

3. Mentorium

ISO/OSI-Referenzmodell & Netzwerke

- Erläutern Sie kurz an Hand eines Bildes den Aufbau des ISO-OSI-Stacks und seine Bedeutung
- Was ist unter dem Begriff „Kanalzuordnung“ zu verstehen?
- Erklären Sie das Aloha Prinzip und die Unterschiede zum CSMA Verfahren.
- In welcher Situation ist CSMA-CA dem CSMA-CD Verfahren vorzuziehen?

- Welche Schicht wird durch das IP-Protokoll unterstützt?
- Was ist eine IP-Adresse und wofür wird sie verwendet?
- Was ist der Unterschied zwischen TCP und UDP?
- Erklären Sie das 3-Wege-Handshake-Verfahren anhand eines selbstgewählten Beispiels.

- Welche Arten von Verschlüsselungsverfahren gibt es? Nennen Sie zu jedem Verfahren ein Anwendungsbeispiel.

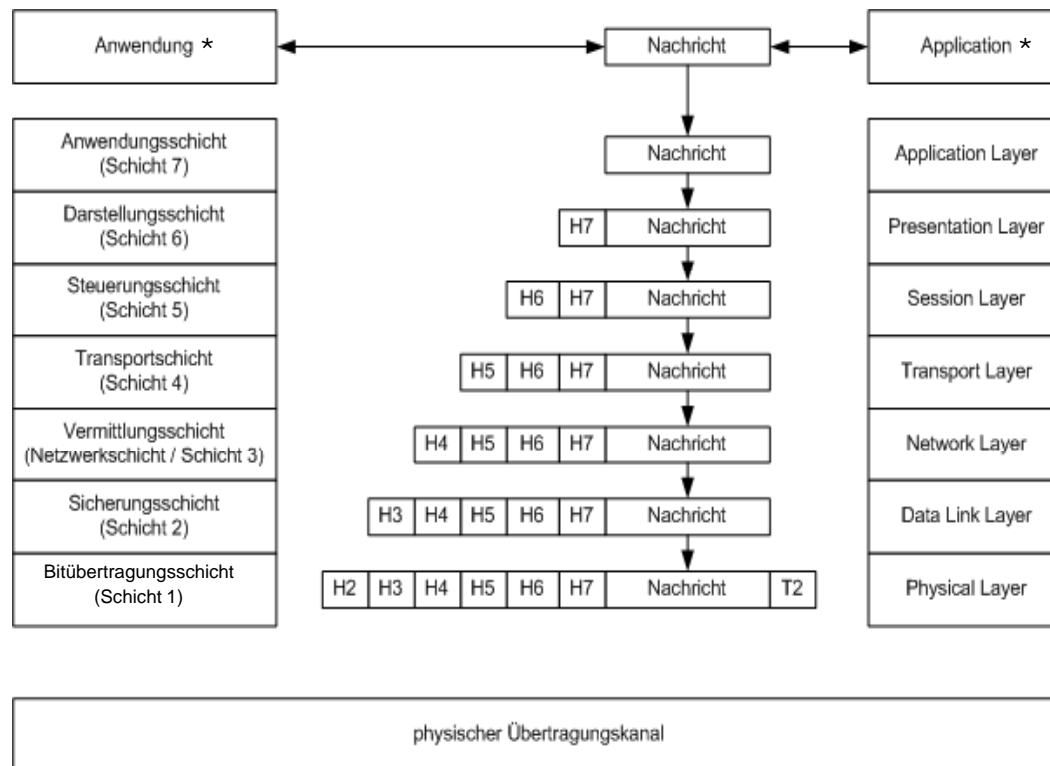
- Erläutern Sie kurz an Hand eines Bildes den Aufbau des ISO-OSI-Stacks und seine Bedeutung

Es handelt sich um **Lösungsvorschläge** und nicht um universal gültige Lösungen!

■ Bedeutung des ISO/OSI-Modells

- Das OSI-Modell wurde im Jahr 1984 als Referenzmodell für Netzwerkprotokolle entwickelt.
- Es ist eine abstrakte Darstellung der Kommunikation zwischen Systemen. Jede der sieben Schichten stellt über klar definierte Schnittstellen Dienste für die übergeordnete Schicht zur Verfügung. Die Definitionen der OSI-Schichten werden in Form von Protokollen (z.B. TCP) realisiert.
- Das OSI-Modell ist kein verbindlicher Standard, sondern ein Referenzmodell zur Darstellung logischer Zusammenhänge.
- Ein vergleichbares Modell ist das TCP/IP-Modell das in den 50er Jahren vom DoD (Department of Defense) entwickelt wurde.

