Kryptologie und Datensicherheit
Übersicht

- Definition
- Grundlagen
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Digitale Signatur
- Authentifizierung
- Schlüsselmanagement

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Definition

- **Kryptologie** = Kryptographie + Kryptoanalyse
- **Kryptographie**: Wissenschaft der Entwicklung von Geheimsystemen
- Anwendung: Sicherheit von Kommunikation und Information, Schutz vor Offenlegung und/oder Änderungen
- Prinzip: Verwendung von Geheim-Codes
- **Kryptoanalyse**: Kunst, Geheimsysteme zu brechen

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Anwendungen

- **Verschlüsselung** von:
  - Daten, z.B. auf Speichermedien und
  - Kommunikationswegen, z.B. E-Mail, Telefon, Internet
- **Digitale Signatur**
- **Authentifizierung**
- Verbergen von Informationen und/oder Nachrichten (**Steganographie**)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

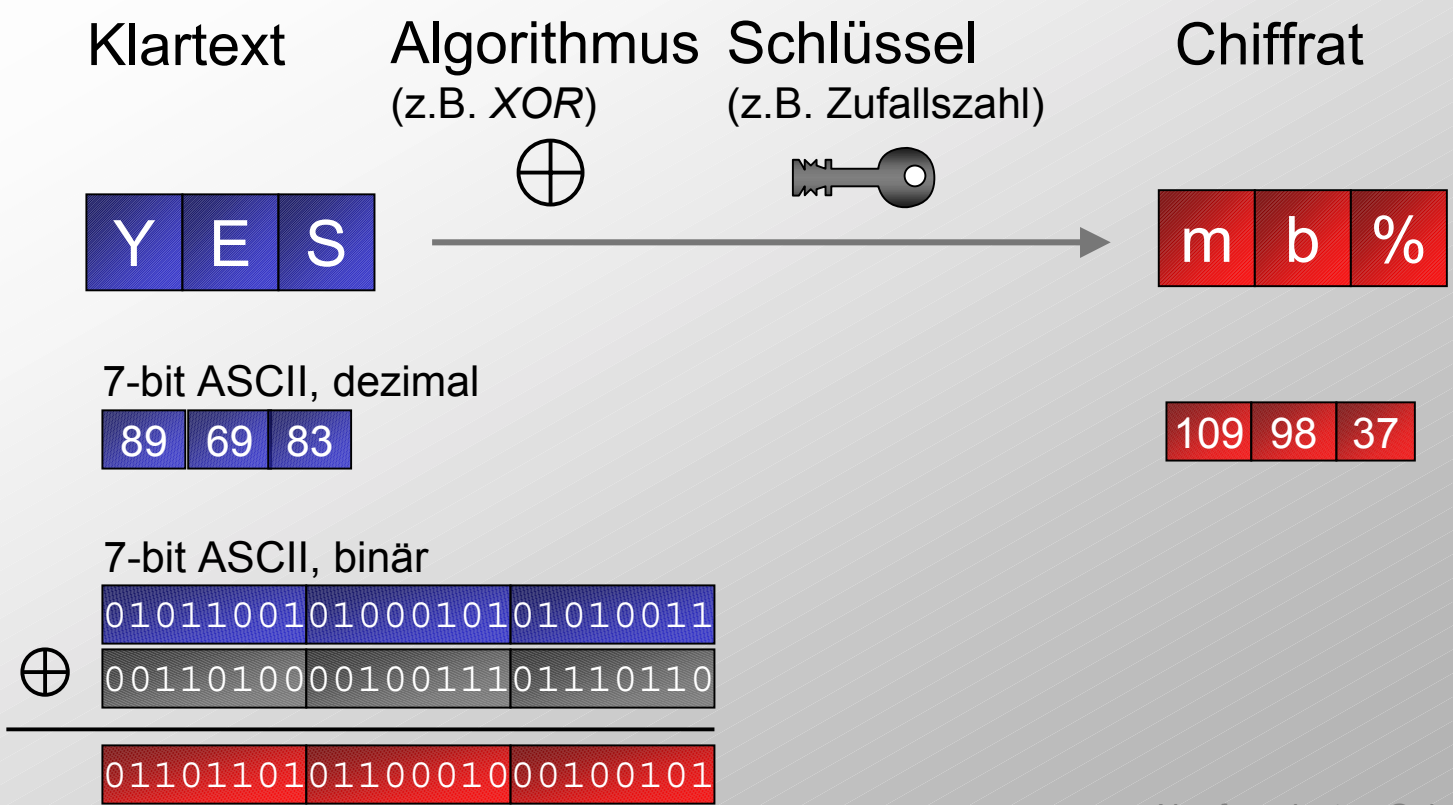
Kryptologie und Datensicherheit
Grundbegriffe

- **Klartext** (engl. *plain text*):
  unverschlüsselter Text
- **Chiffrat** (auch *Chiffretext*, engl. *cipher text*):
  verschlüsselter Text
- **Schlüssel** (engl. *key*):
  Bitfolge bestimmter Länge.
  Verschlüsselung: Klartext wird mit dem Schlüssel über eine mathematische Funktion verknüpft.
- **Verschlüsselungsalgorithmus** (engl. *algorithm*):
  Mathematische Funktion, die die Verknüpfung von Klartext und Schlüssel beschreibt.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Grundbegriffe (Abbildung)



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Historie (1)

600 v.Chr.	Prophet Jeremia, Kap.25, Vers 26	Verschlüsselung des Wortes *Babylon* durch Substitution
500 v.Chr.	Skytala, Sparta	Auf Zylinderrolle aufgewickelter Pergamentstreifen → Transposition der Buchstaben
1940	Enigma	Verschlüsselungsmaschine der Deutschen Wehrmacht im 2.Weltkrieg, basiert auf Substitution

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Historie (2)

1976	Diffie und Hellman	Grundprinzip der asymmetrischen Verschlüsselung
1977	Data Encryption Standard (DES), IBM	Symmetrisches Block-Chiffre-Verfahren
1977	Rivest-Shamir-Adleman (RSA)	Asymmetrisches Verfahren, basiert auf Primzahlzerlegung großer Zahlen
2000	Advanced Encryption Standard (AES), Rijndael	Neuer Standard für symmetrische Verschlüsselungen

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Vier Grundprinzipien der Datensicherheit

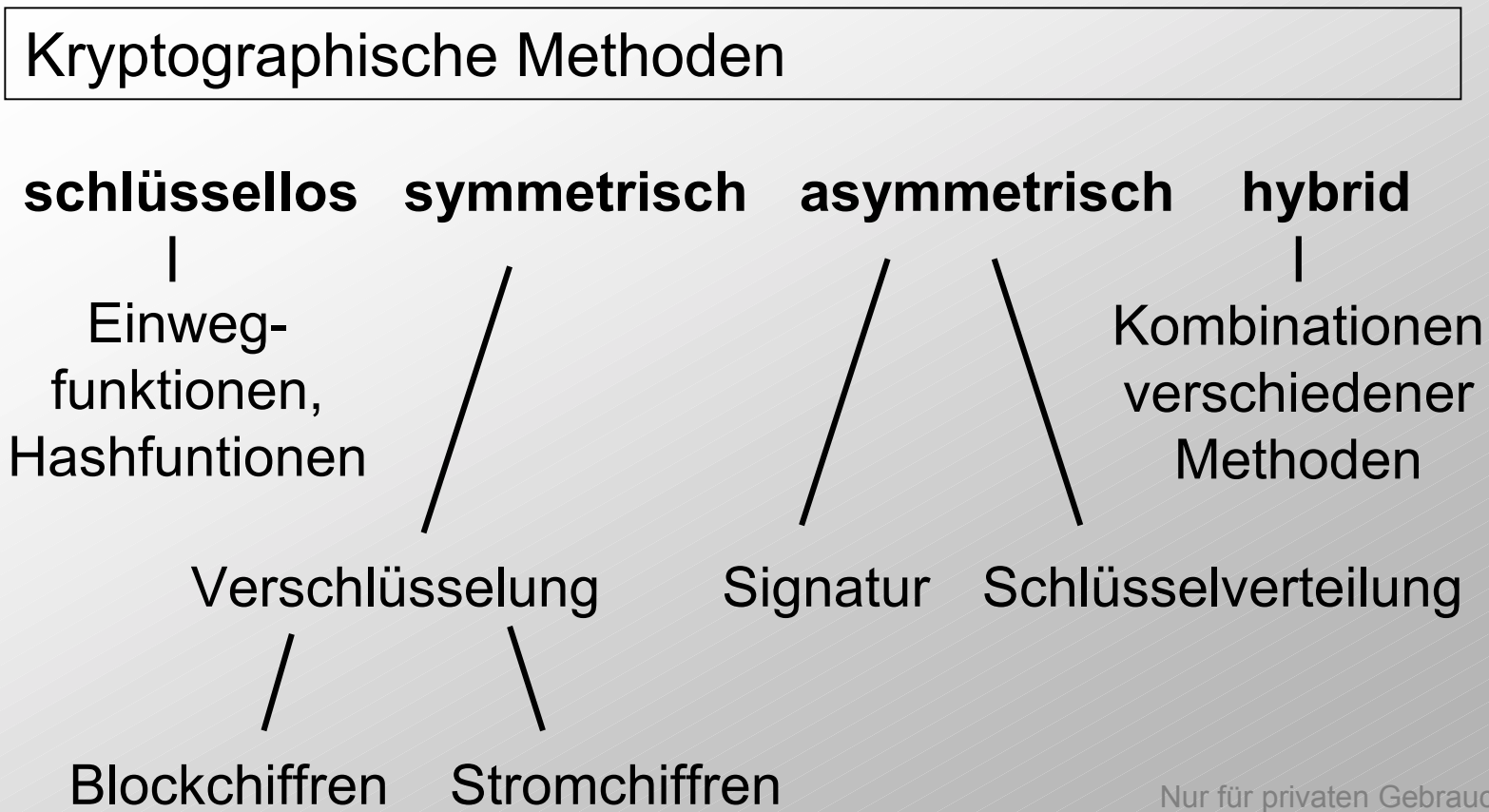
- **Vertraulichkeit**: Unbefugte können Informationen nicht lesen
- **Integrität**: Informationen können nicht unerlaubterweise verändert werden
- **Verbindlichkeit**: Senden/Empfang kann nicht abgestritten werden
- **Verfügbarkeit**: Daten werden zuverlässig transportiert und sind verfügbar

