**Uke 36 – Datamaskinens historie**

**Kuleramma (Abacus):** Oppfunnet ca. 2500 f.Kr. i Mesopotamia, brukt til addisjon og subtraksjon av store tall

**Herman Holleriths maskin:** Brukte hullkort for å registrere folk. Bidro til oppstarten av Tabulating Machine Company som senere ble IBM

**Harvard Mark I (1944):** Datamaskin basert på mekaniske rele. Produsert av IBM. Kunne gjennomføre 3 addisjoner/subtraksjoner per sek.

**Bug:** Innsekt som skapte problemer for kjøring av datamaskiner, sitat fra Grace Hopper

**Vakuumrør:** Erstattet mekaniske rele i datamaskiner. Forbedringer: Mindre slitasje, ingen bevegelige deler, kunne sås av/på flere 1000 ganger i sekundet, mye raskere enn rele

**ENIAC – Electronic Numerical Integrator and Computer (1946):** Første generelle programmerbare elektroniske datamaskin. Brukte radiorør. Utførte 500 operasjoner per sekund

**Transistoren:** Oppfunnet i 1947. Samme prinsippet som rele og radiorør

**Uke 37 – Binær representasjon: Introduksjon og tall**

**Addisjon av binærtall:** Still opp tallene over hverandre som vanlig addisjon.

-0 + 0 = 0  
-0 + 1 = 1  
-1 + 1 = 10  
-1 + 1 + 1= 11

**Bits og bytes:** 8-bits = 1 byte (256 ulike verdier).

**16-bits datamaskiner:** Opererer med 2 bytes, minne har 2 bytes med adresser

**Representasjon av positive og negative binærtall:**

-Kan representere første bit som fortegn (1 negativ og 0 positiv)

-2-komplement

**Flyttall:**

-1 bit til fortegn  
-8 bit til eksponent  
-23 bit til signiifikanten

Text

Description automatically generated

**Uke 38 – Binær representasjon: Bokstaver, lyd og bilde**

**ASCII (1963):** American Code for Information and Interchange. Brukte 7-bit kode: støtte for 128 forskjellige tegn. Kun bokstaver i det engelske alfabetet.

**Extended ASCII (1978):** Brukte 8-bit kode: støtte for 256 forskjellige tegn. Støtte for bokstaver fra andre språk enn engelsk.

**UNICODE (1992):** Standard, større for alle bokstaver i alle språk inkludert asiatiske språk. Mest brukte versjonen bruker 16-bit. Brukes f.eks. på web.

**Digitalisering av lyd (fra ADC til DAC):** -Sampling: ADC tar punktprøver av elektrisk signal mange ganger i sekundet og sjekker spenningsnivå. Spenningsnivået blir representert med et tall som kan være positivt eller negativt.   
 -Samplingsfrekvens: Antall avlesninger av signalet per sekund (Hz).   
 -Nyquist regel: Dobbel samplingsfrekvens av høyeste lydfrekvens.  
 -Bit-dybde: Oppløsning på lyden, Vanlig med: 16,24,32 og 48 bit.  
 -Utregning av antall bytes: sek(s) X samplingsfrekvensen(hz) X bit-dypde(bytes)

**Representasjon av bilder:** -Oppløsning: piksler x piksler  
 -Tetthet: Antall piksler per fysisk areal. Måles i Pixels Per Inch (PPI)  
 -Lagring av ikke-komprimert fargebilde: r,g,b,r,g,b,r,g,b …

**Uke 39 - Binær representasjon: Video, komprimering og hex**

**Digital video:** Hvert bilde kalles en frame. Hastigheten på video måles i Frames per second (f.eks. KBit/sek). Bitrate er mengden av piksel-informasjon i hvert bilde.

**Datakomprimering:** er å kode data til å bruke færre bit enn original representasjon. Gjøres for å gjøre det raskere å overføre bilder og redusere lagringsplass.

**Tapsfri komprimering:** F.eks. ZIP og PNG. Gir ikke tap av opprinnelig data.   
 -Run-length-koding:  
 -Reduserer repeterende data  
 -Legger til data om antall representasjoner  
 -Vil redusere antall bytes ved mye repeterende data  
 -Vil ikke redusere antall bytes hvis det ikke er repeterende data

**Lossy komprimering:** Fjerner unødvendig eller mindre viktig informasjon. Fjerner infomasjon som er vanskelig for mennesker å oppdage.

**Lossy lydkomprimering:** Benytter seg av «perceptual coding», koding av data som tar hensyn til menneskelig persepsjon. Koder ulike frekvensbånd med ulik presisjon.

**Lossy komprimering av bilde (jpeg):** Deler opp bilder i blokker av 8x8 piksler. Lagrer enklere mønster per blokk som krever mindre data.

