Symmetrische und Asymmetrische Kryptographie

Technik Seminar 2012

Inhalt

- Symmetrische Kryptographie
  - Transpositionchiffre
  - Substitutionchiffre
  - Aktuelle Verfahren zur Verschlüsselung
  - Hash-Funktionen
  - Message Authentication Code
- Asymmetrische Kryptographie
  - Verschlüsselte Datenübertragung
  - Digitale Signatur
  - Zeitstempel
  - Zertifikate
  - Sicherheit
- Hybride Verschlüsselung

Symmetrische Kryptographie

- Älteste Art der Kryptographie
  - Erste bekannte Anwendung → alte Ägypter ca.3000v.Chr.
  - Caesar-Chiffre im alten Rom
- Chiffrier- und Dechiffrierschlüssel gleich
- Stromchiffre:
  - Zeichen- bzw. Bitweise Verschlüsselung
- Blockchiffre
  - Klartext in Blöcke gleicher Länge
  - Blockweise Verschlüsselung
  - Eventuell Füll-Bits benutzen (Padding)

Transpositionschiffren

- Veränderung der Buchstaben- bzw. Bitfolge
- Beispiel:
  - „Kryptografie“ soll mittels einer 3x4 Matrix verschlüsselt werden:

$$\begin{pmatrix} K & R & Y & P \\ T & O & G & R \\ A & F & I & E \end{pmatrix}$$

  - Die Spalten werden nun in der Reihenfolge 4,1,2,3 neugeordnet
  - Es ergibt sich der Chiffretext: „PREKTAROFYGI“
  - Entschlüsselung durch Häufigkeitsanalyse und Anagramming

Substitutionschiffren

- Ersetzen von Buchstaben durch Buchstaben oder Zahlen
- In Kombination mit Transpositionschiffre
  - → Produktchiffre
- Verschiedene Arten:
  - Monoalphabetische Susbtitution
  - Homophone Substitution
  - Polyalphabetische Substitution

Monoalphabetische Substitution

- Verschlüsselung mit nur einem Geheimalphabet
- Beispiel:
  - Klartext: „SUBSTITUTION“

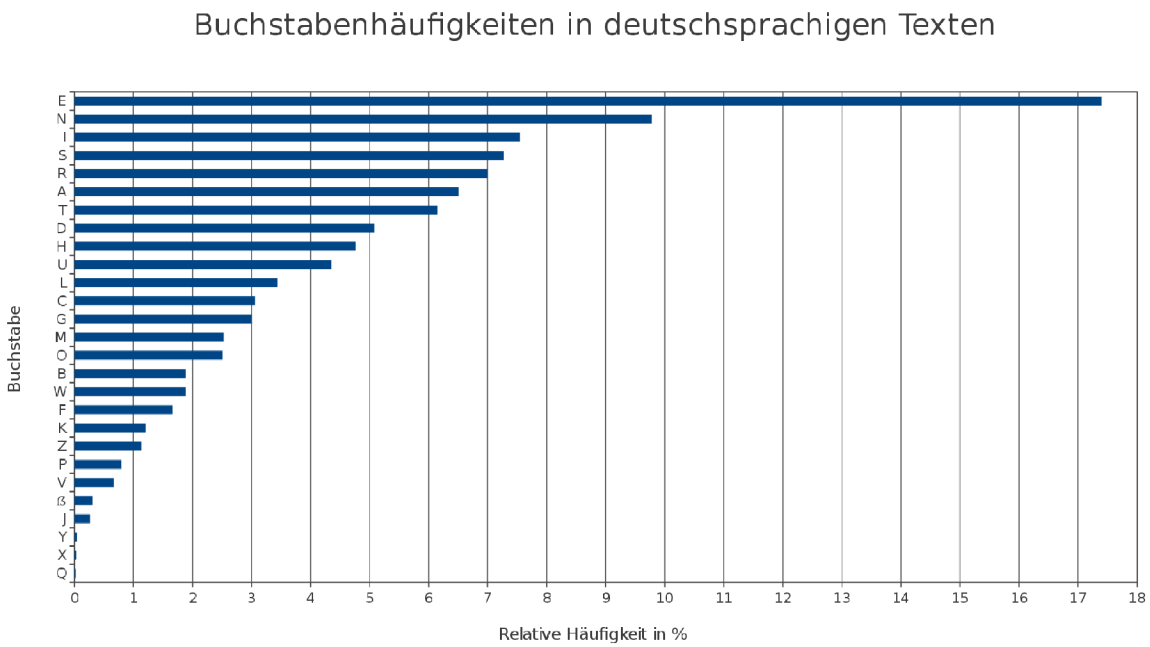
Normales Alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Geheimalphabet:	Q	W	E	R	T	Z	U	I	O	P	A	S	D	F	G	H	J	K	L	Y	X	C	V	B	N	M