→ Kryptographische Methoden implementieren die Prinzipien 1 - 3

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Kryptographische Methoden: Klassen



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Kryptographische Methoden: Bewertungskriterien

- Grad der erreichbaren Sicherheit
- Eignung für bestimmte Anwendungen
- Implementierungsaufwand
- Datendurchsatz

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

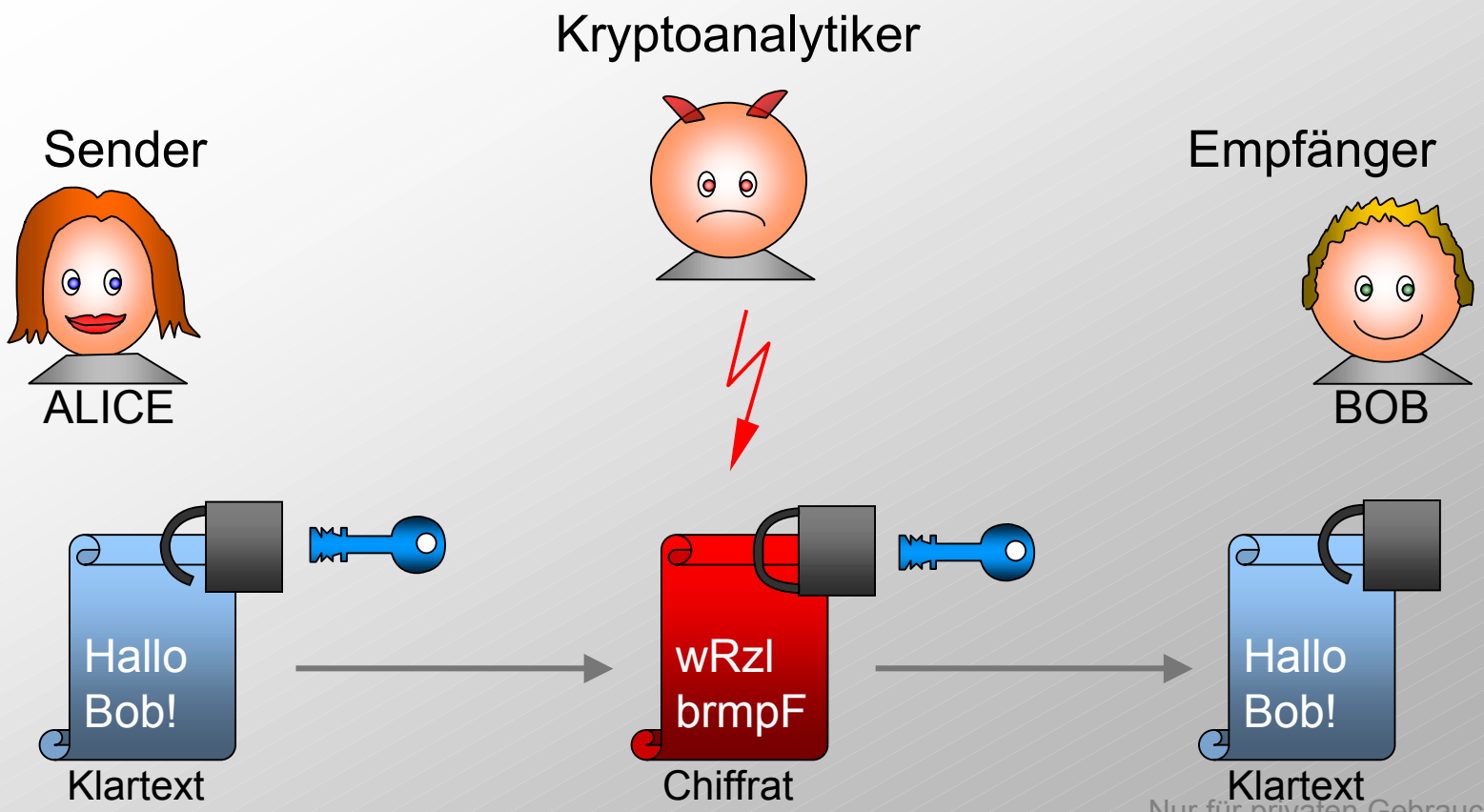
Kryptologie und Datensicherheit
Kryptoanalyse: Angriffsarten

- Reiner Chiffretextangriff (engl. *known ciphertext attack*):
  - Angreifer kennt nur den Chiffretext
- Angriff mit bekanntem Klartext (engl. *known plaintext attack*):
  - Angreifer kennt Chiffretext und dazu gehörigen Klartext
- Angriff mit frei wählbarem Klartext (engl. *chosen plaintext attack*):
  - Angreifer kann beliebigen Klartext verschlüsseln lassen

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Kryptographischer Kanal



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Kerckhoff‘ sches Prinzip

- Auguste Kerckhoff, 1883
- Sicherheit eines kryptographischen Verfahrens darf abhängen von ...

Geheimhaltung des Verschlüsselungs-Algorithmus:	→ NEIN
Geheimhaltung des Verschlüsselungs-Schlüssels:	→ JA

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Perfektes Verschlüsselungssystem

- Perfektes Verschlüsselungssystem:

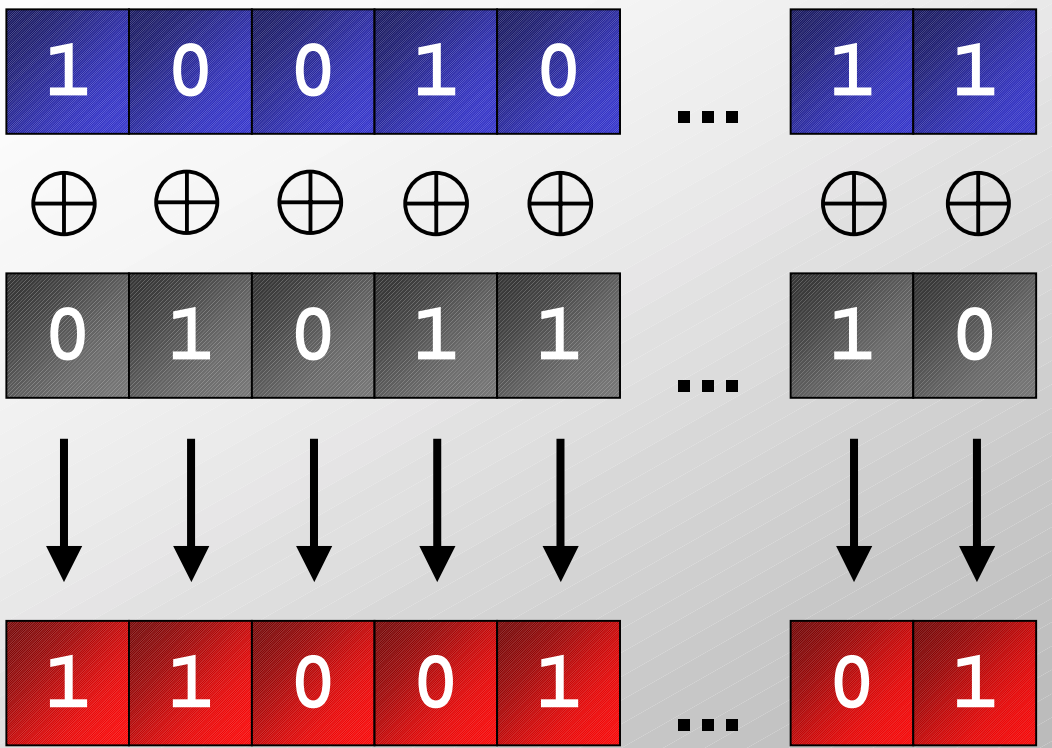
  Kenntnis des Chiffretextes gibt dem Kryptoanalytiker keine zusätzliche Information über den Klartext

