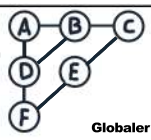
Agenten: Teile eines Systems, die Prozesse ausführen und Entscheidungen treffen. Beinhalten Komponenten, die ihre Umwelt wahrnehmen (z.B. Sensoren) und eigene Handlungsentscheidungen treffen (= autonomes Verhalten). Gesammelte Informationen fließen in Entscheidungsprozesse mit ein. Als Ergebnis der Entscheidung werden Aktoren (= Baueinheiten, die elektrische Signale in mechanische Bewegungen umsetzen) angesteuert, die Einfluss auf ihre Umwelt nehmen. **Arten der Modellierung:** Grundvoraussetzung sind Sensoren und Aktoren (= Kommunikationsschnittstellen von Agenten).
• Regelbasierte Agenten (= Reflexagenten): Beinhaltet Wenn-Dann-Regeln, die Aufgaben des Agenten in einem Satz von Regeln definieren; •Zielorientierte Agenten: Vergleicht Soll-Ist-Zustand, um Aktionen zu definieren, die zur Erreichung des Soll-Zustands beitragen.• Nutzenbasierte Agenten: Stellt die Maximierung des individuellen Nutzens in den Vordergrund, z.B. durch Abgleich verschiedener Möglichkeiten und derer Auswirkungen. Agent kann außerdem eine Risikoeinschätzung selbstständig vornehmen.

Clusterkoeffizient: Gibt an, wie stark die Nachbarn ki eines Knotens i untereinander vernetzt sind, d.h. wie viele Kanten zwischen zwei Nachbarn j und k existieren. **Globaler Koeffizient:** Clusterkoeffizient für alle Knoten eines Graphen (= Mittelwert der lokalen Clusterkoeffizienten). **Berechnung Globaler Clusterkoeffizient**: 1. Zähle die Anzahl der existierenden Kanten zwischen den Nachbarn des Knotens. 2. Teile diese Anzahl durch die mögliche Anzahl der Kanten zwischen den Nachbarn des Knotens.

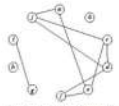


A hat zwei Nachbarn, beide miteinander vernetzt = 1
B hat drei Nachbarn, 1 vernetzt = 1/3
C hat zwei Nachbarn, keine Vernetzung = 0
D hat drei Nachbarn, 1 vernetzt = 1/3, E = 0, F = 0

Globaler Clusterkoeffizient = (1+1/3+0+1/3+0+0) / 6
= (1 + 2/3) / 6 = 5/3 : 6/1 = 5/3 x 1/6 = **5/18**

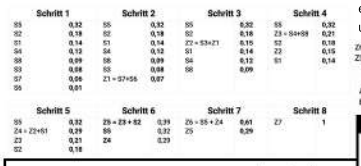
Durchmesser: Weiteste Weg (Anzahl Sprünge) zwischen zwei Knoten, der im Graphen auftaucht. 1.Suche die weitesten voneinander entfernten Knoten. 2. Bestimme die Anzahl der Sprünge, die notwendig sind, um von einem dieser Knoten zu dem jeweils anderen zu gelangen. **Mittlerer Weg:** Von A nach B = 1, von A nach C = 2, A nach D = 1, A nach E = 3, A nach F = 2. (1+2+1+3+2) / 5 = **9/5**

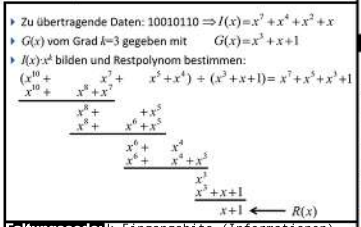
Eisverkäufer Problem: Gefangenendilemma. Veranschaulicht, dass das Bestreben jeden Mitglieds einer Gemeinschaft darin besteht, maximalen Erfolg zu erzielen, was jedoch zu einem Zustand führen kann, der für alle Mitglieder schlechter ist.**Beispiel:** 2 Eisverkäufer teilen 1000m breiten Badestrand. Optimale Position für Kunden liegt bei 250m und 750m, da maximal 250m Fußweg = gleicher Profit für beide Verkäufer. Verkäufer 1 positioniert sich 100m näher an Verkäufer 2, was höheren Umsatz für 1 und niedrigeren Umsatz für 2 zur Folge hat. Verkäufer 2 rückt 100m näher an Verkäufer 2, wodurch wieder **gleicher Profit entsteht. Irgendwann stehen beide nebeneinander bei in Mitte bei 500m Abstand. Fußgänger verlieren Lust auf Eis, da Weg zu weit. Beide Verkäufer haben gleiche Chance auf Umsatz,** jedoch ist dieser geringer (= Situation nachteilig für beide). Kooperation = gut, Konkurrenz = schlecht.**Erdös Renyi :** Zufallsgraph. Modell beinhaltet N Knoten und Wahrscheinlichkeit p. Menge E gibt Anzahl Kanten zwischen Knoten wieder. Um Small World zu bauen, werden z.B. Knoten A und B betrachtet und mit Wahrscheinlichkeit p eine Kante zwischen A und B hinzugefügt. Nun betrachtet man weitere denkbare Kanten, wobei aufgrund von Wahrscheinlichkeit p niemals garantiert werden kann, dass zusammenhängender Graph entsteht. **Nachteile:** •Keine Garantie auf zusammenhängen Graph, •Feste Anzahl Knoten. Soziale Strukturen sind jedoch in ständiger Veränderung (Knoten kommen hinzu /werden entfernt), •Zufallsgraphen Modell hat grundsätzlich Small World Eigenschaften, bildet soziale Strukturen aber nur schlecht ab.**Gefangenendilemma:** Das Gefangenendilemma ist ein mathematisches Spiel aus der Spieltheorie. Es modelliert die Situation zweier Gefangener, die beschuldigt werden, gemeinsam ein Verbrechen begangen zu haben. Die beiden Gefangenen werden einzeln verhört und können nicht miteinander kommunizieren. Kooperation führt für beide zu niedrigerer Strafe. **Kronzeugenregel:** Gesteht nur einer, wird dieser freigelassen, der andere muss z.B. für 5 Jahre hinter Gitter.