Klartext:	S	U	B	S	T	I	T	U	T	I	O	N
Chiffretext:	L	X	W	L	Y	O	Y	X	Y	O	G	F

- Nachteil:
  - Geringe Sicherheit gegen statistische Analyse
  - Abhilfe: homophone Substitution

Homophone Substitution

- Kein Geheimalphabet, sondern Zahlen von 0 bis 99
  - Entsprechend der Buchstabenhäufigkeit verteilt



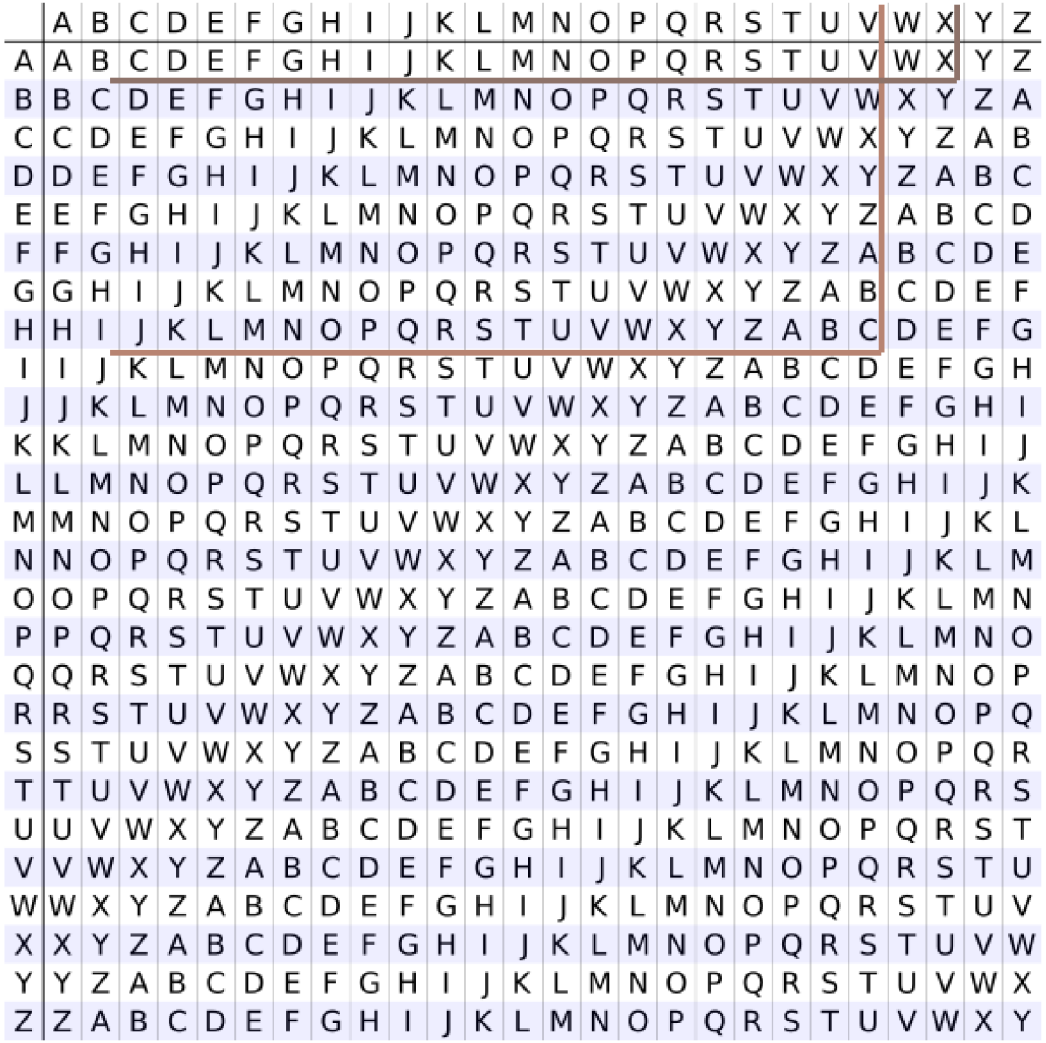
- z.B. „N“ kriegt: 01 23 54 21 53 98 87 67 45 33
- Beim Verschlüsseln zufällig zugeordnet

