Datensicherheit

Vorlesung 2: 01.12.2025

Wintersemester 2025/2026 h_da

Heiko Weber, Lehrbeauftragter

Teil 2: Datensicherheit
Themenübersicht der Vorlesung

1. Einführung / Grundlagen / Authentifizierung & Autorisierung
2. Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain
3. Softwaresicherheit / Schadsoftware
4. Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung
5. Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet
6. Datenschutzgesetze / Technische & Organisatorische Maßnahmen
7. Organisationssicherheit / Managementsysteme / Zusammenfassung

Krypto-Begriffe

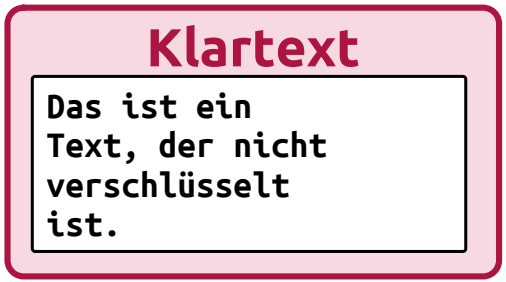
- **Kryptografie**: Methoden zur Ver- und Entschlüsselung
- **Kryptoanalyse**: Bewertung der Stärken und Schwächen von Kryptographie
- **Kryptologie**: Kryptografie + Kryptoanalyse + Methoden für weitere Schutzziele, die aus der Kryptografie hervorgegangen sind wie Stenografie
- **Quanten-Kryptografie**: Ver- und Entschlüsselung mit Quantencomputern (die vermutlich Primfaktorzerlegung und diskrete Logarithmen in überschaubarer Zeit berechnen können)
- **Post-Quanten-Kryptografie (PQC)**: Kryptografie ist so entworfen, dass sie auch resistent gegen Angriffe von Quantencomputern ist

Kryptografische Primitive

- einfache Bausteine, auf denen Kryptografie aufbaut
- Beispiele
  - kryptografisch sichere Hashfunktionen
  - kryptografisch sichere Zufallszahlengeneratoren
  - Block- und Stromchiffreverfahren (Verschlüsselung)
- wenn zugrundeliegende kryptografische Primitive als unsicher gelten, führt das üblicherweise dazu, dass die darauf aufbauenden Kryptoverfahren auch unsicher sind

Klartext / Geheimtext

- **Klartext** = die unverschlüsselten Daten
  - Verschlüsselung wurde ursprünglich nur für Textdaten verwendet, deswegen der Begriff „Klartext“
  - die meisten Verschlüsselungsverfahren können aber für alle Daten verwendet werden, also auch Binärdaten



- **Geheimtext** = die verschlüsselten Daten
  - müssen erst entschlüsselt werden, bevor sie lesbar werden
  - wird auch als „Chiffretext“ bezeichnet