Ein Erdös-Renyi Zufallsgraph mit 10 Knoten und 9 Kanten

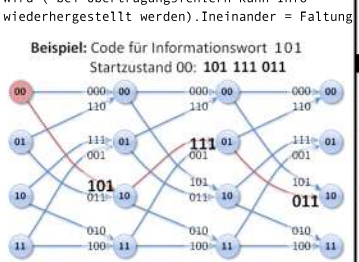
HITS: Hyperlink Induced Topic Search (HITS) Strukturanalysealgorithmus zur Identifikation von Hubs und Authorities zu einem bestimmten Thema im Webgraph. Algorithmus empfängt von Suchmaschine eine Menge S von Seitenvorschläge zu bestimmtem Thema. Menge von Seiten = Root Set S. Menge S ist jedoch nur ein kleiner Webuntergraph zu bestimmtem Thema. Um eng vernetztes Cluster zu erhalten, wird Menge S iterativ um Knoten erweitert, die auf S referenzieren bzw. auf die S referenziert (= base set). Es entsteht Graph G, welcher S, inklusive aller expandierender Knoten, beinhaltet. **Authority:** Seite dessen Inhalt sehr gut zur Suchanfrage passt, die der Benutzer gestellt hat bzw. wenn die Seite einfach sehr gut zu einem bestimmten Thema passt. Hub-Wert: Knoten, die selber meistens jedoch keine Authority sind, die aber auf eine oder mehrere Authorities verweisen. **Berechnung:** Der Authority-Wert des Knoten x ergibt sich aus der Addition der Hub-Werte der Knoten v1 bis v4. Je mehr die Knoten w1 bis w3, also die Knoten auf die der Knoten x verweist, Authorities für dieses Thema sind, desto mehr ist dieser Knoten x auch ein Hub für dieses Thema. **Page Rank:** Google Algorithmus zur Einschätzung der strukturellen Position einer Webseite, um Grad der Vernetzung (= wie stark andere auf einen Knoten verweisen) zu ermitteln.Jede Seite erhält eine Zahl (=PageRank), welche widergibt, wie stark andere Seiten auf diese Seite verweisen. **Hoher Page Rank:** Wahrscheinlichkeit, dass eine Person zufällig die Seite ermittelt, steigt. **Berechnung:** Der PageRank besteht sehr stark aus den Page Ranks aller Knoten, die auf diesen Knoten verweisen. Je renommierter die Webseite, von welcher die Verlinkung kommt, desto wichtiger erscheint die verlinkte Webseite.**Preferential Attachment:** Modell für Small Worlds. Grundidee: Neue Knoten versuchen sich mit Knoten zu vernetzen, die bereits hohe Anzahl von Verbindungen zu anderen Knoten besitzen. Je mehr Verbindungen ein existierender Knoten hat (= Valenz), desto größer die Wahrscheinlichkeit, dass ein neuer Knoten mit diesem Knoten verbunden wird.**Eigenschaften:** •Sehr viele Knoten haben eine geringe Valenz und sehr wenige Knoten haben eine sehr hohe Valenz. Und etwas mehr liegen in der Mitte.•Es sind beliebig wachsende Graphen möglich, da Anzahl Teilnehmer nicht begrenzt.

