# Inhalt der Vorlesung „Rechnerkommunikation“

- Einführung
- Anwendungsschicht
- Transportschicht
- Netzwerkschicht
- Sicherungsschicht
- Physikalische Schicht

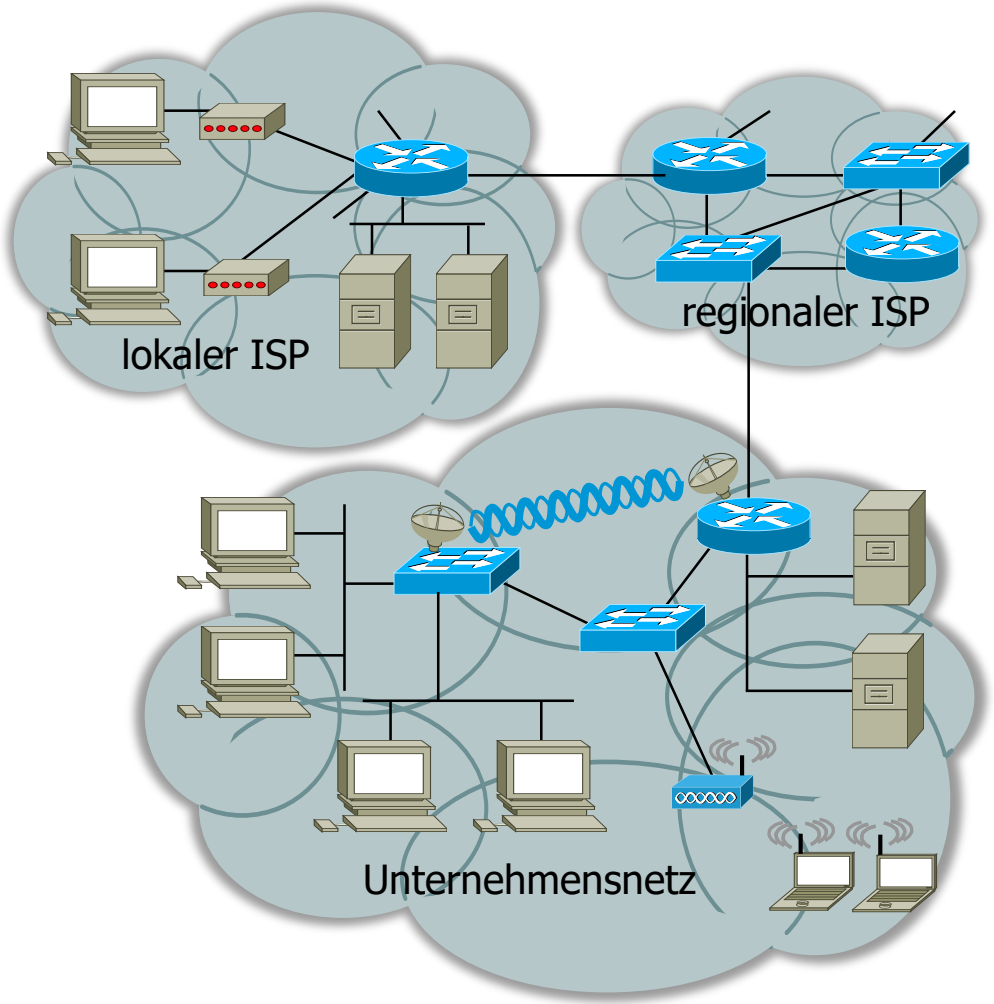
# Einführung

- Beispiele für Rechnerkommunikation
- Konzept der Lehrveranstaltung
- Klassifikation von Kommunikationssystemen
- Protokolle
- Netzwerksicherheit
- Geschichte
- Literatur

# Beispiele für Rechnerkommunikation

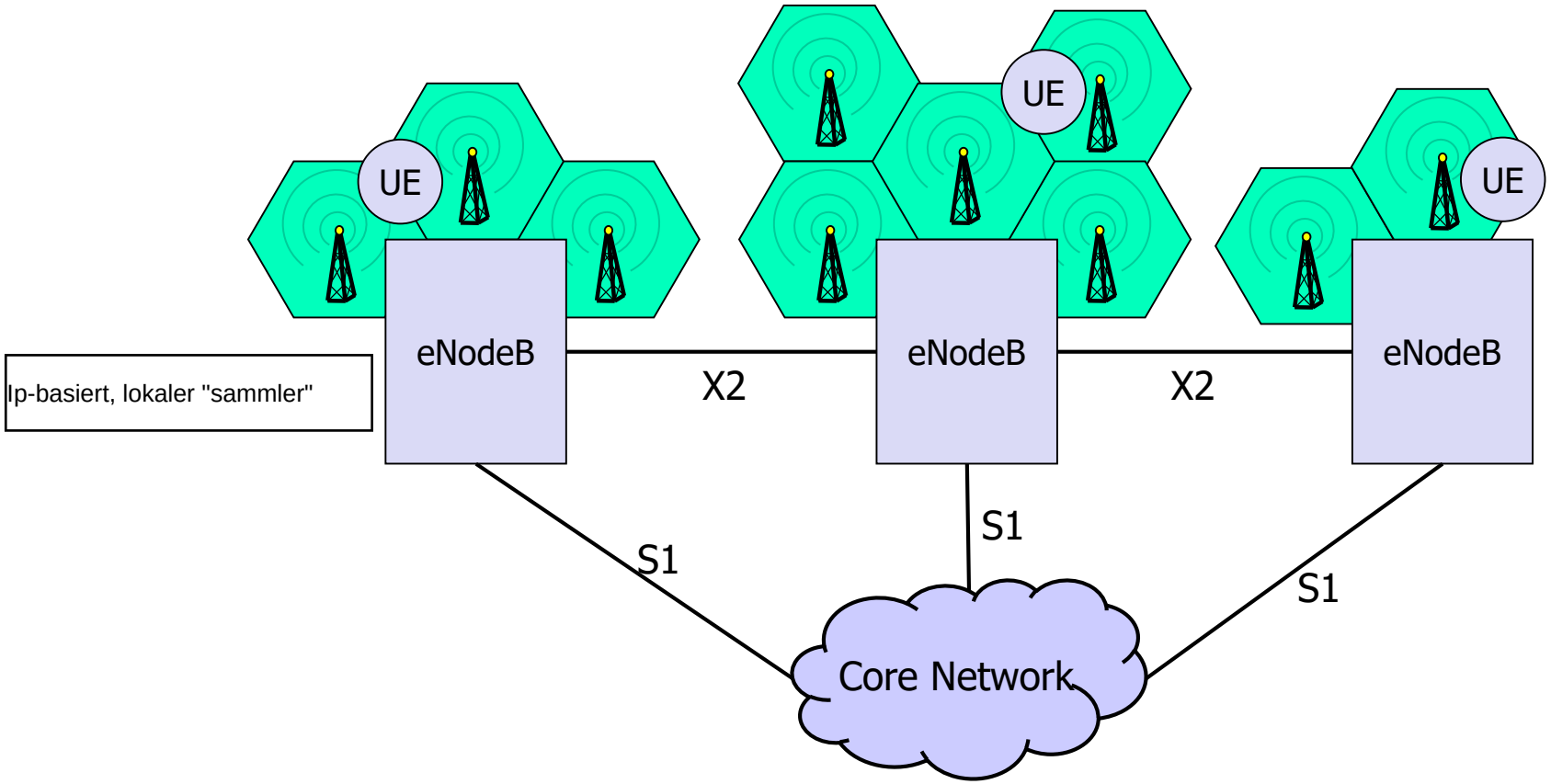
- IP-Netz (Internet)
  - Kommunikation zwischen Anwendungen auf Endsystemen (Host, Server)
  - Verwendung von Internet-Protokollen (u.a. TCP, UDP, IP) und weiteren (z.B. Ethernet, WLAN)
  - Infrastruktur besteht u.a. aus Vermittlungseinheiten (Router, Switches, WLAN Access Points)
  - leitungsgebundene und drahtlose Verbindungen
  - Unterscheidung von Zugangsnetz und Kernbereich
  - Internet Service Provider (ISP)

Lokal vs Isp-Netze




Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

# Beispiele für Rechnerkommunikation




Quelle: Jochen H. Schiller, Vorlesungsunterlagen "Mobile Communications", FU Berlin

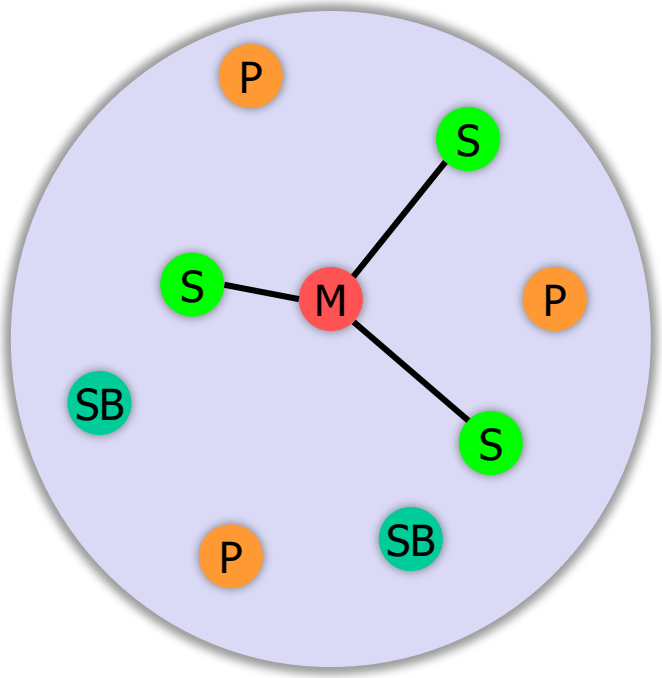
- Long Term Evolution (LTE)
  - mobile Telekommunikation der 4. Generation
  - Mobilstation (User Equipment), Radio Access Network (OFDM)
  - Evolved Packet Core (EPC) basierend auf IP

e.g. Handy

# Beispiele für Rechnerkommunikation

Quelle: Jochen H. Schiller, Vorlesungsunterlagen "Mobile Communications", FU Berlin

- Bluetooth
  - Bsp. für Wireless Personal Area Network (WPAN)
  - verbreitete drahtlose Anbindung von Peripheriegeräten an PC
  - Pikonetz: Ansammlung von Geräten die sich spontan (ad-hoc) vernetzen z.B. Handy zu lautsprecher
  - ein Gerät wird zum Master, die anderen verhalten sich als Slaves
  - Master bestimmt Frequenzsprungfolge, Slaves müssen dieser folgen
  - Kommunikation immer Master ↔ Slave IMMER sternförmig
  - Verbindungen für Daten und Sprache, diverse Konfigurationsmöglichkeiten

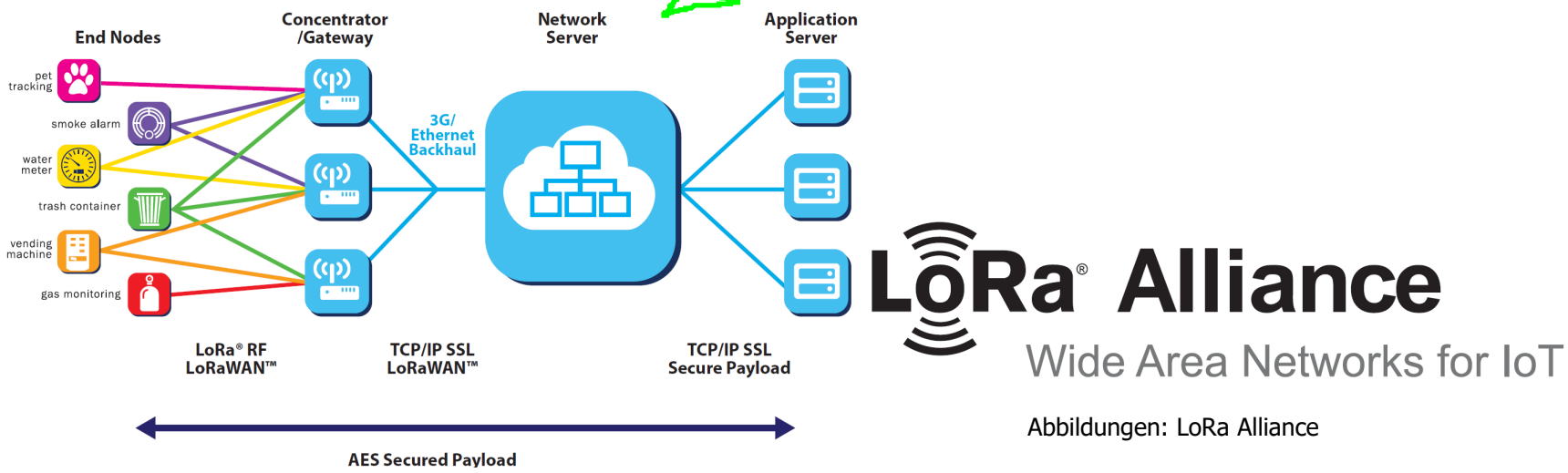



M: Master P: Parked
S: Slave SB: Standby

# Beispiele für Rechnerkommunikation

- Long Range Wireless Area Network (LoRaWAN)
  - Low-Power Wide-Area Network (LPWAN) im ISM-Band (868 MHz)
  - Internet-of-Things (IoT)-Anwendungen
  - niedrige Datenraten (bis 50 Kbit/s)
  - hohe Reichweite (bis 10 km)
  - Chirp Spread Spectrum mit unterschiedlichen Spreizfaktoren
  - verschlüsselte Daten

Wasser, Gaß, Stromzähler, Rauchalarme, Haustiere




LoRa® Alliance
Wide Area Networks for IoT

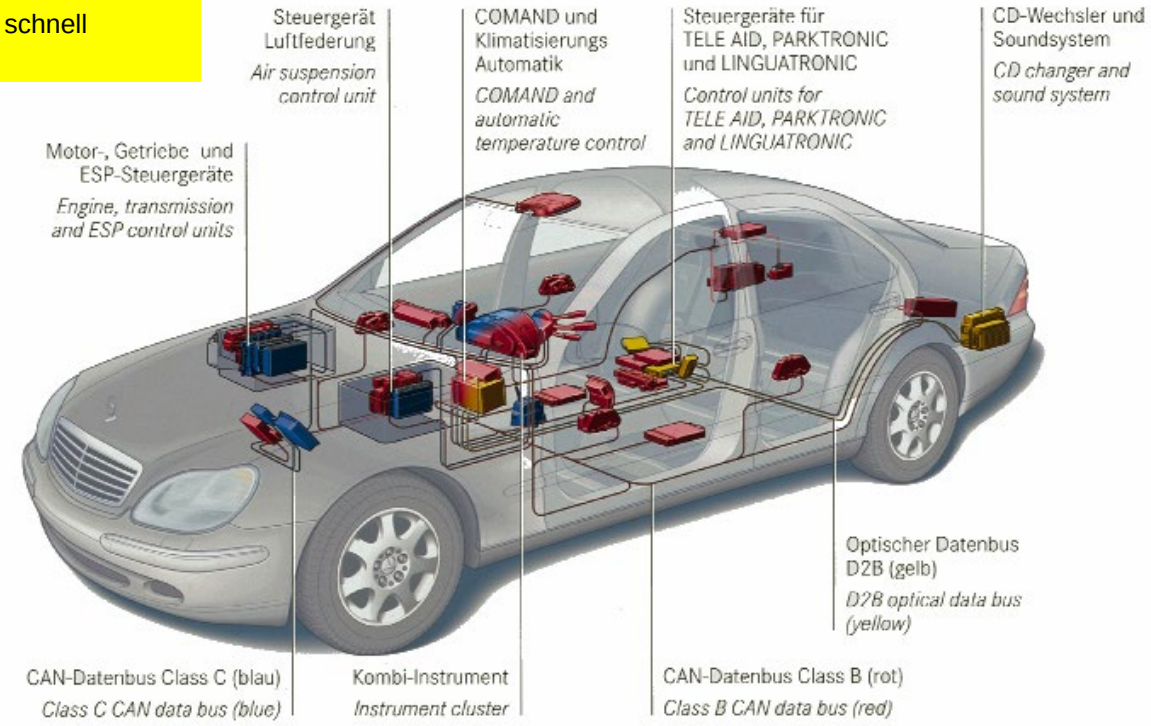
Abbildungen: LoRa Alliance

# Beispiele für Rechnerkommunikation

- Vernetzung im Fahrzeug
  - heutige Mittelklasse- und Oberklasse-Fahrzeuge besitzen ca. 60 bis 100 elektronische Steuergeräte (Electronic Control Units, ECUs) für Antriebsstrang, Fahrerassistenz, Komfort, Infotainment (aber Tendenz zu weniger Steuergeräten)
  - Controller Area Network (CAN) verbreitetes Bussystem zur Kommunikation
  - besondere Anforderungen an Zuverlässigkeit, Echtzeit
  - auch „Vehicle-to-Anything" über Mobilfunk

