Grundzüge betrieblicher Kommunikationsnetze - Fragenkatalog

1) Erläutern Sie die Bedeutung der Kommunikation für die modernen Geschäftsprozesse!

Die Kommunikation hat in heutigen Geschäftsprozessen eine hohe Bedeutung. Dies gilt sowohl für die interne als auch für die externe Kommunikation. Ein Unternehmen besitzt eine Ablauf- (Prozesse) und Aufbauorganisation (Hierarchie) → Strukturbruch. D.h. es ist notwendig festzulegen, „wer was" macht. Die Kommunikation ist notwendig, um einen reibungslosen Betrieb zu gewähren und die Prozesse so möglichst effizient und effektiv zu gestalten. Extern gibt es entlang der Lieferkette einen Informationsaustausch. Um den so genannten Bullwhip-Effekt zu verhindern, ist ein funktionierender Informationsfluss zwischen den verschiedenen Akteuren innerhalb einer Lieferkette notwendig. Der Bullwhip-Effekt beschreibt das Phänomen, dass Änderungen der Endkundennachfrage zu Schwankungen der Bestellmenge führen, die sich wie ein Peitschenhieb entlang der Logistikkette aufschaukeln können. Daher ist auch eine funktionierende Kommunikation zwischen Unternehmen und Kunden wichtig. Bei zunehmender Globalisierung und Konkurrenzdruck ist ein effizientes CRM und langfristige Kundenbindung wichtig, um am Markt bestehen zu können. Dazu ist es notwendig mittels Kommunikation die Wünsche und Bedürfnisse der Kunden möglichst genau zu erfahren.

2) Wie ist der Innovationsgrad im Bereich der Kommunikation zu bewerten?

Hoch, etwa Faktor 2 – 3 im Vergleich zur Informationsverarbeitung.

3) Skizzieren Sie das Zusammenwachsen von Information und Kommunikation!

Es können drei miteinander verbundene Ebenen des Zusammenwachsens unterschieden werden:

1. **technische Ebene**:
   Ergibt sich aus der Erweiterung der technischen Komponenten für die Kommunikation um Entwicklungen aus der DV-Welt. Rechner (d.h. informationsverarbeitende Systeme) bilden heute zunehmend die Knoten von Netzwerken an Stelle von Relais.
2. **Ebene der Leistungsbereiche**:
   Ergibt sich aus der Kommunikation zwischen Rechnern. Durch den vermehrten Einsatz von Einzelplatzrechnern und dem damit verbundenen Nachteil der dezentralen Datenverarbeitung wurden lokale Netzwerke geschaffen, um die isolierten Arbeitsplatzsysteme miteinander zu vernetzen. Dadurch sind verschiedene Formen eines Rechnerverbundes realisierbar:
   - Datenverbund
   - Lastverbund
   - Funktions- / Betriebsverbund
   - Intelligenzverbund
   - Kommunikationsverbund
   - Verfügbarkeitsverbund
3. **Ebene der Aufgabenbereiche**:
   Im Bürobereich gibt es zwei Aufgabenbereiche:
   - Erzeugen und Auswerten von Daten bzw. Informationen (Büroautomation)
   - Nachrichten- und Informationsaustausch (Bürokommunikation)

   Aus Sicht der IuK-Technik ergeben sich somit zwei Optimierungspotenziale (Büroautomation und Bürokommunikation). Die Ausnutzung beider Potenziale ist jedoch miteinander verknüpft, da sonst Medienbrüche entstehen. Heute versuchen WFMS IT-gestützte Geschäftsprozesse in einer heterogenen IuK-Systemlandschaft zu realisieren, unter Berücksichtigung verwendeter Daten bzw. Informationen.

4) Welche Arten von Rechnerverbunden kennen Sie?

Datenverbund: Gestattet gemeinsame Nutzung von im Netz gespeicherten Daten. (Bsp.: Fileserver)

Lastverbund: Erlaubt Verteilung von Lasten, insbesondere in Stoßzeiten. Partiell überlastete Rechner werden durch Umverteilung von Aufträgen entlastet und gleichzeitig bessere Antwort- und Transaktionszeiten durch eine gleichmäßige Verteilung der Aufgaben erzielt. (Bsp.: Cluster)

Funktionsverbund: Die Funktionalität eines Netzes wird durch Einbeziehung spezieller ins Netz integrierter Rechner oder Geräte erweitert. So ist es möglich, Spezial-Hardware (z.B. ein DB-Rechner oder Vektorrechner) an mehreren Orten verfügbar zu machen, ohne dass diese dort physisch vor-

handen sein müssen. Häufig ergeben sich hieraus zwei Klassen von PCs: Clients (Nutzer) und Server (Anbieter eines gemeinschaftlich genutzten Dienstes). (Bsp.: Netzdrucker)

Leistungs-/Intelligenzverbund: Die Lösung aufwändiger Probleme wird auf mehreren Rechnern verteilt. Der Lösungsweg wird so zerlegt, dass verschiedene Rechner Teilprobleme parallel lösen können. Voraussetzungen dafür sind die Möglichkeit der Problemzerlegung, der notwendige Informationsaustausch und eine Möglichkeit der Synchronisation.

Sicherheits-/Verfügbarkeitsverbund: Dient der Ausfallsicherheit. Steigert die Verfügbarkeit des Gesamtsystems bzw. erreicht eine Mindestleistung auch bei Ausfall von einzelnen Komponenten. Einfachste Form: Ein Stand-By-Rechner übernimmt die Aufgaben eines anderen ausgefallenen Gerätes.

Kommunikationsverbund: Ermöglicht die Kommunikation zwischen Personen über Rechner eines Netzes. Bsp.: Versenden von Nachrichten, Texten, Graphiken von einem Netzknoten zu einem anderen.

5) Definieren Sie die Begriffe Information, Daten, Nachricht, Zeichenträger, Syntax, Semantik und Pragmatik!

Information: Zweckorientiertes Wissen; Menge von Daten, die zu einem vorgegebenen Zweck bereitgestellt und ausgewertet werden; Nützliche Daten

Daten: Informationen, die in Form von formatierten Zeichenmengen zur Verarbeitung aufbereitet sind

Nachricht: Informationen, die in Form formatierter Zeichenmengen zur Übertragung aufbereitet sind

Zeichenträger: Repräsentation eines Zeichens

Syntax: Lehre von den formalen Beziehungen zwischen Zeichenträgern/Zeichenträgermengen (Zeichenträgerebene)

Semantik: Lehre von den Beziehungen zwischen Zeichen und Bezeichnungen (Bedeutungsebene)

Pragmatik: Lehre von den Beziehungen zwischen Zeichen und Zeichennutzern, d.h. individuellen Interpretation (Informationsebene)

6) Wie sieht ein einfaches Modell für die Face-to-Face-Kommunikation aus?

Das Medium in der Face-to-Face-Kommunikation ist die Luft. Der Sender hat eine zu übertragende Nachricht (Information mit Übertragungsziel). Diese wird für die Übertragung in Daten und schließlich in einzelne Zeichen entsprechend den jeweiligen Regeln für das Übertragungsmedium kodiert. Über das Medium Luft werden die Zeichen über ihren Zeichenträger (Schallwellen) an den Empfänger gesandt, welcher die Zeichen dekodiert, Daten erhält und entsprechend Informationen (bzw. die Nachricht) ableiten kann.