Polyalphabetische Substitution

- Substitution mit mehreren Geheimalphabeten
- Schlüssel K wird zu Schlüsselstring erweitert
  - Schlüsselstringlänge = Klartextlänge
- Zeichenweise Verschlüsselung mit Vigenère-Quadrat
  - Spalte über Klartextbuchstaben bestimmt
  - Zeile über Schlüsselstringbuchstaben bestimmt

- Beispiel: „SUBSTITUTION“ wird mit dem Schlüssel „HALLO“ verschlüsselt
  - Schlüsselstring: „HALLOHALLOHA“
  - Geheimtext = „ZUMDHPTFEWVN“

Vigenère-Quadrat



	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
A	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	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	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
Z	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

One-Time-Pad

- Art der Vigenère-Verschlüsselung
- Unbrechbar, selbst mit unbegrenzten Ressourcen
- Bedingungen:
  - Schlüssellänge = Klartextlänge
  - Schlüssel durch wahren Zufallsgenerator erzeugt
  - Nur einmalige Verwendung des Schlüssels
- Nachteil:
  - Schlüssel muss von einem vertrauenswürdigen Boten überbracht werden
- Anwendung:
  - Geheimagenten
  - Heißer Draht zwischen Washington und Moskau

Aktuelle Verfahren

- Data Encryption Standard (DES)
  - 1976 als Standard für US-Regierung eingeführt
  - Nicht Sicher, da Schlüssellänge = 56bit
- Triple-DES (3DES)
  - Erweiterung des DES (Mehrfachausführung)
  - Hoher Rechenaufwand → langsam
  - Gilt als relativ sicher (Security Level 6)
- Advanced Encryption Standard (AES)
  - Nachfolger von DES und 3DES
  - Seit 2000 als Standard für symmetrische Verschlüsselung
  - Gilt als unbrechbar (Security Level 8)
  - Anwendung: WPA2, RAR-Archive

Hash-Funktionen

- Liefert eine „Zusammenfassung“ von einer Datei
  - → Fingerabdruck der Datei
- Bildet eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge fester Länge(Hash) ab
- Bedingungen für kryptografische Hash-Funktion:
  - Einwegfunktion
  - Kollisionsresistenz
- Bekannte Funktionen:
  - MD5 (gilt nicht mehr als sicher, da Kollision)
  - SHA (Standard, jedoch SHA-1 unsicher; jetzt→ SHA-2 bzw. SHA-3)

Message Authentication Code (MAC)