Immer und schnell

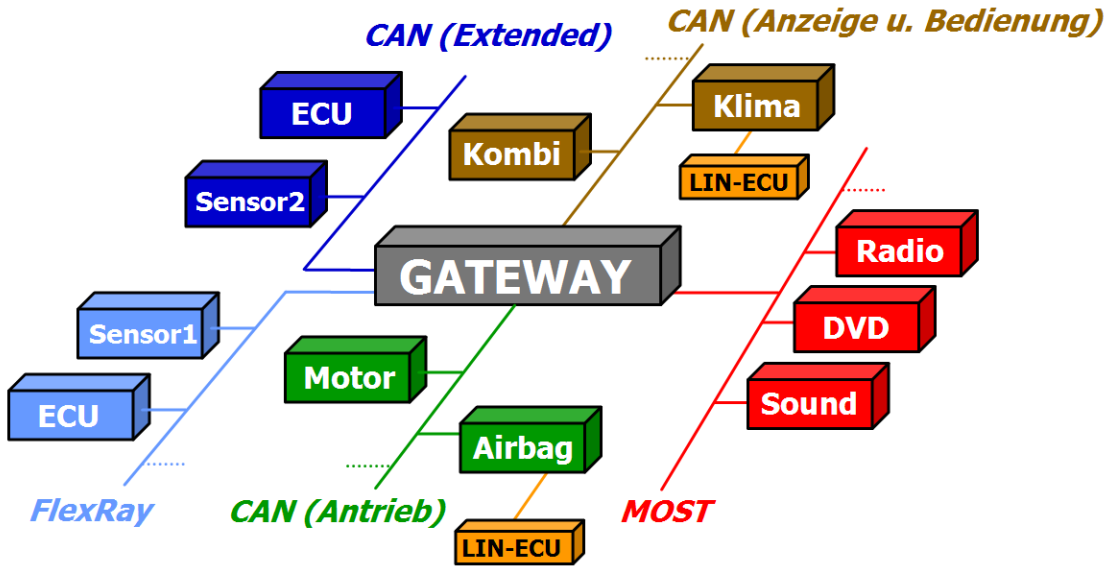
Kommunikation auf die Umgebu




Quelle: Daimler

# Beispiele für Rechnerkommunikation

- Beispielhafte Vernetzungsarchitektur im Fahrzeug
  - zentrales Gateway
  - Anschluss der ECUs über mehrere CAN-Busse und weitere Bussysteme (z.B. FlexRay mit höheren Raten, MOST mit noch höheren Raten für Infotainment, Automotive Ethernet)
  - an ECUs weitere Busse, z.B. Local Interconnect Network (LIN)
  - „Informatik in der Fahrzeugtechnik“ Master spezialisierung
  - INI.FAU
    INGOLSTADT INSTITUTE DER FRIEDRICH-ALEXANDER-UNIVERSITÄT ERLANGEN-NÜRNBERG



# Beispiele für Rechnerkommunikation

- Gemeinsame Aspekte trotz Technologievielfalt
  - Netztopologie: Anordnung der Kommunikationsgeräte
  - Hierarchisierung in Protokollschichten, Beschreibung von Nachrichtenformaten und Protokollverhalten
  - Adressierung, Wegesuche und Weiterleitung von Nachrichten Routing
  - Flusskontrolle: Steuerung der Senderate, ohne Empfänger zu überlasten
  - Überlastkontrolle: Steuerung der Senderate, um das Netz vor Überlast zu schützen
  - Fehlersicherung: Ausgleich von Bitfehlern und Verlusten
  - Medienzugriff: Koordination des Zugriffs mehrerer Sender auf gemeinsames Medium
  - Bitübertragung: Kodierung und Modulation
  - Netzwerksicherheit: Verschlüsselung, Authentifizierung etc.
  - Leistung: erreichbare Durchsätze und Verzögerungszeiten
  - Zuverlässigkeit: Wahrscheinlichkeit von Verlusten und Ausfällen

# Einführung

- ✓ Beispiele von Rechnernetzen
- Konzept der Lehrveranstaltung
- Klassifikation von Kommunikationssystemen
- Protokolle
- Netzwerksicherheit
- Geschichte
- Literatur

# Konzept der Lehrveranstaltung

- Nutzen von Rechnernetzen
  - Zugriff auf entfernte Informationen Webbrowsing
  - Informationsaustausch Email
  - Steuerung entfernter Geräte smartphone fernsteuerung, SSH
  - gemeinsame Nutzung von Betriebsmitteln Drucker
  - Leistungssteigerung und Fehlertoleranz google Compute cloud, Failover zu anderen Computern

- Bedeutung von Rechnernetzen
  - starkes Wachstum von Anzahl und Nutzung in den letzten 20 Jahren
  - Basistechnologie, Infrastruktur für alle Lebensbereiche:
    Büro, Verwaltung, Bildung, Unterhaltung, E-Commerce, Telearbeit, Fertigung, Straßenverkehr, elektrisches Energiesystem, weitere kritische Infrastrukturen, eingebettete Geräte, Internet der Dinge, …
  - Netzwerk- und andere Industrie: Entwerfen, Entwickeln, Installieren, Betreiben, Verwalten der HW und SW von Rechnernetzen
  - viele Produkte benötigen Kommunikation
  - viele SW-Programme benötigen Kommunikation

# Konzept der Lehrveranstaltung

- Bedeutung des Internets
  - globales Netz von Rechnernetzen
  - größtes und wichtigstes Rechnernetz
  - Konversion zu Internet-Technologien

Handy: whatsapp statt SMS

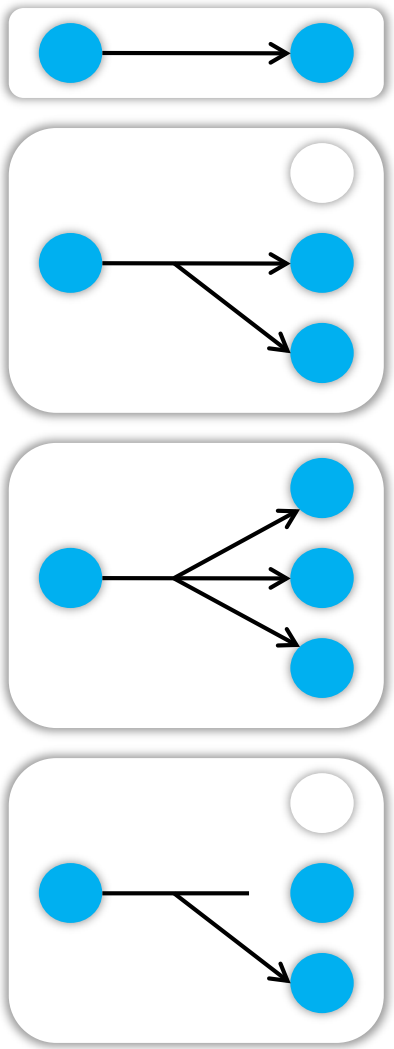
- Inhalt von Rechnerkommunikation
  - Netzwerke werden am Beispiel des **Internets** untersucht
  - die **Schichten** werden dabei von oben nach unten durchlaufen (Anwendungsschicht, Transportschicht, Netzwerkschicht, Sicherungsschicht, physikalische Schicht)
  - dabei werden **grundlegende Mechanismen** von Rechnernetzen behandelt
  - **analytische Ansätze** zur Auslegung
  - **Netzwerksicherheit** als übergreifender Aspekt
  - Vertiefung durch Programmierübungen und theoretische Übungen

# Einführung

- ✓ Beispiele von Rechnernetzen
- ✓ Konzept der Lehrveranstaltung
- Klassifikation von Kommunikationssystemen
- Protokolle
- Netzwerksicherheit
- Geschichte
- Literatur

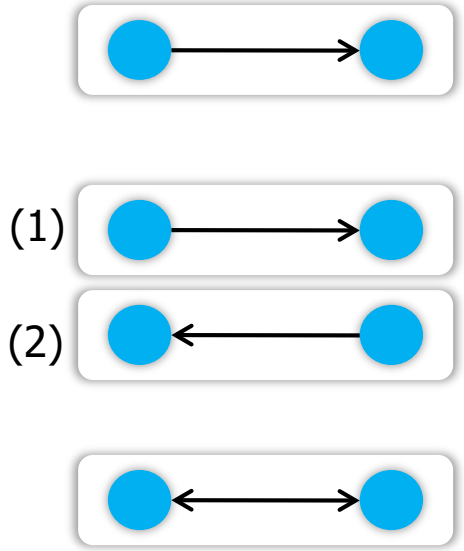
# Klassifikation von Kommunikationssystemen

- Einige Unterscheidungsmerkmale …
- Kommunikationsart
  - Unicast (Punkt-zu-Punkt): ein Sender, ein Empfänger meistens
  - Multicast (Punkt-zu-Mehrpunkt, Gruppenruf): ein Sender, ein Gruppe von Empfängern medienteilung auf viele Nutzer
  - Broadcast (Rundruf): an alle Teilnehmer des Netzes nur lokal, sonst überla
  - Anycast: ein Empfänger aus einer Gruppe möglicher Ziele Z.B. DNS server: einer Reicht



# Klassifikation von Kommunikationssystemen

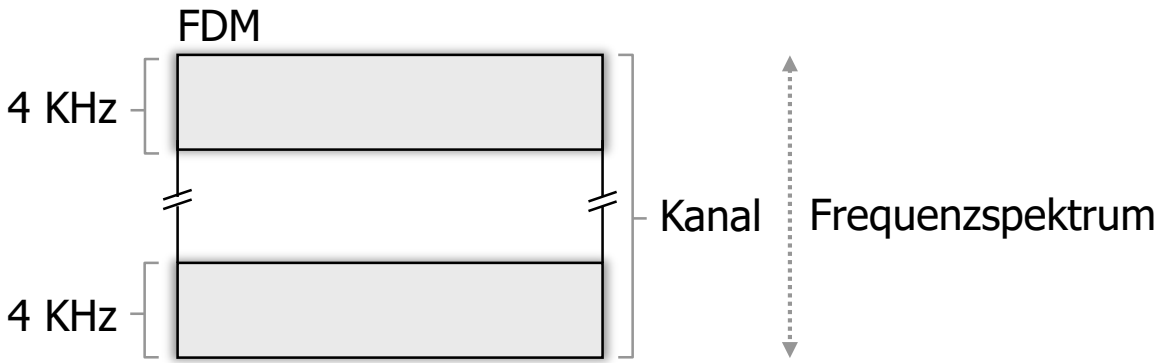
- Übertragungsart
  - Übertragungsrichtung
    - simplex: unidirektionale Verbindung
    - halbduplex: bidirektionale Verbindung mit Umschalten, also nicht gleichzeitig in beide Richtungen
    - (voll-)duplex: gleichzeitig in beide Richtungen

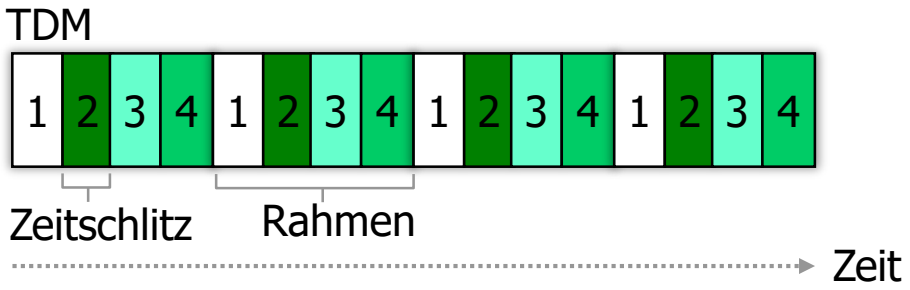


# Klassifikation von Kommunikationssystemen

- Multiplexverfahren: Verwendung eines physikalischen Mediums durch mehrere Geräte
  - Frequenzmultiplex (Frequency Divsion Multiplex, FDM): Geräte verwenden verschiedene Teile des Frequenzspektrums Viele Frequenzen über Glasfaser
  - Zeitmultiplex (Time Divsion Multiplex, TDM): Geräte wechseln sich zeitlich ab

Bus-systeme




Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

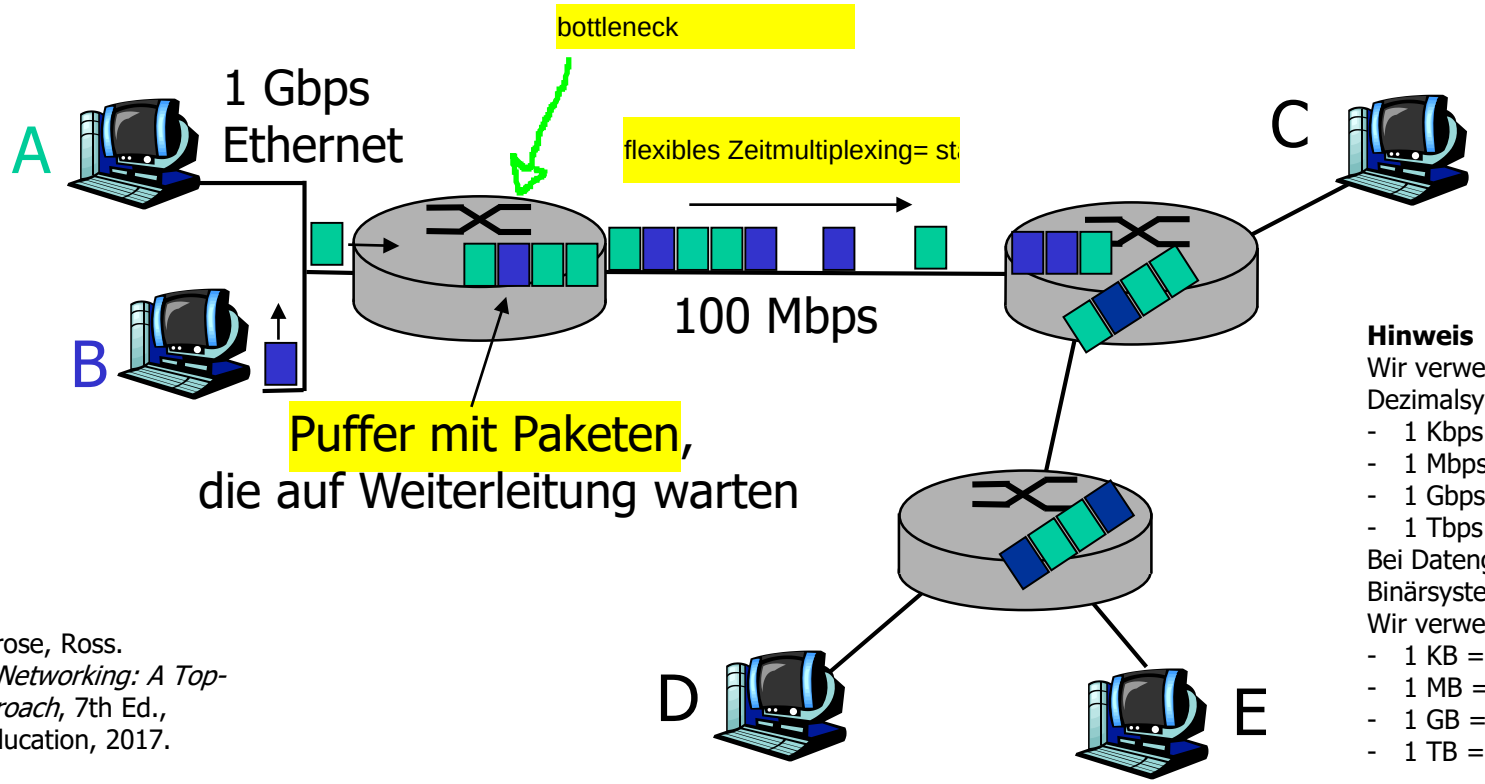
Rahmen= Wiederholungsperiodizität

# Klassifikation von Kommunikationssystemen

- Vermittlungsart
  - Leitungsvermittlung
    - zwischen Sender und Empfänger wird mittels Signalisierung ein Kanal zur Übertragung aufgebaut (z.B. durch Zeit- oder Frequenzmultiplex)
    - die zur Verfügung stehende Bitrate muss fest auf die Kanäle aufgeteilt werden bis vor kurzem standard in Tel
    - bis vor Kurzem Standardverfahren in der Telefonie, bei schwankenden Datenaufkommen mit vielen Pausen ineffizient keine dynamische bitrate->man verliert datendurchsatz
  - Paketvermittlung
    - Sender schickt Daten in Paketen, die einzeln zum Empfänger gelangen
    - die Bitrate wird effizienter aufgeteilt
    - kurzfristiges höheres Datenaufkommen kann über Puffer abgefangen werden höhere Latenz, oder overflow
    - dies kann zu Verzögerungen und Pufferüberläufen führen

# Klassifikation von Kommunikationssystemen

- Statistisches Multiplexen
  - vergleicht man Paketvermittlung mit den bei der Leitungsvermittlung bekannten Multiplexverfahren, so erscheint diese wie statistisches Multiplexen




Quelle: Kurose, Ross.
*Computer Networking: A Top-Down Approach*, 7th Ed.,
Pearson Education, 2017.

