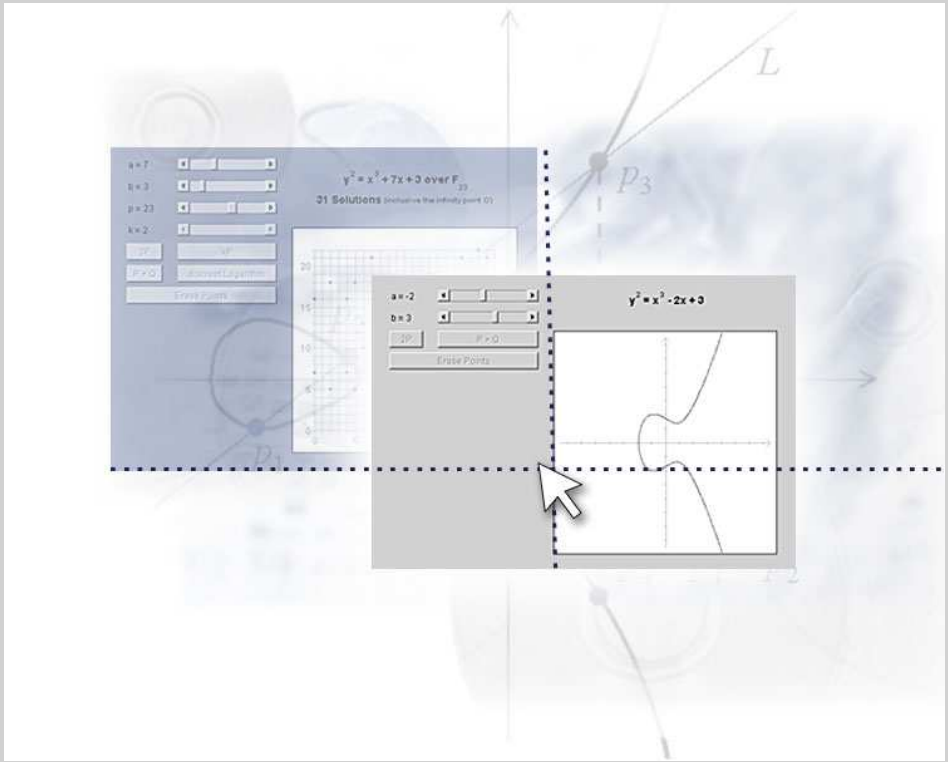
FernUniversität in Hagen



Multimediale Lernmodule

Multimediale Lernmodule

Lehrgebiet Kommunikationssysteme
Prof. Dr.-Ing. Firoz Kaderali

in Zusammenarbeit mit
MMK GmbH, Hagen

Gliederung

Kurseinheit 1

Gliederung

Kurseinheit 1

1 Sicherheit in GSM-Netzen

In dem Kurs **Sicherheit in GSM-Netzen** werden folgende multimedialen Lernmodule eingesetzt:

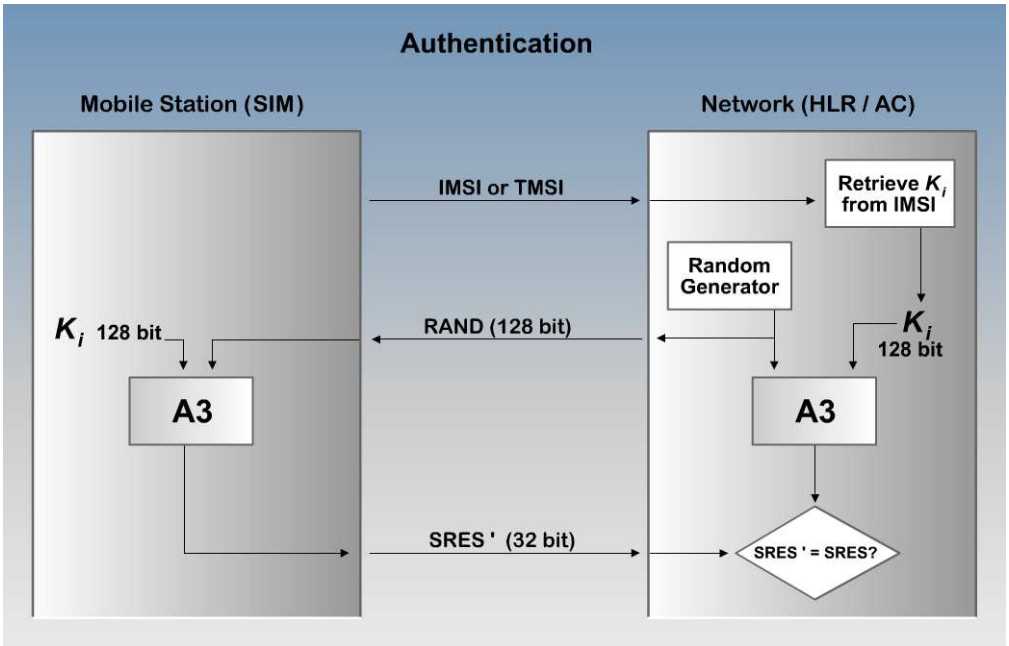
- Abschnitt 1.1 Animation Authentifizierung - Challenge and Response
- Abschnitt 1.2 Animation Vertraulichkeit
- Abschnitt 1.3 Animation Pseudonym
- Abschnitt 1.4 Animation Authentication Center
- Abschnitt 1.5 Animation Verteilte Datenbanken

1.1 Authentifizierung - Challenge and Response

Authentication of the Subscriber

Authentication is the corroboration that an entity is the one claimed or, in this context, the verification of the identity of the SIM card. The user authenticates itself to the SIM card with its PIN, and the SIM card authenticates to the network with cryptographic strong authentication algorithm. Subscriber authentication is of major interest to each operator (protect the network against unauthorized use, correct billing, preventing masquerading attacks). The authentication algorithm in GSM is denoted as A3 and is implemented in the Authentication Center (AC) of the home network, i. e. the Home Public Lands Mobile Network (HPLMN), and in the SIM. The method employed between HLR/AC and a SIM is a Chellenge-Response mechanism using cryptographic secure random numbers. Thereby, a 128-bit authentication key Ki is used, which is kept in the SIM card (subscriber side) and in the AC (network side). The animation shows the basic procedure for the authentication of the SIM by the network. After establishing the identity of the SIM, the VLR sends an authentication request to the network. This request contains the IMSI (or TMSI) which is needed to retrive the secret on the network side (which is an individual subscriber authentication key Ki). The network then generates a non-predictable 128-bit random number RAND which is sent to the MS as a chellenge (via the VLR). This chellenge changes each time the protocol is run. To compute the Signed RESponse SRES to the chellenge RAND, the SIM uses the algorithm A3 with RAND and the key Ki (stored in the SIM) as input data. The algorithm A3 ia actually an one-way function with a 32-bit output SRES. SRES is then transmitted to the VLR (which may be in a foreign network). There it is compared with the value SRES computed by the home network which is received by the AC. The AC has used the same RAND and the key Ki which is associated with the identity claimed by the subscriber. The MS is granted access to the network by the VLR only if the value of SRES received from the MS equals the value received for SRES from the HLR/AC. Only in this case it can be assumed that the SIM is in possession of the right subscriber key Ki and that its identity is the one claimed.

The authentication process takes less then 500 ms. When a user has moved to a new VLR, the new VLR will normally establish the subscriber's identity by requesting the IMSI from the old VLR. Note that the individual subscriber keys are not transmitted over the network - they are only used in the challenge-response protocol for authentication and key agreement.



Animation 1.1-1: Authentifizierung

IMSI:

International Mobile Subscribing Identity

TMSI:

Temporary Mobile Subscribing Identity

Ki:

geheimer Schlüssel des Mobilfunkteilnehmers (128 Bit)

RAND:

Zufallsbitfolge / Challenge (128 Bit)

SRES / SRES':

Response (32 Bit)

SRES = A3(Ki, RAND)

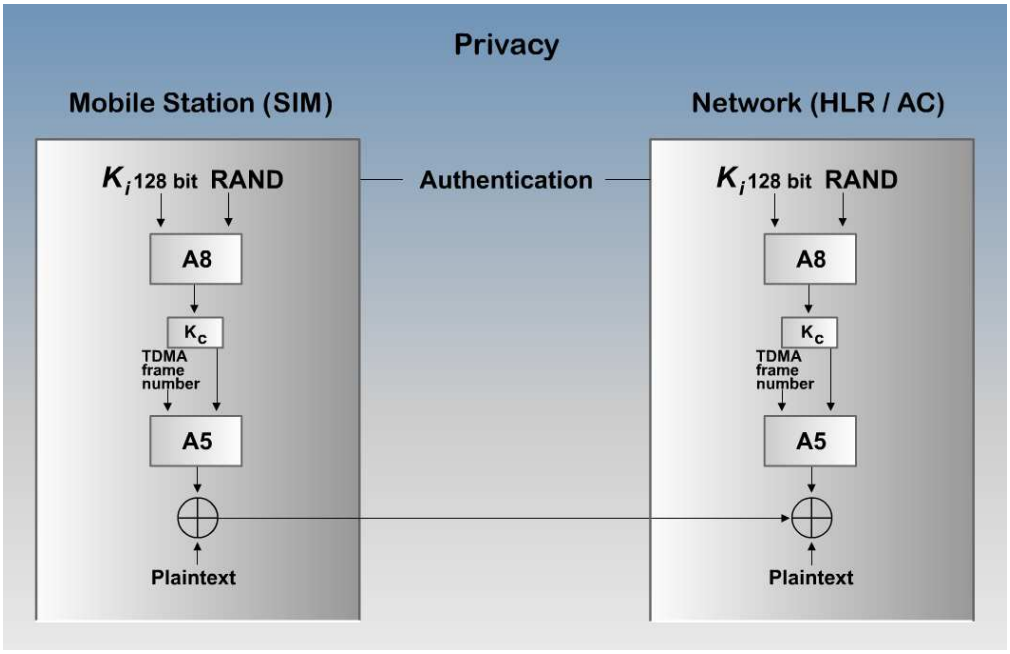
Der Algorithmus **A3** sollte eine gute Einwegfunktion sein. Er ist nicht europaweit standardisiert.

1.2 Vertraulichkeit - Stromchiffre mit wechselnden Sitzungsschlüsseln

Enciphering

The purpose of this security service is to ensure the privacy of the user information carried in both traffic and signalling channels and of user-related signalling elements on the radio path. The activation of this service is controlled by the network. It is started by the base station by sending a start cipher command to the MS.

A standard cipher algorithm called A5 is contained as dedicated hardware in mobile equipment and base stations. A5 is a stream cipher14, and because of its high encryption rate is suitable for real time applications as telephony. The plain text is organised into blocks of 114 bits as this is the amount of data which is transmitted during a time slot. The key stream, which is Key generation and enciphering a sequence of bits to be XORed (modulo 2 addition) with the data block, is produced by the algorithm A5 as an output block of 114 bits. The generation of the key stream from the A5 algorithm is controlled by the key Kc (input parameter). This key is derived in the SIM as part of the authentication process using the network operator specific key generation algorithm A8 and the same RAND and Ki as in the authentication algorithm A3. The process of cipher key generation and enciphering is shown in the animation.



Animation 1.2-1: Vertraulichkeit

Ki:

geheimer Schlüssel des Mobilfunkteilnehmers (128 Bit)

RAND:

Zufallsbitfolge (128 Bit)

Kc:

Sitzungsschlüssel (64 Bit)

Kc = A8(Ki, RAND)

TDMA:

Rahmennummern der zu verschlüsselnden Daten

$\oplus$**:**

Modulo-2-Addition des Ausgabebitstroms **A5(TDMA, Kc)** und des Klartextbitstroms

Der Algorithmus **A8** ist netzbetreiberabhängig und nicht europaweit standardisiert.

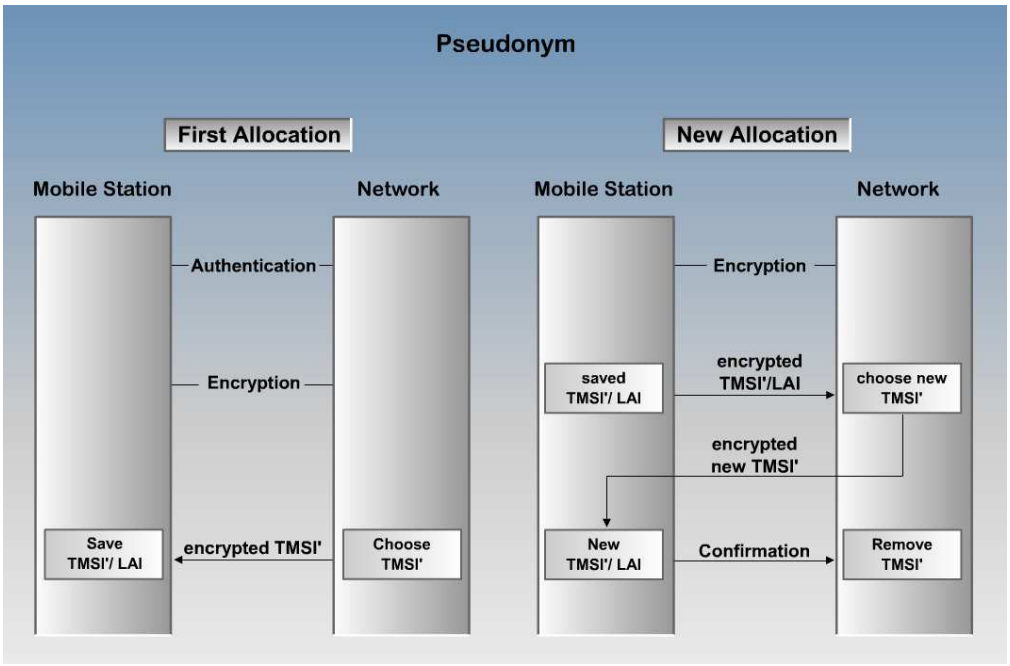
Der Algorithmus **A5** ist ein Pseudozufallszahlengenarator, der europaweit standardisiert und nur den Herstellern zugänglich ist.

1.3 Pseudonym

Um der Bedrohung der Bewegungsprofilerstellung begegnen zu können, bedient man sich in GSM der Technik der Pseudonyme.

Die Grundidee ist, dass in der Regel selbst beim Authentifizierungsvorgang keine für einen Angreifer verwertbaren Kennungen über die Funkschnittstelle gehen sollen. Das Challenge and Response Verfahren muss im Prinzip nur beim allerersten Einbuchen ins Netz unter Bekanntgabe der Teilnehmerkennung IMSI erfolgen. Wenn diese erste Authentifizierung stattgefunden hat und zudem Vertraulichkeit hergestellt wurde, kann nun eine geheime, nur dem Netz und dem Teilnehmer bekannte temporäre Identitätsnummer TMSI verabredet werden, mit der sich der Teilnehmer für kommende Gespräche anmeldet um die Authentifizierung und den Schlüsselaustausch vorzunehmen.

Die Kenntnis der IMSI eines Teilnehmers genügt also einem Angreifer nicht, wenn er die Bewegungen eines bestimmten Teilnehmers rekonstruieren will. Er muss in der Lage sein, die verschlüsselt übertragenen TMSI zu entschlüsseln, um einen neuerlichen Einbuchvorgang des Teilnehmers als solchen wahrzunehmen.