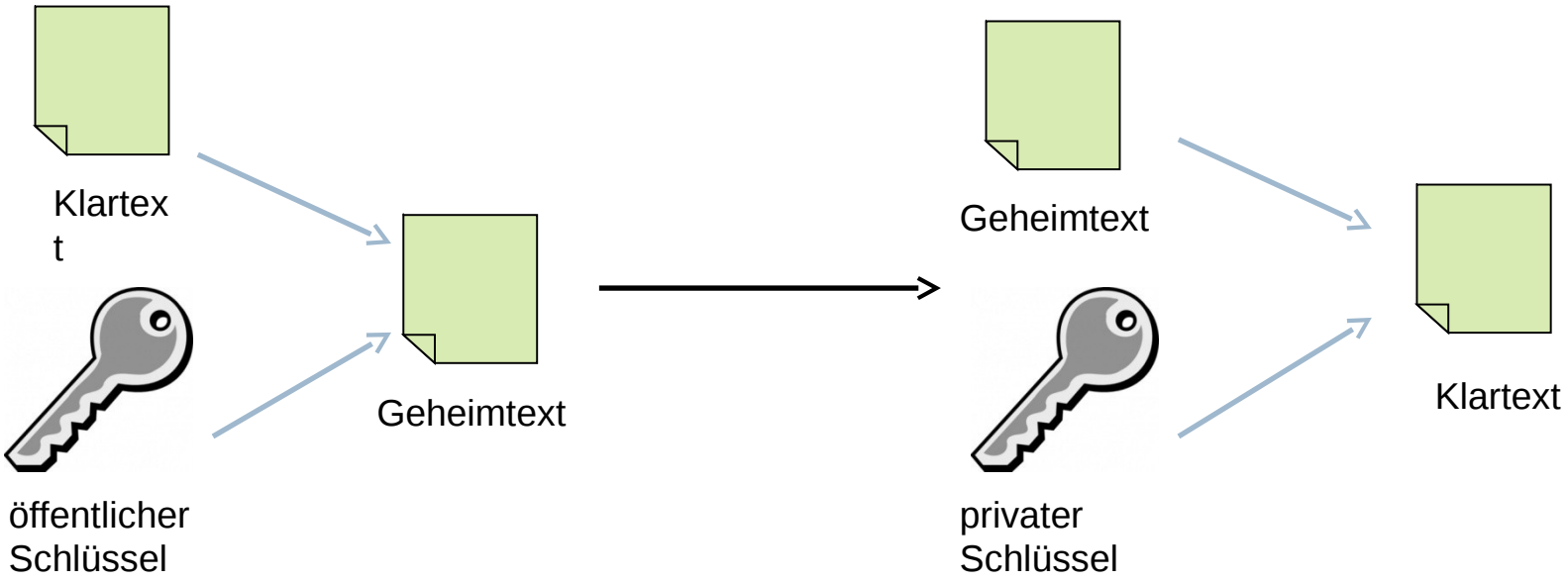
- Zur Überprüfung der Authentizität einer Nachricht
- Keine Geheimhaltung der Nachricht
- Spezielle Hash-Funktionen:
  - Aus beliebigem Schlüssel K und beliebiger Klartext x wird ein MAC-Wert fester Bitlänge bestimmt
  - Ohne Kenntnis des Schlüssels K ist es dem Angreifer unmöglich zu einem Text den richtigen MAC zu bestimmen
- Sender heftet MAC an Nachricht an
- Empfänger generiert neuen MAC und vergleicht diesen mit dem vorhandenen

Asymmetrische Kryptographie

- Geschichte:
  - 1975 erste Idee von Whitfield Diffie und Martin Hellman
  - 1977 Veröffentlichung von RSA
- Prinzip:
  - Schlüsselpaar mit öffentlichem (public-key) und privatem (private-key) Schlüssel
  - Private-key bleibt beim Erzeuger des Schlüsselpaares
  - Schlüsselgenerierung mittels echtem Zufallsgenerator
  - Realisierung über Einwegfunktionen
  - Multiplikation von Primzahlen
  - Diskreter Logarithmus