- ISO/OSI-Stack kurz erläutert



Merksätze zur Schichtenabfolge:

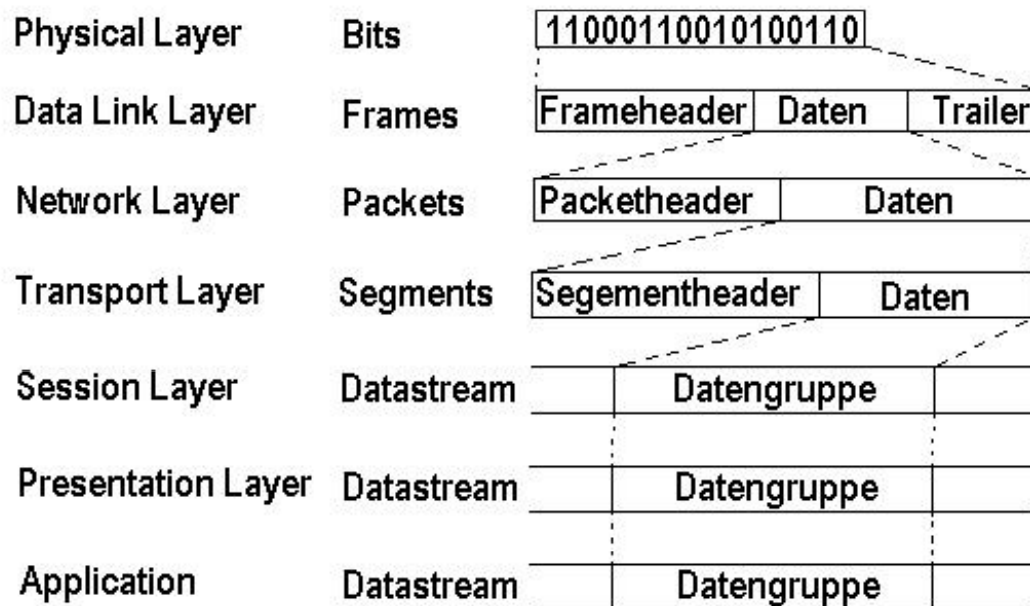
„Please Do Not Throw Salami Pizza Away“ (Physical Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, usw.)

Deutsche Variante:

„Alle deutschen Schüler trinken verschiedene Sorten Bier“ (Anwendungsschicht, Darstellungsschicht, ...).

* z.B. Browser

- ISO/OSI-Stack kurz erläutern, Bild erstellen, Datenpakete der einzelnen Schichten:



- Was ist unter dem Begriff „Kanalzuordnung“ zu verstehen?

- Die Kanalzuordnung oder Medienzugriffskontrolle ist eine Erweiterung der Sicherungsschicht des ISO/OSI-Modells durch IEEE. Zu diesem Zweck wird die Sicherungsschicht in zwei Unterschichten unterteilt:
 1. Logical Link Control (LLC) dient der Datensicherung auf Verbindungsebene
 2. Media Access Control (MAC) regelt den kontrollierten Medienzugriff
- Je nach konkreter Umsetzung der MAC findet der Zugriff auf das Medium *kontrolliert* oder *konkurrierend* statt.
- Kontrollierter Zugriff (engl. **C**ollision **A**voidance) bedeutet, dass der Zugriff auf das Medium so geregelt wird, dass keine Kollisionen auftreten können.
Beispiel Schulunterricht:
 - Viele Schüler möchten reden; wenn sie das gleichzeitig tun, versteht man aber nichts. Deshalb melden sich die Schüler, und der Lehrer bestimmt, wer reden darf. In diesem Fall wird die MAC durch einen zusätzlichen Kommunikationskanal umgesetzt, denn zusätzlich zum akustischen Datenübertragungsmedium Schall kommt hier das visuelle Synchronisationsmedium Licht. Ausgeklügelte Netzwerkprotokolle machen zusätzliche Kommunikationskanäle überflüssig.
- Konkurrierender Zugriff (engl. **C**ollision **R**esolution) bedeutet, dass jeder auf das Medium zugreifen darf und dass es Regeln gibt, wie Kollisionen ohne Komplikationen behandelt werden. Beispiel Telefonat:
 - Beginnen die Partner gleichzeitig zu sprechen, so hören sie sofort auf, jeder wartet eine zufällige Zeitspanne lang, und wer zuerst wieder zu reden beginnt, hat das Wort.