**Hinweis**
Wir verwenden für Datenraten immer Angaben im Dezimalsystem:
- 1 Kbps = $10^3$ Bits pro Sekunde
- 1 Mbps = $10^6$ Bits pro Sekunde
- 1 Gbps = $10^9$ Bits pro Sekunde
- 1 Tbps = $10^{12}$ Bits pro Sekunde

Bei Datengrößen sind Angaben sowohl im Binärsystem als auch im Dezimalsystem verbreitet. Wir verwenden, falls nicht anders angegeben:
- 1 KB = $2^{10} \cdot 8$ Bits $\approx 10^3 \cdot 8$ Bits
- 1 MB = $2^{20} \cdot 8$ Bits $\approx 10^6 \cdot 8$ Bits
- 1 GB = $2^{30} \cdot 8$ Bits $\approx 10^9 \cdot 8$ Bits
- 1 TB = $2^{40} \cdot 8$ Bits $\approx 10^{12} \cdot 8$ Bits

# Klassifikation von Kommunikationssystemen

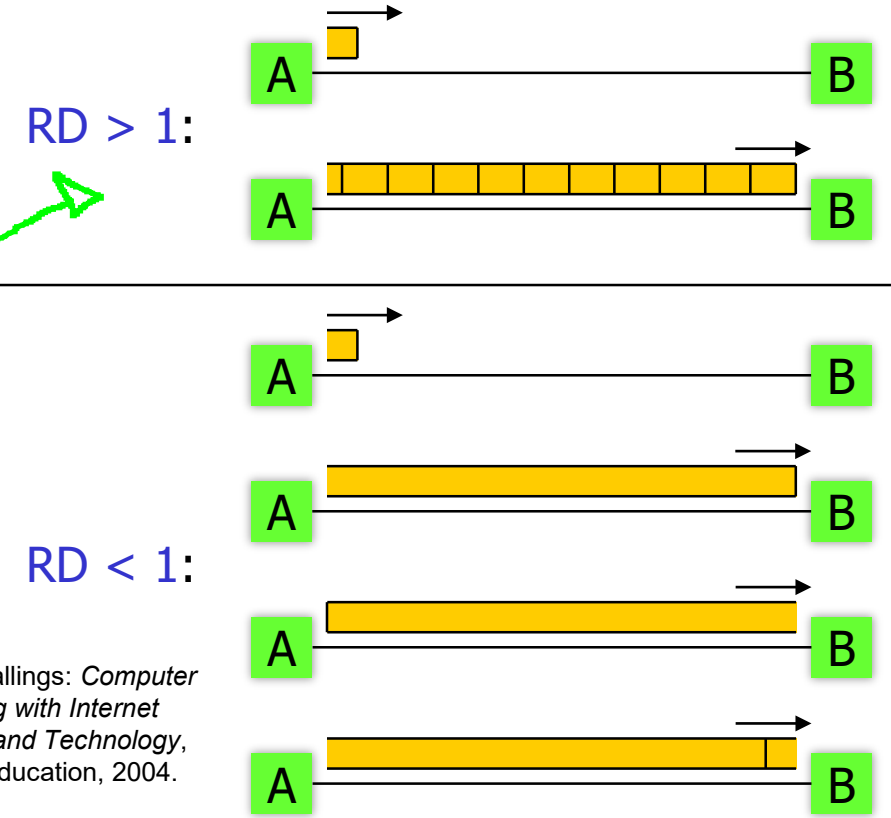
- Übertragungsmedium
  - leitungsgebunden
    - z.B. verdrillte Kupferdrähte, Glasfaser
    - Bitraten von Kbps bis viele Gbps
    - Signalausbreitungsgeschwindigkeit v ist etwas weniger als Lichtgeschwindigkeit c, z.B. 2/3 c ≈ $2 \cdot 10^8$ m/s = 200 m/µs Latenz des Kabels
    - kleine Bitfehlerraten, bei Glasfaser z.B. $10^{-10}$
  - drahtlos wir betrachten nur terrestrisch
    - z.B. Funk (terrestrisch, Satellit), Infrarot, sichtbares Licht
    - Bitfehlerraten hoch wegen verschiedener Probleme bei der Ausbreitung von Funkwellen: $10^{-5}$ bis $10^{-2}$
    - außerdem treten Bitfehler oft in Schüben (Bursts) auf

# Klassifikation von Kommunikationssystemen

- Entfernung
  - Systembusse (z.B. PCI), Peripheriekommunikation (z.B. USB, Bluetooth)
  - lokale Netze (LANs)
    - einige Kilometer, Ausbreitungsverzögerung z.B. 2,5 km/v = 12,5 µs
  - Metropolitan Area Networks (MANs)
    - urbane Region, 50-100 km
  - Wide Area Networks (WANs)
    - weltweit, Ausbreitungsverzögerung z.B. 10.000 km/v = 50 ms
- Bitrate
  - 56 Kbps für Modem bis viele Gbps (Glasfaser, Satellit)
  - Produkt von Bitrate R und Ausbreitungsverzögerung D = l/v ergibt das Datenvolumen auf der Kommunikationsstrecke
    - R = 100 Mbps, l = 2,5 km ⇨ R·l/v ≈ 833 Bits
    - R = 1 Gbps, l = 10.000 km ⇨ R·l/v ≈ 3,97 MB
  - in Kombination mit Fehlersicherung und Medienzugriff relevant für Effizienz

# Klassifikation von Kommunikationssystemen

- Produkt aus Bitrate und Verzögerung
  - Bitrate R, Ausbreitungsverzögerung D vom Sender zum Empfänger
  - einfacher Kanal, A sendet ohne Unterbrechung an B




effektiv wirkt die Leitung als Puffer!

RD ist die anzahl de

Die Pufferungskapazität ist alsoRD*1

Quelle: Stallings: *Computer Networking with Internet Protocols and Technology*, Pearson Education, 2004.

# Klassifikation von Kommunikationssystemen

- Kanalpuffergröße in Bits

$$R \cdot D = \frac{D}{1/R} = \frac{l/v}{1/R} = \frac{Ausbreitungsverzögerung}{Bitsendezeit}$$

= Anzahl gesendeter Bits während sich das erste Bit vom Sender zum Empfänger ausbreitet = Kanalpuffergröße in Bits

- Beispiel für RD > 1:
  - R = 100 Mbps, l = 4800 km, v = $3 \cdot 10^8$ m/s
  - $$RD = 100 \cdot 10^6 \frac{Bits}{s} \cdot \frac{4800 \cdot 10^3 m}{3 \cdot 10^8 m/s} = 1600 \cdot 10^3 Bits \approx 195 KB$$
- Beispiel für RD < 1:
  - R = 10 Mbps, d = 10 m, v = $2 \cdot 10^8$ m/s
  - $$RD = 10 \cdot 10^6 \frac{Bits}{s} \cdot \frac{10 m}{2 \cdot 10^8 m/s} = 0{,}5 Bits$$

# Klassifikation von Kommunikationssystemen

- Kanalpuffergröße in Paketen
  - mit Paketgröße L:

$$a = \frac{R \cdot D}{L} = \frac{l / v}{L / R} = \frac{Ausbreitungsverzögerung}{Paketsendezeit}$$

= Anzahl gesendeter Pakete während sich das erste Bit vom Sender zum Empfänger ausbreitet = Kanalpuffergröße in Paketen

Wichtig

- einige Werte für a ($v = 3 \cdot 10^8$ m/s):

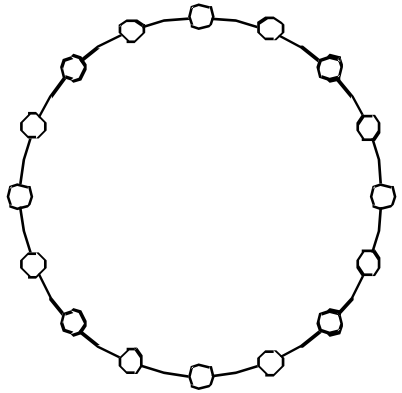
| Bitrate | Paketgröße | Entfernung | a |
|---|---|---|---|
| 500 Kbps | 136 Bits | 10 m | 0,0001 |
| 1 Mbps | 1500 Bytes | 10 m | 0,0000028 |
| 1 Mbps | 1500 Bytes | 1 Km | 0,00028 |
| 1 Mbps | 1500 Bytes | 10 Km | 0,0028 |
| 1 Mbps | 1500 Bytes | 100 Km | 0,028 |
| 1 Mbps | 1500 Bytes | 1.000 Km | 0,28 |
| 1 Mbps | 1500 Bytes | 10.000 Km | 2,8 |
| 1 Mbps | 1500 Bytes | 36.000 Km | 10 |
| 10 Mbps | 1500 Bytes | 10 Km | 0,028 |
| 10 Mbps | 1500 Bytes | 100 Km | 0,28 |
| 100 Mbps | 1500 Bytes | 100 m | 0,0028 |
| 100 Mbps | 1500 Bytes | 10 km | 0,28 |
| 100 Mbps | 1500 Bytes | 1.000 km | 27,8 |
| 1 Gbps | 1500 Bytes | 100 m | 0,028 |
| 1 Gbps | 1500 Bytes | 10 km | 2,8 |
| 1 Gbps | 1500 Bytes | 1.000 km | 277,8 |
| 1 Gbps | 1500 Bytes | 36.000 km | 10.000 |
| 100 Gbps | 1500 Bytes | 100 m | 2,8 |
| 100 Gbps | 1500 Bytes | 10 km | 277,8 |
| 100 Gbps | 1500 Bytes | 1.000 km | 27.777,8 |
| 100 Gbps | 1500 Bytes | 36.000 km | 1.000.000 |

Quelle: Stallings: *Computer Networking with Internet Protocols and Technology*, Pearson Education, 2004.

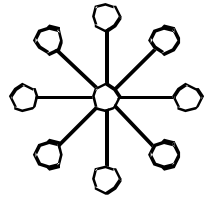
# Klassifikation von Kommunikationssystemen

- Topologie

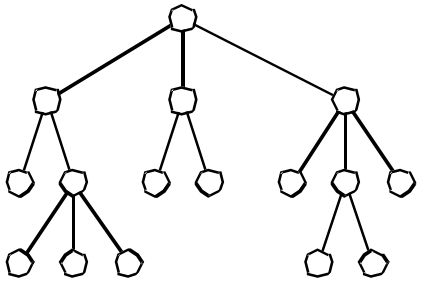
Bus
(linear)



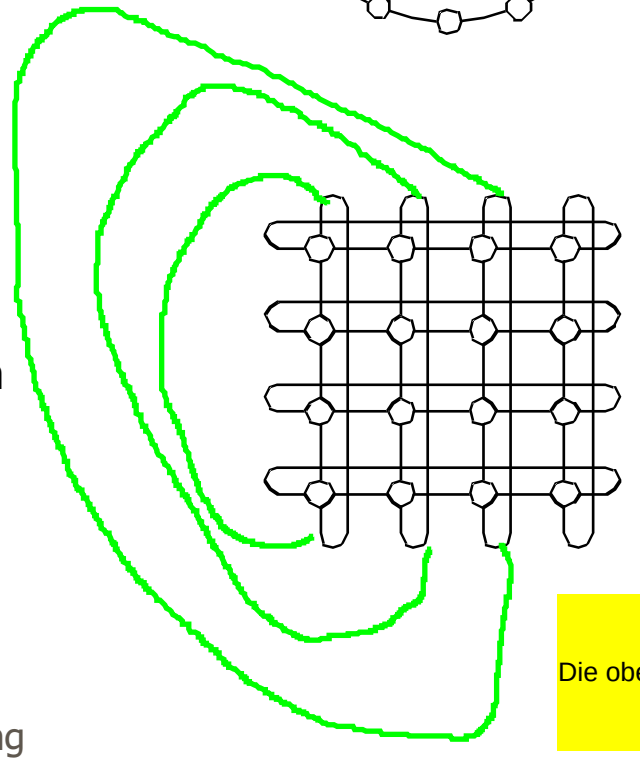
Ring



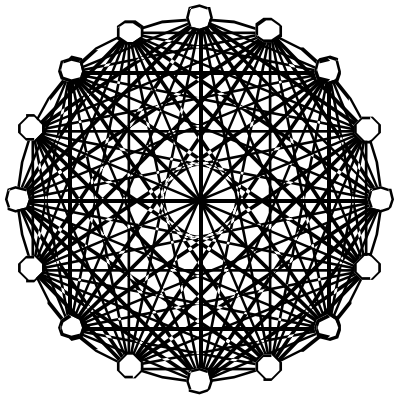
Stern



Baum



2D-Torus



vollständig
vermascht

Die oberen/unteren, bzw linke/rech

# Einführung

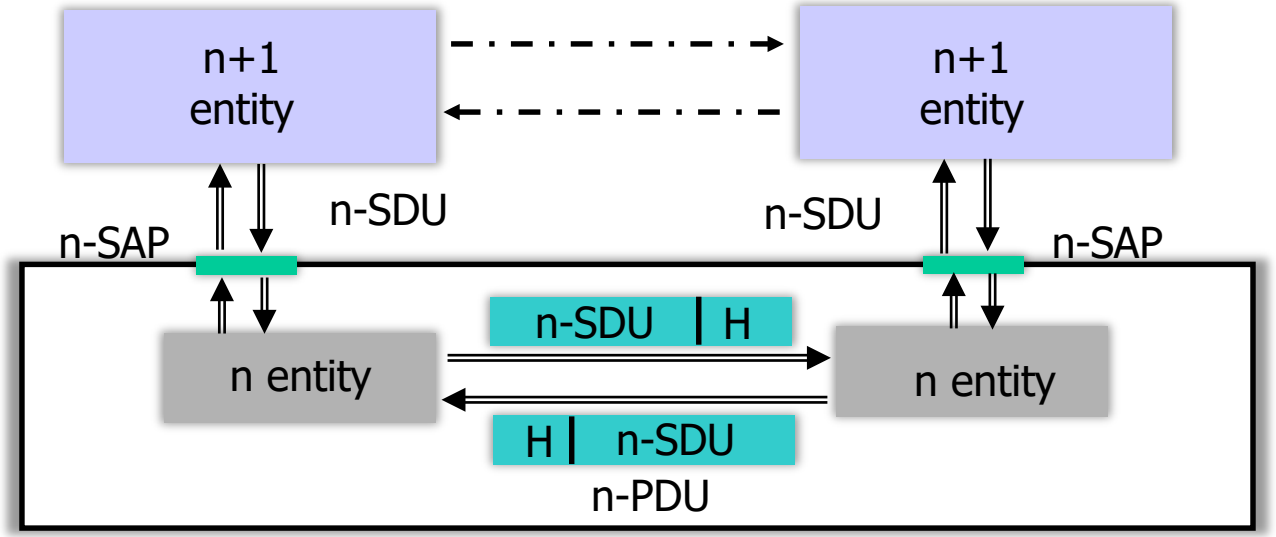
- ✓ Beispiele von Rechnernetzen
- ✓ Konzept der Lehrveranstaltung
- ✓ Klassifikation von Kommunikationssystemen
- Protokolle
- Netzwerksicherheit
- Geschichte
- Literatur

# Protokolle

- Rechnernetze sind komplex
  - Endgeräte, Switches, Router, Schnittstellenkarten, Leitungen, Kanäle, Verbindungen
  - Nachrichten
  - Mechanismen zur Fehlersicherung, Fluss- und Überlastkontrolle, Adressierung, Wegsuche, Weiterleitung, Medienzugriff, …
- Protokolle
  - wesentliches Strukturierungsprinzip
  - legen Nachrichtenformat und Verhalten der Kommunikationspartner fest
  - Beispiel: Hypertext Transfer Protocol (HTTP)
    - HTTP-Client erfragt Inhalte von HTTP-Server
    - 2 Arten von Nachrichten: Anfrage und Antwort
    - festgelegte Formate beider Nachrichten
    - festgelegtes Verhalten von HTTP-Client und HTTP-Server

# Protokolle

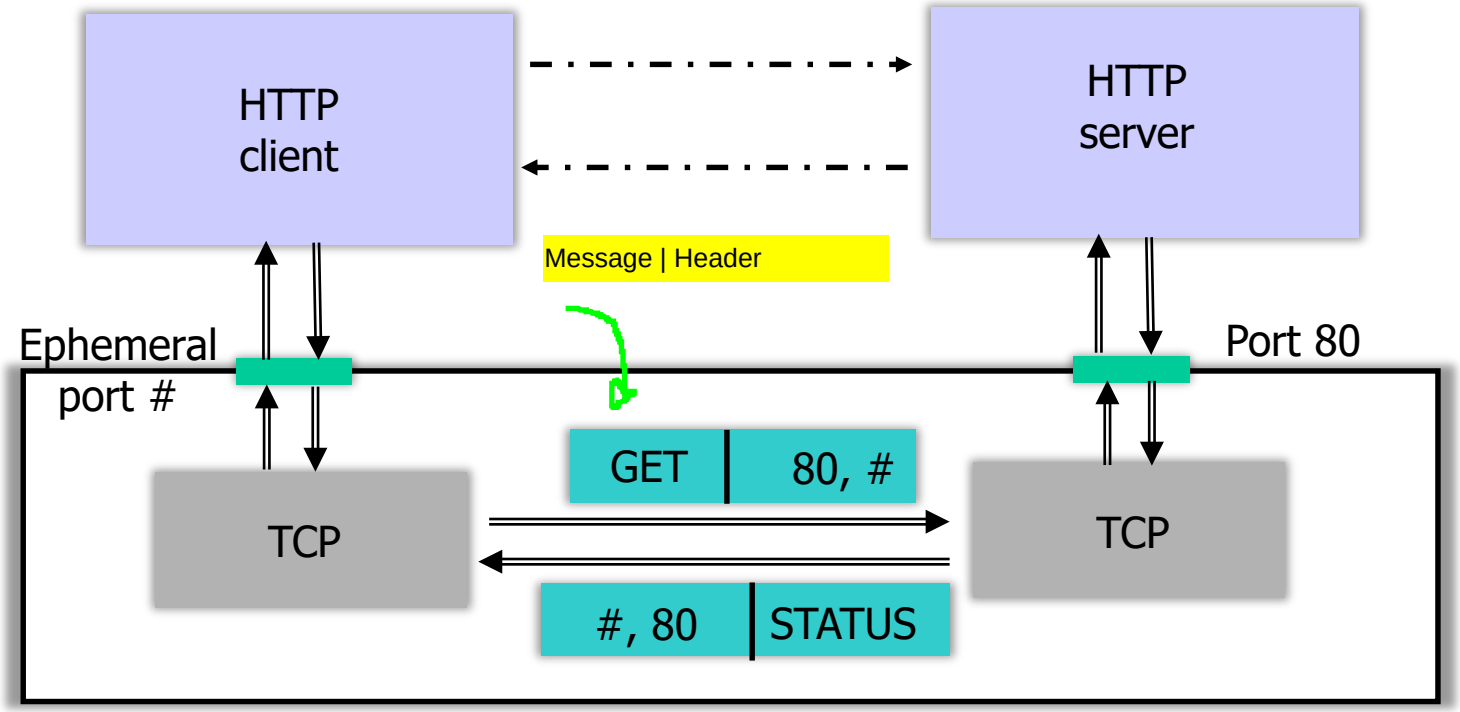
- Strukturierung in Schichten
  - Instanzen der Schicht n+1 nutzen die Dienste der Schicht n
  - Dienst wird zwischen Schichten an Dienstzugangspunkten (Service Access Points, SAPs) angeboten, dafür werden Service Data Units (SDUs) übergeben
  - Instanzen der Schicht n auf verschiedenen Hosts tauschen Protocol Data Units (PDUs) aus, jede PDU enthält einen Kopf (Header)




Quelle: Leon-Garcia, Widjaja: *Communication Networks: Fundamental Concepts and Key Architectures*, 2nd ed., McGraw-Hill, 2004.

# Protokolle

- Beispiel: HTTP nutzt die Dienste der Transportschicht




Quelle: Leon-Garcia, Widjaja: *Communication Networks: Fundamental Concepts and Key Architectures*, 2nd ed., McGraw-Hill, 2004.