Ver- und Entschlüsselung

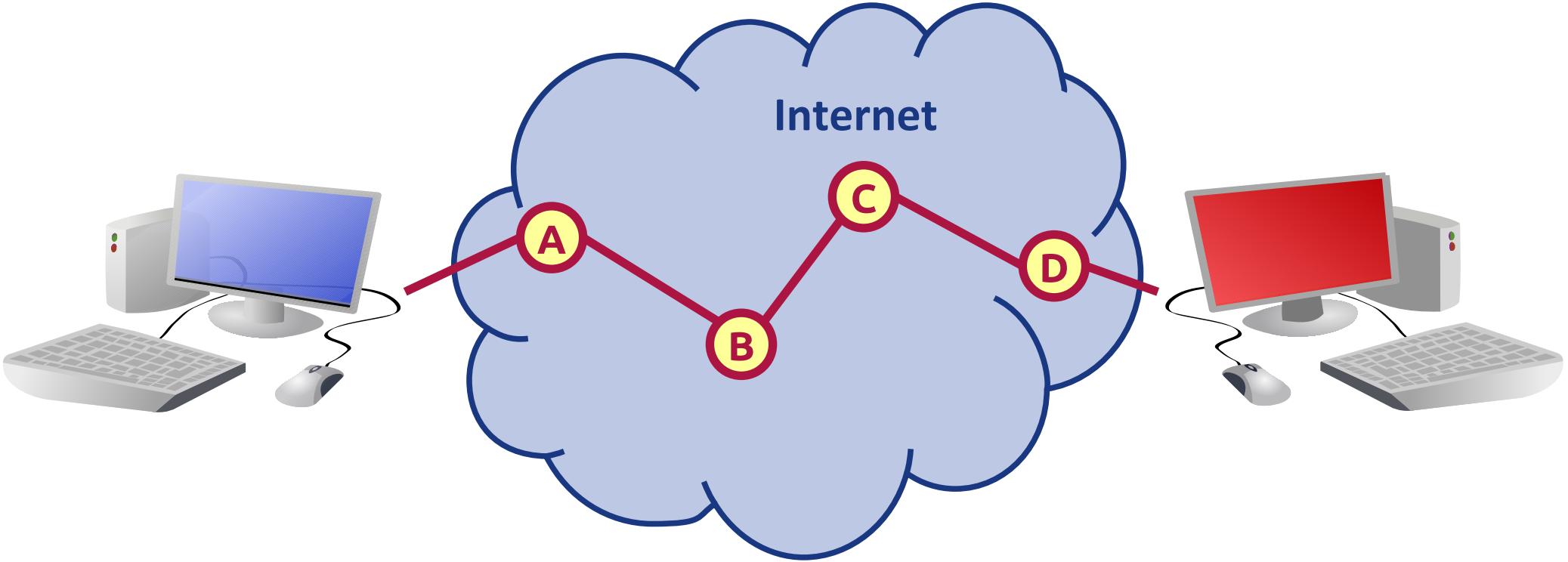
- **Verschlüsselung**

- **Entschlüsselung**

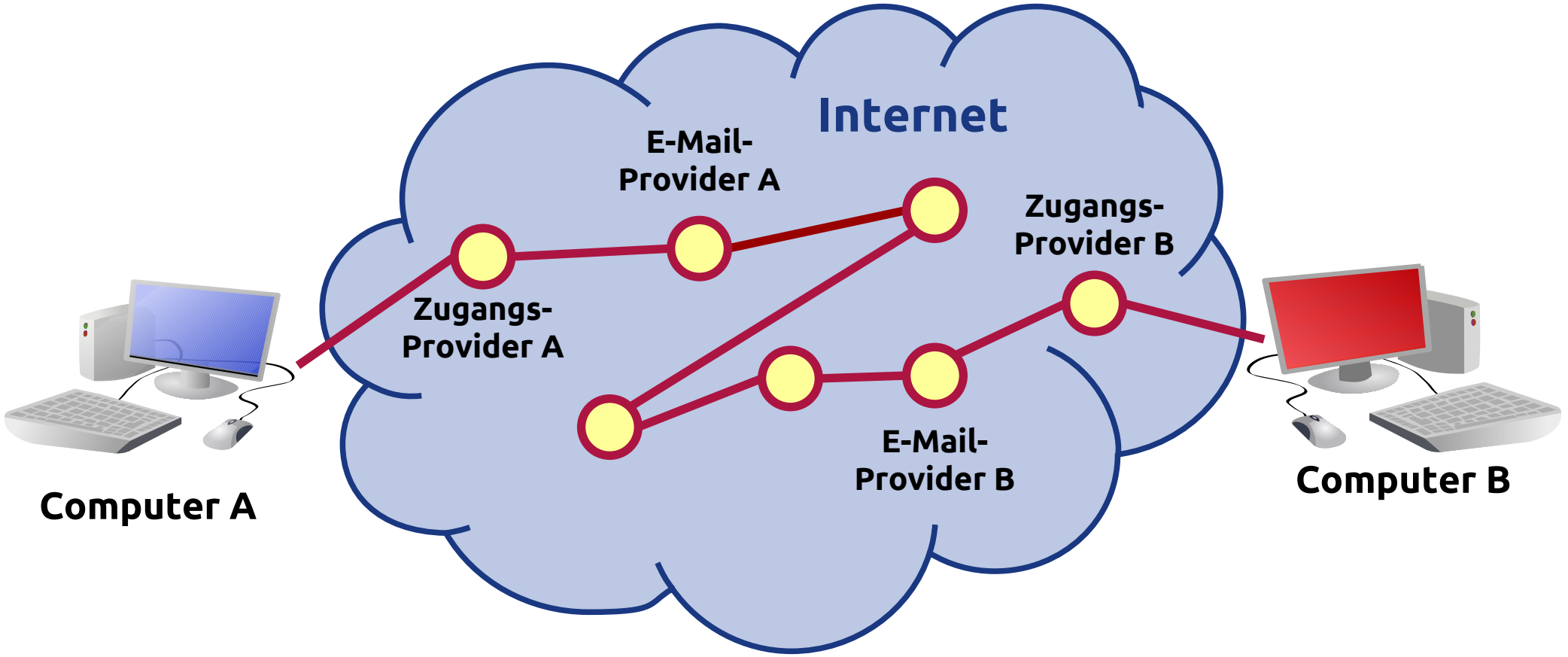
Wieso Verschlüsselung?

