel muss so hoch sein, dass es rechnerisch unmöglich ist, den richtigen Schlüssel mit einem Brute-Force-Angriff innerhalb einer angemessenen Frist zu entdecken. Viele Verschlüsselungsalgorithmen steigern ihre Zuverlässigkeit durch Erhöhung der Länge ihrer Schlüssel. Mit der Länge der Schlüssel wird mehr Rechenleistung für die Ver- und Entschlüsselung der Daten benötigt. Daher ist es wichtig, einen solchen Verschlüsselungsalgorithmus zu wählen, der den Mittelweg zwischen der notwendigen Sicherheit und den Rechenkosten der Datensicherung findet.

Moderne kryptographische Algorithmen können nach zwei Kriterien aufgeteilt werden: nach dem Typ des eingesetzten Schlüssels und nach der Art ihrer Arbeit mit Daten.

Nach dem Typ des eingesetzten Schlüssels gibt es:

a) Algorithmen mit privaten Schlüsseln, symmetrische Kryptographie. Ein symmetrisches Kryptosystem verwendet Verschlüsselungsverfahren, in denen sowohl der Sender als auch der Empfänger den gleichen Schlüssel besitzen (oder seltener, in denen sich ihre Schlüssel unterscheiden, aber rechnerisch einfach voneinander abgeleitet werden können). Ein Beispiel eines symmetrischen Kryptosystems ist der **AES**-Standard (engl. *Advanced Encryption Standard*).

b) Algorithmen mit öffentlichen Schlüsseln, asymmetrische Kryptographie. Diese Kryptographie verwendet zwei Schlüssel: einen öffentlichen Schlüssel zur Verschlüsselung der Daten und einen entsprechenden privaten (geheimen) Schlüssel zur Entschlüsselung der Daten. Offensichtlich gibt es zwischen den beiden Schlüsseln eine mathematische Beziehung - trotzdem ist es rechnerisch unmöglich, den privaten Schlüssel von dem öffentlichen Schlüssel abzuleiten. Der Benutzer oder das Subjekt veröffentlicht seinen öffentlichen Schlüssel und hält den privaten Schlüssel geheim. Jeder, der den öffentlichen Schlüssel hat, kann Informationen verschlüsseln, aber nicht entschlüsseln. Nur die Person, die den entsprechenden privaten Schlüssel hat, kann die Informationen entschlüsseln.

Der Hauptvorteil der Kryptographie mit öffentlichen Schlüsseln besteht darin, dass Subjekte ohne eine vorhandene Sicherheitsregelung Nachrichten auf eine sichere Weise austauschen können. Sowohl der Sender als auch der Empfänger brauchen keine geheimen Schlüssel über sichere Kanäle zu teilen: die Kommunikation umfasst nur öffentliche Schlüssel und kein privater Schlüssel wird übertragen oder geteilt.

Nach der Art, wie die Algorithmen mit Daten arbeiten, können Chiffren wie folgt aufgeteilt werden:

a) Blockchiffren arbeiten mit Datenblöcken einer fixen Länge mit einer verschlüsselten unveränderlichen Transformation. Sie zerteilen die Nachricht in Blöcke und verschlüsseln jeweils einen Block. Wenn die Blockchiffre als sicher betrachtet werden kann, wird selbstverständlich auch der resultierende Geheimtext eines einzelnen Blocks als sicher angesehen - wenn er individuell analysiert wird. Wenn jedoch mehrere Nachrichten mit demselben Schlüssel verschlüsselt werden, führen identische Blöcke der Daten zu identischen Blöcken des Geheimtextes. Daher kann ein Angreifer eine Wiederholung von Blöcken in der Nachricht leicht erkennen. Deshalb werden Blockchiffren in einer solchen Anwendung nicht empfohlen und es werden dann andere sichere Betriebsmodi verwendet.

b) Stromchiffren wandeln ein Symbol des Klartextes direkt in ein Symbol des Geheimtextes. Die Transformation basiert auf dem Generieren einer verschlüsselten pseudozufälligen Folge, die als ein kryptographischer

Schlüsselstrom arbeitet. Dieser Schlüsselstrom ist grundsätzlich ein Strom von Bits, der mit dem Klartext kombiniert wird, um jeweils ein Bit oder Byte zu verschlüsseln und den Geheimtext zu erzeugen.

Im Modul wird die folgende Terminologie verwendet:

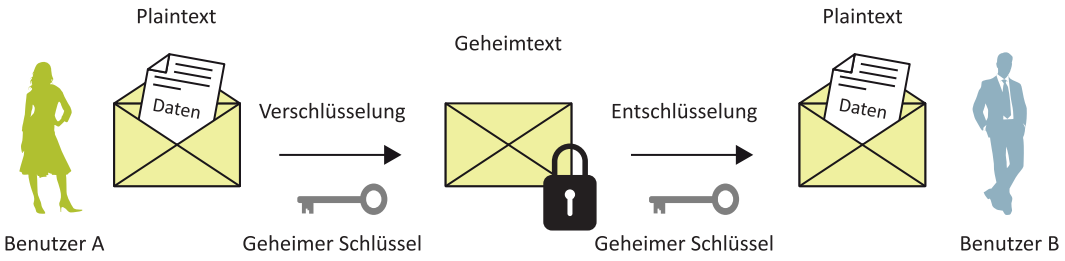
- Ein Klartext oder Plaintext ist die Nachricht, die zu senden und dem Empfänger zuzustellen ist.
- Ein Geheimtext oder Chiffretext ist ein Ergebnis eines Kryptosystems, das durch Verschlüsselung des Klartextes entsteht.
- Die Verschlüsselung ist der Prozess der Änderung des Inhaltes eines Klartextes zum Zweck des Verdeckens der übertragenen Informationen.
- Die Entschlüsselung ist die inverse Operation zur Verschlüsselung; es handelt sich um den Prozess der Wiedergewinnung der Nachricht in Form eines Klartextes aus ihrer verschlüsselten Form (dem Geheimtext).
- Ein Schlüssel ist eine Zeichenkette, die zur Verschlüsselung des Klartextes oder zur Entschlüsselung des Geheimtextes verwendet wird.
- Die Kryptoanalyse ist die Wissenschaft des Entzifferns von Codes und Chiffren.
- Ein Hash ist ein Algorithmus, der eine Textfolge einer beliebigen Länge in eine Textfolge einer fixen Länge umwandelt.
- Eine Chiffre ist ein kryptographischer Algorithmus, d. h. eine mathematische Funktion zur Ver- und Entschlüsselung.
- Die Schlüsselverwaltung ist der Prozess, mit dem ein Schlüssel erzeugt, gespeichert, geschützt, übertragen, geladen, verwendet und zerstört wird.

2 Kryptographie mit symmetrischen Schlüsseln

Die Kryptographie mit symmetrischen (geheimen) Schlüsseln ist der Prozess der Ver- und Entschlüsselung von Daten mittels eines einzigen Schlüssels. In dieser Kryptographie können die Schlüssel zur Verschlüsselung des Klartextes und zur Entschlüsselung des Geheimtextes identisch sein (übliche Variante) oder eine einfache Transformation verwenden (weniger verwendete Variante). Das größte Problem dieser Systeme besteht in der Tatsache, dass sich der Sender und der Empfänger auf einen gemeinsamen Schlüssel einigen müssen. Darüber hinaus ist ein sicherer Kanal zwischen dem Sender und dem Empfänger zum Austausch des geheimen Schlüssels erforderlich.

Die beiden Parteien müssen den Schlüssel schützen - seine Offenbarung seitens einer Partei kann zu einer Offenlegung der Information führen.

Die Verschlüsselung mit symmetrischen Schlüsseln hat die folgende Abfolge: Der Benutzer A möchte eine Nachricht dem Benutzer B senden und möchte dabei garantieren, dass nur der Benutzer B die Nachricht lesen kann. Zur Sicherung der Übertragung erzeugt der Benutzer A einen geheimen Schlüssel, verschlüsselt die Nachricht mit diesem Schlüssel und sendet sie dem Benutzer B. Der Benutzer A wählt dann, wie er den geheimen Schlüssel an den Benutzer B übergibt - er braucht den geheimen Schlüssel, um die verschlüsselte Nachricht lesen zu können. Nachdem der Benutzer B den geheimen Schlüssel empfangen hat, kann er die Nachricht entschlüsseln, um den ursprünglichen Text zu erhalten.



2.1 Kryptographie mit symmetrischen Schlüsseln

Jeder Verschlüsselungsalgorithmus muss die folgenden Anforderungen erfüllen:

- Diffusion: Jedes Bit des Klartextes beeinflusst viele Bits des Geheimtextes und jedes Bit des Geheimtextes wird von vielen Bits des Klartextes beeinflusst.
- Konfusion: Man soll strukturierte Beziehungen (insbesondere Linearität) zwischen dem Klar- und Geheimtext vermeiden, auf denen bekannte Angriffe basieren.
- Zufälligkeit: Der Geheimtext soll als zufällig gewählt aussehen und gute statistische Eigenschaften haben.
- Einfachheit.

- Effizienz: Der Verschlüsselungsalgorithmus soll in verschiedenen Hard- und Softwareplattformen äußerst schnell arbeiten.

Das größte Problem der symmetrischen Kryptosysteme liegt darin, dass der Prozess der Übertragung der Schlüssel zum Empfänger empfindlich gegen Sicherheitsrisiken ist. Die Übertragung des geheimen Schlüssels via Internet in einer E-Mail-Nachricht ist unsicher. Eine verbale, telefonische Kommunikation des Schlüssels kann abgehört werden. Ähnlich riskant ist die Briefpost, da ein Abfangen möglich ist.

Die Sicherheitsrisiken der Kryptographie mit geheimen Schlüsseln wurden durch die Kryptographie mit öffentlichen Schlüsseln weitgehend beseitigt. Symmetrische Kryptosysteme werden häufig zur Verschlüsselung von Daten auf Festplatten verwendet. Die Person, welche die Daten verschlüsselt, hat den Schlüssel bereits und es gibt kein Problem mit der Schlüsselverteilung.

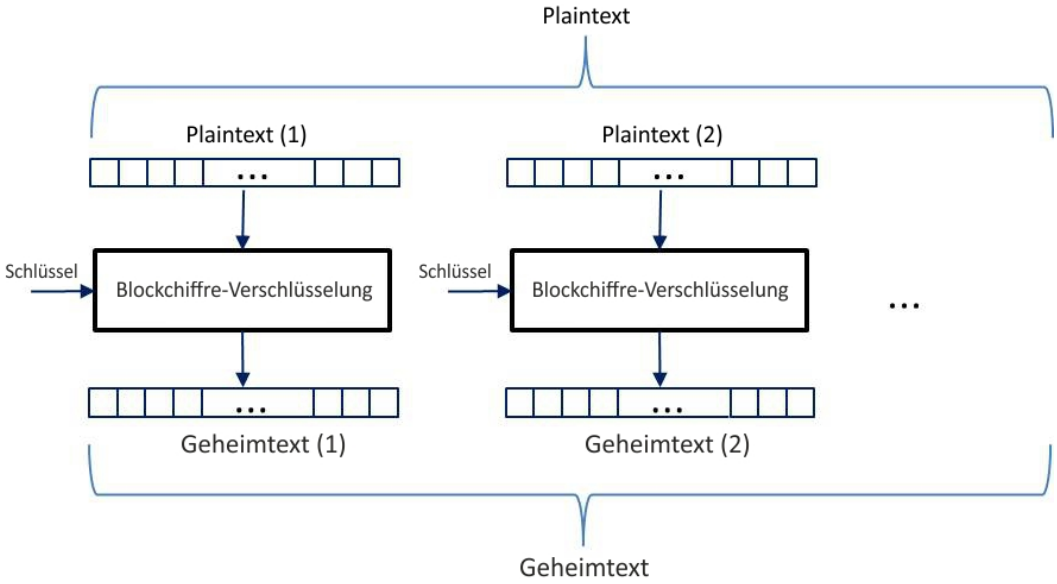
Wie schon in der vorigen Sektion erwähnt wurde, gibt es eine wichtige Aufteilung der symmetrischen Kryptosysteme in Strom- und Blockchiffren. Heutzutage wird der Einsatz von Blockchiffren den Stromchiffren vorgezogen.

2.1 Algorithmen der Blockchiffren

Blockchiffren transformieren eine Gruppe von Symbolen des Klartextes in eine Gruppe von Symbolen des Geheimtextes. So wird die Verschlüsselung des Klartextes blockweise realisiert.

