Datensicherheit und Datenschutz

Datensicherheit

Schutz von Daten

Datenschutz

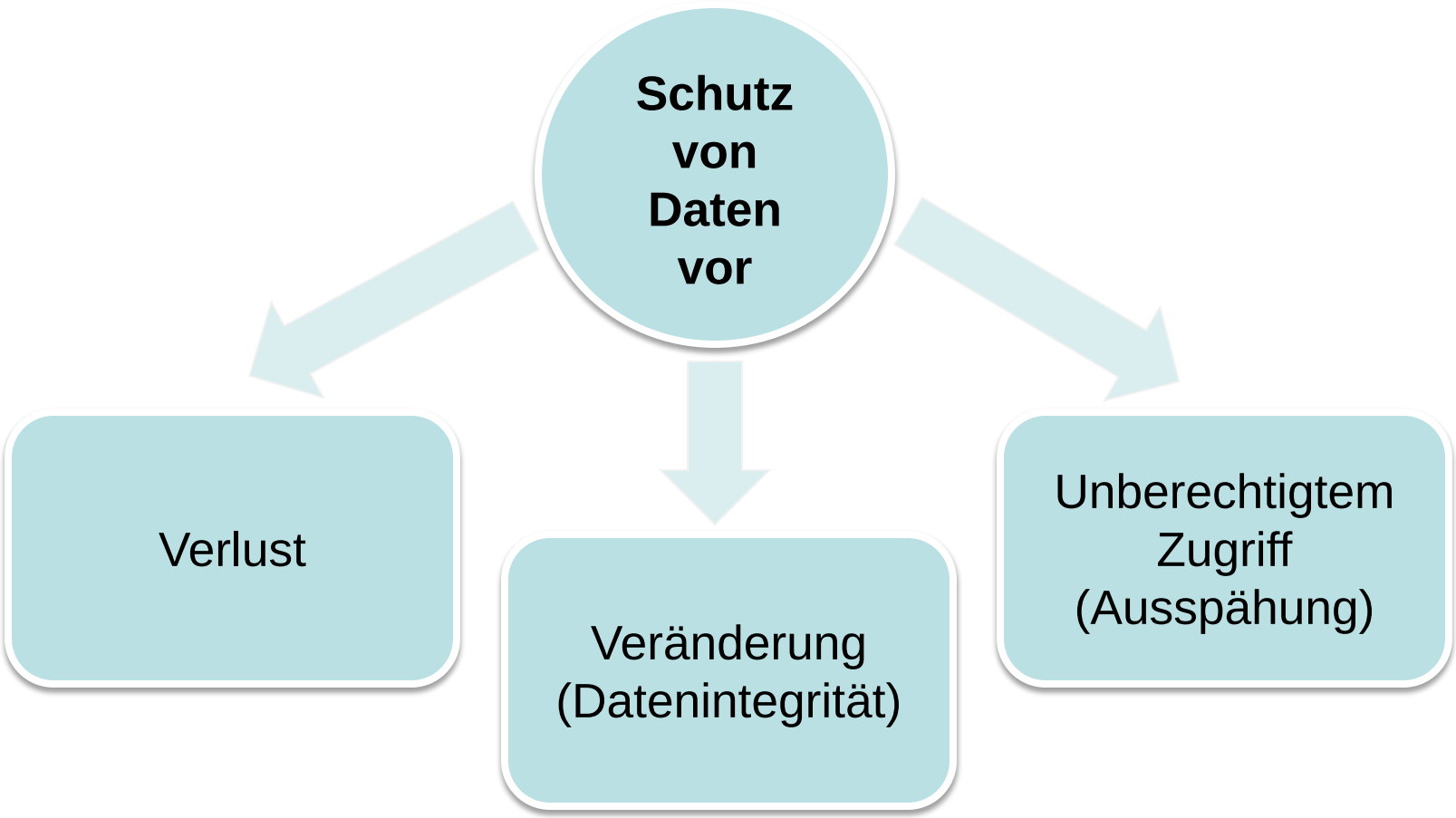
(setzt Datensicherheit voraus)

