Prüfungsfragen

1. Vorlesung, 07.03.2024

Fragen:

- Was sind die 3 Voraussetzungen für ein Shared Medium?
  - Zugriffsverfahren aufs Medium
  - Eindeutiges Adressierungsschema
  - Selbstbeschränkung
- Was ist der Unterschied zwischen Unicast/Multicast/Broadcast?
  - Unicast
    - Nachricht an einen
  - Multicast
    - Nachricht an mehrere
  - Broadcast
    - Nachricht an alle
- Welche Komponenten gibt es in Netzwerken?
  - Kanten/Pfade
  - Knoten
    - Quellen: erzeugt daten
    - Senken: nimmt daten auf und verarbeitet sie
    - Forwarding (Hub, Switch, Router)
- Wozu wird IPv6 benötigt?
  - Um weiterhin global IP-Adressen verteilen zu können / um der Knappheit von IPv4-Adressen Herr zu werden.
- Was umfasst die OSI-Schicht 1 (Physical Layer)?
  - Das Übertragungsmedium / die Hardware (zb. Spannungspegel)

- Welche Sicherheitsrisiken ergeben sich durch IoT-Geräte im Haus?
    - Ungewollte Fernsteuerung des IoT-Geräts von außen
    - Auslesen von sensiblen Daten von außen (Wann ist jemand zuhause, Netzwerktraffic, Kamerabilder…)
    - IoT-Gerät wird Teil eines Botnets (Störerhaftung?)
- Wie funktioniert Adressierung in Layer 2 und in Layer 3?
    - Adressieren von Knoten (nicht Nachrichten)
    - Layer 2: MAC-Adresse
    - Layer 3: IP-Adressen
    - (auch damit rechnen können)

2. Vorlesung, 14.03.2024

Fragen:

- Wie funktioniert Dezibelrechnung?
    - dB ist ein Verhältnis zwischen zwei Größen
    - L = 20 * log_10(Verhältnis) dB
    - Schall: dBa
    - dBm: Referenzgröße ist 1 mW
    - dB kann Rechnungen vereinfachen, z.B.: Quelle schickt Signal, wird mehrfach gedämpft um unterschiedliche Faktoren, Dämpfungen müssen multipliziert werden. Wenn man die Dämpfung in dB hat kann man diese einfach addieren
    - Bei LWL wichtig, es gibt ein Dämpfungsbudget, üblich 7 dB
- Was sind die Anwendungsgebiete von PoE (Power over Ethernet)?
    - Netzwerkgeräte, durch PoE spart man sich ein separates Netzteil für das Gerät (Bspw. Kameras, Telefone, WLAN-Accesspoints, IoT-Geräte)

    - Verschiedene Leistungsklassen zwischen 15W und 90W Ausgangsleistung
- Was ist der Kuhzungeneffekt?
    - Kontakte sind mit Gold beschichtet (reagiert nicht mit Sauerstoff, allerdings teuer und weich). Dadurch nutzt sich die Beschichtung leicht ab, die Anzahl der Steckzyklen ist begrenzt.
- Was ist das Dämpfungsbudget von verschiedenen Lichtwellenleitern?
    - 7 dB zwischen Sender und Empfänger
    - in Multimode kommt man 300-500 m
- Was ist ein isotroper Kugelstrahler?
    - Eine Antenne, die von einem Punkt aus in alle Richtungen gleichmäßig sendet (was nicht erwünscht ist). In der Realität nur annähernd gut umsetzbar, aber relevant als Referenzmodell.
    - Anderer Antennentyp: Richtantenne
- Wie entsteht ein Standard?
    - Interessengruppen/ VertreterInnen diskutieren und einigen sich auf etwas (was nicht zwingend gut sein muss)

3. Vorlesung, 21.03.2024

Fragen:

- Wofür verwendet man Twisted-Pair-Leitungen?
    - Um Störungen in Telefonie-/Datenleitungen einzudämmen.
    - Paare sind verdrillt (Twisted Pair) damit die Wirkung auf andere Leiter schwächer ist (weniger Übersprechen). Würde nichts bringen, wenn zwei