# Protokolle

- ISO Open Systems Interconnection (OSI)
  - verbreitete Terminologie
  - Kommunikation wird durch Instanzen (Entities) durchgeführt
  - Dienst (Service)
    - Beschreibung, was eine Instanz anbietet
    - ähnlich zu der öffentlichen Schnittstelle einer Softwarekomponente
  - Protokoll (Protocol)
    - Beschreibung, wie die Instanzen interagieren, um Dienst zu realisieren
    - Nachrichtenformate, Verhaltensregeln
    - eine Beschreibung der Implementierung, aber noch nicht die Implementierung
  - Schicht (Layer)
    - Zusammenfassung von Instanzen
  - Schichtenarchitektur
    - System von Schichten, bei denen die Funktion der einzelnen Schichten und das Prinzip der Interaktion untereinander festgelegt ist

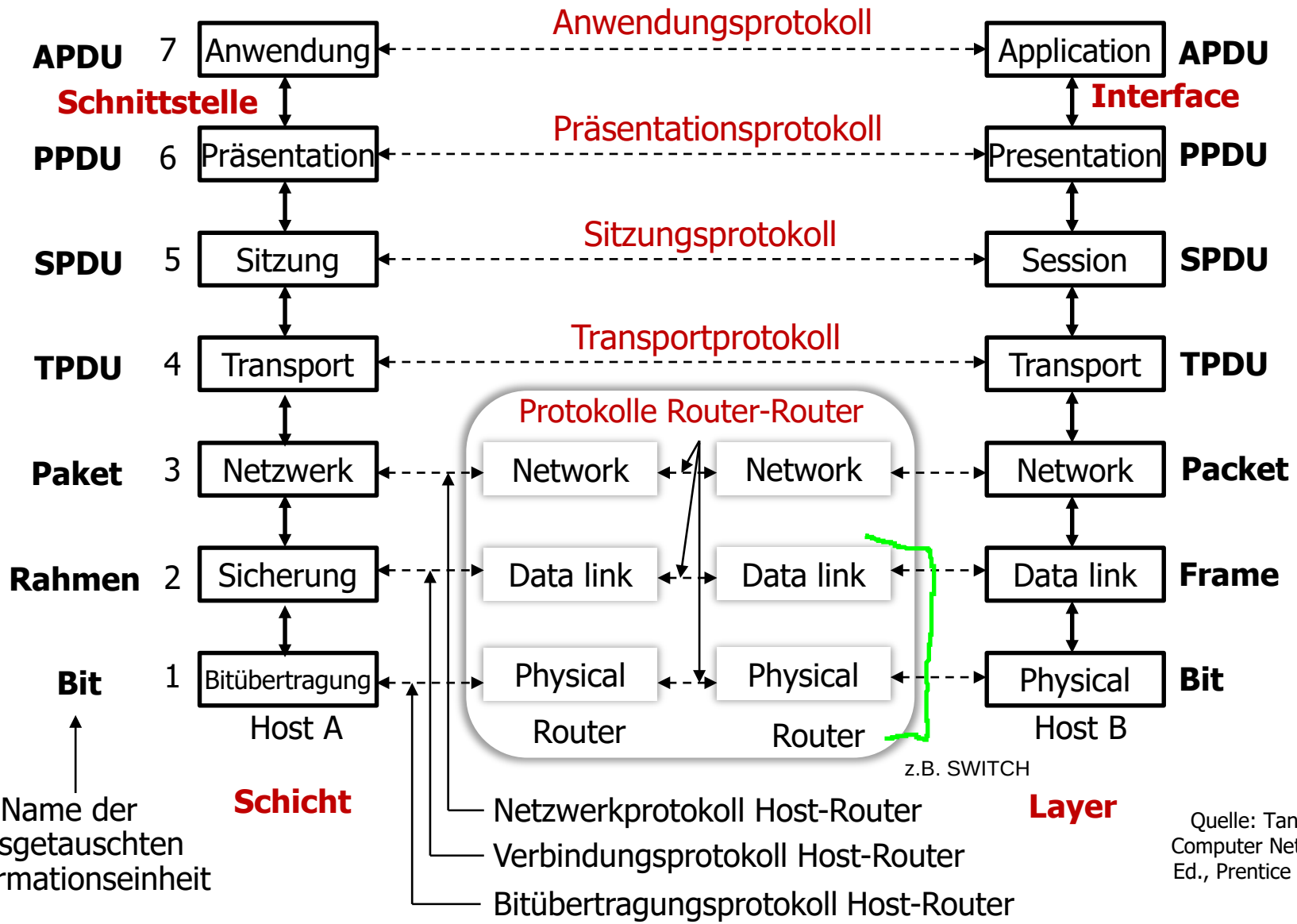
E.g. HTTP erlaubt anfrage/herunterladen von Webinhalten

Wie ist eine GET nachricht aufgebaut, was soll d

Welche Funktionen gehören zu welchen Schichten?

# Protokolle

PDU=Protokoll-Data-Unit




Quelle: Tanenbaum. Computer Networks. 5th Ed., Prentice Hall, 2011.

# Protokolle

- Bitübertragungsschicht (Physical Layer)
  - mechanische, elektrische und prozedurale Eigenschaften zur Übertragung von Bits: Zeitsynchronisation, Kodierung, Modulation, …
- Sicherungsschicht (Data Link Layer)
  - Medienzugriff und gesicherte Übertragung von Rahmen (Frames): Rahmensynchronisation, Fehler- und Flusskontrolle, …
- Netzwerkschicht (Network Layer)
  - Übertragung von Paketen bzw. Datagrammen: Verbindungsaufbau, Wegwahl, Vermittlung, Betriebsmittelverwaltung, …
- Transportschicht (Transport Layer)
  - zuverlässiger Ende-zu-Ende Transport von Segmenten
- Sitzungsschicht (Session Layer)
  - Kommunikation zwischen Anwendungen
- Darstellungsschicht (Presentation Layer)
  - Syntax und Semantik der ausgetauschten Informationen, z.B. mit Abstract Syntax Number One (ASN.1) oder XML
- Anwendungsschicht (Application Layer)
  - Kommunikation der Anwendungsprozesse mit anwendungsspezifischen Informationen

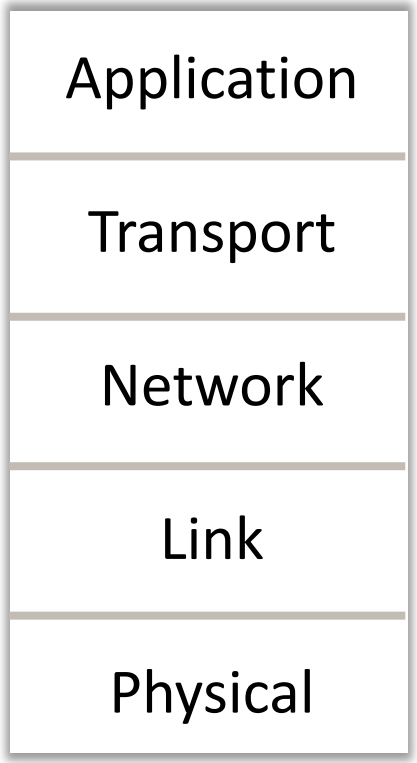
z.B. MSB zuerst oder zuletzt?

Diese gibt es im internet nicht (hat sich nicht durchgesetzt)

# Protokolle

- Schichtenarchitektur im Internet
  - OSI-Referenzmodell hat sich nicht durchgesetzt, vereinfachtes Modell des Internet ist verbreitet
  - Anwendungsschicht
    - Netzwerkanwendungen (HTTP, FTP, …)
  - Transportschicht
    - Transport von Segmenten zwischen Anwendungen (TCP, UDP)
  - Netzwerkschicht
    - Datagramme zwischen Hosts über Router (IP), Weiterleitung, Wegewahl (Routing)
  - Sicherungsschicht
    - Rahmen zwischen benachbarten Geräten, Medienzugriff, Sicherung
  - Bitübertragungschicht
    - binäre Formate, Modulationsverfahren

5-Level schicht



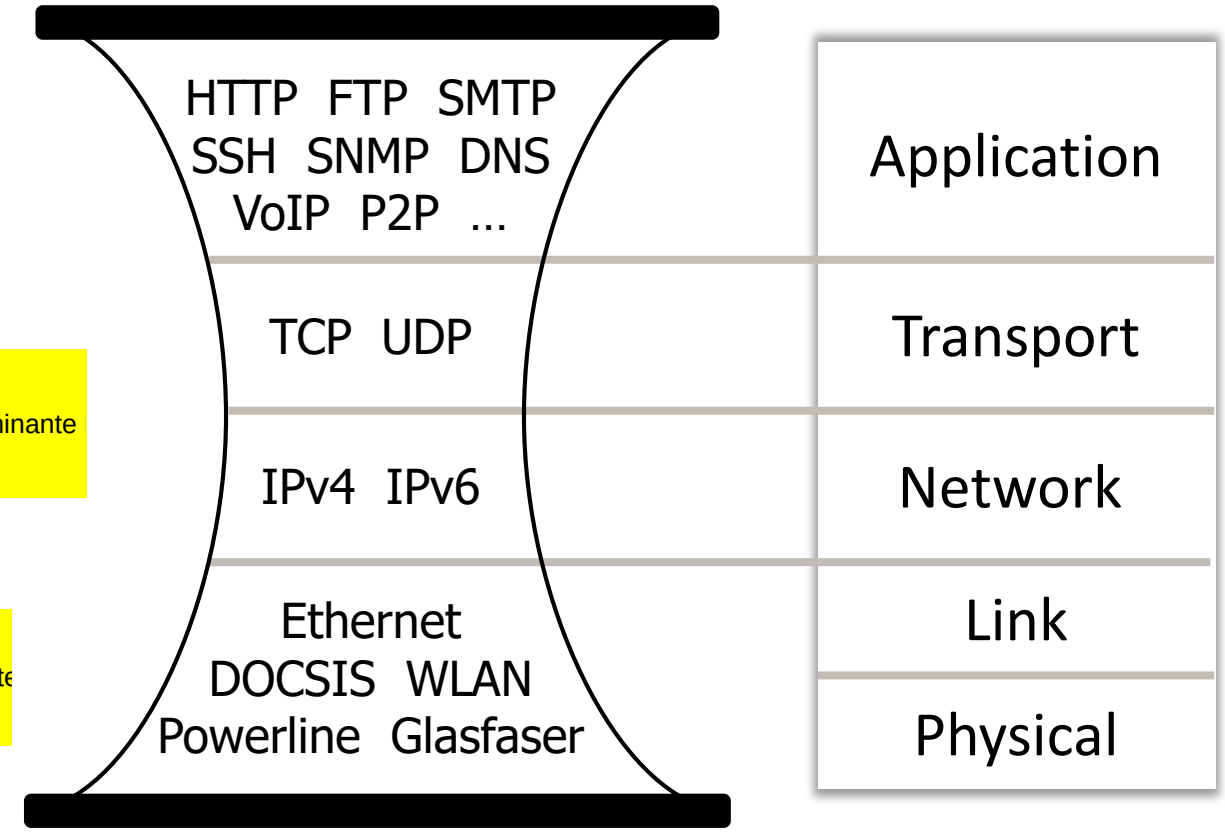
# Protokolle

- Schichtenarchitektur: In der Praxis eher eine Sanduhr (Internet hourglass)

- Vielzahl von Protokollen in Anwendungsschicht
- Transportschicht dominiert von TCP/UDP
- Netzwerkschicht dominiert von IPv4/IPv6
- Vielzahl von Technologien in der Sicherungs- und Bitübertragungsschicht

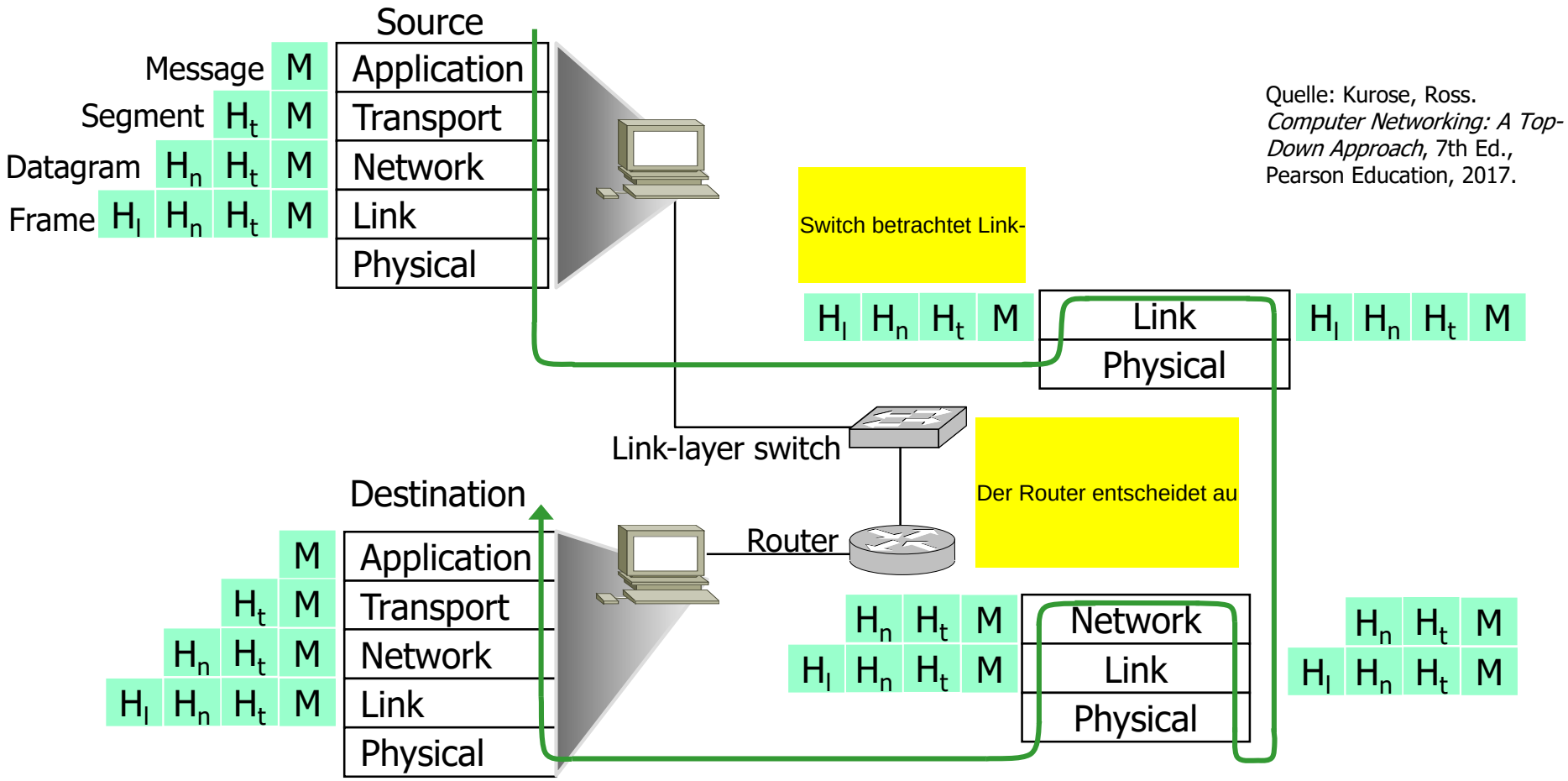
wenige, dominante

DOCSIS ist Inte



# Protokolle

- Weg einer Nachricht zwischen Anwendungen
  - Abstieg: jeweils ein Kopf dazu, Aufstieg: Kopf wird entfernt




Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

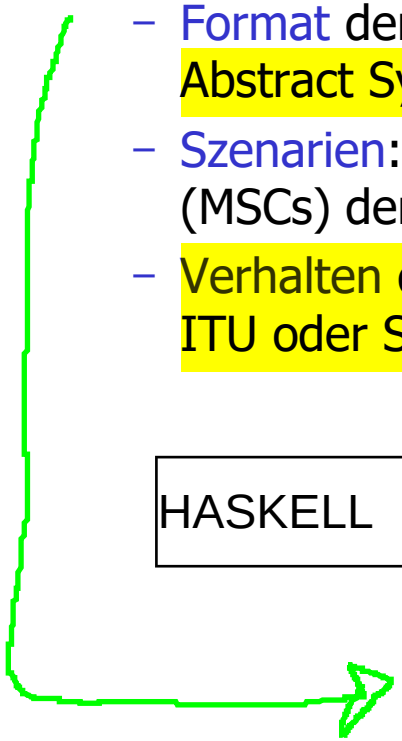
# Protokolle

- Implementierung von Protokollen
  - die Schichten unterhalb der Anwendungsschicht sind typischerweise Teil des Betriebssystems
  - die Dienste der Transportschicht können durch Betriebssystemaufrufe genutzt werden
  - die meisten Programmiersprachen stellen APIs hierfür zur Verfügung, z.B. Objekte und Methoden in Java (java.net)
  - im Betriebssystem verschiedene Realisierungsmöglichkeiten, für Effizienz wird das mehrmalige Kopieren von SDUs bei der Übergabe vermieden, stattdessen Übergabe von Referenzen

    Nicht jedes Protokoll hat einen unabhängigen Prozess.Man üb
- Cross-Layer Optimierung
  - die saubere Trennung in Schichten wird in der Realität oft nicht eingehalten, z.B. werden zur Steigerung der Effizienz Mechanismen der Bitübertragungs- und der Sicherungsschicht gekoppelt

# Protokolle

- Beschreibung von Protokollen
  - Protokolle werden in Dokumenten von Standardisierungsgremien festgelegt
  - informelle Beschreibung: bei IETF verbreitet, zusätzlich Referenzimplementierungen Fucking Fantastic...
  - formale Beschreibung
    - Format der Nachrichten: ähnlich wie Datenstrukturen in Programmiersprachen, z.B. mit Abstract Syntax Notation One (ASN.1) der ISO
    - Szenarien: typische Abläufe des Nachrichtenaustauschs, z.B. Message Sequence Charts (MSCs) der ITU bzw. Sequenzdiagramme in der UML
    - Verhalten der Instanzen: Automaten, z.B. Specification and Description Language (SDL) der ITU oder Statecharts in der UML