7) Was ist ein Code? Nennen Sie Beispiele!

Ein Code legt den vor der Kodierung verwendeten Zeichenvorrat (Urvorrat) und den Zielvorrat, sowie eine Kodierungsvorschrift fest. Die Vorschrift bildet Elemente des Urvorrats auf Elemente des Zielvorrats aber oder Zeichenfolgen des Urvorrats auf Elemente des Zielvorrats ab.
Beispiele: Morsecode, EBCDIC, ASCII, ANSI

8) Erläutern Sie das ISO/OSI-Referenzmodell für die Datenkommunikation (bzw. erläutern Sie die Aufgaben der Schicht „x" des ISO/OSI-Referenzmodells für die Datenkommunikation)!

ISO/OSI-Modell (ISO: International Standards Organization, OSI: Open System Interconnection): Das ISO/OSI Referenzmodell ist ein Schichtenmodell zur Strukturierung des Problems „Datenübertragung". Es besteht aus 7 Schichten, wobei die Schichten 1-4 als transportorientierte Schichten und die

Schichten 5-7 als anwendungsorientierte Schichten bezeichnet werden.
Bei der Übertragung müssen sowohl auf Empfänger als auch auf Senderseite die 7 Schichten vorhanden sein. Die oberste Schicht stellt die Kommunikation her. Die Daten werden dann an die darunter liegenden Schichten übergeben, wobei jede Schicht diese Nutzdaten um Steuerungsdaten ergänzt. Die unterste Schicht (Physical Layer) überträgt dann die Daten über ein physikalisches Übertragungsmedium zu der anderen Anwendung. Dort wandern die Daten von unten nach oben, wobei jede Schicht die entsprechenden Steuerungsdaten entnimmt und interpretiert. Dem Empfänger werden zum Schluss nur die Daten übergeben, die von dem Sender auf den Weg gebracht wurden.
Merkspruch "**P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way!".

Schicht 1: Physical Layer / Bitübertragungsschicht

- Übertragung eines Datenstroms über einen Kommunikationskanal d.h. legt die elektronischen, funktionalen und prozeduralen Parameter und Hilfsmittel für die physikalische Verbindung zwischen den beiden Knoten fest (Knoten-zu-Knoten-Verbindung). Dazu zählen Prozeduren zum Aufbau, Abbau sowie zur Aufrechterhaltung der physikalischen Verbindung.
- Als Dienst für Schicht 2: Bereitstellung der physikalischen Verbindung und der transparente Transport von Dateneinheiten
- Keine Fehlererkennung der Bitfolge → ungesichert

Schicht 2: Data Link Layer / Sicherungsschicht

- Realisiert die gesicherte Übertragung von Daten zwischen zwei im Netz direkt benachbarten Entities d.h. der Empfangsknoten fordert den Senderknoten ggf. auf, ein fehlerhaftes Datenpaket noch einmal zu senden. Wenn die Wiederholung aus irgendwelchen Gründen nicht möglich ist, liegt ein nicht behebbarer Fehler vor.
- Funktionen:
  - Segmentieren: Einteilung des zu übertragenen Datenstroms in Datenblöcke, denen jeweils eine Prüfziffer hinzugefügt wird
  - Kontrollieren (on die Pakete richtig übertragen wurden)
  - Fehlerbehandlung
  - Flussteuerung
- Dienste für Schicht 3: unbestätigte verbindungsunabhängige Dienste (keine feste Verbindung, keine Paketempfangsbestätigung, keine Rekonstruktion bei Datenverlust → Geschwindigkeit statt Sicherheit), bestätigte verbindungsunabhängige Dienste (einzelne Bestätigung jedes Pakets, keine feste Verbindung) und verbindungsorientierte Dienste (Reihenfolge der Pakete gesichert, feste Verbindung)

Schicht 3: Network Layer / Vermittlungsschicht

- Effiziente Übertragung zwischen Senderstation und Empfangsstation d.h. Übertragung der Pakete vom Ausgangsknoten zum Zielknoten mit evtl. Springen über mehrere Netzwerkknoten.
  - adaptives Verfahren (Anpassung an augenblickliche Situation im Netz → Neuberechnung der Routing-Tabellen in gewissen Abständen)
  - nicht adaptiv (Fluten: Weitergabe jeder Nachricht an alle benachbarten Knoten)
  - statisches Routen (Wege in einem Netzwerk werden „einmalig“ konfiguriert → Routingtabelle)
- Unterste Schicht der Ende-zu-Ende Übertragung
- Wegwahl (Routing) einschließlich Verwaltung der benötigten Ressourcen bei den beteiligten Netzknoten und Fehlerbehandlung
- Multiplexen mehrerer Verbindungen über einzelne Teilstrecken
- Flusskontrolle gegen Überlastung durch zu schnelle Datenübertragung
- Unterteilung in:
  3 a) Subnet Access → wickelt die teilspezifischen Protokolle ab (Routing im Teilnetz)
  3 b) Subnet Enhancement → ergänzt die Funktionen der Teilnetze so, dass die Anforderung der Schicht 3 c) erfüllt werden
  3 c) Internet → wickelt teilnetzunabhängige Protokolle ab (Routing zu den Gateways etc.)

Schicht 4: Transport Layer / Transportschicht

- Bildet die Schnittstelle zwischen transportorientiertem und anwendungsorientiertem Protokoll d.h. realisiert die gesicherte und reihenfolgegerechte Übertragung von Daten zwischen dem Sende- und Empfangsknoten
- Richtet eine logische Ende-zu-Ende Verbindung zwischen zwei Prozessen ein, überwacht diese und baut diese ab
- Kann die Gesamtnachricht in Einzelpakete zerlegen (Segmentierung) oder mit anderen Nachrichten zu sinnvoll behandelbaren Einheiten zusammenfassen (Blocking)
- Dienste:
  - Klasse 0: keine Fehlerkontrolle, kein Splitten / Multiplexen
  - Klasse 1: einfache Fehlerbehandlung, keine zusätzliche Fehlerkontrollen, aber Versuch der Fehlerbehebung
  - Klasse 2: Multiplexklasse: bei Bedarf mehrere Transportverbindungen über eine Netzverbindung
  - Klasse 3: Funktion von Klasse 1 + 2
  - Klasse 4: zusätzlich zu Klasse 3 wird die Vollständigkeit, Eindeutigkeit und Sequenz der Pakete beim Datagrammdienst garantiert, Fehlerbehandlung/-erkennung