- Realisierung:
  Vernamchiffre (auch *one-time-pad*):
  Klartext und Schlüssel werden bitweise mit *XOR* verknüpft.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
One-time-pad (Beispiel), vgl. Stromchiffre



Klartext
Länge *m*

Algorithmus
XOR

Schlüssel
Zufallszahl, Länge *m*

Chiffrat
Länge *m*

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung (1)

- Engl. *private-key cryptography*, *single-key cryptography*
- Gleicher (oder leicht voneinander ableitbare) Schlüssel für Verschlüsselung und Entschlüsselung
- Sender und Empfänger haben jeweils eine Kopie des Schlüssels
- Schlüssel muss geheim gehalten werden (daher die Bezeichnung *privater Schlüssel*)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung (2)

- Algorithmen basieren auf Kombination und Iteration relativ einfacher Verfahrensschritte.
- Schritte werden in *Runden* (engl. *rounds*) wiederholt.
- Operationen für Ver- und Entschlüsselung sind symmetrisch.
- Schlüsselverteilungsproblem:
  Vor der Nachrichtenübermittlung muss der Schlüssel über einen sicheren Kanal übermittelt werden.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung (3)

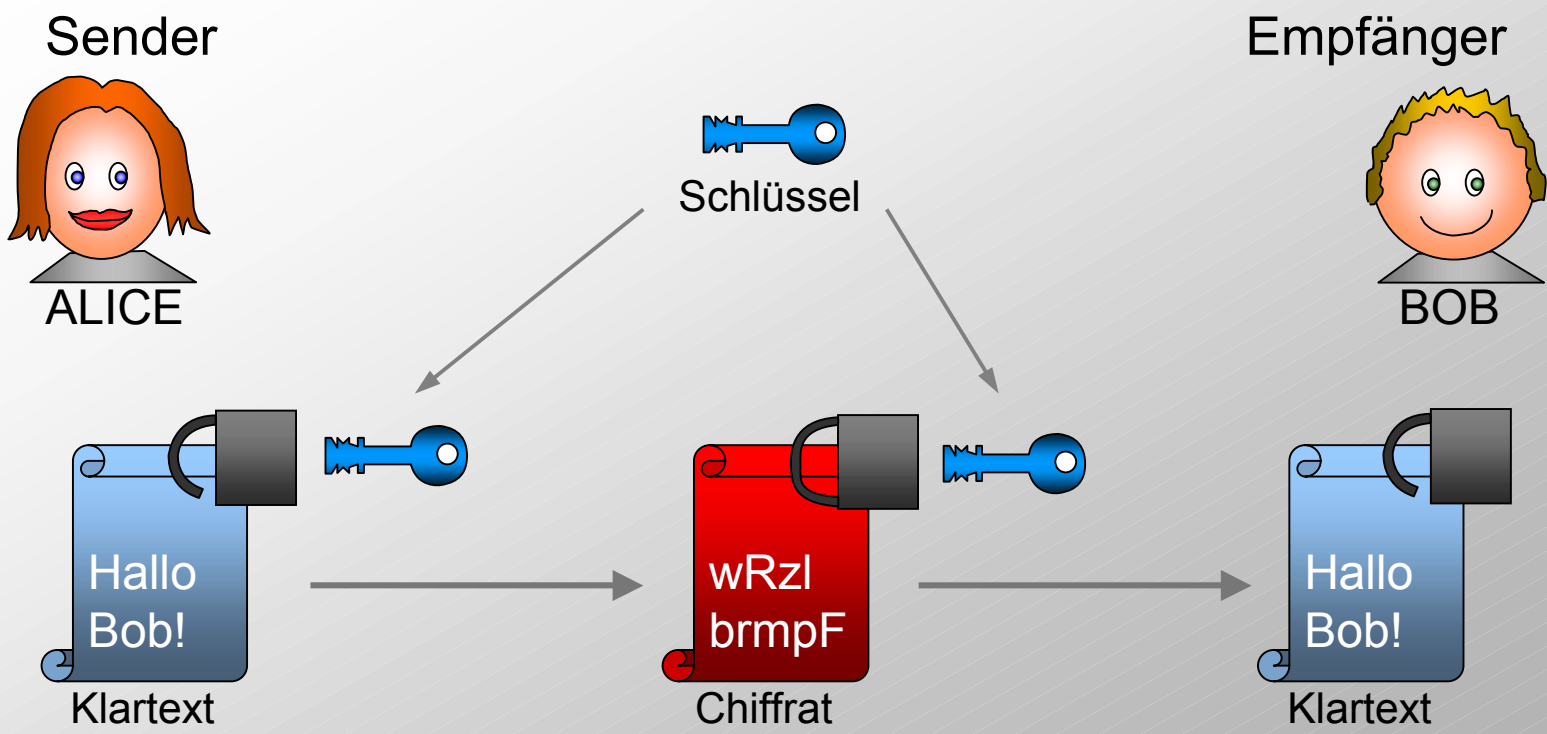
- **Beispiele** für symmetrische Algorithmen:
  - Advanced Encryption Standard (*AES*)
  - Data Encryption Standard (*DES*, *Triple-DES*)
  - International Data Encryption Algorithm (*IDEA*)
  - Ron‘s Codes (*RC2*, *RC4*, *RC5, RC6*)

- **Anwendung**:
  - Vertraulichkeits- und Integritätsschutz (Unbefugte können Informationen weder lesen noch verändern.)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung (Abbildung)



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung (Ablauf)

Alice und Bob haben einen gemeinsamen geheimen Verschlüsselungs-Schlüssel.

1) Alice verschlüsselt die Nachricht mit diesem Schlüssel.
2) Die Nachricht wird verschlüsselt von Alice zu Bob übertragen.
3) Bob entschlüsselt die Nachricht mit dem selben Schlüssel.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Grundlegende symmetrische Methoden

- **Substitution** (engl. *substitution cipher*): Ersetzung von Klartextzeichen durch Zeichen aus dem Geheimalphabet
- **Transposition** (engl. *transposition cipher*): Vertauschung von Zeichenpositionen im Klartext
- **Produktverschlüsselung** (engl. *product cipher*): Kombination aus Substitution und Transposition

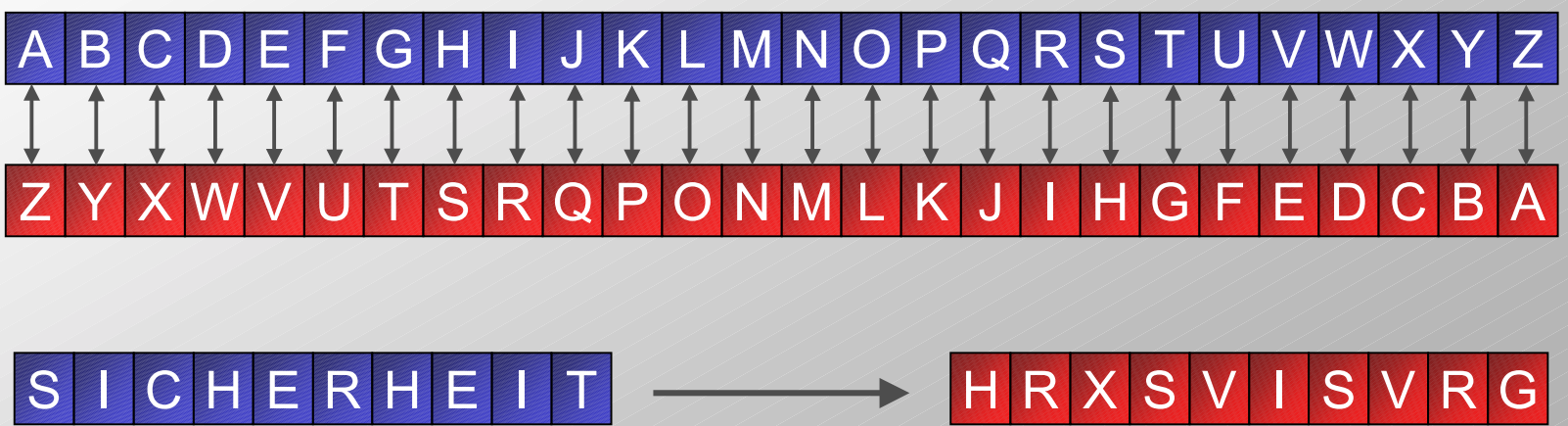
Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Substitution

Beispiel:

Buchstabe im Alphabet an n-ter Stelle wird durch denjenigen ersetzt, der rückwärts gezählt an n-ter Stelle steht.



