

# **Security**

Sommersemester 2022  
(LV 4120, 7240)

dienstags, 08:15 bis 09:45

Prof. Dr. Bernhard Geib

### Worum geht es in der Einführung?

- Womit beschäftigt sich die Informationssicherheit?
    - ✓ Ziele und Merkmale
    - ✓ Themenbereiche und Abgrenzung
  - Vorlesungsübersicht
    - ✓ Gliederung und Inhalte
    - ✓ Anwendungsbeispiele
  - Organisation der Lehrveranstaltung
    - ✓ Vorlesung, Übungen und Klausur
    - ✓ Ablauf und Vereinbarung zur Leistungsbewertung
    - ✓ Hilfsmittel und Unterrichtsmaterial
    - ✓ Quellen- und Literaturangabe
-

### Die vier wesentlichen Sicherheitsbereiche:

Funktionale Sicherheit (Safety)		
Computersicherheit IT-Sicherheit	Cyber-Sicherheit	Informationssicherheit (Security)

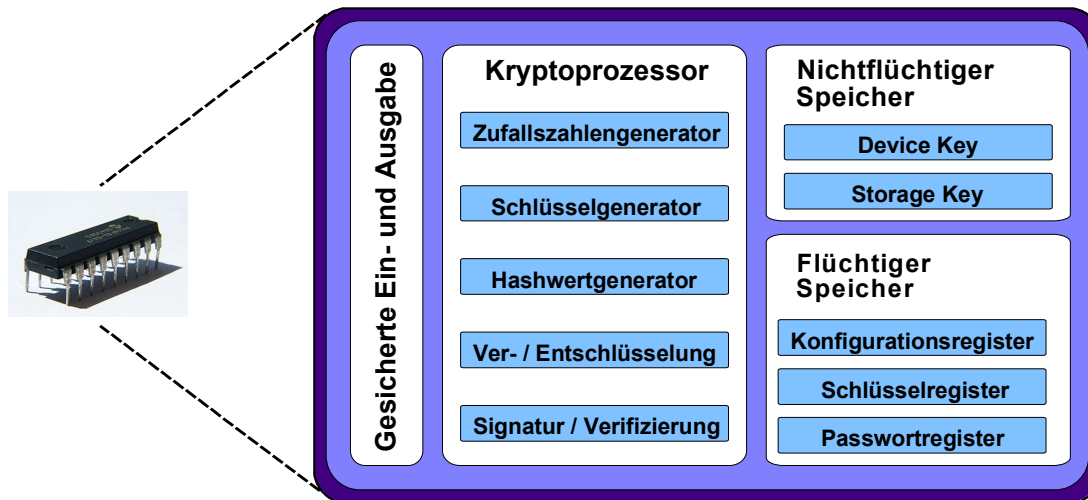
- Sicherheitsthemen und -fragestellungen sind seit Jahrzehnten allgegenwärtig.
- Täglich erreichen uns Meldungen über Identitätsdiebstahl und Datenklau durch Cyber-Kriminelle und andere Angreifer.
  - ✓ Methoden der Informationsgeheimhaltung
  - ✓ Datenunversehrtheit
  - ✓ Systemverfügbarkeit

## Kap. 1: Einführung und Motivation

### Einleitung:

- Worum geht es in dieser Lehrveranstaltung?
  - Was verstehen wir unter Security?
  - Wozu brauchen wir Informationssicherheit?
  - Welche Rolle spielt die Kryptologie?
  - Angestrebte Lernergebnisse (Zielsetzung)
  - Inhalte der Vorlesung und Gliederung
  - Organisation, Konzeption und Leistungsnachweis
  - Literatur und Hilfsmittel
-

## Worum geht es in dieser Lehrveranstaltung?



Trusted Platform Module (TPM 2.0)

Infineon SLB9665TT20

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

## 1. Kennenlernen von Krypto-HW

Sichere Infrastruktur für Trusted Computing

- Zertifizierungs- und Signierungsinfrastrukturen
- Schlüsselverwaltung für kritische Infrastrukturen
- Offene, vertrauenswürdige Datenverarbeitung

## Worum geht es in dieser Lehrveranstaltung?



ISDN - Bus- / Port- Schlüsselgerät ElcroDat 6-2

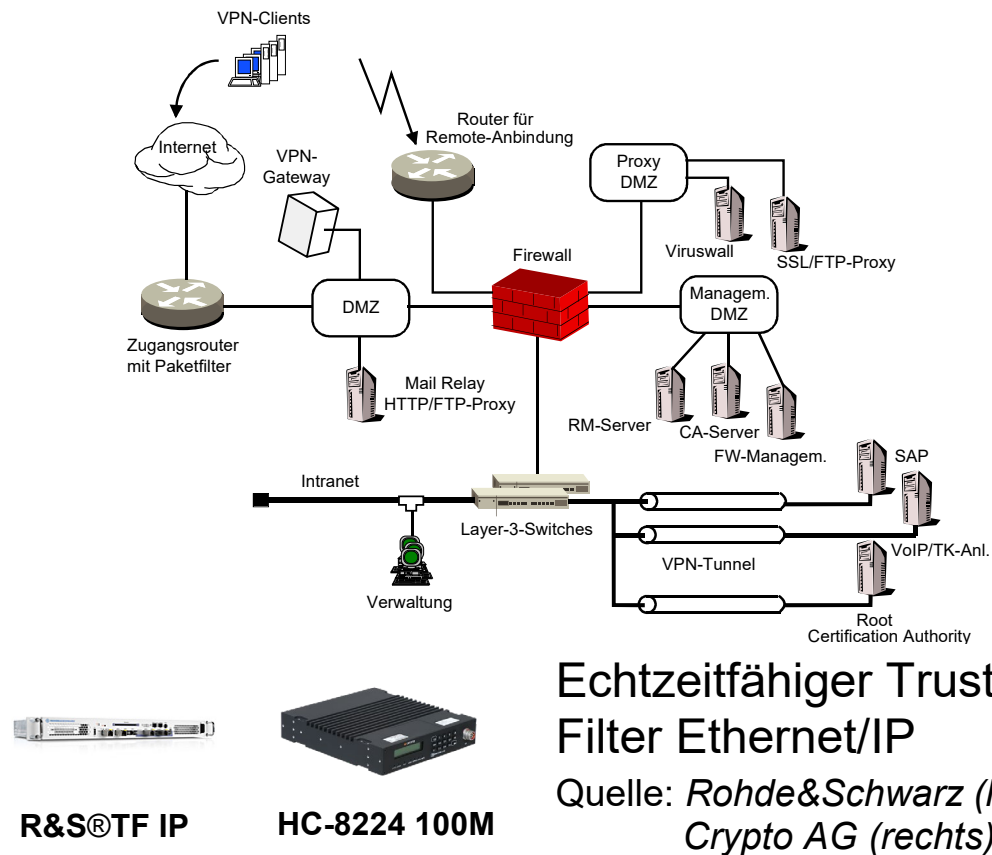
Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

## 2. Anwendung von Krypto-Devices

Sichere Kommunikation  
(Verwaltung, Militär,  
Sicherheitsbehörden)

- Chiffrier- und Dechiffrierung
- Zufällige Schlüsselgenerierung
- Sprache, Daten, Video

## Worum geht es in dieser Lehrveranstaltung?



### 3. Absicherung einer IT&TK-Infrastruktur

Sicherer Übergang zwischen Sicherheitsdomänen

- Separierung von Ethernet- und IP-Netzwerken
- Zustandslose Protokollfilterung
- Netzwerkverschlüsselungsplattform

## Einteilung und Abgrenzung?

### **Funktionssicherheit** (engl. *safety*):

zielt auf Übereinstimmung der Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität ab (Gefahrenabwendung, Ausfallsicherheit, Schutz von Leib und Leben).

### **IT-Sicherheit** (engl. *IT-security*):

umfasst alle Vorkehrungen zum Schutz von elektronisch gespeicherten Informationen sowie informationstechnischen Systemen (SW & HW).

### **Datenschutz** (engl. *privacy*):

regelt die Verwendung und Weitergabe personenbezogener Daten (informationelles Selbstbestimmungsrecht gemäß BDSG & DSGVO).

---



## Was verstehen wir unter Informationssicherheit?

- ist gemeinhin ein Oberbegriff und beinhaltet sowohl die Cyber- und Internet-Sicherheit als auch die IT-Sicherheit.
- erweitert insbesondere die IT-Sicherheit um die Sicherheit von nicht technisch gespeicherten und nicht elektronisch verarbeiteten Daten.
- sicherstellen, dass es zu keiner unerlaubten Informationsveränderung, zu keinem unerlaubten Informationsgewinnung oder zu keiner unerlaubten Informationsvorenthaltung kommt.
- verwendet den vom BSI entwickelten IT-Grundschutz als eine bewährte Methodik für den systematischen Aufbau eines dem individuellen Schutzbedarf angemessenen und wirksam angepassten IT-Systems.

### Was verstehen wir unter Kryptologie?

#### **Kryptologie:**

Wissenschaft der Verfahren zur Geheimhaltung von Nachrichten, aber auch zu deren Brechung. Kryptologie vereinigt Kryptographie und Kryptanalyse.

#### **Kryptographie:**

Geheimschriftkunde – offen versendete Nachrichten sollen durch Verschlüsselung bzw. Chiffrierung für Unbefugte nicht lesbar sein.

#### **Kryptanalyse:**

Meist mathematische und statistische Methoden zur Entzifferung von Geheimtexten, d.h. Informationen unbefugt erlangen.

---

---

### Wozu brauchen wir Kryptologie?

- Kryptologie ist als mathematische Disziplin wissenschaftlich fundiert und anerkannt.
- Mathematik liefert – jedenfalls im Prinzip – Rechtfertigung für die „Stärke“ einer Sicherheitsmaßnahme.
- Im Idealfall lässt sich beweisen, dass ein kryptographischer Algorithmus ein gewisses Sicherheitsniveau hat (oder halt nicht).

Damit kann der **Nachweis** erbracht werden, dass für eine bestimmte Anwendung der beanspruchte **Sicherheitswert** tatsächlich erreicht wird.

## **Angestrebte Lernergebnisse (Zielsetzung):**

Nach Absolvieren dieser Kurseinheit sollten Sie

- Verfahren zur Authentifizierung von Teilnehmern verstanden haben und auswählen können,
- Methoden der Informationsverschlüsselung einordnen, in ihrer Wirkung analysieren und in der Praxis anwenden können,
- Vorkehrungen zur Datenintegrität und Geheimhaltung sensibler Dateninhalte beurteilen und sicherstellen können,
- Konzept für Einweg- und Hashfunktionen verstanden haben sowie Probleme beim Schlüsselaustausch behandeln können.