Die Symbole des Klartextes werden in Blöcke gruppiert und eine kryptographische Transformation wird dann mittels des Schlüssels angewendet. Das Ergebnis der Verschlüsselung ist ein Block des Geheimtextes, der die Größe des Klartextes besitzt.

Die Größe des Klartextes muss dem Mehrfachen der Blocklänge nicht genau entsprechen. Dann wird üblicherweise der letzte Block durch Padding gefüllt. In Abhängigkeit vom Betriebsmodus muss jedoch kein Padding erforderlich sein. Das Prinzip der Ver- und Entschlüsselung auf der Basis der Blockchiffre ist auf dem folgenden Bild gezeigt.



2.2 Modell der Blockchiffre

Die meisten Blockchiffren arbeiten in einem iterierten Modus. Das heißt, dass die Verschlüsselung über viele Runden erfolgt. Jede Runde wiederholt eine Reihe von Operationen mit den Daten mittels eines unterschiedlichen „Subschlüssels“, der von dem ursprünglichen Schlüssel abgeleitet wurde. Die Operationen in jeder Runde umfassen normalerweise eine Substitution, Permutation und Erweiterung von Schlüsseln. Diese Chiffren sind als *Substitutions-Permutations-Netzwerke* (**SPN**, engl. *substitution-permutation network*) und Feistelchiffren bekannt. Weil die Substitution häufig der einzige nichtlineare Teil der meisten Chiffren ist, werden S-Boxen (engl. *substitution box*) sehr sorgfältig gewählt werden, um einen guten Schutz gegen kryptographische Angriffe zu gewährleisten.

Die Entschlüsselung erfolgt analogisch. Dabei wird auf Blöcke des Geheimtextes dieselbe Transformation mittels des gleichen Schlüssels (bei symmetrischen Kryptosystemen) wie bei der Verschlüsselung angewendet. Das Ergebnis dieses Prozesses sind entschlüsselte Blöcke des Klartextes.

Typischerweise haben die Blöcke des Klar- und Geheimtextes 64 oder 128 Bits.

Vorteile der Blockchiffren:

- hohe Diffusion
- Immunität gegen Verfälschung (es ist schwierig, Symbole hinzuzufügen, ohne entdeckt zu werden)

Die meistverwendeten Algorithmen der Blockchiffren sind:

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Es wird nicht empfohlen, dieselben Bits des geheimen Schlüssels zur Verschlüsselung der gleichen Teile des Klartextes zu verwenden. Wenn ein Algorithmus für mehrere identische Blöcke des Klartextes angewendet wird, werden mehr identische Blöcke des Geheimtextes erzeugt. Es stehen Möglichkeiten zur Verfügung, die Blöcke des Klartextes mit den Blöcken des Geheimtextes zu verdecken und zu mischen, die den Angriffen durch Modifizierung der Blöcke vorbeugen. Diese Methoden werden als Betriebsmodi der Blockchiffren bezeichnet.

Betriebsmodi der Blockchiffren

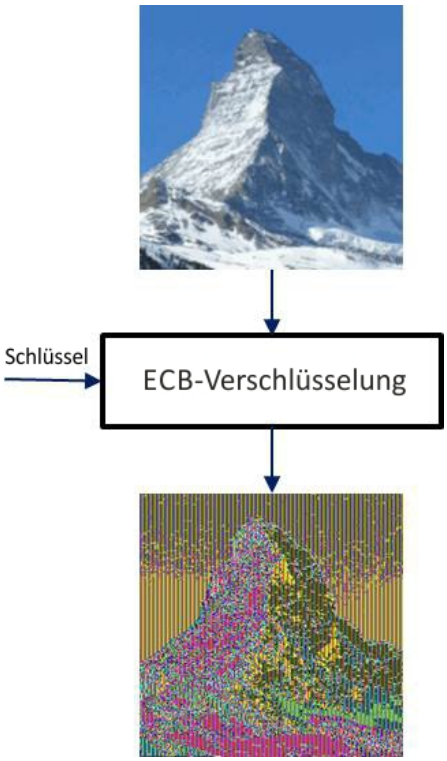
Blockchiffren können auf verschiedene Art und Weise für die Geheimhaltung und Fehlerbehebung eingesetzt werden. Die Wahl des Betriebsmodus beeinflusst die Geschwindigkeit, die Geheimhaltung und die Fehlerfortpflanzung.

ECB-Modus (Electronic Code Book)

Dieser Modus stellt die grundlegende Chiffre ohne jede Modifizierung dar. Die Nachricht wird in Blöcke aufgeteilt und jeder Block des Klartextes wird gesondert, unabhängig von anderen verschlüsselt. Daher gibt es keine gegenseitige Abhängigkeit zwischen den Blöcken und als Folge davon wird dieser Modus nicht empfohlen. Die Anwendung dieses Modus bringt einige Nachteile:

- verbleibende offene Struktur des Klartextes
- Empfindlichkeit gegen Angriffe durch Modifizierung der Blöcke (sie können umgestellt werden und ihre Umstellung oder Wiederholung kann die Nachricht ändern)
- Möglichkeit der Ausnutzung eines mit demselben Schlüssel verschlüsselten Geheimtextes als Quelle für Angreifer

Eine typische Schwachstelle der ECB-Verschlüsselung ist die Kodierung eines Bitmap-Bildes (z. B. eine bmp-Datei). Nicht einmal ein so starker Verschlüsselungsalgorithmus, der den ECB-Modus verwendet, kann seinen Inhalt nicht effizient verdecken.

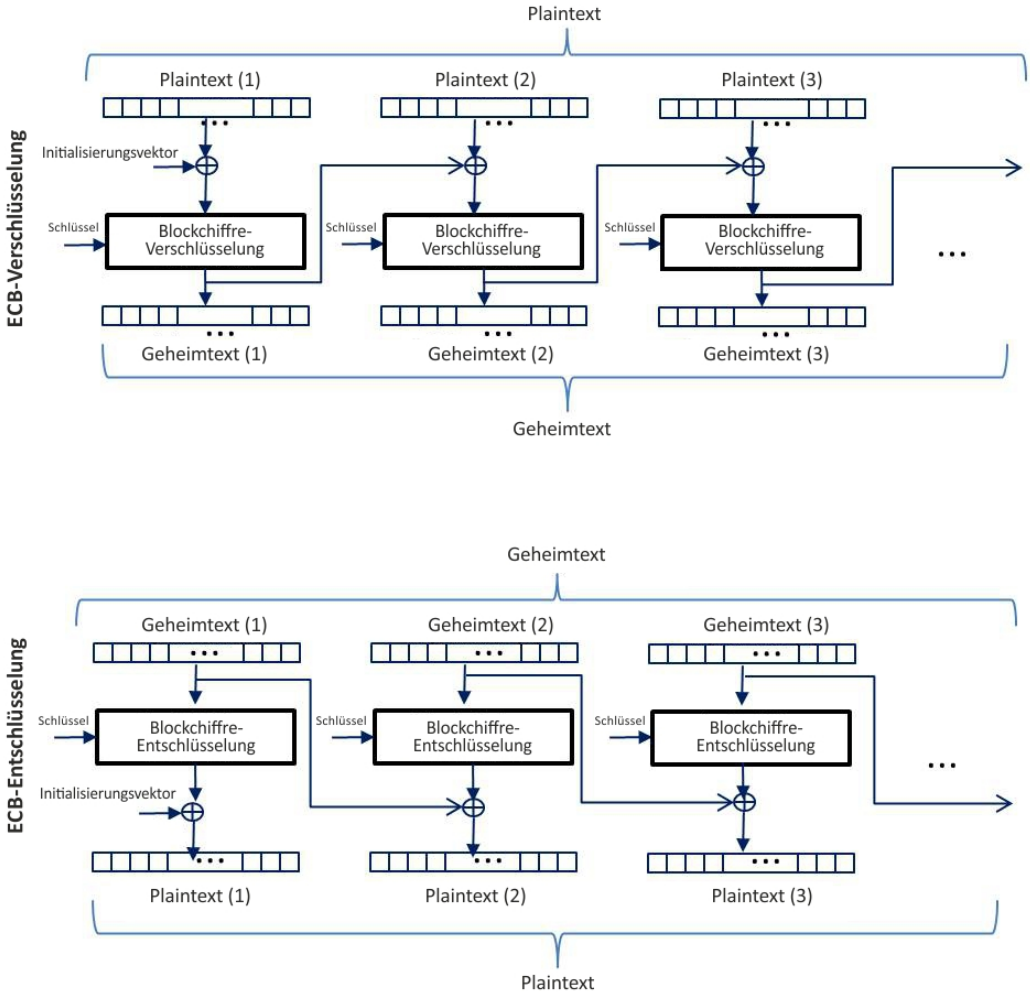


2.3 Verschlüsselung eines bmp-Bildes im ECB-Modus

CBC-Modus (Cipher Block Chaining)

Der CBC-Modus kombiniert („verkettet") Blöcke des Klartextes mit vorigen Blöcken des Geheimtextes. Dazu ist ein Initialisierungsvektor IV erforderlich, der mit dem ersten Block des Klartextes kombiniert wird.

Vor der Verschlüsselung an sich wird die Operation XOR mit dem Vektor IV und dem ersten Block des Klartextes durchgeführt. Das Ergebnis wird danach verschlüsselt und damit erhält man den ersten Block des Geheimtextes. Für die weiteren Blöcke wird der vorige Geheimtext anstatt IV angewendet. Die Verkettung führt dazu, dass der Block g_j des Geheimtextes vom Block k_j des Klartextes und vom vorigen Block des Geheimtextes g_{j-1} abhängig ist. So kann man sagen, dass der Block g_j des Geheimtextes vom aktuellen und allen vorigen Blöcken des Klartextes abhängt.



2.4 Ver- und Entschlüsselung im CBC-Modus

Die Verwendung des CBC-Modus löst die Nachteile des ECB-Modus, aber hat zwei eigene Nachteile:

- Parallele Verschlüsselung ist nicht möglich. Der Block k_{j+1} kann nicht vor oder während der Verschlüsselung des Blocks k_j verschlüsselt werden, weil man noch g_j braucht. Eine parallele Entschlüsselung ist jedoch möglich: Der Block k_j des Klartextes erfordert die Blöcke g_j und g_{j-1} des Geheimtextes.

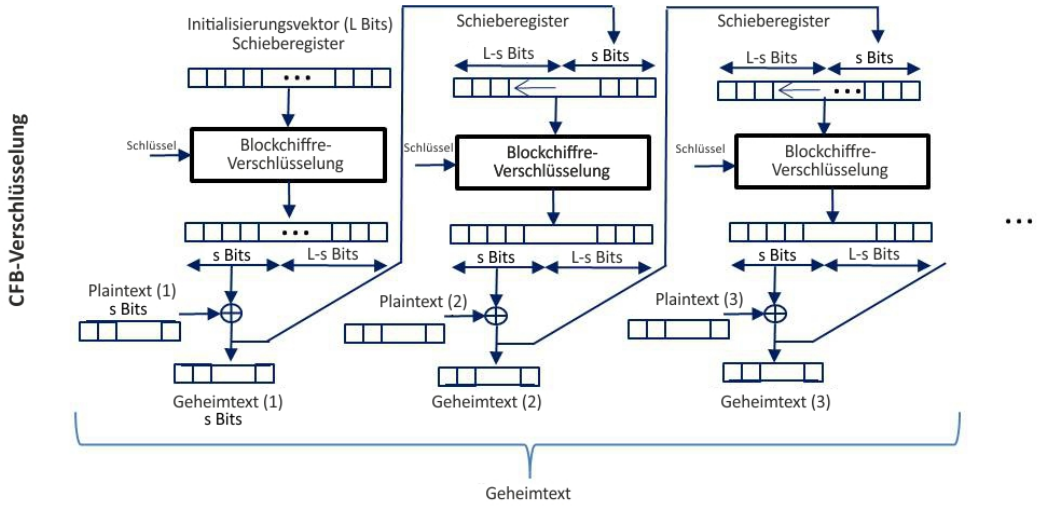
- Fehlerfortpflanzung. Ein Fehler in einem einzigen Bit während der Übertragung des Blocks g_j wird nicht nur zu einem Fehler im Block k_j, sondern auch zu einem Fehler im Block k_{j+1} führen. Jedoch nur ein Bit des Block k_{j+1} wird beeinflusst. Dies wird als eine „beschränkte Fehlerfortpflanzung" bezeichnet.