Verschlüsselte Datenübertragung

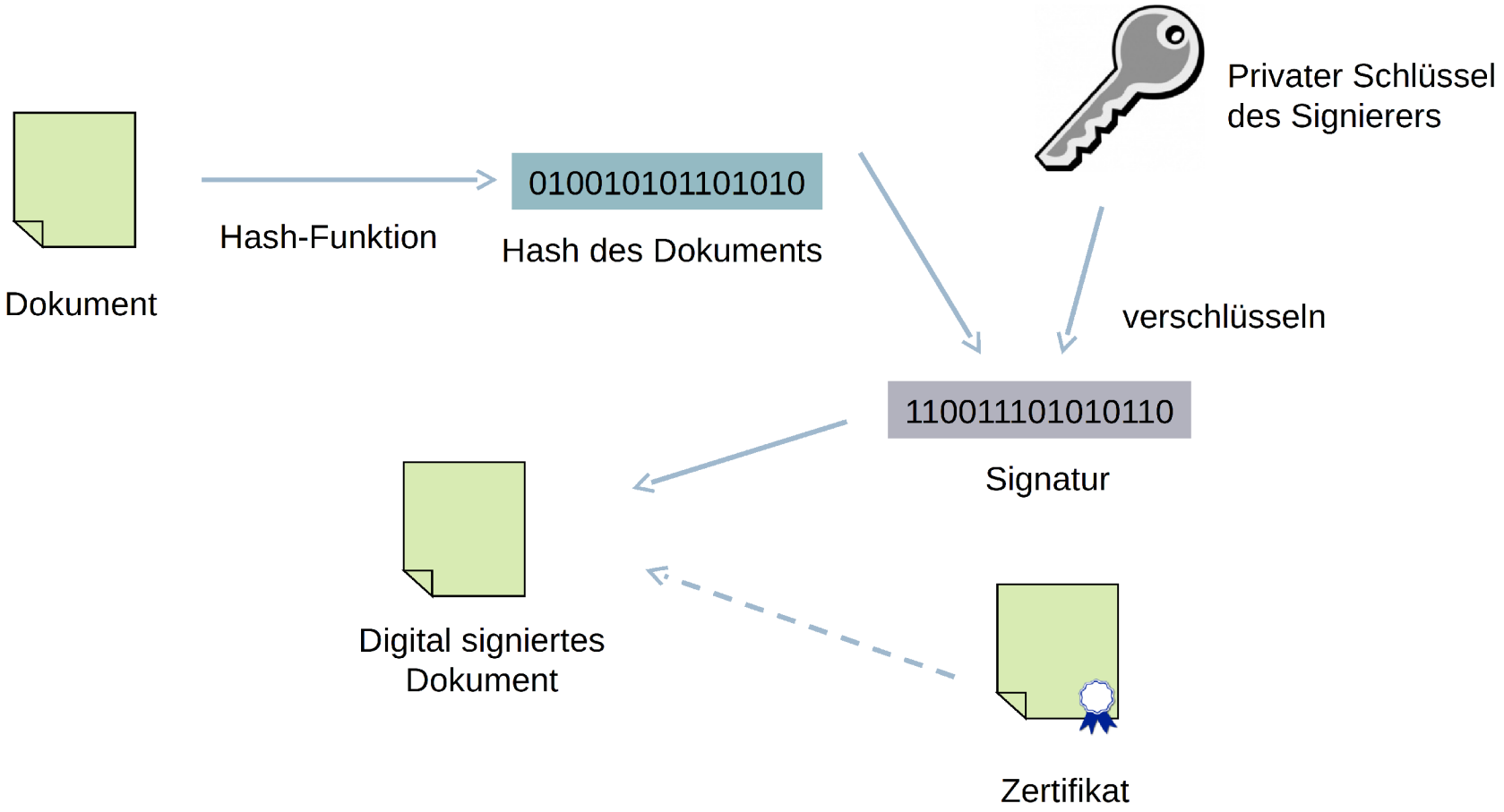
- Schlüsselpaar wird vom Empfänger erzeugt
- Öffentlicher Schlüssel wird an den Sender übertragen