## Typische Fragestellungen:

Aus Sicht eines Anwenders ergeben sich die Fragen

- Warum ist Sicherheit nötig (IT-Sicherheitsgesetz, kritische Infrastrukturen) und wie ist sie erreichbar?
  - Mit welchen Kosten ist Sicherheit verbunden?
  - Was ist für ein erfolgreiches E-Business (IT-gestützter Arbeitsablauf) nötig?
  - Wie ist die Risikolage (Gefahrenlage, Angreifer und Täter, Konsequenzen)?
-

## Inhalte der Vorlesung und Gliederung:

1. Einführung in die Informationssicherheit
  2. Algebraische Strukturen und elementare Zahlentheorie
  3. Monoalphabetische Chiffren und deren Analyse
  4. Symmetrische Verfahren und moderne Blockchiffren
  5. Einwegfunktionen
  6. Asymmetrische Kryptosysteme
  7. Schlüsselmittelmanagement und Zufallszahlen
  8. Kryptographische Protokolle und Anwendungen
-

## Organisation und Leistungsnachweis:

- Lehrform: Vorlesung und Praktikum / Übung
- ECTS / SWS: **5 cp / 4**
  - 2 SWS Vorlesung
  - 2 SWS Praktikum / Übung
- Gesamtaufwand: **150 h** (etwa 8 h pro Woche)
  - Anwesenheit Vorlesung und Praktikum 60 h
  - Vorbereitung und Nachbereitung Vorlesung 30 h
  - Bearbeitung der Praktikumsaufgaben 60 h
- Leistungsnachweis: **Klausur** (90-minütig mit Formelsammlung)

## Konzeption der Lehrveranstaltungen:

### Vorlesungen

- Vorlesungen werden im Präsenz oder in Corona-Zeiten online jeweils für alle Studierenden des Semesters gemeinsam abgehalten.
- Die Vorlesung findet jeweils dienstags von 08:15 bis 09:45 Uhr statt.
- Anwesenheitspflicht besteht nicht.
- Die Lehrveranstaltung wird am Semesterende mit einer schriftlichen Prüfung (Klausur) abgeschlossen.
- Formale Voraussetzung für das Antreten zur Vorlesungsprüfung ist die rechtzeitig erfolgte Prüfungsanmeldung.



## Übungen und integriertes Praktikum

- Übungen dienen der praktischen Vertiefung und Ergänzung des Vorlesungsstoffs bzw. der Verständnisbildung.
- Sie werden in Teilgruppen (25 bis 30 Teilnehmer) ca. und wöchentlich in Einheiten zu jeweils 90 Minuten durchgeführt.
- Die Teilnahme am Übungsbetrieb bereitet die Studierenden gezielt auf die theoretischen und praktischen Anforderungen der Klausur vor (typische Sicherheitsthemen / sicherheitstechnische Fragestellungen).
- Die Gruppeneinteilung erfolgt jeweils zu Beginn eines Semesters im Rahmen der Belegung.
- Eine Beurteilung der Übungsteilnahme erfolgt nicht.

## Konzeption der Lehrveranstaltungen:

### Übungen und integriertes Praktikum (Fortsetzung)

- Die Teilnahme an den Übungen ist in Corona-Zeiten nicht verpflichtend, wird allerdings empfohlen.
- Integriert in theoretische Übungen sind Praktikumsaufgaben betreffend die Anwendung kryptographischer Algorithmen wie Verschlüsselung, Signaturen, Authentifizierung und Schlüsselmittelherstellung).
- Als Programmiersprache kommt C zur Anwendung.

### Sprechstunde:

**mittwochs zwischen 10:30 und 11:30 Uhr im Raum C 210  
oder nach Vereinbarung**

---

## Literatur und Hilfsmittel:

- Albrecht Beuelpacher: Kryptographie, Vieweg
- Wolfgang Ertel, Angewandte Kryptographie, Fachbuchverlag
- Johannes Buchmann: Einführung in die Kryptographie, Springer
- Claudia Eckert: IT-Sicherheit, Oldenbourg Verlag
- Ditmar Wütjen: Kryptographie, Spektrum Akademischer Verlag
- Bruce Schneier: Applied Cryptography, John Wiley & Sons

## Papers und Dokumentation zur Lehrveranstaltung:

[www.cs.hs-rm.de/~rnlab/LVaktuell/Security/](http://www.cs.hs-rm.de/~rnlab/LVaktuell/Security/)

---

## Zur Verfügung gestelltes Material:

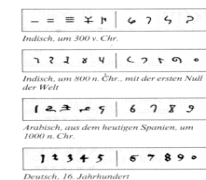
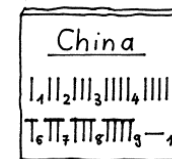
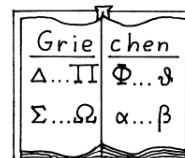
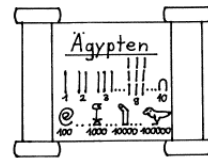
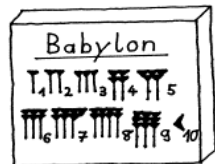
- Vorlesungsfolien (Kapitel 1 bis 8) als PFD
- Grundlagen zur Zahlentheorie (Skript, 52 S.) als PDF
- Aufgabensammlung (passend zum Skript Zahlentheorie)
- Übungsunterlagen (Aufgabenblätter 1 bis 12) als PDF
- Übersicht der verwendeten kryptographischen Funktionen (Kryptolibrary mit 76 Moduln)
- Formelsammlung (abgestimmt auf Vorlesungsschwerpunkte)

Alles Weitere ist zu finden unter:

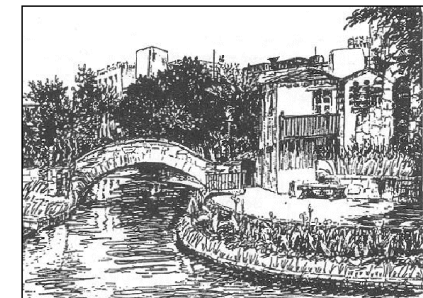
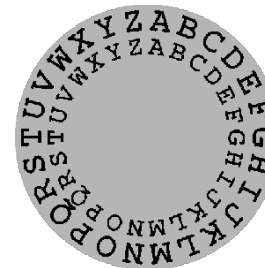
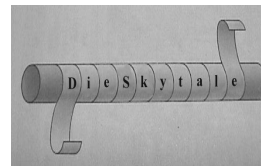
**[www.cs.hs-rm.de/~rnlab/LVaktuell/ Security/Material/](http://www.cs.hs-rm.de/~rnlab/LVaktuell/Security/Material/)**

---

## Zur Verfügung gestelltes Material:



## Begriffe und Grundlagen der Zahlentheorie



## Security

Sommersemester 2022  
(LV 4120 und 7240)

Formelsammlung

## Aufgaben- sammlung mit Beispiel- Lösungen

## Security

Sommersemester 2022  
(LV 4120 und 7240)

Aufgabenblätter

## **Kap. 1: Einführung in die Informationssicherheit**

### **Teil 1: Begrifflichkeiten**

- IT-Systeme
- Sicherheitsbegriffe
- Aktuelle Sicherheitslage
- Effiziente Angriffstechniken

### Was ist ein IT-System?

Unter dem Begriff Informationstechnisches System (IT-System) versteht man jegliche Art elektronischer datenverarbeitender Systeme.

Kurz: Ein IT-System ist ein dynamisches technisches System mit der Fähigkeit zur Speicherung, Übertragung und Verarbeitung von Daten.

- Computer, Großrechner, Serversysteme, Datenbanksysteme
  - Prozessrechner, digitale Messsysteme, Microcontroller-Systeme
  - Informationssysteme, Kommunikationssysteme, Verteilte Systeme
  - Betriebssysteme, eingebettete Systeme
  - Mobiltelefone, Handhelds, digitale Anrufbeantworter, u.v.a.m.
-

## **Sicherheitsbegriffe:**

### **Schwachstelle oder Sicherheitslücke:**

Fehler in einem IT-System, durch die ein Angreifer in ein Computersystem eindringen oder im IT-System Schaden verursachen kann.

### **Bedrohung:**

Eine Bedrohung ist eine potentielle Gefahr mit zeitlichem, räumlichem oder personellem Bezug zu einem Schutzziel bzw. Schutzobjekt.

### **Gefährdung:**

Trifft eine Bedrohung auf eine Schwachstelle (z. B. technische oder organisatorische Mängel), so entsteht eine Gefährdung.

---



### **Sicherheitsbegriffe:**

#### **Risiko:**

Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz (Schadenshöhe) bezogen auf ein konkretes Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit).