CFB-Modus (Cipher Feedback)

Laut der Definition von NIST ist der CFB-Modus ein Vertraulichkeitsmodus, der die Rückkopplung der nacheinander folgenden Segmente des Geheimtextes in die Eingangsblöcke des Klartextes einschließt, um Ausgangsblöcke zu generieren. Mit diesen Blöcken und mit dem Klartext wird dann die XOR-Operation ausgeführt,

um den Geheimtext zu erzeugen. Ein wichtiger Parameter in diesem Modus ist die ganze Zahl s, wobei $1 \leq s \leq L$. L ist dabei die Länge des Blocks.

Der erste Eingangsblock ist der Initialisierungsvektor IV. Im Prinzip nimmt der CFB-Verschlüsselungsprozess als Eingang die L-s niedrigstwertigen Bits des vorigen Eingangs zusammen mit den s Bits des vorigen Geheimtextes und verschlüsselt sie. Dann werden mit den s höchstwertigen Bits und den entsprechenden s Bits des Blocks des Klartextes die XOR-Operation ausgeführt, um den nächsten Block des Geheimtextes zu erzeugen. Dieser Modus wird auf dem folgenden Bild gezeigt.



2.5 CFB-Verschlüsselung

Falls s=1, transformiert der CFB die Blockchiffre in eine Stromchiffre und verschlüsselt die einzelnen Bits.

Dieser Modus kann wie der CBC-Modus nicht parallel eingesetzt werden. Das heißt, dass mehrere Chiffreoperationen bei der Verschlüsselung nicht durchgeführt werden können, aber bei der Entschlüsselung schon.

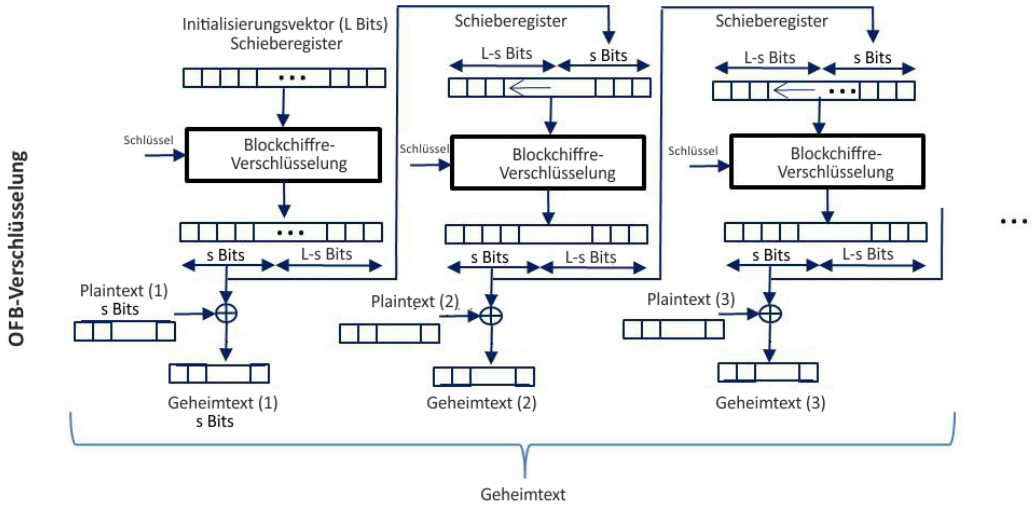
Was die Fehlerfortpflanzung betrifft, ein Fehler in einem Bit des Geheimtextes verursacht einen Fehler nicht nur in dem entsprechenden Block des Klartextes, jedoch auch Fehler in den folgenden Blöcken des Klartextes.

OFB-Modus (Output Feedback)

Der OFB-Modus arbeitet wie folgt:

Der erste Eingangsblock ist der Initialisierungsvektor IV. Der entsprechende Eingangsblock wird verschlüsselt und die s höchstwertigen Bits des Ausgangs dieser Verschlüsselung werden auf zwei Weisen verwendet: als Eingang des nächsten Blocks und als Summand mit s Bits des Klartextblocks für die XOR-Summe. So wird der Ergebnisblock des Geheimtextes erzeugt.

OFB ist tatsächlich eine Form der Stromchiffre. Der OFB-Modus wird auf dem folgenden Bild gezeigt.



2.6 OFB-Verschlüsselung

Es ist offensichtlich, dass Fehler in diesem Modus nicht fortgepflanzt werden - ein Fehler in einem Bit in g_j beeinflusst nur das entsprechende Bit in k_j.

Der Hauptvorteil des OFB-Modus im Vergleich mit dem CFB-Modus ist der folgende:

Falls IV bekannt ist, können die Ausgangsblöcke vorverarbeitet werden, bevor man den Klartext (oder Geheimtext bei der Entschlüsselung) kennt.

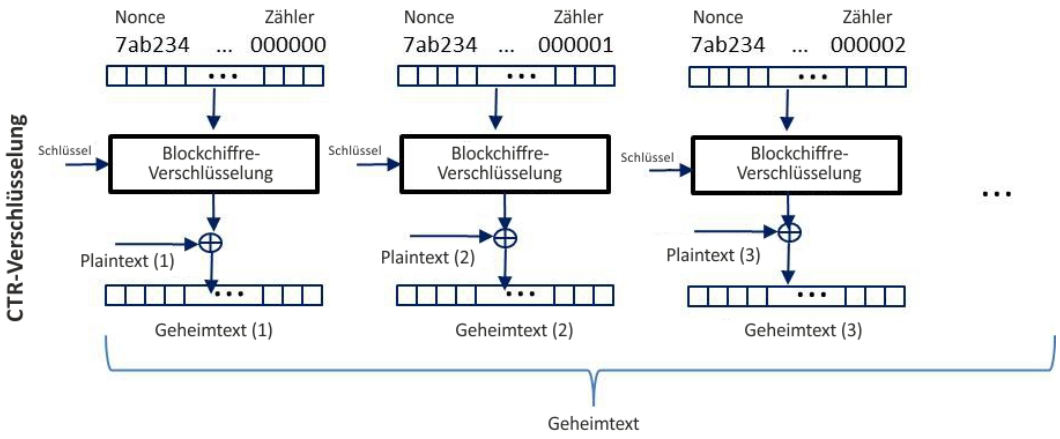
Der OFB-Modus hat die folgenden Nachteile:

Weder die Ver- noch Entschlüsselung können parallel ausgeführt werden, weil jeder Eingangsblock von den Ergebnissen der vorigen Verschlüsselungsfunktion abhängt.

Weil es hier keine Fehlerfortpflanzung gibt, kann ein aktiver Angreifer den Klartext ändern, um Auswirkungen auf den Geheimtext zu beobachten.

CTR-Modus (Counter)

Der CTR-Modus basiert auf der Verschlüsselung einer Menge von Eingangsblöcken, die als Zähler bezeichnet werden. Mit den Ausgangsblöcken und dem Klartext wird dann die XOR-Operation ausgeführt, um den Geheimtext zu generieren, und umgekehrt. Nach der Initialisierung des Zählers werden die weiteren Zählerblöcke mittels der Inkrementfunktion abgeleitet. Der Zähler ist üblicherweise in zwei Sektionen aufgeteilt: Nummer der Nachricht und Nummer des Blocks im Rahmen der Nachricht. Dabei ist es entscheidend, dass sich der Wert des Zählers für den gleichen Schlüssel nicht wiederholt. Der CTR-Modus wird auf dem folgenden Bild gezeigt.



2.7 CTR-Verschlüsselung

In diesem Modus werden Fehler nicht fortgepflanzt - falls ein Block infolge eines Übertragungsfehlers modifiziert ist, wird nur dieser Block falsch entschlüsselt.

Hauptvorteile des CTR-Modus:

Sowohl CTR-Verschlüsselung als auch CTR-Entschlüsselung können parallel ausgeführt werden - es gibt keine Verbindung zwischen den einzelnen Prozessen.

Eine Vorverarbeitung ist möglich: die Verschlüsselungsfunktionen können verwendet werden, bevor man den Klartext (oder Geheimtext bei der Entschlüsselung) kennt.

Hauptnachteil:

Wie beim OFB-Modus kann ein Angreifer den Klartext kontrolliert ändern.

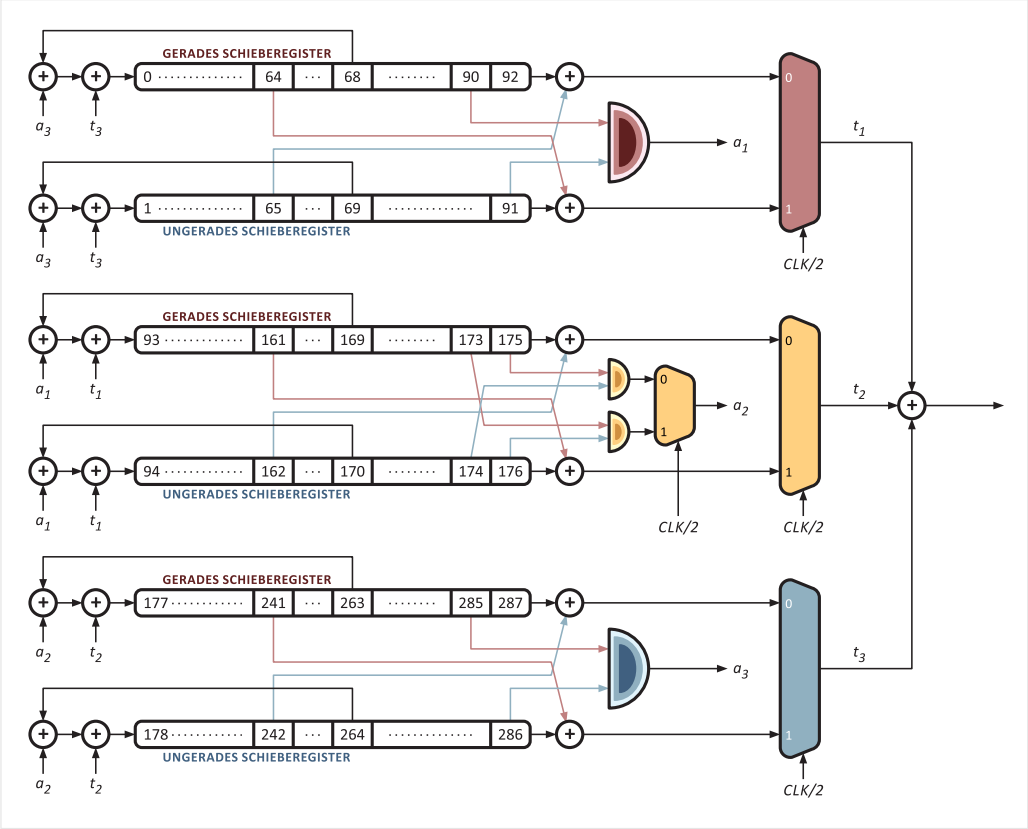
Allgemeine Bemerkungen

Der CBC-Modus ist der Beste für eine allgemeine Verschlüsselung von Dateien oder Paketen. Wenn eine hohe Geschwindigkeit der Verschlüsselung gefordert wird, sollte man den CTR-Modus wählen. Wenn Fehlerfortpflanzung vermieden werden soll und es Rauschen im Übertragungskanal gibt, ist OFB eine gute Variante. Und wenn es ein Risiko gibt, dass ein Byte oder ein Bit gelöscht wird, sollte der CFB-Modus mit s=8 oder s=1 eingesetzt werden.

2.2 Algorithmen der Stromchiffren

Ein Stromchiffre ist eine symmetrische Chiffre, die mit einer zeitabhängigen Transformation der einzelnen Elemente des Klartextes arbeitet. Dies wird durch Hinzufügen eines Elementes vom Schlüsselstrom in ein Element des Klartextes erreicht. Der Schlüsselstrom ist eine pseudozufällige Folge (eine Folge, die für einen Angreifer als zufällig erscheint), die von einem endlichen Automaten erzeugt wird. Der Anfangszustand des Automaten wird von einem geheimen Schlüssel und einem öffentlichen Parameter bestimmt.

Die Sicherheit einer Stromchiffre ist völlig vom Schlüsselstrom abhängig. Er muss unvorhersehbar sein, um einem Angriff erfolgreich vorzubeugen.