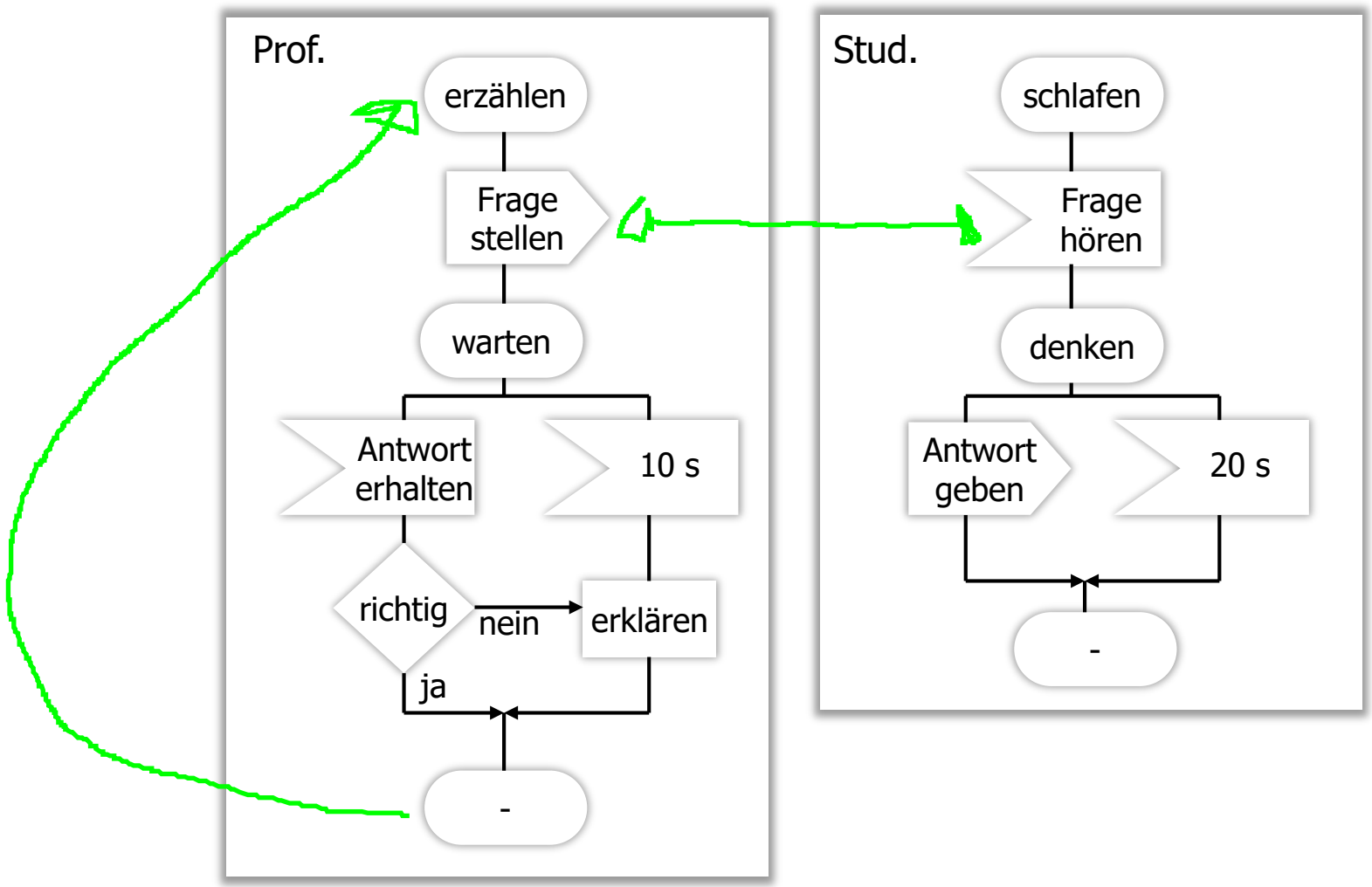


HASKELL

WIR WERDEN DIESE NICHT VERWENDEN!!!!!!!!!!WHYYYYYYYYYYYYYY

# Protokolle

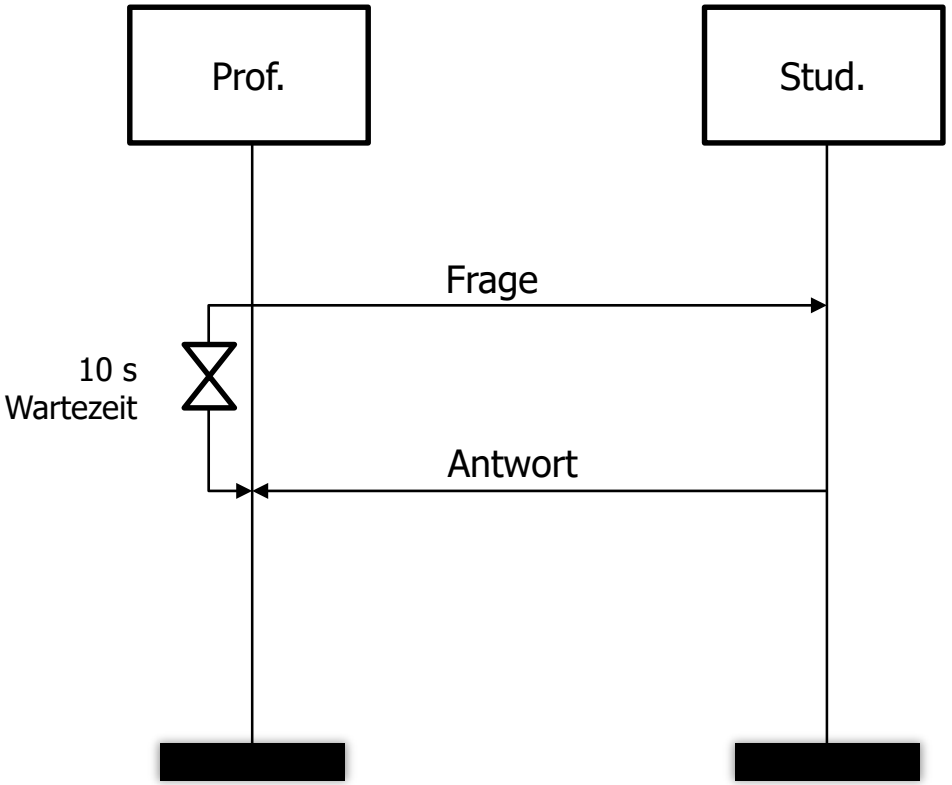
- Bsp. für SDL



# Protokolle

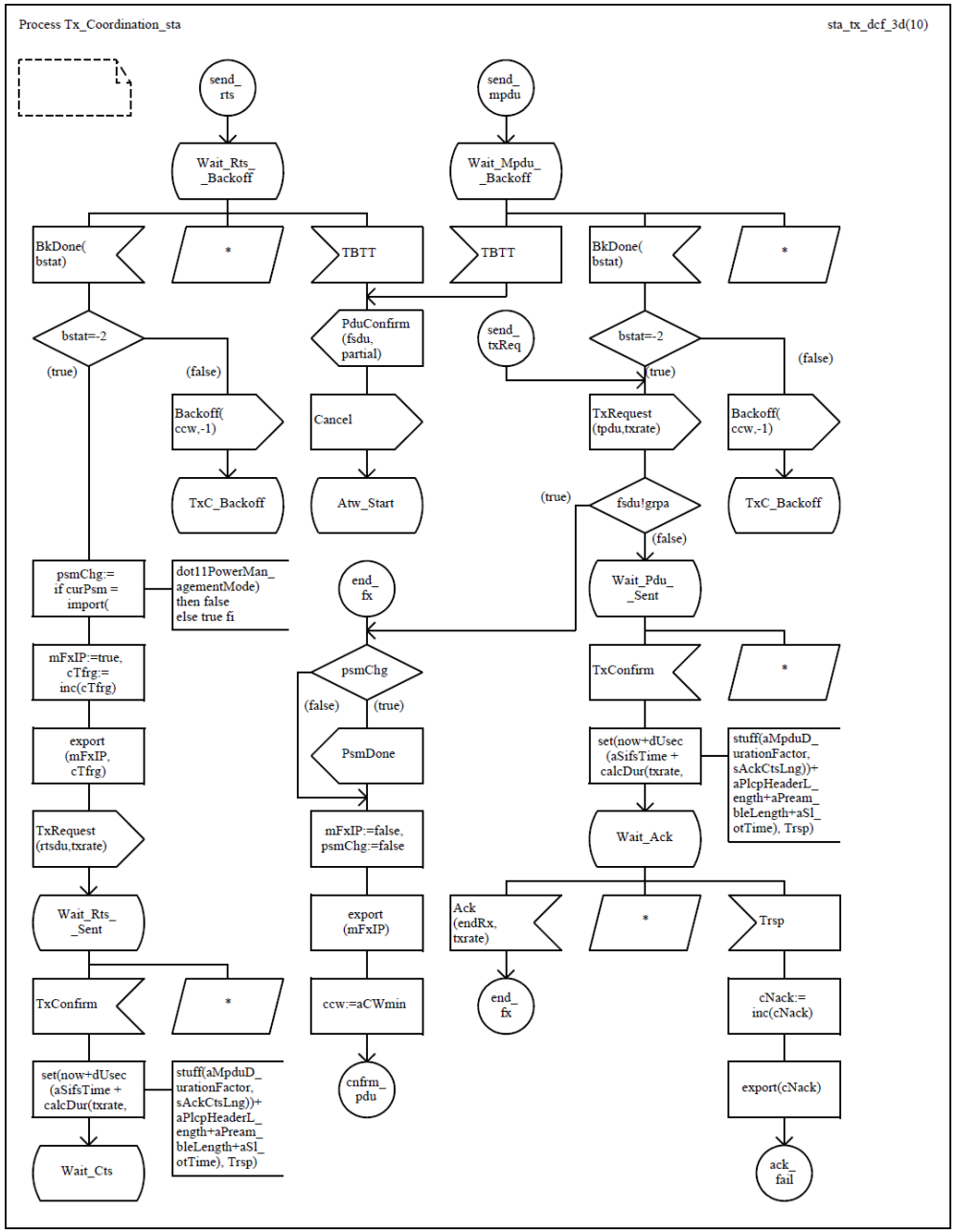
- Bsp. für MSC

Modelliert Datenfluss



# Protokolle

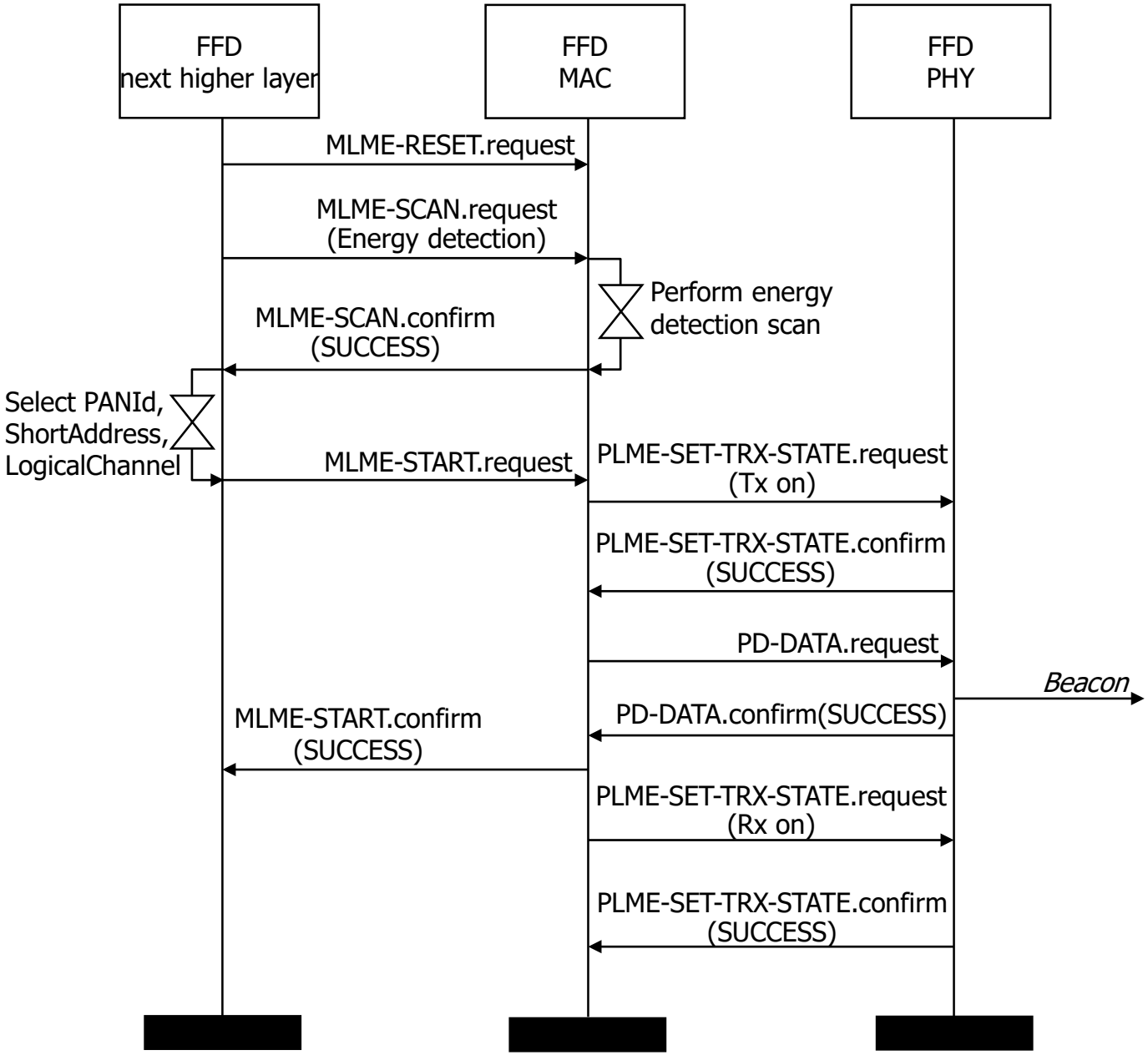
- Bsp. für SDL
  - Teil der Spezifikation des Medienzugriffs im aktuellen IEEE 802.11-2012 WLAN Standard
  - ein Automat, der Eingaben erhält und Ausgaben erstellt



# Protokolle

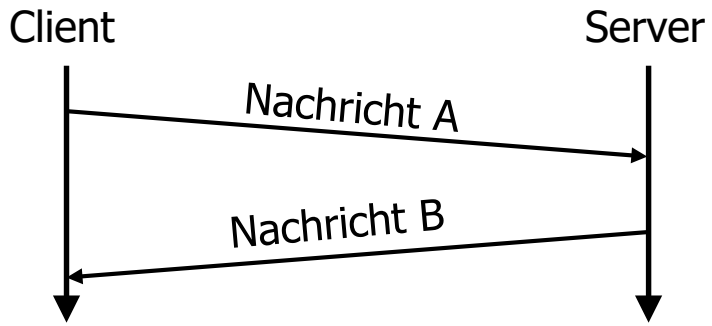
- Bsp. für MSC
  - Teil der Spezifikation des Medienzugriffs im 802.15.4 LR-WPAN Standard, 2003
  - senkrechte Linien heißen Lebenslinien und sind Instanzen zugeordnet

Das Zigbee Protokol für IOT-Low-power



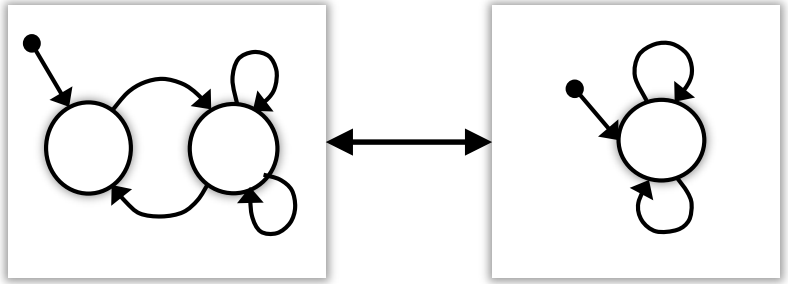
# Protokolle

- Protokollbeschreibung in VL Rechnerkommunikation
  - meist informell
  - Szenarien (informell, nicht gemäß MSC)




  - manchmal kommunizierende Automaten: Statecharts wie in UML

KILL ME!!!!