Signal Zeitliche und räumliche Änderung einer oder mehrerer physikalischer Größen zum Zweck der Informationsübertragung. Man unterscheidet drahtgebundene (= Veränderung der physikalischen Größen Spannung und Strom) und drahtlose Übertragung (=Veränderung von Frequenz, Amplitude, Trägermedium). **Signalklassen:** • Zeit- und Wertkontinuierlich = analog; • Zeit- und Wertdiskret = digital.**Arten von Signalen:** • Deterministische Signale: Periodisch (Sinus), Nicht-Periodisch (Pendel), Quasiperiodisch (EKG). • Stochastische Signale: Stationär (Rauschen), Nicht-Stationär (Nutzsignal, z.B. Sprache/Musik).**Small Worlds:** Netwerk mit Vielzahl abkürzender Verbindungen. Selbst in großen (sozialen) Netzwerken ist jeder der Teilnehmer mit einer kleinen Anzahl anderer Teilnehmer verbunden, wodurch überraschend kurze Pfade zwischen Teilnehmern entstehen. Durchschnittliche Pfadlänge = 6 (selbst in großen Netzwerken).**Tiefpass bei AD-Wandlung:** Analog-Digital-Wandler ist Bestandteil eines digitalen Verarbeitungssystems, welches analoge Signale mit Hilfe eines digitalen Signalprozessors (DSP) verändert. Hierzu müssen Signale zunächst mit Analog-Digital-Wandler digitalisiert werden. Dieser filtert analogen Signale durch einen Tiefpass und vermeidet Aliasing-Effekte.**Sample and Hold:** Auf den Tiefpass folgt ein sogenanntes Sample and Hold. Das dient dazu, das der Analog-Digital-Wandler ausreichend Zeit hat, einen Eingangswert zu verarbeiten und zu digitalisieren. Am Ausgang des digitalen Signalprozessors folgt die Digital-Analog-Wandlung. Während der Digital-Analog-Wandlung eines einzelnen Wertes kann es zu sogenannten Glitsches kommen (= Abweichungen von dem eigentlichen Zielwert). Diese Glitches werden durch einen sogenannte Deglitcher (was auch nichts anderes ist als ein Sample and Hold Glied) wieder aufgefangen.**TCP Sliding Window/Congestion Control:** Dienen Überlaststeuerung/Flusssteuerung. **Congestion Control:** Erkennt Überlastung bei Übertragung. Router auf Schicht 3 können einige Pakete zwischenspeichern. Ist dieser Zwischenspeicher voll, werden weitere ankommende Pakete stillschweigend verworfen. TCP erkennt diesen Zustand durch erhöhte Paketverlustraten (nicht bestätigte Pakete) und reduziert die Senderate. Durch langsames Steigern der Senderate tastet sich TCP an die Überlastungsgrenze heran. **• TCP Sliding Windows: Vermeidet Überlast beim Empfänger. Empfänger gibt bei Bestätigung an, wieviel Daten er zu empfangen bereit ist, bevor sein Empfangspuffer überläuft. (=Window) => Sender stellt basierend nächsten** Burst zusammen => Empfänger steuert den Informationsfluss. Trifft nun die Bestätigung für das erste Segment im Fenster beim Sender ein, so wird das Fenster um ein Segment weitergeschoben (Sliding), und das nächste Segment wird gesendet. **Beispiel TCP Sliding Window:** 4.800.000 Bit/s sollen gesendet werden. Empfangsbestätigung trifft mit 100ms Verzögerung ein. Berechne Empfangspuffergröße: 4.800.000 Bit/s * 0,1sek = 48.000 Bit/s. 48.000 Bit/s : 8 = 60.000 Bytes. **Huffman Code:** Transformiert häufig auftretende Zustände in möglichst kurze Codewörter. **Iterationsschritte:** Zustände werden zunächst nach Auftrittswahrscheinlichkeit sortiert: • Zustände sm und sn mit den kleinsten Auftrittswahrscheinlichkeiten pm und pn werden zu einem neuen Zustand pz = pn + pn zusammengefasst.• Vorgang wird wiederholt, bis nur noch zwei Zustände verbleiben. Zustand mit größter Auftrittswahrscheinlichkeit erhält Code 0, der andere Code 1. **Führe die Huffman Codierung für das nachfolgende Alphabet durch und berechne die durchschnittliche Codewortlänge:** Von rechts nach links können nun die Codeworte gebildet werden. Immer dann, wenn ein Symbol aus der Zusammenfassung zweier Symbole entstanden ist, wird eine neue Binärstelle angefügt. Dabei hat sich die Konvention eingebürgert, dem in der Tabelle weiter obenstehenden Symbol eine 1 anzufügen, dem unteren eine 0. **Durchschnittliche Codewortlänge:** (0,14 * 3) + (0,18 * 2) + (0,08 * 4) + (0,12 * 3) + (0,32 * 2) + (0,01 * 5) + (0,06 * 5) + (0,09 *3)=2,72





Faltungscode: k Eingangsbits (Informationen) werden auf n Ausgangsbits (Code) abgebildet. Zuordnung Informationen -> Code abhängig von bisher codierten Informationen, wodurch Information auch in Folgezuständen kodiert wird (=bei Übertragungsfehlern kann Info wiederhergestellt werden).Ineinander = Faltung



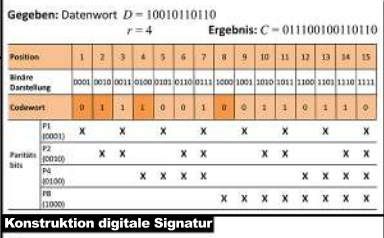
System: Menge von interagierenden, unabhängigen Komponenten und Schichten, welche einem bestimmten Zweck dienen. Komponenten besitzen Aufgaben und Schnittstellen (z.B. Informationsaustausch mit anderen Komponenten). Komponenten können selbst Systeme sein und in Teilkomponenten aufgeteilt werden.**Eigenschaften**• Besteht aus Komponenten, die miteinander in Beziehung stehen.• Ist von seiner Umwelt durch Systemgrenze getrennt.• Erfüllt mindestens eine Funktion und hat ein beschreibbares Verhalten

Antwort: I(x) = 111 001 00 = x^7+x^6+x^5+x^2; G(x) = x^5+x^2+1. Der Grad des Generalpolynoms ist 5, also wird I(x) mit x^5 multipliziert = x^12+x^11+x^10+x^7. Restpolynom bestimmen: (x^12+x^11+x^10+x^7) : (x^5+x^2+1) = x^7+x^6+x^5+x^4+x^3+x^2; R(x) = x^3 + x^2 = 1100. Berechnung Prüfsumme: C(x) = I(x) * x^5 + R(x) = x^12 + x^11 + x^10 +x^7 +**x^3 +x^2** = 111 001 000 **1100.**
Empfänger Fehler Check: 111 001 000 1100 = (x^12 + x^11 + x^10 +x^7 +x^3 +x^2) : (x^5+x^2+1) = x^7+x^6+x^5+x^4+x^3+x^2, Rest = 0 (korrekt).