Schutz von Personen

(über die die Daten Aussagen zulassen; Privacy)

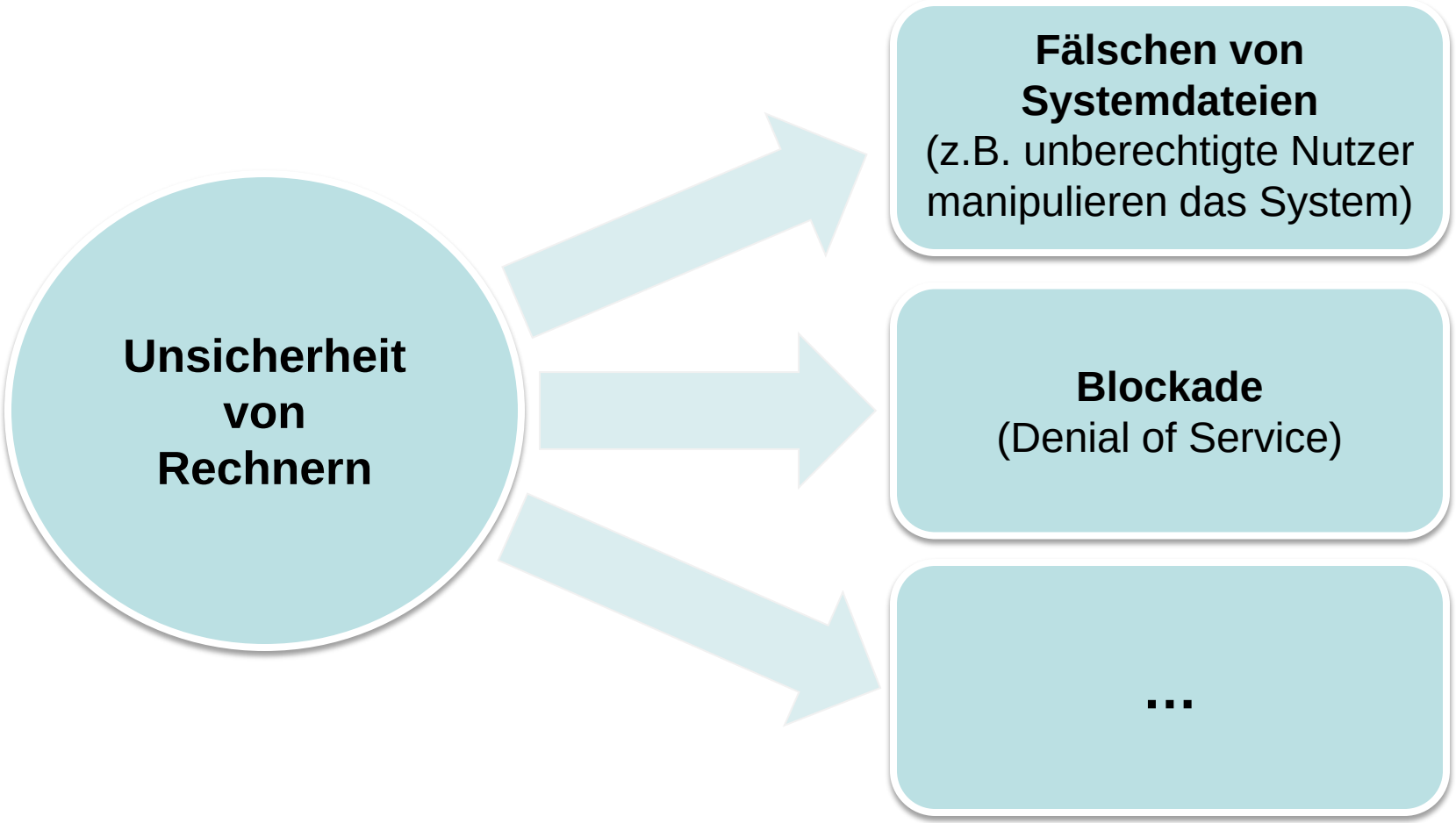
Datensicherheit

(passiv und aktiv)