Animation 1.3-1: Pseudonym

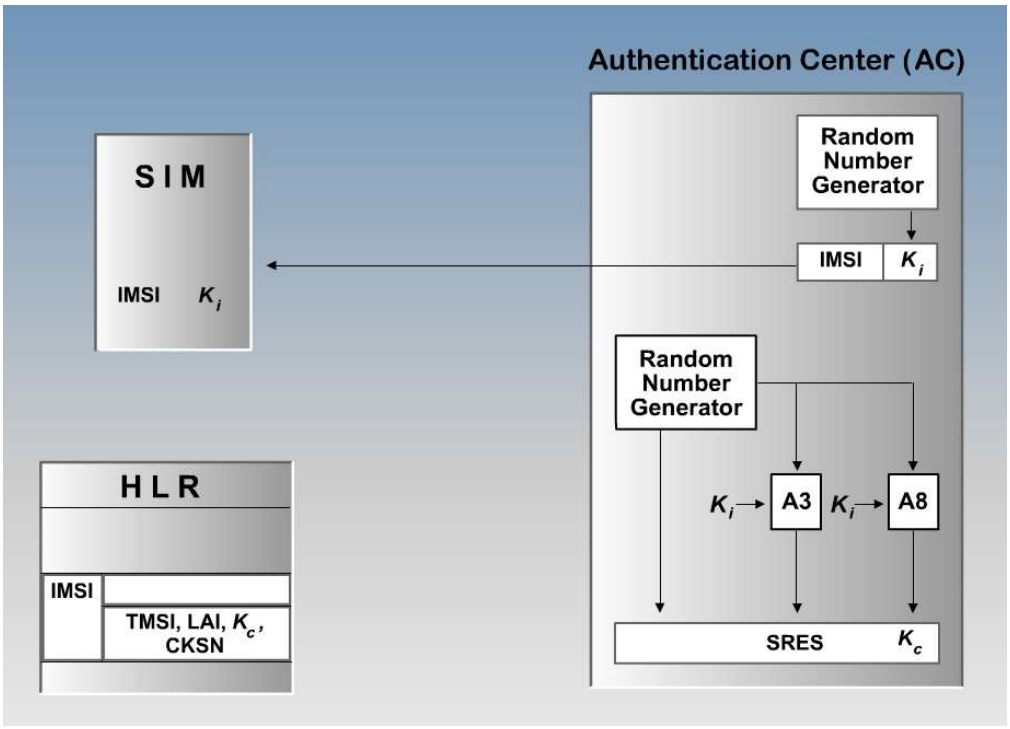
1.4 AC - Authentication Center

The central point of the security services in GSM networks are the authentication centers (AC), which are assigned to each mobile switchung center (MSC). They generate and store the IMSI and the authentication key Ki for each subscriber, which are also stored in the subscriber's SIM. Using the algorithms A3 and A8, a triples of random bit streams RAND, signed responses SRES and session keys Kc are generated in the AC in advance, and than they are saved in the associated HLR, in conjunction with the appropriate identifier.

The specific security and administrative requirements for an authentication center are not standardized but left to each network operator. The GSM 3.20 standard only states that the individual subscriber authentication keys Ki are stored in an AC and that an AC also contains the authentication algorithm A3 and the cipher key generating algorithm A8. A malfunction or a temporary loss of the information contained in an AC would have severe consequences for the security as it affects the generation of the authentication triplets. Since other information about the subscriptions, including the possibly black lists of barred subscriptions, is contained in HLR, it is logical to "integrate" the AC into HLR. In networks with more than one HLR, the backup and overload facilities could be distributed over several HLR /ACs. Key management is a major issue when designing an AC. The method used for generating and storing potentially several million individual subscriber authentication keys and the handling of the authentication request are of importance for both the secure and the smooth running of the network. There are two standard methods to generate keys. They may be generated by using a random number generator or by deriving them from user related data with the help of an algorithm under the control of a

master key MK. Both methods have their advantages and disadvantages. The main advantage of deriving a key from non-secret (subscribtion) data under a master key is that such derivable keys need not be stored and that the back-up of the subscriber keys is reduced to the back-up of the master key. No databanks containing secret information are thus required in the AC.

When an authentication request comes from the VLR, the AC would just load the relevant data, say the IMSI, into the algorithm and derive the individual subscriber authentication key Ki from this data using the top secret master key MK. This method has a few undesirable effects if it is not managed with extreme care from both an administrative as well as a security point of view. The main problem is of course to keep the very secret key MK secret. Anybody comming into possesion of this key could (if he knows the method of deriving Ki and the algorithms A3 and A8) compromise every SIM card issued under MK. The method can also lead to the production of ”identical” SIMs. If the same IMSI has been used by mistake to generate the keys for two SIMs, these SIMs will be identical from a security point of view, i.e. they contain the same IMSI and Ki. One can avoid the risk of producing identical SIMs by combining subscription data with random data. Using a random number generator to produce the subscriber authentication keys insures that all strings consisting of 128 its are equally likely. This advantage can not be achieved by an algorithm using IMSIs as an input. As there is no ”link” between the subscription and the authentication key, all keys have to be stored in a database of the AC and have to be backed-up at a physically different location. To protect the keys against authorized reading in the AC they have to be stored in an encrypted form. The key (or keys) using for decrypting the subscriber authentication keys is clearly very sensitive.



Animation 1.4-1: AC - Authentication Center

IMSI:

internationale Kennung des Teilnehmers

Ki:

geheimer Schlüssel des Teilnehmers (128 Bit)

RAND:

Zufallsbitfolge (128 Bit)

SRES:

Antwortsequenz (32 Bit)

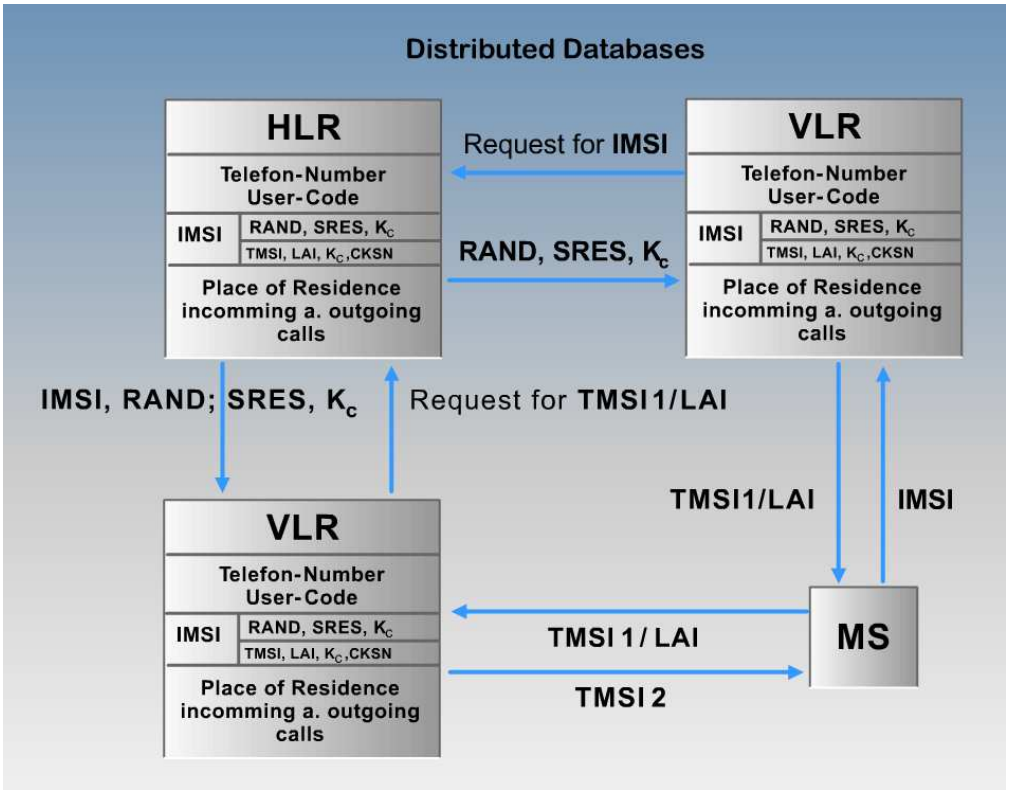
Kc:

Sitzungsschlüssel (64 Bit)

1.5 Verteilte Datenbanken

In the typical signalling protocol between a user and the network presented above, we did so as if all information required for the authentication and encryption processes reside in one place in the network. But in reality, the data are distributed physically in several databases. Messages, information and parameters between the distributed databases are transferred with strictly defined protocol sequences.

To illustrate the principle of distributed databases, we describe here the process when a user want to access network which is not his home network. A user can access the network from anywhere with its IMSI. The VLR of the visited radio network part requests the necessary data from the home register (HLR) and receives sets of random bit streams RAND, associated responses SRES and session keys Kc, which it stores for the time of the visit. The VLR assignes a temporary identity TMSI1 to the user, which is transmitted to him encrypted. On the animation the message sequence is presented very simplified. This also regards the message sequences between the databases (HLR-VLR and VLR-VLR), which belongs to the SS7. When the user moves to another network location area, also belonging to the ”foreign” network, he can authenticate itself with his pseudonym TMSI1 and the LAI of the last network location area. The responsible VLR of the new network location area requests the requred data (RAND, SRES, Kc) from the issuer of the pseudonym TMSI1, the VLR1. The VLR2 generates a new pseudonym for the user, TMSI2, and sends it encrypted with Kc to him. Note that if user is outside the home network, the visited network requests sets of (RAND, SRES, Kc) from the home network, and this allows the visited network to communicate with the handset without gaining access to the algorithms A3 and A8. As the SIMs and their contents (including A3 and A8) are controlled by the respective network operators, this structure leaves room for national and business policy enforcement. The algorithm A5, on the other hand, has to be supported by all networks and end devices in order to interoperate properly.



Animation 1.5-1: Verteilte Datenbanken

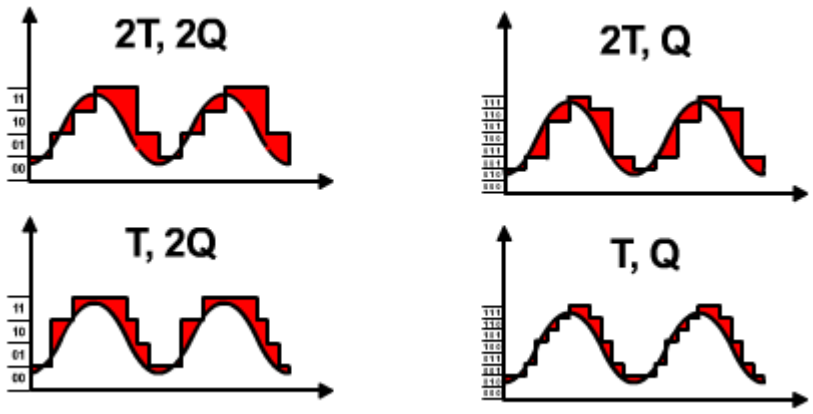
2 Internettechniken

In dem Kurs **Internettechniken** werden folgende multimedialen Lernmodule eingesetzt:

2.1 Pulse Code Modulation

A similar task in the context of digital communication is the digitization of speech. The most frequently employed principle is pulse code modulation (PCM). In PCM, speech is sampled 8000 times per second. Each of the samples is represented by 8 bits. So, one out of 256 values can be assigned to each sample.

The quantization error in PCM depends on the length of the sampling interval and the width of the quantization interval. Animation 2.1-1 shows the differences in the resulting quantization error.



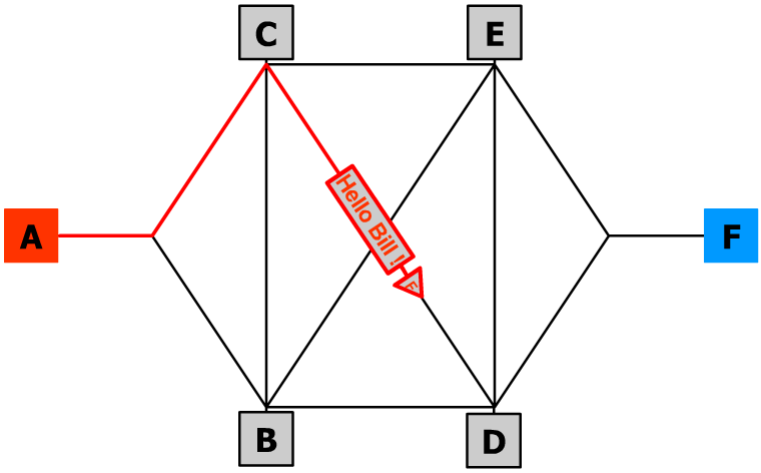
Animation 2.1-1: Pulse Code Modulation

2.2 Message Switching and Packet Switching

In message switching no direct path of transmission exists between the participants. The message is stored temporarily in intermediate nodes. In case of message switching from participant A to participant B, the message which has to be transmitted is provided with address and control information, temporarily stored in the switch, and possibly after passing several switches transferred to the receiver as one unit.

In packet switching mode, the message which is to be transmitted from participant A to B is divided into packets. Each packet is provided with destination and control information and is seperately transmitted via the network.

Animation 2.2-1 exemplifies the two transmission modes **message switching** and **packet switching**.



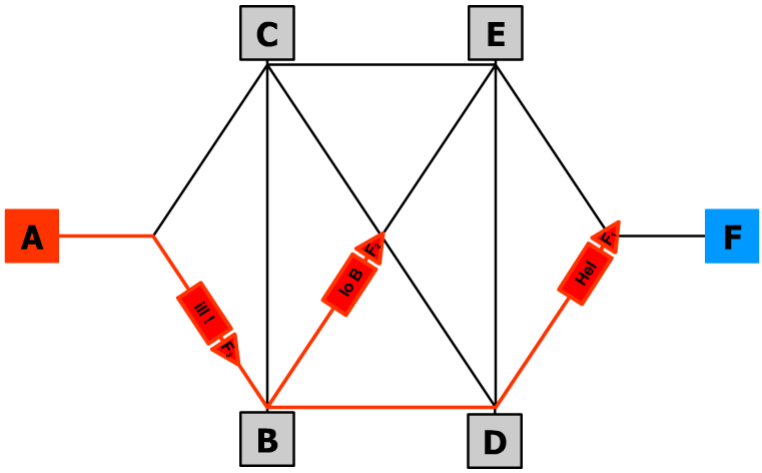
Animation 2.2-1: Message Switching and Packet Switching

2.3 Packet Switching with Datagrams

In **packet switching** mode, the message which is to be transmitted from participant A to B is divided into packets. Each packet is provided with destination and control information and is seperately transmitted via the network.

Packet switching can be realized in two different operational modes: connectionless and connection-oriented.

In the connectionless or **datagram** mode, each packet of the communication process is provided with destination and control information as well as a sequence number. The packets are sent to the destination independent from each other. Thus, packets can take different paths across the network and possibly overtake each other. By using a sequence number for each of the packets, the receiver can reorder the packets and reassemble them to the original message. The datagram packet switching mode is also used in the Internet.



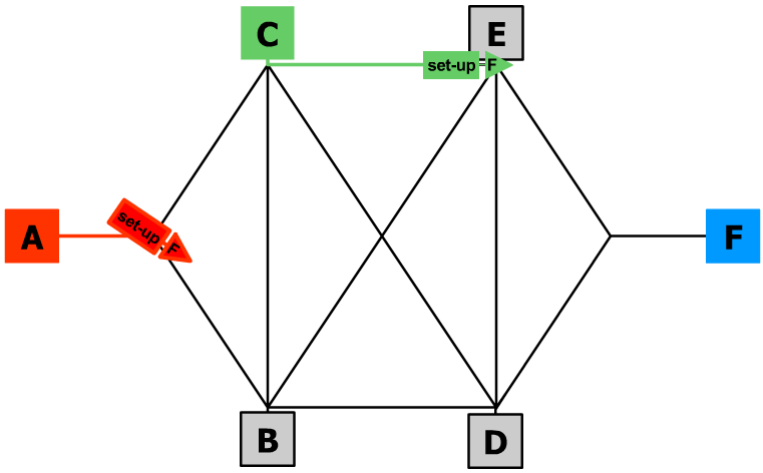
Animation 2.3-1: Packet Switching with Datagrams

2.4 Packet Switching in a Virtual Circuit

In **packet switching** mode, the message which is to be transmitted from participant A to B is divided into packets. Each packet is provided with destination and control information and is seperately transmitted via the network.