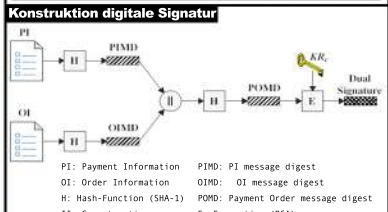
Hamming Code: Fehlerreduktionsverfahren, das dort verwendet wird, wo nicht mit klassischer Fehlerkorrektur gearbeitet werden kann und fehlerhafte Datenbestände vom Empfänger nicht erneut angefordert werden können.Jedes Bit im Codewort erhält fortlaufende binäre Nummer, beginnend mit 1.
Aufgabe1: Codewort länge n=15 (11111 00000 1111). Wie viele Paritätsbits werden benötigt? **Antwort:** 2^0= 1; 2^1= 2; 2^2=4; 2^3=8; 2^4*16 = 5 Paritätsbits

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Binär	0001	0010	0011	0100	0101	0110	0111	1000	1001											
Codewort	X	X	1	X	1	1	1	X	1	0	0	0	0	0	1	X	1	1	1	1

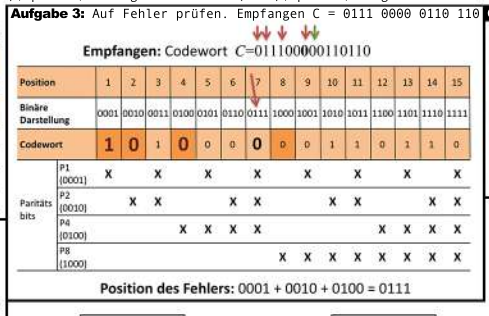
Aufgabe2: p1 = 0, da gerade Anzahl Positionen (4x1); p2 = 1, da ungerade Anzahl (5x 1); p3 = 1, da gerade Anzahl (3x1); p4 = 0; da gerade Anzahl (4x1)



Konstruktion digitale Signatur



Aufgabe 3: Auf Fehler prüfen. Empfangen C = 0111 0000 0110 110



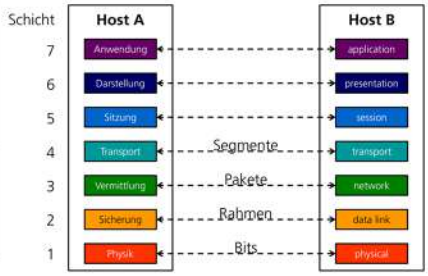
Chicken Game/Feiglingspiel:

		Fahrer A	
		Ausweichen	Weiterfahren
Fahrer B	Ausweichen	4/4	2/6
	Weiterfahren	6/2	0/0

Maximaler Nutzen:

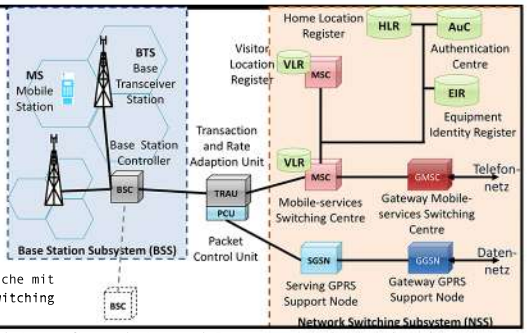
	1	2	3	4
A	weiter	ausweichen	weiter	ausweichen
B	ausweichen	weiter	ausweichen	weiter