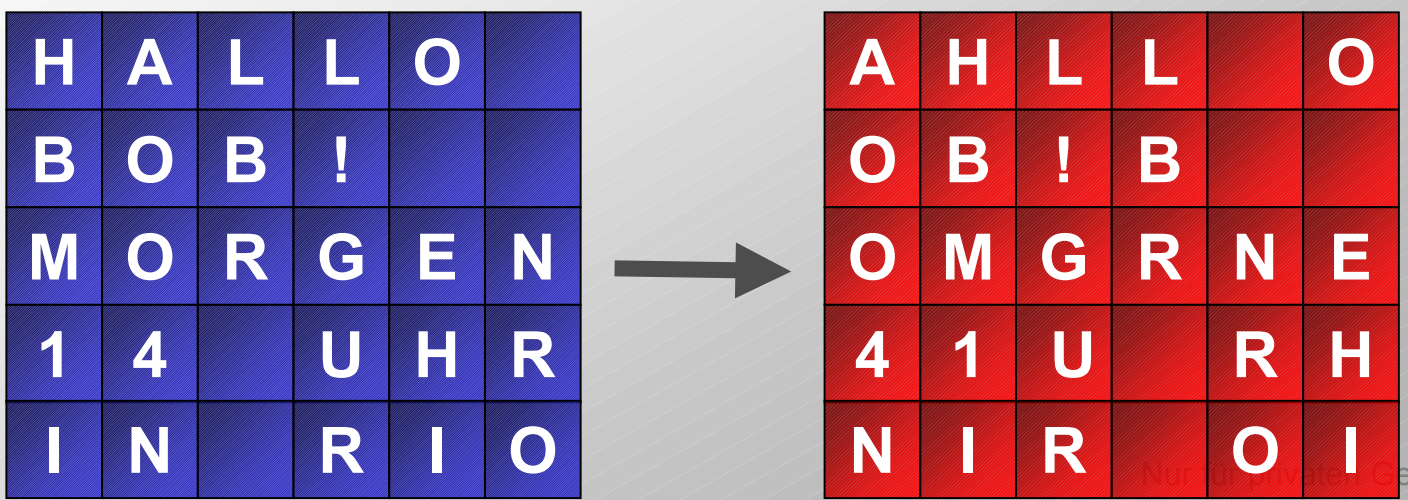
Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Transposition

Beispiel:

Spaltentransposition: Vertauschen von Spalten gerader Spaltennummer mit Spalten ungerader Spaltennummer.



Nur für private Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Diffusion und Konfusion

- Begriffe aus der **Informationstheorie** (Claude Shannon)
- **Diffusion**: Veränderung der in einem Klartext erhaltenen Redundanzen (z.B. Häufigkeiten von Buchstaben und Buchstabenfolgen).
- **Konfusion**: Verschleierung der Zusammenhänge zwischen Klartext, Geheimtext und Schlüssel.
- Moderne symmetrische Verschlüsselungs-verfahren berücksichtigen Diffusion und Konfusion.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung: Implementierung

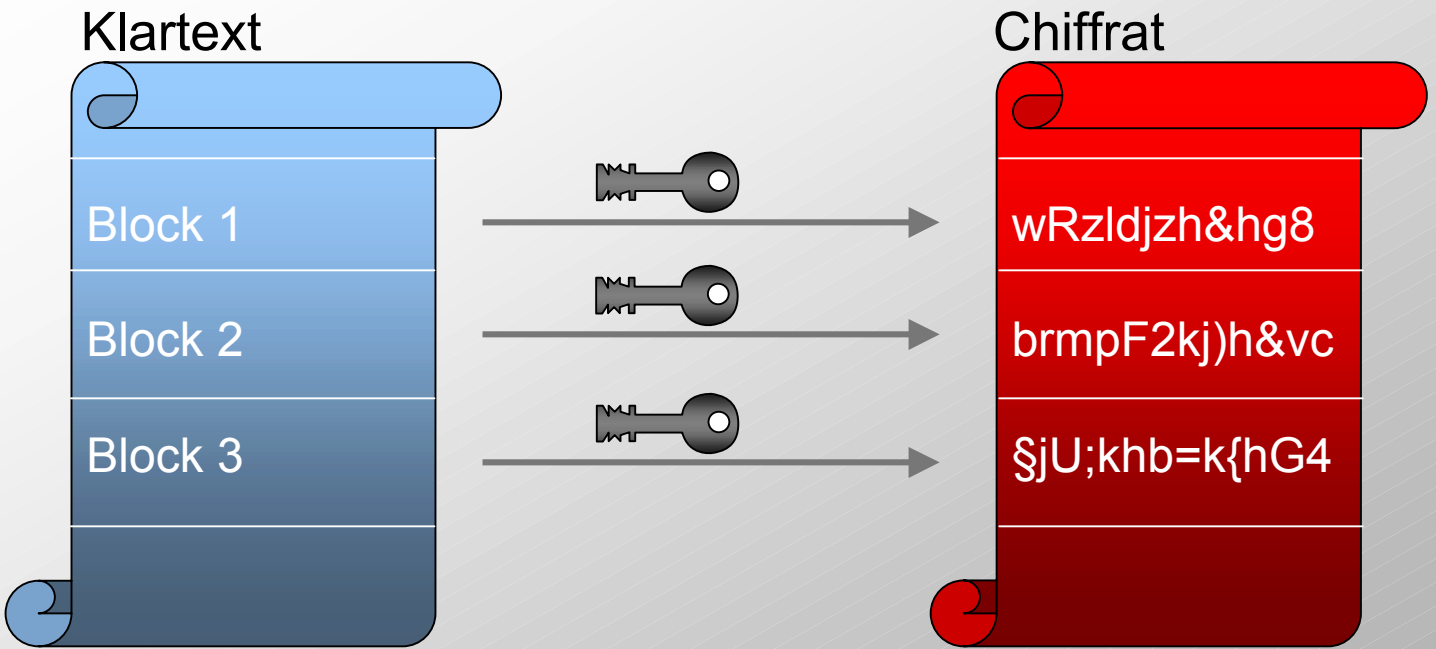
Implementierungsarten:

- **Blockchiffre**: Klartext wird in Abschnitte fester Länge zerlegt, die separat verschlüsselt werden (Beispiele: *AES*, *DES*, *IDEA*, *RC2*).
- **Stromchiffre**: Klartextzeichen werden sequenziell (einzeln) mit Schlüsselstrom verknüpt (Beispiel: *XOR*-Verknüpfung mit *one-time pad*).

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

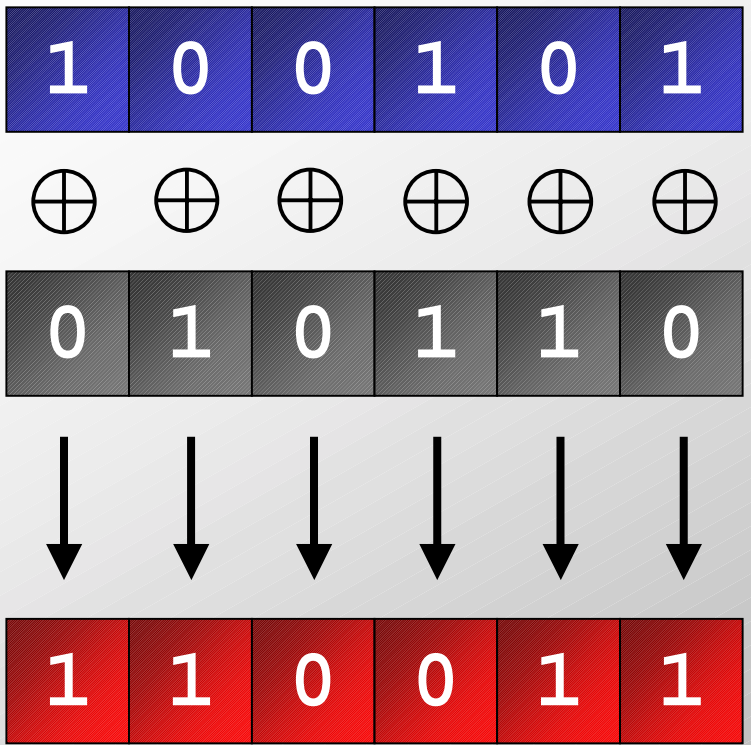
Kryptologie und Datensicherheit
Blockchiffre



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Stromchiffre (Beispiel)



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Symmetrische Verschlüsselung: Vorteile/Nachteile