- es ist oft nicht möglich, Daten physisch gegen Zugriff zu schützen
  - Festplatten von Laptops
  - USB-Speicher
  - Handy-Speicher
  - ...
- Daten werden oft über unsichere Netzwerke (z. B. das Internet) übermittelt und durchlaufen dabei viele Knoten, auf denen sie mitgehört werden können
  - E-Mails
  - Online-Banking-Daten
  - Online-Shopping-Daten
  - ...

Computer-Internet-Kommunikation



Computer-Kommunikation für E-Mails

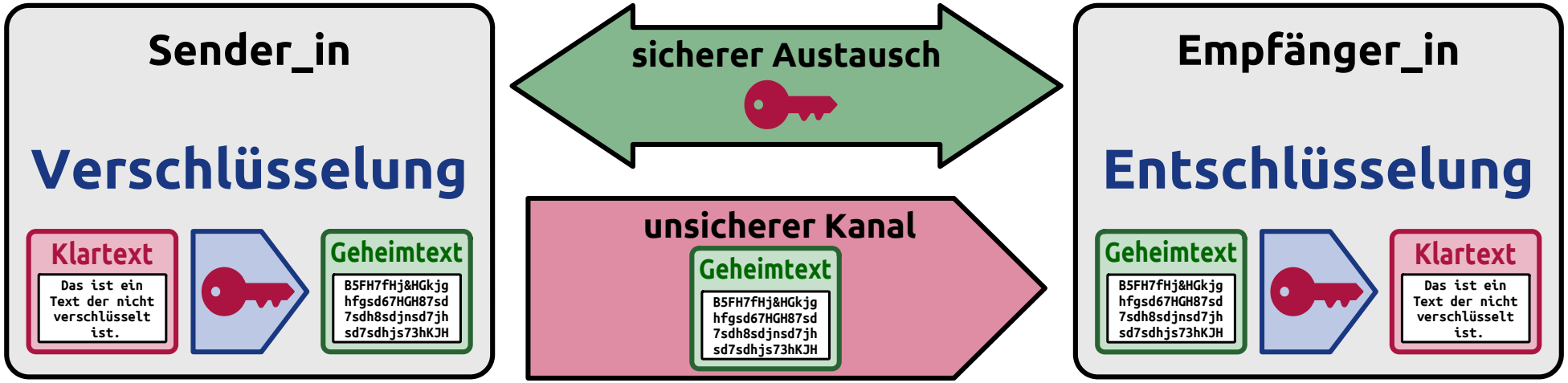


Anforderung an Ver- und Entschlüsselungsverfahren

- Sicherheit darf nicht von der Geheimhaltung des Ver- und Entschlüsselungsverfahrens abhängen!
  - „Security by Obscurity“ ist keine Sicherheit

- das **Kerkhoffs'sche Prinzip:**
  die Sicherheit eines Ver- und Entschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus
- Ver- und Entschlüsselungsverfahren, die heute als sicher gelten, erfüllen das Kerkhoffs'sche Prinzip
- wenn der Schlüssel geheim gehalten wird und der Verschlüsselungsalgorithmus kryptografisch sicher ist, ist der Aufwand des Knackens der Verschlüsselung abhängig von der Schlüssellänge