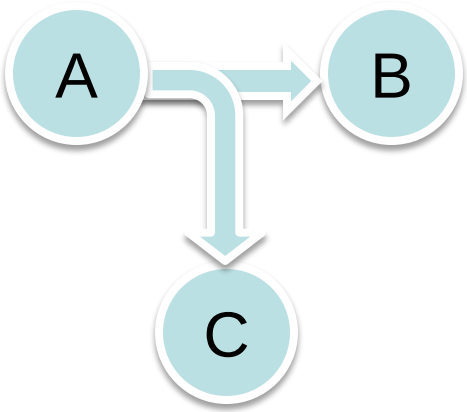
Datensicherheit

Datenverarbeitung

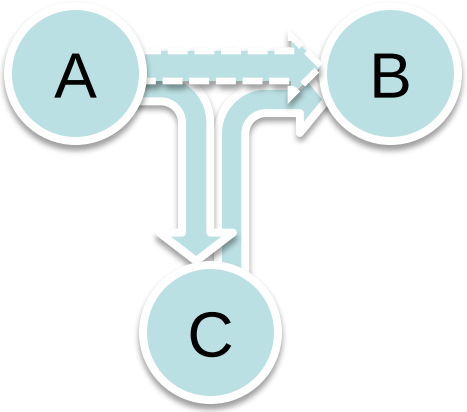


Datensicherheit

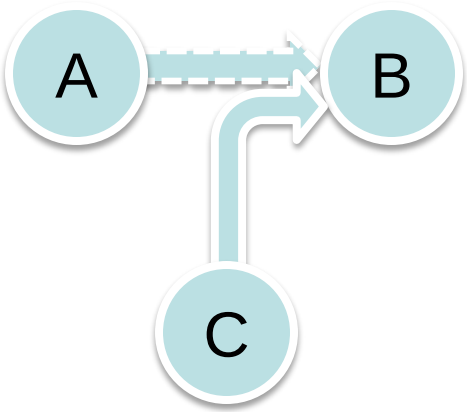
Datenkommunikation



Vertraulichkeit
(Verschlüsselung)



Integrität/Verbindlichkeit



Authentizität

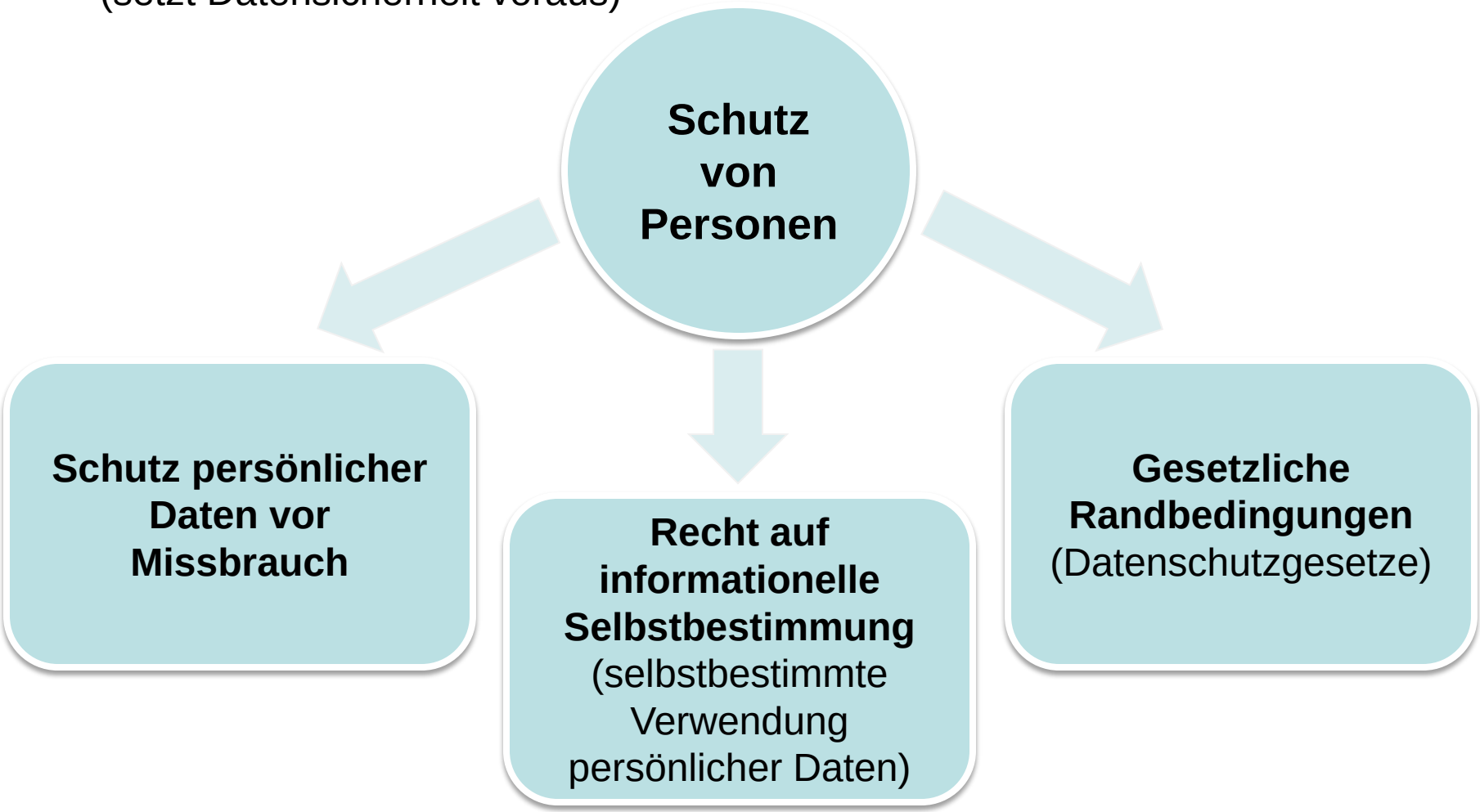
(Elektronische Signatur)