Paare gleich verdrillt sind, daher werden sie unterschiedlich verdrillt (können auch jeweils geshielded sein).
    - Weil man ein Echo vom eigenen Signal zurückbekommt, wird dieses durch einen Filter herausgenommen.
    - Um Wärme besser abzuleiten, werden dickere Leitungen verwendet (kann dann nicht mehr für PoE verwendet werden).
    - **UTP =** Unshielded Twisted Pair
      STP = Shielded Twisted Pair
    - wird verwendet in tertiären Netzwerken (vom Stockwerksverteiler zu Endgeräten) (primär und sekundär benutzt glasfaser)
- Welche Arten von Crosstalk gibt es?
    - Crosstalk = Übersprechen. Wenn ein Signal in einem Schaltkreis oder Kanal ungewünschte Nebeneffekte bei anderen Schaltkreisen / Signalen auslöst.
    - Drei Arten von Crosstalk:
        - Near End Crosstalk
        - Far End Crosstalk
        - Alien Crosstalk
- Was ist der Unterschied bei der Angabe der Qualität von Komponenten/der ganzen Strecke?
    - Qualität von Komponenten (Kategorie) ist quasi nicht messbar, weil bei einem Kabel immer die Stecker auch einen Einfluss haben.
    - Qualität der Strecke durch Messung der gesamten Verbindung.
        - pass: Messung liegt auf jeden Fall über dem Grenzwert (auch mit Toleranz).
        - pass*: Messung könnte über oder unter dem Grenzwert liegen (nicht sicher wegen Toleranz).

    - Subfrage: Unterschied Klasse/Kategorie
        - Permanent Link (ohne Patchkabel) vs. Channel (inkl. Patchkabel)
        - Kategorie bezieht sich auf die einzelnen Komponenten
        - Klasse bezieht sich auf die gesamte Strecke
- Wie stehen Wellenlänge/Frequenz/Lichtgeschwindigkeit im Verhältnis zueinander?
    - Licht kann verlangsamt werden
    - $f = \frac{c}{\lambda}$, wobei f die Frequenz, λ die Wellenlänge und c die Lichtgeschwindigkeit ist

4. Vorlesung, 18.04.2024

Vortrag: Switches und STP
Vortrag 2: VLANs, Trunking, Link Aggregation

Fragen:

- Was ist der Unterschied zwischen Broadcast- und Collision Domain?
    - switch beschränkt collision domain ohne broadcast domain zu beschränken
    - Die Collision Domain besteht aus den Geräten, bei denen bei gleichzeitigem Schreiben auf das shared Medium Kollisionen entstehen können
    - Die Broadcast Domain besteht aus den Geräten, die sich untereinander bei einem Broadcast “hören” können
- Wie kann ein Switch intern aufgebaut sein?
    - (Stern vs. Mesh), CPU, Input und Output Queues, Tabellen

- In welche beiden Sublayer wird Layer 2 aufgeteilt?
    - Logical Link Control (LLC)
        - Ermöglicht es, mehrere Layer 3 Protokolle nebeneinander zu verwenden.
    - Media Access Control (MAC)
        - Teilt Nachrichten in Frames auf, fügt Header/Trailer hinzu, macht Error Detection/Correction.
- Was ist der Unterschied zwischen portbasierten und tagged VLANs?
    - Portbasiertes VLAN:
      Jedem Port eines Switches wird genau ein VLAN zugewiesen. Wenn der Switch eine Nachricht an einem Port bekommt, wird diese dem VLAN zugeordnet, das auf dem Port konfiguriert ist.
    - Tagged VLAN:
      Dem Ethernet-Frame wird ein Tag-Feld hinzugefügt. Dieses enthält die VLAN-ID, wodurch der Frame einem VLAN zugeordnet werden kann.
- Was ist ein Accessport, Trunkport, Trunk-Link?
    - Accessport:
      Ein Port eines Switches, dem genau ein VLAN zugewiesen ist, wie bei portbasiertem VLAN.
    - Trunkport:
      Ein Port eines Switches, über den Nachrichten aus unterschiedlichen VLANs geschickt werden. Die Nachrichten werden dazu getagged, wie bei tagged VLAN.
    - Trunk-Link:
      Eine Verbindung zwischen zwei Switches, auf der die Nachrichten unterschiedlicher VLANs, mit Hilfe von Tagging, zusammengefasst werden.
- Wo benutzt man Link Aggregation?