Symmetrische Verschlüsselung

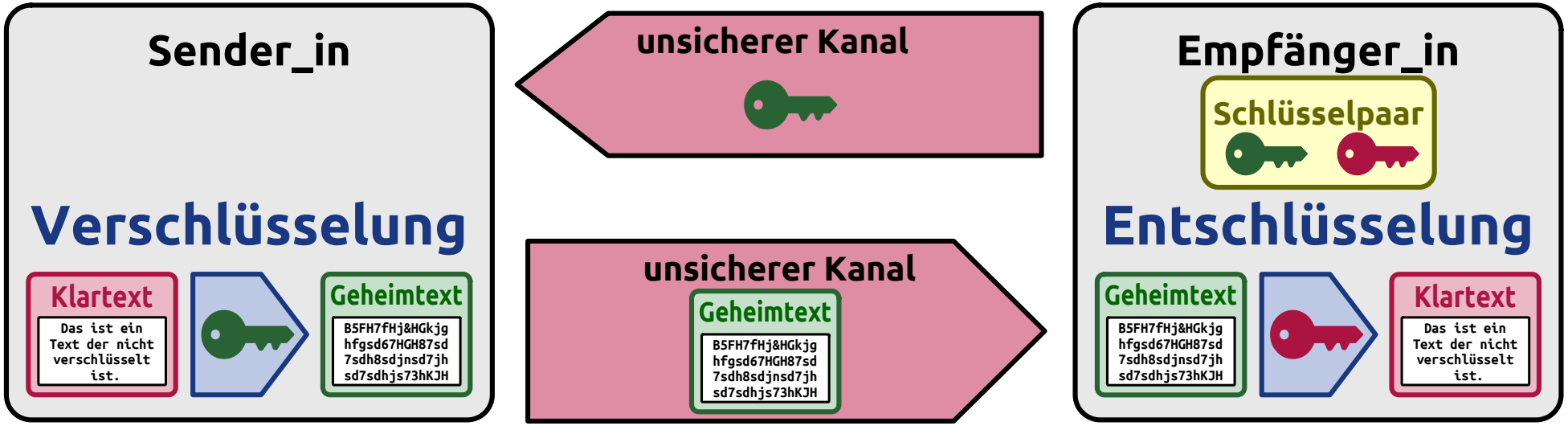


1. über eine sichere Methode wird der geheime Schlüssel ausgetauscht
2. mit dem geheimen Schlüssel wird verschlüsselt
3. über den unsicheren Kanal wird der Geheimtext verschickt
4. mit dem gleichen geheimen Schlüssel wird entschlüsselt

Symmetrische Verschlüsselung

- symmetrisch = ein Schlüssel zur Ver- und Entschlüsselung
- **Vorteile**
  - sehr effizient/schnell
  - wenn die Nachricht für viele Empfänger_innen bestimmt ist, muss sie nur einmal verschlüsselt werden
- **Nachteile**
  - erfordert eine sichere Methode zum Schlüsselaustausch, bevor Nachrichten ausgetauscht werden können
    - z. B. sicherer Kanal oder Schlüsselaustauschverfahren wie Diffie-Hellman
- **Beispiele**
  - A5/1 (GSM), RC4 (HTTPS, SSH1, WEP, WPA), DES, Triple-DES, AES
    DES = Data Encryption Standard, AES = Advanced Encryption Standard

Asymmetrische Verschlüsselung (Public Key)



1. Empfänger_in hat ein Schlüsselpaar (öffentlicher und privater Schlüssel)
2. über einen unsicheren Kanal wird der öffentliche Schlüssel publik gemacht
3. mit dem öffentlichen Schlüssel wird verschlüsselt
4. über den unsicheren Kanal wird der Geheimtext verschickt
5. mit dem geheimen Schlüssel wird entschlüsselt

Asymmetrische Verschlüsselung (Public Key)

- asymmetrisch = ein Schlüssel zum Verschlüsseln und ein anderer Schlüssel zum Entschlüsseln
- **Vorteile**
  - kein Schlüsselaustausch über sicheren Kanal notwendig
  - Sender_in entscheidet, für welche_n Empfänger_in die Nachricht bestimmt ist
- **Nachteile**
  - aufwändiger/langsamer als symmetrische Verschlüsselung
  - wenn eine Nachricht für mehrere Empfänger_innen bestimmt ist, muss sie für alle Empfänger_innen gezielt verschlüsselt werden
- **Beispiele**
  - RSA, ElGamal