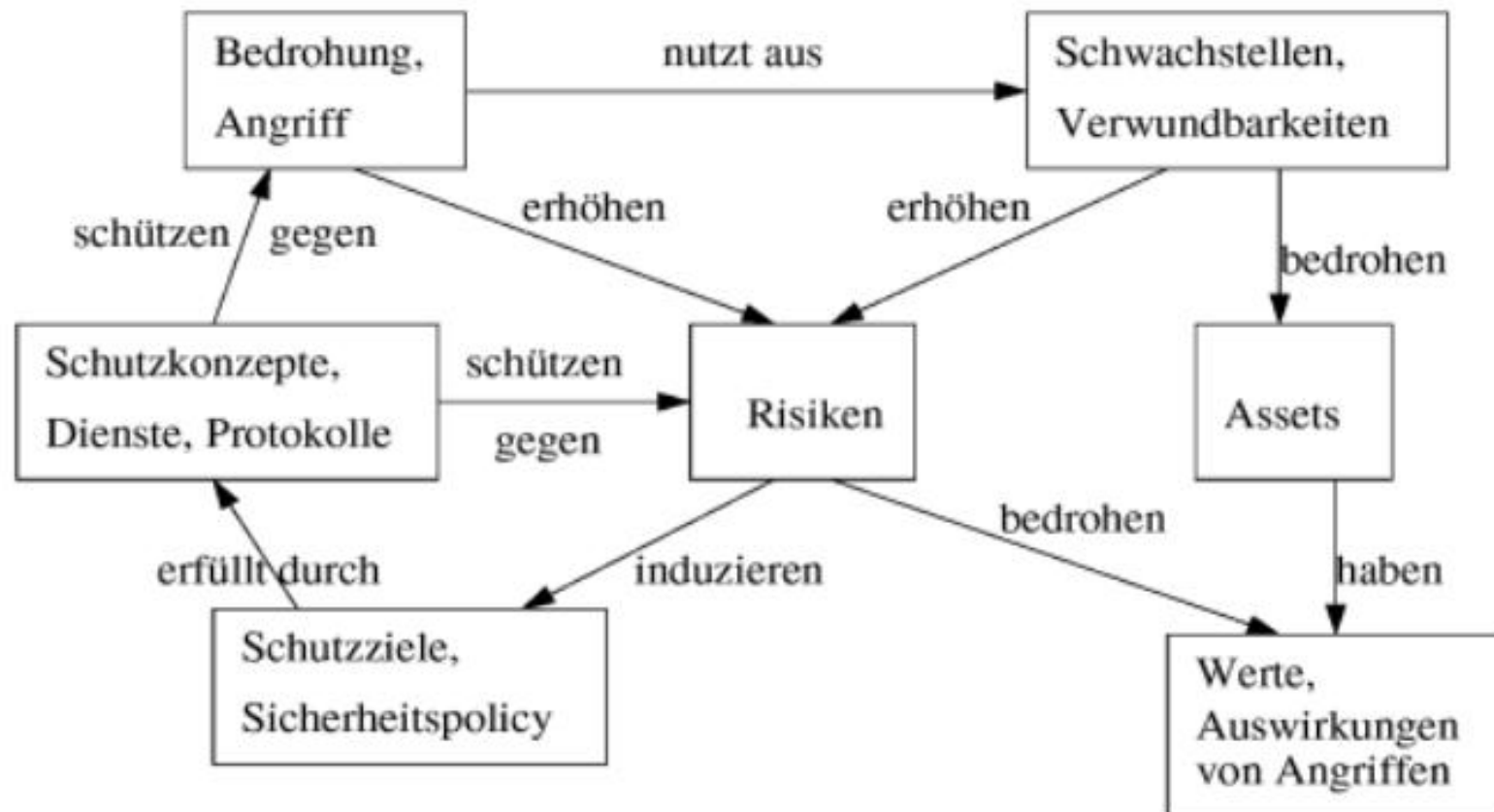
#### **Eintrittswahrscheinlichkeit:**

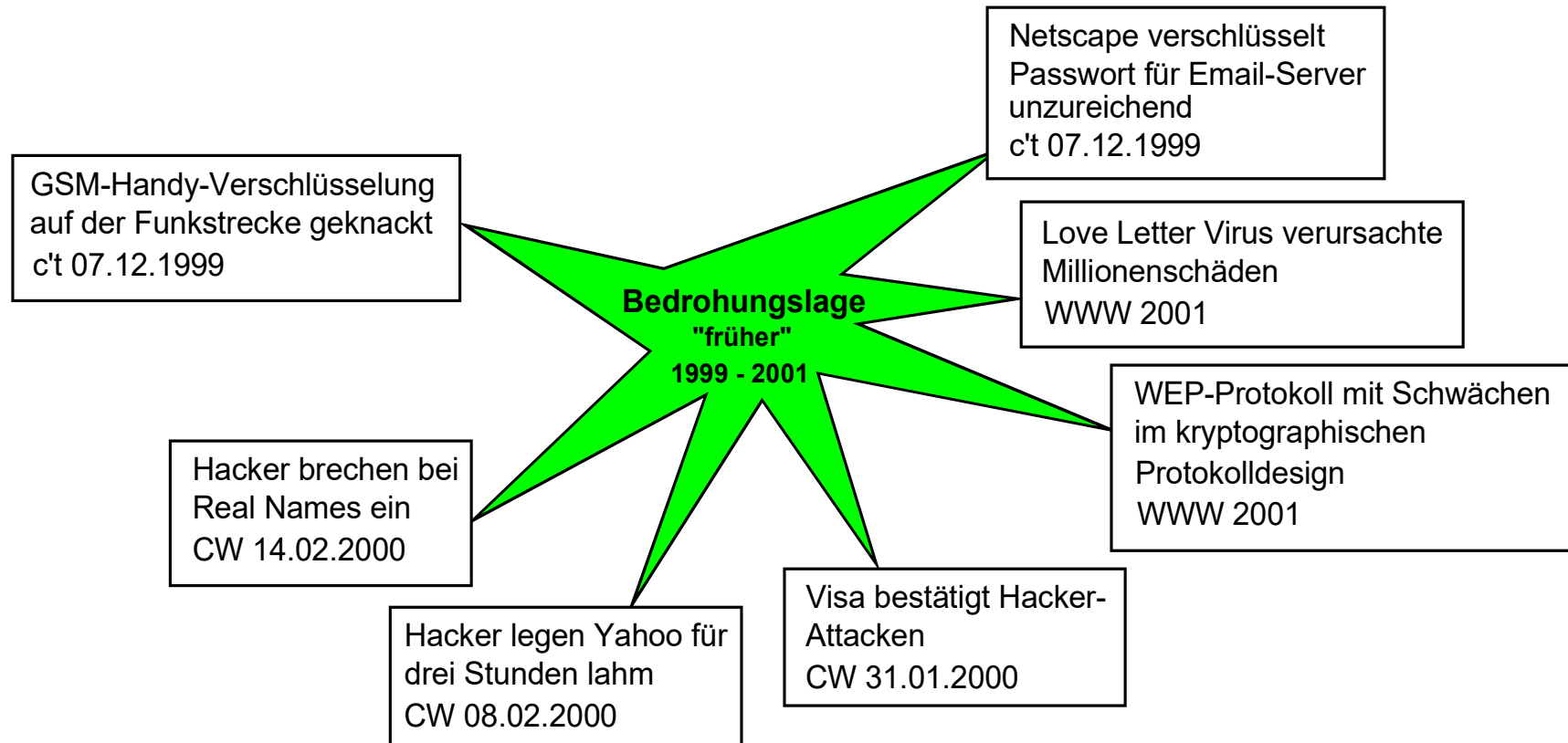
Ist die Wahrscheinlichkeit dafür, dass ein Schutzziel gebrochen wird.

#### **Schadenshöhe:**

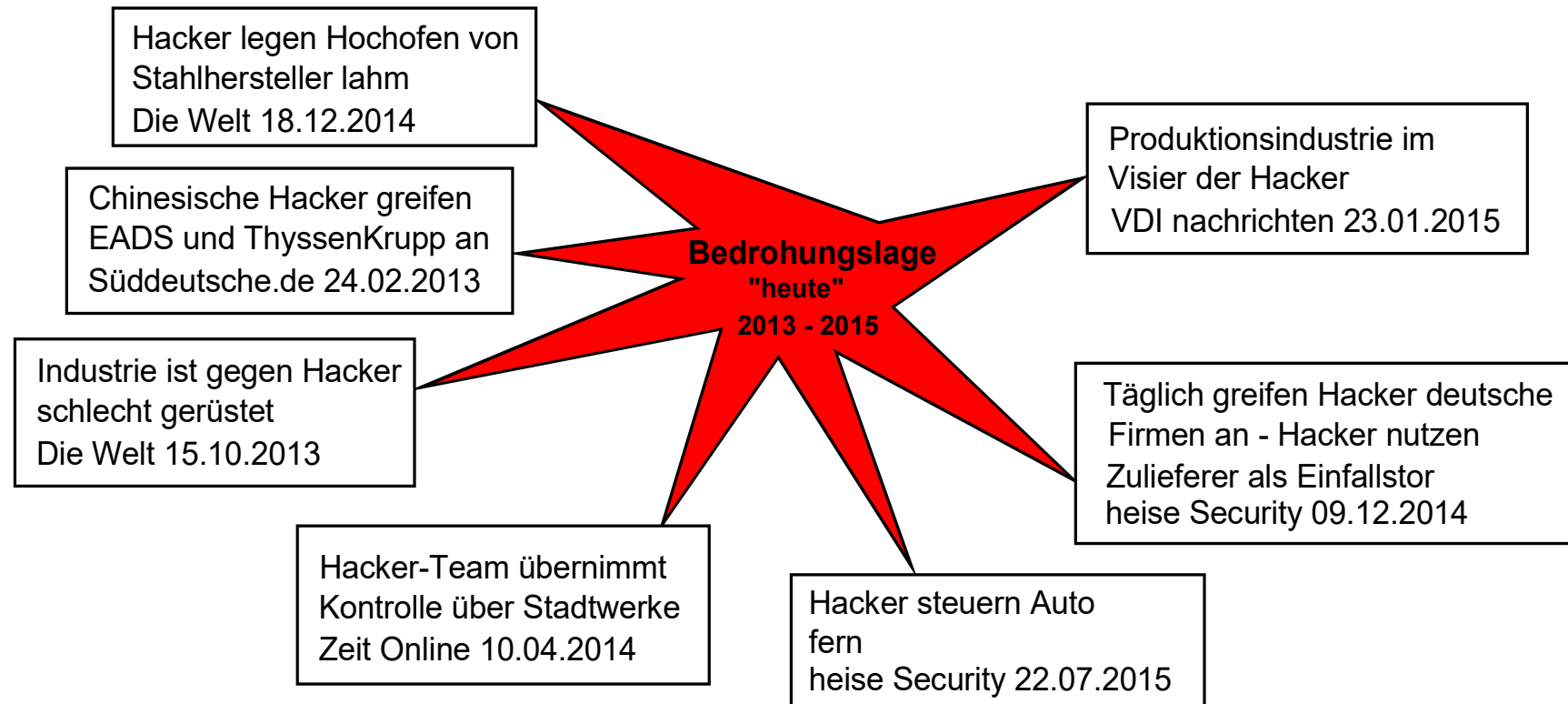
Höhe des Schadens (monetär oder nicht monetär), der sich aus einem Schadensszenario (erfolgreicher Angriff auf ein IT-System durch Ausnutzen einer Schwachstelle) ergibt.

---





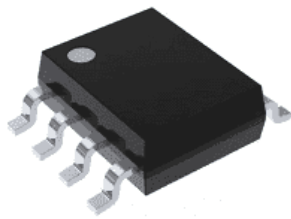
⇒ Lokal beschränktes Schadensausmaß



⇒ Angriffe mit existenzbedrohendem Schadensausmaß

### Fehlerinjektion:

Ziel der Angriffsmethode ist es, Kryptoprozessoren zu kompromittieren, indem man die Ausführung von Maschinenbefehlen unterbricht bzw. stört.



Dadurch können Befehle

- falsch geladen,
- ungültige Daten weitergereicht oder
- Instruktionen übersprungen werden.



Die Technik der Fehlerinjektion stammt aus den **1970er Jahren** als sie zum ersten Mal verwendet wurde, um Fehler auf Hardwareebene zu induzieren.