Schicht 5: Session Layer / Kommunikationssteuerungsschicht

- Realisiert eine „Sitzung“, d.h. stellt die Schnittstelle zwischen anwendungsorientierten höheren Schichten und der „Echtzeit“-Datenkommunikationsebene dar. Sie stellt die Mittel zur Verfügung, Teilnehmerverbindungen von Datenendeinrichtungen zu Datenendeinrichtungen aufzubauen, geregelt durchzuführen und auch wieder zu beenden. Auf jeder Verbindung der Schicht findet zu jedem Zeitpunkt nur jeweils eine Session statt!
- Beziehung zwischen Verbindung auf Schicht 5 und Verbindung auf Schicht 4:
  - Eine Verbindung auf der Session Layer entspricht genau einer Transportverbindung und umgekehrt
  - Mehrere Sessions werden über eine Transportverbindung abgewickelt
  - Eine Session wird (nacheinander) über mehrere Transportverbindungen durchgeführt
- Synchronisierung der Datenübertragung

Schicht 6: Presentation Layer / Darstellungsschicht

- Passt die Darstellung der Daten der kommunizierenden Prozesse an die Darstellung an, die für den Transfer benötigt wird
- Kann Daten verschlüsseln oder komprimieren

Schicht 7: Application Layer / Anwendungsschicht

- Realisiert die Schnittstelle zum Sender / Empfänger der Kommunikation und stellt grundsätzliche Anwendungen von Kommunikationssystemen zur Verfügung:
  - File Transfer
  - Remote Job Entry
  - etc.

9) Bewerten Sie die Schnittstelle zwischen der Schicht 4 und der Schicht 5 des Modells!

Trennung zwischen anwendungs- (5 – 7) und transportorientierten (1 – 4) Schichten → QoS (Bewegtbildkommunikation vs. Dateiübertragung)

10) Was sind Peer-to-Peer-Entitäten; wie kommunizieren diese miteinander?

Peer-to-Peer-Entität
- Entitäten befinden sich auf derselben Schicht (bei Sender und Empfänger)
- kommunizieren miteinander

Kommunikation
- über Dienste der darunter liegenden Schicht
- im Header / Trailer befinden sich die Steuerdaten für die entsprechende Ebene

11) Kennen Sie alternative Ansätze zum ISO/OSI-Referenzmodell für die Datenkommunikation?

TCP/IP-Stack: Der Unterschied zum ISO/OSI-Referenzmodell besteht darin, dass die Schichten 5 bis 7 im TCP/IP-Stack als eine Schicht (Anwendungsschicht) angesehen werden.

12) Welche Arten von Leitern unterscheidet man? Welche Leiter spielen heute die größte Rolle? Was bedeuten Begriffe/Spezifikationen wie CAT-5?

Metallische und Nicht-Metallische Leiter

Kupferkabel
- Koaxial („Antennenkabel"): Innenleiter aus Kupfer mit Isolierung und Mantel
  - Realisiert die Schnittstelle zum Sender / Empfänger der Kommunikation und stellt grundsätzliche Anwendungen von Kommunikationssystemen zur Verfügung:
  - Thicknet / Yellowcable: 1 cm Durchmesser, Kabellänge bis 500m (10 Base 5)
  - Thinnet / Cheapernet: 0,5 cm Durchmesser, Kabellänge bis 185 m (10 Base 2)
- Twisted Pair („Adernpaare"): isolierte Adern, die umeinander gedreht sind
  - UTP (Unshielded Twisted Pair) → die einzelnen verdrillten Adernpaare besitzen keine extra Einzelabschirmung
  - STP (Shielded Twisted Pair) → jedes Adernpaar ist einzeln abgeschirmt
  - Screened: Sowohl UTP als auch STP gibt es screened. Screened bedeutet, dass zusätzlich alle Adernpaare durch einen Gesamtmetallschirm abgesichert sind

Lichtwellenleiter: Ein dünner Glasfaden umgeben von einer konzentrischen Glasschicht (cladding), hoher Biegeradius.

Die größte Rolle spielen heute UTP Kabel. Sie können in verschiedene Kategorien eingeteilt werden, die Auskunft über die Eigenschaften des Kabels geben:

Kategorie	Übertragungsrate	Einsatzgebiet
1	1 Mbps	Analoge Sprachübertragung
2	4 Mbps	IBM Verkabelung Typ 3
3	10 Mbps	10-Base T, 100 Base T4 , ISDN
4	16 Mbps	16 Mbit Token Ring
5	100 – 1000 Mbps	100 Base Tx, 1000 Base T, ATM
6	1000 Mbps	100 Base T, 1000 Base T, ATM
7	Im Normierungsstadium	

13) Was bedeutet Routing; welche Ansätze für das Routing kennen Sie?

Wegwahl in vermaschtem Netz (s.o., Schicht 3). Routing ist das „Wegfinden" innerhalb eines Netzes. Dazu werden sogenannte Routingtabellen verwendet, in denen bekannte Zieladressen aufgelistet sind.

Statisches Routing: Die Routingtabellen werden manuell angelegt
Dynamisches Routing: Der Router legt die Routingtabelle selbst an und „pflegt" diese
Internes Routing: Kann in einem autonomen System z.B. geschlossenem Firmennetz eingesetzt werden. Ziel: möglichst effizient von der Quelle zum Ziel
Externes Routing: Zwischen autonomen Systemen

14) Was versteht man unter Leitungsvermittlung, was unter Paketvermittlung? Was sind jeweils die Vor- und Nachteile und die sich daraus ableitenden Einsatzgebiete?

Leitungsvermittlung (circuit switching): Feste Leitungsverbindung vom rufenden zum gerufenen Teilnehmer, die den Teilnehmern exklusiv zur Verfügung steht.

Vorteile
- Garantierte, bestimmte Dienstgüte (Datenrate, Verzögerung), die nur von den Leitungscharakteristika abhängt, nicht von äußeren Umständen (z.B. Netzbelastung) → transparente Ende-zu-Ende Verbindung
- Verarbeitungsaufwand für Zwischenknoten entsteht nur beim Verbindungsaufbau

- Keine netzseitigen Vorgaben bzgl. der zu verwendenden Protokolle erforderlich (Absprachen zwischen den Kommunikationspartnern)

Nachteile
- Reservierung der Netzwerkressourcen erfolgt während des Verbindungsaufbaus und der Verbindung; dadurch schlechte Auslastung der Ressourcen, wenn die Kommunikationspartner nicht erreichbar sind oder die Verbindung nicht während der gesamten Dauer ihres Bestehens voll auslasten
- Zahl der schaltbaren Verbindungen begrenzt
- Der Teilnehmer kann „besetzt" sein
- Zusammenbruch der Leitungsverbindung führt zum Zusammenbruch der Kommunikation

→ Leitungsvermittlung ist geeignet, wenn die Kommunikationspartner die volle Leitungskapazität für einen nicht geringen Zeitraum benötigen (Senden von Daten mit gleichmäßig hoher Datenrate [Sprachkommunikation], Übertragung großer Datenmengen). Das wichtigste und größte leitungsvermittelnde Netz ist das Fernsprechnetz.

Paketvermittlung (packet switching): Die Nachricht wird in ein Paket mit fester Maximallänge zerlegt, die als geschlossene Einheit jeweils auf einen individuellen Weg über Zwischenknoten (wo sie zwischengespeichert werden) zum Empfänger gesandt werden.