    - Lineare Erhöhung der Datenrate zwischen 2 Netzwerkgeräten (anstatt in 10er Potenz durch nächste Ethernet Generation)
    - Erhöhung der Redundanz einer Verbindung/Link (Redundanz nur von Interface zu Interface, Geräte bleiben Single-Points-Of-Failures)

5. Vorlesung, 25.04.2024

Vortrag: 802.1x
Vortrag 2: IPv4/IPv6

Fragen:

- Wie funktioniert IPv4-Netzberechnung?
    - Netzwerk und Broadcastadresse aus IP-Adresse und Subnetzmaske berechnen
    - Nimm irgendeine IP-Adresse und überlege dir, wie du das Netz Teilen kannst (Subnetting) oder mehrere “benachbarte” Netze die du zusammenfügen willst (Supernetting)
    - Berechne für alle Netze (Kontrolle)
        - Adresse des Netzes (Hostteil ist 0)
        - Broadcast adresse (Hostteil ist 1)
        - 1. / letzte Hostadresse
        - Anzahl der Hostadressen

IP-Adresse:	172.0.0.1	IP-Adresse:	172.0.0.1
Subnetzmaske:	$\wedge$ 255.0.0.0	$\neg$ Subnetzmaske:	$\vee$ 0.255.255.255
Adresse des Netzes:	172.0.0.0	**Broadcast-Adresse:**	127.255.255.255

Abbildung 1: Beispiel zur Berechnung der Adresse des Netzes und Broadcast-Adresse

- Was ist MAC-Table-Flooding?

    - eine Attacke wobei Einträge aus MAC-Tables herausgedrängt werden
- Was sind die 3 Komponenten von IEEE 802.1X?
    - Supplicant (Antragsteller):
      Fordert Zugriff auf das Netzwerk und startet damit den Authentifizierungsprozess.
    - Authenticator (Unterhändler):
      Leitet die Identität des Antragstellers an den Authentication-Server weiter und die jeweilige Antwort wieder zurück.
    - Authentication-Server:
      Verwaltet die Datenbank mit gültigen Anmeldedaten.
- Warum reichen MAC-Adressen nicht bzw. warum werden IP-Adressen benötigt?
    - Lokalisierung =› Es kann geroutet werden aufgrund der hierarchischen strukturierung in Netze und Subnetze
    - auch damit alle Adressen eindeutig sind
- Was ist der Unterschied zwischen Primary Role und Management Role eines Switches (oder auch anderen Geräten)?
    - Switches haben eine Primary Role (Pakete weiterleiten) und eine Management Role (Konfiguration kann geändert oder abgefragt werden). Wenn er voll ausgelastet ist, muss er entscheiden, wie er seine Ressourcen für das Bearbeiten dieser beiden Rollen verteilt.
- Welche Vorteile hat IPv6 gegenüber IPv4?
    - Security (IPSec inkludiert), QoS, mehr Adressen
    - man braucht keine Address Translation
    - DHCP wird nicht benötigt

6. Vorlesung, 02.05.2024

Vortrag: ARP, DNS, ARP___DNS.pdf

Fragen:

- Nennen Sie 3 DNS-Record Typen.
  - A-Record: Datenfeld ist IPv4-Adresse, Größe 4 Byte
  - AAAA-Record: Datenfeld ist IPv6-Adresse, Größe 16 Byte
  - MX-Record: bezieht sich auf Mail Exchange, definiert einen oder mehrere E-Mail-Server, die zur entsprechenden Domain gehören.
  - TXT-Record: enthält unstrukturierten Text, etwa Details über das Unternehmen, das hinter der Domain steht.
  - C-Name: Alias auf andere Domain
  - Ptr: Pointer für reverse DNS (?)
- Für was steht DNS? Was tut es? Wofür braucht man es?
  - Domain Name System. Es ist ein System, welches menschenlesbare Namen für Webseiten (zb example.com) auf IP-Adressen auflöst (93.184.215.14).
- Für was steht Reverse-DNS? Was tut es? Wofür braucht man es?
  - Bei Reverse DNS Lookup soll zu einer IP-Adresse der Name gefunden werden. Wird häufig von E-Mail-Servern verwendet, um zu überprüfen, ob eine Nachricht von einem gültigen Server stammt, bevor diese in das Netzwerk eingespeist wird.
- Wofür braucht man ARP?
  - ARP = Address resolution protocol

    - OSI Layer 3 Adressen (IPv4) zu OSI Layer 2 Adressen (MAC) aufzulösen. Da im Subnetz über die MAC Adresse kommuniziert wird.
- Was ist ARP Spoofing?
    - “Man in the Middle attack” in LAN (auf MAC Ebene)
    - Abhilfe: Nur vertraute Teilnehmen in eigenen LAN (eigenes Gäste Netzwerk)
    - A: Durch gezielte ARP Replies den ARP-Cache von anderen Teilnehmern im Netz so zu verändern, dass eine IP-Adresse einer falschen MAC-Adresse zugeordnet ist.
- Was ist das Gegenstück zu ARP in IPv6?
    - Neighbor Discovery Protocol (NDP)

7. Vorlesung, 16.05.2024

Vortrag: Routing

Fragen:

- Wofür werden Routing-Metriken verwendet?
    - Um eine optimale route zu ermitteln
    - ttl = time to live -> um endlosschleifen zu verhindern
- Welche Arten von Routing gibt es?
    - statisch: Es sind bereits alle Routing-Tables vorgegeben. Jeder Router weiß genau, welches Netz er über welches Interface erreichen kann.
    - dynamisch: Die Routing-Tables werden im Router zur Laufzeit erstellt. Hierfür muss es einen Austausch zwischen den Routern geben, mit verschiedenen Protokollen. (Unterteilung in Distance Vector und Link State)

- Was versteht man unter Hop-Count?
    - Der Hop-Count beschreibt, über wie viele Knoten ein bestimmter Netzwerkteilnehmer erreichbar ist. Dieser wird gerne als Metrik für Routing-Algorithmen verwendet.
- Wo werden Pfade und deren Eigenschaften innerhalb eines Routers gespeichert?
    - In Routingtabellen
    - Sollte in non-volatile memory gespeichert werden.
- Was sind die Vor- und Nachteile von hierarchischem Routing?
    - Vermindert durch den hierarchischen Aufbau den Datenverkehr im Netz und steigert die Effizienz.
    - Bessere Kontrolle über den Datenverkehr.
    - Verringert unnötige Routingupdates und Schleifen im Netz.
    - Netzwerk ist sehr gut skalierbar.
    - Einfach zu warten und zu organisieren.
    - Fehlersuche wird durch die Unterteilung in Teilnetze einfacher.
    - Nachteil: keine Redundanzen (weil baum-Struktur)
- Was sind autonome Systeme?
    - Ein Autonomes System beschreibt einen Verbund von Routern, die eine gemeinsame Routing-Policy haben. Hierfür gibt es interne (Interior Gateway Protocol, zB. RIP), und externe (Exterior Gateway Protocol, zB. BGP) Protokolle, um innerhalb sowie zwischen verschiedenen AS (z.B. ISP) zu Routen.
    - => Aufeinander abgestimmt konfiguriert