Packet switching can be realized in two different operational modes: connectionless and connection-oriented.

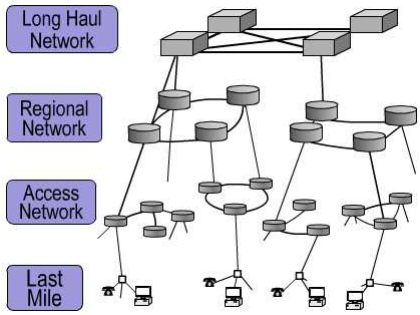
Before starting data transmission in the connection-oriented transmission mode, the path from participant A to B across the network is determined. Thus a **virtual circuit** is set up. Similar to circuit switching we can distinguish three different phases of a virtual circuit: the set-up, the connection phase and the termination. Each transmitted packet takes the same path via the network. In this way, the packets arrive at their destination in correct order and no additional sequence number is required. Packets which belong to a virtual circuit only need a reduced address information to reach their destination. Consequently, the packet overhead is reduced. During the connection phase of the virtual circuit, the links contained in its transmission path are not exclusively available for it alone but may also be used by other virtual circuits in the network as well.



Animation 2.4-1: Packet Switching in a Virtual Circuit

2.5 Hierarchical Communication Network

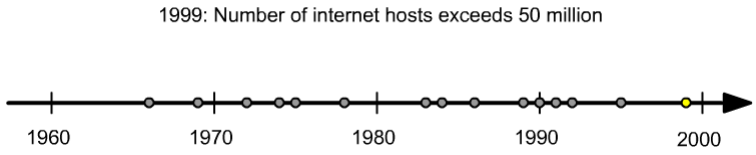
Large communication networks like national telephone and data networks can be divided into different layers as shown in Animation 2.5-1. Such communication networks are able to provide telecommunication services to a large number of subscribers (customers) which are scattered in a wide area.



Animation 2.5-1: Hierarchical Communication Network

2.6 Evolution of the Internet

Animation 2.6-1shows the evolution of the Internet and the World Wide Web from 1966 to 1999.

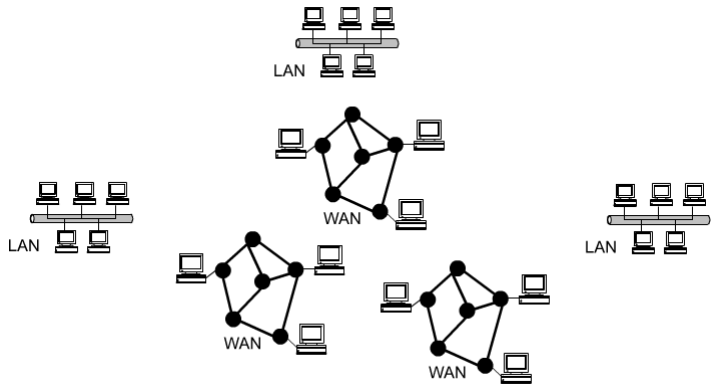


Animation 2.6-1: Evolution of the Internet

2.7 Internetwork

Historically, the Internet is a network of independent data networks. These data networks were built by a multitude of different organizations and enterprises whose networks differed in size between LANs and WANs. Besides the differences in size there also existed a diversity in networking technologies. This diversity in technologies is a result of the varying requirements posed by different organisations. For instance, a small company connects its computers with a LAN technology. A large enterprise, on the other hand, interconnects the different sites with WAN technology. Since there exists no networking technology that fits all the needs, a technology that permits the interconnection of multiple heterogeneous networks is required. The scheme that allows the interconnection of different networking technologies is called internetworking.

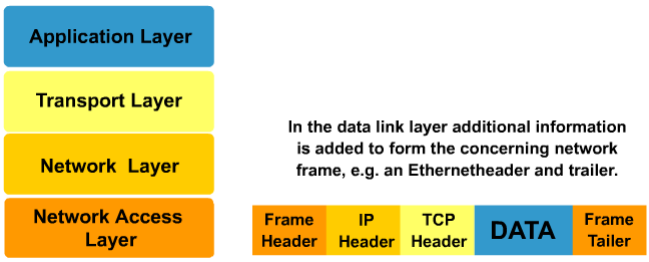
Animation 2.7-1 shows hows two distant terminals in different LANs (Local Area Networks) communicate with each other.



Animation 2.7-1: Internetwork

2.8 Packaging data for transmission

Software and hardware operating on TCP/IP networks typically consist of a wide range of functions to support communication activities. To reliably exchange data between computers many seperate procedures must be carried out. One of these procedures is Packaging data for transmission. This procedure is shown in Animation 2.8-1



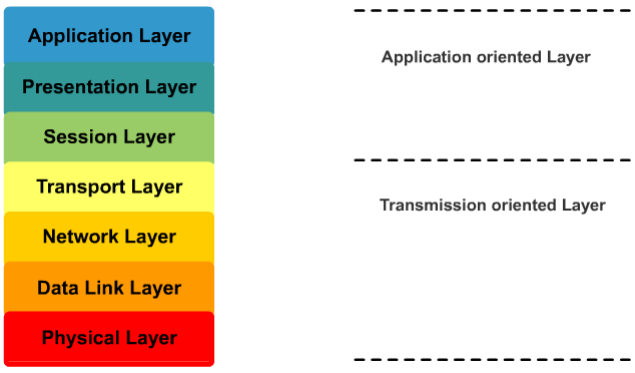
Animation 2.8-1: Packaging data for transmission

2.9 OSI Reference Model

The OSI model was an international effort to create standards for computer communication and generic application services. The OSI reference model permits the interconnection of systems of different origins which respect the standards and protocols of this model.

The OSI model is not concerned with the internal architecture of systems but with their external behaviour. Seven standardized layers correspond to two groups of functions: The transmission oriented layers and the application oriented layers.

Show Animation 2.9-1.



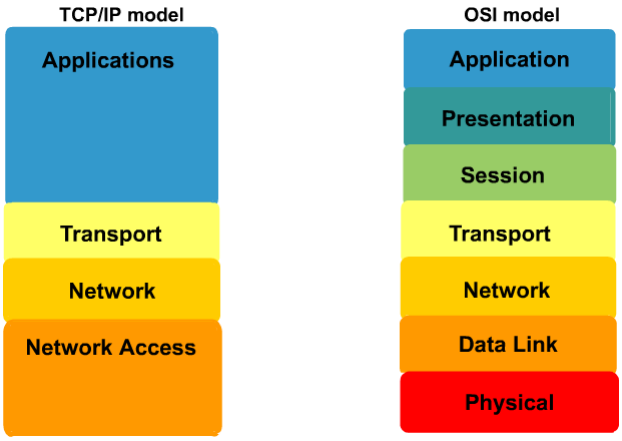
Animation 2.9-1: OSI Reference Model

2.10 TCP vs. OSI

There is no official TCP/IP model as there is in the case of OSI. But based on the protocol standards that have been developed, the communication tasks for TCP/IP can be organized into four relatively independent layers:

- Application layer
- Transport layer
- Network layer
- Network access layer

In Animation 2.6-1 the TCP/IP and the OSI layers are shown in comparison to each other.

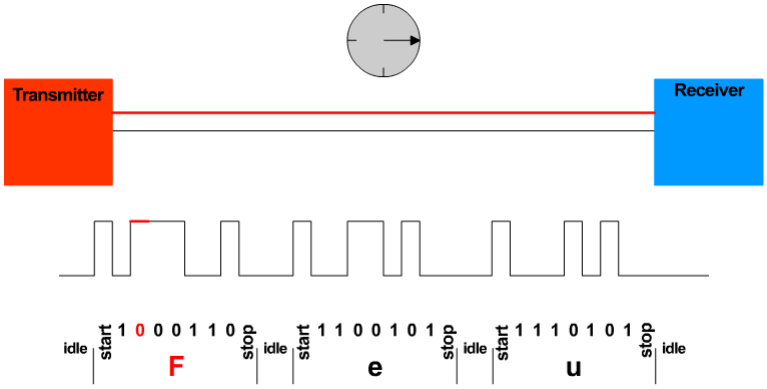


Animation 2.10-1: TCP vs. OSI

2.11 Asynchronous Transmission

A communication process is called asynchronous if the communication devices do not need to coordinate before sending data. In practice this means, that the sender can wait an arbitrary time before sending data and the receiver must be ready at any time to accept the data. Asynchronous communication is useful for devices like computer keyboards which can be operated any time by the user. If a key of a keyboard is touched data flows from the keyboard to the computer. As soon as the key is released the data flow stops.

Asynchronus Transmission is shown in Animation 2.11-1.

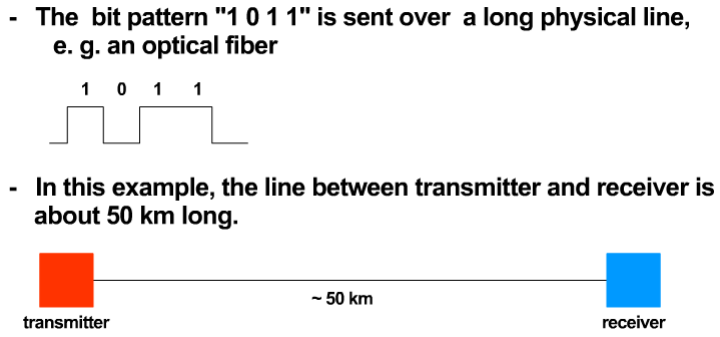


Animation 2.11-1: Asynchronous Transmission

2.12 Dispersion on long transmission lines

Dispersion is a kind of delay distortion which occurs because the spectral components of a signal travel at different velocities. As a consequence, the signal broadens and different parts of the signal start to interfere with each other. This phenomenon is called intersymbol interference (ISI).

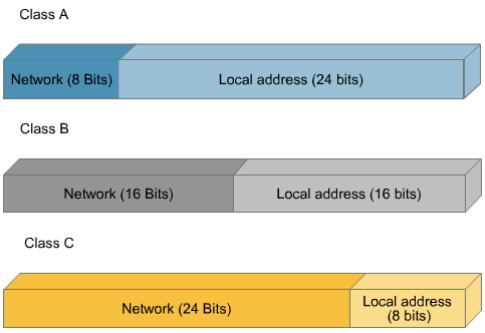
This is shown in Animation 2.12-1



Animation 2.12-1: Dispersion on long transmission lines

2.13 IP Address Classes

Five types of IP address classes have been defined, named Class A, B, C, D and E. The formats of class A, B, and C which are the traditional address classes are displayed in Animation 2.13-1.

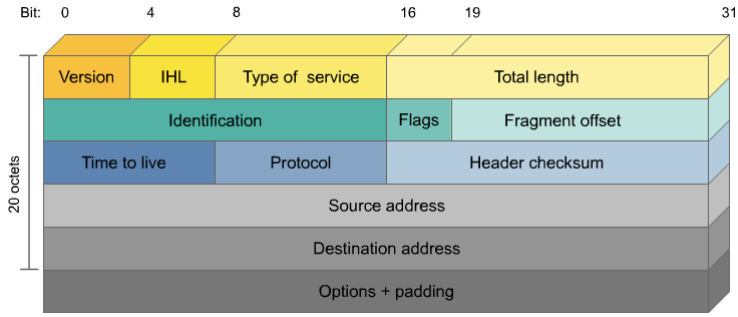


Animation 2.13-1: IP Address Classes

2.14 IP Header Files

At the network layer, IP datagrams consist of header and data. The header contains detailed and extensive information describing routing information for the datagram such as the source and destination address. IP headers have a length of at least 20 bytes. All the IP headers are organized into four-byte words since nodes and routers normally process four bytes simultaneously.

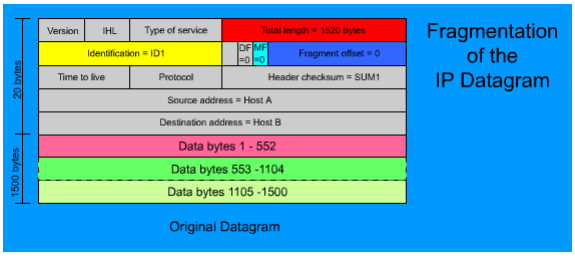
By looking at the meanings of the different IP datagram header fields (as shown in Animation 2.14-1), it becomes easier to understand how datagrams are created and routed through the network.



Animation 2.14-1: IP Header Files

2.15 IP Packet Fragmentation

Animation 2.15-1 shows the exemplary fragmentation of an IP datagram.

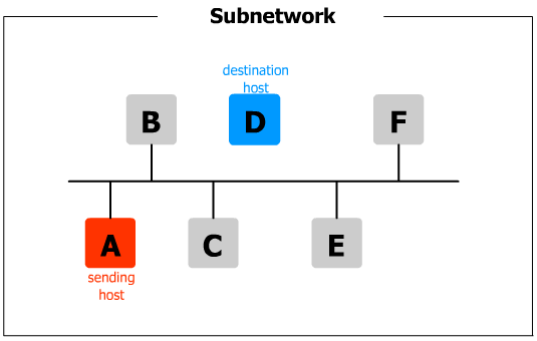


Animation 2.15-1: IP Packet Fragmentation

2.16 Direct Routing

Direct routing takes place when the source node checks the destination address and determines that it is in the same IP network, the same subnet, and the same physical network. In this case, the host uses the Address Resolution Protocol (ARP, see Section 3.4.2) to send a broadcast to the local network and map the IP address to a link layer address, e. g. an Ethernet address. The node then encapsulates the datagram into a link layer frame and directly sends it to the datagram's destination.

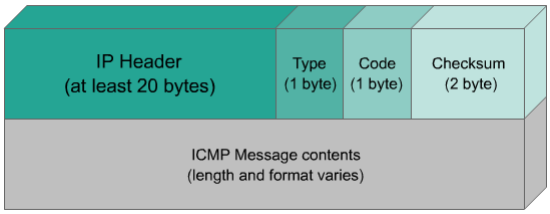
This ist shown in Animation 2.16-1.



Animation 2.16-1: Direct Routing

2.17 ICMP Message

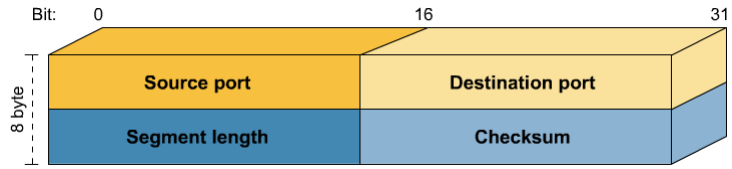
As illustrated in Animation 2.17-1 ICMP messages have a simple structure: The first field after the IP header is the type field with a length of one byte. This field indicates the function the message fulfills. The following field, the code field, has a length of one byte. It includes further information about the content of the message, e. g. a more specific description of an error. The checksum is a 2-byte number. It is applied to the ICMP message starting from its type field.