Vorteile
- Keine exklusive (unnötige) Reservierung von Ressourcen
- Auch bei unregelmäßiger und insgesamt geringer Nutzung durch die einzelnen Teilnehmer ist eine sehr gute Auslastung der Verbindungswege möglich, da über einen physikalischen Übertragungskanal mehrere Kommunikationsverbindungen geführt werden können
- Netzzugriff wird garantiert (allerdings nicht mit garantierter Dienstgüte)
- Ausfall von Knoten oder Verbindungsstrecken führt nicht notwendigerweise zum Zusammenbruch einer Kommunikationsverbindung
- Über einen Netzzugang ist die Verbindung zu mehreren Kommunikationspartnern möglich

Nachteile
- Durch die mit jedem Paket zu übertragenden Steuerinformationen entsteht ein Overhead
- Für jedes Paket entsteht in jedem Zwischenknoten Bearbeitungsaufwand und außerdem Bedarf an Speicherplatz für Zwischenspeicherung
- Zusätzlicher Aufwand
  - Auf Seiten des Senders: Zerlegung der Pakete
  - Auf Seiten des Empfängers: Wiederherstellung der Sequenz der Pakete; Nachfordern verlorener Pakete, Erkennen von Duplikaten etc.
- Durchsatz (Datenrate) hängt von der sich dynamisch verändernden Verkehrslast ab

→ Paketvermittlung ist bei unregelmäßiger und stoßweise auftretender Last geeignet (typisch für Datenkommunikation).

Zwei Betriebsarten möglich:
Verbindungslos: Paket hat individuellen Weg. Die Pakete werden jeweils als in sich geschlossene Einheit auf einem individuellen Weg ausgehend vom Sender über Zwischenknoten bis zum Empfänger transportiert. Ein Paket wird bei jedem Zwischenknoten solange gespeichert, bis die Entscheidung gefallen ist, auf welchem Weg es weiter übertragen wird und dieser Weg „frei" ist.
Verbindungsorientiert: Aufbau der Verbindung analog zu Leitungsvermittlung. Bearbeitungsaufwand verringert sich, da der Weg nicht für jedes Paket gesondert ermittelt und gespeichert werden muss. Allerdings kann, wenn der Weg einmal festliegt, keine dynamische Anpassung des Übertragungsweges mehr erfolgen.
Vergleich: Verbindungsloser Dienst eignet sich vor allem dann, wenn in unregelmäßigen Abständen kurze Nachrichten zu übertragen sind. Verbindungsorientierter Dienst ist besser geeignet bei großen zu übertragenden Datenmengen.

15) Welche Probleme bezüglich der Datendarstellung bestehen aus der Sicht der Datenkommunikation? Wie ist der grundsätzliche Ansatz, diese zu lösen?

Probleme:
- unterschiedliche eingesetzte Codes bei Computern
- unterschiedliche Darstellungsformate für Zahlen (z.B. Integer-Größe, …)
- unterschiedliche Nummerierung der Bits eines Bytes (0..7 / 7..0)

Lösung: Transfercodes (besteht aus zwei Komponenten):
- Transfersyntax (ASN.1) [Definition von Datenstrukturen]
- Encoding-Rules (Abbildung der Typen auf die Bitebene)

16) Wie werden Komprimierungsalgorithmen klassifiziert?

- Verlustfrei vs. Verlustbehaftet
- Entropiekodierung vs. Quellkodierung
  - Die Entropiekodierung ist eine Methode zur verlustfreien Datenkompression, die jedem einzelnen Zeichen eines Textes eine unterschiedlich lange Folge von Bits zuordnet. Im Gegensatz dazu stehen Stringersatzverfahren, die eine Folge von Zeichen des Originaltextes durch eine Folge von Zeichen eines anderen Alphabets ersetzen. Eine Entropiekodierung ist unabhängig vom Inhalt, beispielsweise Läuflängenkodierung: Anstatt die Zeichen 1111111111 zu speichern, wird nur 1x10 gespeichert (also zehn Mal das Zeichen 1), was natürlich viel kürzer ist. Das kann man machen, auch wenn man nicht weiß, was das jetzt eigentlich für Daten sind.
  - Die Quellkodierung ist abhängig vom Inhalt, zum Beispiel beim Algorithmus um Bilder abzuspeichern. Dieser Algorithmus funktioniert nur bei Bilddaten, ist also abhängig vom Inhalt.

17) Welche grundsätzlichen Arten der Verschlüsselung werden unterschieden? Wie sind die jeweiligen Vor- und Nachteile?

Symmetrische Verschlüsselung (128 Bit – 256 Bit)

Vorteile:
- Gute Performance

Nachteile:
- Sicherer Austausch des Schlüssels muss gewährleistet sein (secret key)
- Nicht zum Signieren geeignet
- Für jeden Kommunikationspartner muss ein eigener Schlüssel gespeichert werden
- Angreifbar durch Brute-Force Attacken

Asymmetrische Verschlüsselung (1024 Bit – 4096 Bit)

Vorteile:
- Keine Schlüsselübergabe (private key, public key)
- Kann zum Signieren verwendet werden

Nachteile:
- Schlechte Performance (Faktor 100 langsamer als symmetrische Verschlüsselung)

Hybride Verschlüsselung (Mischung aus Asymmetrischer und Symmetrischer Verschlüsselung)

Vorteil:
- Sehr sicher

Nachteil:
- Sehr aufwendig / langsam

18) Welche Klassen von Netzwerken unterscheidet man?

- GAN: Global Area Network (Internet)
- WAN: Wide Area Network (begrenztes Gebiet, bspw. Land)
- MAN: Metropolitan Area Network (Stadtnetze)
- CAN: Campus Area Network
- LAN: Local Area Network

Die Übergänge sind aber z.T. fließend.

19) Was ist eine Topologie; welche Arten unterscheidet man?

Topologie: Strukturmuster
- der Verkabelung (physikalische Topologie)
- der Zugriffsart auf das Medium (logische Topologie)

Netzwerktopologien:
- Bus
- Ring
- Stern
- Baum
- Vermaschte Netze

Prinzipiell lässt sich jede physische Topologie mit jeder logischen Topologie verknüpfen. Die logische Topologie von Rechnernetzen kann von der physischen abweichen.

20) Stellen Sie kurz die klassischen Netze im LAN-Bereich vor!

Ethernet (802.3)
- Nicht echtzeitfähig
- Sehr kostengünstig
- Relativ schlechtes Lastverhalten
- 5-4-3 Regel
- Anwendung: Bürobereich

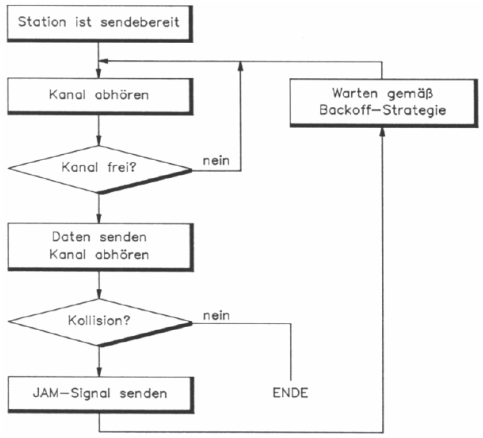
Token Bus (802.4)
- Hohe Ausfallsicherheit (pures Bussystem)
- Ring Topologie
- Reihenfolge der Stationen wird nicht durch die hardwaremäßige Verbindung, sondern rein logisch durch die Adresszuordung erledigt
- Jede Station kennt ihren Nachfolger
- Echtzeitfähig
- Teuer
- Anwendungsgebiet: Automobilindustrie

Token Ring (802.5)
- Logisch: Ringstruktur
- Physikalisch: Token Ring / Token Passing
- Sehr stabil
- Sehr teuer
- Echtzeitfähig
- Anwendungsgebiet: überall, wo Prozesse in Echtzeit gesteuert werden

Alle Netze können ca. 10 Mbit/s und bestehen aus Koaxialkabel.