### Fehlerinjektion:

- Power/Clock Glitch Fault Injection (**PGFI**); Angriffspunkt: Pin-Zugriff; kurzfristiges Abschalten der Spannungsversorgung (voltage glitch) oder Einfügen eines Taktpulses (clock glitch)
  - Light/Laser Fault Injection (**LFI**); Angriffspunkt: Chip-Oberfläche; z. B. Optischer Bereich: 3 THz – 300 PHz (Peta); 100  $\mu\text{m}$  – 1 nm
  - Elektromagnetische Fault Injection (**EMFI**); Angriffspunkt: Chip-Oberfläche; z. B. Mikrowellen (Hochfrequenz): 300 MHz – 300 GHz; 10 cm – 1 mm
  - Body Biased Fault Injection (**BBFI**); Angriffspunkt: Chip-Oberfläche; Hochspannungsimpuls auf das Schaltungssubstrat
  - Softwareimplementierte Fault Injection (**SWIFI**); Angriffspunkt: Software-system; unterschieden wird zwischen Kompilerzeit- und Laufzeit-Injektion
-

---

## Kap. 1: Einführung in die Informationssicherheit

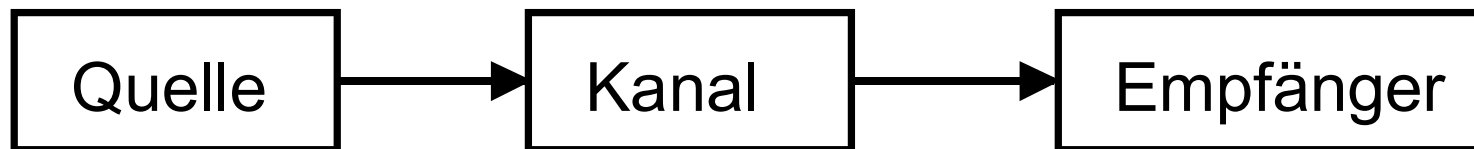
### Teil 2: Daten, Nachrichten und Informationen

- Terminologie
- Nachrichten- und Informationsmodelle
- Kryptosysteme

## Codierungstheorie (US-amer. Mathematiker Claude Shannon)

Nachrichten möglichst effizient und möglichst fehlerfrei übertragen bzw. speichern (z. B. Rundfunk, Fernsehen, Telefon, Datenspeichersysteme, Rechnernetze etc.)

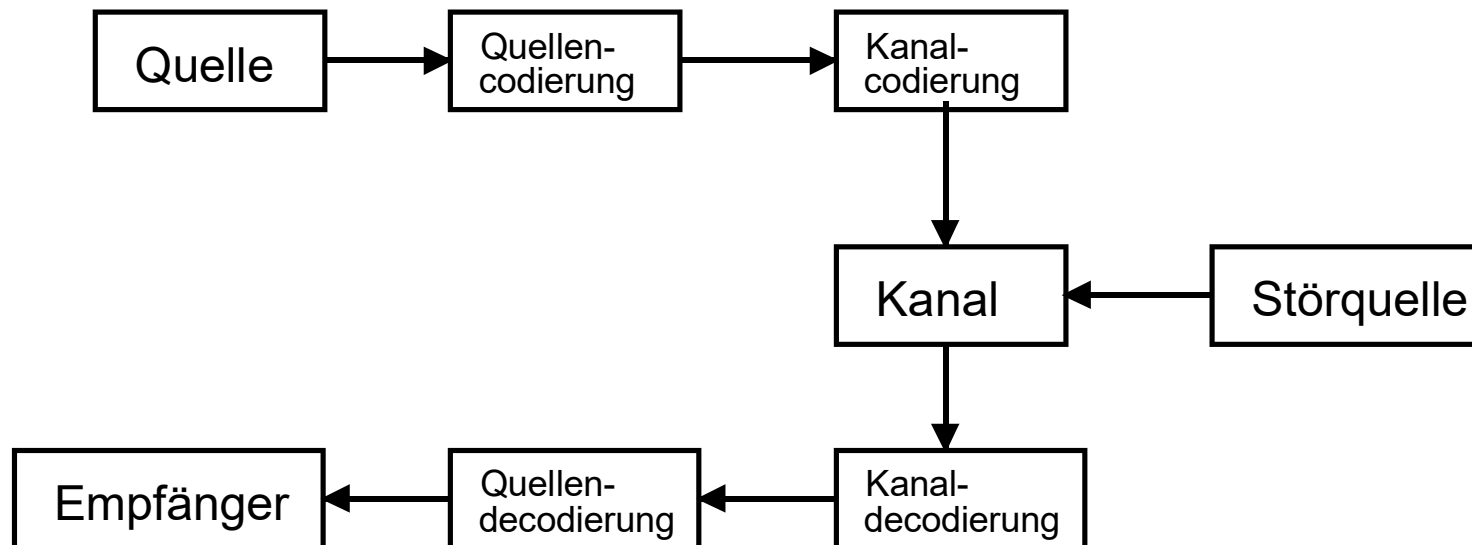
Einfachstes Modell:



- Viele Quellen besitzen Redundanz (Weitschweifigkeit, Überbestimmtheit)
- Fast alle Kanäle unterliegen Störungen (Rauschen)

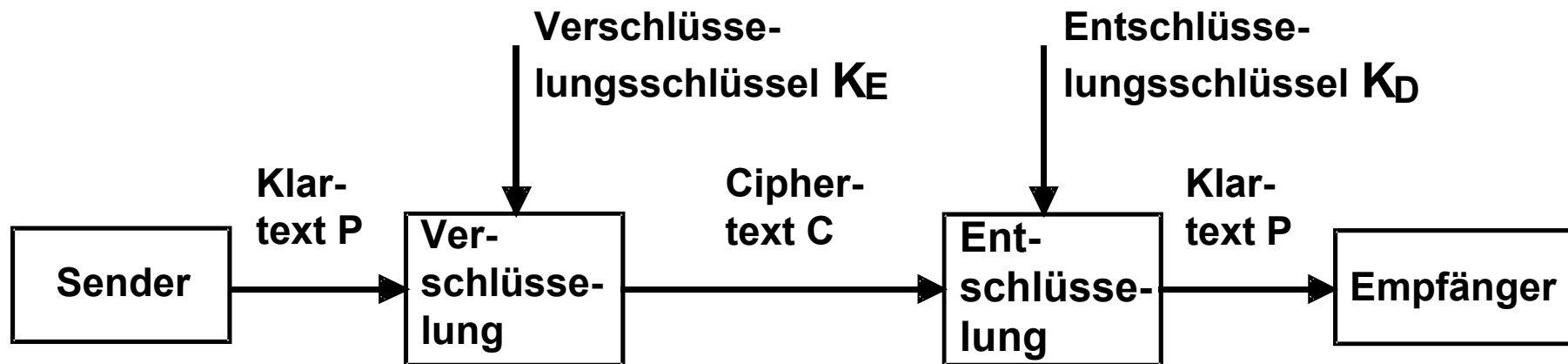


Verfeinertes Modell:



- Eliminierung der Redundanz (Datenkompression oder Quellencodierung)
- Gezieltes Hinzufügen von Redundanz (Kanalcodierung)

Kryptosystem:

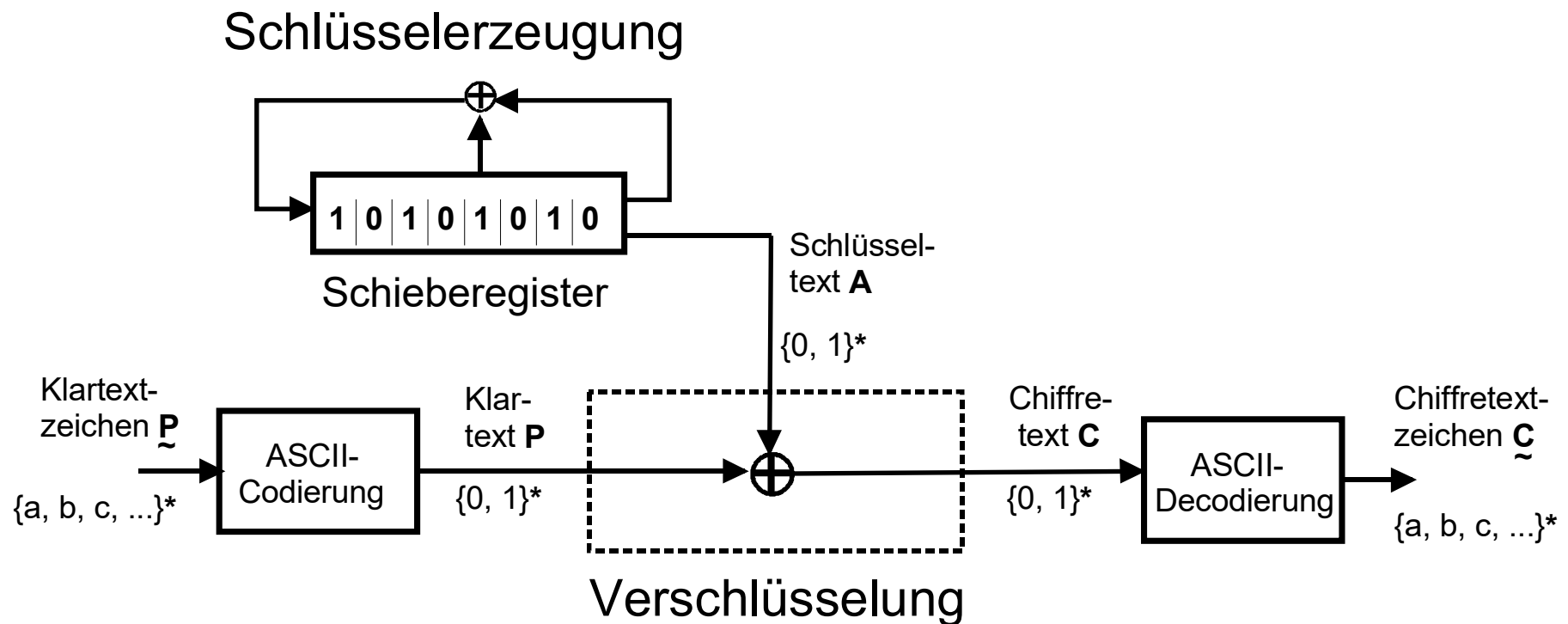


- Schlüsselgesteuerte Transformation (asymmetrisch)
- Formale Beschreibung durch das Quintupel: ( P, C, K, E, D )  
( **P** = Plaintext, **C** = Ciphertext, **K** = Key, **E** = Encryption,  
**D** = Decryption)

