TECHNISCHE UNIVERSITÄT DARMSTADT

AMBIENT INTELLIGENCE

Vorlesung 12: Sicherheit in AmI-Systemen

TECHNISCHE UNIVERSITÄT DARMSTADT

AGENDA

1 Begriffsbestimmung

2 IT-Sicherheitsziele

3 IT-Sicherheitsmaßnahmen

4 Risikoanalyse

5 Anwendung auf AmI-Systeme

6 Lernziele

BEGRIFFSBESTIMMUNG

TECHNISCHE UNIVERSITÄT DARMSTADT

SICHERHEIT

Security

Sicherheit eines Systems vor Störungen durch

- höhere Gewalt
- technisches Versagen
- versehentliche oder fahrlässige menschliche Fehlhandlungen
- vorsätzliche menschliche Handlungen

Betriebssicherheit, Safety

Sicherheit der Umgebung eines Systems vor Störungen durch das System

IT-SICHERHEITSZIELE

MÖGLICHE IT-SICHERHEITSZIELE

- **Verfügbarkeit:** Daten/IT-Ressourcen sollen zur Verfügung stehen, wenn benötigt.
- **Vertraulichkeit:** Daten sollen nicht von Unbefugten gelesen werden können.
- **Integrität:** Daten sollen nicht unbemerkt von Unbefugten modifiziert werden können.
- **Authentizität:** Der Urheber von Daten/Aktionen soll eindeutig identifiziert werden können.
- **Nichtabstreitbarkeit (Non-Repudiation)**
  - **der Urheberschaft:** Der Urheber von Aktionen soll seine Urheberschaft nicht abstreiten können.
  - **des Empfangs:** Der Empfänger von Daten soll deren Empfang nicht abstreiten können.
- **Anonymität:** Der Urheber von Daten/Aktionen soll nicht identifiziert werden können.

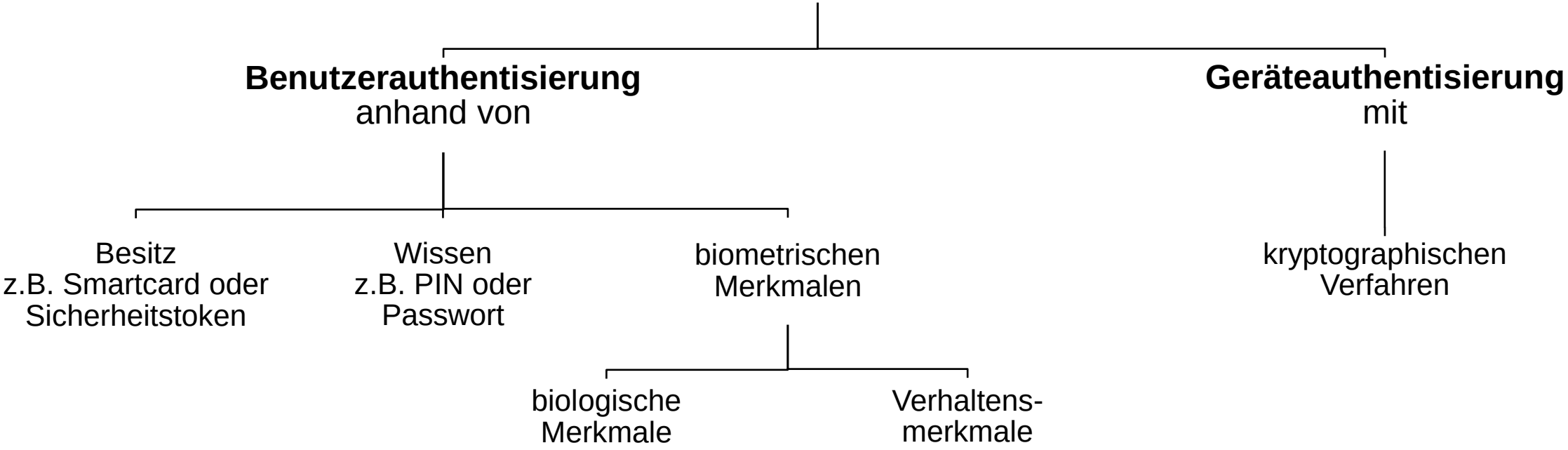
IT-SICHERHEITSMAßNAHMEN

IT-SICHERHEITSMAßNAHMEN

- Beispiele
  - Benutzerauthentisierung, Zugriffskontrolle und Rechteverwaltung
  - manipulationsgeschützte Gehäuse, verschlossene Türen, Log-Dateien, Firewalls
  - Vier-Augen-Prinzip
  - auf kryptographischen Verfahren basierende Sicherheitsmaßnahmen (z.B. Geräteauthentisierung)
- kosten Zeit und Geld, sind unbequem für die Benutzer
- sollten dennoch in allen Phasen des Lebenszyklus von IT-Systemen berücksichtigt werden

AUTHENTISIERUNG

Prüfung der Zugriffsberechtigung auf IT-Ressourcen



KRYPTOGRAPHISCHE VERFAHREN

- Verfahren mit mindestens einem Parameter (Schlüssel) zur Transformation von Klartext in unverständlichen Geheimtext (Verschlüsselung) und zur Rücktransformation von Geheimtext in Klartext (Entschlüsselung)
  - symmetrische kryptographische Systeme:
    zur Ver- und Entschlüsselung wird derselbe, geheime Schlüssel verwendet
  - asymmetrische kryptographische Systeme:
    zur Ver- und Entschlüsselung werden zwei verschiedene Schlüssel verwendet
- schlüssellose Verfahren wie kryptographische Hashfunktionen
- kryptographische Protokolle: Abfolge von Schritten,
  um bestimmte Sicherheitsanforderungen zu erfüllen

TECHNISCHE UNIVERSITÄT DARMSTADT

SICHERHEIT KRYPTOGRAPHISCHER VERFAHREN

- Schwierigkeit (Komplexität) der Berechnung der Umkehrung (Abbildung, die jedem Funktionswert die zugehörigen Urbilder zuordnet)
  - Einwegfunktionen und
  - Einwegfunktionen mit Hintertür
- sollte auf der Geheimhaltung von Schlüsseln beruhen anstatt auf der Geheimhaltung von Algorithmen [Kerckhoffs-Prinzip, nach Auguste Kerckhoffs (1835–1903)].
  - "Security by Obscurity" hat sich oftmals als schwach erwiesen.