Asymmetrische Verschlüsselung und Quantencomputer

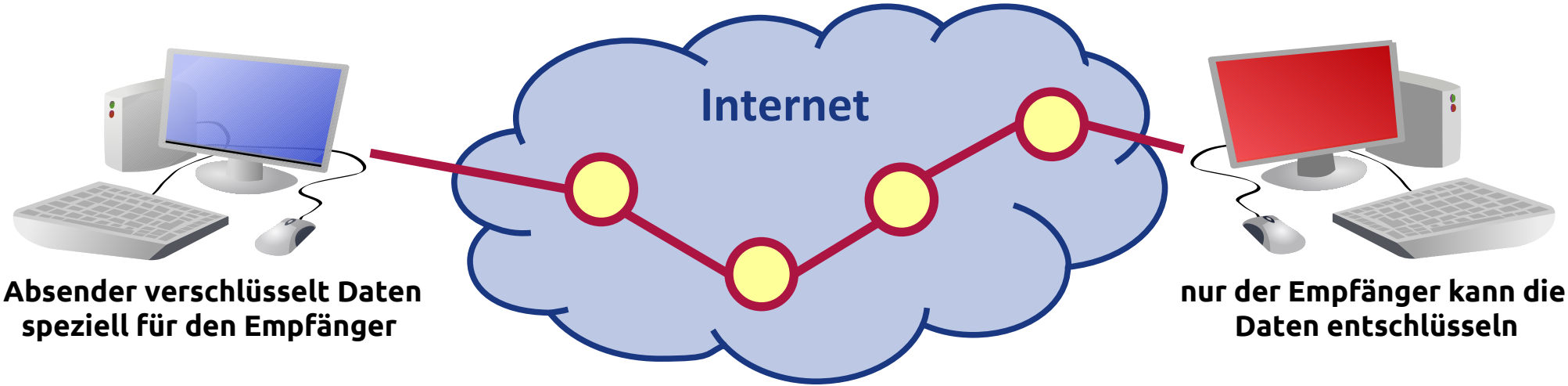
- Die aktuell gängigen asymmetrischen Verschlüsselungsverfahren basieren auf dem Prinzip, dass normale Computer die mathematische Aufgabe einer Primfaktorzerlegung von sehr großen Zahlen und der Berechnung von diskreten Logarithmen nur sehr langsam lösen können.
- Quantencomputer können diese mathematische Aufgabe vermutlich viel schneller lösen. Das bedeutet, dass die heute eingesetzten asymmetrischen Verschlüsselungsverfahren nicht mehr sicher sein werden, wenn Quantencomputer einen gewissen Reifegrad erreicht haben.
- Das National Institute of Standards and Technology (NIST) hat deswegen 2016 einen Wettbewerb gestartet, bei dem aus der Forschung ein neuer Standard für eine quantensichere asymmetrische Verschlüsselung erarbeitet werden soll. Aktuell gibt es noch keine Entscheidung über den neuen Standard.
- Am 23. August 2024 hat die NIST die finalen Version der ersten drei Post-Quanten-Kryptoverfahren veröffentlicht.
  Weitere Infos dazu unter: https://csrc.nist.gov/projects/post-quantum-cryptography
- Für symmetrische Verschlüsselungsverfahren stellen Quantencomputer keine Bedrohung dar.

Hybride Verschlüsselungsverfahren

- asymmetrische Verschlüsselungsverfahren sind wesentlich langsamer und erfordern mehr Rechenleistung als symmetrische, deswegen sind sie für größere Datenmengen nicht geeignet
- symmetrische Verschlüsselungsverfahren bringen den Vorteil, dass sie keinen vorher geteilten Schlüssel erfordern
- **Ziel**
  - Vorteile von symmetrischer und asymmetrischer Verschlüsselung kombinieren
- **hybrider Ansatz**
  - symmetrischer Schlüssel mit asymmetrischem Verfahren verschlüsselt
  - Daten mit symmetrischen Verfahren verschlüsselt
- wird zum Beispiel bei PGP und S/MIME für E-Mail-Verschlüsselung verwendet