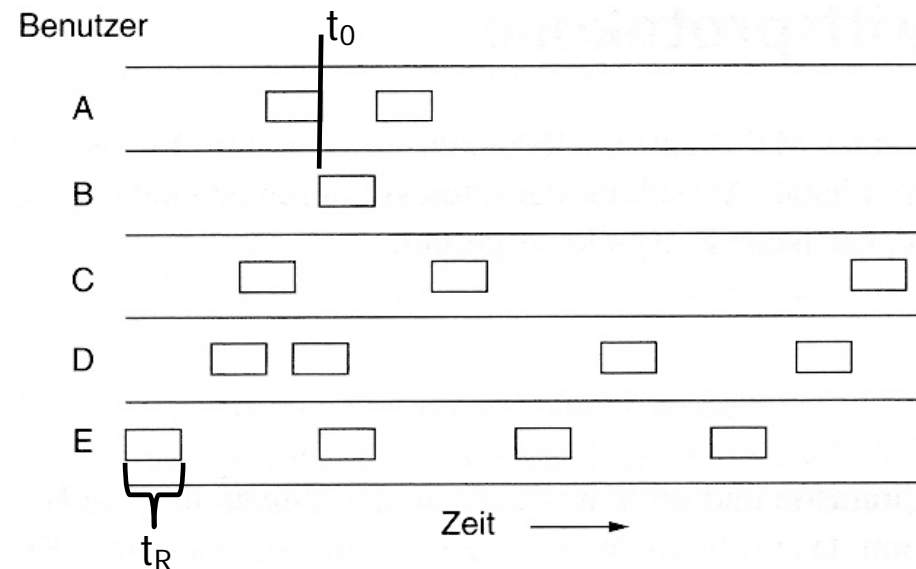
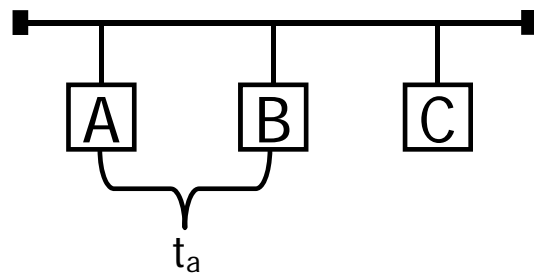
Quelle: Wikipedia

- Die MAC-Unterschicht beschäftigt sich also mit der von mehreren Parteien gleichzeitigen Verwendung eines Kommunikationskanals.
- Um das geschilderte Verhalten auch in lokalen Netzen zu ermöglichen, existieren verschiedene Verfahren zur Kollisionserkennung und –vermeidung die auf der MAC-Unterschicht Anwendung finden.
 - ALOHA
 - CSMA/CD
 - CSMA/CA

- Erklären Sie das Aloha Prinzip und die Unterschiede zum CSMA Verfahren.