Optischer Telegraph

EINWEGFUNKTION

- mathematische Funktion, deren Umkehrung wesentlich schwieriger zu berechnen ist als die Funktion selbst
- anschauliches Beispiel
  - Einwegfunktion: Heraussuchen einer Telefonnummer aus dem Telefonbuch bei gegebenem Namen
  - Umkehrfunktion: Heraussuchen eines Namens aus dem Telefonbuch bei gegebener Telefonnummer – um so schwieriger, je länger die Telefonnummer und je dicker das Telefonbuch
- Berechnung von Funktionswerten sollte schnell gehen
- Umkehrung sollte nach dem Stand von Wissenschaft und Technik mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden können
  - auch bei Brute-Force-Angriffen (erschöpfendem Ausprobieren aller möglichen Werte)

EINWEGFUNKTION MIT HINTERTÜR

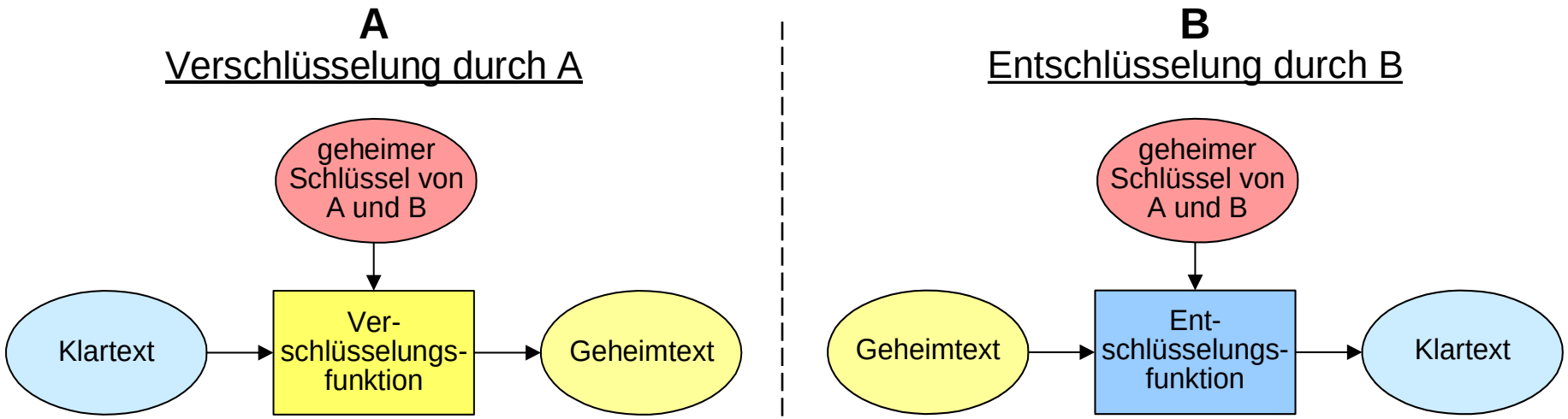
- Einwegfunktion,
  - deren Umkehrfunktion leicht mit Hilfe einer zusätzlichen Information (durch die Hintertür) berechnet werden kann
- Beispiel
  - Einwegfunktion mit Hintertür:
    symmetrische oder asymmetrische Verschlüsselungsfunktion
  - Umkehrfunktion: Entschlüsselungsfunktion
    - bei gegebenem Schlüssel leicht zu berechnen
    - ohne Kenntnis des Schlüssels nicht mit vertretbarem Aufwand zu berechnen

IT-SICHERHEITSMAßNAHMEN

SYMMETRISCHE KRYPTOGRAPHISCHE SYSTEME

SYMMETRISCHES KRYPTOGRAPHISCHES SYSTEM

- Verschlüsselungs- und Entschlüsselungsfunktion verwenden denselben geheimen Schlüssel
- Vorteil: hoher Datendurchsatz
- Blockverschlüsselung oder Stromverschlüsselung