2.8 Trivium, Beispiel einer Stromchiffre

Stromchiffren fordern manchmal weniger Ressourcen (z. B. Größe des Codes oder Chips) für ihre Implementierung im Vergleich mit Blockchiffren. Deshalb sind sie für die Anwendung in beschränkten Umgebungen attraktiv, z. B. für Handys.

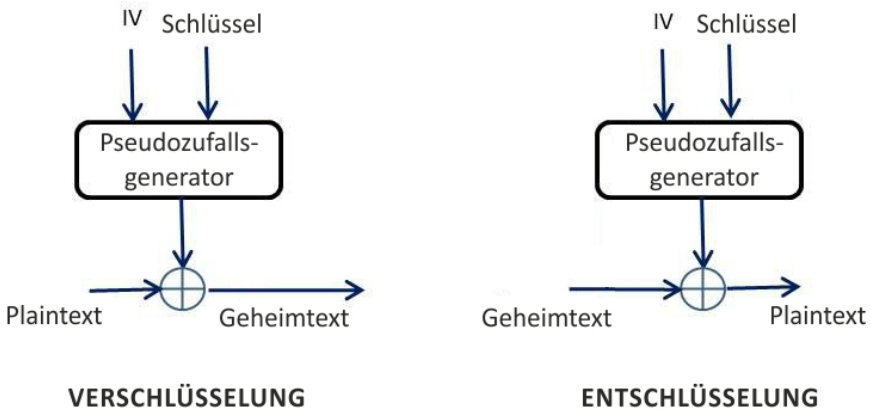
In vielen Bereichen (z. B. Internetsicherheit) sind sie weniger beliebt als Blockchiffren. Es gibt jedoch auch Ausnahmen: z. B. Stromchiffre RC4.

Typen der Stromchiffren

Eine Stromchiffre generiert aufeinanderfolgende Elemente des Schlüsselstroms auf der Basis des internen Zustandes. In einer synchronen Stromchiffre wird der Mechanismus der Zustandsaktualisierung unabhängig vom Klar- und Geheimtext aktualisiert. Im Gegenteil dazu aktualisieren selbstsynchronisierende Stromchiffren ihren Zustand aufgrund der Elemente des vorigen Geheimtextes.

Synchrone Stromchiffren

Eine synchrone Stromchiffre ist eine solche Stromchiffre, in der der Schlüsselstrom unabhängig von dem Klar- und Geheimtext generiert wird. Der Schlüsselstrom wird üblicherweise von einem Pseudozufallsgenerator erzeugt und mit dem geheimen Schlüssel des ganzen Prozesses parametrisiert.



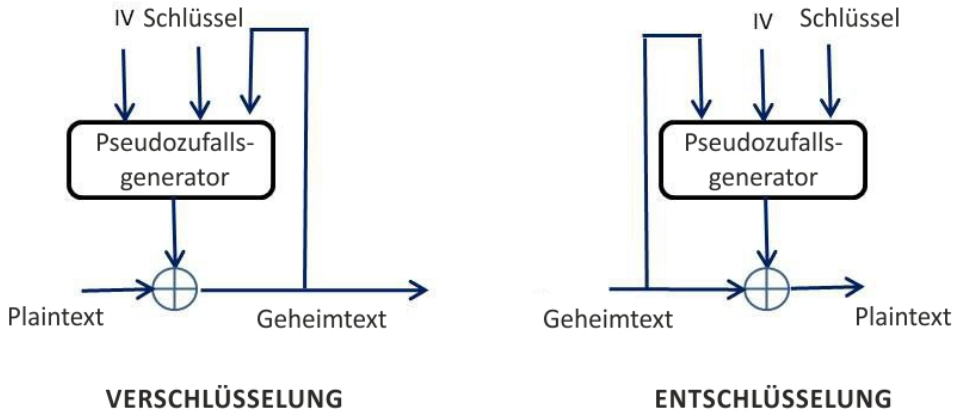
2.9 Synchrone Stromchiffre

Die wichtigsten Eigenschaften der synchronen Stromchiffren umfassen:

- Keine Fehlerfortpflanzung. Ein Fehler eines einzigen Bits in g_j beeinflusst nur das entsprechende Bit in k_j. Der Übertragungsfehler beeinflusst die Entschlüsselung weiterer Elemente nicht.
- Für eine richtige Entschlüsselung müssen der Sender und Empfänger synchronisiert werden. Wenn ein Bit bei der Übertragung hinzugefügt oder gelöscht wird, müssen sie noch einmal synchronisiert werden.

Selbstsynchronisierende Stromchiffren

In selbstsynchronisierenden Stromchiffren hängt der Schlüsselstrom vom geheimen Schlüssel, aber auch von der Zahl *t* der Elemente des Geheimtextes ab, die schon erzeugt oder gelesen wurden. Damit unterscheiden sich selbstsynchronisierende Stromchiffren von synchronen Stromchiffren.



2.10 Selbstsynchronisierende Stromchiffre

Die selbstsynchronisierenden Stromchiffren haben die folgenden Eigenschaften:

- Selbstsynchronisierung. Wenn einige Bits des Geheimtextes gelöscht, hinzugefügt oder geändert werden, ist die Chiffre imstande, die richtige Entschlüsselung nach einigen Bits automatisch wiederherzustellen.
- Begrenzte Fehlerfortpflanzung. Die Auswirkung eines Fehlers eines Bits ist begrenzt: nur einige Elemente des Geheimtextes werden falsch entschlüsselt.

3 Kryptographie mit öffentlichen Schlüsseln

Die Kryptographie mit öffentlichen Schlüsseln wurde entwickelt, um die Sicherheitsprobleme der symmetrischen Verschlüsselung zu lösen. Dies wurde durch Verwendung von zwei Schlüsseln anstatt nur eines Schlüssels erreicht. Dabei wird ein Schlüssel zur Verschlüsselung und der andere zur Entschlüsselung eingesetzt.

Dieses System wird als ein asymmetrisches Kryptosystem bezeichnet, weil beide Schlüssel zum Vollenden des Prozesses notwendig sind. Diese zwei Schlüssel sind als Schlüsselpaar bekannt. In einem asymmetrischen Kryptosystem ist einer der Schlüssel frei verfügbar. Daher wird dieses Verfahren auch als Kryptographie mit öffentlichen Schlüsseln bezeichnet. Der andere Schlüssel wird dann als geheimer oder privater Schlüssel bezeichnet. Wie sein Namen schon ahnen lässt, ist er nicht verteilbar, sondern muss vertraulich beim entsprechenden Inhaber bleiben. Weil das Schlüsselpaar in einer mathematischen Beziehung steht, können die Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden und umgekehrt. An dieser Stelle ist darauf hinzuweisen, dass es nahezu unmöglich ist, den privaten Schlüssel von dem öffentlichen Schlüssel abzuleiten.

Der größte Nachteil der asymmetrischen Kryptosysteme besteht darin, dass der private Schlüssel nach einer ausreichenden Zeitdauer und mit genug Rechenleistung schließlich doch vom öffentlichen Schlüssel entdeckt und damit die Nachricht entschlüsselt werden kann. Deshalb beruhen diese Systeme auf Schlüssel, die wirklich groß sind (üblicherweise mit 1024 oder 2048 Bits). Je länger die verwendeten Schlüssel sind (d. h. je mehr Bits sie haben), desto schwieriger ist die Brute-Force-Entschlüsselung.

Die Algorithmen der Kryptographie mit öffentlichen Schlüsseln basieren auf mathematischen Problemen, die zurzeit keine effiziente Lösung haben. Für den Benutzer ist es leicht, ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel zu generieren und sie zur Ver- und Entschlüsselung einzusetzen. Diese mathematische Komplexität erschwert wesentlich die Ableitung eines richtig erzeugten privaten Schlüssels vom öffentlichen Schlüssel. Die Sicherheit der asymmetrischen Kryptosysteme wird so geschützt und die Stärke des Algorithmus besteht in dieser Schwierigkeit. So kann der öffentliche Schlüssel bekanntgemacht werden, ohne dass die Sicherheit eines solchen Systems gefährdet wird. Die Sicherheit hängt nur von der Geheimhaltung des privaten Schlüssels ab. Die Algorithmen mit öffentlichen Schlüsseln, im Gegensatz zu symmetrischen Kryptosystemen, erfordern keinen sicheren Kanal für den initialen Austausch eines geheimen Schlüssels (oder mehrerer solcher Schlüssel) zwischen den kommunizierenden Parteien.

Asymmetrische Kryptosysteme werden für zwei Zwecke verwendet: Verschlüsselung mit öffentlichen Schlüsseln und digitale Signaturen. Die Verschlüsselung mit öffentlichen Schlüsseln wird zur Verschlüsselung geheimer Nachrichten verwendet, wobei nur die Person, die den geheimen Schlüssel besitzt, die Nachricht entschlüsseln und lesen kann. Eine digitale Signatur ist eine

Nachricht, die mit einem geheimen Schlüssel des Senders unterzeichnet wird und von jeder Person verifiziert werden kann, die auf den öffentlichen Schlüssel des Senders zugreifen kann. Beide Anwendungen stellen Beispiele der Vertraulichkeit und Authentizität der Daten mittels der Kryptographie mit öffentlichen Schlüsseln dar.

Im Vergleich zu Algorithmen mit geheimen Schlüsseln sind Algorithmen mit öffentlichen Schlüsseln langsam. Um dieses Problem zu lösen, wird ein öffentlicher Schlüssel zur Verteilung des geheimen Schlüssels eingesetzt. Dieser geheime Schlüssel wird dann zur Verschlüsselung der Benutzerinformation verwendet.

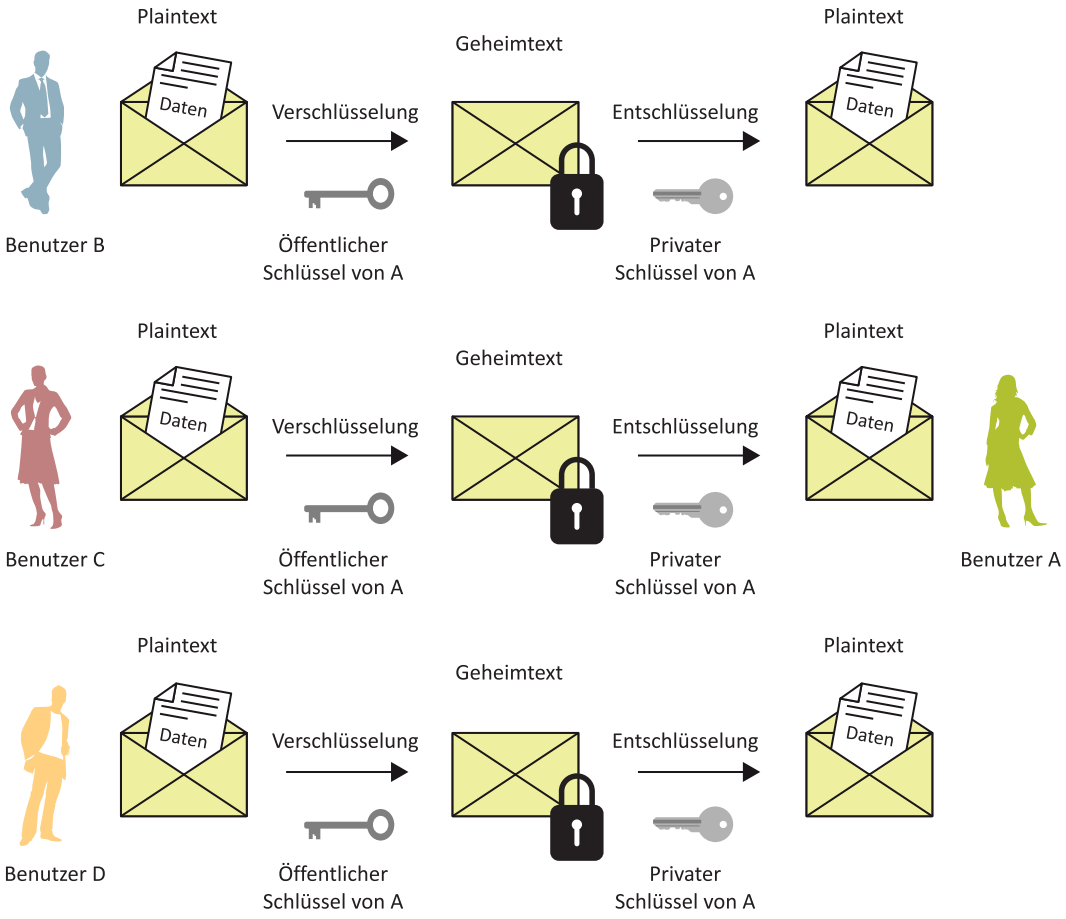
Weil die Schlüsselverwaltung viel einfacher bei den asymmetrischen Kryptosystemen im Vergleich zu den symmetrischen ist, wird häufig falsch angenommen, dass sie sogar trivial ist. Darüber hinaus glauben Benutzer auch fälschlicherweise, dass die Verschlüsselung mit einem öffentlichen Schlüssel sicherer als symmetrische Verschlüsselung ist. Tatsächlich hängt die Sicherheit jedes Systems von der Länge seines Schlüssels und dem Rechenaufwand ab, der zum Knacken der Chiffre gebraucht wird.