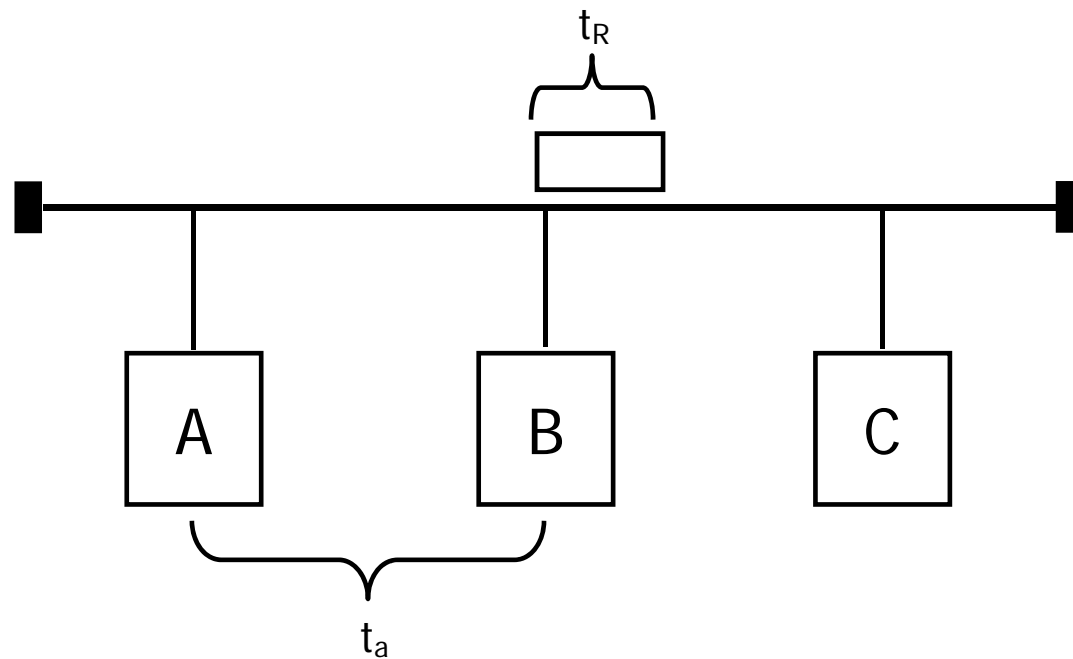
- Das einfachste und älteste Zugriffsverfahren für Busnetze, beruht darin, jede Station sofort bzw. zu Beginn einer Zeitscheibe 'ohne Rücksicht auf Verluste' senden zu lassen. Dieses Vorgehen ist als ALOHA-Protokoll bekannt und wurde ursprünglich 1971 für die Satelliten-Kommunikation im ALOHAnet entwickelt, welches die vielen Inseln um Hawaii mit der Universität von Honolulu verband. Es war ursprünglich als Satelliten-/Funknetz gedacht und bildete später die Grundlage für das Ethernet-Protokoll.
- ALOHA ist ein stochastisches Zugriffsverfahren in Netzen ohne Kanalabtastung, das in seinen unterschiedlichen Modifikationen (zeitunabhängiges also reines, pure ALOHA oder zeitabhängiges, unterteiltes, slotted ALOHA) nie Bedeutung im Umfeld der lokalen und regionalen Kommunikation erlangt hat.
- Die von ALOHA abgeleiteten CSMA-Verfahren verfügen zusätzlich über Kanalabtastung und sind daher wesentlich effizienter.

- Die Probleme mit dem ALOHA-Verfahren sollen an einem Beispiel erläutert werden. Drei Stationen seien an einen duplexfähigen Bus angeschlossen:



Sei t_R die Rahmenübertragungszeit und die t_a Signallaufzeit von Station A zu Station B.

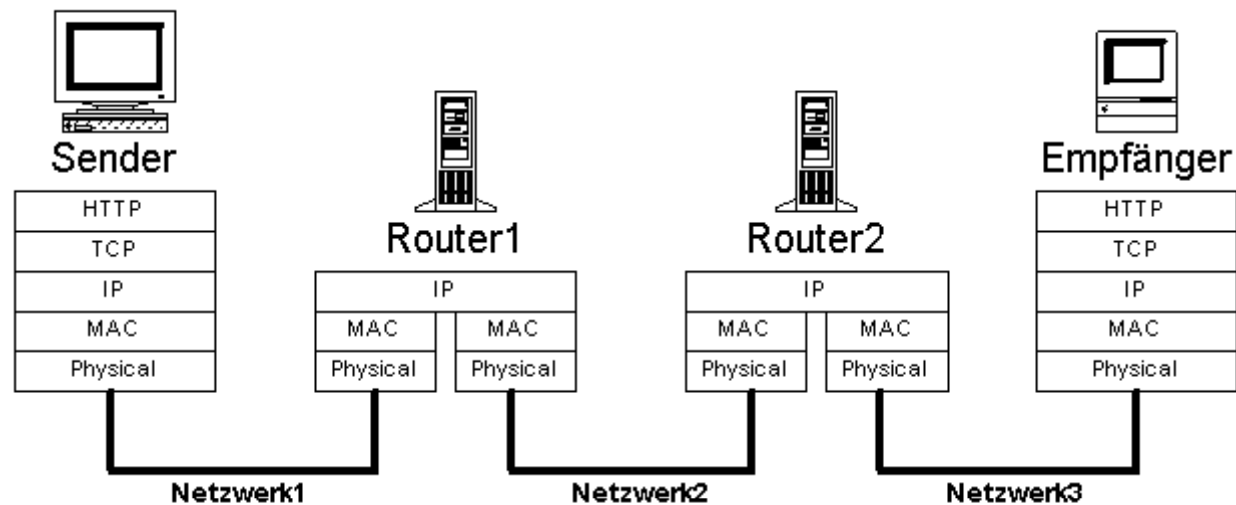
B beginnt zum Zeitpunkt t_0 eine Übertragung an Station C. Diese Übertragung kann nur dann erfolgreich durchgeführt werden, wenn nicht während des Zeitintervalls $[t_0 - t_R - t_a, t_0 + t_R - t_a]$ Station A ihrerseits mit der Übertragung eines Rahmens der Länge t_R beginnt