21) Skizzieren Sie das CSMA/CD-Verfahren sowie die Backoff-Strategie!

CSMA/CD: Carrier Sense Multiple Access / Collision Detection



Jede Station kann zu senden beginnen, wann sie will, da die einzelnen Stationen jederzeit und konkurrierend Zugang (Multiple Access) zum gemeinsamen Übertragungsmedium haben. Die sendewilligen Stationen jedoch hören vor dem Senden ihrer Daten das Netz ab, ob nicht bereits ein anderes Gerät Daten überträgt (carrier sense). Falls zwei Stationen bei freiem Medium gleichzeitig mit dem Senden beginnen sollten, wird die Datenübertragung durch Kollisionserkennung (collision detection) abgebrochen.

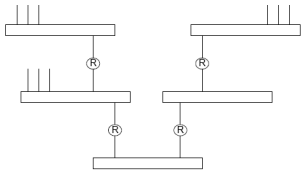
Die sendewillige Station hört das Medium ab, bevor sie eine Übertragung startet. Findet sie das Medium frei, beginnt sie mit der Übertragung. Während der Übertragung hört die sendende Station das Medium weiter ab. Die Sendestation bricht die Datenübertragung ab, falls sie eine Kollision feststellt (erkennbar dadurch, dass sie etwas anderes hört als sie selbst gesendet hat), und startet nach einer durch die Backoff-Strategie festgelegten Wartezeit einen neuen Übertragungsversuch. Nach dem Erkennen einer Kollision sendet sie ein Jam-Signal. Dieses Signal stellt sicher, dass alle Stationen das Auftreten der Kollision registrieren und ihrerseits gemäß der Backoff-Strategie warten. Dies ist eine Vorsichtsmaßnahme, da es zu einer sicheren Kollision kommt, wenn mehrere Stationen während einer laufenden Übertragung sendebereit werden und unmittelbar nach Beendigung dieser Übertragung selbst zu senden beginnen.

Backoff-Strategie (zufällig):
1. Kollision (2 Möglichkeiten): direkt senden oder 1 Zeiteinheit warten
2. Kollision (4 Möglichkeiten): direkt senden, 1, 2 oder 3 ZEs warten
3. Kollision (8 Möglichkeiten): direkt senden, 1, 2, 3, 4, 5, 6 oder 7 ZEs warten
…
10. Kollision (2^{10} Möglichkeiten)
…
16. Kollision (bis zur 16. Kollision immer 2^{10} Möglichkeiten)
Danach Aufgabe, Netzwerkkarte meldet "Netzwerk zur Zeit nicht verfügbar"

22) Wie ist der grundsätzliche Aufbau eines Ethernet; was bedeutet die 5-4-3-Regel?

5-4-3 bedeutet, dass das Ethernet maximal 5 Segmente, 4 Repeater und 3 Segmente mit Endgeräten umfassen darf.

Grundsätzlicher Aufbau anhand 10 BASE T:
- 5,4,3 Regel
- Stern
- Verbindungen maximal 100 Meter



23) Welche wichtigen Ethernet-Varianten kennen Sie?

10 Base 5
- 10 Mbit/s Basisband
- 500 m Segmentlänge
- bis zu 500 Stationen
- Koaxialkabel
- Busverkabelung

10 Base 2
- 10 Mbit/s Basisband
- 185 m Segmentlänge
- Koaxialkabel
- Busverkabelung

10 Base T:
- UTP Kabel
- Sterntopologie
- Multiport-Repeater = Hub
- zunächst Halbduplex, dann vollduplex

100 Base T (Fast Ethernet)
- 100 Mbit/s
- UTP Kabel
- Sterntopologie

1000 Base Tx bzw. Fx (Gigabit Ethernet)
- Kollisionen spielen keine Rolle → Paket kann trotzdem richtig empfangen werden
- nicht mehr voll abwärts kompatibel, weil größere Mindestpaket-Größe

10000 Base Fx (10 Gigabit Ethernet)
- kein CSMA/CD

24) Was bedeuten die Begriffe Repeater, Hub, Bridge, Router, Switch?

Repeater
- Schicht 1
- Empfängt ein Signal, verstärkt dieses und sendet es weiter

Hub
- Schicht 1
- Multiport-Repeater (Repeater mit mehr als zwei Anschlüssen, sendet ungerichtet an alle Teilnehmer im Netz), ermöglichen Sternverkabelung

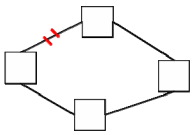
Bridge
- Schicht 2
- übernimmt grundsätzlich die Aufgaben eines Hubs
- kann MAC-Adressen von Quelle und Ziel lesen, baut entsprechende Routing-Tabelle (MAC-Adresse ↔ Port) auf [MAC-Addr.: weltweit eindeutige Adresse für eine Netzwerkkomponente in einem lokalen Netz], „lernt“ also welches Gerät sich hinter welchem Anschluss verbirgt
- sämtliche Protokolle werden unbearbeitet weitergeleitet
- kann unterschiedliche Übertragungsraten und Zugriffsverfahren umsetzen

Router
- Schicht 3
- kann heterogene Netze verbinden
- verwendet Routingtabelle (gibt an, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netzwerk erreichbar ist)
- entscheidet über den schnellsten Transportweg
- verwendet IP-Adressen statt MAC-Adressen

Switch
- Schicht 2 oder 3, Bridge oder Router mit Switching-Technologie
- sind in der Lage mehrere Datenpakete gleichzeitig und praktisch ohne Verzögerung von dem jeweiligen Eingangsport zu den Ausgangsports zu vermitteln
- für Neugeräte heute selbstverständlich

25) Was bedeutet der Begriff Spanning-Tree?

Verfahren/Algorithmus, der die Funktionalität eines Ethernets auch dann herstellt, wenn es physikalisch einen Zyklus gibt. Ist implementiert in Repeatern/Routern: es wird festgelegt, welche Verbindung nicht „aktiv" ist.



26) Was sind Broadcasts, was Multicasts; wie schätzen Sie deren mögliche Auswirkungen auf ein Netz ein?

