Folge 2 / Kapitel 2.1:
Technologische Grundlagen
Verschlüsselung und digitale Signatur

Prof. Dr. Walter Lösel
Fachbereich Betriebswirtschaft
Georg-Simon-Ohm-Fachhochschule Nürnberg

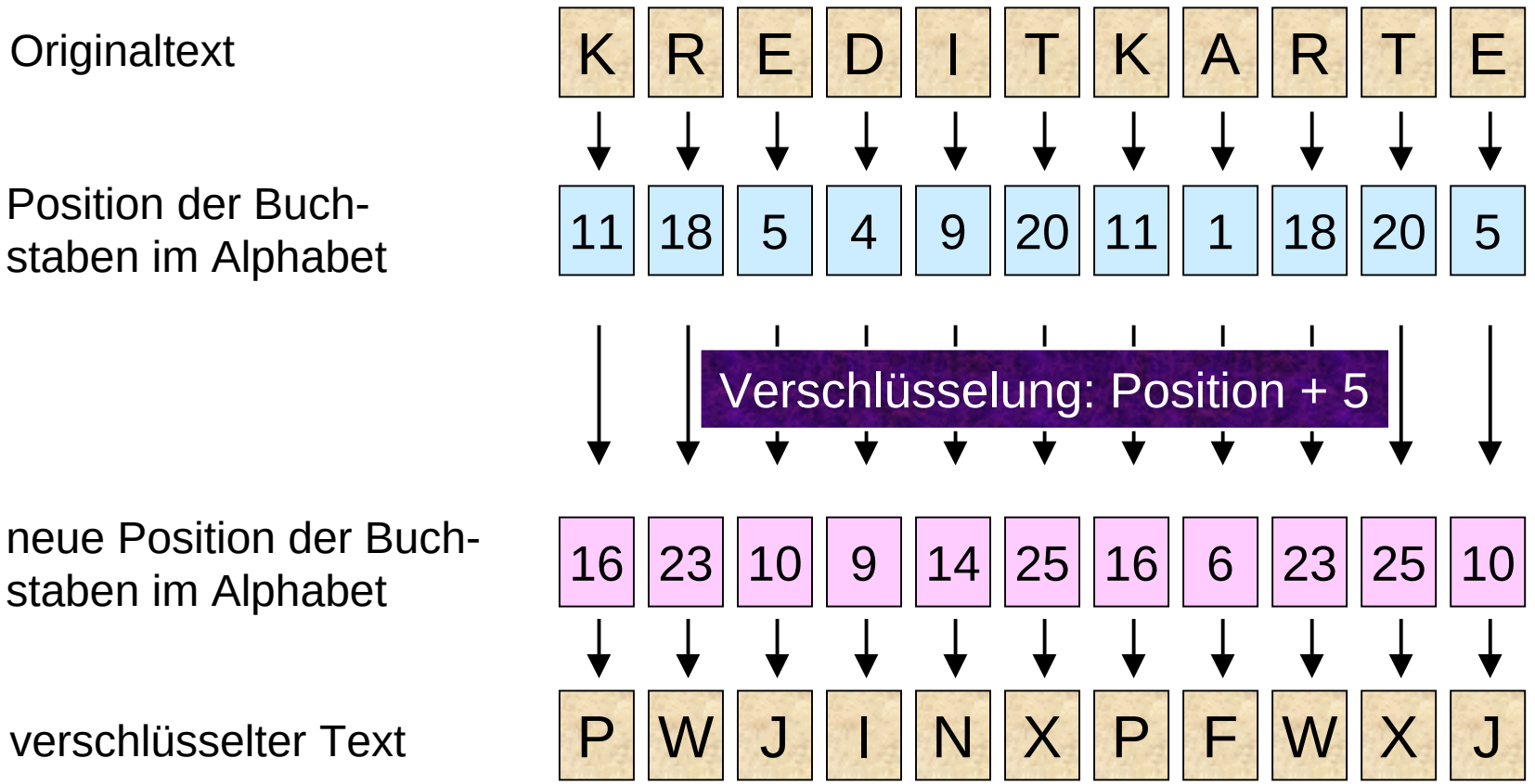
Gliederung

1. Anforderungen an eine sichere Übertragung

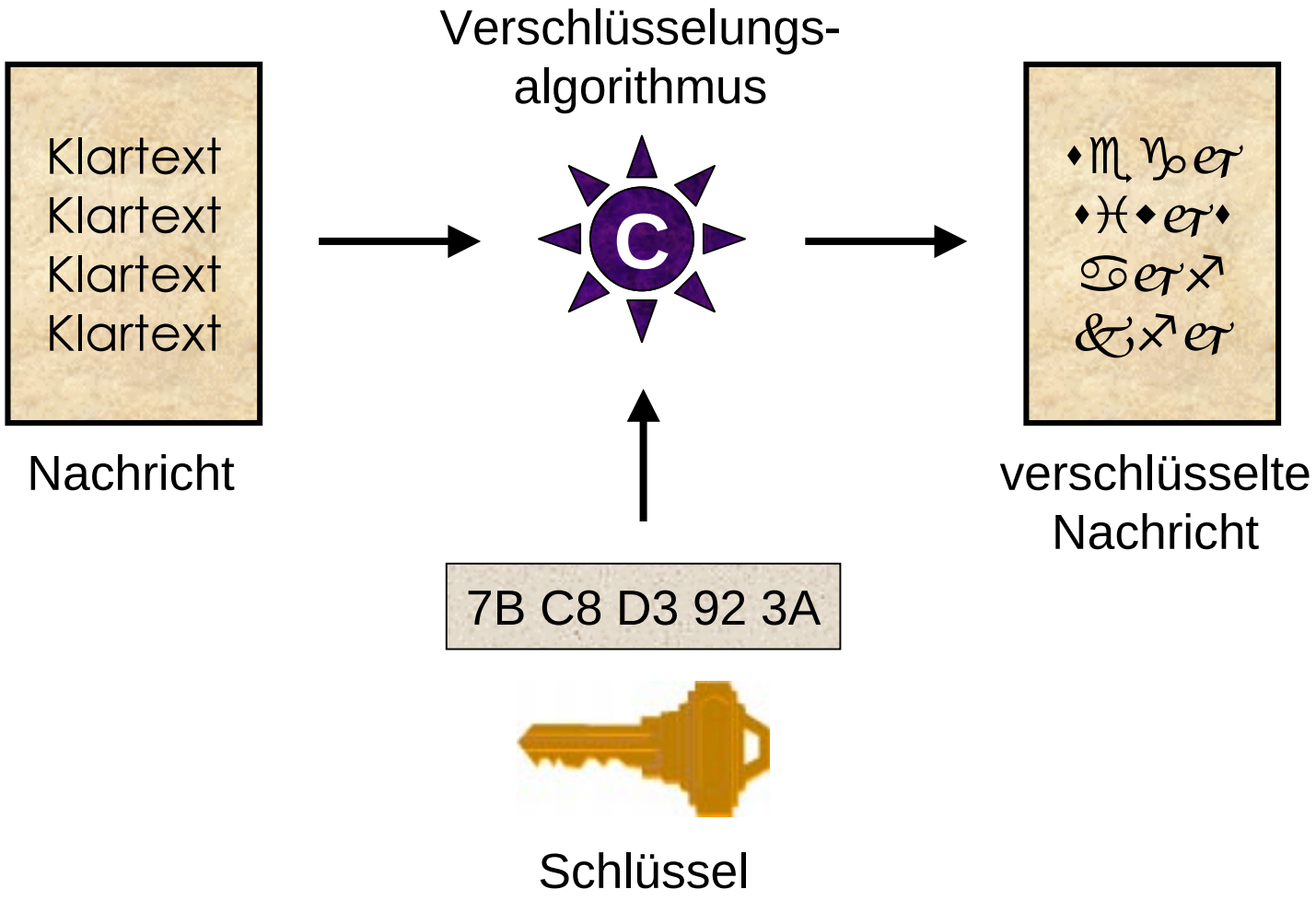
- Vertraulichkeit
  - Nachrichten sollen nicht von Unbefugten gelesen werden können!
- Integrität
  - Nachrichten sollen nicht unerkannt verfälscht werden können!
- Identität
  - Eine Nachricht soll ihrem Absender eindeutig zugeordnet werden können!
- Authentizität
  - Die Identität des Absenders soll überprüfbar sein!