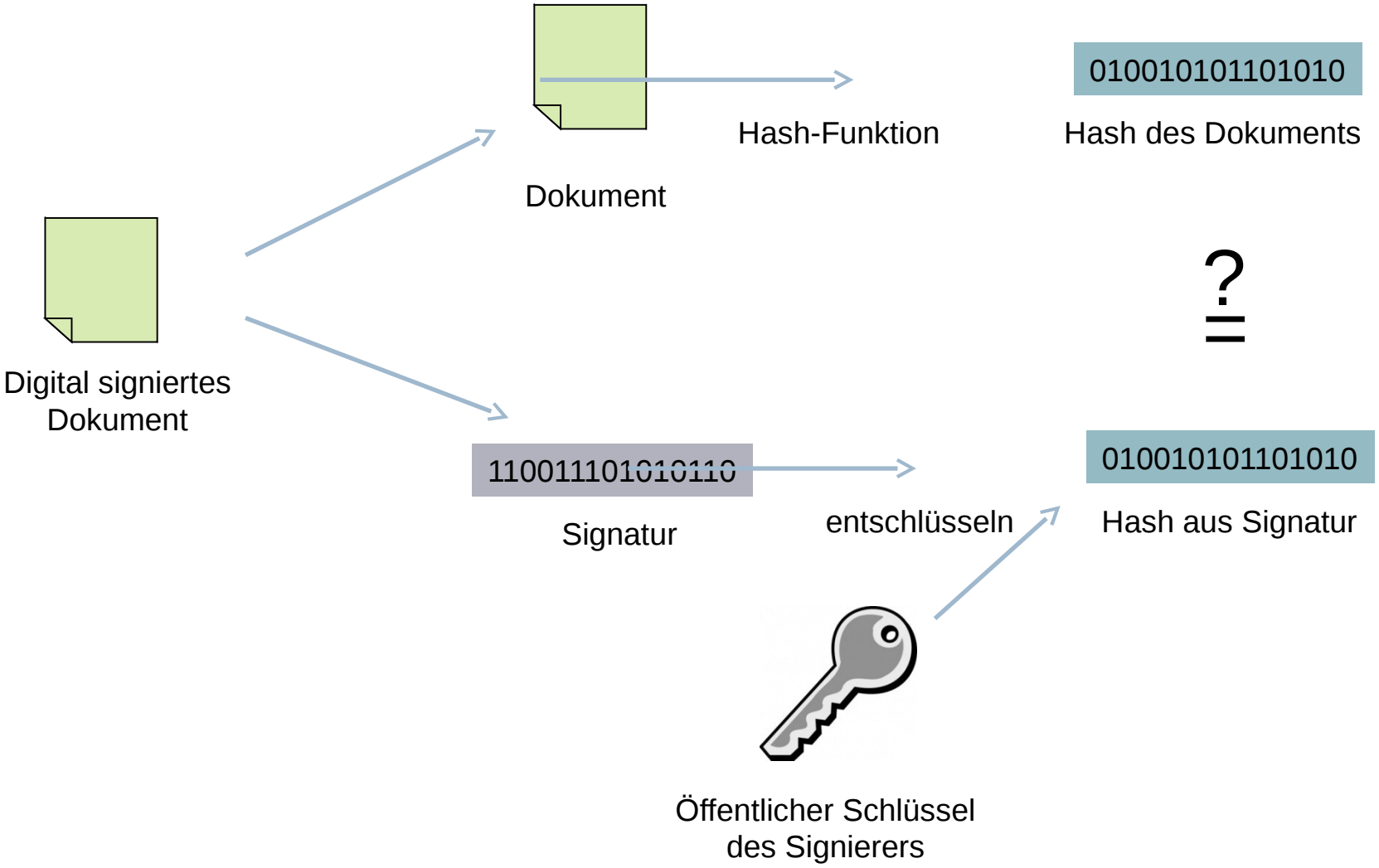
Digitale Signatur

- dient zur Bestimmung der Echtheit eines Dokuments
- Anwendungsbereiche:
  - Geschäftsbereich:
  - Digitale Verträge (E-Commerce)
  - Übermittlung sensibler Daten (z.B. medizinische Daten)
  - Staatlicher Bereich:
  - Online Amtsgänge (neuer Personalausweis)
  - Privater Bereich:
  - E-Mail
- Hashfunktionen zur Komprimierung → schnellere Anwendung