Broadcast: Alle Knoten im Netzwerk empfangen die Nachricht.
Multicast: Nachrichten werden an mehrere Teilnehmer einer Gruppe oder an eine geschlossene Teilnehmergruppe übertragen, ohne dass sich beim Sender die Bandbreite mit der Zahl der Empfänger multipliziert wird (Gruppe dynamisch festlegbar) → hohe Netzwerkbelastung, ab einer gewissen Last sollten Bridges Broadcasts nicht weiterleiten

27) Skizzieren Sie, worin sich das bei WLAN eingesetzte CSMA vom klassischen Ethernet-CSMA unterscheidet! Wofür sind die 802.11-Standards gedacht?

WLAN: CSMA/CA → Collision Avoidance (Kollisionen vermeiden)

Wie können Kollisionen vermieden werden?
1. Anmeldung einer Sendung:
   RTS-Paket (Request to Send)
   CTS-Paket (Clear to Send)
2. In jedem Paket steht die Länge des Pakets (als Sendezeit).
3. Bestätigung des Eingangs der Nachricht durch den Empfänger Ack(nowledgement)
4. Gap = Lücke/Pause zwischen den Nachrichtensendungen
   aber: Kollisionen sind nicht vollständig zu vermeiden

Wofür sind die 802.11 Standards gedacht?
Für relativ energiestarke Geräte (z.B. Laptop ja, Handy nein)

28) Was ist Bluetooth? Skizzieren Sie stichpunktartig die wichtigsten Charakteristika!

- Funknetz für energieschwache Geräte
- Point-to-Point
- Pico-Netze
  - 1 Master, bis zu 8 Slaves, bis zu 255 Sleepern (schlafende Slaves)
  - Master bestimmt das Frequenz-Hopping, d.h. in schnellem Rhythmus wird die Sendefrequenz gewechselt
- Scatter-Netze: Verbindung von Pico-Netzen über Stationen, die in mehreren Pico-Netzen sind (kann nicht jedes Bluetooth-Gerät)

29) Wie erfolgt die Datenübertragung bei ATM?

- Slots (kurz, feste Länge) statt Frames
- Verwürfelung der Slots einer Nachricht (aus statistischen Gründen: QoS-Parameter sind nämlich statistische Werte) - im Gegensatz zu sequentiell, d.h. Pakete werden bewusst in eine unterschiedliche Reihenfolge gebracht und versendet.

30) Was ist Außenbandsignalisierung; was bedeutet der Einsatz des Verfahrens für die Kompatibilität von ATM zum ISO-OSI-Referenzmodell?

Außenbandsignalisierung statt Inbandsignalisierung → eigener Kanal für die Signalisierung, also z.B. für die Nachricht, dass ein Verbindungsaufbau und von wem welcher Kommunikationsdienst gewünscht wird

Bsp. ISDN:

D-Kanal (Signalisierung 16 kbit/s)

B-Kanal 1 (Datentransfer max. 64 kbit/s)

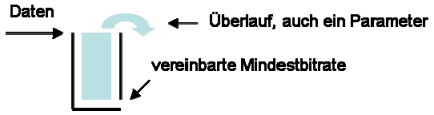
B-Kanal 2 (Datentransfer max. 64 kbit/s)

Kompatibilität
ISO/OSI: eindimensional
ATM: dreidimensional (Control/Signalisierung, User/Nutzdaten, Management/interne Netzwerkdaten)
- man benötigt 3-mal ISO/OSI Stack, um ATM zu realisieren
- etwas inkompatibel

31) Erläutern Sie den QoS-Ansatz von ATM! Was ist insbesondere das Leaky-Bucket-Verfahren?

Vertrag zwischen dem Netz und jedem Nutzer, bestehen aus:

Grunddienst
- CBR (Constant Bit Rate), konstante zugesicherte vereinbarte Bitrate = teuer
- VBR (Variable Bit Rate), zugesicherte maximale Bitrate = auch teuer
- AVR (Available Bit Rate), garantierte Basisrate + Maximalrate, Leaky-Bucket-Verfahren (Pakete werden in eine FIFO-Schlange einsortiert



- UBR (Undefined Bit Rate), am günstigsten

QoS-Parameter, z.B.
- Cell Loss Rate: Anzahl der verloren gehender Slots
- Cell Error Rate: Anzahl der verfälschten Slots
- Jitter: maximaler Abstand zwischen zwei Zellen einer Sendung usw.

32) Grenzen Sie die Begriffe Internet, Intranet und Extranet voneinander ab! Nennen Sie Klassen von Diensten, die ein Intranet anbieten kann! Welche Akteure kann man in einem Internet unterscheiden?

Internet
Weltweites Netzwerk auf Basis von TCP/IP mit mehreren Millionen Rechnern, für jedermann offen (GAN)

Intranet
Kommunikationsnetz auf Basis von Internet-Technologien, das dem Informationsaustausch innerhalb einer begrenzten Interessensgemeinschaft dient → intra-organisationell (Sensible Daten → Sicherheit)

Extranet
Variante des Intranets, bei dem Informationsflüsse aus dem Internet und dem Intranet verknüpft sind.

Dienste im Intranet
- Kommunikation und Zusammenarbeit
- Information-Sharing and Management
- Navigation = Informationsverlinkung
- Zugriff auf Anwendungen
- Netzwerk Service
- Mitarbeiter-Portale → Wissensmanagment

Akteure im Internet

- Informationsanbieter
- User
- Webmaster….

33) Erläutern Sie die Begriffe „Dienst im Internet“ und „Protokoll“! Nennen Sie fünf Dienste im Internet sowie für die einzelnen Dienste jeweils das bzw. die dahinter stehenden Protokolle!

Ein Dienst ist eine Funktion(alität), die im Internet zur Verfügung gestellt wird. Realisiert werden die Dienste durch entsprechende Protokolle.

Dienst	Protokoll
E-Mail	SMTP, POP3, IMAP4
News	NNTP
World Wide Web	HTTP
Filetransfer	FTP
Terminalzugang	TELNET
Chat	IRC
Directory Service	LDAP
Name Service	NSP (setzt auf UDP auf)

34) Was ist die Aufgabe der Protokolle IP, TCP und UDP; welcher Ebene des ISO/OSI-Referenzmodells sind die einzelnen Protokolle zuzuordnen?

TCP, IP und UDP sind Teil der Protokollfamilie für das Internet.

IP
- Schicht 3
- Transportprotokoll
- Aufgabe: Segmentierung der Daten in Pakete

TCP
- Schicht 4
- Aufgabe: Sicherung des Transports/der Übertragung
- Transportprotokoll

UDP
- Schicht 4
- Aufgabe: Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen
- keine Fehlerkorrektur, daher effizient

35) Was ist eine IP-Adresse; wie ist der Aufbau einer solchen Adresse?