Maßnahmen zur Datensicherheit

- Physischer Schutz von DV Anlagen und Netzen
- Zugriffskontrolle über Identitäten, Rollen usw.
- Authentifizierung (sichere Feststellung der Identität)
- Verschlüsselung (Vertraulichkeit)
- Virenschutz, Malware
- …

Datenschutz

(setzt Datensicherheit voraus)



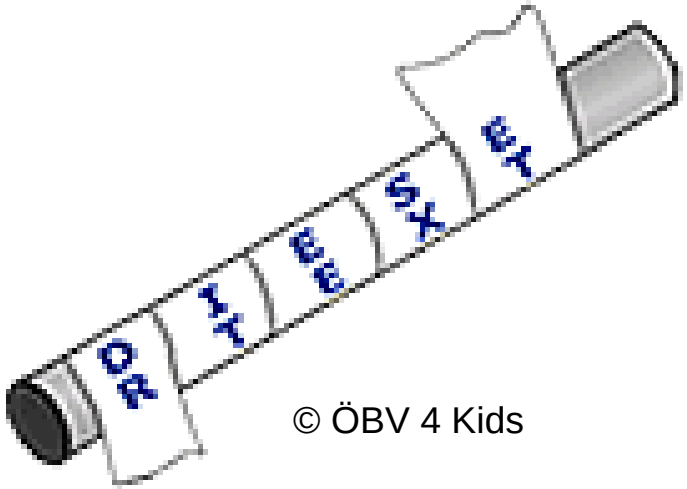
Maßnahmen zur Datensicherheit und Datenschutz

Organisatorische Maßnahmen	Technische Maßnahmen
• Personal • Verfahren • Policies (Regeln, Rollen, Verantwortlichkeiten)	• Rechnersicherheit • Netzsicherheit • Softwarequalität/sicherheit