Der meistverwendete Algorithmus mit öffentlichen Schlüsseln ist ***RSA***.

3.1 Funktionsweise der Kryptographie mit öffentlichen Schlüsseln

Anwendung der Kryptographie mit öffentlichen Schlüsseln zum Zwecke der Vertraulichkeit

Nehmen wir ein Beispiel: Benutzer B möchte eine Nachricht dem Benutzer A senden. Der Benutzer B verschlüsselt die Nachricht mittels des öffentlichen Schlüssels des Benutzers A und der Benutzer A entschlüsselt die Nachricht mit seinem eigenen privaten Schlüssel. Weil diese zwei Schlüssel ein Schlüsselpaar schaffen, kann nur der private Schlüssel des Benutzers A die Datei entschlüsseln. Wenn eine andere Person den Geheimtext abfängt, wird sie nicht imstande sein, ihn zu entschlüsseln, weil nur der private Schlüssel des Benutzers A zur Entschlüsselung verwendet werden kann. Dieses Verfahren bietet keine Authentifizierung, dass die Nachricht wirklich vom Benutzer B stammt, weil der öffentliche Schlüssel des Benutzers A allen bekannt werden kann. Es garantiert jedoch die Vertraulichkeit der Nachricht, weil nur der Benutzer A die Nachricht entschlüsseln kann.

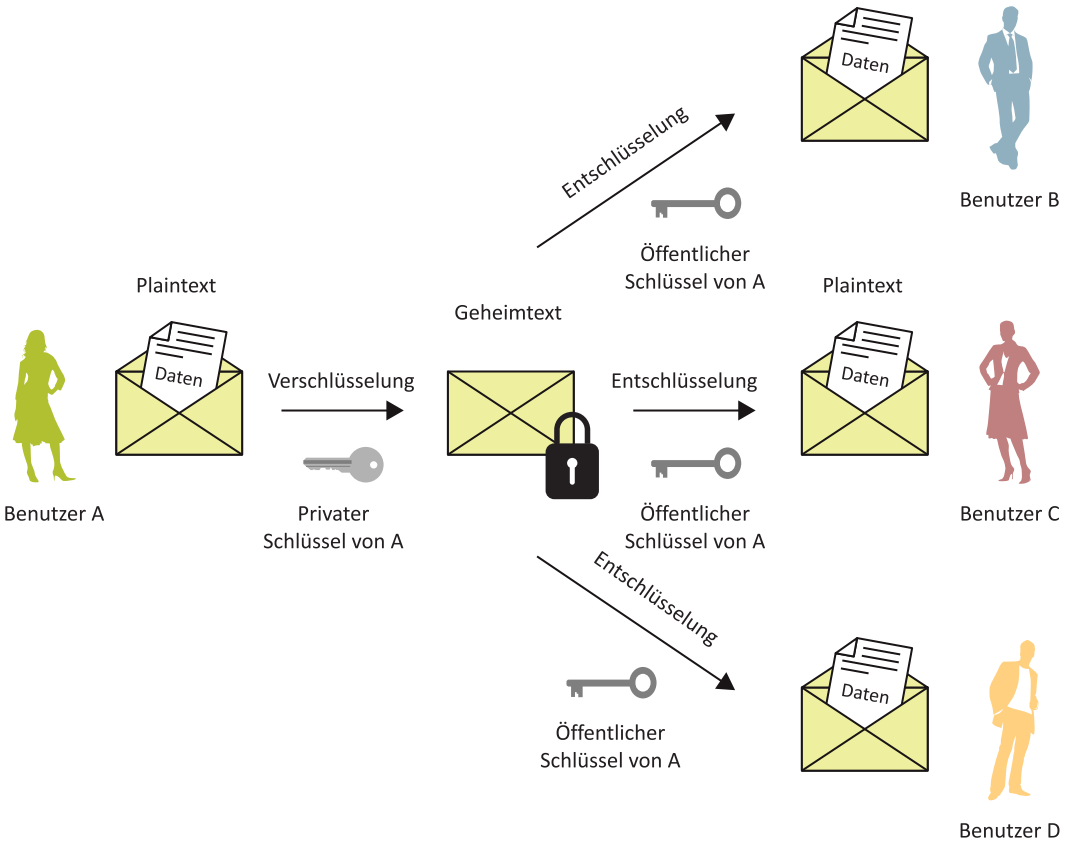


3.1 Modell der Kryptographie mit öffentlichen Schlüsseln (zum Zwecke der Vertraulichkeit des Dateninhaltes)

Dieses Verfahren stellt eindeutig sicher, dass Daten, die einem Benutzer gesendet werden, nur mit seinem öffentlichen Schlüssel verschlüsselt werden können, falls die Vertraulichkeit erforderlich ist. Analogisch kann die Entschlüsselung nur mittels des privaten Schlüssels erfolgen, welchen der Empfänger der Daten besitzt. Daher können Nachrichten sicher ausgetauscht werden. Sender und Empfänger brauchen keinen geteilten Schlüssel, wie bei der symmetrischen Verschlüsselung. Die ganze Kommunikation erfordert nur öffentliche Schlüssel, private Schlüssel werden weder übertragen noch geteilt.

Anwendung der Kryptographie mit öffentlichen Schlüsseln zum Zwecke der Authentifizierung

Zur Authentifizierung muss der Benutzer A die Nachricht mit seinem privaten Schlüssel verschlüsseln und der Benutzer B wird sie mit dem öffentlichen Schlüssel des Benutzers A entschlüsseln. So wird die Authentifizierung geleistet, dass die Nachricht vom Benutzer A stammt, aber es wird keine Vertraulichkeit garantiert, weil der öffentliche Schlüssel des Benutzers A allen bekannt ist. Daher kann jede Person mit dem öffentlichen Schlüssel des Benutzers A die Nachricht entschlüsseln.



3.2 Modell der Kryptographie mit öffentlichen Schlüsseln (zum Zwecke der Authentifizierung der Datenquelle)

Anwendung der Kryptographie mit öffentlichen Schlüsseln zum Zwecke der Authentifizierung und Vertraulichkeit

Um sowohl die Vertraulichkeit als auch Authentifizierung sicherzustellen, muss der Benutzer B den Klartext zuerst mit seinem privaten Schlüssel verschlüsseln, wobei

die Authentifizierung garantiert wird. Dann wird der Benutzer B den öffentlichen Schlüssel des Benutzers A zur Verschlüsselung der Nachricht verwenden, um die Vertraulichkeit zu garantieren.

Der Nachteil dieses Systems besteht darin, dass es sehr zeitaufwendig und komplex ist, weil die Ver- und Entschlüsselung mit öffentlichen Schlüsseln viermal durchgeführt werden muss und der Schlüssel lang sein muss (1024 bis 4094 Bits).

4 Hybride Systeme: Kombinationen der symmetrischen und asymmetrischen Verschlüsselung

Der Nachteil der Kryptographie mit öffentlichen Schlüsseln besteht in der ziemlich langen Dauer des Prozesses, weil die Schlüssel lang sind (1024 bis 4094 Bits). Die symmetrische Kryptographie ist dagegen viel schneller, weil ihre Schlüssel kürzer sind (40 bis 256 Bits). Ihr Problem liegt jedoch in der Verteilung der Schlüssel. Beide Verfahren können zusammen eingesetzt werden, um eine bessere Verschlüsselung zu bieten. So können Vorteile durch Kombination genutzt und Nachteile überwunden werden.

Konkret verwenden hybride Systeme Algorithmen mit öffentlichen Schlüsseln für eine sichere Teilung des geheimen Schlüssels der symmetrischen Kryptosysteme. Die Nachricht an sich wird dann mit dem empfangenen geheimen Schlüssel verschlüsselt und dann dem Empfänger gesendet. Weil das Verfahren der Schlüsselteilung sicher ist, wird der symmetrische Schlüssel zur Verschlüsselung für jede gesendete Nachricht geändert. Daher wird er manchmal als Sitzungsschlüssel (engl. *session key*) bezeichnet. Wenn ein solcher Sitzungsschlüssel abgefangen wird, kann damit der Abfänger nur die spezifische Nachricht entschlüsseln, die mit diesem Schlüssel verschlüsselt wurde. Um weitere Nachrichten zu entschlüsseln, müsste der Abfänger weitere Sitzungsschlüssel abfangen.

Der Sitzungsschlüssel, der mit dem Algorithmus der öffentlichen Schlüssel verschlüsselt wurde, und die zu sendende Nachricht, die mit dem Algorithmus der geheimen Schlüssel verschlüsselt wurde, werden automatisch zusammen gepackt. Der Empfänger verwendet seinen privaten Schlüssel zur Entschlüsselung des Sitzungsschlüssels und diesen Sitzungsschlüssel zur Entschlüsselung der Nachricht. Viele Anwendungen setzen dieses System ein.

Dieses kombinierte Verfahren hat die folgenden grundlegenden Schritte:

1. Verschlüsselung des Klartextes mittels eines zufälligen Schlüssels (eines symmetrischen Kryptosystems).

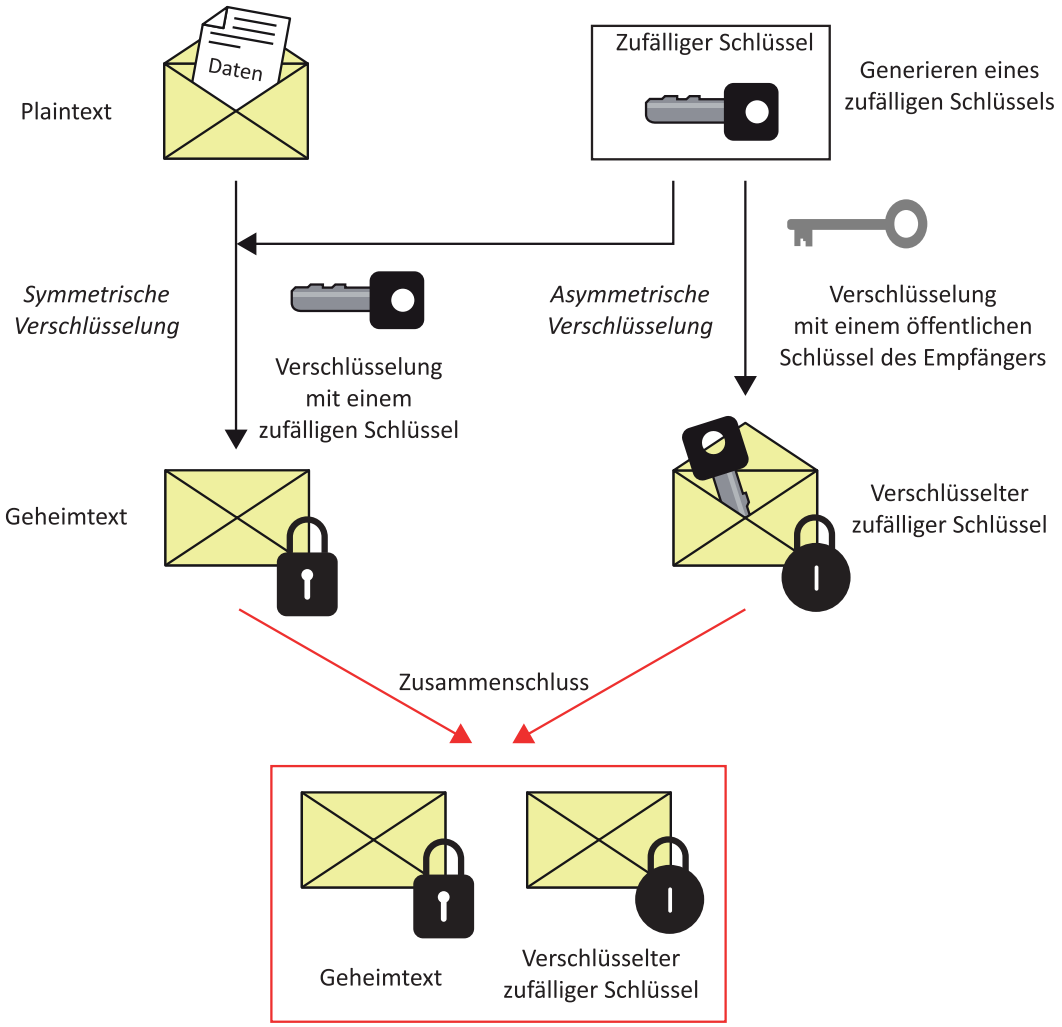
2. Verschlüsselung dieses zufälligen Schlüssels mittels des öffentlichen Schlüssels des Empfängers (eines asymmetrischen Kryptosystems). Senden des verschlüsselten zufälligen Schlüssels dem Empfänger. Der Empfänger kann jetzt den zufälligen Schlüssel mit seinem privaten Schlüssel entschlüsseln.