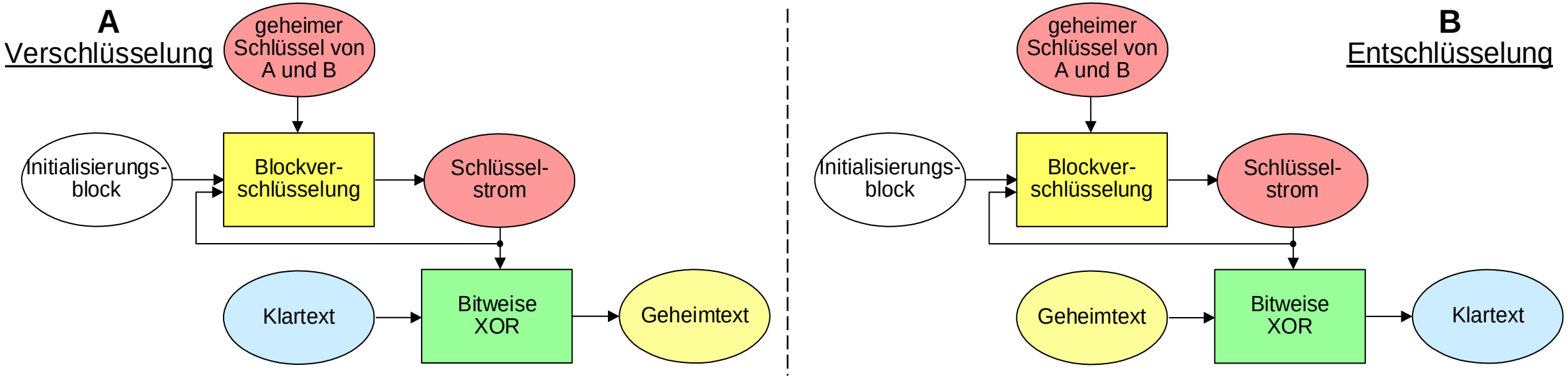


BEISPIELE BLOCK-VERSCHLÜSSELUNGSVERFAHREN

- **DES** (Data Encryption Standard, 1977)
  - Schlüssellänge: 64 Bit, davon 8 Paritätsbits, also effektiv nur 56 Bit
  - kann heutzutage mittels Brute-Force-Angriffe gebrochen werden
- **Triple-DES**
  - modifiziertes DES-Verfahren mit dreifachem Aufruf des DES-Algorithmus mit drei Schlüsseln
- **AES** (Advanced Encryption Standard)
  - 2000 von NIST als Nachfolger von DES ausgewählt
  - variable Schlüssellänge (z.B. 128, 192 oder 256 Bit)

BEISPIEL STROM-VERSCHLÜSSELUNGSVERFAHREN

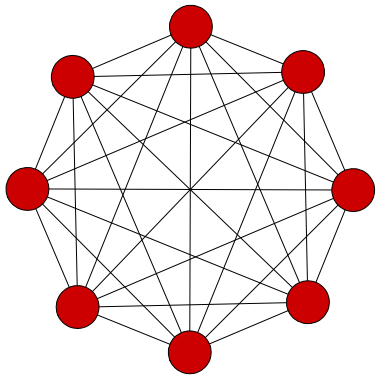
- Blockverschlüsselungsverfahren im Output-Feedback-Modus zur Erzeugung eines pseudozufälligen Schlüsselstroms

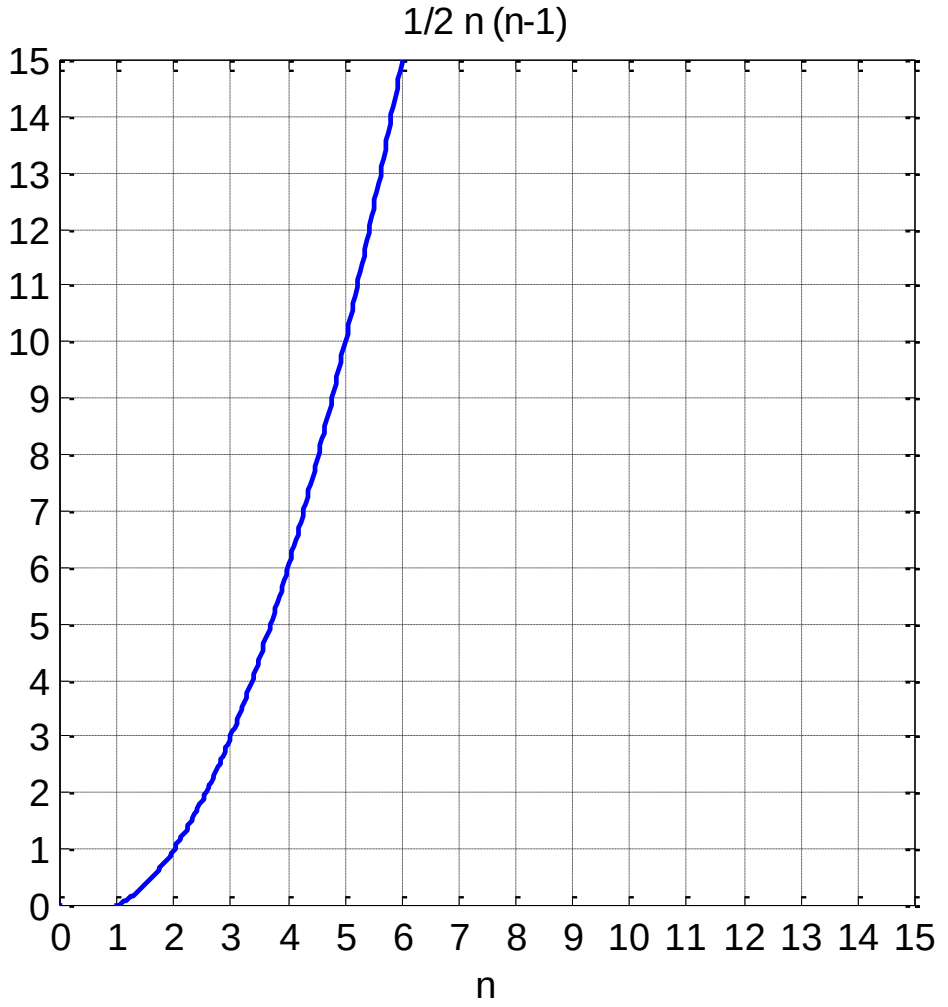


TECHNISCHE UNIVERSITÄT DARMSTADT

SCHLÜSSEL-VERTEILUNGS-PROBLEM

- Wenn *n* Kommunikationspartner jeweils paarweise untereinander vertraulich kommunizieren wollen, werden $\frac{n(n-1)}{2}$ verschiedene Schlüssel benötigt.





SCHLÜSSELVERTEILUNGS-PROBLEM

- Bevor die Übertragung geheimer Nachrichten möglich ist, müssen Schlüssel verteilt werden, die ebenfalls geheim bleiben müssen.
- Anderweitig gesicherter Übertragungskanal wird benötigt:
  - z.B. mit anderem Schlüssel verschlüsselt.