### Namensgebung:

Klartext <b>P</b> (plaintext)	lesbarer Text einer Nachricht (message), z. B. Buchstaben, Zahlenfolge, Zeichenkette etc., welche man vertraulich übermitteln möchte
Geheimtext <b>C</b> (ciphertext)	verschlüsselte, tatsächlich übermittelte Nachricht (Zeichenkette über dem gleichen Alphabet A oder einem anderen Alphabet B)
Schlüssel <b>K</b>	Geheimnis (Parameter, der in der Rechenvorschrift zur Anwendung kommt, Sicherheit → Kerckhoffs)
Chiffrieralgorithmus <b>E</b> bzw. <b>D</b>	Rechenvorschrift zum Ver- bzw. Entschlüsseln mit $C := E(P, K)$ und $P := D(C, K^{-1}) = D(E(P, K), K^{-1})$
Vorgang	chiffrieren = verschlüsseln → encryption (enc E) dechiffrieren = entschlüsseln → decryption (dec D)

## Prinzip einer Stromchiffre



Die 26 möglichen Verschiebechiffren des Alphabets:

<u>Klartext:</u>		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
<u>Chiffretexte:</u>	<b>0</b>	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	<b>1</b>	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
<b>Schlüssel</b>	<b>2</b>	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
<b>k</b>	<b>3</b>	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
<b>↓</b>	<b>4</b>	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	<b>5</b>	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	<b>6</b>	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	<b>7</b>	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	<b>8</b>	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	<b>...</b>																										
	<b>25</b>	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

## Beispiel (**Vigenère**-Chiffre)

Plaintext:

- $P = s c h w a c h s t e l l e n a n a l y s e$

Ciphertext:

- $C = X H M B F H M X Y J Q Q J S F S F Q D X J$

Key:

- $K = 5$

Encryption:

- $E = z \rightarrow (z + k) \bmod n$  ;  $z = \text{Plaintextzeichen}$

Decryption:

- $D = z' \rightarrow (z' - k) \bmod n$  ;  $z' = \text{Ciphertextzeichen}$

## Prinzip einer **Hill**-Chiffre (Lester S. Hill; 1891-1961, US-amer.) Mathematiker, Lehrer und Kryptograph

Ausgangslage:

- Restklassenring  $\mathbf{Z}_p = \{0, 1, \dots, p - 1\}$  mit  $p \in \mathbf{IP}$  ist ein Körper.
- In einem Körper existiert die **modulare Inverse**.

Algorithmus:

Verschlüsselung:  $\mathbf{C} = \mathbf{P} \cdot \mathbf{K} \pmod{p}$       $\mathbf{C}$  = Chifftrat

Entschlüsselung:  $\mathbf{P} = \mathbf{C} \cdot \mathbf{K}^{-1} \pmod{p}$       $\mathbf{P}$  = Klartext

$\mathbf{K}$  = Schlüsselmatrix

$\mathbf{C}$ ,  $\mathbf{P}$ ,  $\mathbf{K}$  sind Matrizen, z. B.  $3 \times 3 \rightarrow 64$  Bit Blocklänge



(1912 – 1954)

### Alan Mathison Turing

- britischer Mathematiker und Kryptoanalytiker (Bletchley Park, 1943)
- einflussreichster Theoretiker der Computerentwicklung (Colossus)
- legte die theoretischen Grundlagen der frühen Informatik (Berechen- und Entscheidbarkeit)
- maßgeblich an der Entzifferung von Enigma-verschlüsselten Funksprüchen beteiligt

Von 1945 bis 1948 im National Physical Laboratory, Teddington, tätig am Design der **A**utomatic **C**omputing **E**ngine (ACE)

---



### Shannonsche Theorie

Wichtige **Konstruktionsprinzipien** für die kryptographische Sicherheit sind Konfusion und Diffusion.

#### **Konfusion:**

Die Konfusion einer Blockchiffre ist dann groß, wenn die statistische Verteilung der Chiffretexte in Abhängigkeit von der Verteilung der Klartexte für den Angreifer zu groß ist (keine Ausnutzbarkeit).

#### **Diffusion:**

Die Diffusion einer Blockchiffre ist dann groß, wenn jedes einzelne Bit des Klartextes (und des Schlüssels) möglichst viele Bits des Chiffretextes beeinflusst (typisch etwa 50 %).

---

### Komplexität:

Das Entscheidungsproblem **PRIMES** besteht darin, zu entscheiden, ob es sich bei einer gegebenen natürlichen Zahl  $z > 1$  um eine Primzahl handelt. Dabei sei die Zahl  $z$  zur Basis  $b \in \mathbb{IN}$  dargestellt.

Die dazugehörige Sprache sei mit  $L_b = L[\mathbf{PRIMES}, b]$  bezeichnet.

Satz:

Sei  $L_1 := L[\mathbf{PRIMES}, 1]$ . Erst 2002<sup>1)</sup> konnte gezeigt werden, dass gilt:

**$L_1$  liegt in  $P$**

d. h. es gibt eine DTM, deren Laufzeit von der Ordnung  $O(n^3)$  und damit polynomial beschränkt ist.

1) Drei indische Mathematiker: M. Agrawal, N. Kayal und N. Saxena

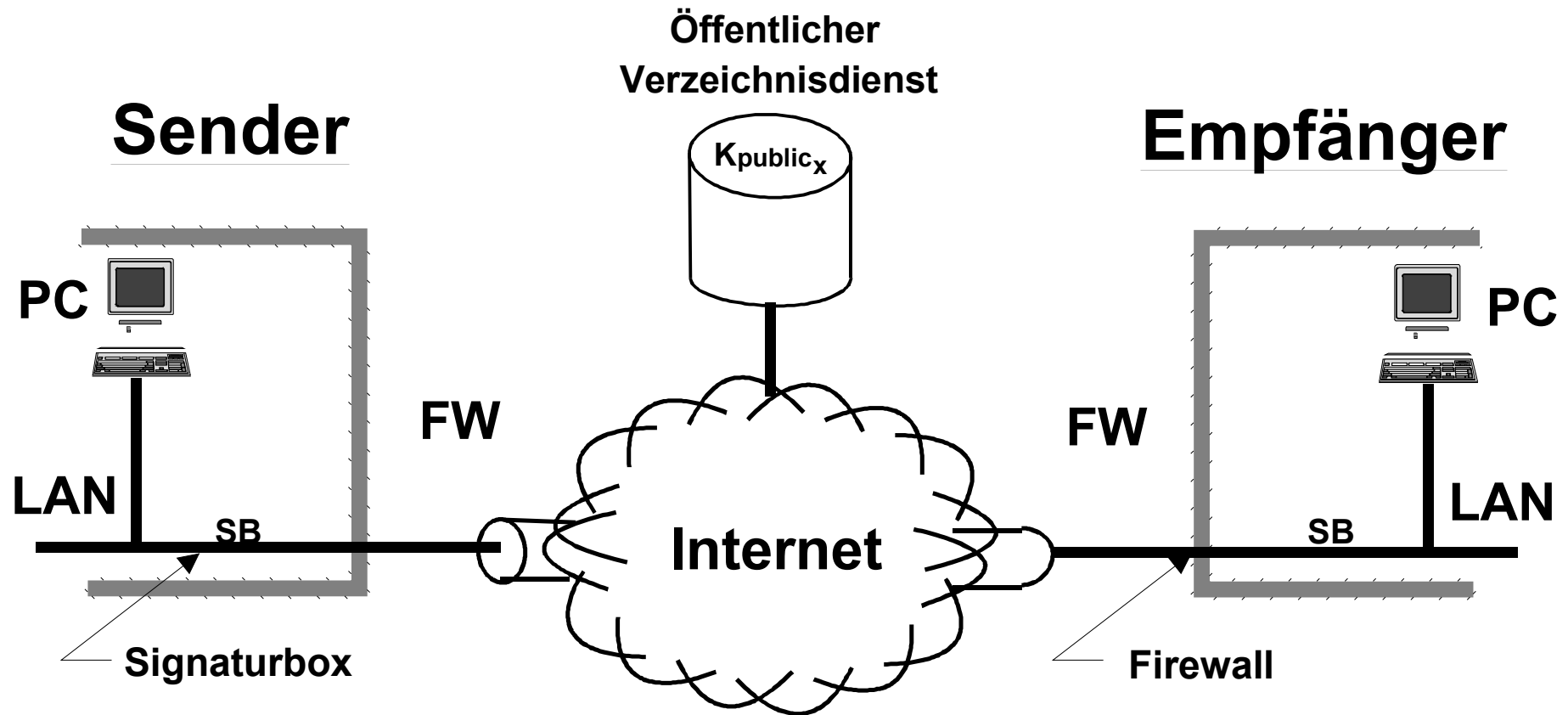
---

---

## Kap. 1: Einführung in die Informationssicherheit

### Teil 3: Schutzziele der Datensicherheit

- Begrifflichkeiten im Kontext von Datensicherheit
- Sicherheitsanforderungen und Sicherheitsziele
- Verschlüsselungsfunktionen und -algorithmen
- Kryptographische Hashfunktionen und digitale Signaturen
- Schlüsselmittel



---

**Sicherheitsanforderungen** werden i. a. mit handelnden Subjekten und schützenswerten Objekten verknüpft.

- **was** soll geschützt werden?  $\Rightarrow$  schützenswerte Objekte
- **vor wem** oder was soll geschützt werden  $\Rightarrow$  handelnde Subjekte

Die (positive) Verknüpfung von Subjekten und Objekten wird im folgenden **Schutzziel** oder **Sicherheitsziel** genannt.

Zur Erreichung der Sicherheitsziele (Schutzziele) müssen geeignete **Sicherheitsdienste** bzw. **Sicherheitsfunktionen** und -maßnahmen bereitgestellt werden.

**Sicherheitsfunktionen** werden durch ihnen zugrunde liegenden **Sicherheitsmechanismen** (Sicherheitsalgorithmen) realisiert.

---

**Sicherheit** ist die Wahrscheinlichkeit, einen bezifferbaren oder nicht bezifferbaren Schaden zu verhindern oder zumindest auf ein erträgliches Restmaß (Restrisiko) einzuschränken ⇒ Schutzziele

### Grundlegende Sicherheitsziele:

Vertraulichkeit → Schutz gegen unautorisierte Kenntnisnahme

Integrität → Schutz gegen unautorisierte Veränderung

Verfügbarkeit → Schutz gegen unautorisierte Vorenthaltung/  
Verweigerung

Verbindlichkeit (Authentizität) → Schutz gegen Verlust der Beweisbarkeit/  
Zurechenbarkeit und nicht Abstreitbarkeit

## Grundlegende Sicherheitsfunktionen und -maßnahmen:

### 1. Vertraulichkeitsschutz

**Kryptographische Algorithmen** sind Berechnungsvorschriften, d. h. mathematisch / logische Funktionen zur Ver- und Entschlüsselung von Nachrichten.