3. Senden der verschlüsselten Daten. Diese verschlüsselten Daten können mit dem Schlüssel entschlüsselt werden, der mittels des öffentlichen Schlüssels vom asymmetrischen Schlüsselpaar verschlüsselt wurde.

Diese hybriden Verschlüsselungssysteme sind weitverbreitet. Beispiel einer Anwendung ist *Secure Shell* (**SSH**) zur Sicherung der Kommunikation zwischen dem Kunden und dem Server und *Pretty Good Privacy* (**PGP**) zum Senden von Nachrichten. Vor allem ist dieses Verfahren das Herzstück von *Transport Layer*

Security (**TLS**), die stark von Webbrowsern und -servern zur Sicherstellung eines sicheren Kommunikationskanals genutzt wird.

Dieses Verfahren wird auf dem folgenden Bild gezeigt.



4.1 Modell der hybriden Verschlüsselung (zum Zwecke der Vertraulichkeit des Dateninhaltes)

5 Hashfunktionen

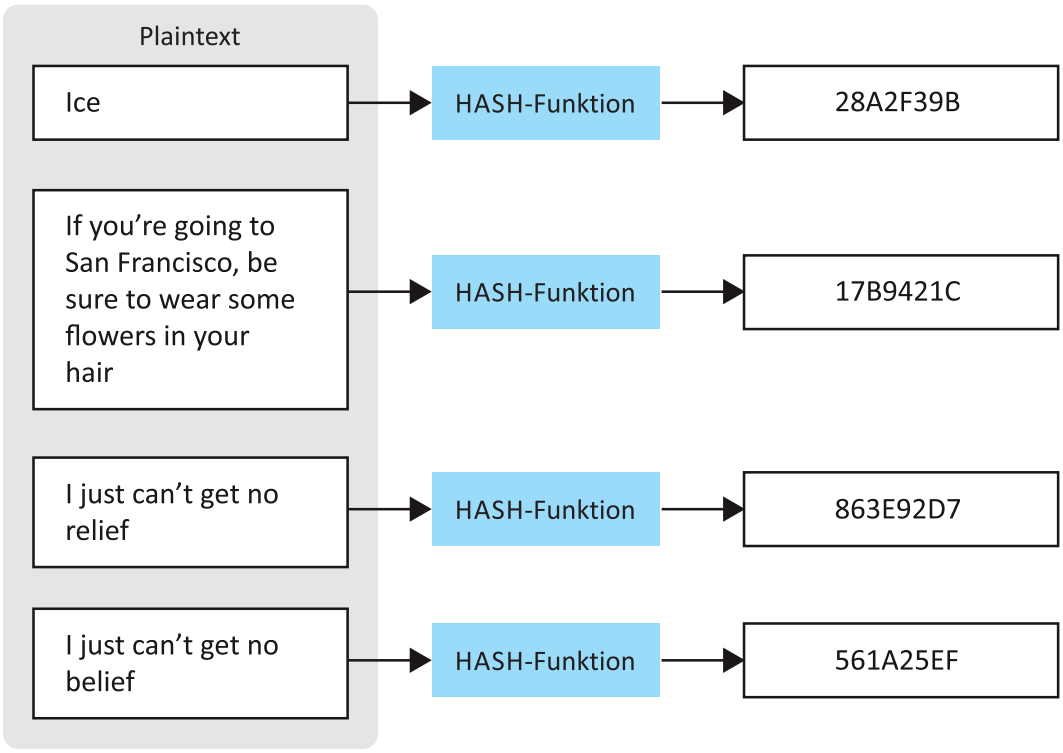
Der Begriff Hashfunktion stammt historisch aus der Informatik, wo er eine Funktion bezeichnet, die eine Folge einer beliebigen Länge in eine Folge einer fixen Länge zusammenfasst. Eine Änderung der Eingangsdaten wird (sehr wahrscheinlich) den Hashwert ändern. Hashfunktionen mit dieser Eigenschaft haben eine Reihe von allgemeinen Anwendungen in der Rechentechnik, aber in der Kryptographie werden sie wegen weiterer zusätzlicher Eigenschaften gewählt. Kryptographische Hashfunktionen können eingesetzt werden, um die Nachrichtenintegrität zu garantieren, um die Authentizität der Informationen zu schützen, um Risiken der Ablehnung (engl. *repudiation*) vorzubeugen und um Passwörter zu sichern. Im Unterschied zu den Algorithmen mit geheimen und öffentlichen Schlüsseln haben Hashfunktionen keinen Schlüssel.

An kryptographische Hashfunktionen werden die folgenden grundlegenden Anforderungen gestellt:

- beliebige Länge des Eingangs
- fixe Länge des Ausgangs
- Einfachheit der Berechnung des Hashwertes für jede Nachricht
- Unidirektionalität (rechnerische Unmöglichkeit der Ableitung der Nachricht vom gegebenen Hashwert)
- Unmöglichkeit einer Änderung der Nachricht ohne eine Änderung des Hashwertes
- Kollisionssicherheit (Unmöglichkeit des Findens von zwei unterschiedlichen Nachrichten, die den gleichen Hashwert haben)

Der Hashwert stellt eine längere Nachricht oder ein Dokument dar, von dem er berechnet wurde. Diese Kurzfassung (auf Englisch *message digest* genannt) ist ein „digitaler Fingerabdruck“ des größeren Dokumentes.

Die Hauptrolle einer kryptographischen Hashfunktion liegt bei digitalen Signaturen. Darüber hinaus kann der Hashwert veröffentlicht werden, ohne dass der Inhalt des Dokumentes verraten werden muss, von dem der Hashwert abgeleitet wurde.



5.1 Hashfunktion

6 Digitale Signatur

Digitale Signaturen stellen die wichtigste Entwicklung der Kryptographie mit öffentlichen Schlüsseln dar und bieten die Sicherheit, die sonst schwierig implementiert werden kann. Eine digitale Signatur ist eine elektronische Signatur, die zur Identitätsauthentifizierung des Senders einer Nachricht oder des Unterzeichners eines Dokumentes dient und das mit der Möglichkeit der Sicherstellung der Integrität der Nachricht. Digitale Signaturen sind leicht transportierbar und können nicht von einer unbefugten Person imitiert werden.

Digitale Signaturen basieren auf handgeschriebenen Signaturen, die für Eigentumsrechte oder Bestätigung des Nachrichteninhaltes verwendet werden.

Handgeschriebene Signaturen müssen die folgenden Eigenschaften haben:

- ***Die Signatur ist sicher*** – Die Signatur soll nicht imitierbar sein und ein eventueller Versuch der Fälschung der Signatur soll leicht erkannt werden.
- ***Die Signatur erlaubt eine Authentifizierung*** – Die Signatur identifiziert eindeutig den Inhaber, der das Dokument unbeschränkt und bewusst unterzeichnet hat.
- ***Die Signatur ist nicht übertragbar*** – Die Signatur schafft einen Teil des Dokumentes und ein unbefugtes Subjekt kann sie zu einem anderen Dokument nicht übertragen.
- ***Das unterzeichnete Dokument ist unveränderbar*** – Das Dokument kann nach dem Unterzeichnen nicht modifiziert werden.
- ***Die Signatur ist unleugbar*** – Der Inhaber der Signatur kann die Unterzeichnung des Dokumentes nicht bestreiten.

In Wirklichkeit wird keine dieser Eigenschaften bei den handgeschriebenen Signaturen konsistent erfüllt und daher können sie diskreditiert werden. Digitale Signaturen sollen alle diesen Eigenschaften auch haben. Es gibt jedoch einige Probleme bei der praktischen Realisierung der digitalen Signaturen. Digitale Dateien können leicht kopiert werden, ein Teil des Dokumentes kann in ein anderes Dokument übertragen werden und das unterzeichnete Dokument kann leicht modifiziert werden.

Eine digitale Signatur soll die folgenden Anforderungen erfüllen:

- Die Signatur muss ein Bitmuster sein, das ***von der unterzeichneten Nachricht abhängt***.
- Die Signatur muss einige ***unikale Informationen des Senders umfassen***, um Fälschung und Leugnen vorzubeugen.
- Die Realisierung und Implementierung der digitalen Signatur muss ***ziemlich einfach*** sein.

- Die ***Fälschung*** der digitalen Signatur muss ***rechnerisch unmöglich*** sein, sowohl durch Erzeugung einer neuen Nachricht zur bestehenden digitalen Signatur als auch durch Erzeugung einer betrügerischen digitalen Signatur zu einer bestehenden Nachricht.

- Es muss praktisch möglich sein, eine Kopie der digitalen Signatur zu speichern.

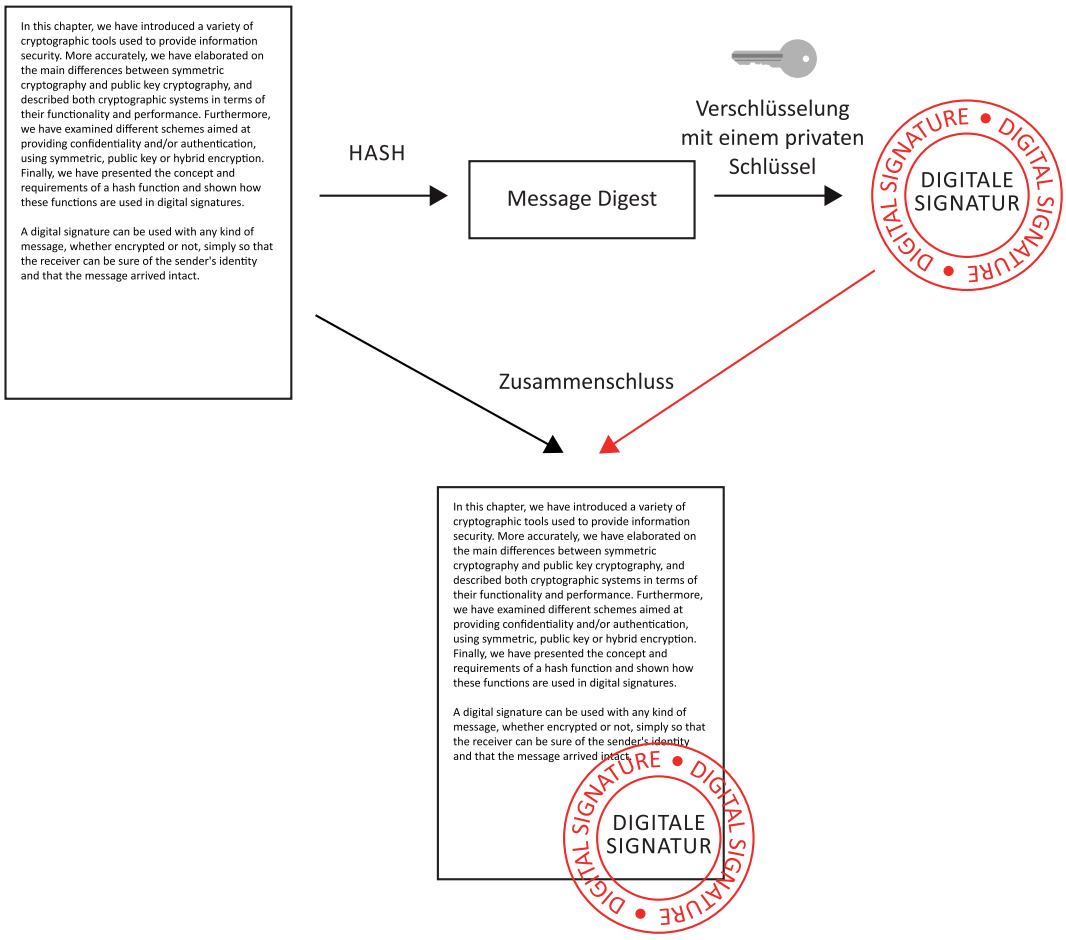
Eine digitale Signatur kann mit jedem Nachrichtentyp verwendet werden, wenn auch sie verschlüsselt ist oder nicht, einfach so, dass sich der Empfänger sicher der Identität des Senders und der unverletzten Zustellung der Nachricht sein kann.