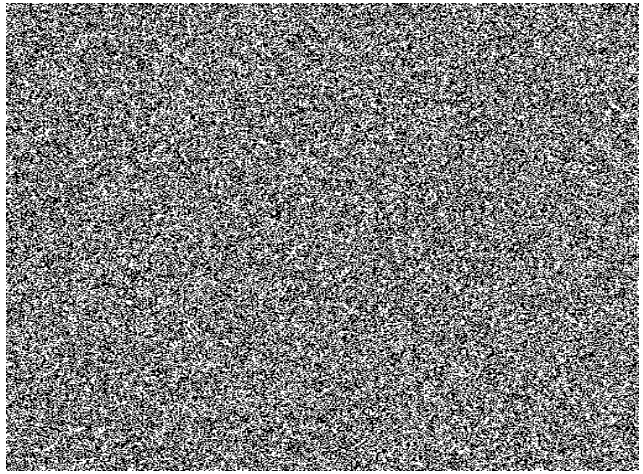
Ende-zu-Ende-Verschlüsselung

- wenn der Sender die Daten verschlüsselt und erst der Empfänger sie wieder entschlüsseln kann, wird von Ende-zu-Ende-Verschlüsselung gesprochen
- bietet ein hohes Maß an Vertraulichkeit
- Problem: Aus Sicherheitsgründen müssen Daten analysiert werden, bevor der Empfänger sie nutzt (z. B. um Schadsoftware oder Phishing-Angriffe zu erkennen)
- mehr dazu in dersung 4 zu Netzwerksicherheit

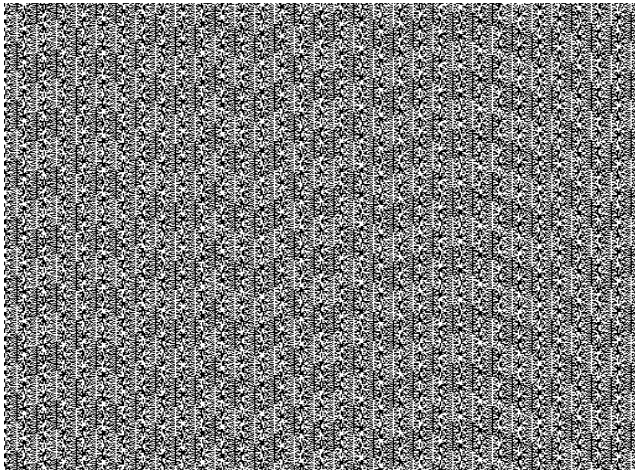


Zufallszahlen

- die meisten Krypto-Verfahren basieren auf der Annahme, dass gute Zufallszahlen erzeugt werden können
- Computer können keine echten Zufallszahlen erzeugen, sondern nur Pseudozufallszahlen



echte Zufallszahlen



Rand()-Funktion eines Computers

Hash-Funktionen

- Analogie: Fingerabdrücke für Daten
- im Idealfall eine Einwegfunktion, die aus beliebig großen Eingabedaten einen fixen Wert (Hashwert) berechnet
- effizient berechenbar
- unterschiedliche Eingabewerte sollen zu unterschiedlichen Ausgabewerten führen
  - ist real nicht möglich, weil für beliebig große Eingabewerte ein Ausgabewert mit einer fixen Länge berechnet wird
  - möglichst wenige Kollisionen sollen auftreten
- Beispiele
  - MD5, SHA (Secure Hash Algorithm), RIPEMD - *MD = Message Digest*
  - für Kryptografie aktuell sehr verbreitet: SHA-256 und SHA-512

Asymmetrische Verschlüsselung (Public Key)

Schlüsselpaar

Öffentlicher Schlüssel

Privater Schlüssel

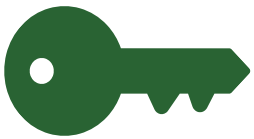
Verschlüsselung mit öffentlichem Schlüssel
Entschlüsselung mit privatem Schlüssel

FOLGENDES GEHT AUCH!
Verschlüsselung mit privatem Schlüssel
Entschlüsselung mit öffentlichem Schlüssel

Prinzip hinter Digitalen Signaturen

Digitale Signaturen

- basieren auf asymmetrischer Verschlüsselung
- geheimer Schlüssel zum Signieren
- öffentlicher Schlüssel zum Überprüfen der Signatur
- gängige Verfahren
  - RSA PSS (Probabilistic Signature Scheme)
  - DSA (Digital Signature Algorithm)
  - ECDSA (Elliptic Curve Digital Signature Algorithm)



Um die Signatur zu überprüfen, wird der öffentlicher Schlüssel der signierenden Person benötigt.