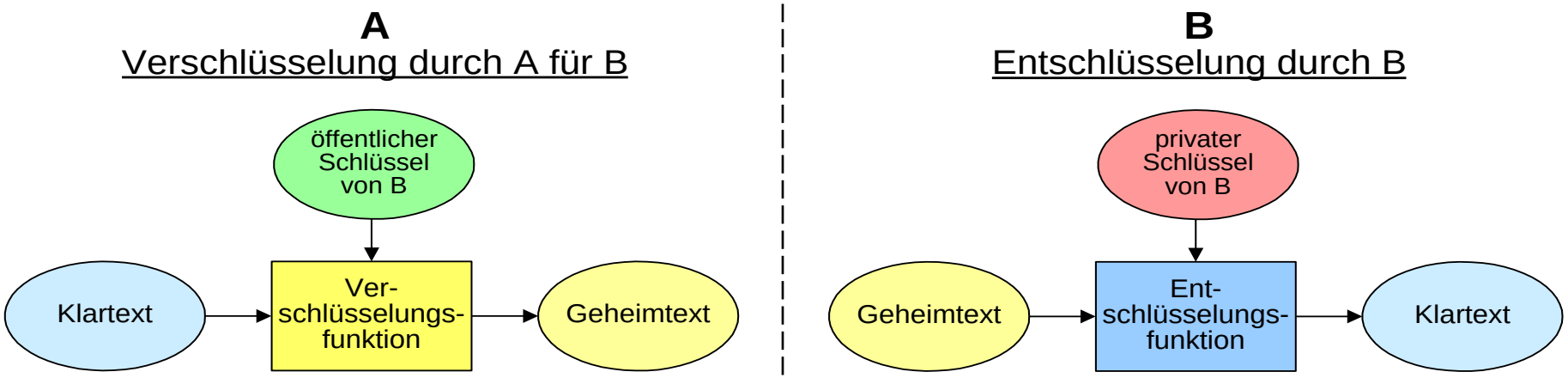
TECHNISCHE UNIVERSITÄT DARMSTADT

IT-SICHERHEITSMAßNAHMEN

ASYMMETRISCHE KRYPTOGRAPHISCHE SYSTEME

ASYMMETRISCHES KRYPTOGRAPHISCHES SYSTEM

- Verschlüsselungs- und Entschlüsselungsfunktion verwenden zwei verschiedene Schlüssel,
  - die zusammengehören,
  - aber nicht mit vertretbarem Aufwand aus dem jeweils anderen berechnet werden können.
- Auch wenn einer der Schlüssel veröffentlicht wird, bleibt der andere geheim.
- Vorteil: einfachere Schlüsselverteilung als bei symmetrischen kryptographischen Systemen



BEISPIELE ASYMMETRISCHER KRYPTOGRAPHISCHER SYSTEME

- **RSA** [Algorithmus von Ron Rivest, Adi Shamir und Leonard Adleman, 1977]
  - Sicherheit beruht darauf, dass es schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen.
    - Primfaktorzerlegung sehr großer Zahlen ist mit den heute bekannten Verfahren praktisch nicht durchführbar, auch wenn nicht prinzipiell unmöglich.
  - Schlüssellänge variabel
  - empfohlene Schlüssellänge 2048 Bit (256 Oktetts) [siehe z.B. SOGIS (Senior Officials Group – Information Systems Security): Agreed Cryptographic Mechanisms. https://sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf]
  - relativ langsam

$$n = \prod_{i=1}^{N} p_i, \text{wobei alle } p_i \text{ Primzahlen sind}$$

BEISPIELE ASYMMETRISCHER KRYPTOGRAPHISCHER SYSTEME

- **ECC (Elliptic Curve Cryptosystem)**
  - Sicherheit beruht darauf, dass es schwierig ist, das diskrete Logarithmus-Problem im Kontext elliptischer Kurven zu lösen.
  - Schlüssellänge variabel
  - Schlüssellänge nur 224 Bit (28 Oktetts) für die gleiche Sicherheit wie mit 2048-Bit-RSA-Schlüssel
  - erfordert weniger Rechenzeit und kürzere Schlüssellänge als RSA-Kryptosystem
  - noch nicht so weit verbreitet wie RSA-Kryptosystem

$$x = \log_b a, \text{wenn } a = b^x$$

TECHNISCHE UNIVERSITÄT DARMSTADT

IT-SICHERHEITSMAßNAHMEN

HASHFUNKTIONEN

HASHFUNKTION (STREUWERTFUNKTION)

- mathematische Funktion mit der Eigenschaft,
  - Eingabewerte einer beliebigen, endlichen Länge auf einen Ausgabewert mit fester Länge abzubilden (**Datenreduktion**).
- wird eingesetzt z.B.
  - zum leichteren Auffinden von Daten in Datenbanken,
  - zur Berechnung von Prüfsummen.

KRYPTOGRAPHISCHE HASHFUNKTION

- Hashfunktion *h* mit den Eigenschaften,
  - dass es nicht mit vertretbarem Aufwand möglich ist, zwei verschiedene Eingabewerte *x* und *x'* zu bestimmen, deren Funktionswerte *h*(*x*) und *h*(*x'*) übereinstimmen (**Kollisionsresistenz**),
  - dass es nicht mit vertretbarem Aufwand möglich ist, aus einem Funktionswert *y* einen Eingabewert *x* mit der Eigenschaft *h*(*x*) = *y* zu bestimmen (**Einwegfunktion**).
- wird eingesetzt z.B.
  - um unbefugte Modifikationen an Datenobjekten entdecken zu können (Sicherung der Integrität, dank Kollisionsresistenz),
  - um Passwörter sicher zu speichern (Sicherung der Vertraulichkeit, da Einwegfunktion).
- Kollisionen sind möglich, da sehr großer Definitionsbereich auf kleineren Wertebereich abgebildet wird.
- Um Kollisionsresistenz und die Einweg-Eigenschaft zu erreichen, muss Länge der Hashwerte groß sein (mindestens 28 Oktetts empfohlen).