Bei **symmetrischen Algorithmen** wird zum Chiffrieren und zum Dechiffrieren immer der gleiche Schlüssel **K** benutzt.

Bei **asymmetrischen Algorithmen** werden zum Ver- und Entschlüsseln zwei unterschiedliche Schlüssel **K<sub>1</sub>** bzw. **K<sub>2</sub>** benutzt, die allerdings miteinander korrespondieren. Es gilt:

$$\mathbf{C} := E(\mathbf{M}, \mathbf{K}_1) \text{ und } \mathbf{M} := D(\mathbf{C}, \mathbf{K}_2) = D(E(\mathbf{M}, \mathbf{K}_1), \mathbf{K}_2)$$

## Grundlegende Sicherheitsfunktionen und -maßnahmen:

### 1. Vertraulichkeitsschutz (Fortsetzung)

Man unterscheidet bei Kryptoalgorithmen zwischen **Stromchiffren** und **Blockchiffren**.

- Stromchiffren: Zeichen für Zeichen
- Blockchiffren: Nachricht **M** in Blöcke z. B. der Länge  $n = 64$  Bit aufgeteilt

Die Vereinigung von Algorithmus, zugehörigen Schlüsseln und den verschlüsselten Nachrichten (Kryptogramme) wird **Kryptosystem** genannt.

Der **Schlüsselraum**, d. h. die Menge, aus der ein Schlüssel gewählt wird, sollte möglichst groß sein. Er sollte mindestens so groß sein, dass der Aufwand (Kosten, Zeit, Speicherplatz/Datenmenge) für einen Angriff unakzeptabel hoch wird.



## Grundlegende Sicherheitsfunktionen und -maßnahmen:

### 2. Integritätsschutz

Man unterscheidet beim Integritätsschutz zwischen **Hashfunktionen** und **digitalen Signaturen**.

Eine Hashfunktion **hash** ist eine Abbildung, die für eine beliebig lange Nachricht **M** einen Funktionswert **H** (den Hashwert) fester Länge liefert.

$$H = \text{hash}(M)$$

Darüber hinaus muß sie gewisse Bedingungen (Einwegeigenschaft, Kompressionseigenschaft, Kollisionsfreiheit) erfüllen.

Eine Besonderheit sind schlüsselabhängig Hashfunktionen, sogenannte **Keyed-Hash Message Authentication Code (HMAC)**.

## Grundlegende Sicherheitsfunktionen und -maßnahmen:

### 2. Integritätsschutz (Fortsetzung)

Eine digitale Signatur ist ein Datensatz **Sig<sub>T</sub>**, der zusätzlich zu einem Dokument **M** erzeugt wird und dabei das signierte Dokument eindeutig einem Teilnehmer **T** zuordnet:

$$\mathbf{Sig}_T = \mathbf{sig}(H, \mathbf{Sk}_T)$$

Verwendung findet bei der Signaturerstellung der **geheime** Schlüssel des Teilnehmers T.

Bei der Signaturprüfung wird der zugehörige **öffentliche** Schlüssel des Teilnehmers T benötigt.

⇒ Public Key System

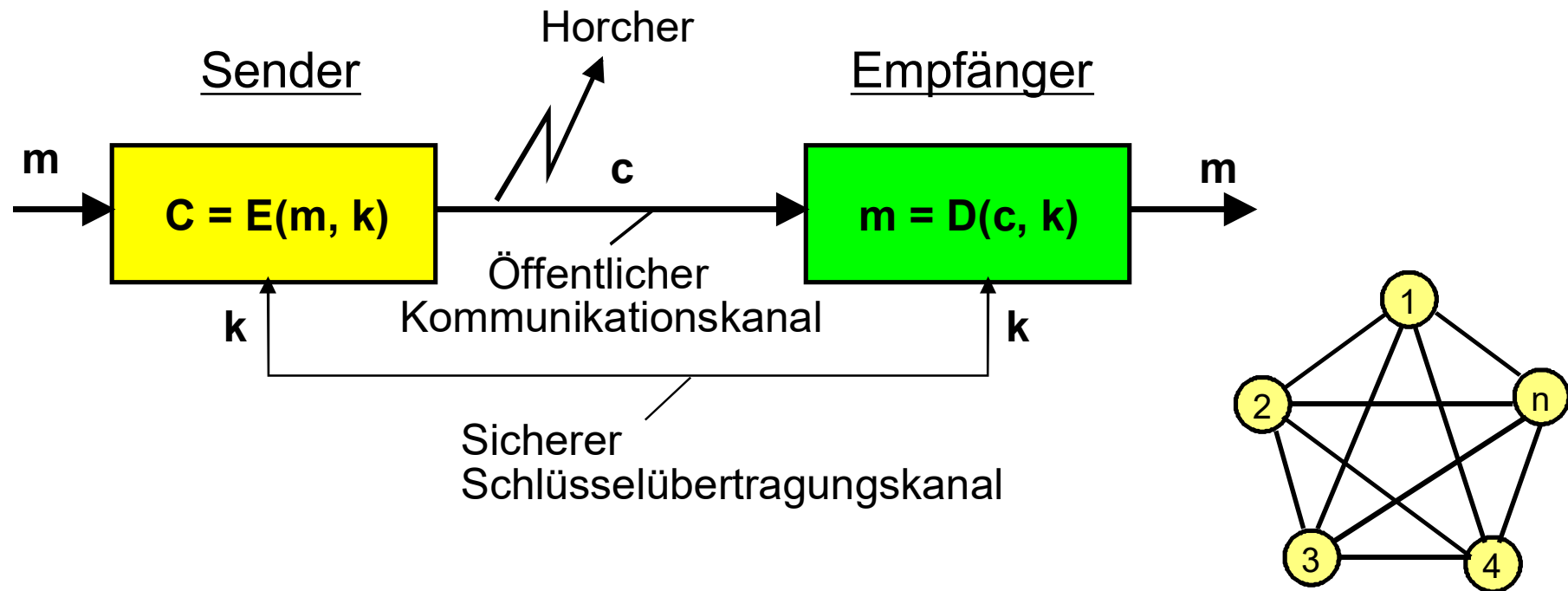
---

## Kap. 1: Einführung in die Informationssicherheit

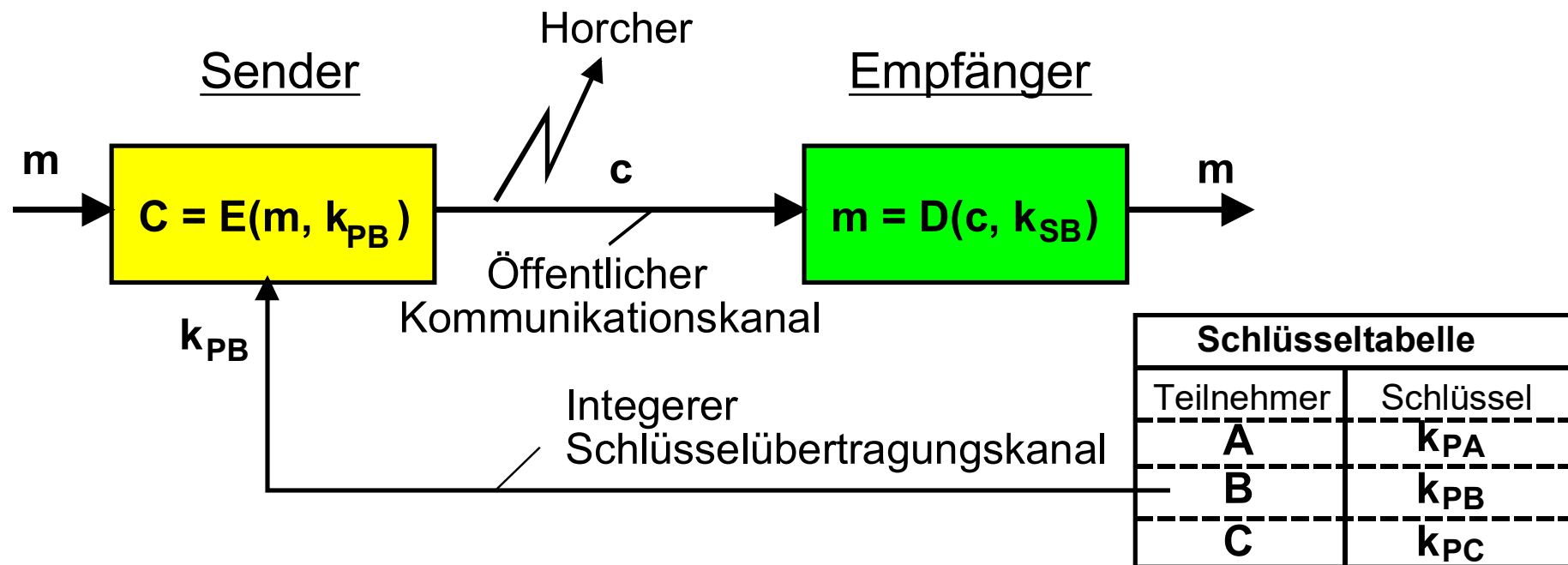
### Teil 4: Basismechanismen der Kryptologie (Überblick)

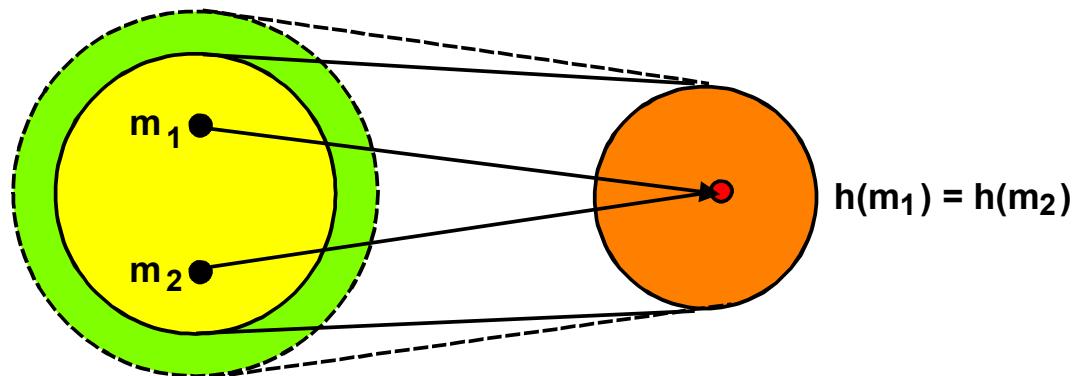
- Symmetrische Ver- und Entschlüsselung
- Asymmetrische Ver- und Entschlüsselung
- Kryptographische Hashfunktionen
- Message Authentication Code
- Digitale Signaturen
- Schlüsselmittelmanagement und Zufallszahlen