A = 6 + 2 + 6 + 2 = 14
B = 2 + 6 + 2 + 6 = 14



ISO Schichtenmodell: Schichtenarchitektur. Ordnet Kommunikationsabläufe in Schichten ein, wobei jede Schicht nur Dienste der darunterliegenden Schicht in Anspruch nehmen kann / Dienste für höhere Schicht zur Verfügung stellt. **P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way. **Schicht 1, Physische Übertragungsschicht (Physical Layer):** AUFGABEN-> Bitweise Übertragung von Signalen zwischen benachbarten Systemen unter Verwendung des Übertragungsmediums (z.B. Koaxialkabel, Glasfaserkabel). DIENSTE-> Zum Aufbau, Abbau und Unterhaltung von (ungesicherten) physikalischen Verbindungen zwischen benachbarten Systemen und physikalische Bitübertragung, wobei Parameter wie Spannungspegel und Pulslänge beachtet werden müssen. FUNKTIONEN -> Aktivieren/Deaktivieren der physikalischen Verbindung; Bitweise Übertragung und Verwaltung von Signalen über physischen Übertragungsmedium(= Leitungskodierung), sowie Fehlerbehandlung/-verwaltung (z.B. Resynchronisierung). **Schicht 2, Sicherungsschicht (Data Link Layer):** AUFGABEN-> Gesicherte, fehlerfreie Datenübertragung von Data Frames mit Hilfe einer eigenen physikalischen Adressierung sicher (= Frame Bildung). Jeder Teilnehmer besitzt hierzu eine eindeutige Hardware Adresse (MAC Adresse), die mit - von der Vermittlungsschicht kommenden – Paketen verknüpft wird. DIENSTE-> Medienzugriffssteuerung / Flusskontrolle, die regelt, wann Station das Medium zum Senden verwenden darf, damit keine Kollisionen auftreten (nicht notwendig bei Point-to-Point und Switch Verbindungen). FUNKTIONEN -> Multiplexing (Splitten oder Zusammenfassen der Bitübertragungsstrecken = Segmentierung); Flussregelung / Medienzugriffskontrolle zwischen benachbarten Systemen (Carrier Sense Multiple Access/Collision Detection (CSMA/CD)). **Schicht 3, Netwerk-/Vermittlungsschicht (Network Layer):** AUFGABEN-> Verwaltung und Betrieb von Netzverbindungen / gesicherten Teilstrecken und Netzrouten zur Datenübertragung (= Wegevermittlung), wobei optimaler Weg durch Netzwerk genommen wird. DIENSTE-> Auf- und Abbau von Verbindungen (z.B. mit Internet Protocol (IP) und Network Address Translation (NAT)); Datenübermittlung über Netzwerkverbindungen/Netzrouten (= Ende-zu-Ende Vermittlung, Paketierung); Fehlermeldungen und -verwaltung (Internet Control Message Protocol (ICMP)). FUNKTIONEN -> Verwaltung und Betrieb von Netzverbindungen; Flussregelung und Optimierungen im Kommunikationsnetz; Fehlerbehandlung und -verwaltung. **Schicht 4, Transportschicht:** AUFGABEN-> Segmentiert Datenströme der Anwendungsschicht, um diese Segmente über die Vermittlungsschicht gesichert und transparent zum Zielknoten weiterzuleiten (= virtuelle Verbindung). DIENSTE-> Auf-/Abbau von Ende-zu-Ende Verbindungen, sowie Datenübertragung (= Dienst-zu-Dienst-Vermittlung, Sockets, UDP, UCP); Fehlerbehandlung und -verwaltung, Flusskontrolle (= inkl. Rückbestätigung für korrekte Zustellung). **Schicht 5, Sitzungs-/Kommunikationsschicht (Session Layer):** AUFGABEN-> Betreibt und verwaltet Sitzungen zwischen verschiedenen Anwenderinstanzen (z.B. mit Cookie-Management = Verwaltung von verbindungsunabhängigen Sitzungen). DIENSTE-> Dienste für den Auf- und Abbau von Sitzungen zwischen Anwenderinstanzen; Durchführung von Sitzungen (Dialogverwaltung, Synchronisation, Datenübermittlung). **Schicht 6, Darstellungsschicht (Presentation Layer):** AUFGABEN-> Empfangene Daten für die Präsentation aufbereiten und zu sendende Daten für Übertragung in geeignete Formate überführen (= einheitliche Darstellung von Daten in heterogenen Systemen), sowie Verschlüsselung und Komprimierung von Daten. **Schicht 7, Anwendungsschicht (Application Layer):** AUFGABEN-> Applikationen einordnen, welche durch untere Schichten Zugang zu Netzwerkdiensten erhalten. Bekannte Protokolle sind HTTP, DNS, IMAP, POP3 etc

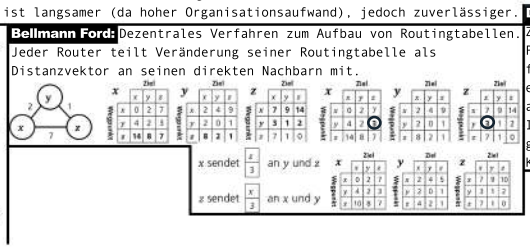
GSM: Mobilfunkkommunikation basiert weltweit auf Global System for Mobile Communication (GSM). **BTS:** Im zellulären GSM-Netz ist jedes Endgerät (= Mobile Station) durch eine Base Transceiver Station (BTS) eindeutig identifizierbar, wobei eine Base Transceiver Station (BTS) immer mehrere Zellen, welche eine Fläche ergeben, verwaltet. **BSC:** Die BTS sind drahtgebunden mit dem Base Station Controller (BSC) verbunden, welcher wiederum Gespräche zwischen zwei (an ihn angebundene) BTS vermittelt.Die BSC sind wiederum mit anderen BSC vernetzt. **BSS:** Das System, bestehend aus mehreren BTS, die an einem BSC angeschlossen sind, wird als Base Station Subsystem (BSS) bezeichnet. **TRAU, MSC und VLR:** Der Übergang vom BSC in das Kernnetz des Mobilfunkanbieters erfolgt über die Transaction and Rate Adaption Unit (TRAU), welche den bis dahin komprimierten Audiostrom in einen unkomplizierten Audiostrom umwandelt und mit Mobile-services Switching Centre (MSC) angeschlossen, welche wiederum ein Visitor Location Register (VLR) führen, welches Teilnehmer registrieren, die sich aktuell in einer Zelle befinden. **GMSC:** Gateway Mobile-services switching Centers (GMSC) übernehmen eine besondere Rolle, da sie Verbindung zu Telefonnetzen anderer Anbieter herstellen.**HLR:** Beim Home Location Register (HLR) handelt es sich um eine zentrale Datenbank, die Benutzerdaten hinterlegt, um z.B. Kosten für Gespräche abzurechnen.**AuC und EIR:** Zur Authentifizierung der Nutzer ist das Authentication Center (AuC) notwendig. Mit Hilfe des Equipment Identity Register (EIR) werden außerdem alle, für den Mobilfunkanbieter registriere Geräte erfasst (ermöglicht z.B. Blacklisting von Geräten). **PCU und SGSN:** Packet Control Unit (PCU) Zusatzmodul trennt paketorientierte (= Internet) von leitungsgebundenen (= Telefonie) Daten und leitet sie an den Serving GPRS Support Node (SGSN) weiter (GRPS = Datennetzvariante, ähnlich dem UMTS), welche mit Gateway GRPS Support Nodes (ähnlich dem MSC) verbunden sind, die Verbindung ins Internet besitzen. Das gesamte wird als Netzwork Switching Subsystem (NSS) bezeichnet und ist das Gegenstück zum Base Station Subsystem (BSS).