- In welcher Situation ist CSMA-CA dem CSMA-CD Verfahren vorzuziehen?

- Grundproblem: senden zwei oder mehr Stationen gleichzeitig, so kann der Inhalt für einen Empfänger nicht mehr gelesen werden, d.h. die Daten gehen verloren. Es existieren nun zwei prinzipielle Möglichkeiten, mit solchen Kollisionen umzugehen:
 1. Man versucht Kollisionen zu verhindern. Eventuell lassen sich Kollisionen zwar nicht ganz vermeiden, es wird jedoch versucht, die Wahrscheinlichkeit dafür zu reduzieren.
 2. Man verhindert Kollisionen nicht, integriert aber Mechanismen, um sie zu entdecken und später zu behandeln.
- Dieses Problem gilt sowohl für drahtgebundene Netze als auch für drahtlose Netze. IEEE 802.3 definiert hierzu für das kabelgebundene Ethernet das Verfahren CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Dieses kann Kollisionen zwar nicht vermeiden allerdings können Kollisionen erkannt werden, da das Medium ständig abgehört wird und die Stationen so feststellen können, ob ihre Rahmen unverändert übertragen werden. Liegen Kollisionen vor, führen sie die Transmission nach einer Wartezeit erneut durch.
- Die Kollisions-Entdeckung setzt allerdings voraus, dass eine Station gleichzeitig senden und empfangen kann. Diese Voraussetzung ist bei Funk-Netzen nicht gegeben. Hier kann die Funk-Hardware nur wechselweise zum Senden oder Empfangen genutzt werden. Für WLAN wird deshalb das alternative Verfahren CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) benutzt:
- Mit diesem Verfahren wird die Wahrscheinlichkeit für Kollisionen gering gehalten. Zusätzlich wird durch ein Quittierungsverfahren erreicht, dass im Falle von Kollisionen die Nutzdaten nicht unerkannt verloren gehen.

- Welche Schicht wird durch das IP-Protokoll unterstützt?



- Das IP-Protokoll bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokoll-Familie und ist aus Sicht des ISO/OSI-Referenzmodells ein Protokoll der Vermittlungsschicht.
- Es ermöglicht, dass mittels IP-Adresse und Subnetzmaske (subnet mask) für IPv4, bzw. Präfixlänge bei IPv6, Computer innerhalb eines Netzwerkes in logische Einheiten, so genannte Subnetze, gruppiert werden können.
- Es sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Die Übertragung der Daten führt in beiden Fällen jeweils über das gesamte Kommunikationsnetz und schließt die Wegesuche (Routing) zwischen den Netzknoten mit ein.
- Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden können. Dabei gelangen weitervermittelte Pakete in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.
- Um dies zu ermöglichen gehört der Aufbau und die Aktualisierung von Routingtabellen und die Fragmentierung von Datenpaketen zu den wichtigsten Aufgaben der Vermittlungsschicht und damit des IP-Protokolls.
- Hardware auf dieser Schicht: Router, Layer-3-Switch (BRouter)

- Was ist eine IP-Adresse und wofür wird sie verwendet?