Eine IP-Adresse wird auf Schicht 3 ("IP"-Schicht) realisiert. Sie besteht aus der Netz-ID (Netzwerkadresse) und der Host-ID. Eine IP-Adresse (IPv4) besteht aus vier Bytes und ist in der Form xxxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx (binäre Notation) bzw. 0-255.0-255.0-255.0-255 (dezimale Notation) aufgebaut. Sie kennzeichnet einen Rechner in einem Netzwerk. IP-Adressen werden in 3 Klassen unterteilt:

Class A: Das erste Bit ist eine 0, d.h. die IP-Adresse liegt zwischen 0.xxx.xxx.xxx und 126.xxx.xxx.xxx (127.0.0.1 bezeichnet den Localhost). Anzahl Netzwerke: 126 , Anzahl Netzwerkknoten: 16.777.216 (2^{24}) -2, Subnetzmaske: 255.0.0.0

Class B: Die ersten beiden Bits sind 10, d.h. die IP-Adresse liegt zwischen 128. 0.xxx.xxx und 191. 255.xxx.xxx. Anzahl Netzwerke: 16.384, Anzahl Netzwerkknoten: 65.536 (2^{16}) -2, Subnetzmaske: 255.255.0.0

Class C: Die ersten Bits lauten 110, d.h. die IP-Adresse liegt zwischen 192.0..0.xxx und 223.255.255.xxx. Anzahl Netzwerke: 2.097.152, Anzahl Netzwerkknoten: 256 (2^8) -2, Subnetzmaske: 255.255.255.0

Die IP-Adressen 192.168.xxx.xxx sind für den privaten Gebrauch bestimmt. Die Subnetzmaske bestimmt, welcher Teil der IP-Adresse die Netz- bzw. welche die Host-ID darstellt:

	Beispiel 1	Beispiel 2	Beispiel 3
IP-Adresse	120.96.1.200	172.96.1.200	192.96.1.200
Subnet-Mask	255.0.0.0	255.255.0.0	255.255.255.0
Netz-ID	120	172.96	193.96.1
Host-ID	96.1.200	1.200	200

36) Was ist eine URL? Skizzieren Sie die Grundstruktur der URL und geben Sie ein Beispiel für eine URL!

Eine URL (Uniform Resource Locator) ist ein dienstunabhängiges Adressierungsschema. Es besteht aus zwei Teilen:
- Teil 1: Spezifikation des Dienstes = generelles Schema
- Teil 2: Spezifisch für den Dienst = spezifisches Schema

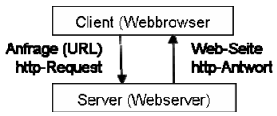
Beispiele
http://www.uni-due.de
mailto: stefan.eicker@icb.uni-due.de

37) Was ist das WWW, was sind die „Player" im Bereich des WWW?

Das WWW (World Wide Web) ist ein Dienst. Es entstand 1989 als Projekt am CERN in Genf.
„Player": W3C (World Wide Web Consortium): Gremium zur Standardisierung das World Wide Web betreffender Techniken, z.B. HTML, CSS und XML. Neben dem W3C gibt es auch noch Industrie-Konsortien.

38) Skizzieren Sie den Ablauf, den das http-Protokoll vorsieht!

Das Hypertext Transfer Protocol basiert auf einer zustandslosen Client-Server-Architektur.



39) Nennen Sie fünf Sprachen, die zur Spezifikation von Web-Seiten verwendet werden!

HTML/xHTML
- Hypertext Markup Language
- Inhalt, Struktur und Layout

CSS
- Cascading Style Sheets
- Layout

XML
- Extended Markup Language
- Inhalt und Struktur (Trennung von Inhalt und Darstellung)

VRML
- Virtual Reality Modelling Language
- Definition dreidimensionaler Räume

Grafikformate
- GIF
- JPEG
- PNG ..

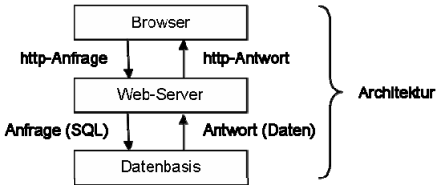
40) Erläutern Sie das Domain Name System!

Das DNS erlaubt es, statt unhandlicher numerischer IP-Adressen einen Computer mit einem Host-Namen anzusprechen. Die Auflösung der Namen erfolgt über einen DNS-Server, der mit Hilfe von Listen die Zuordnung von IPs zu den entsprechenden Namen pflegt. Die Namen werden von rechts nach links aufgelöst, beginnend mit der sogenannten Top-Level-Domain (Länderorientiert (.de) oder Funktionsorientiert (.org)). Es folgen durch einen Punkt getrennt ein oder mehrere Domain-Namen. Der Eintrag ganz links entspricht dem Hostnamen.
Allgemeiner Aufbau: Rechnername.[subdomain.]domain.top-level-domain

41) Erläutern Sie, wofür im Web einerseits clientseitige und andererseits serverseitige Dynamik benötig wird! Skizzieren Sie insbesondere die Architektur datenbankgestützter Web-Anwendungen!

Clientseitige Dynamik
- Validierung von Benutzereingaben
- Navigationselemente (z.B. Tree View)
- Animationen

Serverseitige Dynamik
- Dynamische Textbausteine (Datum, Uhrzeit, Counter)
- Profiling (One-To-One-Markierung, gezielt Leute ansprechen [z.B. Amazon])
- Datenbankzugriff (Produktkataloge)
- eCommerce (Warenkorbsysteme)
- Intranets (Dokumentenmanagementsysteme)



42) Welche Sicherheitsprobleme bestehen im Internet?

- Datenübertragung bei allen gängigen Internet Diensten unverschlüsselt: IP-Datagramme können in jedem weiterleitenden Knoten im Internet eingesehen werden (keine Abhörsicherheit)
- IP-Adresse zur eindeutigen Authentifizierung der Kommunikationspartner nicht geeignet: keine fixe Verbindung zwischen IP-Adresse und Nutzer; Versand gefälschter Datenpakete möglich (keine Verlässlichkeit der Senderadresse)
- Zahlreiche Sicherheitslücken im Domain Name Service (DNS): durch das sogenannte DNS-Spoofing kann ein Anbieter unter einem beliebigen Domainnamen im Internet auftreten
- Datenintegrität nicht gewährleistet: jeder weiterleitende Knoten im Internet ist in der Lage, IP-Datagramme herauszufiltern oder zu modifizieren

43) Was ist eine Firewall, welche drei Grundtypen/-funktionen werden unterschieden?

Eine Firewall ist ein System, das Richtlinien zur Zugriffsbeschränkung zwischen zwei Netzwerken durchsetzt. Sie schützt Netze/Rechner gegen Angriffe von außen. Grundtypen:

Paketfilter
- Prüfung jedes einzelnen IP-Pakets (Schicht 3)
- Begrenzung auf bestimmte Absender- und Empfängeradresse
- Oft in Routern integriert; auch softwaretechnische Lösung

Circuit Level Gateways
- Transportprotokollebene (TCP, UDP) (Schicht 4)
- Überwachung von Verbindungen

Application Gateways (Proxy Server)
- Gateway führt alle Aktionen stellvertretend für den Client aus der eigentliche Client wird von außen nicht bemerkt und kann (erst einmal) nicht angegriffen werden
- aufwendigste Form
- Erkennen von dienst-/protokollabhängigen Angriffsmustern

44) Stellen Sie kurz Internet-Protokolle vor, die versuchen, Sicherheit zu realisieren!