BEISPIEL FÜR KRYPTOGRAPHISCHE HASHFUNKTION

- **SHA-224** (Secure Hash Algorithm 224 Bit)
  - Länge des Hashwerts: 224 Bit (28 Oktetts)

TECHNISCHE UNIVERSITÄT DARMSTADT

IT-SICHERHEITSMAßNAHMEN

KRYPTOGRAPHISCHE PROTOKOLLE

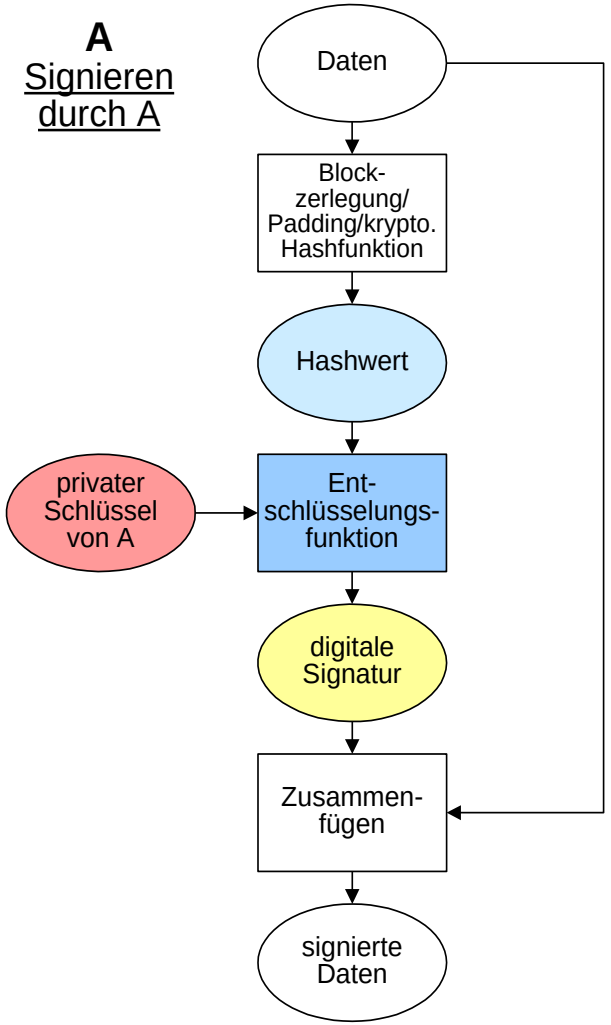
DIGITALE SIGNATUR

- Daten
  - die anderen Daten beigefügt oder mit ihnen logisch verknüpft sind
  - zum Nachweis der Authentizität und Integrität
  - mit einem asymmetrischen Verschlüsselungsverfahren erzeugt und überprüfbar

} elektronische Signatur im Sinne der eIDAS-(Electronic Identification, Authentication and Trust Services) Verordnung (EU)

SIGNATUR-ERZEUGUNG

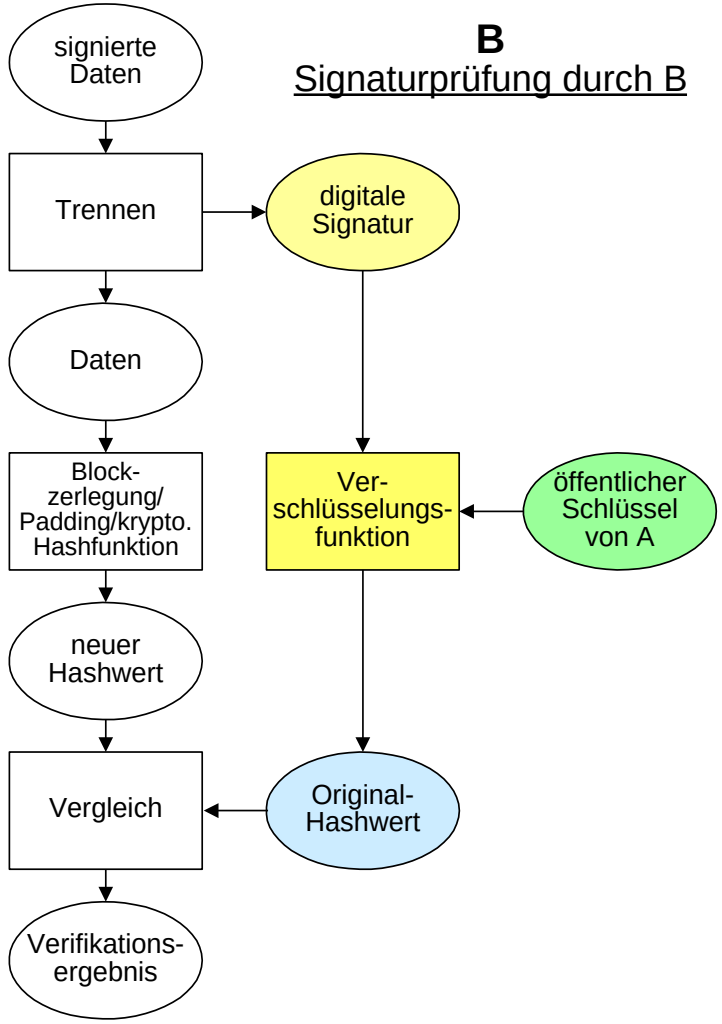
- unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens
  - zur Sicherung der Authentizität
- und einer kryptographischen Hashfunktion
  - zur Sicherung der Integrität
  - Vorteil: Nur relativ kurzer Hashwert wird mit privatem Schlüssel transformiert