Signieren

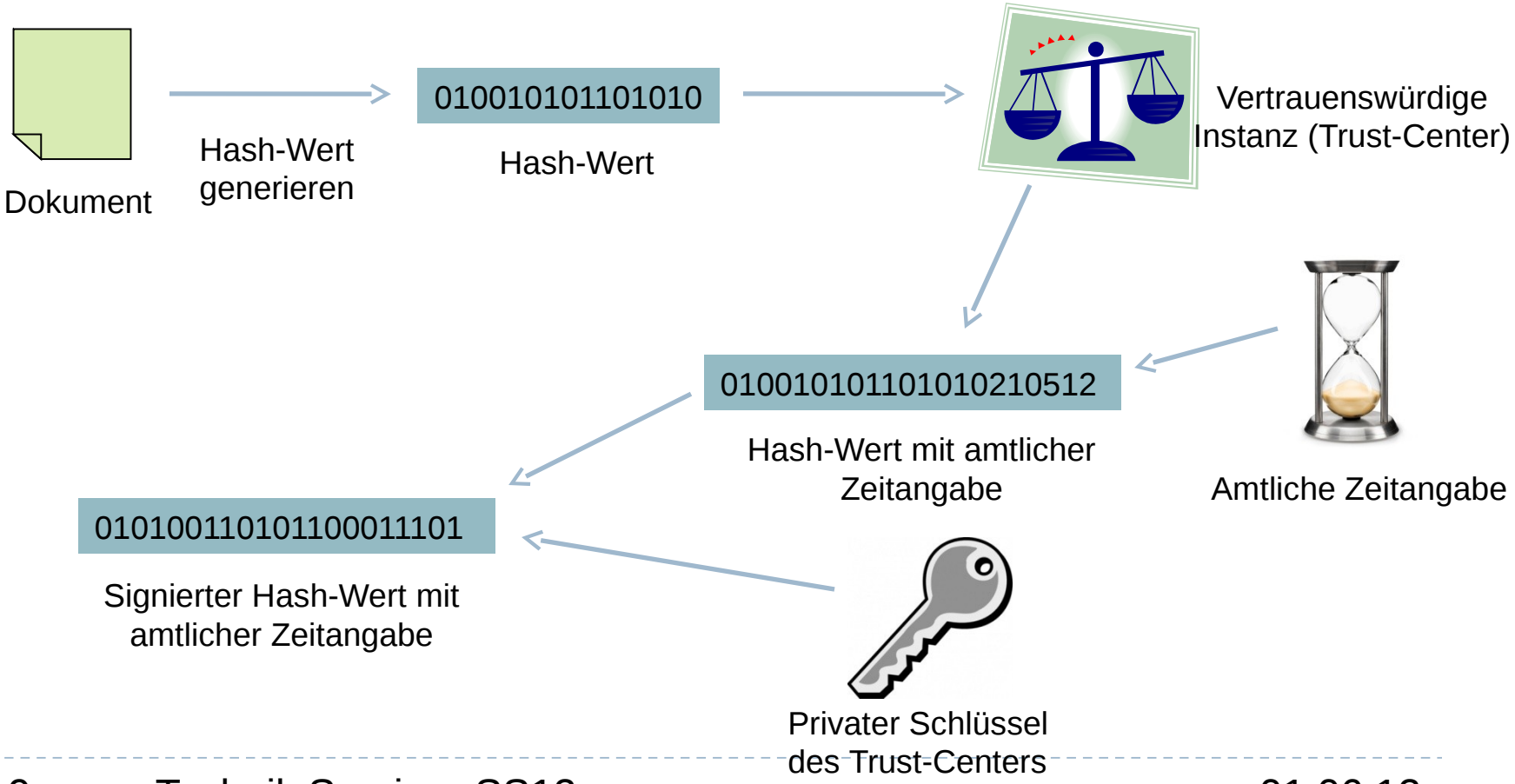

Privater Schlüssel
des Signierers
Dokument
Hash-Funktion
010010101101010
Hash des Dokuments
verschlüsseln
110011101010110
Signatur
Digital signiertes
Dokument
Zertifikat

Überprüfen


Hash-Funktion
010010101101010
Hash des Dokuments
Dokument
?
Digital signiertes Dokument
110011101010110
Signatur
entschlüsseln
010010101101010
Hash aus Signatur
Öffentlicher Schlüssel des Signierers

Zeitstempel

- Mögliches Umdatieren verhindern
- Ablauf:



Zertifikate

- Dienen der Absicherung des Schlüsselaustausches
- „Personalausweis“ in digitaler Form
  - Wird von Trust-Center ausgegeben
- Enthält:
  - Namen des Inhabers, sowie seinen öffentlichen Schlüssel
  - Seriennummer, Gültigkeitsdauer und Namen der Zertifizierungsstelle
- Oberste Zertifizierungsinstanz:
  - Bundesnetzagentur
  - Zertifiziert einzelne Trust-Center

Sicherheit

- Theoretische Sicherheit ist bestimmt durch die Schlüssellänge
- Zum Bewerten der verschiedenen Verfahren gibt es „Security levels“
- „Security Level“ von n bit
  - 2n Rechenschritte mit der best bekannten Attacke erforderlich
  - 80-bit : geringe Sicherheit < 4 Jahre
  - 128-bit : hohe Sicherheit; ca. 30 Jahre
  - 256-bit : In absehbarer Zukunft unbrechbar