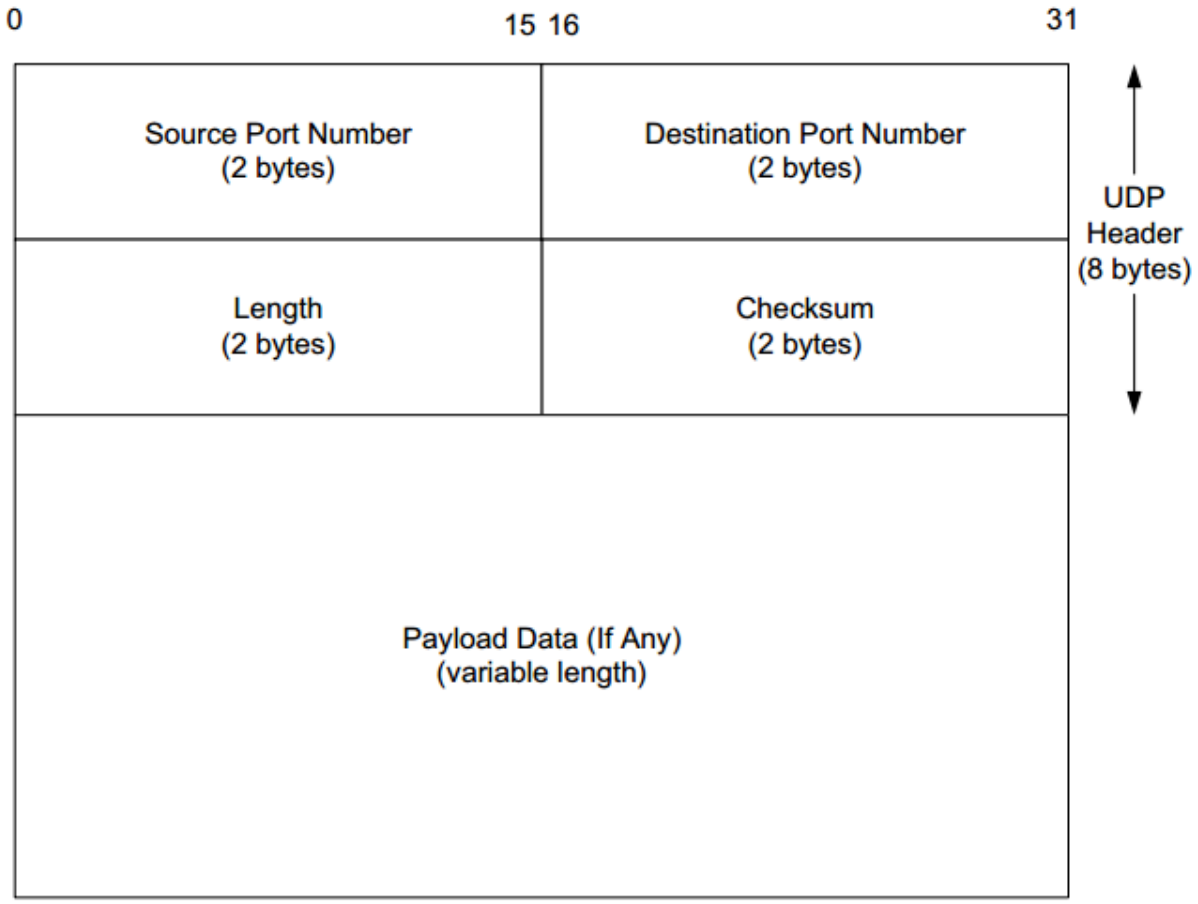
8. Vorlesung, 23.05.2024

Vortrag: DHCP DHCP Paper.pdf
Vortrag 2: TCP, UDP

Fragen:

- Wozu wird DHCP verwendet?
    - Das Dynamic Host Configuration Protocol (DHCP) ist ein Client-Server-Protokoll, das die Vergabe von IP-Adressen und die Konfiguration von Netzwerkparametern bei Clients automatisiert.
    - laufende dynamische(= veränderliche) Einstellung
- Wie ist der Kommunikationsablauf bei DHCP?
    - Der Ablauf der IP-Adressvergabe erfolgt über vier Broadcast-Nachrichten:
    - Der Client sendet zunächst eine DHCPDISCOVER-Nachricht, um bekanntzugeben, dass er eine neue IP-Adresse benötigt.
    - Alle zuständigen DHCP-Server antworten mit einer DHCPOFFER-Nachricht, mit welcher sie dem Client eine freie IP-Adresse und ggf weitere Netzwerkparameter anbieten.
    - Der Client sucht sich aus den erhaltenen Offers eines aus, und sendet eine DHCPREQUEST-Nachricht, in welcher er bekanntgibt, für welche der angebotenen IP-Adressen er sich entschieden hat.
    - Der Server, von dem dieses Angebot gekommen ist, antwortet mit einer DHCPACKNOWLEDGE-Nachricht, mit welcher die Vergabe bestätigt wird.
- Wofür wird bei DHCP die Lease Time verwendet?

    - Die Lease Time kann bei der IP-Adressvergabe verwendet werden, um die Adressen nur für eine bestimmte Zeit zu vergeben. Nach Ablauf dieser Zeit gilt die IP-Adresse automatisch wieder als verfügbar, ein Client, der sie weiterhin nutzen will, muss beim DHCP-Server rechtzeitig um eine Lease-Verlängerung ansuchen.
- Was ist ein Relay Agent?
    - Ein DHCP-Relay-Agent leitet DHCP-Nachrichten von dem Quellnetzwerk (in dem der Client ist) in das Netzwerk, in welchem der DHCP-Server verbunden ist, weiter. Relay-Agents können auf Managed Switches oder Routern implementiert werden. Vorteil: Nur ein DHCP-Server pro Organisation nötig; weniger Wartungsaufwand.
- Was ist der wesentliche Unterschied zwischen TCP und UDP?
    - TCP = Transmission Control Protocol
    - UDP = User Datagram Protocol
    - Verwendung von UDP bei hoher Übertragungsgeschwindigkeit und geringer Latenz (z.B.: Videostreaming), Verwendung von TCP wenn Datenintegrität, vollständige und fehlerfreie Zustellung notwendig ist (z.B.: E-Mail, Dateiübertragung) (wie in einen Wald hinein rufen)
    - TCP ist verbindungsorientiert (stabile Verbindung zwischen Kommunikationsteilnehmer wird zu Beginn aufgebaut = 3-way-handshaking, TCP ist zuverlässig (verlorene Datensegmente werden erkannt und können erneut gesendet werden, falsche Reihenfolge der Datensegmente wird korrigiert),
- Wie ist der Aufbau von einem UDP Datagram?



9. Vorlesung, 06.06.2024

Vortrag: Streaming
Vortrag 2: TLS

Fragen:

- Erklären Sie die Funktionsweise von HLS und DASH.
  - HLS = HTTP Live Streaming
  - DASH = Dynamic Adaptive Streaming over HTTP
  - Bei HLS und DASH wird Inhalt in eine Reihe von kleinen HTTP-basierten Dateisegmenten (meist 6-10 Sekunden lang) aufgeteilt. Diese Segmente werden kontinuierlich heruntergeladen und in einem Puffer