Auf Anwendungsschicht (Schichten 5-7): S-HTTP *(HTTPS nur in Verbindung mit SSL)*
- dient zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser

Auf Transportschicht (Schicht 4): SSL (Secure Socket Layer)
- Verschlüsselung der Verbindung
- z.Z. häufigstes Sicherungsverfahren
- zunächst asymmetrische Public-Key-Verbindung zwischen Browser und Server, über die ein symmetrischer Schlüssel und Zertifikate ausgetauscht werden kann
- dann symmetrische Verschlüsselung für eigentliche Datenübertragung

Auf Vermittlungsschicht (Schicht 3): IPsec
- Verschlüsselung für IP-Pakete
- soll Vertraulichkeit, Authentizität und Integrität gewährleisten

45) Was ist ein digitaler Fingerabdruck, was eine digitale Unterschrift, und wofür werden sie eingesetzt?

Digitaler Fingerabdruck
- Hash-Funktion, Text wird einem Wert zugeordnet
- aus binären Daten unterschiedlicher Länge wird eine Zeichenkette fixer Länge erzeugt
- Verfälschungssicherheit effizienter realisieren als durch vollständige Verschlüsselung der Nachricht
- Einsatz:
  - Integrität von Dokumenten
  - Hilfsmittel für Digitale Signaturen

Digitale Unterschrift
- Sender verschlüsselt seine Nachricht / seinen Hash-Wert mit seinem Private Key
- Empfänger entschlüsselt mit Public Key des Senders
- Dokument ist nicht authentisch/integer, wenn Entschlüsselung fehlschlägt
- Einsatz:
  - Authentizität
  - Integrität
  - Nichtabstreitbarkeit des Absenders

→ rechtsgültige Unterschrift!

46) Welche Angriffsarten werden im Bereich der Kryptographie unterschieden?

Brute-Force-Angriff
- Ausprobieren von sämtlichen Zeichenkombinationen
- damit sind alle Schlüssel zu brechen (Kosten- und Zeitfrage)

Known-Plaintext-Angriff
- Sowohl verschlüsselter Text als auch Klartext liegen vor
- Analyse von kryptographischen Mustern mit dem Ziel, diese entweder zu „brechen“, d.h. ihre Schutzfunktion aufzuheben bzw. zu umgehen, oder ihre Sicherheit nachzuweisen und zu quantifizieren

Replay-Angriff
- Eine komplette Nachricht wird kopiert und erneut eingespielt, durch Reaktionszeit kann auf das Verschlüsselungsverfahren geschlossen werden

Man-in-the-middle-Angriff
- Ein Dritter stellt sich zwischen die Kommunikationspartner, d.h. fängt die Daten zu seinem Zweck ab und sendet sie hinterher an den Ursprungsempfänger weiter

47) Was ist ein Zertifikat?

Ein Zertifikat stellt den Zusammenhang zwischen einem öffentlichen Schlüssel und einer bestimmten Person her. Sie sind signiert mit dem privaten Schlüssel der Zertifizierungsstelle. Angaben:

- Name des Zertifikatinhabers (ggf. Pseudonym)
- Öffentlicher Schlüssel des Zertifikatinhabers
- Authentisierungsalgorithmus des Zertifikatinhabers
- Name der Zertifizierungsinstanz, Staat
- Gültigkeitszeitraum
- Einschränkung auf bestimmte Anwendungen
- Attribute des Signaturschlüsselinhabers (ggf. Attributzertifikat)
- Angaben darüber, dass es ein qualifiziertes Zertifikat ist
- Nummer des Zertifikats

Zertifikate können auch zurückgerufen werden (als ungültig erklärt), wenn
- die evtl. vorhandene Gültigkeitsdauer abläuft
- der Authentisierungsalgorithmus unsicher geworden ist
- oder manuell vom Besitzer, wenn z.B. ein Dritter Kenntnis vom geheimen Schlüssel erlangt hat.

48) Erläutern Sie jeweils mit ein bis zwei Sätzen, was der jeweilige Dienst beinhaltet: Leased Link-SFV, Leased Link-DDV, EthernetConnect, VPN-Basic, IntraSelect, Mobile IP VPN, Datex-L, Datex-P, Datex-M, T-ATM, Frame Link Plus, Citynetz → WAN-Dienste (Telekom)

Leased-Link-SFV: Hierbei handelt es sich um eine Standard-Festverbindung (Standleitung im Telefonnetz), die eine permanente Telefon- und Datenkommunikation zwischen zugeordneten Endstellen rund um die Uhr ermöglicht.

Leased-Link-DDV: Hierbei handelt es sich um eine Datendirektverbindung. Es ist eine Standleitung rein für die Datenkommunikation, bei der beliebige Protokolle verwendbar sind. Über das Netzkontrollzentrum der DTAG werden DDV permanent überwacht. Fällt die DDV aus, kann so schnell auf den Ausfall reagiert und Gegenmaßnahmen eingeleitet werden.

EthernetConnect: EthernetConnect stellt eine transparente Ethernet-Verbindung her. Lokale Netzwerke an verschiedenen Unternehmensstandorten können mit bis zu 1 Gbit/s verbunden werden, so dass ein „großes Ethernet“ entsteht. Es wird im Glasfasernetz von T-Systems geführt und unterliegt ständiger Überwachung.

VPN-Basic: Ein Virtual Private Network (VPN) ermöglicht die Nutzung öffentlicher Netze zur Datenübertragung innerhalb eines gesicherten Tunnels. Das Ergebnis ist ein privates Netzwerk für einen geschlossenen Benutzerkreis, in dem allen Nutzern sämtliche Dienste und Anwendungen der vernetzten LANs zur Verfügung stehen – auch mobil. So ist es möglich auch im unsicheren Internet sicher zu kommunizieren. „Basic“ = von Telekom fest eingerichtet.

IntraSelect: siehe VPN-Basic, noch komfortabler

Mobile IP VPN: siehe IntraSelect, aber für mobile Geräte

Datex-L: Ist ein leitungsvermittelndes Datennetz (gewesen).

Datex-P: Beim Datex-P handelt es sich um ein digitales Netz der Deutschen Telekom zur Datenübertragung mit Paketvermittlung. Genutzt wird der Dienst insb. für E-Cash, Point-of-Sale-Anwendungen etc. Er ist geeignet für Anwendungen, die eine zuverlässige Kommunikationsverbindung benötigen, aber nur vergleichsweise kleine Datenvolumen senden/empfangen.

Datex-M: Das „M“ steht für Multimegabit. Datex-M ist ein Hochgeschwindigkeitsnetz zur Verbindung von LANs. Es läuft jedoch aus und ist somit für Neukunden nicht mehr nutzbar.

T-ATM: ATM als Dienst. Es ist einer der Datex-M-Nachfolger.

FrameLink Plus: FrameLink Plus ist ein flexibler Festanschluss, um mehrere Standort miteinander in Verbindung zu setzen. Es bietet feste virtuelle Verbindungen, die eine Mindestübertragungsbandbreite garantieren.

Citynetz: Das Citynetz ist ein breitbandiges Datennetz, das Großstädte in Deutschland verbindet. Es bietet eine hohe Bandbreite bei vergleichsweise geringen Kosten.