SIGNATUR-PRÜFUNG

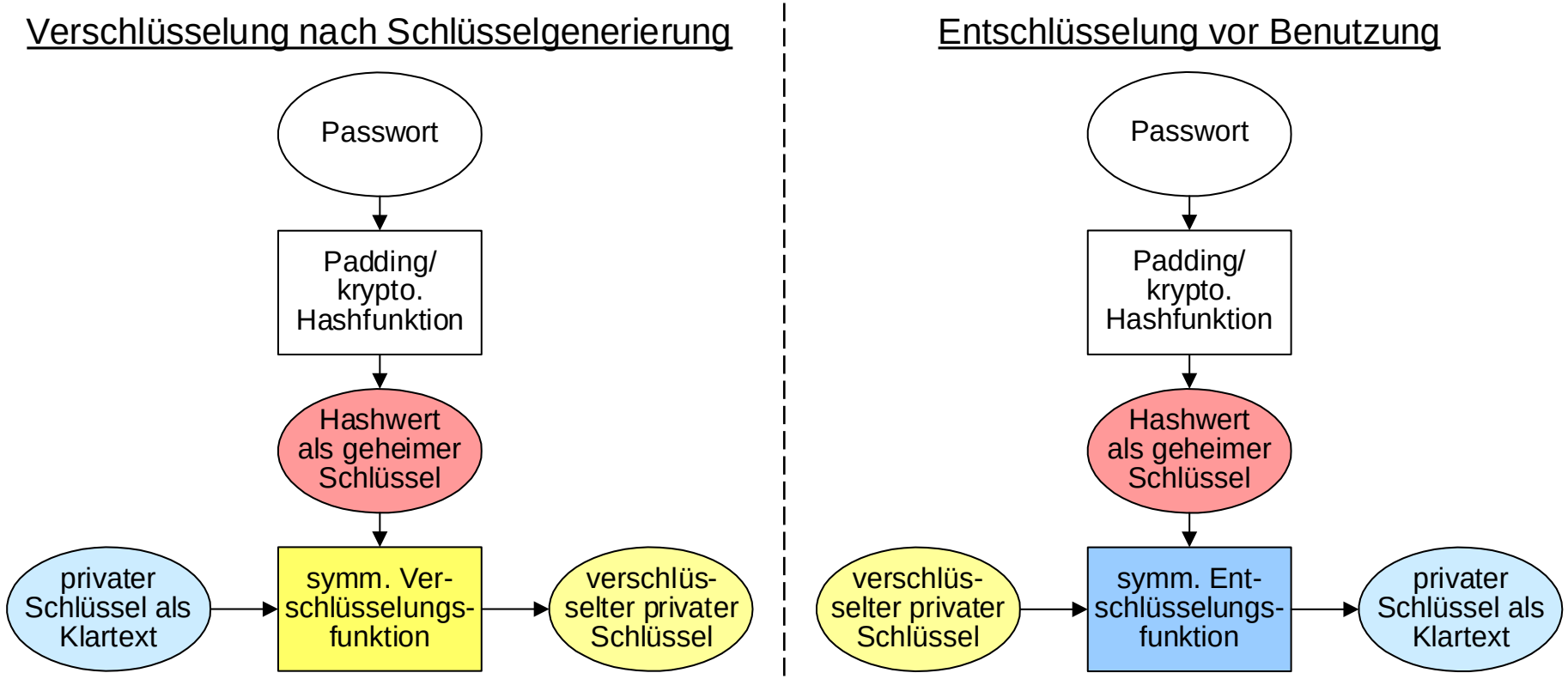
- Wenn neuer Hashwert = Original-Hashwert, dann muss die digitale Signatur
  - mit Hilfe des privaten Schlüssels von A und
  - aus den gleichen Daten

  erzeugt worden sein.



SCHUTZ DER VERTRAULICHKEIT DES PRIVATEN SCHLÜSSELS

- Privater Schlüssel zu lang zum Merken (256 Oktetts empfohlen bei RSA) – muss kryptographisch geschützt oder in Hardware Security Module gespeichert werden