# Basismechanismen im Überblick Symmetrische Verschlüsselung



# Basismechanismen im Überblick Asymmetrische Verschlüsselung





hier:

Prinzip einer Hashfunktion  
**mit Kollision**

### Basisprinzip:

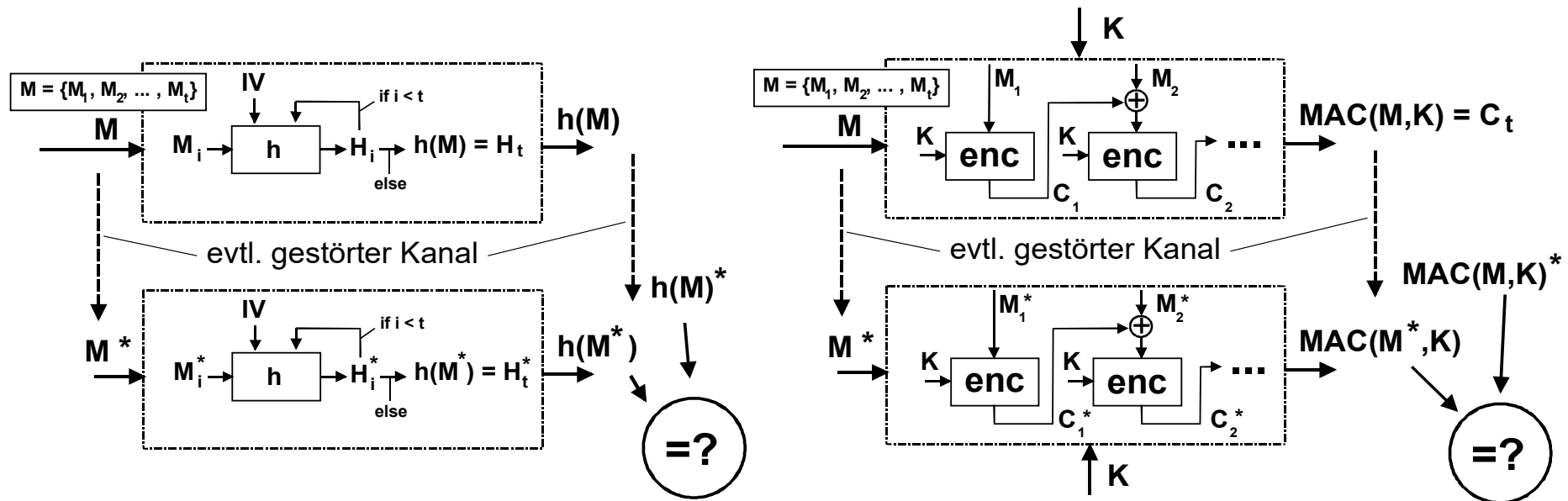
- Nachricht beliebiger und Hashwert fester Länge (typ. 128 Bit)
- Digitaler Fingerprint

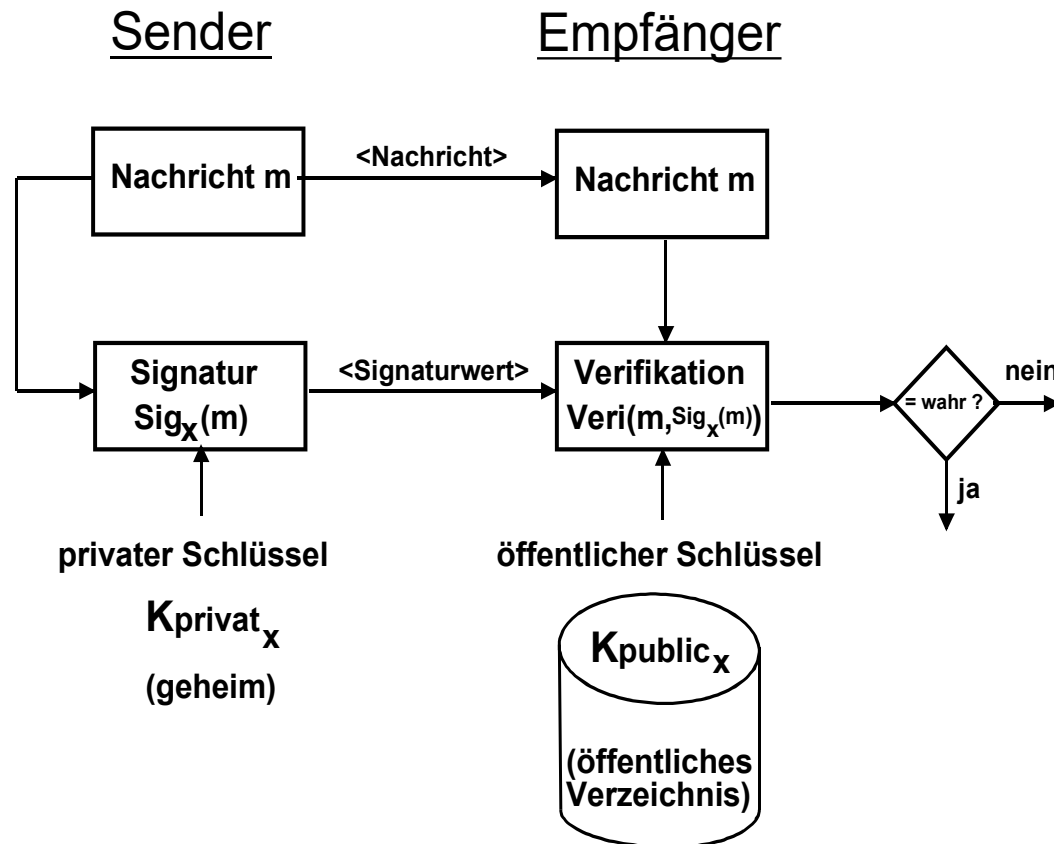
### Eigenschaften:

- kollisionsresistent
- mit und ohne geheimen Schlüssel (→ **MD** bzw. **MAC**)

## Message Digest (**MD**)

## Message Authentication Code (**MAC**)





### Basisprinzip:

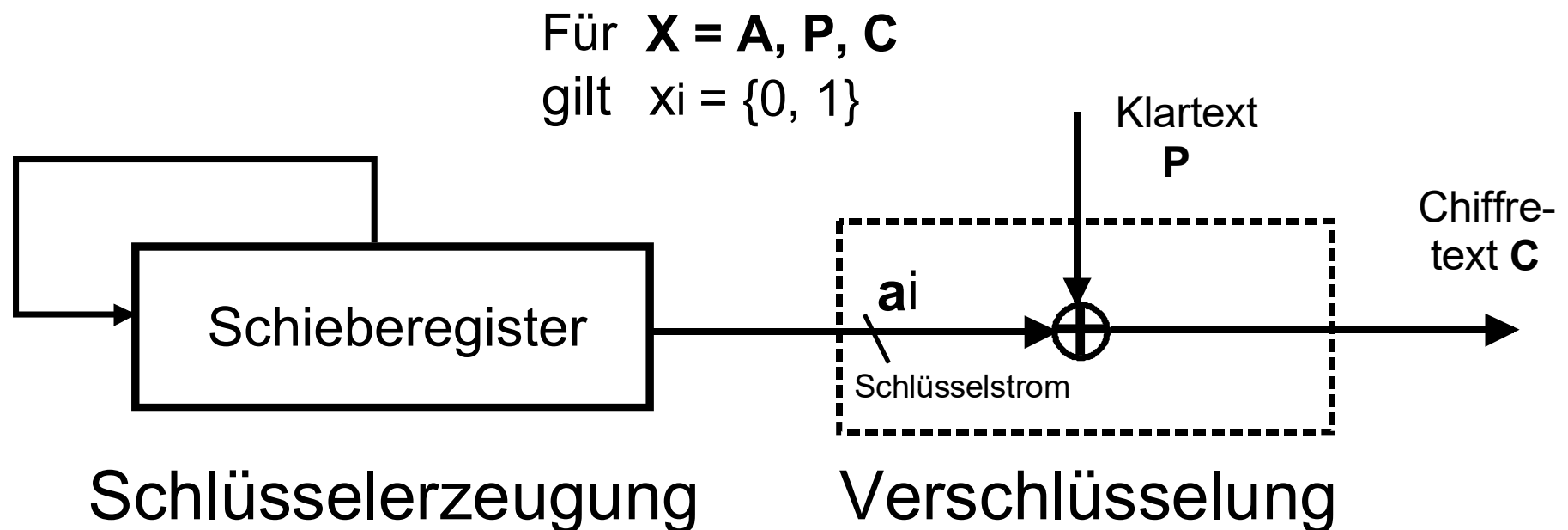
- Privater (geheimer) und öffentlicher Schlüssel
- Signaturwert mit privatem Schlüssel

### Eigenschaften:

- Nachweisbarkeit
- Nicht Abstreitbarkeit
- Authentizität
- Echtheit
- Identitätsnachweis



## Lineare rückgekoppelte Schieberegister



## Kap. 1: Einführung in die Informationssicherheit

### Teil 5: Kryptanalyse

- Das Prinzip von Kerckhoffs
- Typen von Attacken
- Angriffsstrategien und Analyseverfahren
- Klassifizierung der Sicherheit von Kryptosystemen
- Steganographie

### Alexandre Auguste Kerckhoffs von Nieuwenhof (niederl. Philologe, 1835 – 1903)

- Klassische Kryptographie ist geprägt vom Wechselspiel zwischen Kryptographie und Krypanalyse (Erkenntnisse → Entwicklungen).
- Die Sicherheit eines Kryptosystems darf nicht von dessen Geheimhaltung, sondern nur von der Schlüssellänge abhängen.

Seien  $\mathbf{P}$ ,  $\mathbf{C}$ ,  $\mathbf{K}$  die Mengen der Plaintexte, Chiffretexte bzw. Schlüssel und  $\mathbf{E} : \mathbf{P} \times \mathbf{K} \rightarrow \mathbf{C}$  ein Verschlüsselungssystem. Ist ein Kryptoanalytiker im Besitz eines Plaintext-Chiffretextpaares  $(p, c) \in \mathbf{P} \times \mathbf{C}$ , so kann der verwendete Schlüssel  $k$  durch **vollständige Suche** ermittelt werden, da  $\mathbf{E}(p, k) = c$  gelten muss.