- Die IP-Adresse ist die eindeutige logische Adresse eines Computersystems und dient der Identifikation innerhalb eines Netzwerkes. Sie ist nicht an Hardware oder Software gebunden und kann individuell unter Beachtung von bestimmten Regeln vergeben werden. Eine IP-Adresse darf in einem Netzwerk nur einmal vorkommt.

- IP Adressen besteht aus 4 Oktetten (Byte)
- 2 Teilen: Dem Netzanteil und dem Hostanteil

- Interne IP-Adressen?
- Diese Bereiche erlauben ein internes Netzwerk, ohne dass diese Hosts von außen erreichbar sind.
- 10.x.x.x = Klasse A Adressen
- 172.16.x.x bis 172.31.x.x = Klasse B Adressen
- 192.168.x.x = Klasse C Adressen

- Was ist der Unterschied zwischen TCP und UDP?

- TCP (Transport Control Protocol) ist ein zuverlässiges, verbindungsorientiertes, paketvermittelndes Transportprotokoll. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.
- Im Unterschied zum verbindungslosen UDP (User Datagram Protocol) stellt TCP einen virtuellen Kanal zwischen zwei Endpunkten einer Netzverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP (Internet-Protokoll) auf. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt.

- Erklären Sie das 3-Wege-Handshake-Verfahren anhand eines selbstgewählten Beispiels.

- Beim Transport von Nachrichten benötigen die teilnehmenden Instanzen eine Möglichkeit sicherzustellen, dass die von ihnen kontaktierte Instanz die Nachricht erhalten hat.
- In der Kommunikation tritt dieses Problem immer dann auf, wenn zwischen den Kommunikationspartnern ein unsicherer Übertragungskanal vorliegt.
- Man wählt daher ein dreistufiges Verfahren zum Verbindungsaufbau, den so genannten Drei-Wege-Handshake.
- Beispiel Terminvereinbarung per E-Mail:
 - Möchte Anton sich mit Berta verabreden, werden folgende Nachrichten ausgetauscht:
 - Anton schickt Berta einen Terminvorschlag
 - Berta schickt Anton eine Bestätigung des Termins
 - Anton schickt Berta eine Bestätigung, dass er Bertas Bestätigung erhalten hat
- Schritt 3 ist dabei notwendig, damit Berta weiß, ob Anton die Bestätigung erhalten hat. Nachricht Nummer 2 könnte ja verloren gegangen sein und Berta würde alleine zu dem Treffen erscheinen, da Anton keine Bestätigung erhalten hat.

- Welche Arten von Verschlüsselungsverfahren gibt es? Nennen Sie zu jedem Verfahren ein Anwendungsbeispiel.

- Prinzipiell unterscheidet man zwischen symmetrischen Kryptosysteme und den erst seit wenigen Jahrzehnten bekannten asymmetrischen Krypto-systeme.
- Bei symmetrischen Verfahren werden Ver- und Entschlüsselung mit demselben Schlüssel durchgeführt. Das heißt, Sender und Empfänger müssen vorab diesen geheimen Schlüssel vereinbart haben ihn geheim halten.
- Bei asymmetrischen Methoden hingegen werden zur Ver- und Entschlüsselung nicht derselbe Schlüssel verwendet, sondern es gibt einen öffentlichen Schlüssel (engl.: public key, weshalb asymmetrische Kryptosysteme auch Public-Key-Systeme genannt werden) zur Verschlüsselung sowie einen privaten Schlüssel zur Entschlüsselung.
- Hierdurch ist es möglich jemandem, dessen öffentlichen Schlüssel man kennt, eine geheime Botschaft zu übermitteln. Die nur dieser mithilfe seines privaten Schlüssels wieder entschlüsseln kann. Selbst der Sender ist nicht in der Lage, seine eigene Botschaft wieder zu entschlüsseln.
- In der Praxis sind symmetrische Kryptosysteme leistungsfähiger und deutlich schneller als asymmetrische. Deshalb verwendet man häufig kombinierte Methoden, auch Hybridverschlüsselung genannt, die die Vorteile der asymmetrischen Verfahren, wie öffentliche Schlüssel, mit der Schnelligkeit der symmetrischen Verfahren vereinigen.
- Mehr zur Kryptographieunter: <http://www.cryptool.de/>