Animation 2.17-1: ICMP Message

2.18 UDP Header

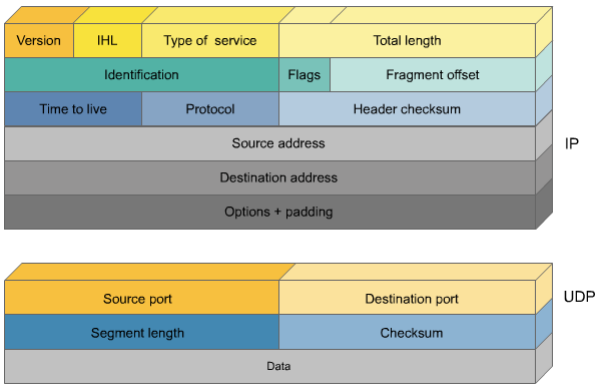
As illustrated in Animation 2.18-1 the UDP header comprises 8 bytes, consisting of four two-byte fields. The first field contains the source port number, the second the destination port number. The value of the third field represents the length of the UDP datagram. The fourth field includes the UDP checksum.



Animation 2.18-1: UDP Header

2.19 Creation of a Pseudo Header

Animation 2.19-1 shows the creation of a pseudo-header to calculate the UDP checksum.

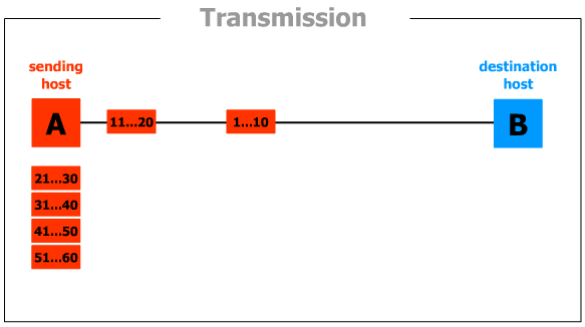


Animation 2.19-1: Creation of a Pseudo Header

2.20 TCP Timeouts

Animation 2.20-1 shows the TCP acknowledgement, timeout and retransmission.

The last TCP byte reaching the receiver had the sequence number 30. Thus, the receiver's acknowledgement number will be 31. This value identifies the number of the next byte which is to be sent by the other side. After receiving this acknowledgement the sender transmits the next bytes numbered for example 31 to 60. Assuming that the sender does not receive the next acknowledgement with the number 61 within a certain time interval it retransmits the bytes 31-60.

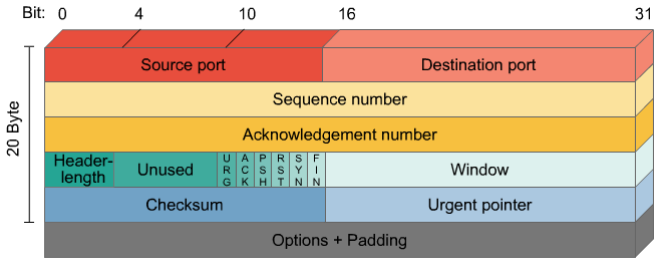


Animation 2.20-1: TCP Timeouts

2.21 TCP Header

The standard TCP header comprises 20 bytes, but it can be longer if options are used.

The TCP header structure is shown in Animation 2.21-1



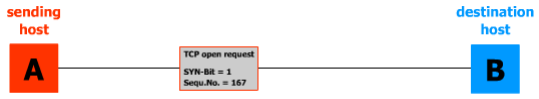
Animation 2.21-1: TCP Header

2.22 Handshake Protocol

To set up a TCP connection between two hosts, the three-way handshake has to be performed. The name of the procedure stems from the fact that three messages SYN (for synchronization), SYN, and ACK (acknowledgement) have to be exchanged to start the connection. The three-way handshake relies on the fact that in TCP connections all the segments have to be acknowledged to provide a reliable link.

Animation 2.22-1shows the steps of the three-way handshake.

When the handshake is completed, both sides can start sending data. The two processes continually acknowledge the receipt of data.

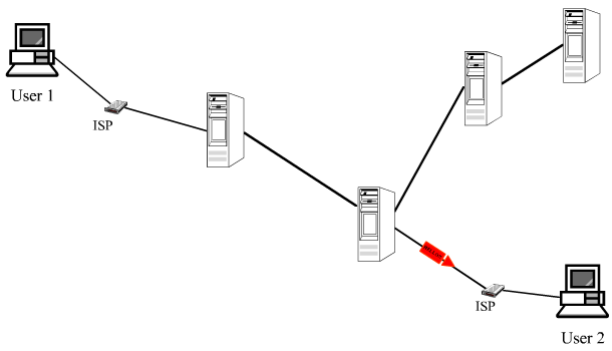


Animation 2.22-1: Handshake Protocol

2.23 One-to-one Communication

The IRC (Internet Relay Chat) is a virtual meeting point. There are several "rooms" where people with various interests can chat in a so-called point-to-multipoint- or one-to-many-communication. You can also "rent" an own room and invite others to join you or leave a room at any time. Furthermore, you can talk to people you meet privately at any time and exchange documents or chat in a "secure" **one-to-one communication**.

Animation 2.23-1 shows an example for a one-to-one communication.

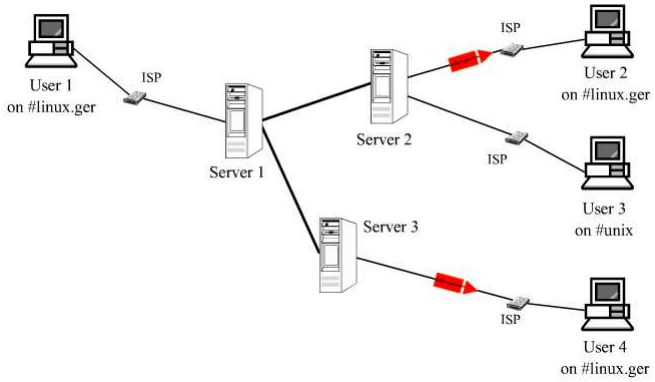


Animation 2.23-1: One-to-one Communication

2.24 One-to-many Comunication

The IRC (Internet Relay Chat) is a virtual meeting point. There are several "rooms" where people with various interests can chat in a so-called point-to-multipoint- or **one-to-many communication**. You can also "rent" an own room and invite others to join you or leave a room at any time. Furthermore, you can talk to people you meet privately at any time and exchange documents or chat in a "secure" one-to-one communication.

Animation 2.24-1 shows an example for a one-to-many communication.

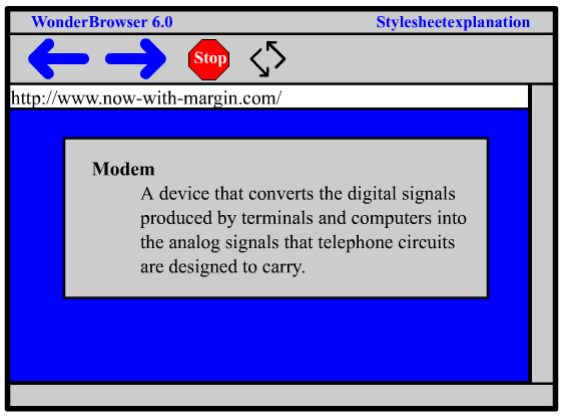


Animation 2.24-1: One-to-many Comunication

2.25 Stylesheet

It is regarded as good style to seperate the visual formatting of HTML documents from the contents. The mechanism that allows this seperation for HTML documents is called Cascading Style Sheets (CSS).

Animation 2.25-1 shows an example of a stylesheet.

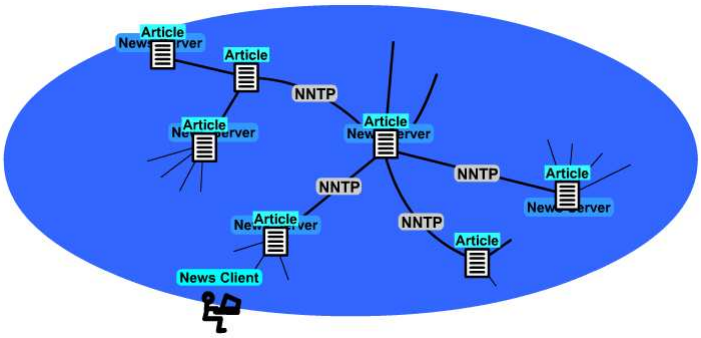


Animation 2.25-1: Stylesheet

2.26 Usenet

Usenet is a world-wide distributed discussion system. It consists of a set of "newsgroups" with names that are classified hierarchically by subject (topic). "Articles" are "posted" to these newsgroups by people on computers with the appropriate software. Articles are similiar to email messages in structure and type of transport mechanisms, but handled by different instances on a computer. Articles are intended for public discussions rather than personal communication and are broadcast to other interconnected computer systems via a wide variety of networks. Some newsgroups are "moderated"; in these newsgroups, the articles are first sent to a moderator for approval before appearing in the newsgroup. Usenet is available on a wide variety of computer systems and networks, but the bulk of modern Usenet traffic is transported over either the Internet (NNTP) or UUCP.

This is exemplified in Animation 2.26-1.



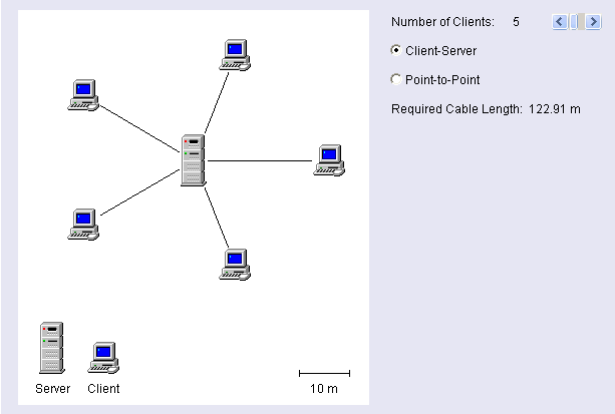
Animation 2.26-1: Usenet

2.27 Client Server Connection

In Animation 2.27-1 you can choose between two connection modes among several computers:

- point-to-point-connection
- client-server-connection

You can choose the number of clients and their position. The required cable length to connect the clients with each other is calculated and displayed automatically.



Animation 2.27-1: Client Server Connection

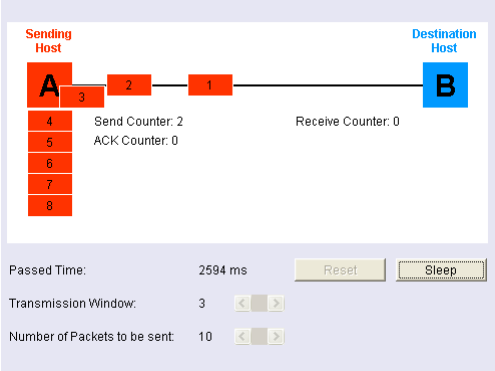
2.28 TCP Packages

Each byte of a TCP stream is numbered, starting with an arbitrary number selected by the sending host. TCP connections are duplex which means that data is transmitted in both directions at the same time. Each host selects an arbitrary starting point for numbering the bytes of its own data stream. The sequence number in the TCP header indicates the number the sending host has assigned to the first byte in the current segment. The numbering starts at an arbitrary number between 0 and $2^32 - 1$ and restarts at zero when the highest value has been reached.

The acknowledgement number contains the value of the sequence number which is expected next from the other side. If the acknowledgement does not arrive within a timeout interval, the data is retransmitted. But instead of waiting for acknowledgement of the receipt of every TCP segment before sending the next segment, TCP implementations define a certain number of bytes, the transmission window, the process will send before it expects an acknowledgement from the other host.

The size of the window is determined on the basis of the maximum number of bytes the host at the other side will accept and on the basis of the time it takes to transmit data from the first host to the second and back again, the round trip time (RTT).

Example: The last TCP byte reaching the receiver had the sequence number 30. Thus, the receiver's acknowledgement number will be 31. This value identifies the number of the next byte which is to be sent by the other side. After receiving this acknowledement the sender transmits the next bytes numbered for example 31 to 60. Assuming that the sender does not receive the next acknowledgement with the number 61 within a certain time interval it retransmits the bytes 31-60.



Animation 2.28-1: TCP Packages

3 Kommunikationsnetze und -protokolle

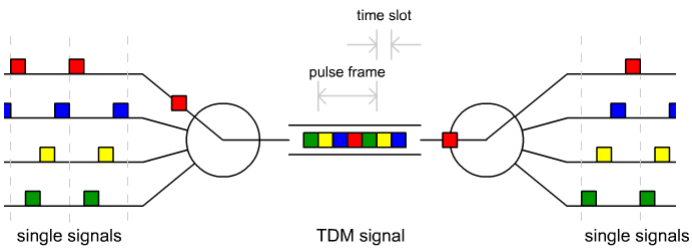
In dem Kurs **Kommunikationsnetze und -protokolle** werden folgende multimedialen Lernmodule eingesetzt:

- Abschnitt 3.1 Animation Time Division Multiplexing
- Abschnitt 3.2 Animation Address Priority
- Abschnitt 3.3 Animation Collision Detection and Resolution
- Abschnitt 3.4 Animation ISDN

3.1 Time Division Multiplexing

Beim Zeitmultiplexverfahren (TDM-Time Division Multiplex) wird der Kanal (zeitlich) periodisch abwechselnd für die Übertragung der einzelnen Signale verwendet. Verwenden n Quellen, die jeweils alle T Sekunden einen Signalwert erzeugen, einen Kanal im Zeitmultiplexverfahren, so muss der Kanal n/T Werte pro Sekunde übertragen. Bei der Zeitmultiplexbildung wird die Periode T in n Intervalle unterteilt. Dies entspricht der Unterteilung des Kanals in n Zeitschlitze. Einem Quellen-Senken Paar steht periodisch alle T Sekunden (d. h. einmal pro Abtastperiode) ein Zeitschlitz zur Verfügung. Es ist auch möglich, einem Quellen-Senken Paar mehr als einen Zeitschlitz pro Periode zuzuteilen, um entsprechend höhere Bitraten zu übertragen. Wird pro Zeitschlitz jeweils lediglich ein Bit übertragen, so bezeichnet man die Multiplexbildung als bitweisebitweise wortweise oder symbolweise Verschachtelungbitweise wortweise oder symbolweise Verschachtelung Verschachtelung. Wird pro Zeitschlitz ein Symbol oder ein Wort übertragen, so bezeichnet man die Multiplexbildung als wortweise oder symbolweise Verschachtelung.

Dieses wird in Animation 3.1-1 veranschaulicht.

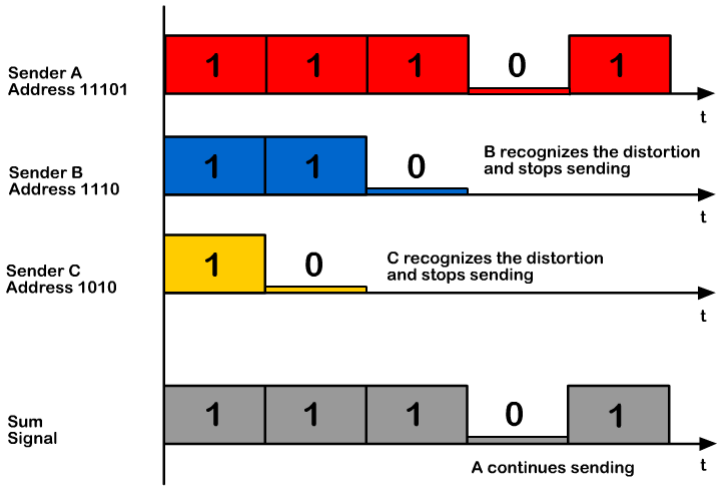


Animation 3.1-1: Time Division Multiplexing

3.2 Address Priority

Die folgende Animation beschäftigt sich mit einer deterministischen Kollisionsauflösungs-Strategie. Hierbei wird die Adressenpriorität für die Kollisionsauflösung verwendet. Animation 3.2-1 bezieht sich auf das Slotted Aloha Verfahren.