Zertifizierungsstelle für Digitale Zertifikate

- Englisch: Certificate Authority (CA)
- Organisation, die digitale Zertifikate herausgibt
- Zuordnung eines digitalen Zertifikats zu einer Person oder Organisation wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Signatur versieht
- weltweit eine Reihe von Zertifizierungsstellen, die berechtigt sind offiziell Zertifikate zu Beglaubigen, denen dann von gewissen Anwendungen (z. B. Web-Browsern oder E-Mail-Programmen) automatisch vertraut wird

Probleme bei Krypto

- Krypto nicht eingesetzt, wo es notwendig wäre
- falsche/unsichere Krypto eingesetzt
  - unpassende Algorithmen
  - unsichere Algorithmen
  - unsichere Implementierung der Algorithmen
- Krypto falsch eingesetzt
  - falsch konfiguriert
  - unbrauchbar, so dass sie nicht benutzt wird
- sichere Krypto in unsicherem System eingesetzt
  - „schwächere“ Angriffspunkte existieren, um die Krypto zu umgehen

Schutzziele der Datensicherheit

Vertraulichkeit		Daten dürfen nur von Berechtigten **gelesen** werden
Verfügbarkeit		Daten müssen für Berechtigte **zugänglich** sein
Integrität		Daten dürfen nur von Berechtigten **erstellt**, **verändert** und **gelöscht** werden
Authentizität		Daten sind vom **angegebenem Ursprung**
Nichtabstreitbarkeit		Inhalte von Daten sind so **beabsichtigt**, wie angegeben

Schutzziele der Datensicherheit

Vertraulichkeit

Verfügbarkeit

Integrität

Authentizität

Nichtabstreitbarkeit

Schutzziele der Datensicherheit

Verschlüsselung

- **Vertraulichkeit**
- Verfügbarkeit
- Integrität
- Authentizität
- Nichtabstreitbarkeit

Schutzziele der Datensicherheit

Digitale Zertifikate

- wird genutzt, um eine Entität (Person, Organisation, Webseite oder weitere Ressource) zu identifizieren
- beinhaltet ein Schlüsselpaar (öffentlicher und privater Schlüssel)
- beinhaltet Informationen über die Entität – zum Beispiel:
  - bei einer Person: den Namen und ggf. die E-Mail-Adresse
  - bei einer Webseite: den Domain-Namen und weitere Informationen über die Webseite
- öffentlicher Schlüssel wird genutzt, um zu überprüfen, dass die Daten wirklich von Zertifikatsinhaber_in kommen
- privater Schlüssel wird von Zertifikatsinhaber_in genutzt, um die Daten zu signieren

Vertrauen (Trust)

- Digitale Signaturen und Digital Zertifikate werden genutzt, um Vertrauen aufzubauen
- wenn Inhalte von einer vertrauenswürdigen Quelle kommen, sind die Inhalte in der Regel auch vertrauenswürdig
- Zertifizierungsstellen sind eine vertrauenswürdige Stelle, deswegen kann den Zertifikaten vertraut werden, wenn sie von einer Zertifizierungsstelle beglaubigt wurden
- die Schutzziele *Integrität*, *Authentizität* und *Nichtabstreitbarkeit* können nur erreicht werden, wenn Vertrauen in die Daten und Datenquellen aufgebaut werden kann