3-Wege-Handschlag: Mehrstufiges Verfahren (= Anfrage, Bestätigung, Gegenbestätigung) zur wechselseitigen Authentifizierung und Verbindungsaufbau zwischen zwei Instanzen. Verbindung gilt als aufgebaut, wenn sich Client und Server gegenseitig bestätigt haben. Die Authentifizierung der einzelnen Transaktionen erfolgt durch eine zufällig generierte Sequenznummer (zufällig = verhindern, dass Angreifer Datenübertragung manipulieren), welche mit Sendezeitpunkt verbunden wird. Nach Ablauf einer vorab definierten Wartezeit (Retransmission Timeout) gilt Segment als verloren und wird erneut gesendet. Wird bei Transmission Control Protocol (TCP) verwendet. **Blinde Signaturen:** Eine Art digitale Unterschrift, die bestätigt, dass ein Dokument o.ä. von einer bestimmten Person zu einem bestimmten Zeitpunkt vorgelegt wurde (= Dokument kann der Person somit eindeutig zugeordnet werden). **Blinde Signaturen + RSA:** Asymmetrisches kryptographisches Verfahren, welches zur Verschlüsselung und Erstellung digitaler Signaturen verwendet wird. Besitzt ein Schlüsselpaar, bestehend aus einem öffentlichen (= zum verschlüsseln) und privaten Schlüssel (= zum entschlüsseln). Anhand des öffentlichen Schlüssels können keine Rückschlüsse auf privaten Schlüssel gezogen werden (= asymmetrisch). **Beispiel RSA Blinde Signaturen:** Alice möchte, dass Bob Nachricht M blind unterschreibt. Bobs öffentlicher Schlüssel lautet (e, N), wobei e = eigentlicher Schlüssel und N = Modulo des Schlüssels. Bobs privater Schlüssel ist d. Damit Bob die Nachricht nicht selbst lesen kann, verknüpft Alice die Nachricht mit einem Blinding Factor k (einem Wert zwischen 1 und N), wodurch sie die verschleierte Nachricht T=M*k^e mod N generiert. Bob signiert T anschließend mit seinem privaten Schlüssel, d.h. er potenziert T mit d und erhält: T^d= ⟦(M*k^e)⟧ ^d mod N= M^d*k mod N. Alice kann die unterschriebene Nachricht anschließend entschlüsseln, indem sie durch k teilt: S = T^d/k =(M^d*k mod N) / k=M^d mod N. **Chord:** Suchprotokoll für P2P-Systeme, welches effiziente binäre Suche nach Inhalten mit Hilfe von verteilten Hashtabellen (= Distributed Hash Functions) ermöglicht,indem Schlüssel auf Knoten abgebildet werden. Hierzu wird ein Chord-Ring aufgebaut: Alle Netzwerkknoten werden in einer Ringstruktur angeordnet, wobei jeder Knoten Verbindungen zu Vorgänger, Nachfolger und bestimmten anderen Knoten des Netzwerks besitzt. Jedem Knoten und Schlüssel wird eine m-Bit lange ID zugeordnet (SHA-1). Ein Schlüssel k wird dem Knoten n zugewiesen, dessen ID grösser oder gleich der ID des Schlüssels k ist. Dieser Knoten wird Successor Knoten von k genannt. Wird Suchanfrage an Knoten gerichtet, prüft dieser, ob sein Nachfolgeknoten für den angefragten Schlüssel zuständig ist. Falls nicht, wird Anfrage so lange weitergeleitet, bis das Ziel erreicht ist.**Content Adressable Network (CAN):** Implementierung von verteilten Hashfunktionen (= Distributed Hash Functions) für die effiziente und zielgerichtete Suche innerhalb von strukturierten Peer-to-Peer-Netzen. CAN verwaltet einen D-dimensionalen kartesischen Raum (= Schlüsselraum), typischerweise eine Fläche (d=2) oder Würfel (d=3). Bei jedem hinzukommenden Peer wird der Schlüsselraum weiter aufgeteilt (= sukzessive Teilung). Über die Zeit entsteht somit eine komplexe Struktur mit vielen kleinen Regionen – jede dieser Regionen, inklusive der darin Daten, wird von mindestens einem Peer verwaltet. Der Schlüsselraum speichert Schlüssel-Wert Paare mit Hilfe einer gleichverteilten, deterministischen Hash-Funktion. Hierzu wird der Schlüssel einem Punkt P im Koordinatenraum zugeordnet. Der Peer, in dessen Region Punkt P liegt, speichert das Schlüssel-Wert-Paar. Um den, zu einem Schlüsselpaar gehörenden Wert zu ermitteln, kann jeder Knoten nun dieselbe Hash-Funktion auf den Schlüssel anwenden, um Punkt P als Speicherort und somit Zugriff auf den Inhalt zu erhalten. Um ein effizientes Routing zu ermöglichen, merken sich alle Peers die IP-Adressen und die Koordinationsfelder, die ihnen und ihren Nachbarn per Hashfunktion zugeordnet sind.**CSMA/CD:** Carrier Sense Multiple Access/Collision Detection. Siehe Sicherungsschicht, Schicht 2 OSI-Schichtenmodell. Bei drahtgebunden oder drahtlosen Übertragungen wird vorab überprüft, ob bereits gesendet wird, um Kollisionen zu verhindern. Wird Kollision festgestellt (= Collision Detection), wird JAM-Signal versendet, damit alle anderen Stationen Sendevorgänge abbrechen. Verfahren wird überwiegend in drahtgebundenen Netzwerken verwendet, da erkannte Kollision in drahtlosen Netzwerken schwierig zu realisieren ist, weil Empfänger während des Sendens abgeschaltet ist. Die Wartezeit bis zum erneuten Senden steigt schrittweise exponentiell, falls es vermehrt zu Kollisionen kommt.