Es wird der Fall betrachtet, dass das erste gesendete Wort eine Adresse ist (die eigene oder die des Empfängers). Tritt nun eine Kollision auf, so werden die Bits auf dem Übertragungsmedium so verfälscht, dass sich bei binärer Übertragung eine physikalische Eins (Pegel auf der Leitung) gegenüber einer physikalischen Null (kein Pegel) durchsetzt. Kann diese Verfälschung von der betroffenen Station vor dem Senden des nächsten Bits erkannt werden und gibt die Station das Senden sofort auf, so kann die andere Station ihre Nachricht ungestört weiter senden. Dieses Verfahren setzt voraus, dass eine unmittelbare Rückkopplung für die Stationen möglich ist, und die Signallaufzeiten so klein sind, dass vor dem Senden des nächsten Bits der Nachricht eine Kollisionserkennung möglich ist. Dieses Verfahren wird im ISDN für den Zugriff auf den Signalisierkanal (D-Kanal) des Basisanschlusses angewandt.



Animation 3.2-1: Address Priority

3.3 Collision Detection and Resolution

Animation 3.3-1: Collision Detection and Resolution

3.4 ISDN

Die S-Schnittstelle ist international genormt und stellt den angeschlossenen Endgeräten die beiden B-Kanäle mit 64 kbit/s und den D-Kanal mit 16 kbit/s für die Übermittlung der Nutz- bzw. Signalisierdaten zur Verfügung. Für die Bereitstellung dieser 144 kbit/s wird auf der Übertragungsstrecke eine Bitrate von 192 kbit/s erforderlich. Eine Bitfehlerrate besser als 10-5 wird zugesichert. Da für jede Übertragungsrichtung eine Doppelader zur Verfügung steht, ist eine einfache Übermittlung des anliegenden Bitstromes mit einem ternären Leitungscode möglich. Es wird der AMI-Code mit einer einfachen Modifikation verwendet. Sie besteht darin, dass eine logische 1 in eine physikalische 0 und eine logische 0 alternierend in eine physikalische +1 bzw. -1 umgesetzt wird. Diese Modifikation bewirkt, dass im Ruhezustand, wenn eine logische Null anliegt, auf der Leitung physikalisch eine alternierende ± 1 Folge gesendet wird - damit bleibt der Bittakt auf der Leitung erhalten. Die Signalamplitude beträgt 750 mV (Null-Spitze).

Da alle Endgeräte bitsynchron senden, können Laufzeitunterschiede zu Bitverfälschungen führen. Eine direkte Kommunikation der Endgeräte untereinander über den Bus ist unabhängig von der Vermittlungsstelle (ggf. Vermittlungsfunktion im NT) nicht möglich.

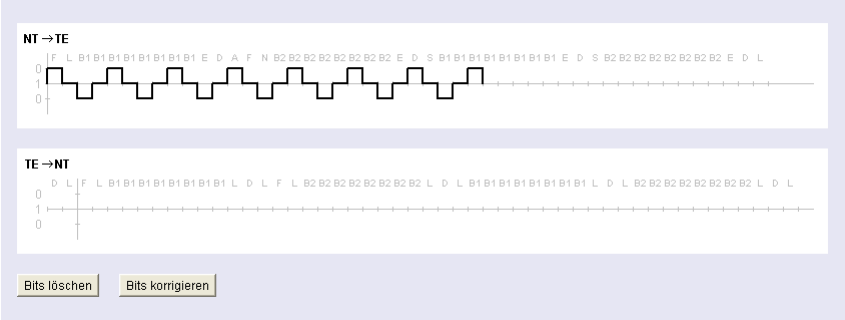
Es ist die Rahmenstruktur der Schicht 1 an der S-Schnittstelle dargelegt. Der Rahmen besteht aus 48 Bit, die in 250 µs übertragen werden. Der Rahmen in Richtung Endgerät zu NT weist einen Versatz von 2 Bit gegenüber dem Rahmen in Richtung NT zum Endgerät auf. Die Lage der beiden B-Kanäle und des D-Kanals ist ersichtlich. Pro Rahmen liegen zwei 8-Bit Wörter pro B-Kanal an. Dies entspricht der PCM Abtastrate von 8 kHz mit 8-Bit Quantisierung (= 64 kbit/s). Die Synchronisation wird nach dem Master-Slave-Prinzip abgewickelt - die Vermittlungsstelle gibt den Takt an. Die Bitsynchronisation beim Endgerät wird über den modifizierten AMI-Code abgeleitet. Die Rahmensynchronisation wird durch das Herbeiführen einer Codeverletzung erzielt. Das Rahmenbit F wird so gesetzt, dass die AMI-Coderegel ($\pm$ 1 stets alternieren), verletzt wird. Eine weitere Codeverletzung wird durch die Codierung der ersten logischen Null, die dem ersten L-Bit des Rahmens folgt, erzeugt. Diese wird spätestens durch das Setzen des) F_A -Bits erwirkt. Diese weitere Codeverletzung sichert die Rahmensynchronisation ab; sie dient auch dazu, die laufende digitale Summe RDS, die durch die erste Codeverletzung erhöht wurde, wieder herabzusetzen. Die F_A, N- und MBits (M-Bit = S Bits) können auch zur Überrahmenbildung verwendet werden - in den Netzen der europäischen Verwaltungen wird dies in der Regel nicht vorgenommen.

- In beiden Richtungen

  2 x 8 Bit B1 - Kanal = 64 kbit/s
  2 x 8 Bit B2 - Kanal = 64 kbit/s
  4 Bit D - Kanal = 16 kbit/s

- 2 Bit Rahmenversatz (Verzögerung im TE)

Wir haben bei der Leitungscodierung gesehen, dass eine Gleichstromfreiheit des laufenden Bitstromes gewünscht ist. Dies wird durch das Setzen des L-Bits, so dass die laufende digitale Summe RDS Null wird, erreicht. In Richtung NT zu TE wird ein L-Bit zum Ausgleich des F-Bits und ein weiteres LBit zum Ausgleich des restlichen Rahmens erforderlich. Da die unterschiedlichen Kanäle in Richtung TE zu NT von unterschiedlichen Endeinrichtungen (TEs) genutzt werden können, ist ein Gleichstromausgleich pro Kanal erforderlich. Die L-Bits werden von den jeweiligen Endgeräten gesetzt.



Animation 3.4-1: ISDN

4 Grundlagen der Kryptologie

In dem Kurs **Grundlagen der Kryptologie** werden folgende multimedialen Lernmodule eingesetzt:

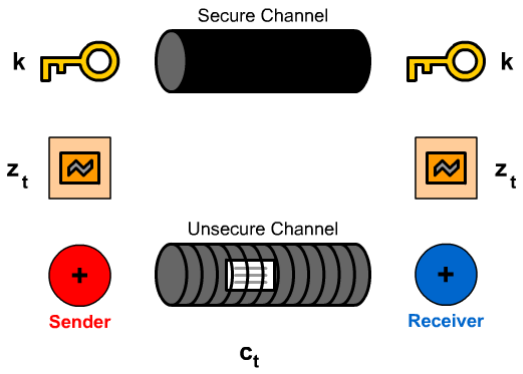
4.1 Additive Stromverschlüsselung

Animation 4.1-1 represents the principle of an **additive stream cipher**.

The follwoing symbols are used: k is the secret, symmetric key, f is the keystream generator, m_t the message sequence and z_t the keystream sequence.

Encryption and Decryption are calculated by the following terms.

- Encryption: $c_t = z_t + m_t$
- Decryption: $m_t = z_t + c_t$



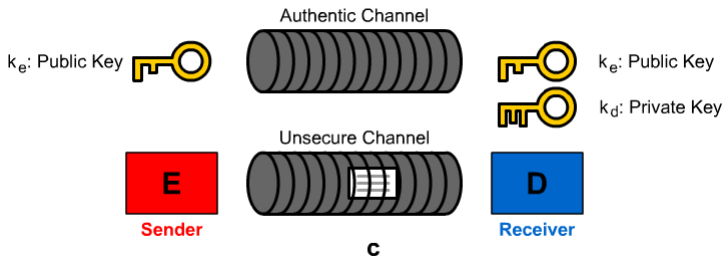
Animation 4.1-1: Additive Stromverschlüsselung

4.2 Asymmetrische Verschlüsselung

Animation 4.2-1 represents the principle of an **asymmetric key encryption** system.

Encryption and Decryption are calculated by the following terms.

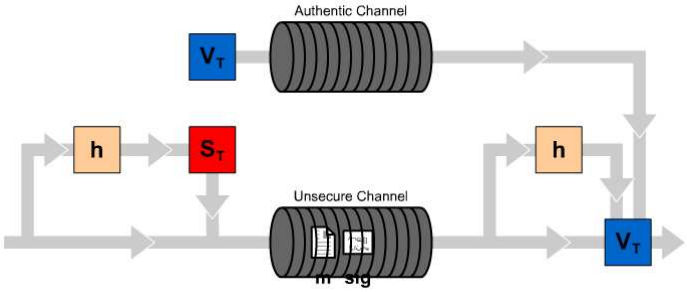
- Encryption: $c = E_{k_e}(m)$
- Decryption: $m = D_{k_d}(c)$



Animation 4.2-1: Asymmetrische Verschlüsselung

4.3 Digitale Signatur

Animation 4.3-1 represents the generation and verification of a **digital signature** with the aid of a hash function.



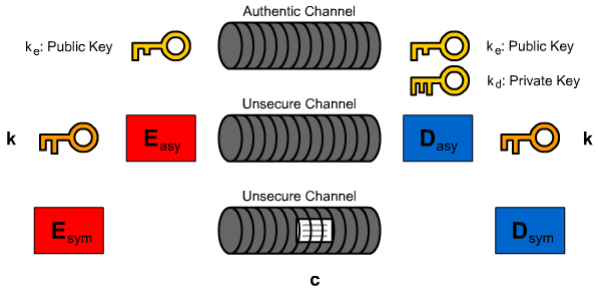
Animation 4.3-1: Digitale Signatur

4.4 Hybride Verschlüsselung

Animation 4.4-1 represents the principle of the **hybrid encryption system**.

Encryption and Decryption are calculated by the following terms.

- Encryption: $c_1 = E_{asy,k_e}(k)$ and $c_2 = E_{sym,k}(m)$
- Decryption: $k = D_{asy,k_d}(c_1)$ and $m = D_{sym,k}(c_2)$



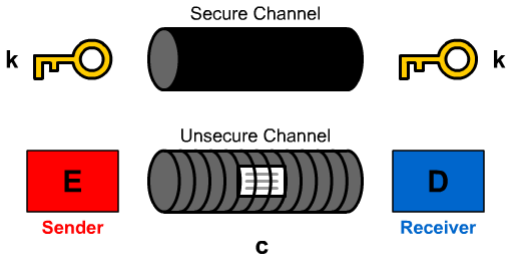
Animation 4.4-1: Hybride Verschlüsselung

4.5 Symmetrische Verschlüsselung

Animation 4.5-1 represents a **symmetric-key encryption** system with the encryption function E, the decryption function D and the secret key k. m means the message and c the ciphertext.

Encryption and Decryption are calculated by the following terms:

- Encryption: $c = E_k(m)$
- Decryption: $m = D_k(c)$



Animation 4.5-1: Symmetrische Verschlüsselung

4.6 Nichtlineares rückgekoppeltes Schieberegister

Animation 4.6-1 ist für den Kurs Grundlagen der Kryptologie entwickelt worden.

Im folgenden wird die Bedienung erläutert:

Als erstes wählt man mit Hilfe des Scrollbars den Wert l - den Grad des Rückkopplungspolynoms c. Hierbei wird automatisch ein neues zufälliges Rückkopplungspolynom $c(c_l, cl-1, ..., c_0)$ und ein neuer zufälliger Initialstatus $s(s_{l-1}, s_{l-2}, ..., s_0)$ angezeigt.

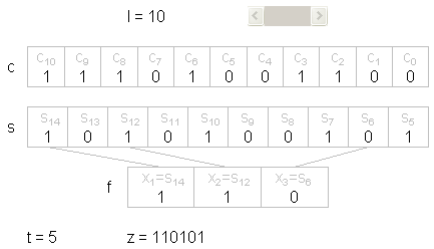
Dann kann man durch Klicken mit der Maus auf die einzelnen Bits das Rückkopplungspolynom c bzw. den Initialstatus s setzen.

Durch Klicken mit der Maus auf die einzelnen Bits der Filterfunktion f werden die Werte für die "tapping sequence" G ausgewählt. Als Funktion f liegt dem Applet immer die Funktion$f(x_1, x_2, x_3) = x_1x_2 \oplus x_3$ zugrunde.

Nun kann man durch Betätigen der Schaltfläche ">" einen Zeitschritt t ausführen. Die Ergebnisbits $z_0, z_1, ..., z_t$ werden rechts von der Funktion f in Form eines Bitstroms dargestellt.

Durch Betätigen der Schaltfläche ">>" werden automatisch viele Zeitschritte hintereinander ausgeführt. Mit "Stop" kann diese Aktion wieder unterbrochen werden.

Nur wenn $t = 0$ ist, können Änderungen an den Startwerten vorgenommen werden. Hat man bereits Zeitschritte ausgeführt, muss man erst durch Betätigen der Schaltfläche "Reset" zum Zeitpunkt $t = 0$ zurückspringen, um dann Änderungen an den Startwerten vornehmen zu können.



Animation 4.6-1: Nichtlineares rückgekoppeltes Schieberegister

4.7 Verschlüsselungsmodi

Animation 4.7-1 demonstrates the different modes of operation.

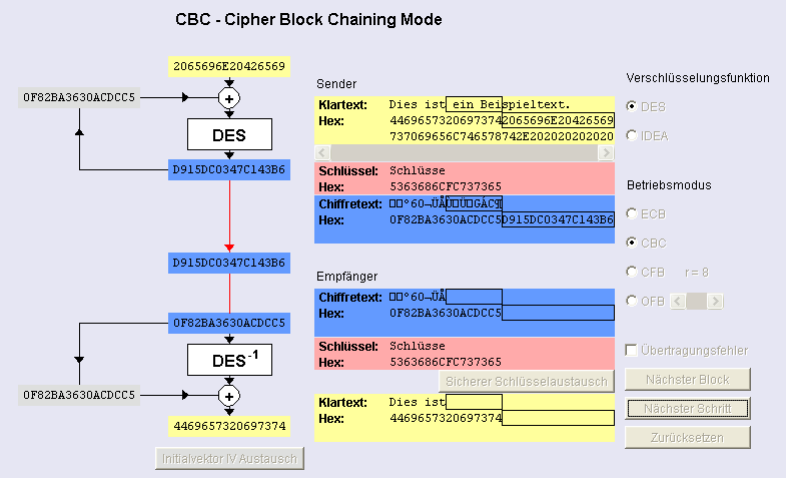
You can choose between the 2 block ciphers **DES** (64 Bit block length / 64 Bit key length) and **IDEA** (64 Bit block length / 128 Bit key length).

The following modes of operation are implemented

- **ECB** - Electronic Codebook Mode
- **CBC** - Cipher Block Chaining Mode
- **CFB** - Cipher Feedback Mode
- **OFB** - Output Feedback Mode

Besides you have several possibilities to experiment with this applet.

- The plaintext and both keys (sender and receiver) can be input in ASCII-Text.
- In the modes CFB and OFB the shortened block length r can be changed.
- In the modes CBC, CFB and OFB the Initialvector IV can be changed.
- You can input transmission errors.
- One block can be transmitted in a film sequence or step by step.