Gliederung

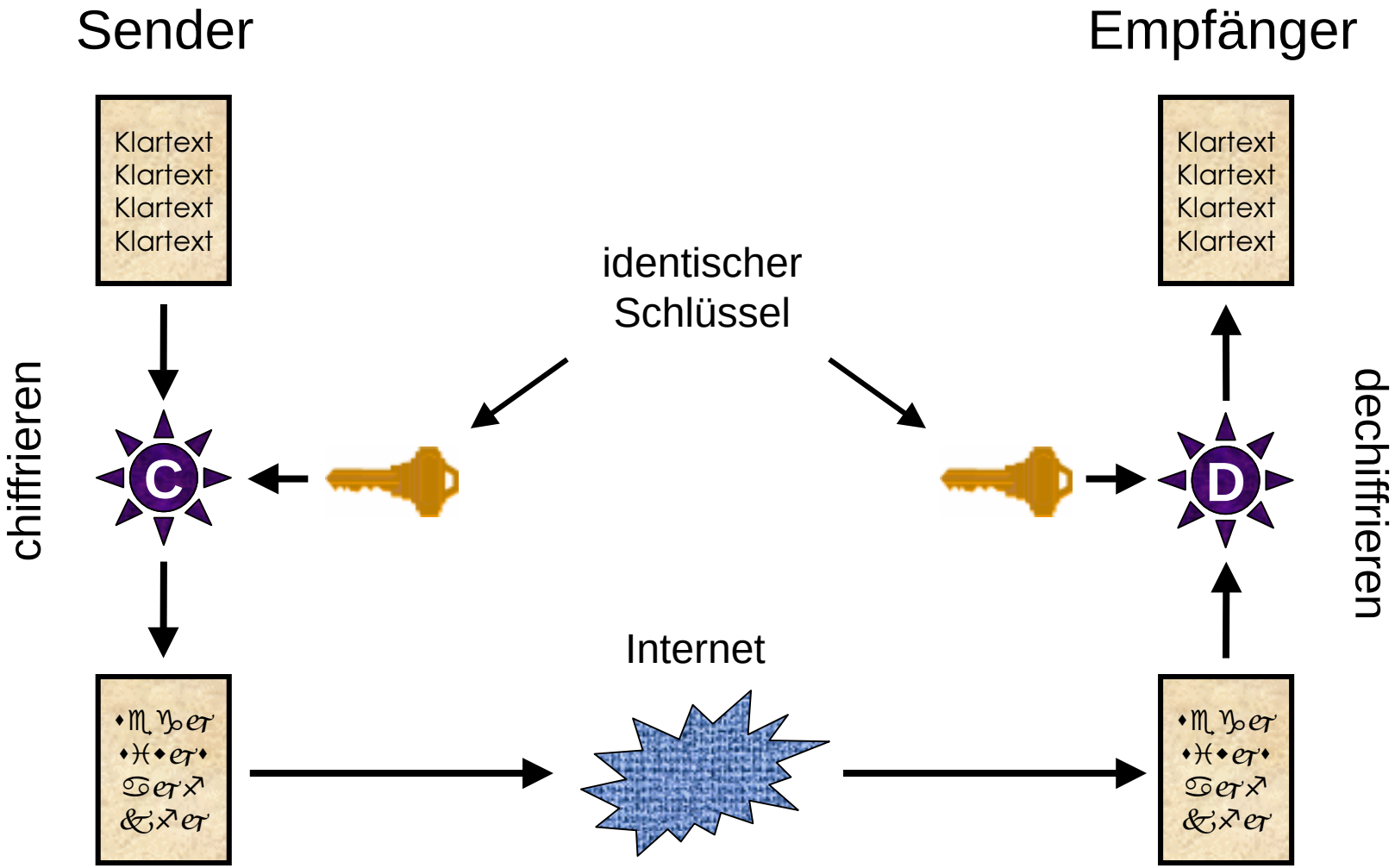
2. Verschlüsselung: Beispiel für die Verschlüsselung von Text



2. Verschlüsselung: Grundprinzip der Verschlüsselung



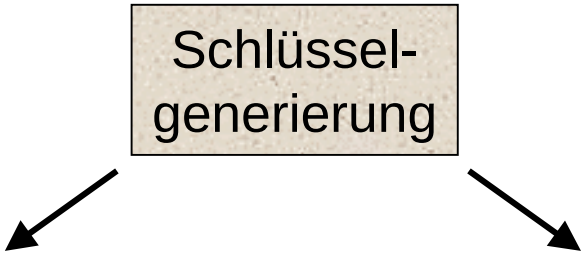
2. Verschlüsselung: Symmetrische Verschlüsselung (I)