---

- **Ciphertext-only-Attack:**

Es besteht lediglich die Möglichkeit, für die Analyse verschlüsselte Daten (ciphertext) in beliebigem Umfang zu verwenden.

- **Known-Plaintext-Attack:**

Es stehen Klartext-Schlüsseltextpaare zur Verfügung, wobei bei der Analyse ausgenutzt wird, dass bestimmte Textphrasen häufig verwendet werden.

- **Chosen-Plaintext-Attack:**

Hier verwendet der Kryptoanalytiker beim Angriff die Chiffre zu selbstgewählten Klartexten.

- **Vollständiges Suchen:**

Die gesamte Schlüsselmenge wird durchsucht, um den jeweils verwendeten Schlüssel zu finden (ohne praktische Bedeutung).

- **Trial and Error:**

Im Gegensatz zur vollständigen Suche wird vorausgesetzt, dass eine Strukturanalyse dazu geführt hat, die Schlüsselwahl einzuschränken.

- **Statistische Methoden:**

Hierbei werden statistische Eigenschaften (Verteilungen) verwendet, um Rückschlüsse auf den zugehörigen Klartext zu ermitteln.

- **Strukturanalyse:**

Ausgenutzt werden spezielle Strukturen mit dem Ziel, effiziente Algorithmen zum Brechen des Kryptoverfahrens zu entwerfen.

---

Ein Kryptosystem heißt

- **absolut sicher**,  
wenn nicht genug Information gewonnen werden kann, um hieraus den Klartext oder den Schlüssel zu rekonstruieren.
  - **analytisch sicher**,  
wenn es kein nichttriviales Verfahren gibt, mit dem es systematisch gebrochen werden kann.
  - **komplexitätstheoretisch sicher**,  
wenn es keinen Algorithmus gibt, der das Kryptosystem in Polynomialzeit in Abhängigkeit der Schlüssellänge brechen kann.
  - **praktisch sicher (→ starke Verfahren)**,  
wenn kein Verfahren bekannt ist, welches das Kryptosystem mit vertretbarem Ressourcen-, Kosten- und Zeitaufwand brechen kann.
-

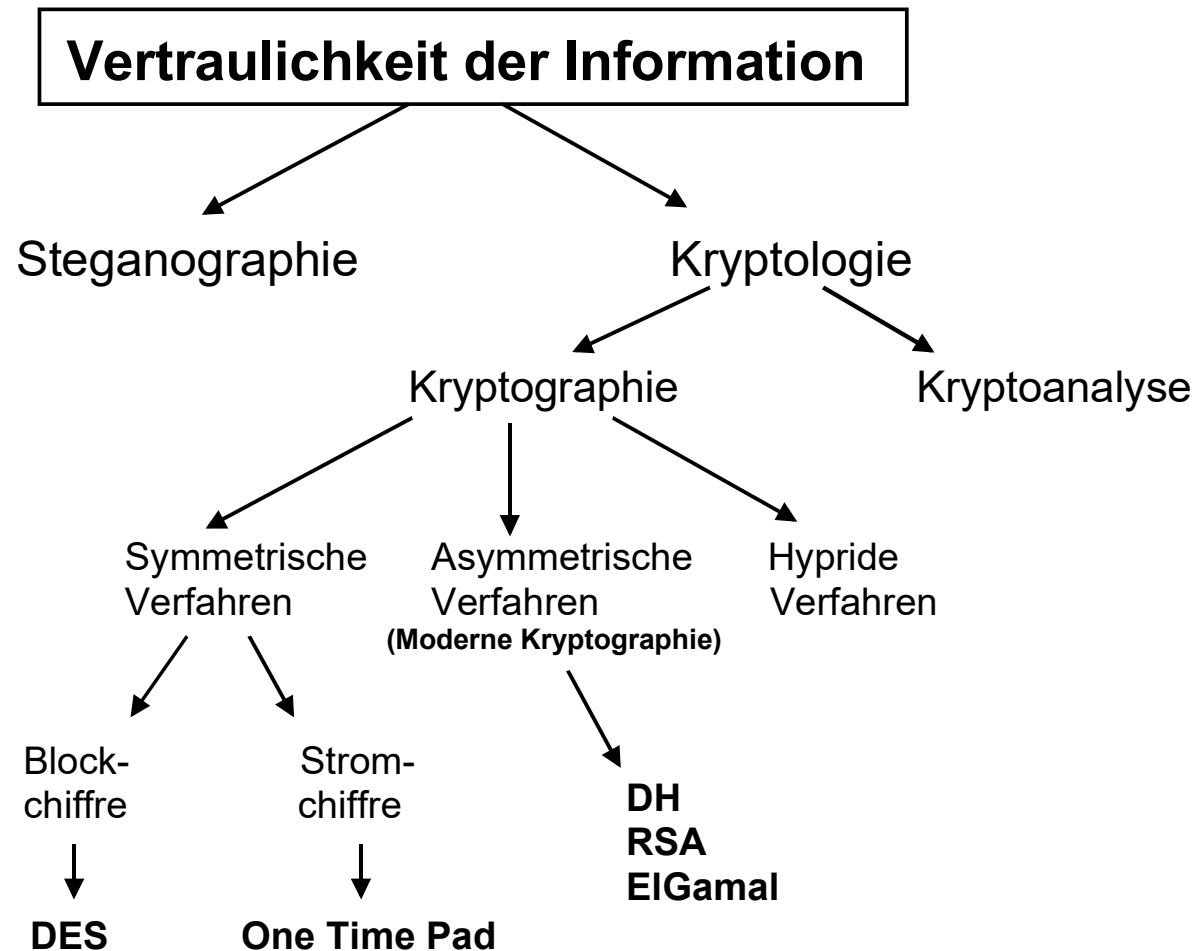
Für die Beurteilung der benötigten Schlüssellänge sind folgende Definitionen sehr hilfreich:

1. Ein **Algorithmus** gilt als **sicher**, wenn

- der zum Aufbrechen nötige Geldaufwand den Wert der verschlüsselten Daten übersteigt oder
- die zum Knacken erforderliche Zeit größer ist als die Zeit, die die Daten geheim bleiben müssen, oder
- das mit einem bestimmten Schlüssel chiffrierte Datenvolumen kleiner ist als die zum Knacken erforderliche Datenmenge.

2. Ein **Algorithmus** gilt als **uneingeschränkt sicher**, wenn der Klartext auch dann nicht ermittelt werden kann, wenn Chiffretext in beliebigem Umfang vorhanden ist  $\Rightarrow$  **starke Kryptographie**.

---





---

D	V	A	B	S	Z
I	H	E	E	S	E
Y	T	E	H	O	T
E	I	Y	T	S	N
I	G	A	E	H	Y
D	O	Y	U	E	I
M	A	N	B	B	L
O	T	I	O	D	S

---

D		A		S	
I				S	
					T
E	I				N
	G		E	H	
				E	I
M		N			
		I			S

### Beispiel für eine verdeckte Botschaft

Was verbirgt sich hinter der folgenden Kleinanzeige?

- Räumung
- Seniorenzug
- Ankauf

**KLEINTRANSPORTE**  
Eriko Yamashita  
  
intelligent - sauber - tadellos  
*Tel: 0126-114719*

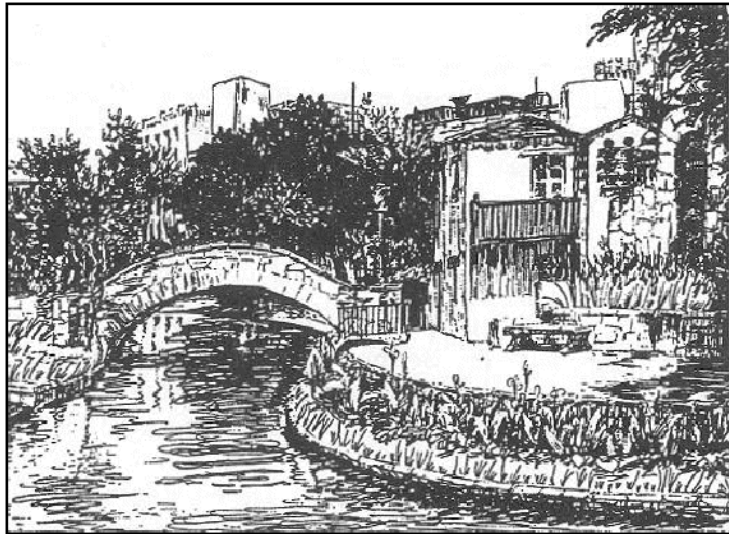


HEGLA

**Hinweis:** Man beachte Anfangsbuchstaben und Tel.-Nr.

### Beispiel für eine verdeckte Botschaft

Wo verbirgt sich die Nachricht? Wie lautet diese?



**Hinweis:** Man beachte den Verlauf des San Antonio Rivers (1945)

- **Semagramme:** Nachrichten, die in Details von Skizzen oder Gegenständen verborgen sind.
- Die Botschaft wurde unter Anwendung des Morsealphabets (kurz, lang und Pause/ Leer-raum) codiert.
- Zeitschema „ein/aus“ optisch aus der Länge der Grashalmen links von der Brücke auf der kleinen Mauer und rechts entlang des Flusses.

David Kahn: The Codebreakers, Macmillan, 1996, S. 155 ff.

---

## Kap. 1: Einführung in die Informationssicherheit

### Zusammenfassung:

- Aufgrund der gegenwärtigen Gefährdungslage im IT-Bereich sind IT-Sicherheitsmaßnahmen (Funktionen) unerlässlich.
- Die Realisierung von IT-Sicherheitsmaßnahmen und -funktionen erfolgt mit den Mitteln der Kryptologie.
- Wir unterscheiden in klassische und moderne Kryptologie (sog. Public Key Cryptographie).
- Besondere Bedeutung in der Praxis hat nach wie vor die Informationsverschlüsselung (Geheimhaltung).

---

## Kap. 1: Einführung in die Informationssicherheit

### Zusammenfassung (Fortsetzung):

- Hashwerte und Message Authentication Codes dienen zum Nachweis der Authentizität der Daten, besitzen aber keine Beweiskraft gegenüber Dritten.
- Eine digitale Signatur wird mittels des geheimen Schlüssels des Urhebers gebildet.
- Die Überprüfung der Korrektheit einer Signatur findet mittels des zugehörigen öffentlichen Schlüssels statt.
- Die Urheberschaft kann gegenüber Dritten bewiesen werden.