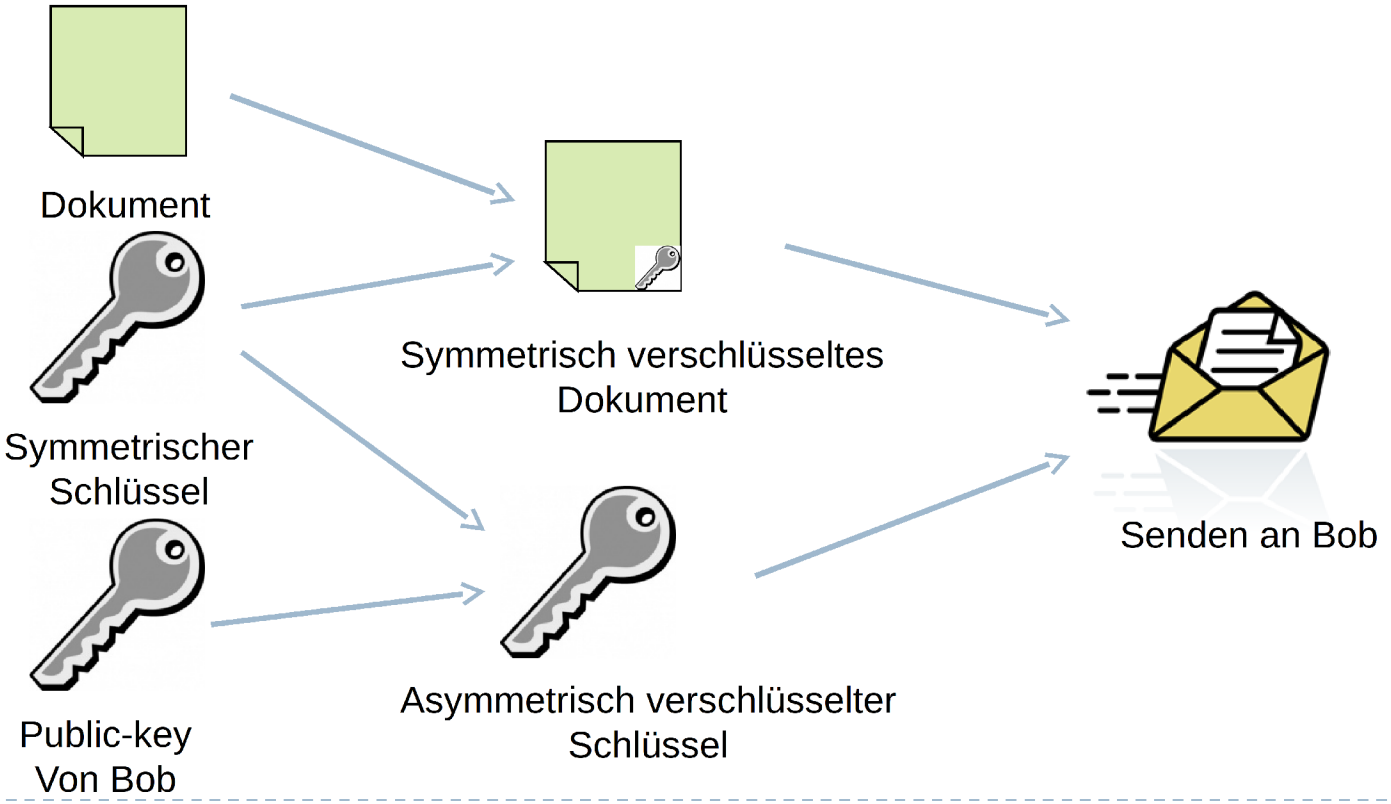
Sicherheit

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

- Problem:
  - Höhere Sicherheit → höherer Rechenaufwand beim Benutzer
  - Beispiel RSA:
  - Erhöhung von 1024 bit auf 3072 bit → 27-fache Dauer bei Ver- und Entschlüsselung

Hybride Verschlüsselung

- Geschwindigkeitsvorteil symmetrischer und Sicherheitsvorteil asymmetrischer Verschlüsselung vereinigt



Vielen Dank