- \+ Einfache Verfahrensschritte
  → gute Implementierbarkeit
- \+ Hoher Datendurchsatz, kurze Schlüssellänge
- \+ Praxiserprobt und bewährt
- − Schlüsselverteilung erfordert sicheren Kanal
- − Erfordert Geheimhaltung bei Sender und Empfänger
- − Kein Verbindlichkeitsschutz
  → digitale Signatur schwer realisierbar
- − Eigener Schlüssel pro Sender-/Empfänger-Paar
  → aufwendige Schlüsselverwaltung

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Asymmetrische Verschlüsselung (1)

- Engl. *public-key cryptography*
- Verschiedene (oder nicht leicht voneinander ableitbare) Schlüssel für Verschlüsselung und Entschlüsselung
- Privater Schlüssel (engl. *private key*) muss geheim bleiben
- Öffentlicher Schlüssel (engl. *public key*) kann veröffentlicht werden
- Bezeichnung *asymetrisch* wegen verschiedener Schlüssel

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

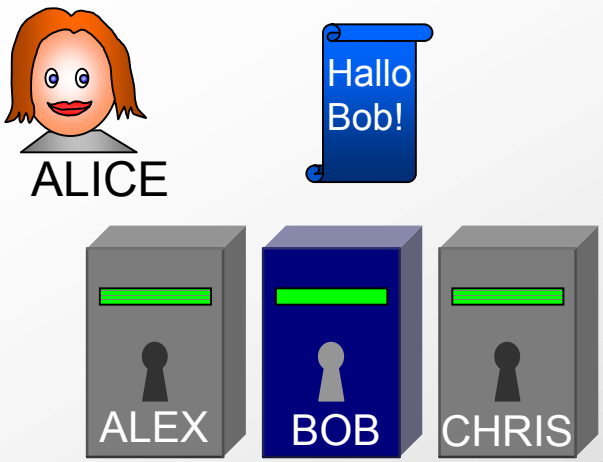
Kryptologie und Datensicherheit
Asymmetrische Verschlüsselung (2)

- Implementierung:
  - Es werden *Einweg-Hashfunktionen* verwendet.
- Beispiele:
  - *RSA* (Rivest-Shamir-Adleman)
  - diskreter Logarithmus (*ElGamal*, *Diffie-Hellman-Schlüsselaustausch*, *Elliptische Kurven*)
- Anwendung:
  - digitale Signatur (Integrität und Verbindlichkeit)
  - Übertragung von verschlüsselten Schlüsseln

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Briefkastenvergleich



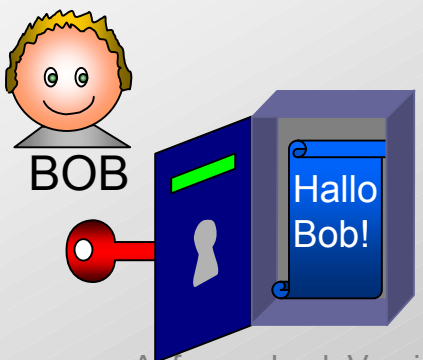
Verschlüsseln

Brief in Bobs Briefkasten einwerfen

Nachricht mit Bobs öffentlichem Schlüssel verschlüsseln

Briefkasten ist frei zugänglich
→ jeder kann einen Brief einwerfen

Öffentliche Schlüssel sind frei zugänglich
→ jeder kann Bob eine verschlüsselte Nachricht senden



Entschlüsseln

Briefkasten öffnen

Nachricht mit Bobs privatem Schlüssel entschlüsseln

Nur Bob hat den Schlüssel

Nur Bob kennt seinen privaten Schlüssel

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Mathematische Basisfunktionen

- Wichtige mathematische Funktionen für asymmetrische Verschlüsselung:
  - Hashfunktion,
  - Einwegfunktion
  - Einweg-Hashfunktion
  - Einwegfunktion mit Falltür

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

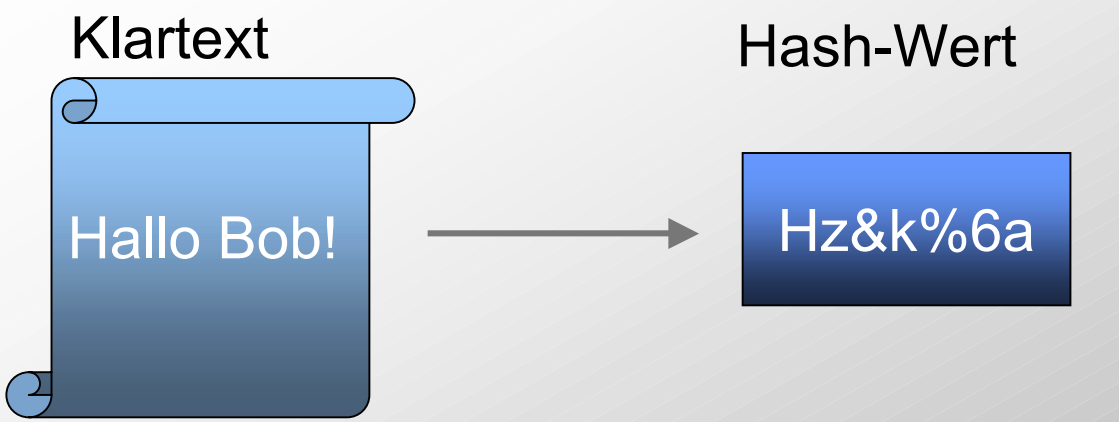
Kryptologie und Datensicherheit
Hashfunktion

- Engl. *hash function*
- Komprimiert Informationen
- Eingabewerte variabler Länge → Ausgabewerte fester Länge
- Schlüssellos
- Muss *kollisionsfrei* sein (d.h. es gibt keine zwei verschiedene Nachrichten mit gleichem Hash-Wert)
- Anwendung: digitale Signatur, Softwarelizenzierung
- Beispiele: *RDS*, *SHA*

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Hashfunktion (Abbildung)



M
mit beliebiger Länge

h(M)
mit fester Länge m

Es gibt kein Paar verschiedener Klartexte *M* und *M‘* ,
für das gilt: *h(M) = h(M‘)*

Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Einwegfunktion

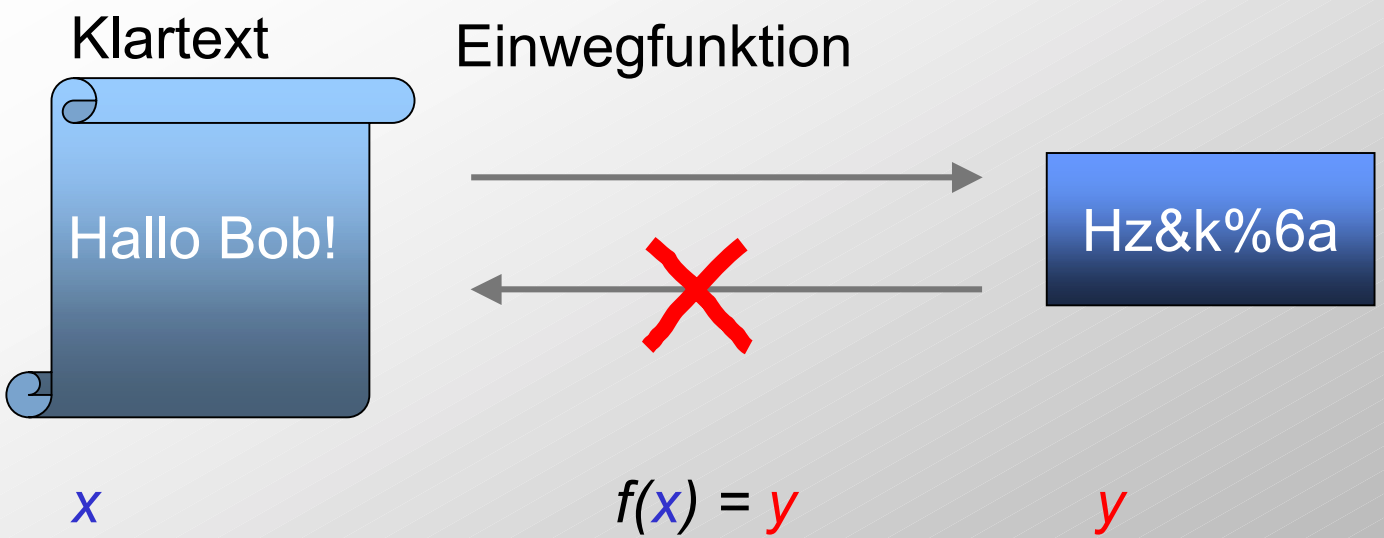
- Engl. *one-way function*
- Abbildung, deren Umkehrfunktion praktisch nicht berechenbar ist
- $f(x) = y$

  → Aus y darf x nicht berechenbar sein.
- Anwendung: z.B. sichere Speicherung von Passwörtern
- Einwegfunktion mit Falltür (engl. *trapdoor one-way function*):
  → Es gibt einen Schlüssel für die Umkehrfunktion.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Einwegfunktion (Abbildung)



Die Umkehrfunktion $f'(y) = x$ ist nicht berechenbar.

Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Einweg-Hashfunktion

- Engl. *one-way hash function*
- Kombination aus Einwegfunktion und Hashfunktion

- Vergleich: Anonyme Abstimmung
  - Abstimmungsergebnis (*1 JA* / *3 NEIN*) ist eine komprimierte Form von Einzelmeinungen (*unmöglich*, *super*, *zu teuer*, *schlecht*)
  - Aus dem Ergebnis können die Einzelmeinungen nicht rekonstruiert werden.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Integritätsmechanismen (1)

- Anwendung der mathematischen Basisfunktionen zur Integritätsprüfung

- Prinzip:
  kryptographische Prüfsumme wird berechnet (Sender) und verifiziert (Empfänger)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Integritätsmechanismen (2)

Sender:

- Nachricht wird um eine redundate Information (Prüfsumme, *Message Authentication Code*) erweitert.
- Prüfsumme wird mittels eines kryptographischen Verfahrens aus der Nachricht berechnet.
- Prüfsumme wird zusammen mit der Nachricht übertragen.

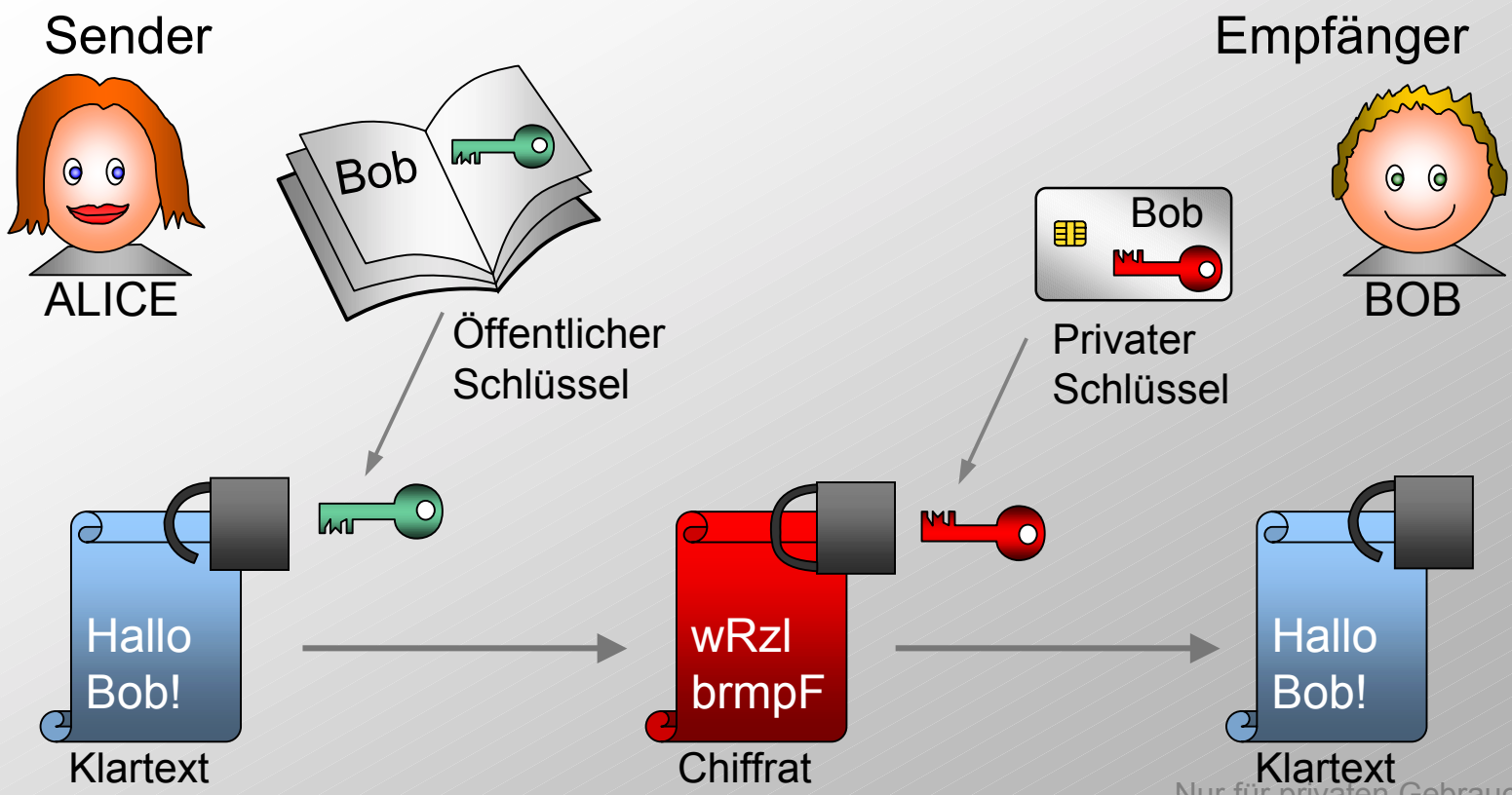
Empfänger:

- Prüfsumme wird berechnet und mit der übertragenen Prüfsumme verglichen.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Asymmetrische Verschlüsselung (Abbildung)



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Asymmetrische Verschlüsselung (Ablauf)

1) Alice entnimmt Bobs öffentlichen Schlüssel aus einem frei zugänglichen Verzeichnis.
2) Alice verschlüsselt die Nachricht mit Bobs öffentlichem Schlüssel.
3) Die Nachricht wird verschlüsselt übertragen.
4) Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel (dieser Schlüssel kann z.B. auf einer Chipkarte stehen).

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Asymmetrische Verschlüsselung: Vorteile/Nachteile

- \+ Hoher Sicherheitsgrad
- \+ Gut geeignet für digitale Signatur
- \+ Einfache Schlüsselverwaltung
- − Große Schlüssellängen erforderlich
- − Geringer Datendurchsatz bei Ver-/Entschlüsselung (durchschnittlich um den Faktor 1000 langsamer als symmetrische Verschlüsselung)
- − Wissenschaftliche Erforschung noch nicht abgeschlossen → Sicherheit ist noch nicht beweisbar
- − Einschränkung freier Verwendbarkeit durch Patente

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

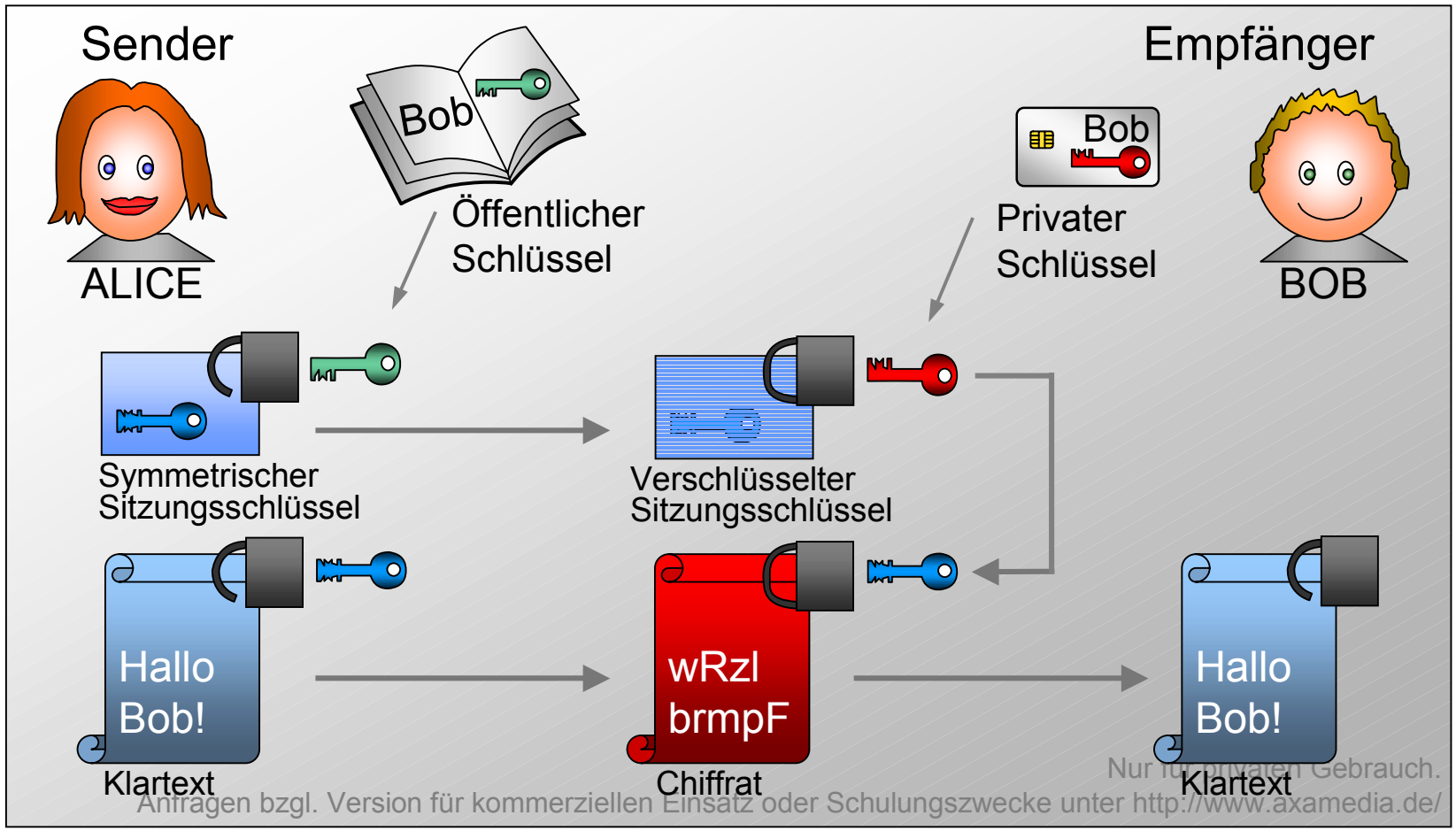
Kryptologie und Datensicherheit
Hybride Verschlüsselung