# Protokolle

- Dienstgüte (Quality-of-Service, QoS)
  - Sammelbegriff für quantitative Aspekte von Rechnernetzen und ihren Protokollen, z.B.:
    - Latenz (Zeit, bis Paket Empfänger erreicht)
    - Jitter (Maß für die Variabilität der Latenz)
    - Durchsatz (übertragene Daten pro Zeiteinheit, nicht gleich der Bruttobitrate)
    - Verlust- und Fehlerrate (z.B. von Bits bzw. Paketen bei drahtloser Übertragung)
    - Verfügbarkeit (Zeitanteil, in dem ein System einsatzfähig ist;
      z.B.: wenn Server 99.99% der Zeit verfügbar ist, dann ist er 4,32 Minuten im Monat unverfügbar)
  - relevant zur Auswahl und Konfiguration von Netzwerkarchitekturen und Protokollen
  - Ansätze: Messung, stochastische/deterministische Analyse, Simulation
  - Unterstützung durch Werkzeuge

Also Brutt-Protokolloverhead

# Einführung

- ✓ Beispiele von Rechnernetzen
- ✓ Konzept der Lehrveranstaltung
- ✓ Klassifikation von Kommunikationssystemen
- ✓ Protokolle
- Netzwerksicherheit
- Geschichte
- Literatur

# Netzwerksicherheit

**Hinweis:** Das Unterkapitel Netzwerksicherheit kann zunächst übersprungen werden und später bei Bedarf gelesen werden. Es enthält grundlegende Mechanismen, die später benötigt werden, um sichere Varianten von Protokollen zu verstehen

- Begriffe
  - Funktionssicherheit (Safety)
    - Eigenschaft eines IT-Systems, dass es nicht durch technisches Fehlverhalten eine Bedrohung für materielle Güter und die körperliche Unversehrtheit darstellt
  - Informationssicherheit (Security)
    - Schutz eines IT-Systems gegen unautorisierte Nutzung
  - Datenschutz (Privacy)
    - Fähigkeit einer natürlichen Person, die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren

Bus im Auto kaputt-> kein airbag

# Netzwerksicherheit

- Schutzziele für die Informationssicherheit
  - Authentizität (Authenticity) digitale signatur
    - Echtheit und Glaubwürdigkeit eines Objekts bzw. Subjekts gewährleisten (z.B. einer Nachricht, eines Absenders, Access-Points, Servers, etc.)
  - Datenintegrität (Integrity)
    - zu schützende Daten können nicht unbemerkt verändert werden (z.B. Verhindern der Manipulation von Nachrichten) Blockchain
  - Informationsvertraulichkeit (Confidentiality) passwörter
    - unautorisierte Informationsgewinnung ist unmöglich (z.B. Verhindern des Lesens einer Nachricht)
  - Verfügbarkeit (Availability)
    - keine unautorisierte Beeinträchtigung des Systems möglich (z.B. Verhindern von Denial-of-Service-Angriffen)
  - Verbindlichkeit (Non-Repudiation)
    - kein Abstreiten von Systemnutzung möglich (z.B. Kaufauftrag kann nicht geleugnet werden)
  - Anonymisierung und Pseudomisierung
    - Verändern personenbezogener Daten, so dass Einzelangaben nicht oder nur mit großem Aufwand natürlichen Personen zugeordnet werden können (z.B. Verhindern der Erstellung von Nutzerprofilen durch Dienstanbieter)

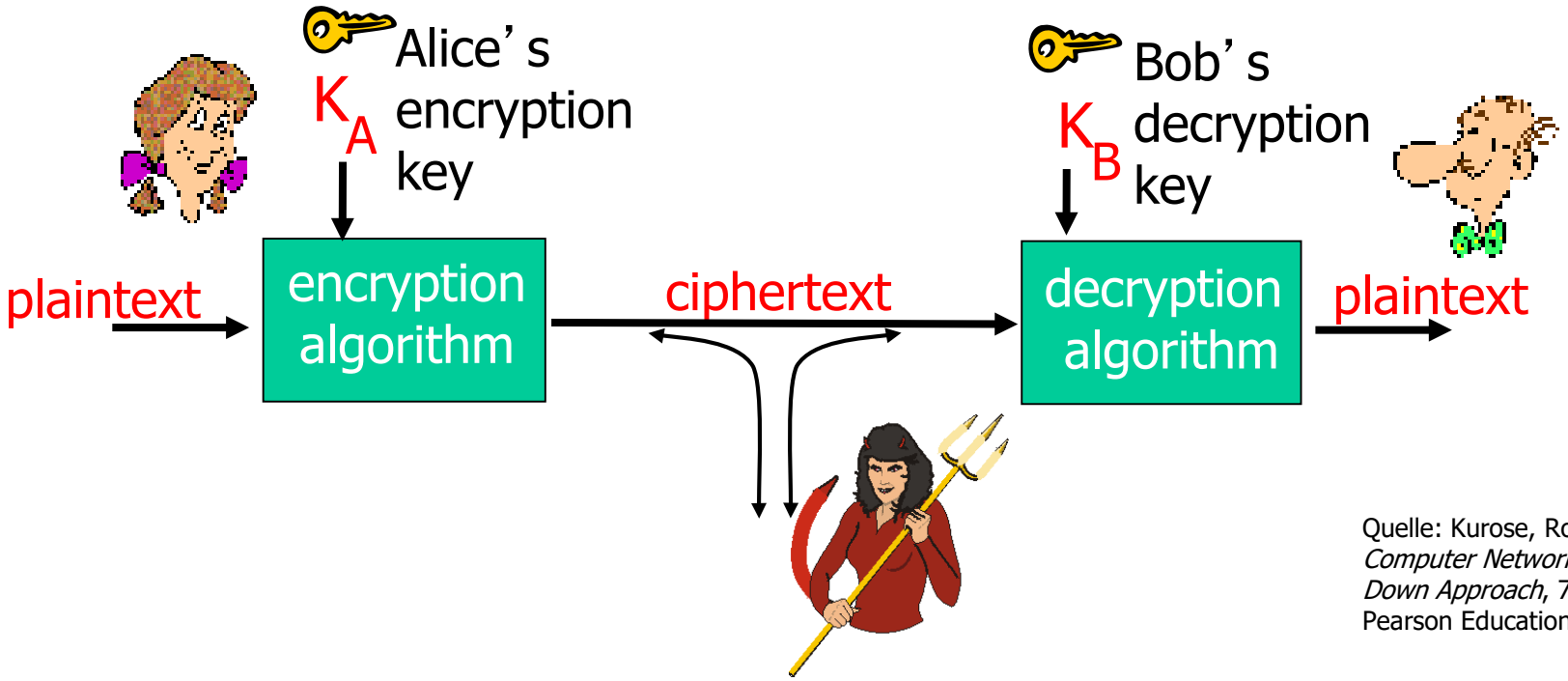
# Netzwerksicherheit

- Begriffe
  - Schwachstelle (Weakness) und Verwundbarkeit (Vulnerability)
    - Schwäche eines IT-Systems, die eine unautorisierte Nutzung ermöglicht
  - Exploit
    - beispielhafte Implementierung zur Ausnutzung von Schwachstellen
  - Angriff (Attack)
    - unautorisierter Zugriffsversuch
    - passive Angriffe: z.B. Abhören (Eavesdropping), Ausspähen von Passwörtern (Sniffing) phishing
    - aktive Angriffe: z.B. Entfernen, Verändern, Einspielen von Datenpaketen, Vorspiegelung falscher Identität (Spoofing, Maskierung), Beeinträchtigung der Verfügbarkeit (Denial-of-Service, DoS)
- Abwehr man-in-the-middle
  - kryptographische Verfahren: Verschlüsselung, Hashfunktionen, Signierung, Challenge-Response-Verfahren
  - operationelle Sicherheit: Filterung (Firewall), Monitoring (Intrusion Detection)

# Netzwerksicherheit

- Kryptografisches System (Kryptosystem)
  - Bestandteile: Klartext, Verschlüsselungsschlüssel, Verschlüsselungsverfahren, Chiffretext, Entschlüsselungsschlüssel, Entschlüsselungsverfahren
  - Kerckhoffs-Prinzip: Sicherheit des Systems darf nicht von der Geheimhaltung des Ver- und Entschlüsselungsverfahrens abhängen

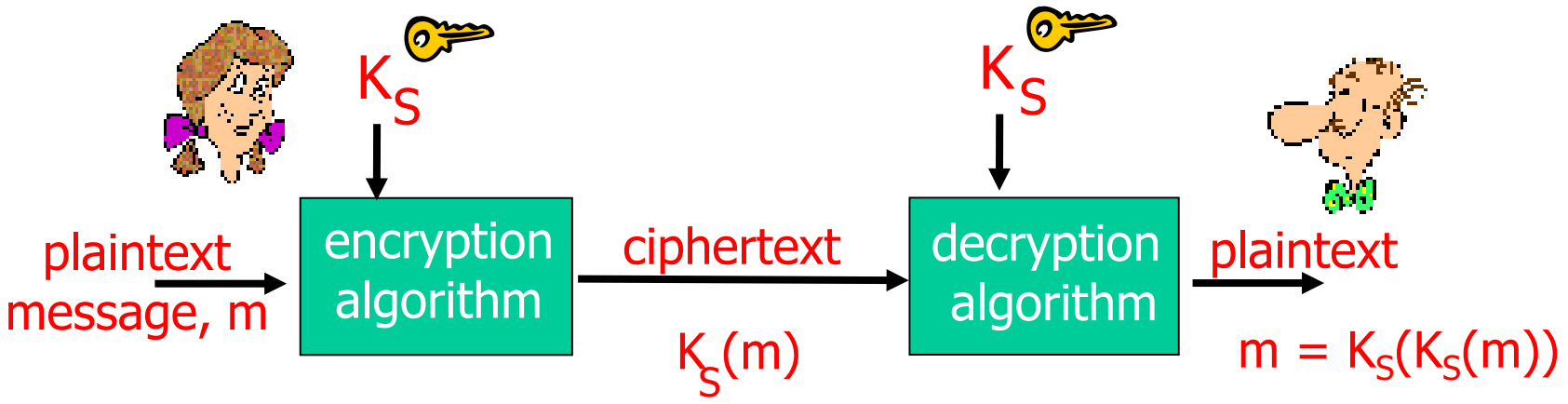
also der verschlüsselungsalgorithmus muss öffentlich sein, nur die schlüssel privat.(sonst kann




Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

# Netzwerksicherheit

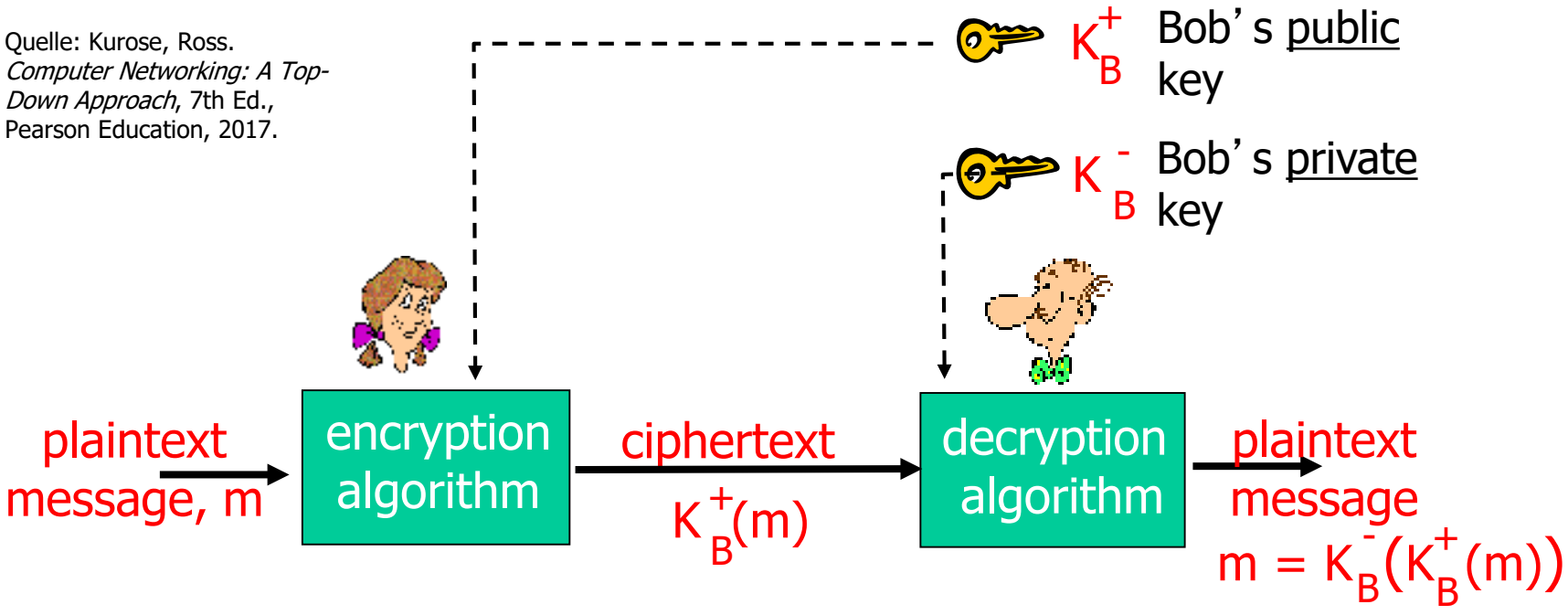
- Symmetrisches Kryptosystem
  - Ver- und Entschlüsselungsschlüssel sind gleich
  - beide Kommunikationspartner benötigen gemeinsamen geheimen Schlüssel (Shared Secret Key), der auf anderem Weg ausgetauscht werden muss
  - Sicherheit hängt von Stärke des Verfahrens und sicherer Verwaltung des Schlüssels ab




Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

# Netzwerksicherheit

- Asymmetrisches Kryptosystem
  - jeder Kommunikationspartner besitzt geheimen Schlüssel (Private Key) $K^-$ und öffentlichen Schlüssel (Public Key) $K^+$
  - aus $K^+$ darf $K^-$ (praktisch) nicht berechenbar sein
  - geheime Schlüssel müssen nur sicher verwaltet, aber nicht ausgetauscht werden



# Netzwerksicherheit

- Symmetrische Verschlüsselung
  - Grundprinzipien
    - Permutation: Vertauschung von Zeichen des Klartexts
    - Substitution: Ersetzen von Zeichen des Klartexts
    - Angriffsarten: Brute Force, Ciphertext-Only, Known-Plaintext, Chosen-Plaintext

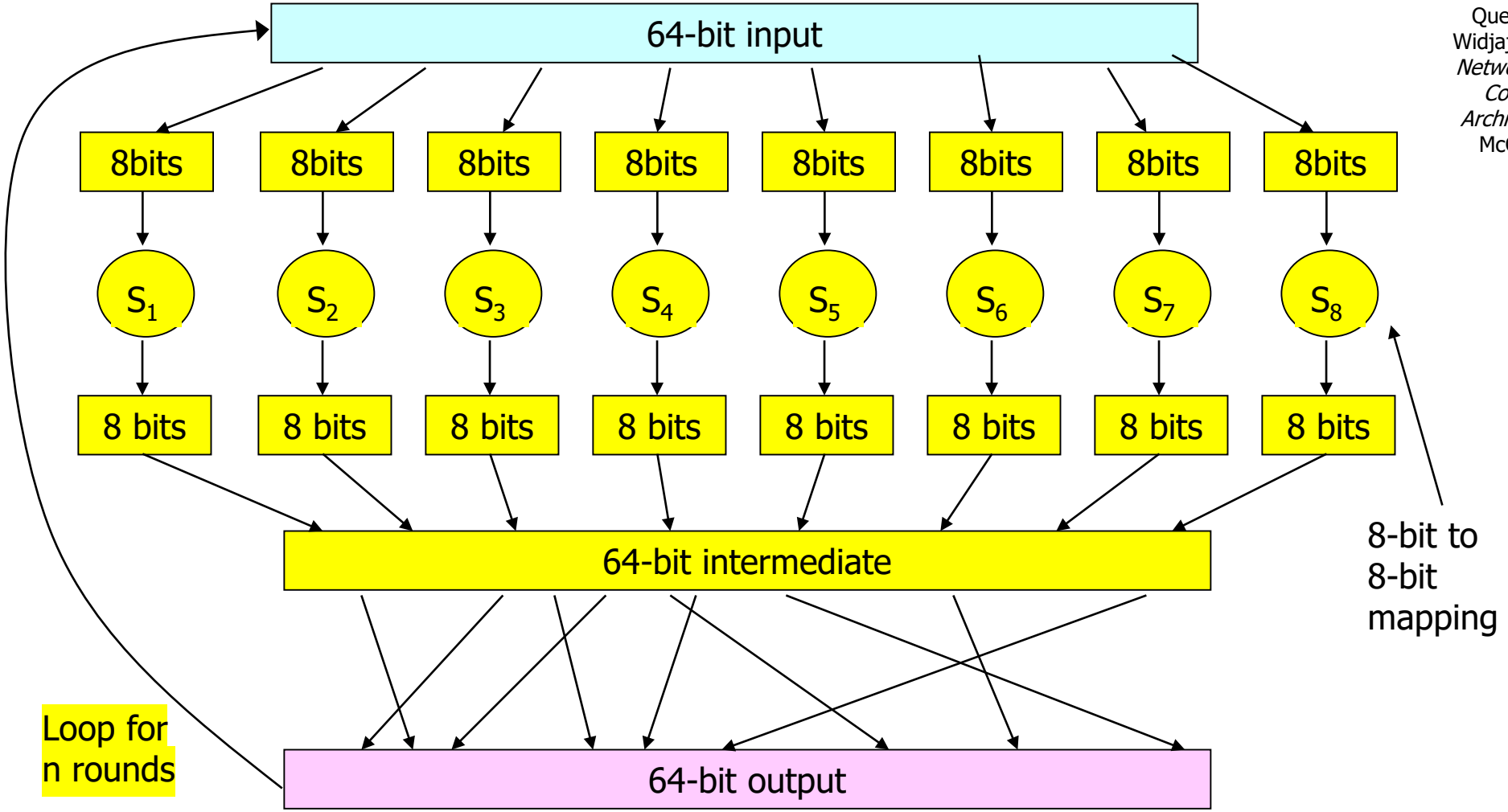
man kennt eine Plaintext und Verschlüssel paar.Choos

  - Blockchiffre (block cipher)
    - Eingabeblöcke fester Länge (z.B. 64, 128 Bits)
    - jeder Eingabeblock wird auf gleiche Weise verschlüsselt
    - einsetzbar, wenn Länge des Klartexts bekannt
    - bekannte Blockchiffre (National Institute of Standards and Technology, NIST)
      - Data Encryption Standard (DES), Blockgröße 64 Bits, Schlüssellänge nur 56 (eigentlich 40) Bits
      - Triple-DES (3DES), dreifache Anwendung von DES, Schlüssellänge 168 (eigentlich 112) Bits
      - Advanced Encryption Standard (AES), Blocklänge 128 Bits, Schlüssellänge 128-256 Bits

standard

# Netzwerksicherheit

- Beispielhafter Aufbau einer Blockchiffre:




Quelle: Leon-Garcia, Widjaja: *Communication Networks: Fundamental Concepts and Key Architectures*, 2nd ed., McGraw-Hill, 2004.