2. Verschlüsselung: Symmetrische Verschlüsselung (II)

- Kennzeichen
  - Zur Ver- wie auch zur Entschlüsselung verwenden beide Kommunikationspartner den gleichen Schlüssel.
- Stärke
  - Algorithmen arbeiten sehr schnell.
- Schwachpunkt
  - Schlüssel muss vor Beginn der Kommunikation über einen sicheren Kommunikationsweg ausgetauscht werden.
- Anwendungsbeispiel
  - IDEA = International Data Encryption Algorithm (1992).

2. Verschlüsselung: Asymmetrische Verschlüsselung (I)



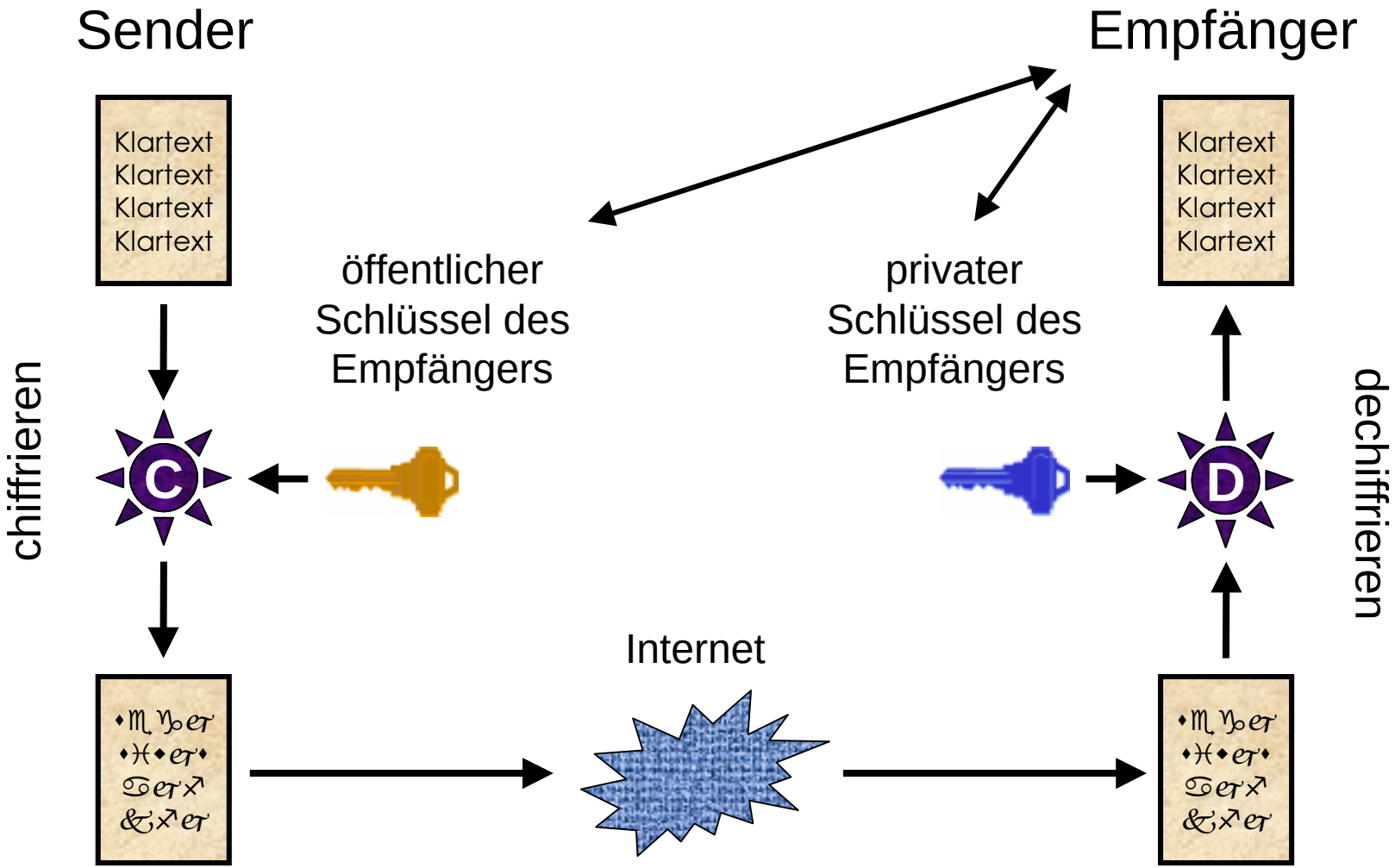
Public Key
(öffentlicher Schlüssel)