- Kombination symmetrische/asymmetrische Verschlüsselung
- Nachricht wird mit einem schnellen symmetrischen Algorithmus (z.B. *DES*) verschlüsselt:
  → hoher Datendurchsatz
- Schlüsselverteilung und gegenseitige Authentifizierung laufen asymmetrisch ab:
  → Schlüssel wird durch asymmetrisches Verschlüsselungs-Verfahren vom Sender zum Empfänger übertragen.
- Beispiel: Pretty Good Privacy (*PGP*)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Hybride Verschlüsselung (Abbildung)



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Hybride Verschlüsselung (Ablauf)

1) Alice entnimmt Bobs öffentlichen Schlüssel aus einem frei zugänglichen Verzeichnis.
2) Alice erzeugt einen Sitzungsschlüssel und verschlüsselt diesen mit Bobs öffentlichem Schlüssel.
3) Alice verschlüsselt die Nachricht mit dem Sitzungsschlüssel.
4) Der Sitzungsschlüssel wird zusammen mit der Nachricht verschlüsselt übertragen.
5) Bob entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel.
6) Bob entschlüsselt die Nachricht mit dem Sitzungsschlüssel.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Digitale Signatur (1)

- **Hash-Wert** der Nachricht, verschlüsselt mit dem privaten Schlüssels des Senders

- Eigenschaften:
  - **Integrität** (Nachricht wurde nicht verändert)
  - **Authentizität** (Identität des Absenders ist sichergestellt)
  - **Verbindlichkeit** (das Absenden ist nicht abstreitbar)

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

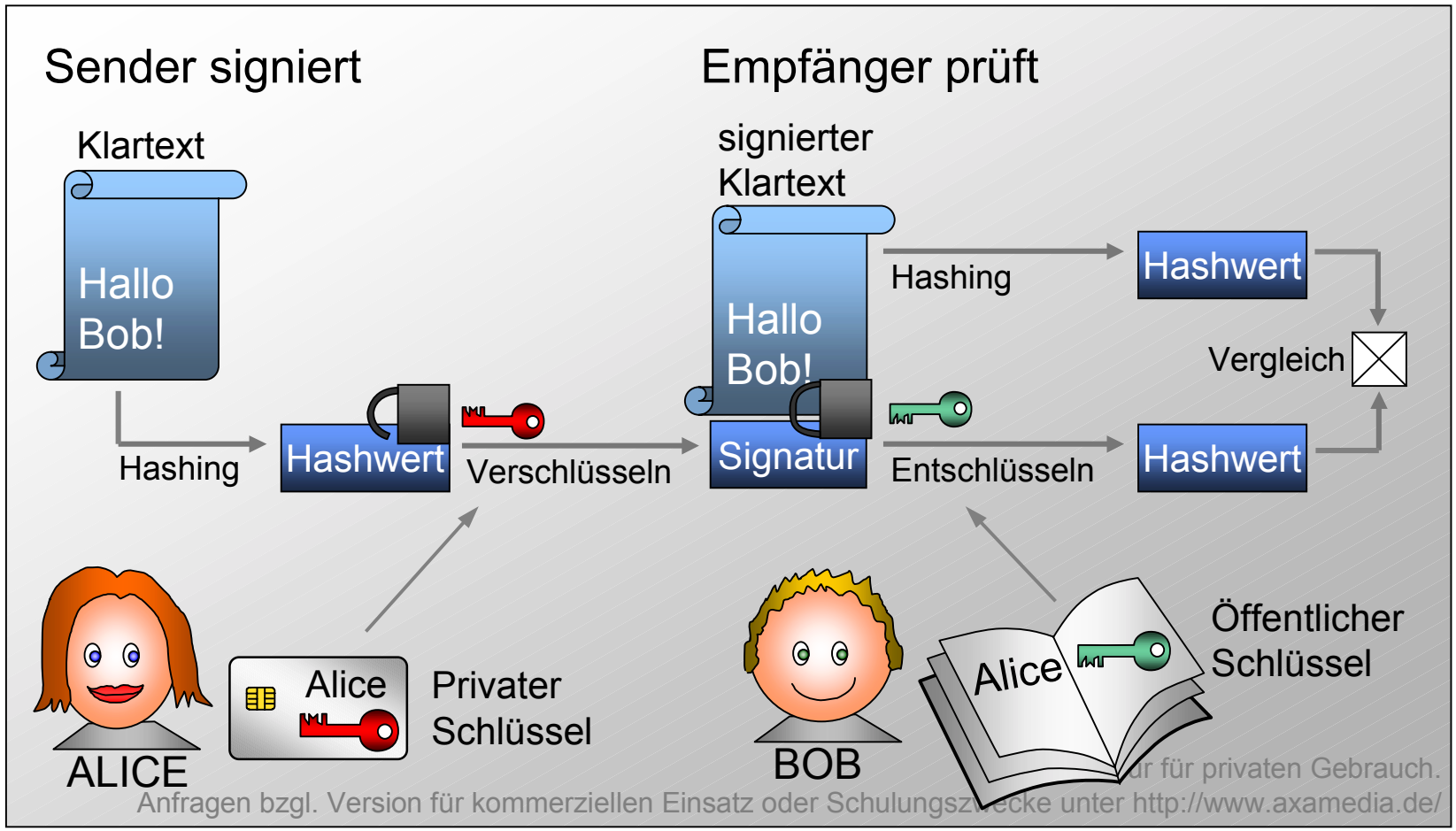
Kryptologie und Datensicherheit
Digitale Signatur (2)

- Signatur wird als **Annotation** (auch engl. *tag*) zur Nachricht gesendet.
- Signatur enthält verschlüsselte Aussagen zu Autor, Inhalt und Datum.
- Asymmetrische Verschlüsselung der kompletten Nachricht ist zu aufwendig:
  → Nur ein Hash-Wert der Nachricht wird verschlüsselt („signiert“).

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Digitale Signatur (Abbildung)



ur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Digitale Signatur (Ablauf) (1)

1) Absender erzeugt mit einem bekannten Verfahren einen **Hash-Wert** aus der Nachricht.
2) Absender verschlüsselt Hash-Wert mit seinem privaten Schlüssel (verschlüsselter Hash-Wert entspricht digitaler Signatur).
3) Empfänger entschlüsselt die Signatur mit dem öffentlichen Schlüssel des Absenders.
4) Empfänger erzeugt mit dem gleichen Verfahren wie der Absender einen Hash-Wert der (unverschlüsselten) Nachricht.
5) Empfänger vergleicht die beiden Hash-Werte.

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Digitale Signatur (Ablauf) (2)

Übereinstimmung der Hash-Werte?

→ Richtiger Absender

→ Nicht nachträglich manipulierte Nachricht

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

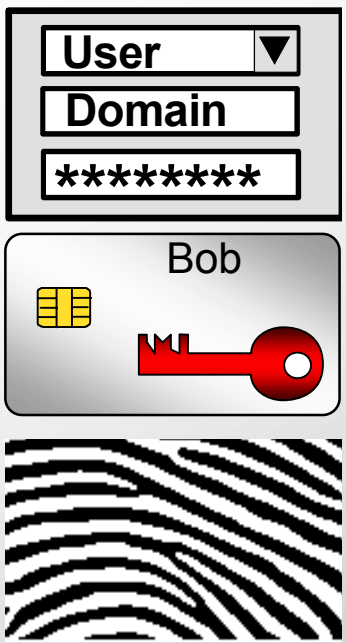
Kryptologie und Datensicherheit
Authentifizierung

- Auch *Authentifikation*
- Definition: Betätigung der **Identität** einer Person
- Authentifizierungsmethoden:
  Wissen – **Besitz** – **Merkmale**
- Statische Authentifizierung: es wird immer der gleiche Authentifizierungs-Code verwendet:
  → Gefahr von *Replay*-Angriff
- Dynamische Authentifizierung: Authentifizierungs-Code hat eine veränderliche Komponente (*number used only once*, z.B. Zufallszahl, Zeitstempel).