Zero Trust-Modell

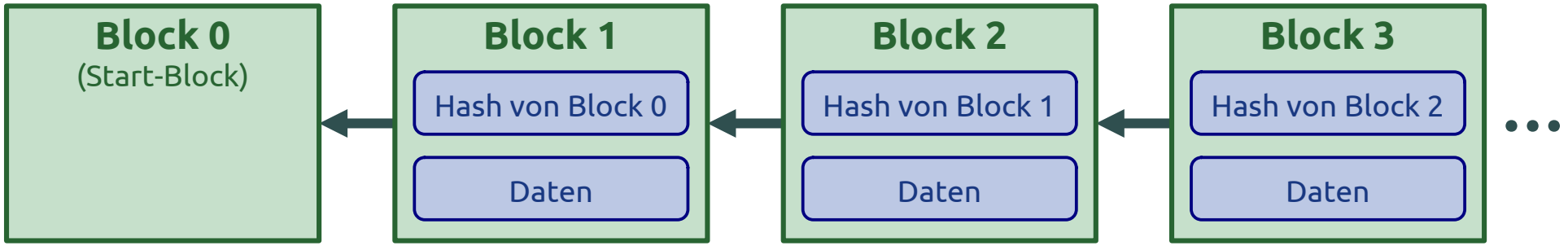
- **Probleme bei Vertrauen**
  - Moderne IT-Infrastrukturen sind extrem komplex und umfangreich.
  - Viele Systeme werden miteinander vernetzt, die oft auch nicht unter der eigenen Kontrolle stehen.
  - Daten werden in externen Systemen verarbeitet oder gespeichert.
  - Externe Personen/Organisationen benötigen Zugriff auf interne Netzwerke.
  - Auch sehr gut gesicherte Systeme sind niemals komplett frei von Sicherheitslücken.
  - Moderne Arbeitsweisen erfordern, dass Mitarbeiter/innen von zuhause oder unterwegs aus arbeiten und teilweise private IT-Ressourcen (Computer, Drucker, Smartphones, …) nutzen.
- **Vertrauen wird immer schwieriger > Zero Trust-Modell**
  - Das Zero Trust-Modell geht davon aus, dass jede Komponente im Gesamtsystem eventuell unsicher sein könnte – auch in internen Netzwerken. Deshalb werden alle Zugriffe und sonstige Aktionen so geprüft, als kämen sie von einer unsicheren Quelle.
  - Es gilt das Prinzip: Vertrauen ist gut, Kontrolle ist besser.
  - Es wird davon ausgegangen, dass nicht alle Sicherheitsvorfälle verhindert werden können, aber diese möglichst gut und schnell erkannt werden sollten, damit darauf reagiert werden kann.

Zero Trust-Prinzipien

- **Umfangreiche Kontrolle**
  - Alles wird überwacht – auch interne Systeme, die eigentlich vertrauenswürdig sein sollten.
  - Anomalien müssen möglichst automatisiert erkannt werden.
    > Security Information and Event Management (SIEM)
- **Prinzip der geringsten Berechtigung**
  - Bei allen Zugriffsberechtigungen wird genau geschaut, dass sie das absolut erforderliche Minimum sind.
  - Es gibt möglichst keine Administrationsberechtigungen, die alles erlauben.
- **Systematische Reaktion auf Vorfälle**
  - Wenn ein Sicherheitsvorfall eintritt, müssen konkrete Vorgehensweisen vorhanden sein, um
    - den Sicherheitsvorfall möglichst schnell zu stoppen,
    - die Ausbreitung des Sicherheitsvorfalls auf möglichst wenige Systeme zu begrenzen und
    - alle betroffenen Daten und System zuverlässig wieder herzustellen.

Blockchain

- Technologie zum Herstellen von Vertrauen ohne zentrale Vertrauensstelle
- Kette von Blöcken – die Blöcke enthalten zwei Arten von Informationen:
  - beliebige Daten (können auch verschlüsselt abgelegt werden)
  - Informationen, um die Integrität der Kette sicherzustellen (Hash-Wert des Vorgänger-Blocks)
- Manipulationssicherheit gewährleistet durch
  - Verteilung von Kopien der Kette auf mehrere Speicherorte (Distributed Ledger)
  - Konsensverfahren: Proof of Work / Proof of Stake



Einsatzbereiche für Blockchain-Technologien

- Kryptowährungen
- NFTs (Non-Fungible Tokens)
- Onlinewahlen
- Protokolle / Audit-Nachweise
- Verträge bis hin zu Smart Contracts
- ...