gespeichert. Beide unterstützen Adaptive Bitrate Streaming durch folgende Manifest-Files:
    - HLS: Eine zentrale M3U8-Datei listet die verfügbaren Segmentdateien auf und gibt an, wie der Player die Segmente abspielen soll.
    - DASH: Eine MPD-Datei (Media Presentation Description) gibt eine Übersicht über die verfügbaren Segmente und die verschiedenen Qualitätsstufen.
- Wird beim Streaming TCP oder UDP bevorzugt?
    - **TCP** wird bevorzugt für On-Demand-Streaming und Streaming über Webbrowser (z.B. HLS, DASH), wo Zuverlässigkeit und Datenintegrität wichtig sind.
    - **UDP** wird bevorzugt für Live-Streaming und Echtzeitanwendungen, bei denen niedrige Latenz und Geschwindigkeit entscheidend sind (z.B. RTMP, RTP).
    - TCP ist verbindungsorientiert, das heißt, es stellt sicher, dass alle Datenpakete in der richtigen Reihenfolge und ohne Verlust übertragen werden. Es bietet Fehlerkorrektur und Datenflusskpontrolle.
    - UDP ist verbindungslos und bietet keine Garantie für die Zustellung der Datenpakete. Es ist jedoch schneller und effizienter, da es weniger Overhead durch Fehlerkorrektur und Datenflusskontrolle hat.
- Wie kommt es dazu, dass man SSL sagt, aber TLS meint?
    - Initial wurde SSL (Secure Sockets Layer) von der Firma Netscape für ihren Webbrowser (Netscape Navigator) entwickelt. Später wurde SSL von mehreren Akteuren / der IETF weiterentwickelt und war seither kein reines Netscape-Produkt mehr und wurde deshalb in TLS (Transport Layer Security) umbenannt.

- Bleibt etwas Verschlüsseltes für immer geheim?
    - etwas Verschlüsseltes bleibt so lange geheim, bis die Verschlüsselung geknackt (z.B. der Key erraten) werden kann. Somit eine Frage der Zeit.
    - Prozessorleistung wird höher mit der Zeit => Brute force zeit wird kürzer
- Was ist der Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren?
    - **Symmetrisch:** Partei A und B ver- und entschlüsseln Nachrichten mit genau einem Key, den beide Parteien besitzen
    - **Asymmetrisch:** Partei A verschlüsselt mit Public Key B, B entschlüsselt mit Private Key B. Umgekehrt verschlüsselt Partei B mit Public Key von A, A kann diese Nachricht mit ihrem Private Key A entschlüsseln.
      Generell gibt es bei asymm. Verschlüsselung pro partei ein Schlüsselpaar (Public Key und Private Key). Eine Nachricht welche mit dem einen Schlüssel des Paares verschlüsselt wurde, kann nur mit dem anderen Schlüssel des Paares entschlüsselt werden.
- Was ist Jitter und wie geht man damit um?
    - **Jitter** bezieht sich auf die Variation in der Zeit zwischen der Ankunft von Datenpaketen in einem Netzwerk. In einem idealen Szenario sollten Pakete in regelmäßigen Abständen ankommen, aber in der Praxis können Verzögerungen auftreten, die zu unregelmäßigen Ankünften führen.
    - Umgang mit Jitter:
        - **Jitter-Puffer**: Ein Jitter-Puffer sammelt eingehende Pakete und gibt sie in regelmäßigen Abständen weiter, um die Schwankungen auszugleichen. Dies kann die wahrgenommene

Qualität der Übertragung verbessern, führt jedoch zu einer leicht erhöhten Verzögerung.
    - **Netzwerkoptimierung**: Durch die Optimierung der Netzwerkinfrastruktur, wie z.B. die Priorisierung von Echtzeitdatenverkehr und die Vermeidung von Überlastungen, kann Jitter reduziert werden.
    - **Quality of Service (QoS)**: QoS-Einstellungen in Netzwerken können dazu verwendet werden, bestimmten Datenverkehr zu priorisieren, um sicherzustellen, dass Echtzeitanwendungen die benötigte Bandbreite und geringe Latenz erhalten.
    - **Bandbreitenerhöhung**: Eine Erhöhung der verfügbaren Bandbreite kann helfen, die Belastung des Netzwerks zu reduzieren und dadurch Jitter zu minimieren.
    - **Redundanz und Pfadoptimierung**: Durch die Implementierung redundanter Netzwerkpfade und die Optimierung der Routing-Strategien können die Auswirkungen von Jitter gemindert werden.
- **Ursache**: Jitter wird durch Schwankungen in der Netzwerklast, Router- und Switch-Überlastungen, variable Latenzzeiten in Netzwerken und die unterschiedliche Verarbeitungsgeschwindigkeit der Pakete verursacht.