- dient zur Verschlüsselung von Nachrichten, die nur mit dem privaten Schlüssel wieder entschlüsselt werden können
- wird allen Kommunikationspartnern bekannt gemacht

Private Key
(privater Schlüssel)

- dient zur Entschlüsselung von Nachrichten, die mit dem dazugehörigen öffentlichen Schlüssel verschlüsselt worden sind
- muss sicher aufbewahrt werden (geheimer Schlüssel)

2. Verschlüsselung: Asymmetrische Verschlüsselung (II)



2. Verschlüsselung: Asymmetrische Verschlüsselung (III)

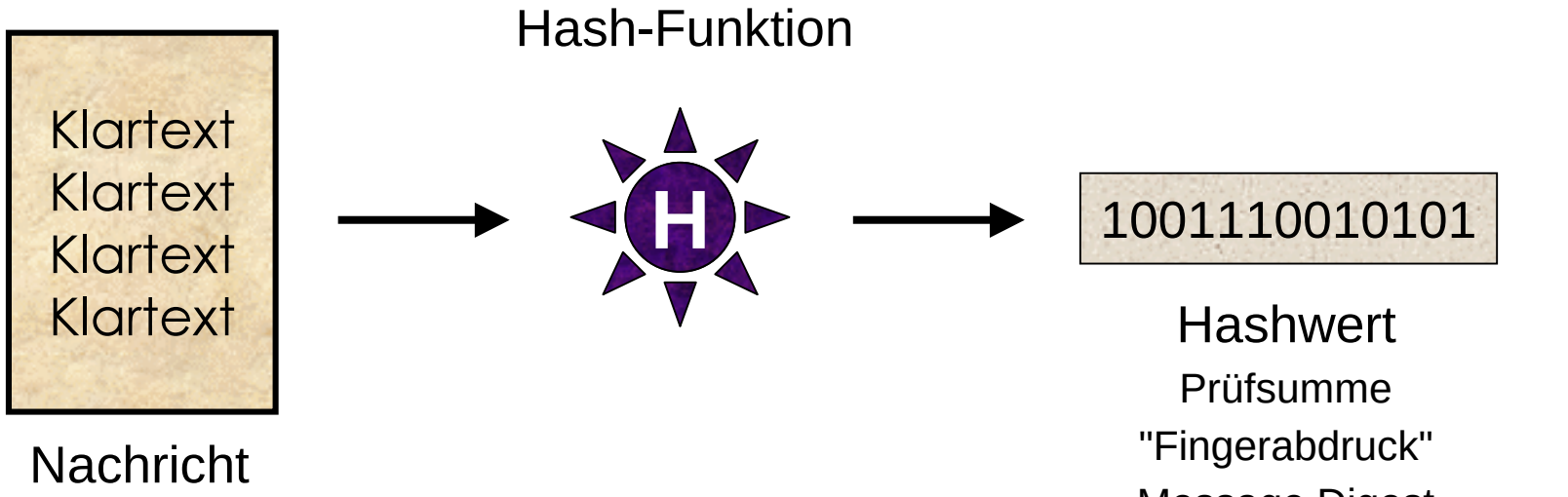
- Kennzeichen
  - Zur Ver- und Entschlüsselung dient ein Schlüsselpaar: der öffentliche und der private Schlüssel.
  - Nachrichten, die mit dem einen Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen anderen Schlüssel wieder entschlüsselt werden.
- Stärke
  - Schlüsselverteilung ist sehr einfach.
- Schwachpunkt
  - Algorithmen arbeiten relativ langsam.
- Anwendungsbeispiel
  - RSA = Algorithmus von Rivest, Shamir, Adleman (1978).