**Distributed Hash Functions :** Datenstruktur, die z.B. Speicherort einer Datei in einem P2P-System speichert. Daten werden gleichmäßig über vorhandenen Speicherknoten verteilt. Jeder Speicherknoten entspricht dabei einem Eintrag in der Hashtabelle. • **Direct Storage:** Daten werden innerhalb der DHT abgelegt.• **Indirect Storage:** Verweis auf die Daten wird innerhalb der DHT abgelegt. **Eigenschaften:** • Fehlertoleranz: Ausfall von Knoten kann kompensiert werden.• Lastenverteilung: Schlüssel werden gleichmäßig auf alle Knoten verteilt. • Robustheit: Funktionsfähig auch bei Störeinflüssen.• Selbstorganisation: Keine manuelle Konfiguration notwendig.• Skalierbarkeit: Kann große Anzahl von Knoten managen. **Duale Signaturen:** Sollten Verifizierbarkeit (= alle Personen sollen Echtheit prüfen können) und Nachrichtenabhängigkeit (= Unterschrift bezieht sich auf bestimmte Nachricht und ist von dieser funktional abhängig) besitzen, um Authentizität und Integrität von Nachrichten sicherzustellen, wie sie beispielsweise für Secure Electronic Transactions (SET) benötigt werden. **Use Case:** Geldtransfer mittels SET im Onlinehandel. Abbuchung vom Konto darf nur durch Käuferkonto erfolgen, der Empfänger darf Erhalt eines Geldbetrags nicht abstreiten können. **Konstruktion duale Signatur :** Aufsplitten einer Nachricht in zwei Teile. Beide Nachrichtenteile werden mit digitaler Signatur verknüpft und mit Hashfunktion verschlüsselt. Beide Hashfunktionen werden anschließend zusammengefasst und erneut per Hashfunktion verschlüsselt und mit dem privaten Schlüssel des Senders verknüpft. Der Empfänger prüft im Anschluss mit Hilfe des öffentlichen Schlüssels die Echtheit, ohne den Inhalt beider Nachrichten zu kennen (z.B. Trennung von Bestell- und Zahlungsdaten).**Freenet:** P2P-System zur Publikation, Replikation und Suche nach Dokumenten, wobei Quelle und Ziel des Datentransfers geheim sind und Verschlüsselung dafür sorgt, dass Knoten nicht bestimmt werden können. Auf Peer gespeicherte Inhalte sind ebenfalls verschlüsselt (= Knoten weiß nicht, was er speichert). Der Benutzer stellt keine Dateien zur Verfügung, sondern reserviert einen bestimmten Anteil an Festplattenspeicher, den Freenet selbstständig mit Daten aus dem Internet belegt. Suche erfolgt durch schrittweises weiterreichen und durchsuchen des Netzwerks, wobei Sender und Empfänger die Anfrage nicht explizit mitgeteilt wird. **Besonderheiten:** • Vollständig dezentral (hohe Fehlertoleranz, Robustheit und Skalierbarkeit).• Automatische Inhaltsreplikation. • Adaptives Routing (nutzt Bandbreite gut aus).• Unterstützt Anonymität.**Gnutella:** Dezentrales P2P-System mit autonomen, selbstorganisierenden Peers, inkl. Datei-Suchfunktion per Flooding (= Broadcasting). **Flooding:** Suchanfragen werden sukzessiv immer wieder an alle Nachbarn gesendet, welche es wiederum an ihre Nachbarn weiterleiten (Ping / Pong Mechanismus). Anzahl der Hops ist durch Time to live limitiert ist (meistens auf 7 = Small Worlds). Alle Peers durchsuchen jeweils ihre lokale Datenbasis bei jedem Request. Der Download erfolgt im Anschluss direkt von der Quelle, wobei der Filetransfer mit HTTP realisiert wird, wodurch Identität des Downloaders und Anbieters offengelegt werden. Mit Flooding entsteht hohe Ressourcenauslastung (= Overhead).**Gnutella2 (KazaA):** KazaA ist Filesharingprogramm, basierend auf Peer-to-Peer-Systemen, welches ähnliche Usability wie Google bietet: Schlüsselwortbasierte Suche, parallele Downloads, Warteschlangenmanagement etc. Gnutella2 ist ein offener Standard (= Protkoll) von KazaA und verwendet Hub- und Blattknoten. Ein Hub beinhaltet Informationen über Blattknoten, inkl. deren Informationsangebot. Pro Hub existieren ca. 5-30 Verbindungen zu anderen Hubs und 300-500 Verbindungen zu Blattknoten. Suchanfragen werden iterativ an andere Hubs gesendet.**Multiplexing:** Siehe Sicherungsschicht, Schicht 2 OSI-Schichtenmodell. Bündelung mehrerer Datenströme und Übertragung über einen gemeinsamen physikalischen Kanal, um optimale Ausnutzung von Leitungen/Frequenzen zu erreichen. **Multiplexverfahrest** Frequency Division Multiplex (FDM) (Frequenzmultiplexverfahren): Mehrere Signale in unterschiedlichen Frequenzbereichen getrennt übertragen. • Space Division Multiplex (SDM) (Raummultiplexverfahren): Übertragungskanäle zur parallelen, aber exklusiven Nutzung durch mehrere Sender und Empfänger bündeln. • Code Division Multiplex (CDM) (Codemultiplexverfahren): Verschiedene Signalfolgen über eine Leitung/Funkfrequenz übertragen und anhand ihrer unterschiedlichen Codierung zuordnen; Empfänger erkannt passend kodiertes Signal und wertet aus.