Es gibt einige mögliche Schemen der digitalen Signaturen. Eines der meistverwendeten basiert auf Hashfunktionen. Wenn dann ein Benutzer ein Dokument digital unterzeichnen möchte, muss er die folgenden Schritte durchführen:

1. Berechnung des Hashwertes des zu unterzeichneten Dokumentes.

2. Asymmetrische Verschlüsselung des Hashwertes mit dem privaten Schlüssel des Senders, um die digitale Signatur zu erzeugen.

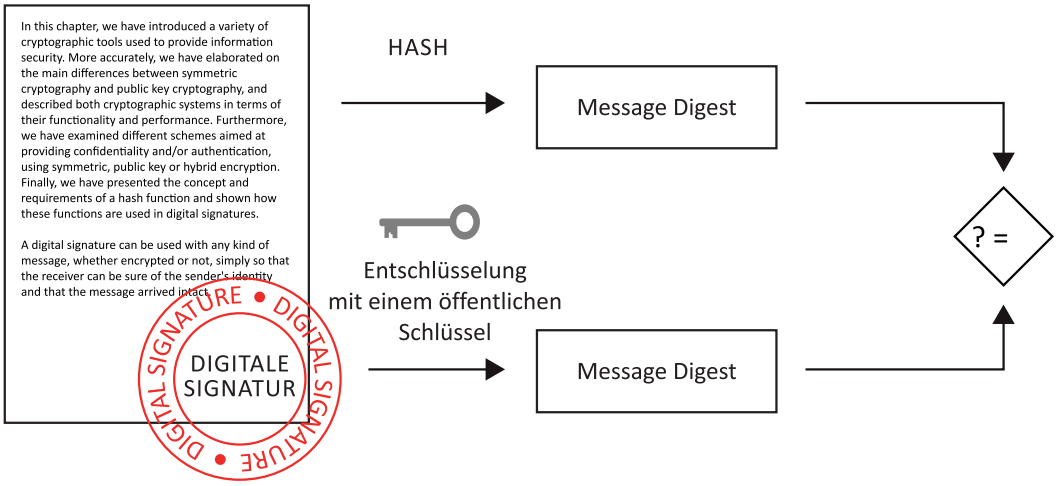
3. Hinzufügen der digitalen Signatur zum Dokument.



6.1 Digitale Signatur auf Basis der Hashfunktion

Der Empfänger kann Authentizität dieser digitalen Signatur nach den folgenden Schritten überprüfen:

1. Berechnung des Hashwertes des Dokumentes (ohne die digitale Signatur).
2. Asymmetrische Entschlüsselung der digitalen Signatur mit dem öffentlichen Schlüssel des Senders, um den Hashwert zu enthüllen.
3. Vergleichen der Ergebnisse der vorigen zwei Schritte.



6.2 Prozess der Verifizierung einer digitalen Signatur auf Basis der Hashfunktion

Falls sich die Hashwerte der ersten zwei Schritte nicht unterscheiden, weiß der Empfänger, dass die unterzeichneten Daten nicht geändert wurden.

7 Schlüsselaustausch. Digitale Zertifizierung

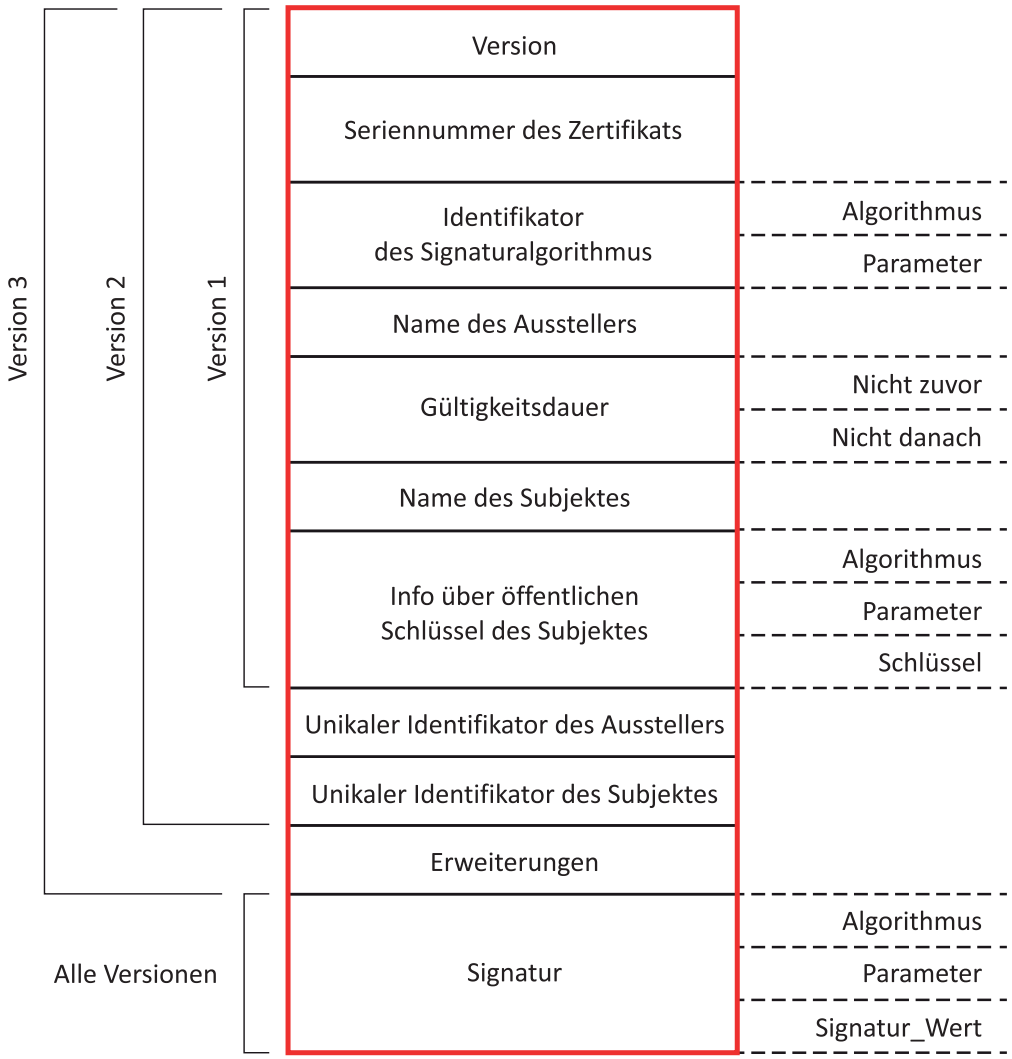
Digitale Signaturen stellen eine der Hauptanwendungen der Kryptographie mit öffentlichen Schlüsseln dar. Für Nachrichten, die durch einen ungesicherten Kanal gesendet werden, kann eine richtig implementierte digitale Signatur dem Empfänger Grund zu der Annahme geben, dass die Nachricht von dem angeführten Sender gesendet wurde. In vieler Hinsicht sind digitale Signaturen äquivalent den traditionellen handgeschriebenen Signaturen, aber richtig implementierte digitale Signaturen können schwieriger als die handgeschriebenen gefälscht werden. Um eine digitale Signatur zu verifizieren, soll der Sender den öffentlichen Schlüssel kennen. Daher ist ein Mechanismus der Schlüsselverteilung erforderlich.

Die effizienteste Lösung beruht auf den Einsatz der digitalen Zertifikate, was die Realisierung des Schlüsselaustausches erlaubt.

Ein digitales Zertifikat ist ein elektronisches Dokument, das zur Identifikation einer Person, eines Servers, einer Firma oder eines anderen Subjektes und zur Verbindung dieser Identität mit einem öffentlichen Schlüssel dient. Es umfasst eine digitale Signatur, die ***den öffentlichen Schlüssel mit der gegebenen Identität*** (Informationen wie Name der Person oder Organisation, Adresse usw.) verbindet. Mittels Zertifikaten kann man überprüfen, ob ein öffentlicher Schlüssel einem Subjekt gehört. Zertifikate helfen beim Verhindern der Verwendung gefälschter öffentlicher Schlüssel zwecks Identitätsbetrugs. Nur der öffentliche Schlüssel, der mit einem Zertifikat zertifiziert wird, wird zu dem entsprechenden privaten Schlüssel des Subjektes passen, das von dem Zertifikat identifiziert wird.

Ein digitales Zertifikat ist eine Datenstruktur, die den öffentlichen Schlüssel eines Subjektes oder Zertifikatsinhabers, Identifikationsdaten des Zertifikatsinhabers, einen Zeitstempel der Zertifikatsgültigkeit und weitere Daten von der Zertifizierungsstelle umfasst. Diese Struktur wird mit dem privaten Schlüssel der Zertifizierungsstelle unterzeichnet und jeder Benutzer kann die Authentizität des Zertifikatsinhaltes mittels des öffentlichen Schlüssels der Zertifizierungsstelle überprüfen. Zertifizierungsstellen sind Subjekte, die Zertifikate erstellen und Identitäten validieren.

Das folgende Bild zeigt die Struktur eines digitalen Zertifikats.



7.1 Struktur eines digitalen Zertifikats

8 Cyberkriminalität: Einleitung

Die Cyber- oder Computerkriminalität ist jede kriminelle Aktivität, die Rechner und Netzwerke betrifft. Sie kann von Betrügereien bis zu unerwünschten E-Mails (Spam) reichen. Sie schließt Angriffe gegen Computerdaten und -systeme, Identitätsdiebstahl, Verteilung von Darstellungen des sexuellen Missbrauchs von Kindern, Betrug bei Internetauktionen, Eindringen in online verfügbare Finanzdienstleistungen, Einführung von Viren, Botnetzen und weitere E-Mail-Angriffe wie Phishing ein.

Um kein Opfer der Cyberkriminalität zu werden und empfindliche Informationen zu schützen, soll man ein geeintes Soft- und Hardwaresystem zur Authentifizierung aller Informationen verwenden, die über das Internet gesendet oder empfangen werden.

Die Cyberkriminalität wird wie folgt definiert: „Straftaten, die gegen Individuen oder Gruppen von Individuen mit einem strafbaren Motiv mit dem Zweck der absichtlichen Beschädigung der Reputation des Opfers oder der direkten oder indirekten Veranlassung eines physischen oder psychischen Schadens des Opfers mithilfe moderner Telekommunikationsnetzwerke wie Internet und Handys (SMS/MMS) begangen werden“. Solche Straftaten können die Sicherheit und finanzielle Gesundheit eines Staats bedrohen. Diese Straftaten finden große Beachtung in den Medien, insbesondere Knacken, Urheberrechtsverletzung, Kinderpornographie und -Grooming. Berühmt sind auch Probleme des Datenschutzes, bei dem vertrauliche Informationen gesetzlich oder sonst verloren oder abgefangen werden.

Es ist wichtig, darauf hinzuweisen, dass es unmöglich ist, jeden Cyber-Angriff vor seiner Auswirkung auf gezielte Subjekte zu erkennen. Daher ist es entscheidend, sich auf die Cyber-Sicherheit zu konzentrieren und Aspekte einer rechtzeitigen Erkennung und Wiederherstellung zu betonen.