Animation 4.7-1: Verschlüsselungsmodi

4.8 Elliptische Kurven

Elliptic curves have been studied by mathematicians for more than a century. An extremely rich theory has been developed around them, and in turn they have been the basis of numerous new developments in mathematics. As far as cryptography is concerned, elliptic curves have been used for factoring and primality proving.

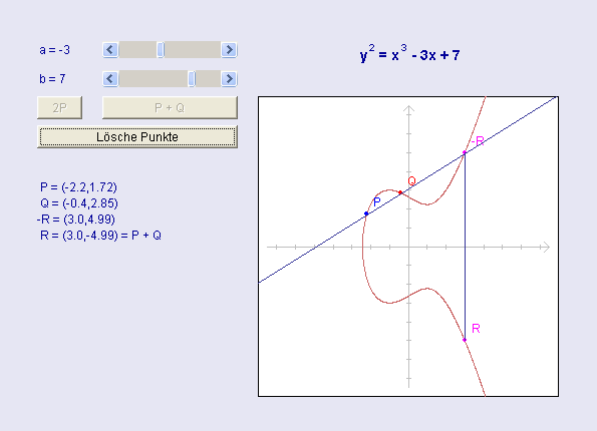
4.8.1 Elliptische Kurven - kontinuierlich

To understand more about the elliptic curve forms, vary the parameter a and b on a continous elliptic curve in Animation 4.8-1.

Try to choose the points P and Q on a continous elliptic curve.

Depending on the chosen point P you can calculate $kP = P + (k-1)P$ with the corresponding button.

Depending on the chosen points P and Q you can calculate $R = P + Q$ with the corresponding button.



Animation 4.8-1: Elliptische Kurven - kontinuierlich

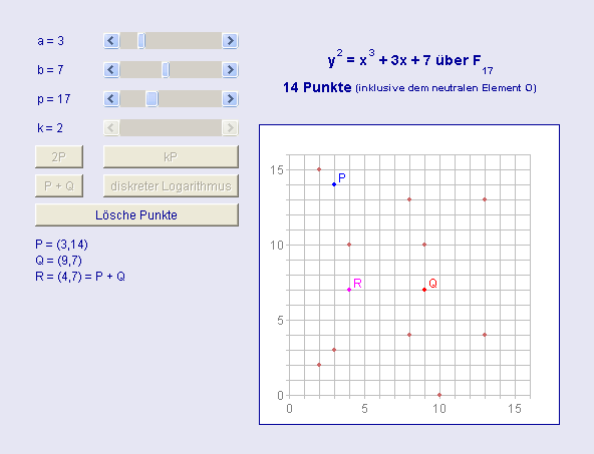
4.8.2 Elliptische Kurven - diskret

To understand more about the elliptic curve forms, vary the parameter a, b, p and k on a discrete elliptic curve in Animation 4.8-2.

Try to choose the points P and Q on a discrete elliptic curve.

Depending on the chosen point P you can calculate $kP = P + (k-1)P$ with the corresponding buttons.

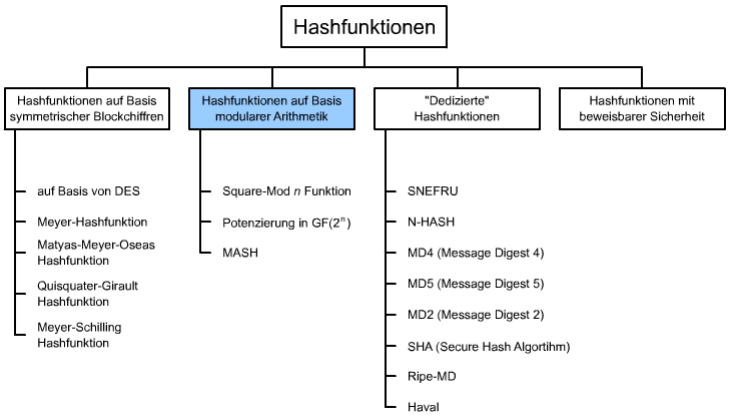
Depending on the chosen points P and Q you can calculate $R = P + Q$ or the discrete logarithm with the corresponding buttons.



Animation 4.8-2: Elliptische Kurven - diskret

4.9 Hashfunktionen

In Animation 4.9-1 you learn much about Hash Functions.



Animation 4.9-1: Hashfunktionen

4.10 Online Krypto-Rechner

Krypto-Rechner

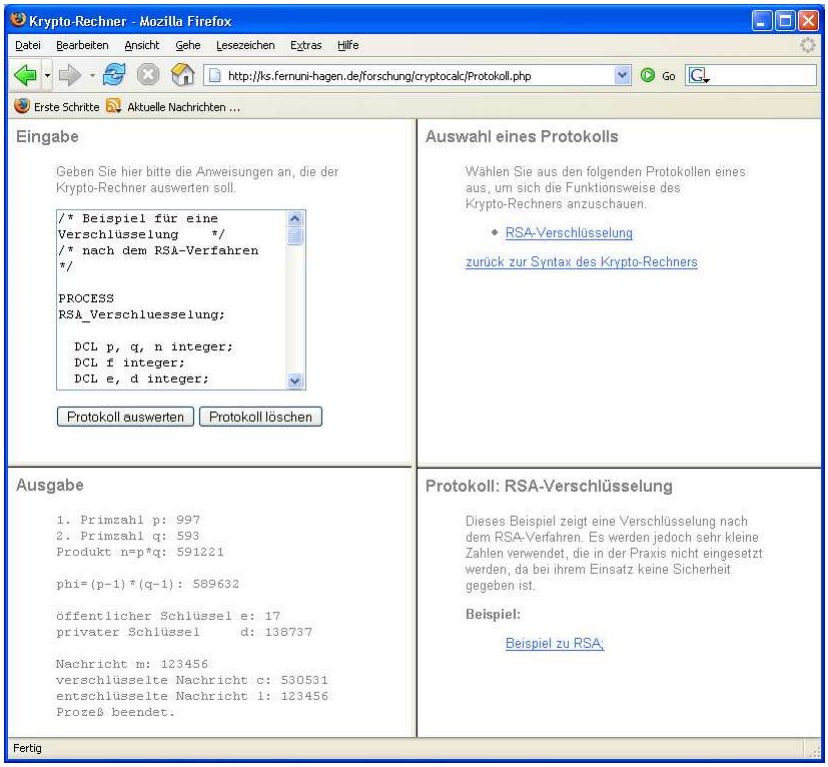
Mit Hilfe des **Krypto-Rechners** sind Berechnungen von Funktionen und Ausdrücken mit hohen Zahlen möglich.

Der Krypto-Rechner kann in zwei Betriebsmodi arbeiten. Bei der Auswertung von einzelnen Ausdrücken können Ausgaben einzelner Anweisungen oder Funktionen erzeugt werden. Dieser Modus ist jedoch wenig geeignet für ganze Protokollabläufe, bei denen eine Folge von Ausdrücken berechnet werden kann. In diesem Fall können Ausgaben durch Aufruf der Funktion writeln erzeugt werden.

Bei der Benutzung des Krypto-Rechners stehen Ihnen neben mathematischen Funktionen (modulare Exponentation, Primzahltests und einfache Faktorisierungsalgorithmen) und Zufallsfunktionen viele Funktionen im Bereich Verschlüsselungsfunktionen (DES, IDEA, RC5), Schieberegisterfunktionen, Polynomfunktionen und Hashfunktionen (Sqaremod, MD5, SHA1) zur Verfügung.

Während der Implementierung des Krypto-Rechners wurde hoher Wert auf Ausführungsgeschwindigkeit gelegt, so dass die Funktionen auch mit hohen Zahlen (z. B. 512 bis 1024 Bit) in angemessener Zeit ausgewertet werden.

Sie finden den online Krypto-Rechner im Internet unter dem Link http://ks.fernuni-hagen.de/forschung/cryptocalc



Online Krypto-Rechner

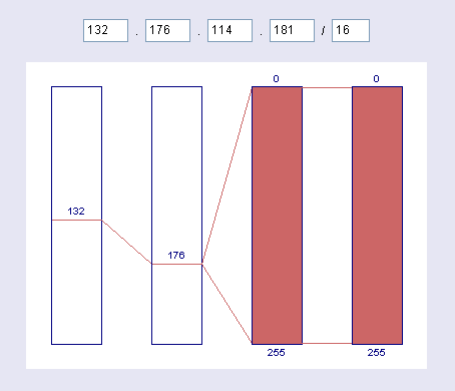
5 Netzwerksicherheit

In dem Kurs **Netzwerksicherheit** werden folgende multimedialen Lernmodule eingesetzt:

- Abschnitt 5.1 Animation IP-Mask
- Abschnitt 5.2 Animation IP-Filter
- Abschnitt 5.3 Animation IP-Tables
- Abschnitt 5.4 Animation HT Access

5.1 IP-Mask

The network address is an IP address in which the least significant bits are set to zero. The number of bits of the IP address which are set to zero depends on the address type. The most significant bits on the left identify the network, the least significant bits identify the individual hosts in the network.



Animation 5.1-1: IP-Mask

5.2 IP-Filter

A more general solution to filter connection oriented services is called stateful inspection. It was suggested to introduce some state into packet filtering process. Consequently, the resulting packet filter rules are dy- namic and context-sensitive, the first attribute also being reflected in the term dynamic packet filtering that is sometimes used as a synonym for stateful inspection.

Stateful inspection (or dynamic packet filtering) looks at the same header information as static packet filtering does, but can also peek into the payload data where the transport and application layer data usually appears. More importantly, stateful inspection maintains state information about passed IP packets. It compares the first packet in a TCP connection to the packet filter rules, and if the packet is permitted, state information is added to an internal database. Think of this state information representing an internal virtual circuit in the firewall on top of the transport layer association. This information permits subsequent packets in that association to pass quickly through the firewall. If the rules for a specific type of service require examining application data, the part of each packet must still be examined.

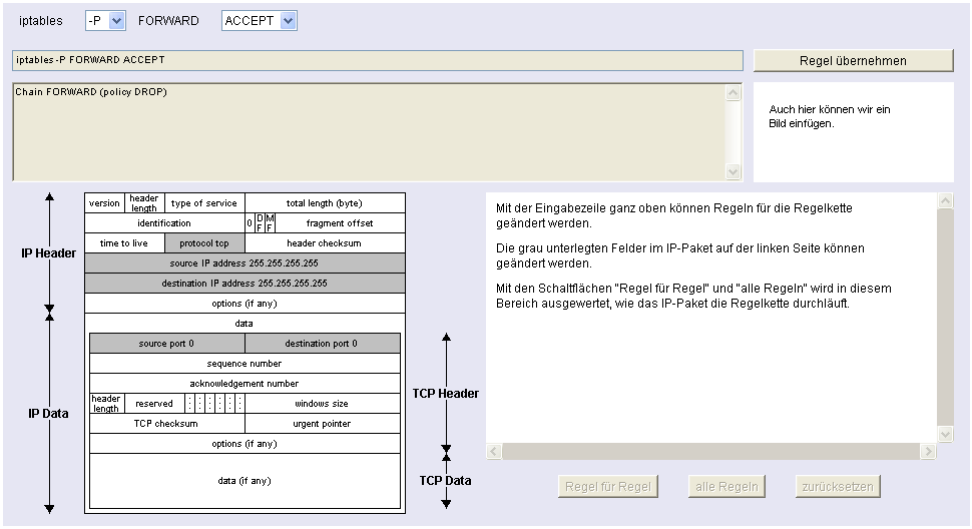
For example, a dynamic packet filtering device can react on seeing an FTP PORT command by creating a dynamic rule permitting a TCP connection back from the FTP server to that particular port number of the client side. Logging, or authentication as required by the rules, generally occurs at the application layer. Although the opportunity for better logging is present, stateful inspection firewalls typically only log the source and destination IP addresses and port numbers, similar to logging with a packet filter or screening router.

In spite of the fact that you can introduce state information to improve the capabilities of a packet filtering device, the problem remains that there is no such thing as an association between a data stream and a previously authenticated and authorized user. To make things worse, there is no such thing as a user on the Internet layer where packet filtering occurs. Consequently, true firewalls must operate above the Internet layer, typically at the transport layer. There are also further problems with stateful packet filtering:

1. State tracking of a packet filter provides the ability to do things that you cannot do therewise, but it also adds complications. First, the packet filter has to keep track of the state. This increases the load on the packet filter, opens it to a number of denial of service attacks, and means that if the router reboots, packets may be denied when they should have been accepted. If a packet may go through redundant packet filters, they all need to have the same state information. There are protocols for exchanging this informa- tion, but it's still a tricky business. If you have redundant routers simultaneously, the state information needs to be transferred between them almost continously, or the response packet may come through before the state is updated.

2. Second, the packet filter has to keep track of state without any guarantee that there is ever going to be a response packet. Not all UDP packets have

responses. At some point, the packet filter needs to give up and to get rid of the rule that will allow the response. If the packet filter gives up early, it will deny packets that should have been accepted, causing delays and unneeded network tra±c. If the router keeps the rule too long, the load on the router will be unnecessarily high, and there is an increased chance that packets will be accepted when they should have been denied. Some protocol specifications provide guidelines, but those are not necessarily useful. For instance, DNS (Domain Name Service) replies are supposed to arrive within 5 seconds, but reply times for name service queries across the Internet can be as high as 15 seconds. An implementation of the protocol specification will almost deny a response that you wanted to accepted.



Animation 5.2-1: IP-Filter

5.3 IP-Tables

Iptables rules for a small network

Now we want to discuss a small network scenario. Suppose our intranet has the subnet IP number 172.16.1.0 with subnet mask 255.255.255.0, which is equal to 24 ones from the left side. The users in the subnet are allowed to access WWW servers on the Internet with their WWW browsers, but no other traffic is allowed. Remember,WWWservers listen usually on port 80 of the TCP protocol for connection requests. A screening router with Linux operating system (kernel 2.4) and installed iptables is physically between the Internet and the local intranet.

The screening router has two network interfaces, one is connected with the Internet and the other with the intranet.

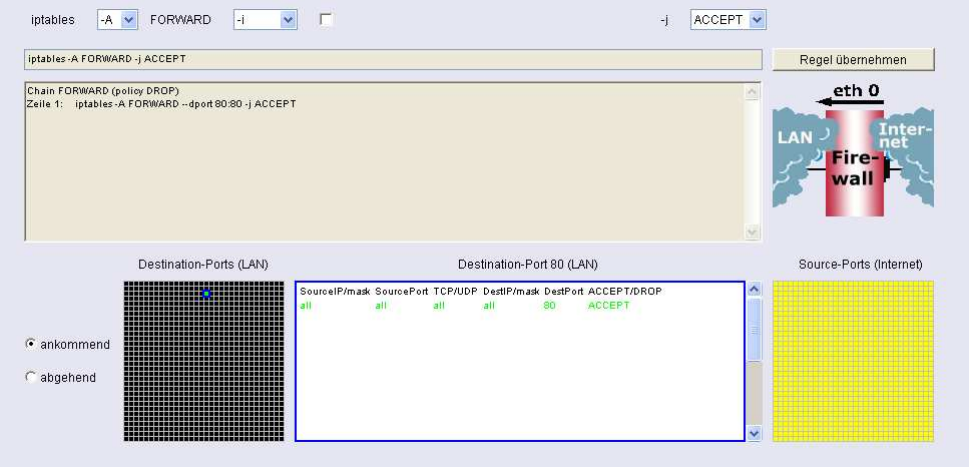
The netfilter kernel module has to be configured to fulfill the above policy for the intranet.