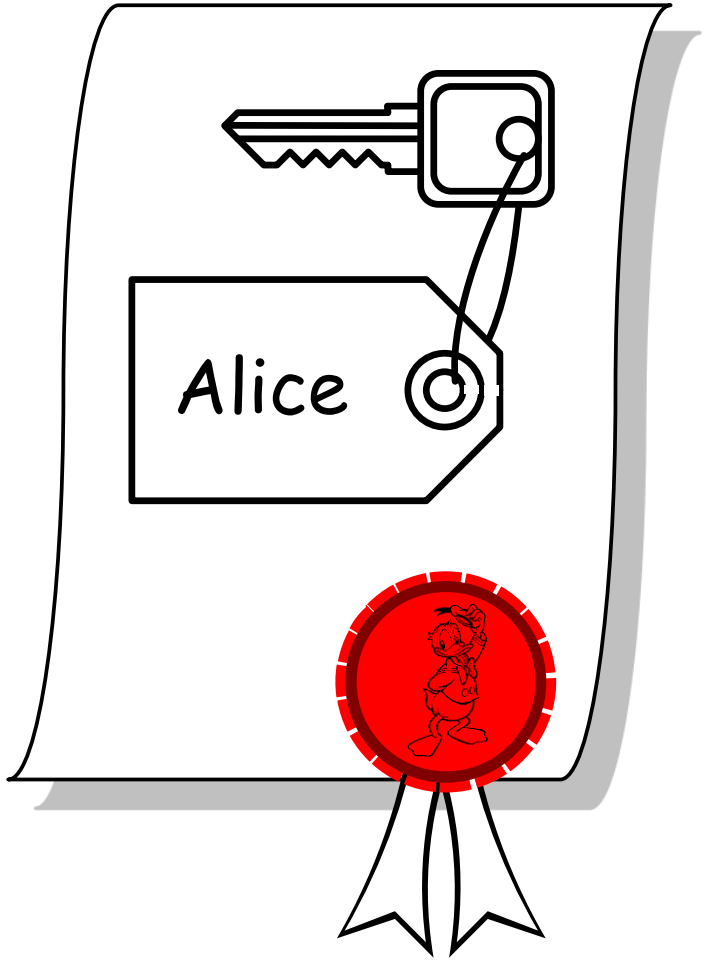


SCHUTZ DER AUTHENTIZITÄT UND INTEGRITÄT DES ÖFF. SCHLÜSSELS

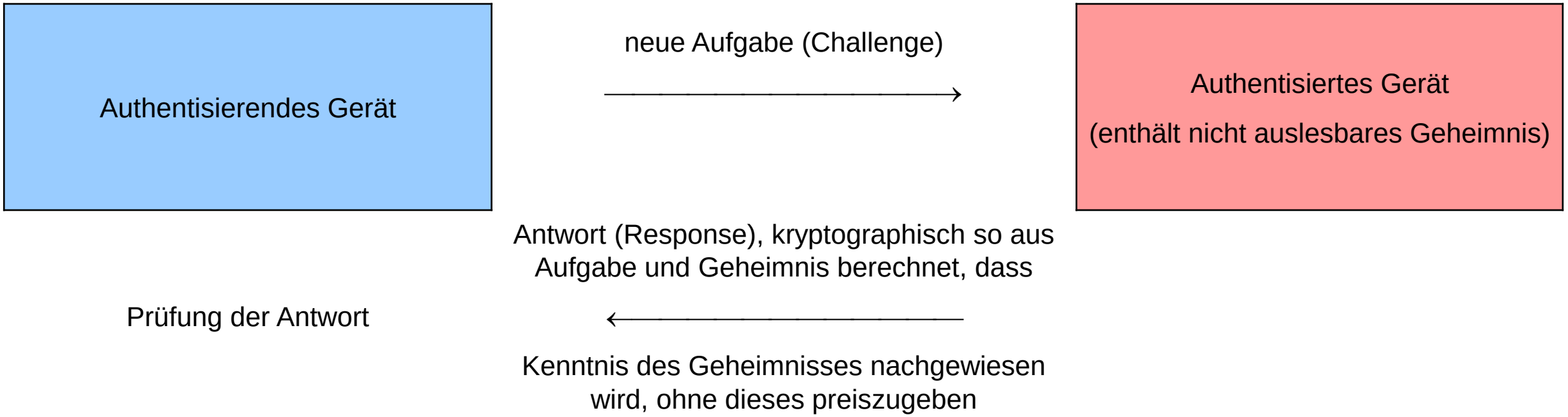
- durch digitale Signatur in einem „Zertifikat“
- nach Schlüsselgenerierung:
  - Signieren des Zertifikats durch
    - einen Zertifizierungsdiensteanbieter (Trusted Third Party) in einer Public-Key-Infrastruktur (PKI) oder
    - andere Benutzer in einem „Web of Trust“ (PGP – Pretty Good Privacy)
- vor Benutzung des öffentlichen Schlüssels:
  - Prüfung der digitalen Signatur des Zertifikats mit Hilfe des öffentlichen Schlüssels des Zertifikatausstellers

ZERTIFIKAT

- elektronische Bescheinigung, mit der ein öffentlicher Schlüssel (und eventuell weitere Informationen) einer Person oder einem Gerät zugeordnet werden
- Inhalt eines Zertifikats
  - öffentlicher Schlüssel
  - Informationen über den Schlüsselinhaber
  - digitale Signatur über den übrigen Zertifikatsinhalt



GERÄTEAUTHENTISIERUNG MIT CHALLENGE-RESPONSE-VERFAHREN



HYBRIDSYSTEME

- Vereinbarung symmetrischer Sitzungsschlüssel aus Zufallszahlen, die mittels asymmetrischer kryptographischer Systeme verschlüsselt zwischen den Kommunikationspartnern ausgetauscht werden