Eine wirksame Reaktion auf einen Vorfall umfasst die folgenden Schritte:

- Identifikation von Gefahren, die die Infrastruktur traf
- Eingrenzung der Gefahr, so dass sie sich nicht weiter im Rahmen der betroffenen Infrastruktur ausbreitet
- Forensische Untersuchung zur Identifikation der beeinträchtigten Systeme und des Eindringens ins Computersystem
- Sanierung/Erholung durch Wiederherstellen der IT-Infrastruktur in den aktiven online Modus nach dem Vollenden der Untersuchungen
- Bericht an das obere Management über die Gefahr und Teilen der Erkenntnis zum Vorfall über geeignete Plattformen, die ein schnelles Teilen der Daten mit Strafverfolgung und anderen Firmen erlauben

Leider wird der oben beschriebene Prozess nur selten verfolgt. Bisher werden Eingrenzung und Sanierung vor allem manuell durchgeführt, was den Prozess ineffizient und unwirksam macht.

9 Angriffstechniken

Sicherheitsangriffe können als verschiedene Arten systematischer Aktivitäten charakterisiert werden, die auf Abschwächen oder Beschädigung der Sicherheit zielen. Aus dieser Perspektive kann ein Angriff als eine systematische Bedrohung definiert werden, die von einem Subjekt künstlich, absichtlich und intelligent generiert wird. Computernetzwerke können vielen Bedrohungen durch verschiedene Angriffswege ausgesetzt werden, einschließlich:

- Social-Engineering-Angriffe, bei denen jemand versucht, einen Zugriff durch soziale Mittel zu erwerben (sich für einen legitimen Systembenutzer oder -administrator ausgibt, Mitarbeiter durch einen Trick dazu bringt, Geheimnisse zu offenbaren usw.)

- Wardialing, bei dem jemand eine Computersoftware und ein Modem zur Suche von Arbeitsplatzrechnern, die ein Modem verwenden und auf Anfragen antworten und damit einen potenziellen Weg ins Unternehmensnetz zeigen.

- **DoS**-Angriffe (*Dienstverweigerung*, engl. *Denial of Service*), einschließlich aller Typen der Angriffe, die einen Computer oder ein Netzwerk überlasten, so dass ihre legitimen Benutzer sie nicht nutzen können.

- Angriffe durch die Nutzung von Protokollen, die bekannte (oder auch unbekannte) Schwachstellen der Netzwerkdienste ausnutzen.

- Angriffe auf Hosts, welche die Verwundbarkeiten in bestimmten Computer-Betriebssystemen, in der Einstellung oder Verwaltung der Systeme ausnutzen.

- Passwort-Rate-Attacken (engl. *Password Guessing*). Passwörter sind Folgen von Symbolen, üblicherweise mit einem Benutzernamen verbunden, die einen Mechanismus der Identifikation und Authentifizierung der Benutzer erlauben. Fast an allen Computern wählen die Benutzer ihre Passwörter. So werden mit der Sicherheit die Endbenutzer belastet, welche die gründlichen Sicherheitspraktiken entweder nicht kennen oder nicht wichtig nehmen. Allgemein kann man sagen, dass Passwörter, an die man sich einfach erinnert, auch einfach zu erraten sind. Die Angreifer haben einige Möglichkeiten zum Erraten der Passwörter.

- Abhören aller Art, einschließlich Stehlen von E-Mail-Nachrichten, Dateien, Passwörtern und weiteren Informationen über eine Netzwerkverbindung.

Die Sicherheitsangriffe können in die folgenden zwei Hauptkategorien aufgeteilt werden:

- passive Angriffe

- aktive Angriffe

9.1 Passive Angriffe

Passive Angriffe versuchen, Informationen vom System zu ermitteln oder auszunutzen, beeinflussen aber die Systemressourcen nicht. Bei einem passiven Angriff wird vom Angreifer der Kommunikationskanal nur überwacht. Ein passiver Angreifer bedroht nur die Vertraulichkeit der Daten.

Passive Angriffe sind beispielsweise Abhören oder Überwachen der Übertragung. Das Ziel des Angreifers besteht in der Gewinnung der übertragenen Information.

Es gibt zwei Typen passiver Angriffe, die mit dem Nachrichteninhalt und der Verkehrsanalyse zusammenhängen:

- Abhören. Allgemein kann man sagen, dass die Mehrheit der Netzwerkkommunikation in einem ungesicherten „Klartextformat“ erfolgt, was es dem Angreifer ermöglicht, der den Zugriff auf Datenpfade im Netzwerk hat, zu lauschen oder die ausgetauschten Daten zu interpretieren. Die Überwachung des Netzwerkes von Lauschern ist grundsätzlich das größte Sicherheitsproblem, das Administratororen in Firmen begegnet. Ohne eine starke Verschlüsselung können die Daten von anderen leicht gelesen werden.

- Verkehrsanalyse. Es handelt sich um einen Prozess des Abfangens und der Untersuchung von Nachrichten, um Informationen von Schemen in der Kommunikation abzuleiten. Dies kann auch dann realisiert werden, wenn die Nachrichten verschlüsselt sind und nicht entschlüsselt werden können. Je höher die Anzahl der verfolgten oder sogar abgefangenen und gespeicherten Nachrichten ist, desto mehr Information kann man ableiten.

9.2 Aktive Angriffe

Aktive Angriffe versuchen, die Systemressourcen zu modifizieren oder ihren Betrieb zu beeinflussen. Dabei versuchen die Angreifer, die übertragenen Daten zu löschen, hinzuzufügen oder sonst zu ändern. Ein aktiver Angreifer bedroht die Datenintegrität, -authentizität und -vertraulichkeit.

Aktive Angriffe umfassen die Modifizierung des Datenstroms oder Erzeugung eines falschen Datenstroms. Sie können in sechs Kategorien aufgeteilt werden:

- Masquerading. Bei diesem Angriff gibt sich den Angreifer für einen berechtigten Benutzer eines Systems aus, um Zugriff auf das System oder höhere Rechte zu erwerben.

- Replay. Bei diesem Angriff werden gültige Datenübertragungen boshaft oder betrügerisch wiederholt oder verzögert. Dies kann entweder ein Absender oder ein Angreifer realisieren, der die Daten abfängt und wiederholt überträgt (vielleicht als ein Teil des Masqueradings).

- Modifizierung von Nachrichten. Der Angreifer beseitigt eine Nachricht, modifiziert sie und gibt sie zurück.

- Man-in-the-Middle. Bei diesen Angriffen fängt ein Eindringling eine Kommunikation zwischen zwei Parteien ab, üblicherweise einem Endbenutzer und einer Webseite, um einen Identitätsdiebstahl oder anderen Betrug zu begehen.

- **DoS** (*Dienstverweigerung*, engl. *Denial of Service*), **DDoS** (*verteilte Dienstverweigerung*, engl. *Distributed Denial of Service)*. Ein DoS-Angriff ist ein Vorfall, bei dem einem Benutzer oder einer Organisation Dienstleistungen einer Ressource entzogen wurde, die sie normalerweise nutzen könnten. Bei einem DDoS-Angriff zielt eine hohe Anzahl von beeinträchtigten Systemen (manchmal als Botnetz bezeichnet) auf ein einziges Objekt.

- *Advanced Persistent Threat* (**APT**). Es handelt sich um einen Netzwerkangriff, bei dem eine unbefugte Person Zugriff aufs Netzwerk erwirbt und dort unentdeckt für eine lange Zeitdauer bleibt. Das Ziel eines APT-Angriffs ist eher das Stehlen von Daten als Beeinträchtigen des Netzwerkes oder der Organisation. Die Opfer sind üblicherweise Organisationen in Bereichen mit hochwertigen Informationen, wie die Landesverteidigung, Betriebe der Produktion und Finanzbranche.

10 Tipps zur Vorbeugung

Die Cyberkriminalität kann direkt vorgebeugt werden - mit ein wenig technischer Unterstützung und Menschenverstand können viele Angriffe vermieden werden. Online Verbrecher möchten ihr Geld möglichst schnell und leicht verdienen. Je schwieriger man diese Aufgabe macht, desto wahrscheinlicher ist es, dass sie ein leichteres Ziel finden. Vielleicht liegt die beste Verteidigung beim Endbenutzer. Je weniger Risiken er eingeht, desto niedriger ist die Wahrscheinlichkeit, dass er zu einem Opfer des Computerangriffs wird. Die folgenden Tipps bieten grundlegende Informationen über die Prävention gegen online Betrügereien.

- Aktualisieren Sie Ihr Computersystem mit den neuesten Patches und Updates. Wenn eine Verwundbarkeit einer Software entdeckt wird, werden üblicherweise Patches herausgegeben. Sie sollen diese Patches und weitere Softwareverbesserungen sofort installieren, um Angreifer von einem Angriff auf Ihren Computer abzuhalten. Die meisten Produktdokumentationen bieten ein Verfahren, wie man Updates und Patches erwerben kann. Einige Anwendungen kontrollieren automatisch, ob ein Update zur Verfügung steht; andernfalls muss man selbst periodisch Updates downloaden. Regelmäßiges Updaten Ihres Computers hält die Angreifer davon ab, die Softwarefehler (Verwundbarkeiten) auszunutzen, über die sie in Ihr System einbrechen könnten. Ein aktuelles Computersystem schützt nicht gegen alle Angriffe, aber erschwert es den Angreifern, den Zugriff aufs System zu erwerben, blockiert viele grundlegende und automatisierte Angriffe und kann einen weniger entschlossenen Angreifer motivieren, einen verletzbaren Computer anderswo zu suchen.

- Sorgen Sie dafür, dass Ihr Computer richtig und sicher konfiguriert ist. Das Installieren eines Systems sofort nach seinem Kauf und sein Belassen mit der Werkseinstellung ist ein häufiger Fehler, den die Anwender bei der Einrichtung eines Netzwerkes machen. Wenn ein Computer installiert wird, sollte man nicht nur prüfen, ob das ganze System richtig arbeitet, sondern auch ob es sicher arbeitet. Die Werkseinstellung verwendet häufig standardmäßige Benutzerkontos und -passwörter, welche die Hacker der ganzen Welt schon kennen. Die Konfiguration der internetbasierten Anwendungen, wie Webbrowser und E-Mail-Software, ist dabei eine der wichtigsten Aufgaben.

- Wählen Sie starke Passwörter und bewahren Sie sie gut auf. Passwörter sind häufig der einzige Schutz der Systeme. Eine Benutzer-ID ist nur ein Name und wird nicht verifiziert, aber das mit diesem Namen verbundene Passwort dient als ein Identifikator. Firewalls und *Angrifferkennungssysteme* (*IDS*, engl. *Intrusion Detection System*) helfen gar nicht, wenn Passwörter kompromittiert wurden. Ein starkes Passwort kann in keinem Wörterbuch gefunden und nicht leicht erraten werden.

- Schützen Sie Ihren Computer mit einer Sicherheitssoftware. Für eine grundlegende online Sicherheit sind einige Typen der Sicherheitssoftware, einschließlich Firewall und Antivirensoftware, erforderlich. Eine Firewall ist ein Soft- oder Hardwareprodukt, das die Informationen, die ins Netzwerk eingehen oder davon empfangen werden, filtert. Damit wird sichergestellt, dass

es zu keinen unbefugten Zugriff auf den Computer kommt. Die Firewall stellt so die erste Verteidigungslinie dar. Antivirensoftware ist ein Computerprogramm, das Dateien überprüft, um Computerviren und weitere Schadprogramme zu identifizieren und zu beseitigen. Ein Virus ist dabei ein selbstreplizierendes Programm, das sich von einem Computer zu einem anderen ausbreiten kann und Aktionen ausführt, die vom Benutzer nicht beabsichtigt wurden und/oder denen er sich nicht bewusst war. Schadprogramme (engl. *malware*) ist ein weitgefasster Begriff und umfasst beispielsweise Viren, Trojaner, Keylogger, Würmer, Adware und Spyware.

- Schützen Sie Ihre persönlichen Angaben. Identitätsdiebstahl schafft ein großes Problem für Leute, die das Internet für bargeldlose Transaktionen und Bankdienstleistungen verwenden. In diesem Bereich der Cyberkriminalität greift ein Verbrecher auf die Daten über Bankkonten, Kredit- und Debitkarten und weitere empfindliche Informationen einer Person zu, um Geld abzuziehen oder um Dinge im Namen des Opfers online zu kaufen. Dies kann zu erheblichen finanziellen Verlusten und sogar zur Beeinträchtigung der Kreditwürdigkeit des Opfers führen. Daher sollte man persönliche Angaben, wie Name, Privatanschrift, Handynummer und E-Mail-Adresse online sorgfältig teilen. Um aber Online-Dienstleistungen nutzen zu können, muss man zwangsläufig persönliche Informationen zwecks Rechnungsschreibung und Lieferung der gekauften Produkte angeben.