# Netzwerksicherheit

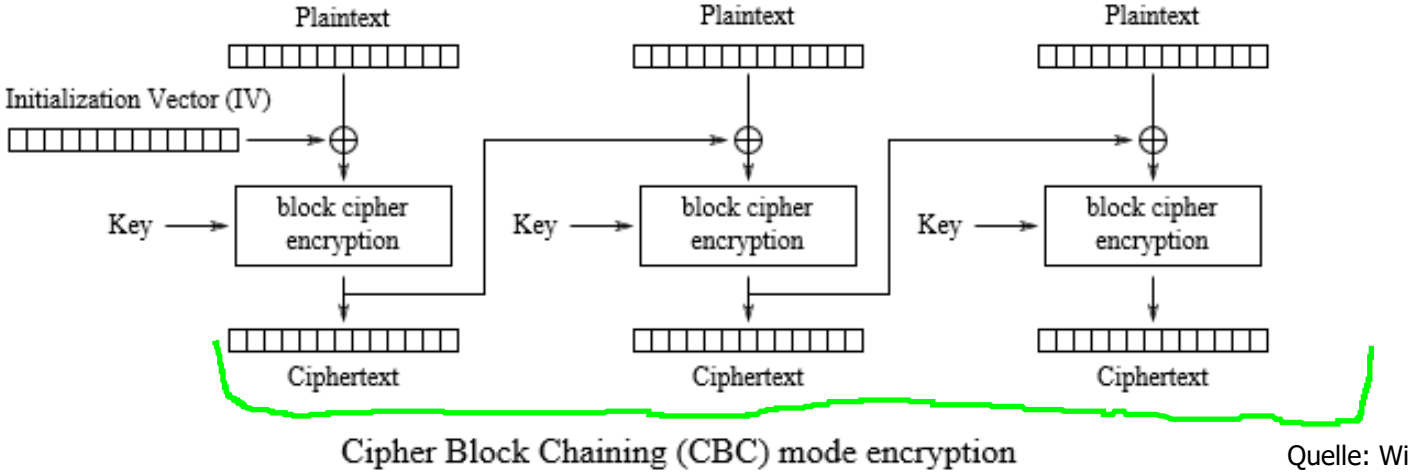
- Stromchiffre (stream cipher)
  - Folgen von Klartextzeichen m(i) werden mit variierender Funktion verschlüsselt, z.B.:
    - Erzeugung eines Stroms von Schlüsseln k(i) mit Zufallszahlengenerator
    - Verschlüsselung: Jedes Klartextzeichen wird mit neuem Schlüssel mit XOR bitweise verknüpft, $c(i) = m(i) \oplus k(i)$
    - Entschlüsselung: Jedes Chiffrezeichen wird mit neuem Schlüssel mit XOR bitweise verknüpft, $m(i) = c(i) \oplus k(i)$
    - Kommunikationspartner benötigen Initialwert (Initialization Vector, IV) eines kryptografischen Zufallszahlengenerators
  - bekannter Stromchiffre: RC4, Zeichengröße von 1-256 Bytes, kein IV nötig

symmetrisches verfahren mit XOR

# Netzwerksicherheit

- Betriebsarten
  - Blockchiffren können mit verschiedenen Betriebsarten als Stromchiffren eingesetzt werden
  - Beispiel: Cipher Block Chaining
    - Verschlüsselung: jeder Eingabeblock wird mit dem vorigen chiffrierten Eingabeblock mit XOR bitweise verknüpft und dann mit dem Blockchiffre verschlüsselt,
      $c(i) = K_S(m(i) \oplus c(i-1))$
    - Entschlüsselung: jeder chiffrierte Block wird mit dem Blockchiffre entschlüsselt und dann mit dem vorigen chiffrierten Eingabeblock mit XOR bitweise verknüpft,
      $m(i) = K_S(m(i) \oplus c(i-1))$

also widerholte anwendung von blockcipher und




Cipher Block Chaining (CBC) mode encryption

Quelle: Wikipedia.

all diese werden aneinandergehängt.Man erhält eine Blockcipher mit beliebiger länge

# Netzwerksicherheit

- Asymmetrische Verschlüsselung
  - Grundprinzip
    - Einwegfunktion f mit Falltür: der Funktionswert y = f(x) ist einfach berechenbar, die Umkehrfunktion $x = f^{-1}(y)$ ist praktisch nur berechenbar mit zusätzlicher Information (= Falltür)
    - Verwendung mathematischer Probleme, für die keine effizienten Berechnungsverfahren bekannt sind
      - Faktorisierung (Zerlegung großer Zahlen in Primfaktoren), z.B. RSA-Verfahren, benötigt relativ langen Schlüssel (mindestens 1024 Bits)
      - diskreter Logarithmus (ElGamal)
      - diskreter Logarithmus auf elliptischen Kurven, schwereres Problem, höhere Sicherheit bei gleicher Schlüssellänge (mindestens 256 Bits)

# Netzwerksicherheit

- RSA-Verfahren (Rivest, Shamir, Adleman)
  - Schlüsselerzeugung
    - wähle zwei große ungleiche Primzahlen p und q
    - berechne $n = p \cdot q$, $\varphi(n) = (p - 1) \cdot (q - 1)$
    - wähle zu φ(n) teilerfremde Zahl e mit $1 < e < \varphi(n)$
    - berechne d, so dass $e \cdot d \bmod \varphi(n) = 1$
    - (n,e) ist öffentlicher Schlüssel $K^+$
    - (n,d) ist privater Schlüssel $K^-$
  - Verschlüsselung
    - $K^+(m) = m^e \bmod n = c$
  - Entschlüsselung
    - $K^-(c) = c^d \bmod n = m$
  - Beweis für $m = (m^e \bmod n)^d \bmod n$ benötigt Elemente der Zahlentheorie

Zum lösen müsste man das inverse von e mod n finden

# Netzwerksicherheit

- Bsp. für RSA-Verfahren mit kleinen Zahlen
  - Primzahlen $p = 5$, $q = 7$, $n = pq = 35$, $\varphi(n) = (p-1)(q-1) = 24$
  - dann z.B. $e = 5$, teilerfremd zu 24
  - und z.B. $d = 29$, $ed-1 = 144$ ist durch $\varphi(n) = 24$ teilbar, daraus folgt $e \cdot d \bmod \varphi(n) = 1$
  - Verschlüsselung: für Klartext $m = (00001000)_2 = 12$ ergibt sich $m^e = 248832$ und $K^+(m) = m^e \bmod n = c = 17$
  - Entschlüsselung: $c^d = 48196857210675091509141182522307169 7$, $K^-(c) = c^d \bmod n = m = 12$
- Vertauschbarkeit von Ver- und Entschlüsselung
  - es gilt auch $K^+(K^-(m)) = (m^d \bmod n)^e \bmod n = m$
  - entspricht einer Verschlüsselung mit dem privaten Schlüssel und einer Entschlüsselung mit dem öffentlichen Schlüssel
  - kann für digitale Signatur verwendet werden

man hängt eine verschlüsselte zahl an z.B. seine email an, und leute können authenzität prüfen, in

# Netzwerksicherheit

## Kryptografische Hashfunktionen

- kurzer „Fingerabdruck" H(m) einer variabel langen Nachricht m
- schwache Hashfunktion
  - leicht zu berechnende Einwegfunktion h = H(m) mit |h| = konstant
  - für gegebenes h ist es praktisch unmöglich, eine Nachricht m' zu finden mit H(m') = h
- starke Hashfunktion
  - schwache Hashfunktion, für die es zusätzlich praktisch unmöglich ist, zwei Nachrichten m und m' zu finden mit H(m) = H(m') minimale kollisionen
- verbreitete Verfahren
  - Message Digest Algorithm 5 (MD5), 1991 von Rivest vorgeschlagen, iterierte Kompressionen, 128 Bit Hashwerte, Kollisionsangriffe bekannt
  - Secure Hash Algorithm (SHA-3), 2012 Gewinner eines Wettbewerbs des NIST, 224-512 Bit Hashwerte

# Netzwerksicherheit

## Message Authentication Code (MAC)

- Hashfunktion MAC(m, $K_{AB}$), die zusätzlich von einem symmetrischen Schlüssel $K_{AB}$ abhängt
- ermöglicht Überprüfung der Datenintegrität
- Einsatz
  - Sender A erzeugt mac = MAC(m, $K_{AB}$) und sendet (m, mac)
  - Empfänger erhält (m‘, mac‘) und überprüft, ob MAC(m‘, $K_{AB}$) = …
- Konstruktion von MACs
  - basierend auf Blockchiffren, z.B. bei AES die einzelnen Blöcke mit dem Schlüssel mit XOR verknüpfen
  - Keyed Hash: Schlüssel an Nachricht anhängen und dann Hashfunktion anwenden: H(m|$K_{AB}$)
  - Hash MAC (HMAC): Variante von Keyed Hash, komplizierterer Aufbau (NIST)

man hashed also die datei selber und schaut, ob das gleiche rausko

also jeden der normalerweise konkatenierten blöcke stattdessen xor.

salting bei passwortspeichern

# Netzwerksicherheit

## Digitale Signatur

- durch asymmetrische Verschlüsselung, bei der zur Verschlüsselung der private Schlüssel und zur Entschlüsselung der öffentliche Schlüssel verwendet wird
- Einsatz
  - Sender erzeugt $K^-(m)$ mit seinem privaten Schlüssel und sendet dies
  - Empfänger erhält dies und entschlüsselt mit dem öffentlichen Schlüssel des Senders $M = K^+(K^-(m))$
- Authentizität: Unter der Voraussetzung, dass der öffentliche Schlüssel eindeutig einer Person zuzuordnen ist, bezeugt dies die Identität des Senders
- Datenintegrität: Eine signierte Nachricht kann nicht unbemerkt verändert werden, da sonst keine Entschlüsselung möglich ist
- Verbindlichkeit: Unter der Voraussetzung, dass der private Schlüssel nicht von anderen verwendet wird, kann der Sender die Signatur nicht zurückweisen

wenn eine Sendung mit einem privatkey signiert wurde, dann kann man auch sicher sein, kann die person das versenden nicht leugnen (sofern der privatkey eindeutig ist)

# Netzwerksicherheit

- Digitale Signatur (Fortsetzung)
  - asymmetrische kryptografische Operationen sind aufwändig
  - daher Kombination mit Hashfunktion: nur Hashwert der Nachricht wird mit digitaler Signatur versehen
  - Einsatz
    - Sender erzeugt $S = K^{-}(H(m))$ und sendet $(m, S)$
    - Empfänger erhält $(m', S')$, und prüft ob $H(m') = K^{+}(S')$
  - ermöglicht genauso Authenzität, Datenintegrität und Verbindlichkeit

zuerst m hashen, dann das gleich wie beim normalen signierendas gleiche, soferr

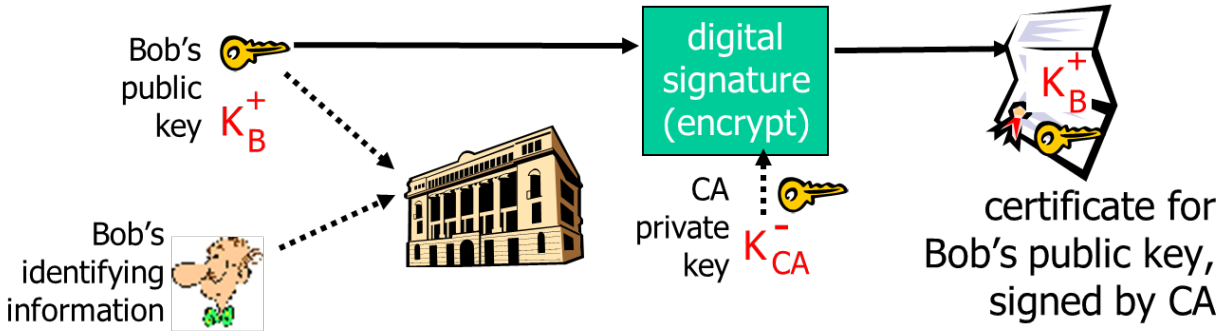
# Netzwerksicherheit

- Zertifizierung
  - digitale Bescheinigung eines öffentlichen Schlüssels
  - verbreiteter Standard für Zertifikate: ITU X.509, enthält
    - Subjektschlüssel: öffentlicher Schlüssel + Algorithmen u. Parameter
    - Signatur: mit privatem Schlüssel des Zertifikatausstellers verschlüsselter Hashwert + Algorithmen u. Parameter
    - Versionsnummer des Standards, Seriennummer (vom Aussteller zu vergeben), Zertifikataussteller (Name der Instanz), Gültigkeitsdauer, Subjektname, ...
  - Zertifizierungsstelle (Trust Center, Certification Authority, CA)
    - bietet Dienste zur Generierung von Schüsselpaaren, Suche und Zertifizierung von Benutzern an, privat oder öffentlich
  - Public Key Infrastructure (PKI)
    - hierarchische Organisation von Zertifizierungsstellen
    - Zertifikate können auf Wurzel zurückgeführt werden
    - Umsetzungs- und Vertrauensprobleme
  - alternativ Web-of-Trust (WoT): Vertrauensnetz

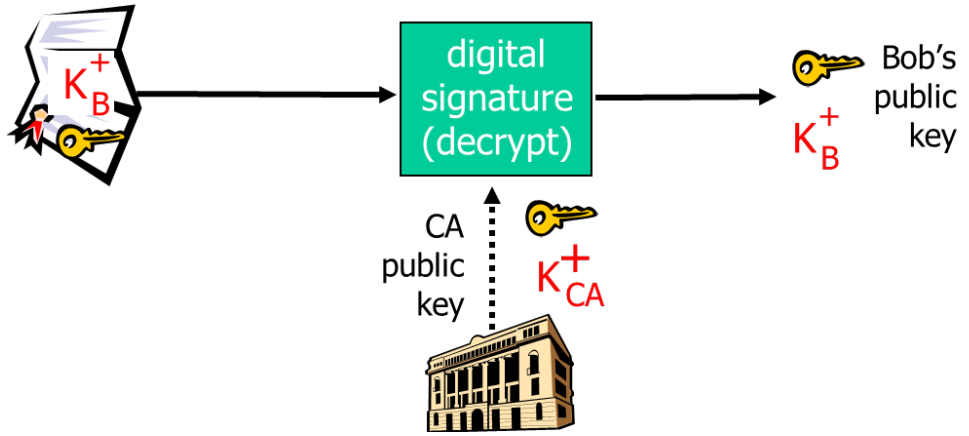
also alle parameter (algo, key, absender

# Netzwerksicherheit

- Zertifikaterstellung:




- Zertifikatauswertung:



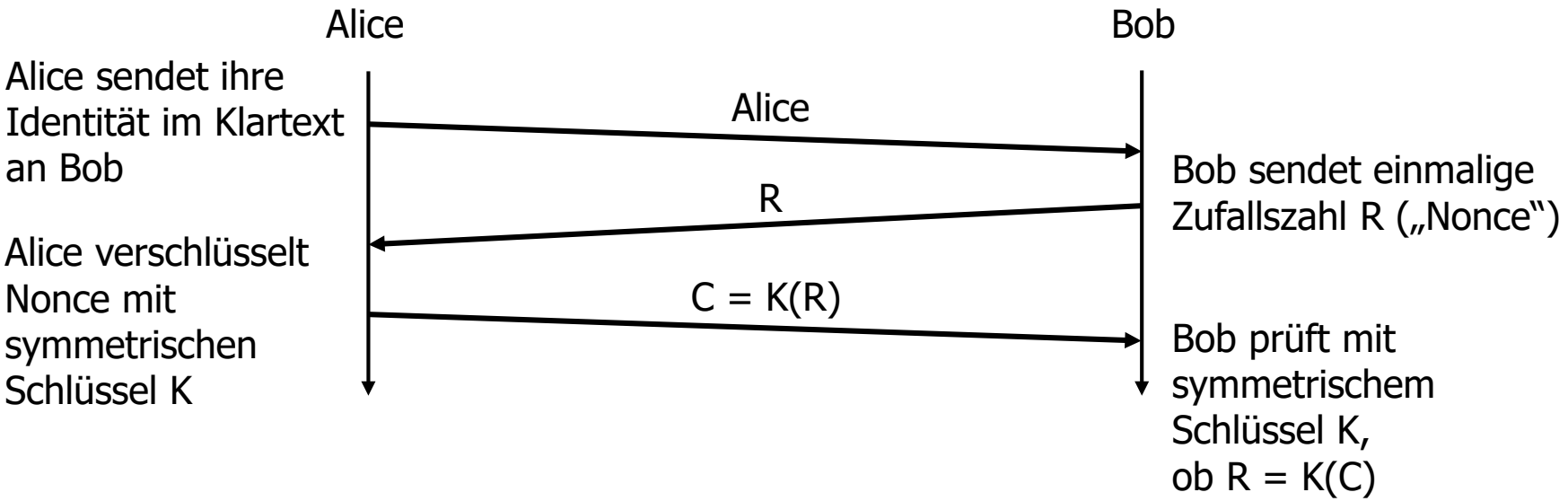

Quelle: Kurose, Ross. *Computer Networking: A Top-Down Approach*, 7th Ed., Pearson Education, 2017.

# Netzwerksicherheit

## Challenge-Response-Verfahren

- zur Authentifikation des Kommunikationspartners
- Verallgemeinerung der Authentifikation durch Wissen (wie z.B. bei Passwörtern)
- Variante mit symmetrischer Verschlüsselung zur Authentifikation von Alice gegenüber Bob (benötigt Kenntnis über gemeinsamen symmetrischen Schlüssel, „shared secret"):

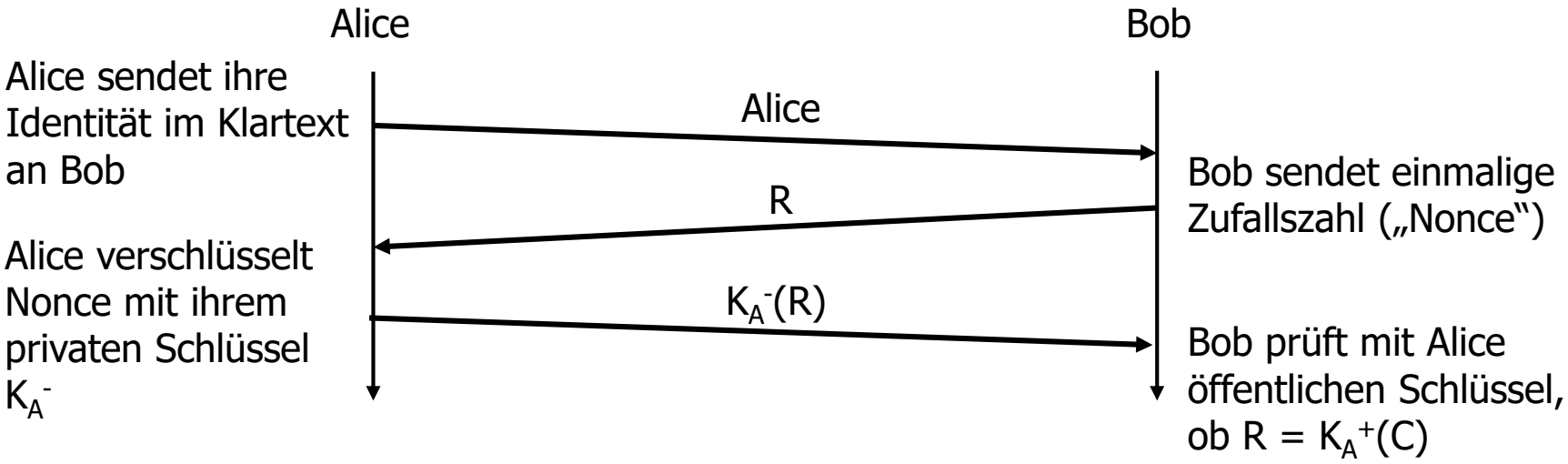
geht auch asymmetrisch, od




man fordert also hier die kenntnis des schlüssels an!