At first the kernel module that provides support for netfilter has to be loaded in the kernel:

Now the commands to build the chains for the filter table, that fulfill the above policy:

```
$ modprobe ip tables
$ iptables -F OUTPUT
$ iptables -P OUTPUT DROP
$ iptables -F INPUT
$ iptables -P INPUT DROP
$ iptables -F FORWARD
$ iptables -P FORWRAD DROP
$ iptables -A FORWARD -m tcp -p tcp -s 0/0 --sport 80 -d 172.16.1.0/24 --syn -j DROP
$ iptables -A FORWARD -m tcp -p tcp -s 172.16.1.0/24 -d 0/0 --dport 80 -j ACCEPT
$ iptables -A FORWARD -m tcp -p tcp -s 0/0 --sport 80 -d 172.16.1.0/24 -j ACCEPT
```

The table filter has not to be specified, because filter is the default table. With the first six commands all three chains in the filter table are cleaned and the default policy of the chains is set to DROP.



Animation 5.3-1: IP-Tables

5.4 .htaccess-Files

Intention of Animation 5.4-1 is to help you understand how .htaccess files can be used to restrict access to certain directories.

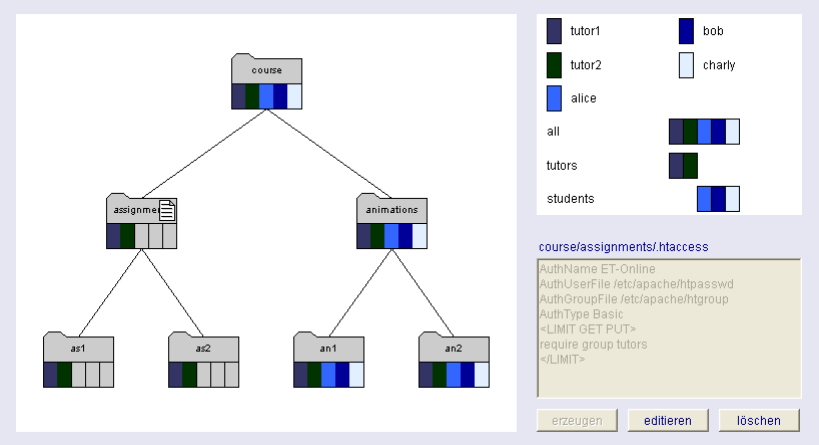
The applet is subdivided into three windows:

- The main window contains the directory structure,
- the legend is displayed in the upper right part and
- the third window contains the content of a certain .htaccess file.

To create a .htaccess file proceed as follows:

- Select the directory you want to protect,
- press the buttons "create" and "edit" to generate the required .htaccess file.
- Finally, select the users who should have access to the directory and press the button "close edit".

The main window is now updated, indication which user has access to which directories.



Animation 5.4-1: HT Access

6 Digitale Bildcodierung

In dem Kurs **Digitale Bildcodierung** werden folgende multimedialen Lernmodule eingesetzt:

- Abschnitt 6.1 Animation Kompressionsverhältnis bei der Videodatenraten-Reduktion
- Abschnitt 6.2 Animation Diskrete Cosinus Transformation
- Abschnitt 6.3 Animation DPCM
- Abschnitt 6.4 Animation Additive und subtraktive Farbmischung
- Abschnitt 6.5 Animation QPSK Modulation

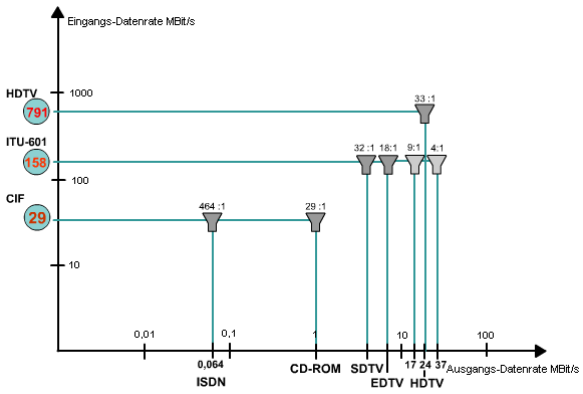
6.1 Kompressionsverhältnis bei der Videodatenraten-Reduktion

Hochaufgelöste Videobilder mit 1920 x 1080 Bildpunkten erfordern netto bei 8 Bit Quantisierung eine Datenrate von 791 Mbit/s, brutto (einschließlich Audio, Austastlücken etc.) bei 10 Bit Quantisierung sogar bis zu 1485 Mbit/s.

Es ist unmittelbar einsichtig, dass diese großen Datenmengen auf konventionellen Übertragungsmedien nicht wirtschaftlich transportiert werden können. Die Übertragungskapazität eines typischen digitalen Satellitentransponders liegt beispielweise bei etwa 40 Mbit/s. Ähnliche Werte gelten auch für die Verbreitung über Kabelnetze. Bei der digitalen terrestrischen Ausstrahlung liegt die korrespondierende Kapazität innerhalb eines konventionelle Fernsehkanals nur bei etwa der Hälfte, 20 Mbit/s.

Diese Diskrepanz zwischen Datenaufkommen und Kapazität führt dazu, dass das digitale Videosignal für die Übertragung mittels eines geeigneten Datenreduktionsverfahrens deutlich komprimiert werden muss.

Animation 6.1-1 veranschaulicht die notwendige Videodaten-Reduktion für drei typische Videosignalformate als Eingangssignal und die Übertragungskapazität einiger Übertragungsmedien.

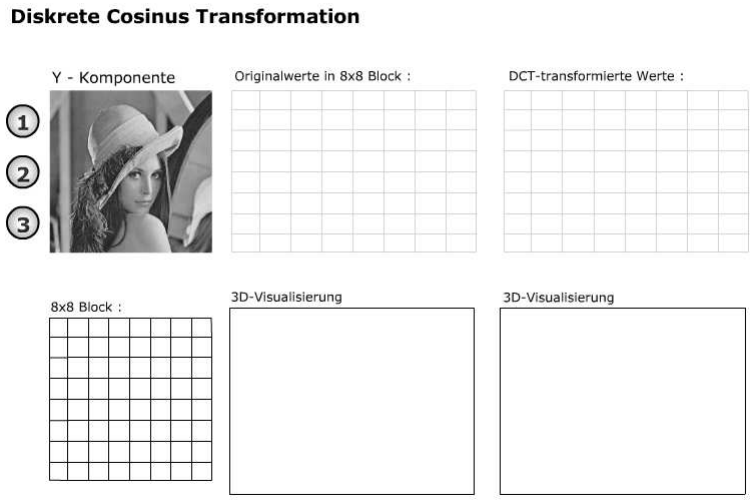


Animation 6.1-1: Kompressionsverhältnis bei der Videodatenraten-Reduktion

6.2 Diskrete Cosinus Transformation

Die nachfolgende Animation 6.2-1 zeigt an Hand einer Testbildvorlage, wie verschiedene Bildblöcke zu einer unterschiedlichen Verteilung der Koeffizienten bei der DCT führen.

Die Animation repräsentiert einen 8 x 8 Pixel großen Bildblock mit fein strukturiertem Bildinhalt (links). Im korrespondierenden DCT-Block (rechts) sind viele Koeffizienten mit großem Betrag10 vorhanden. In dem hier betrachteten Bildblock ist offensichtlich, dass die Korrelation zwischen benachbarten Bildpunkten relativ gering ist.



Animation 6.2-1: Diskrete Cosinus Transformation

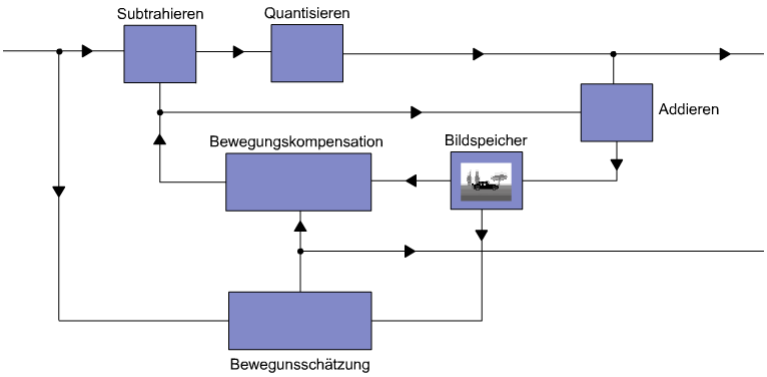
6.3 DPCM

Das Prinzip der Bewegungskompensation

Will man für die bewegten Bildreiche eine gute Prädiktion erzielen, müssen die Bewegungen dieser Bildbereiche für die aktuelle Bewegungsphase geeignet zurechtgerückt werden. Dieser Vorgang wird in der Bildcodierung „Bewegungskompensation“ genannt. Bildsequenzen entstehen durch die zeitliche Abtastung von zeitkontinuierlichen Bildsignalen. Die Bewegung wird dabei ebenfalls zeitlich diskretisiert. Daher ist der Begriff Verschiebungskompensation treffender. Da sich jedoch der Begriff Bewegungskompensation in der Literatur eingebürgert hat, werden nachfolgend beide Begriffe synonym verwendet. Um eine Bewegungskompensation oder Verschiebungskompensation durchführen zu können, ist eine örtliche Lokalisierung der bewegten Objekte und die Schätzung der Verschiebung erforderlich.

Obwohl beide Prädiktoren - wie bei der DPCM üblich - die gleichen Signale verarbeiten, ist die Komplexität zwischen Coder und Decoder unterschiedlich. Die für die Prädiktion erforderlichen Bewegungsinformation (Verschiebungsvektoren und die zugehörige örtliche Objektzuordnung) wird nämlich ausschließlich am Coder erzeugt und zusammen mit dem Differenzbild zum Decoder übertragen. Dieser kann verhältnismäßig einfach mit einem vorherigen Einzelbild und der Bewegungskompensation das aktuelle Einzelbild errechnen.

Animation 6.3-1 zeigt das Prinzip der Bewegungskompensation.



Animation 6.3-1: DPCM

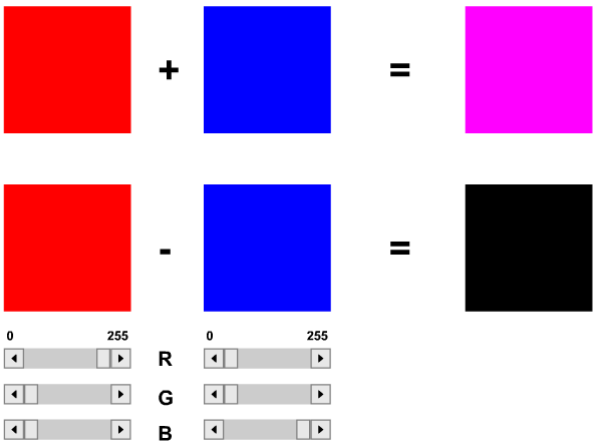
6.4 Additive und subtraktive Farbmischung

Subtraktive Farbmischung

Ein Beispiel für die so genannte subtraktive Farbmischung ist das Zusammenführen verschiedenfarbiger Farbstoffe, wie es bei der Malerei geschieht. Dieses Mischen von übereinander liegenden Farbstoffen kann man als das Zusammenfügen von Farbfiltern mit unterschiedlichen farblichen Absorptionseigenschaften verstehen. So erhält man beispielsweise grünliches Licht, wenn man vor eine weiße Lichtquelle ein blaues und dahinter ein gelbes Filter setzt. Der resultierende Farbeindruck entsteht also durch die nach der optischen Filterung verbleibenden Farbanteile einer ursprünglich weißen Lichtquelle. Dazu wird angenommen, dass die weiße Lichtquelle eine weitgehend kontinuierliche Energieverteilung über das ganze sichtbare Spektrum besitzt. Diese Annahme ist in der Regel für natürliche Lichtquellen gegeben. Die subtraktive Farbmischung wird vielfach auch bei Farbdruckern verwendet, die mit drei oder mehr Grundfarben arbeiten. Als Grundfarben werden dann aber oft gelb, magenta, cyan und ggf. weitere verwendet.

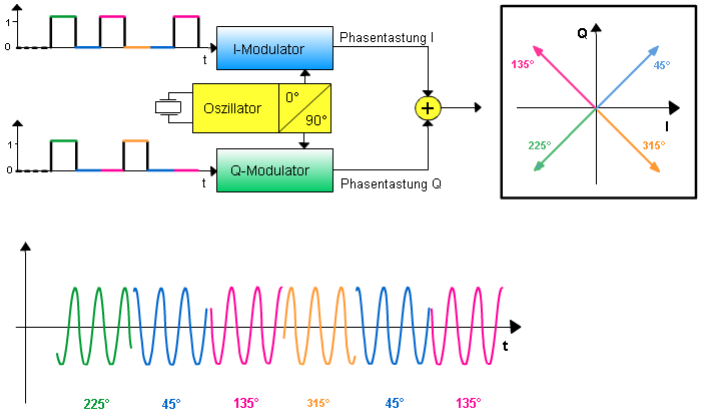
Additive Farbmischung

Dazu entsteht im Gegensatz bei der additiven Farbmischung der resultierende Farbeindruck, in dem kleine, dicht beieinander liegende, selbst leuchtende Farbpunkte aus so großen Entfernung betrachtet werden, dass die einzelnen Farbpunkte nicht mehr separat aufgelöst werden können, sondern ineinander verschmelzen. Ebenso ist die additive Mischung auch durch die Projektion von einem roten, grünen und blauen Bildauszug auf eine gemeinsame Bildwand möglich. Das Wesentliche der additivenMischung liegt darin, dass die Farbanteile der verschiedenen Farben additiv von den Sehzellen des menschlichen Auges wahrgenommen werden. Die additive Mischung funktioniert, solange eine Trennung der einzelnen Farbanteile vom menschlichen Auge nicht in örtlicher oder zeitlicher Richtung möglich ist. In dem zuvor genannten Beispiel mit den kleinen Farbpunkten ist das dann der Fall, wenn ein hinreichend großer Betrachtungsabstand gegeben ist. Die zeitliche Trägheit des menschlichen Auges ermöglicht auch eine additive Farbmischung ohne dass die Farbanteile gleichzeitig vorhanden sein müssen. Vielmehr kann die Farbdarstellung auch gelingen, wenn zeitlich sequenziell gezeigte Farbblitze so schnell auftreten, dass sie vom Auge hinreichend gut zu einem Gesamtfarbeindruck integriert werden. Eine Reihe von Farbbildprojektoren arbeiten nach diesem Prinzip (Farbkreisel).