2. Verschlüsselung: Hybridverfahren

- Kennzeichen
  - Kombiniert die jeweiligen Vorteile der symmetrischen und asymmetrischen Verschlüsselung.
  - Zur Ver- und Entschlüsselung der Nachricht(en) kommt die symmetrische Verschlüsselung zum Einsatz.
  - Hierzu wird vom Sender ein symmetrischer Schlüssel generiert, der nach Abschluss der Kommunikation wieder erlischt (Session Key).
  - Verwendet die asymmetrische Verschlüsselung lediglich zur sicheren Übermittlung des Session Key vom Sender zum Empfänger.
- Anwendungsbeispiel
  - SSL = Secure Socket Layer (Protokollbaustein).

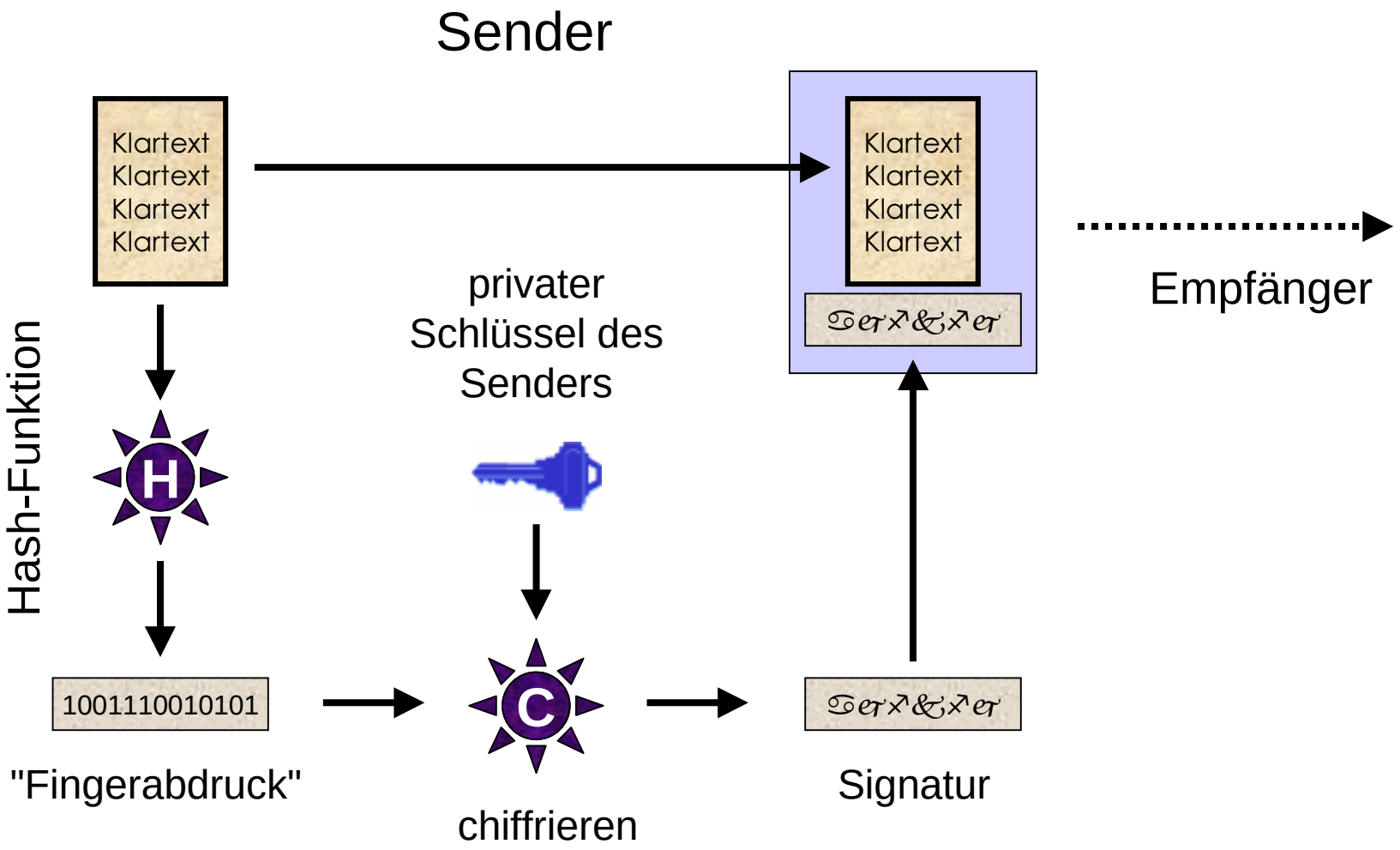
Gliederung

3. Digitale Signatur: Erzeugung eines digitalen "Fingerabdrucks"

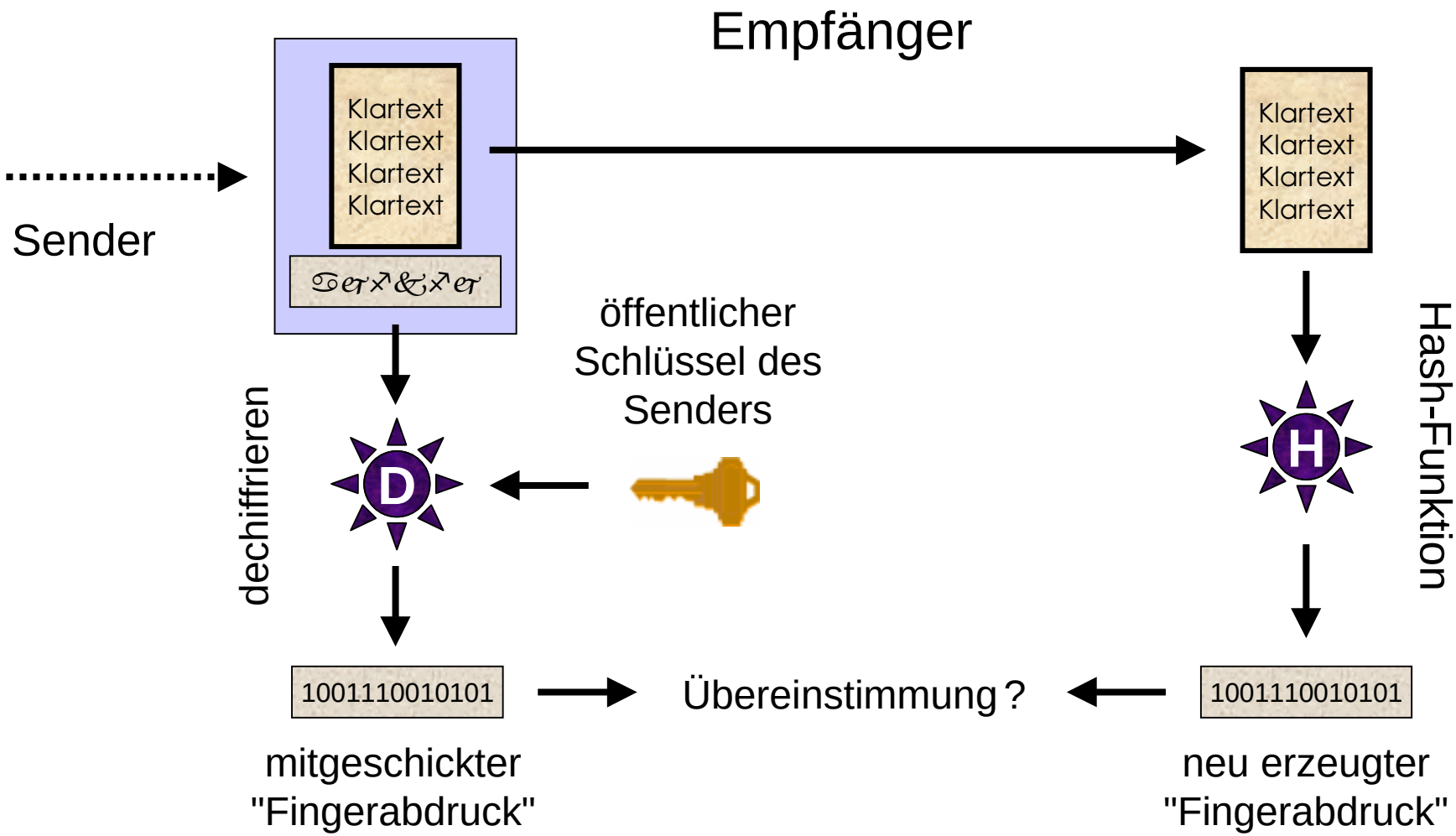


- Der "Fingerabdruck" ist für jeden beliebigen Text absolut eindeutig.
- Aus dem "Fingerabdruck" kann der ursprüngliche Text nicht rekonstruiert werden.