# Netzwerksicherheit

- Challenge-Response-Verfahren (Fortsetzung)
  - Variante mit asymmetrischer Verschlüsselung zur Authentifikation von Alice gegenüber Bob (Bob benötigt öffentlichen Schlüssel von Alice)




  - öffentlicher Schlüssel von Alice muss auf sichere Weise übermittelt werden, sonst „Man-in-the-Middle“-Angriff möglich

# Netzwerksicherheit

## Schlüsselaustausch

- sicherer Austausch von Schlüsseln ist Voraussetzung für den Einsatz von Verfahren zur Verschlüsselung, Authentifikation und Integrität
- dafür werden Schlüsselaustauschprotokolle benötigt
- dabei können leicht Sicherheitsprobleme entstehen
- Needham-Schroeder-Protokolle (1978) stellen Protokoll-Entwurfsmuster dar, auf deren Grundlage die meisten in der Praxis eingesetzten Systeme arbeiten
- 2 Varianten basierend auf symmetrischer und asymmetrischer Verschlüsselung
- beide benötigen einen vertrauenswürdigen Authentifizierungs- und Schlüsselverteilungsserver AS
- auf der folgenden Seite nur die Variante mit symmetrischer Verschlüsselung

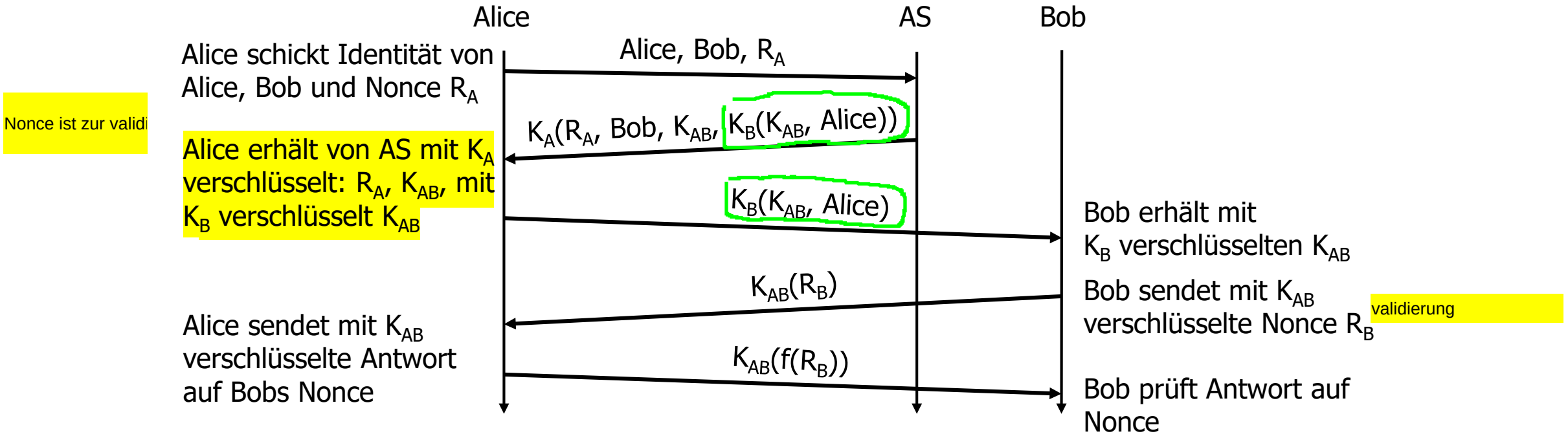
# Netzwerksicherheit

## Schlüsselaustausch mit symmetrischer Verschlüsselung

- AS besitzt symmetrische Schlüssel $K_A$ und $K_B$ für Alice und Bob und erzeugt symmetrischen Sitzungsschlüssel $K_{AB}$
- Alice erhält von AS Sitzungsschlüssel $K_{AB}$, dieser wird ihr zur Weiterleitung an Bob auch mit $K_B$ verschlüsselt geliefert

authentifizierungs server =AS

- Authentifizierung des AS gegenüber Alice und Alice gegenüber Bob



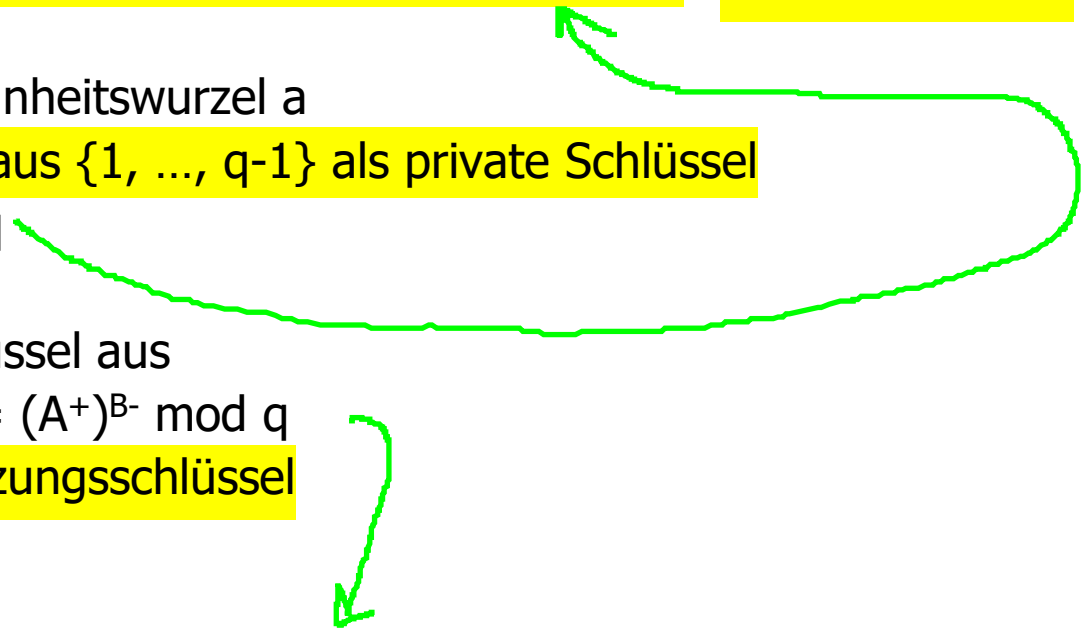

Nonce ist zur validi

validierung

# Netzwerksicherheit

- Diffie-Hellman-Schlüsselaustausch (1976)
  - die Kommunikationspartner berechnen dezentral den gemeinsamen symmetrischen Sitzungsschlüssel, dieser muss nicht über das Medium transportiert werden, kein Authentifizierungs- und Schlüsselverteilungsserver nötig
  - mathematische Grundlagen
    - diskreter Logarithmus über einem Galois-Feld zu einer Primzahl q
    - Einheitswurzel: für alle $1 \leq m \leq q-1$ gibt es ein $1 \leq p \leq q-1$ mit $m = a^p \bmod q$
  - Verfahren
    - öffentlich bekannt: Primzahl q und primitive Einheitswurzel a
    - Alice und Bob wählen Zufallszahlen $A^-$ und $B^-$ aus {1, …, q-1} als private Schlüssel
    - Alices öffentlicher Schlüssel ist $A^+ = a^{A^-} \bmod q$
    - Bobs öffentlicher Schlüssel ist $B^+ = a^{B^-} \bmod q$
    - Alice und Bob tauschen ihre öffentlichen Schlüssel aus
    - Alice berechnet $K_{AB} = (B^+)^{A^-} \bmod q$, Bob $K_{BA} = (A^+)^{B^-} \bmod q$
    - es gilt $K_{AB} = K_{BA}$ , dies ist der gemeinsame Sitzungsschlüssel

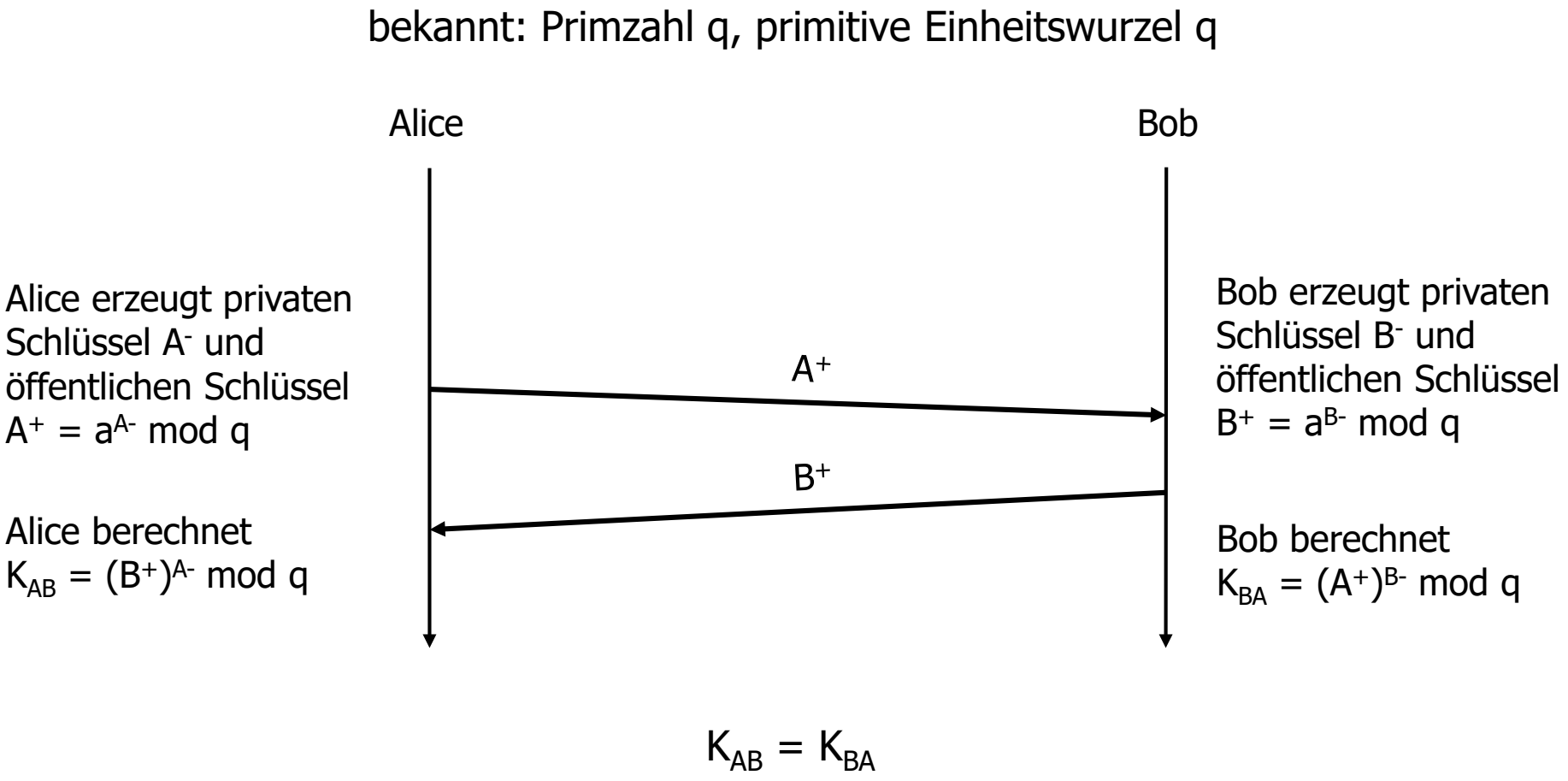
p-te wurzel von m unter mod q



euler-phi funktion

# Netzwerksicherheit

- Diffie-Hellman-Schlüsselaustausch (Fortsetzung)

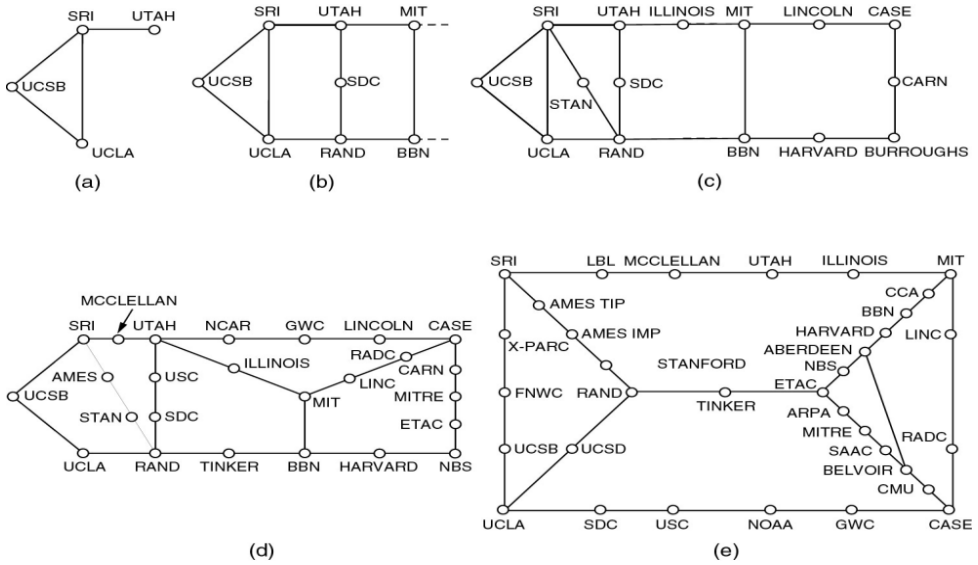


# Einführung

- ✓ Beispiele von Rechnernetzen
- ✓ Konzept der Lehrveranstaltung
- ✓ Klassifikation von Kommunikationssystemen
- ✓ Protokolle
- ✓ Netzwerksicherheit
- ■ Geschichte
- ■ Literatur

# Geschichte

- Meilensteine
  - vor 1970: leitungsvermitteltes Telefonnetz
  - 60er Jahre: erste Konzepte von paketvermittelten Datennetzen, militärische Zwecke, Verbindung von Großrechnern
  - 70er Jahre: ARPAnet, lokale Netze basierend auf Zufallszugriff (Aloha, Ethernet), Konzept des Internetworking




*Growth of the ARPANET (a) December 1969. (b) July 1970. (c) March 1971. (d) April 1972. (e) September 1972.*

Quelle: Tanenbaum. Computer Networks. 5th Ed., Prentice Hall, 2011.

# Geschichte

- Meilensteine
  - 80er Jahre: Entwicklung von Protokollen wie TCP/IP, SMTP, DNS, FTP, Nutzung vor allem im akademischen Bereich
  - 90er Jahre: Entwicklung populärer Anwendungsprotokolle wie HTTP, Verbreitung von Web-Browsern, Kommerzialisierung, geschätzte Nutzeranzahl > 100 Millionen, Sicherheit wird wichtiges Thema, erste drahtlose Netze (WLAN)
  - 00er Jahre: Crash, weiteres Wachstum, weitere Anwendungen, z.B. Internettelefonie, Peer-to-Peer-Systeme, soziale Netzwerke, Cloud Computing, weitere drahtlose Netze (u.a. Bluetooth, ZigBee), DSL, WiFi verbreitet, 3G Mobilfunk mit HSPA, mobiler Datenverkehr überholt Sprachverkehr (2009)
  - 10er Jahre: LTE, 5G, Software Defined Networking,
    Internet der Dinge

# Geschichte

- Gremien zur Standardisierung von Protokollen
  - International Standards Organization (ISO)
    - internationale Standards
    - national: American National Standards Institute (ANSI), ...
  - International Telecommunications Union (ITU)
    - Telekommunikationsstandards, PTTs
    - ITU-T (Telecommunications Sector, früher CCITT)
    - ITU-R (Radiocommunications Sector)
  - European Telecommunications Standards Institute (ETSI)
  - Internet Engineering Task Force (IETF)
    - Request for Comments (RFCs)
  - Institute of Electrical and Electronic Engineers (IEEE)
  - Industrieforen zur schnelleren Entwicklung (vielleicht) und Zertifizierung interoperabler Produkte
    - World Wide Web Consortium (W3C), Object Management Group (OMG), MPLS Forum, WiFi Alliance, Bluetooth Special Interest Group, ZigBee Alliance, …

# Einführung

- ✓ Beispiele von Rechnernetzen
- ✓ Konzept der Lehrveranstaltung
- ✓ Klassifikation von Kommunikationssystemen
- ✓ Protokolle
- ✓ Netzwerksicherheit
- ✓ Geschichte
- ■ Literatur

# Literatur

- Auswahl aus den zahlreichen Lehrbüchern
  - Kurose, Ross. Computer Networking: A Top-Down Approach. 8th Ed., Pearson Education, 2020 (deutsche Übersetzung 6. Ausgabe: Computernetzwerke: Der Top-Down-Ansatz, Pearson Education, 2014)
    - einfache und anschauliche Einführung, Fokus auf Internet, Top-Down-Ansatz, Hauptquelle der Vorlesung
  - W. Stallings. Data and Computer Communications, 10th Ed., Pearson Education, 2014
    - Autor hat große Zahl von Netzwerk-Büchern geschrieben mit jeweils unterschiedlichem Schwerpunkt, werden häufig aktualisiert
  - W. Stallings. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud, Pearson Education, 2016.
    - einfache Einführung zu neueren Netzwerkthemen
  - Tanenbaum. Computer Networks. 5th Ed., Prentice Hall, 2011 (auch auf Deutsch erschienen)
    - früheres Standardlehrbuch über Rechnernetze