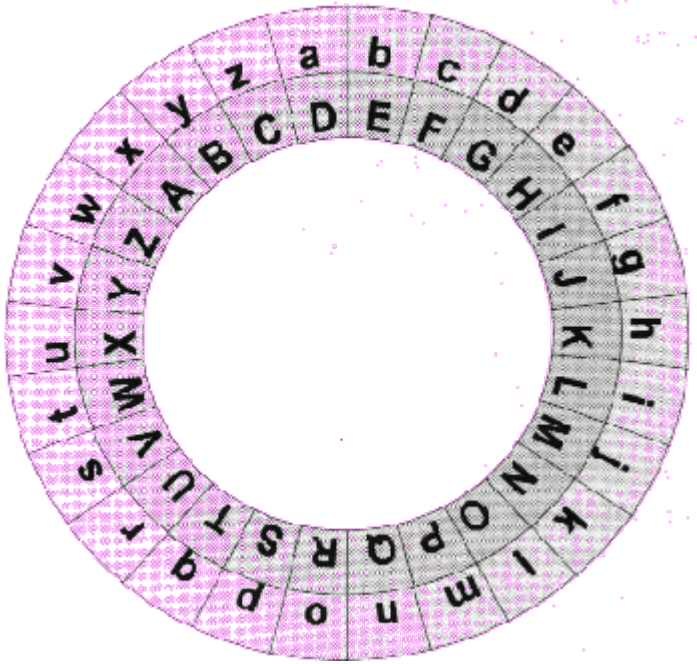

Zertifikate
Regenbögen
Geheimnisse
Skytale von Sparta
Enigma
Man-in-the-Middle
1024bit
Cäsar Chiffre
Logarithmen
Brute Force
Vertrauen
Identitäten
Primzahlen
Hand-Kopf Regel
Elliptische Kurven
Schlüssellänge
PIN /TAN
DES, RSA, AES, ...

Grundlagen

- Hand – Kopf Regel
  - Skytale von Sparta
  - Cäsar Chiffre
  - Enigma
  - Kreditkarte + PIN
  - Krypto-Token + Passwort



© ÖBV 4 Kids



© Uni Bielefeld

Bundesarchiv, Bild 101I-241-2173-09
Foto: Grupp | 1943/1944

Der Weg zu meiner digitalen Identität

Erzeugung eines Schlüsselpaares

Digitale Identitäten bestehen immer aus einer öffentlichen und einer privaten Komponente

Der Weg zu meiner digitalen Identität

Erzeugung eines Schlüsselpaares

Digitale Identitäten bestehen immer aus einer öffentlichen und einer privaten Komponente

Erstellen eines Zertifikat-Antrages

Beinhaltet den öffentlichen Teil meines Schlüssels sowie meine reale Identität

Name, Email, Name eines Rechners,…

Der Weg zu meiner digitalen Identität

Erzeugung eines Schlüsselpaares

Digitale Identitäten bestehen immer aus einer öffentlichen und einer privaten Komponente

Erstellen eines Zertifikat-Antrages

Beinhaltet den öffentlichen Teil meines Schlüssels sowie meine reale Identität	Name, Email, Name eines Rechners,…

Digitale Unterschrift eines Anbieters bestätigt meine Identität

Die „Qualität“ hängt maßgeblich vom Unterschreiber ab	Eigenbedarf etwa für Universitäten, Rechtssicherheit, …

Etwas Mathematik

- Kryptografische Verfahren
  Beruhen darauf, dass der "Hinweg" einfach und schnell, der "Rückweg" jedoch extrem aufwändig berechenbar ist.

  Beispiel Primzahl Faktorierung
  - es ist einfach zwei sehr große Primzahlen, mehrere hundert Stellen lang, zu multiplizieren
  - eine entsprechend große Zahl in Ihre Faktoren zu zerlegen dauert bei derzeitiger Technik und mathematischem Wissen jedoch deutlich länger als die Nutzungsdauer der zu schützenden Daten

- Neuere Verfahren
  Beruhen auf diskreten Logarithmen auf elliptischen Kurven.