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Authentifizierung: Wissen – Besitz - Merkmale



Methode	Beispiel
Wissen („What you know“)	Passwort
Besitz („What you have“)	Chipkarte
Merkmale („What you are“)	Fingerabdruck

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Schlüsselmanagement

- Bereitstellung von Schlüsseln für kryptographische Methoden:

  - Schlüsselerzeugung
  - Schlüsselverteilung
  - Schlüsselspeicherung
  - Schlüsselzerstörung

- Übertragung über kryptographisch gesicherten Kanal

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Public Key Infrastruktur (PKI)

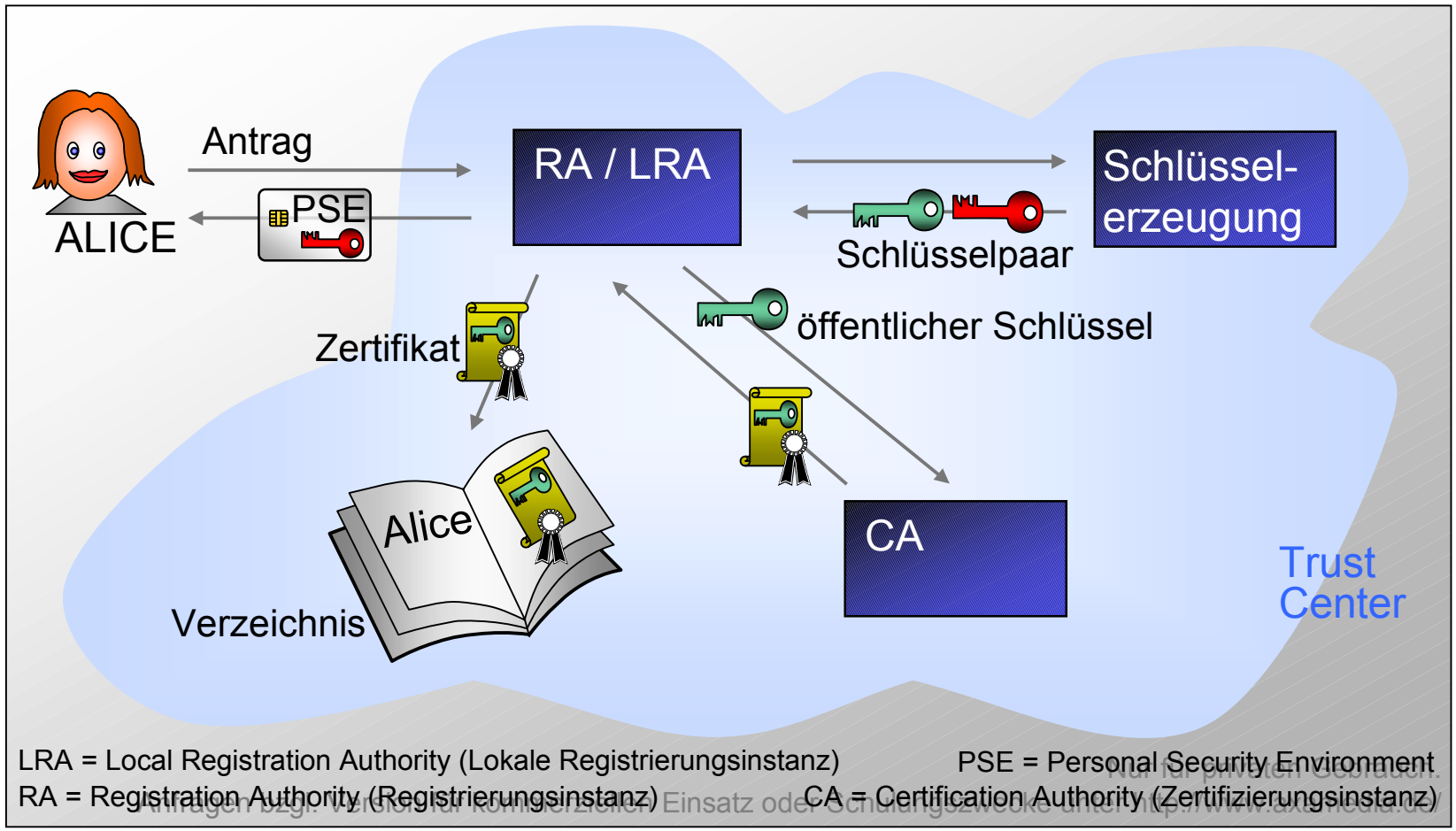
- PKI:
  Gesamtheit der für den Einsatz asymmetrischer Kryptographie in offenen Systemen nötigen Instanzen

- Aufgaben:
  - Nutzer-Registrierung
  - Ausstellen, Verwalten und Prüfen von Zertifikaten

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Public Key Infrastruktur (Abbildung)



LRA = Local Registration Authority (Lokale Registrierungsinstanz)
RA = Registration Authority (Registrierungsinstanz)
PSE = Personal Security Environment
CA = Certification Authority (Zertifizierungsinstanz)

Nur für privaten Gebrauch. Anfragen bzgl. Verleih für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Public Key Infrastruktur: Zertifikat-Erstellung

1) Benutzer stellt einen Antrag auf ein Zertifikat.
2) Registrierungsinstanz bzw. lokale Registrierungsinstanz (*RA*/*LRA*) steuert die Erzeugung eines Schlüsselpaares (privater/öffentlicher Schlüssel).
3) *RA*/*LRA* gibt den öffentlichen Schlüssel zusammen mit den Benutzerdaten an die Zertifizierungsinstanz (*CA*) weiter.
4) *CA* erstellt ein Zertifikat und stellt dieses in ein öffentliches Verzeichnis (*Directory*).
5) *RA*/*LRA* übergibt dem Benutzer ein *Personal Security Environment*, das dessen privaten Schlüssel enthält (z.B. auf einer Chipkarte).

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Registrierungsinstanz (RA)

- Engl. *Registration Authority* (*RA*)
- Prüft Benutzeranträge auf Zertifikat-Erstellung und leitet diese an die *CA* weiter
- Verifiziert die Identität der Antragsteller
- Führt Personalisierung durch und gibt Schlüssel aus
- Lokale Registrierungsinstanz (*LRA*): *RA* innerhalb einer Organisation (z.B. Abteilung in einer Firma)
- *RA* hat vergleichbare Funktion wie Passbehörde

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
Zertifizierungsinstanz (CA)

- Engl. *Certification Authority* (*CA*)
- Vergibt **Zertifikate** (Beglaubigungen):
  - Eindeutige, vertrauenswürdige Verbindung zwischen Namen und öffentlichem Schlüssel einer Person
  - **Integrität** (Echtheit) von öffentlichen Schlüsseln
  - **Authentizität** (Identität) der Eigentümer
  - **Vertrauenswürdigkeit** durch Signatur der *CA*
  - Speicherung in Dateien auf Chipkarten, Disketten, Festplatten, Datenbanken
  - Internationaler Standard: *X.509*

Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

Kryptologie und Datensicherheit
X.509-Zertifikat



Nur für privaten Gebrauch.
Anfragen bzgl. Version für kommerziellen Einsatz oder Schulungszwecke unter http://www.axamedia.de/

Copyright © 2001
Matthias Junk Technische Redaktion

www.axamedia.de

Copyright © 2001 Matthias Junk Technische Redaktion

Diese Publikation ist urheberrechtlich geschützt.
Insbesondere ist die Vervielfältigung, Übersetzung, Mikroverfilmung und die Speicherung und Verarbeitung in elektronischen Systemen (auch auszugsweise) ohne Zustimmung des Autors unzulässig und strafbar. Urhebervermerke sowie sonstige der Identifikation dieser Publikation dienende Merkmale dürfen auf keinen Fall entfernt oder verändert werden.

In dieser Publikation verwendete Bezeichnungen können Marken sein, deren Benutzung durch Dritte die Rechte ihrer Inhaber verletzen kann.

Diese Publikation wurde mit großer Sorgfalt erstellt und intensiv geprüft. Dennoch können einzelne Fehler nicht vollkommen ausgeschlossen werden.
Für fehlerhafte, unvollständige oder nicht aktualisierte Angaben und deren Folgen wird weder eine juristische Verantwortung noch irgend eine Haftung übernommen.