**Lossy videokomprimering:** Fokuserer på endringer i bildet istedenfor representasjon av hvert bilde. Reduserer data basert på likheter i sekvensen av bilder.

**Hex:** Hex lagrer mer info på lite plass

**Multimedia utfordringer:** Multimedia på internett har utfordringer med dårlig bildekvalitet, treg oppdatering som skyldes:  
 -Forsinkelse(latency) Tiden det for informasjon blir laget til den blir levert  
 -Båndbredde (bandwith): Hvor mye data som overføres per tidsenhet (bits/sek)

**Uke 40 – Datamaskinens virkemåte**

**ALU:** En del av prosessoren. Utfører beregninger: addisjon, subtraksjon, inkrement.

**RAM:** Random access memory, datamaskinens arbeidsminne, ikke-persistent: trenger strøm for å huske. Kan hente data fra vilkårlige deler av minne. Bruker adresse for å spesifisere hvor i minne man skal skrive/lese.

**Persistent minne:** Sekundærminne**.** Minne som overlever uten strøm. Ofte større kapasitet enn ikke persistent. Er tregere re enn ikke-persistent. Eksempler er HDD, SSD, minnepinne og CD/DVD.

**Prosessor (CPU):** Hovedoppgave er å kjøre programmer. Programmer består av instruksjoner som datamaskin utfører til punkt og prikke.

**Registre:** CPU har små og raskt minne på chip – registre. CPU har registre for: instuksjonsadresse, instruksjon og mellomlagre.

**Kjøring av programmer i CPU:** Tre faser: Fetch(Hent instruksjon), Decode(Avgjør hva som skal gjøres) og Execute(utfør instruksjon).   
 -Fetch fase:  
 1. Henter adresse for neste instruksjon i instruksjonsadresse-register  
 2. Henter neste instruksjon fra RAM til instruksjons-register  
 -Decode fasen  
 1. Dekoder data i instruksjonsregisterer  
 2. Dekoder instruksjonen  
 3. Dekoder minneadresse for data som skal hentes fra RAM  
 -Execute fasen  
 1. utføre instruksjon  
 2. Lese data fra RAM til register  
 3. Skrive data fra register til RAM

**Prosessor/CPU-klokka:** Synkroniserer alle operasjoner i en datamaskin

**Cache:** Cache er raskt minne på CPU-chip som er mindre størrelse enn RAM. Cache lagrer data som mest sannsynlig skal brukes i framtidig kjøring. CPU sjekker først for data i cache.

**Minnehierarki:**   
 1. Registere  
 2. Cache   
 3. RAM  
 4. Sekundærminne

**Pipelining:** Mer effektiv bruk av CPU slik at flere deler av CPU kan brukes samtidig. Kan kjære fetch, decode og execute parallelt.

**Uke 41 – Nettverk: Del 1**

**Typer nettverk:** -PAN: Personal Area Network - Personlig (Bluetooth)  
 -LAN: Local Area Network – Begrenset Område (rom,bygning, campus)  
 -MAN: Metropolitan Area Network (by)  
 -WAN: Weide area Network (landområde)  
**Ethernet:** Datamaskiner koblet sammen ved hjelp av ethernet-kabel. Datamaskiner på «samme linje»

**MAC-adresse:** Media Access Control. Alle datamaskiner har egne MAC-adresser både for wifi og ethernet,

**Typer MAC-adresse:**   
 -Unicast: Indentifiserer en enkelt unik datamaskin som skal motta pakke  
 -Broadcast: Alle datamaskiner på nettverket skal motta pakke  
 -Multicast: En begrenset sett av datamaskiner på nettverket skal motta pakke.

**Båndbredde:** Hastighet på hvor raskt data kan overføres over ett overføringsmedium. Måles i bits/sekund.

**Kollisjon på lokalnettverk:** Datamaskiner prøver å kommunisere samtidig over samme medium.   
**Løsning på kollisjoner på ethernet:** Når medium er opptatt vente en kort tid + litt vilkårlig tid. Exponential backoff. Ved gjentatt opptatt, doble ventetiden.

**Collision Domain (CD):** Nettverk som deler samme ethernet kabel. Deler opp nettverk i flere Collision Domains ved hjelp av en switch. MAC-adresser avgjør om switch dender data fra en collision domain til en annen.

**Ruting:** Ofte flere veier til å få data fra et sted til et annet. Data transporteres igjennom nettet via ruting. Data sendes fra en ruter/switch til en annen.

**Linjesvitsjing:**   
 -Fungerer som gamle telefonlinjer  
 -Direkte kobling mellom start og endepunkt  
 -Har linja for overføring for seg selv  
 -Resulterer ofte i ubrukt kapasitet i nettet  
 -Brukes fremdeles av f.eks. banker og militæret.