• Time Division Multiplex (TDM) (Zeitmultiplexverfahren): Mehrere Signale werden zeitversetzt übertragen. Sie sind zeitlich ineinander verschachtelt. Die Zeitfenster können synchronisiert und gleich lang oder asynchron und bedarfsabhängig sein.**Synchrones/Asynchrones Multiplexing:** •Synchrones Multiplexing: Abschnitte werden festen Zeitabschnitten zugeordnet. Sendet Station nicht, bleibt Zeitabschnitt ungenutzt. • Asynchrones Multiplexing: Kanalkapazität des physikalischen Kanals wird bedarfsorientiert durch eine zentrale Komponente oder dezentral durch Kooperation der Stationen zugeteilt (= höherer Verwaltungsaufwand).**P2P-Systeme:** Bestehen aus Menge von autarken Komponenten, welche eine gemeinsame Software betreiben, inklusive kompatiblem Interface. Jeder Peer kennt mindestens einen weiteren Peer (= Nachbarschaft). Die Komponenten erfüllen sowohl Client als auch Serverfunktionalitäten (servent). **Eigenschaften:** • Flexibilität: Weitere Peers können hinzugefügt bzw. entfernt werden. • Robustheit: Verschieden Lösungswege für eine Aufgabe. •Skalierbarkeit: Funktioniert für kleine/große Anzahl von Peers gleich gut. **Besonderheiten:** •Keine zentrale Instanz: Reine P2P-Systeme können nicht zentral überwacht oder gesteuert werden.• Struktur und Größe des Netzes ist zumeist nicht bekannt.• Jeder Peer kennt nur Teil des Gesamtsystems.• Peers nehmen Rolle von Client und Server an.**Beispiele:** • Napster (mit zentralen Inhaltsverzeichnis für Dateisuche);•Gnutella und Freenet (mit dezentraler Suchstruktur) **Ping Pong:** Wird für Flooding (Gnutella) verwendet. Der Rechner, der einen Ping erhält, sollte mit einem Pong seiner Adresse antworten und den Ping an seine Nachbarn weiterleiten (= dient der Sicherung des Netzzusammenhangs)**Pure Aloha:** Time Division Multiple Access (TDMA) Multiplexverfahren bzw. Zugriffsprotkoll für Drahtlosnetzwerke. Jede Station kann jederzeit senden, wobei erfolgreiche Übertragungen vom Empfänger quittiert werden. Bei Überlappungen müssen Frames neu gesendet werden und werden nicht quittiert.Man unterscheidet zwischen zeitunabhängigem (= pure) und zeitabhängigem Verfahren (= slotted). **Slotted Aloha:** Teilt Zeit in Zeitschlitze ein. Jede Station darf nur zu Beginn eines Zeitschlitzes senden. Kapazitäten werden auf diese weise besser genutzt und Kollisionen reduziert.**Ubiquitous Computing:** Allgegenwärtige rechnergestützte Informationsverarbeitung = Verknüpfung aller Rechner, die Nutzer Zugriff zu jedem benötigten Service oder Ressourcen des Netztes geben. **Pervasive Computing:** Alldurchdringende Vernetzung des Alltags durch Einsatz intelligenter Geräte (= IoT). **UDP:** Unified Datagram Protocol. Siehe Transportschicht, Schicht 4 OSI-Schichtenmodell. Stellt Segmentierung von Datenströmen und Adressierung von Anwendungen bereit. Die Pakete können verloren gehen, der Reihenfolgenerhalt ist nicht garantiert (wird z.B. für Videostreaming verwendet, wo Paketverluste toleriert werden). **TCP:** Transmission Control Protocol. Verbindungsorientiertes Protokoll, d.h. es wird mit 3-Wege-Handschlag eine Verbindung zwischen Rechner A und B aufgebaut. TCP stellt Segmentierung von Datenströmen und Adressierung von Anwendungen bereit, garantiert außerdem die korrekte Zustellung der Pakete (durch 3-Wege-Handshake), inklusive Reihenfolgenerhalt und Mechanismen zur Flusskontrolle und Überlaststeuerung (Slow Start und Congestion Avoidance). **Unterschiede UDP und TCP:** UDP ist schnell, aber unzuverlässig. TCP ist langsamer (da hoher Organisationsaufwand), jedoch zuverlässiger.

Ablauf Nachrichtenübermittlung Nachrichtenkodierung.

Bellmann Ford: Dezentrales Verfahren zum Aufbau von Routingtabellen. Jeder Router teilt Veränderung seiner Routingtabelle als Distanzvektor an seinen direkten Nachbarn mit.



Dijkstra-Algorithmus: Routingprotokoll, mit Ziel für einen bestimmten Knoten den kürzesten Pfad zu allen anderen Knoten des Graphen zu finden. Hierzu wird bei der Initiierung eine Liste aller bereits bearbeitet Knoten angelegt, die zunächst leer ist. In jedem Iterationsschritt wird ein weiterer Knoten gewählt und der Liste hinzugefügt. Algorithmus endet, wenn keine weiteren Knoten betrachtet werden.