Animation 6.4-1: Additive und subtraktive Farbmischung

6.5 QPSK Modulation

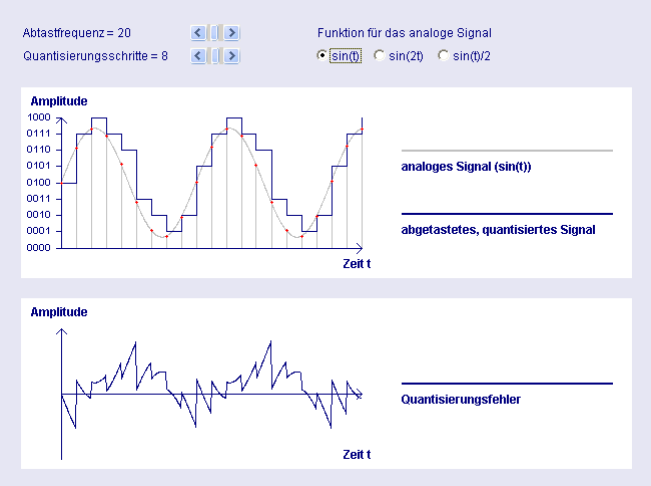


Animation 6.5-1: QPSK Modulation

7 Verschiedene

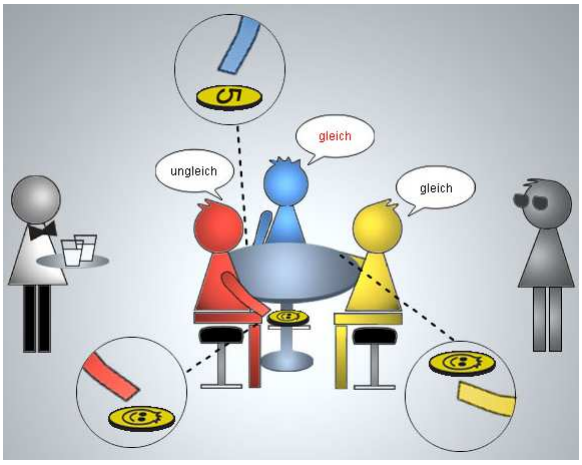
Die folgenden multimedialen Lernmodule sind noch keinem der bisher genannten Themen zugeordnet:

7.1 Pulse Code Modulation



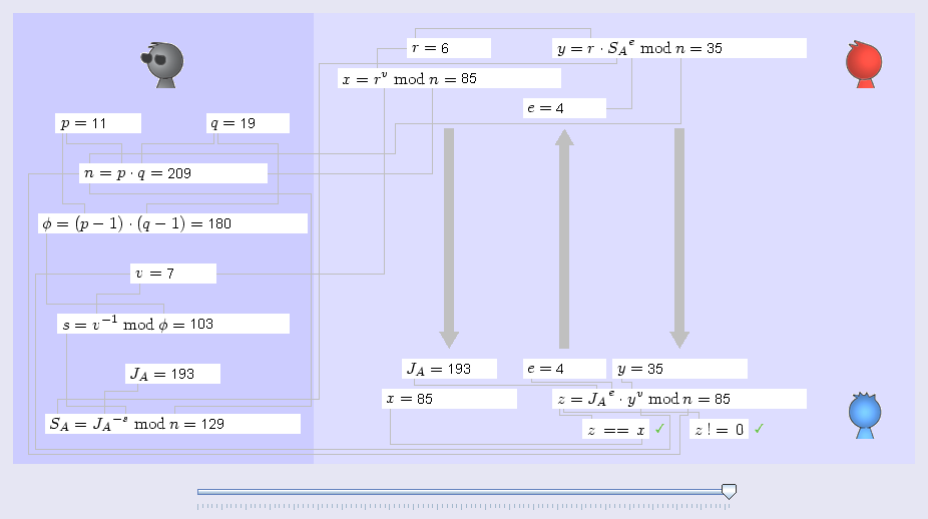
Animation 7.1-1: Pulse Code Modulation

7.2 Dining Cryptographers



Animation 7.2-1: Dining Cryptographers

7.3 Guillou-Quisquater

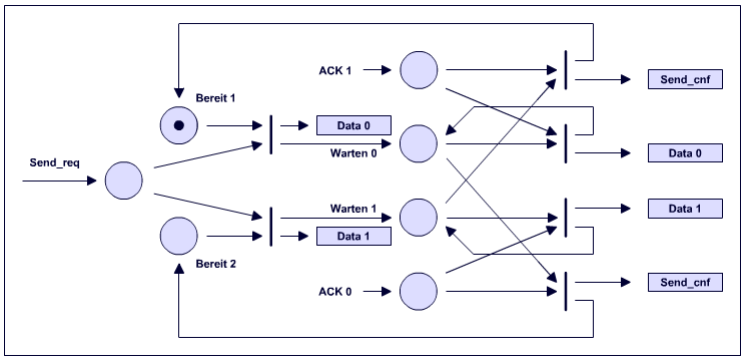


Animation 7.3-1: Guillou-Quisquater

7.4 Petrinetze

Petrinetze arbeiten transitionsorientiert. Sie erlauben Interaktionen zwischen parallelen Prozessen auf einem hohen Abstraktionsniveau darzustellen. Da sie auf Rechnern abgebildet werden können, eignen sie sich gut, Protokollabläufe zu studieren. Sie eignen sich besonders zum Analysieren von Flußabläufen. Sie unterliegen denselben Einschränkungen wie Zustandsautomaten, nämlich daß sie schnell sehr komplex und somit nicht handhabbar werden.

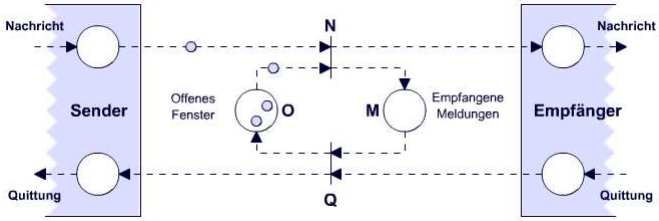
Petrinetze bestehen aus einer Anzahl von Stellen (die durch Kreise dargestellt werden) und einer Anzahl von Transitionen (die durch Striche dargestellt werden). Die Stellen und Transitionen werden durch gestrichelte Kanten zu einem Graph verbunden. Die Kanten, die von einer Stelle ausgehen, enden immer an einer Transition und umgekehrt. An jeder Stelle (d. h. in jedem Kreis) können sich ein oder mehrere Marken befinden. Eine Marke an einer Stelle bedeutet, daß die Bedingung für die Transition, die mit der Stelle geknüpft wird, erfüllt ist. Sind alle Stellen die zu einer Transition gehören mit mindestens einer Marke belegt, so kann die Transition durchgeführt werden - man sagt die Transition kann zünden. Bei der Zündung einer Transition wird jeder Stelle, von der eine Kante zu der Transition führt, eine Marke entnommen und jeder Stelle, zu der eine Kante von der Transition ausgeht, eine Marke hinzugefügt.



Animation 7.4-1: Petrinetze

7.5 Fenstermechanismus

Animation 7.5-1 stellt die Quittierung mit Fenstermechanismus dar. Der Sender darf maximal drei unquittierte Meldungen absenden. Der Sender wird durch eine Stelle, in der pro Nachricht die zum Senden vorliegt eine Marke eingelegt wird und eine Stelle, zu der für jede quittierte Nachricht eine Marke ankommt, modelliert. Der Empfänger wird durch eine Stelle, in die für jede Quittung eine Marke eingelegt wird und eine Stelle, an der jede ankommende Nachricht durch eine ankommende Marke dargestellt wird, modelliert. Zwei Transitionen N (Nachricht wird gesendet) und Q (Quittung wird gesendet) und zwei Stellen O (Offenes Fenster) und M (Empfangene Meldungen) modellieren das Protokoll. Am Anfang der Übertragung werden drei Marken in O gelegt. Dies bedeutet, dass das Fenster ganz offen ist; es dürfen maximal drei Nachrichten abgesendet werden, ohne dass quittiert werden muss. Liegt eine Nachricht vor, so wird eine Marke in die Nachrichtenstelle im Sender gelegt. Die Transition N kann nun zünden. In O bleiben 2 Marken übrig (es können noch zwei Nachrichten ohne Quittung abgesendet werden), in M befindet sich nun eine Marke (eine Nachricht wurde empfangen). Sendet der Empfänger eine Quittung und liegt in M eine Marke, so kann Q zünden, eine Marke wird M (und dem Empfänger) entnommen und eine Marke (Quittung) wird dem Sender gegeben. Ein solches Modell lässt sich leicht auf einem Rechner implementieren und erlaubt verschiedene Abläufe durchzuspielen.

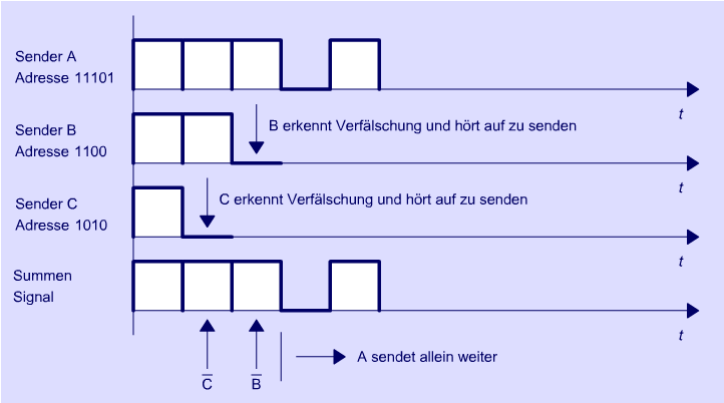


Animation 7.5-1: Fenstermechanismus

7.6 Kollisionsauflösung über Adressenpriorität

Die folgende Animation beschäftigt sich mit einer deterministischen Kollisionsauflösungs-Strategie. Hierbei wird die Adressenpriorität für die Kollisionsauflösung verwendet. Animation 7.6-1 bezieht sich auf das Slotted Aloha Verfahren.

Es wird der Fall betrachtet, dass das erste gesendete Wort eine Adresse ist (die eigene oder die des Empfängers). Tritt nun eine Kollision auf, so werden die Bits auf dem Übertragungsmedium so verfälscht, dass sich bei binärer Übertragung eine physikalische Eins (Pegel auf der Leitung) gegenüber einer physikalischen Null (kein Pegel) durchsetzt. Kann diese Verfälschung von der betroffenen Station vor dem Senden des nächsten Bits erkannt werden und gibt die Station das Senden sofort auf, so kann die andere Station ihre Nachricht ungestört weiter senden. Dieses Verfahren setzt voraus, dass eine unmittelbare Rückkopplung für die Stationen möglich ist, und die Signallaufzeiten so klein sind, dass vor dem Senden des nächsten Bits der Nachricht eine Kollisionserkennung möglich ist. Dieses Verfahren wird im ISDN für den Zugriff auf den Signalisierkanal (D-Kanal) des Basisanschlusses angewandt.



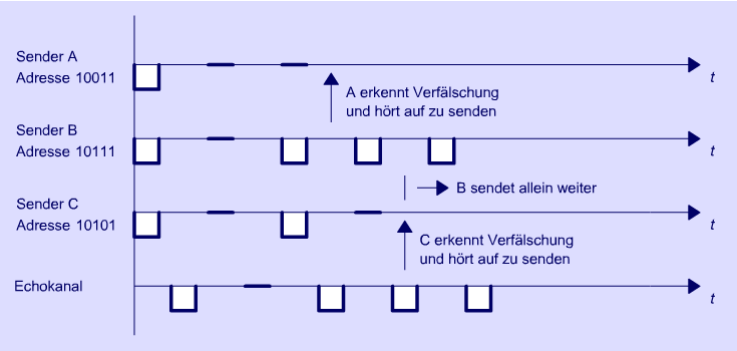
Animation 7.6-1: Kollisionsauflösung über Adressenpriorität

7.7 Summensignal im E-Kanal

Kollisionsauflösung beim Zugriff auf den D-Kanal

Drei Teilnehmer beginnen gleichzeitig auf dem D-Kanal zu senden. Sie haben jeweils eine physikalische Folge zu übertragen.

Animation 7.7-1 zeigt das Summensignal im E-Kanal und das Verhalten der Teilnehmer entsprechend dem D-Kanal-Zugangsprotokoll.



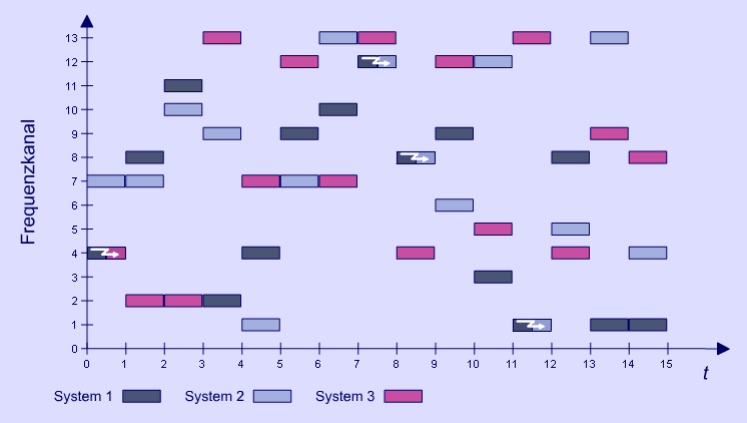
Animation 7.7-1: Summensignal im E-Kanal

7.8 Frequenzsprungverfahren

Die Funktionsweise des Frequency Hopping Spread Spectrum (FHSS) soll hier am Beispiel von IEEE 802.11 konkretisiert werden. Die Übertragung der Informationen geschieht durch Frequenzmodulation einer harmoschen Welle auf dem lizenzfreien 2,4 GHz-Band. Das Frequenzband ist in 79 Kanäle zu je 1 MHz unterteilt auf dem die Sender eine festgelegte Zeit auf einem Kanal senden und danach auf einen anderen Kanal wechseln.

Die Reihenfolge der Kanäle zu denen gewechselt wird, ist durch die dem Sender und Empfänger bekannte Hopping-Sequenz festgelegt. Nutzen mehrere Sender zur selben Zeit den selben Kanal kann es zu Kollisionen kommen, die mit dem CDMAVerfahren aufgelöst werden. Eine Erhöhung der Datenrate von 1Mbit/s auf 2Mbit/s ist möglich, jedoch muss dazu die Bandbreite der Kanäle erhöht werden. Beim Eintritt einer neuen Station in das Funknetz wird versucht ein Beacon-Frame zu empfangen, indem alle Kanäle nacheinander abgehört werden.

Animation 7.8-1 zeigt das Frequenzsprungverfahren exemplarisch anhand der voreingestellten Sendesystemen und einer zufälligen Hopping-Sequenz für jeden Sender. Die Kollisionen sind durch einen Blitz gekennzeichnet.

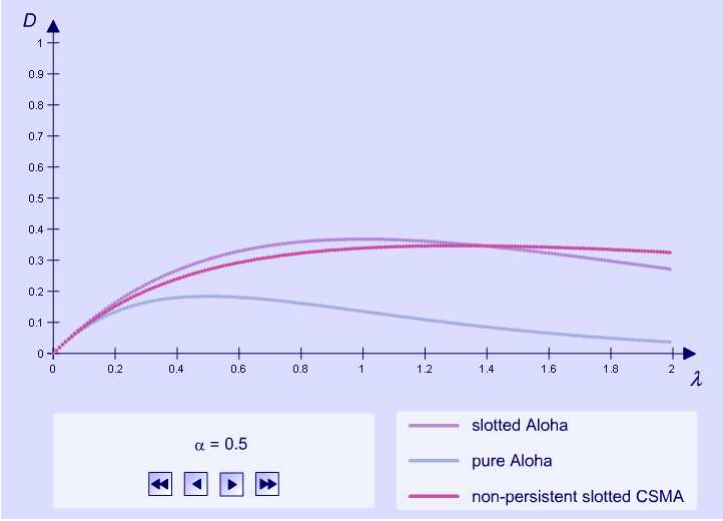


Animation 7.8-1: Frequenzsprungverfahren

7.9 Durchsatz verschiedener CSMA-Verfahren

Heute werden häufig Zugriffsverfahren implementiert, die voraussetzen, dass bevor eine Station auf das Übertragungsmedium zugreift, sie das Medium abhört, um festzustellen, ob es frei ist. Solche Verfahren werden als CSMA-Verfahren bezeichnet.

In Animation 7.9-1 sind die Durchsätze dreier Verfahren (Pure Aloha, Slotted Aloha und non-persistent slotted CSMA) im Vergleich für verschiedene Werte von α in Abhängigkeit von λ aufgezeichnet.



Animation 7.9-1: Durchsatz verschiedener CSMA-Verfahren

Index