3. Digitale Signatur: Ablauf beim Signieren einer Nachricht



3. Digitale Signatur: Ablauf beim Prüfen der Signatur



3. Digitale Signatur
Zusammenfassung

- Kennzeichen
  - Die digitale Signatur einer Nachricht ist ein mit dem privaten Schlüssel des Senders verschlüsselter "Fingerabdruck" des Nachrichteninhalts.
  - Sie stellt die Integrität der Nachricht und die Identität ihres Senders sicher.
  - Eine Manipulation der Nachricht bei der Übermittlung wird zwar nicht verhindert, jedoch vom Empfänger zweifelsfrei erkannt.
  - Die Nachricht kann weder vom Sender noch vom Empfänger nachträglich unerkannt manipuliert werden.
- Anwendungsbeispiel
  - PGP = Pretty Good Privacy (Anwendungssoftware).

Gliederung

4. Zertifikat:
Digitale Signatur nach § 2 Abs. 1 SigG

Eine **digitale Signatur** im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit

einem **Schlüsselzertifikat einer Zertifizierungsstelle** versehen ist,

den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.

4. Zertifikat:
Ablauf der Zertifizierung

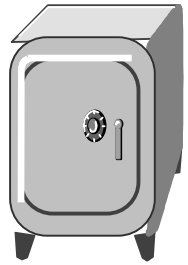
Anwender

- Natürliche Person
- Institution
- Website
- ...

Antrag

Zertifizierungsstelle

- Certification Authority
- Trust Center



- prüft Identität
- generiert und übergibt Schlüsselpaar
- erstellt und übergibt Zertifikat

4. Zertifikat:
Bestandteile eines Zertifikats

Personalausweis		Digitales Zertifikat
• Vor- und Nachname	⟷	• Name oder Pseudonym
• Ausstellende Behörde	⟷	• Zertifizierungsstelle
• Ausstellungsdatum	⟷	• Ausstellungsdatum
• Gültigkeitsdauer	⟷	• Gültigkeitsdauer
• Id-Nr. des Ausweises	⟷	• Id-Nr. der Zertifizierstelle
• Unterschrift		• - - -
• - - -		• Öffentlicher Schlüssel

Zertifikat:
Ausgewählte Zertifizierungsstellen

- T-TeleSec
  - Deutsche Telekom AG — www.telesec.de
- DFN Policy Certification Authority
  - Deutsches Forschungsnetz e.V. — www.cert.dfn.de
- TrustCenter
  - TC Trust Center GmbH — www.trustcenter.de
- GlobalSign
  - GlobalSign NV/SA — www.globalsign.com
- VeriSign
  - VeriSign Inc. — www.verisign.com

Gliederung

5. Zusammenfassung

- Vertraulichkeit
  - wird sichergestellt durch: **Verschlüsselung**
- Integrität
  - wird sichergestellt durch: **Signatur**
- Identität
  - wird sichergestellt durch: **Signatur**
- Authentizität
  - wird sichergestellt durch: **Signatur + Zertifikat**

Gliederung

6. Kontrollfragen

1. Welche Anforderungen sind an eine sichere Übertragung im Internet zu stellen? Erläutern Sie das jeweilige Gefahrenpotenzial anhand eines Beispiels aus dem E-Business.

2. Skizzieren Sie die Arbeitsweise von symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren. Wodurch unterscheiden sich diese Verfahren und wo liegen die jeweiligen Stärken?

3. Was versteht man unter einer digitalen Signatur? Welche Sicherheitsanforderungen werden durch sie erfüllt?

4. Das Signaturgesetz sieht die Einrichtung von Zertifizierungsstellen (Trust Center) vor. Welche Funktion haben solche Einrichtungen? Welche Dienstleistungen könnten sie erbringen?

Literaturhinweis

- Bitzer, Frank / Brisch, Klaus M.:
  Digitale Signatur
  - Grundlagen, Funktion und Einsatz -
  Springer Verlag 1999

Vielen Dank
für Ihre
Aufmerksamkeit!