RISIKOANALYSE

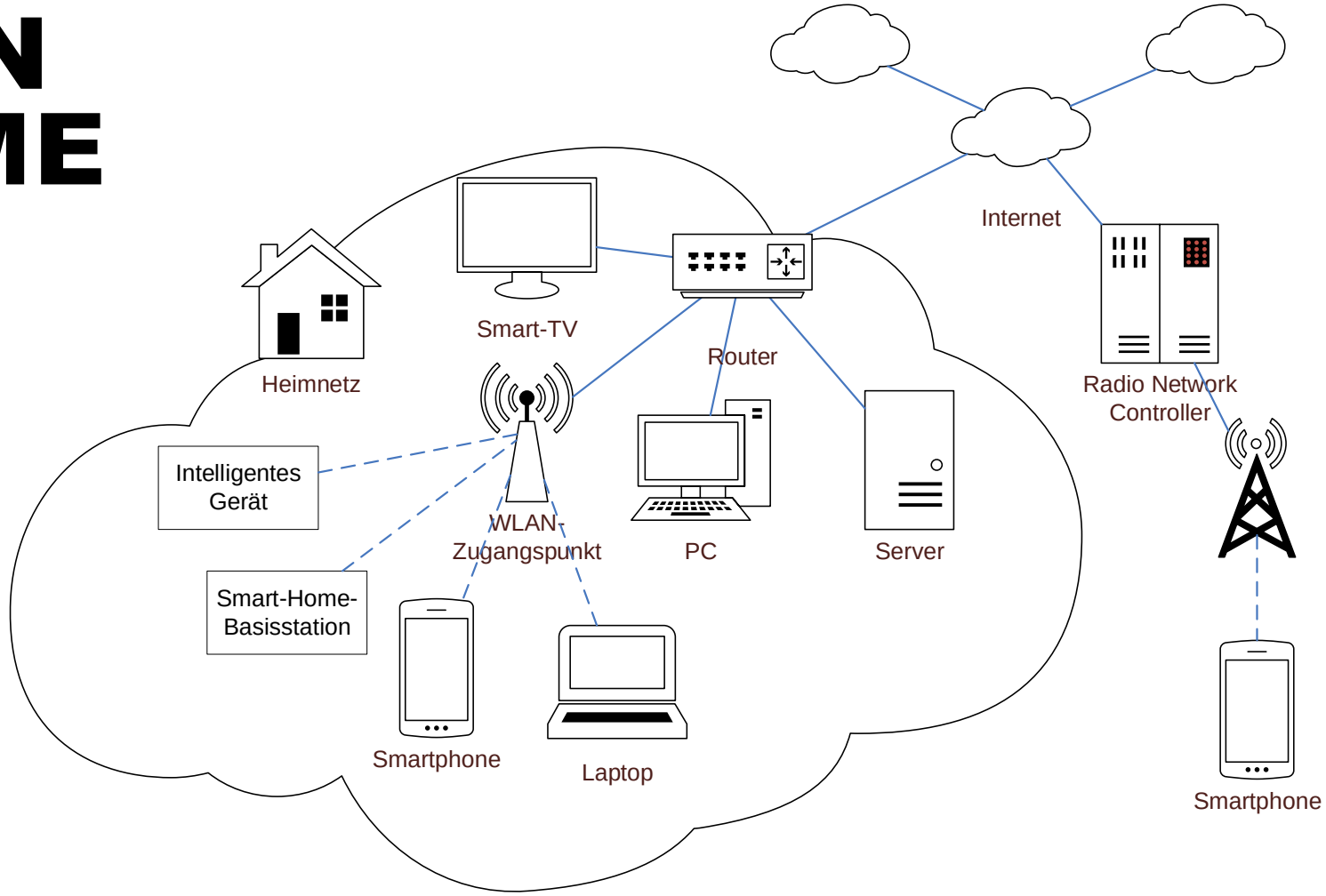
RISIKOANALYSE

- Abwägung: Sicherheit ↔ Kosten und Benutzerfreundlichkeit
  1. Identifikation der zu schützenden Werte
  2. Identifikation der Bedrohungen
  3. Bewertung des Risikos (Eintrittswahrscheinlichkeit von Schadensfällen × Schadenswert)
  4. Auswahl von Gegenmaßnahmen (dabei Balance von Kosten und Risiko beachten)
     - technische Sicherheitsmaßnahmen
     - eventuell Versicherung (bei großem Schadensumfang und kleiner Eintrittswahrscheinlichkeit)
  5. Bewertung des Restrisikos
- Für den Fall normalen Schutzbedarfs gibt es Standard-Sicherheitsmaßnahmen, z.B. im IT-Grundschutzhandbuch des BSI [http://www.bsi.bund.de/gshb].

ANWENDUNG AUF AMI-SYSTEME

BEDROHUNGEN IM SMART-HOME

- z.B.
  - Fernsteuerung durch Unbefugte
  - Verlust der Verfügbarkeit
  - Einbindung in Botnetze
  - Verlust der Privatsphäre / Ausspähen der Wohnung



TECHNISCHE UNIVERSITÄT DARMSTADT

PANIKMACHE?

Security) 7-Tage-News) 11/2019) **Sicherheitsforscher befehligen Alexa, Siri & Co. via Laserstrahl**

heise+ | **heise+** Exklusive Tests, Ratgeber & Hintergründe

Sicherheitsforscher befehligen Alexa, Siri & Co. via Laserstrahl

Angreifer könnten unter Umständen Sprachassistenten in einem Lichtstrahl codierte Befehle unterschieben und so etwa ein smartes Türschloss öffnen.

Internet der Dinge

Das verrät Ihr kaputter Staubsauger noch alles über Sie

Ausrangierte Smarthome-Geräte landen auf eBay-Kleinanzeigen, dem Flohmarkt oder im Müll. Oft haben sie noch viele Daten über ihren Vorbesitzer gespeichert. Ein Hacker hat Dutzende gebrauchte Geräte gekauft - und Erstaunliches gefunden.

HOME » TECH » PAAR ERLEBT HACKERANGRIFF AUF SEINE GOOGLE NEST-KAMERA

Paar erlebt Hackerangriff auf Smart-Home-Geräte — plötzlich sprach ein Mann durch die Google Nest-Kamera zu ihnen

SMART-HOME-BASISSCHUTZ

[https://bsi.bund.de/smarthome]

- Software aktualisieren, wenn Sicherheitsupdates verfügbar
- Keine voreingestellten Standardpasswörter verwenden
- Firewall des Routers aktivieren
- Verschlüsselung der Kommunikation der IoT-Geräte aktivieren und IoT-Geräte nur mit dem Internet verbinden, wenn ein Fernzugriff unbedingt notwendig ist
- VPN für eine gesicherte Verbindung ins Heimnetz nutzen
- Separates WLAN für IoT-Geräte einrichten
- Physischen Zugriff auf Geräte durch Dritte verhindern
- Risiken, die mit der Nutzung von IoT-Geräten einhergehen können, bedenken

LERNZIELE

LERNZIELE

- Was für Bedrohungen sind AmI-Systeme ausgesetzt?
- Was für IT-Sicherheitsziele gibt es?
- Was für IT-Sicherheitsmaßnahmen gibt es in AmI-Systemen?
- Wie können geeignete IT-Sicherheitsmaßnahmen ausgewählt werden?