⇨ Oftmals Kombination von mehreren Verfahren
insbesondere symmetrische (schnell) mit asymmetrischen (sicher)

Sichere (verschlüsselte) Email Übertragung

Verifikation

Absender "A" benötigt öffentlichen Schlüssel des Empfängers "E" und überprüft diesen an Hand der digitalen Unterschrift

Verschlüsselung

"A" verschlüsselt Text mit öffentlichem Schlüssel von "E"

Versand

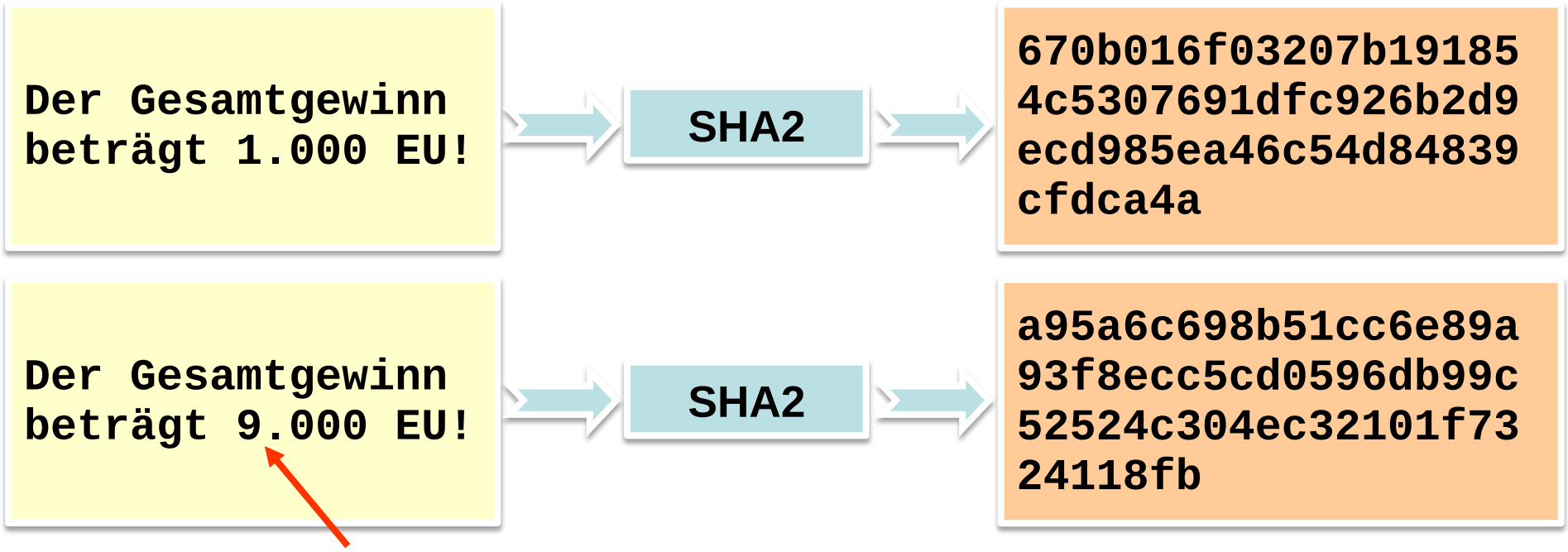
Übermittlung der verschlüsselten Email

Entschlüsselung

Nur "E" kann die Email entschlüsseln, da ausschließlich sie im Besitz des passenden privaten Schlüssels ist.

Hash-Funktionen

- Eine Hash-Funktion erzeugt aus einer großen Quellmenge eine kleine Zielmenge oft fester Länge
  - nicht eindeutig aber Kollisionen werden möglichst vermieden
  - stellt eine Art Fingerabdruck dar



Digitale Unterschrift

Absender

- Berechnung des Hashwerts der Daten
- Verschlüsselung des Hashwerts mit privatem Schlüssel
- Übertragung von digitaler Signatur, Dokument und Zertifikat an Empfänger

Empfänger

- Überprüfung des Zertifikats
- Berechnung des Hashwerts des Dokuments
- Entschlüsselung der digitalen Signatur mit öffentlichem Schlüssel des Absenders
- Vergleich mit selbst berechnetem “Fingerabdruck“

Zahlenspiele mit Hash-Funktionen

Anzahl der Werte
einer heute üblichen
Hash-Funktion SHA256

Anzahl der Wassermoleküle
unter der Annahme, die Erde
bestünde komplett aus Wasser