**Meldings-svitsjing:** -Fungere på samme måte som sending av fysisk post  
 -Data blir sendt via flere stopp (hops)  
 -Data kan sendes via forskjellige ruter  
 -Sikrer overføring og bedre mot feil sammenlignet med linjesvitsjing

**Hop count:** Antall hop blir registrert i meldingen. For mange hop betyr at noe har gått galt i rutingen.

**Nettverkspakker:** Meldinger deles opp i en eller flere mindre datapakker. Pakkeformatet er definert av Internett Protokollen (IP).

**Protokoll:** En protokoll i kontekst av nettverk et sett regler for hvordan informasjon skal utveksles.

**Internett protokollen (IP):** Pakker over internett må følge internett-protokollen. Lavnivå protokoll. IP = IP header + data

**UDP (user datagram protocol):**   
 -Legger til UDP header i tillegg til IP header  
 -UDP header inneholder portnummer og sjekksum  
 -IP får pakke til riktig datamaskin, UDP får pakke til riktig program  
 -UDP gir lite overhead (krever lite ekstra data)  
 -UDP gir kjapp dataoverføring.

**TCP (transmission control protocol):**   
 -Legger tile n TCP header til IP headeren.  
 - Sikrer at datapakker kommer fram.   
 -Sørger for riktig rekkefølge på pakker hos mottaker  
 -Tilpasser utsending av data til nettkapasitet  
 -Inkluderer mottaker-adresse, portnummer, sjekksum, pakkenummer  
 -Gir bekreftelse på mottatt pakke for avsende  
 -Sender pakker på nytt som ikke ble mottatt

Timeline

Description automatically generated

**Sjekksum:** Sjekker om mottatt data er den samme som ble sendt. Beregner summen av data i pakken til et 16-bitstall (for UDP/TCP)Finnes også andre tester som paritetsbit, rekk/kolonne paritet.

**Kilder til feil i overføring av data:** Interferens, Forvrengning, Demping

**Effekt av overføringsfeil av data:**   
 -Enkelt-bit feil: En bit i en blokk av data er endret, mens alle andre er intakte  
 -Burst-feil: Flere bit in en blokk av data er endret  
 -Tvetydighet: Signalet som ankommer mottaker er vanskelig å avgjøre om det er 0 eller 1

**Håndtere feil på overføring av data på nettverk:** -Forward Error Correction (FEC): Legge til informasjon til data som mottaker kan bruke for å sjekke at mottatt data er korrekt.  
 -Automatic Repeat reQuestt (ARQ): Sender og mottaker utveksler meldinger for å sikre at data ble mottatt korrekt.

**Sjekke overføringsfeil:**   
 -16-bit checksum: brukt i UDP/TCP protokollen  
 -Paritetsbit: Single Parity Checking (SPC)  
 -Legges til en paritetsbit til en streng av data, hvor verdi av paritetsbit avhenger av om antall 1-bit er par- eller oddetall.  
 -Rekke/Kolonne paritet: Row and Column (RAC) Parity  
 -Beregner paritet bade for rekke og kolonne av data som overføres  
 -Paritet = 1 hvis antall 1enere er oddetall  
 -Paritet = 0 hvis antall 1ere er partall  
 -Sikrere sjekk av overføringsfeil enn enkelt paritetsbit  
-Syklisk rekundanssjekk: Cyclic Redundancy Codes (CRCs)  
 -Brukes i høyhastighetsnettverk  
 -Fungerer uansett lengde på data som skal sendes. Meget bra detekteriing av feil i dataoverføring. Kan utføres veldig raskt med maskinvare.

Table

Description automatically generated

**Uke 42 – Nettverk: Del 2**

**DNS:** Oppslagsbok for nettsteder. Oversetter domene navn til IP-adresser. Domain Name System/Server.

**OSI 7-lags referansemodell:**   
 -Applikasjon: Representerer programmer som brukes på nettet  
 -Presentasjon: Sørger for at informasjon blir presentert riktig. F.eks. tekstkoding  
 -Sesjon: Etablerer en forbindelse mellom to parter som utveksler data, benytter protokoller som UDP og TCP, stenges etter bruk  
 -Transport: Punkt-til-punkt overføring, feilhåndtering, feilfiksing (UDP,TCP)  
 -Nettverk: Ruting- og svitsj-teknologier  
 -Data link: MAC-adresser, kollisjonsdeteksjon, «exponential back-off»  
 -Fysisk: Håndtere lektriske signaler på kabel eller radiosignaler

**WWW:** systemet som blant annet tilbyr nettsider og nettsteder

**Internett:** Infrastrukturen, nettverket der data blir utvekslet.

**HTTP:** Protokoll i applikasjonslaget for overføring av data mellom en nettleser og webserver. Forkortelse for Hypertext Transfer Protocol. HTTPS er kryptert overføring.

**TCP/IP 5-lags nettverksmodell:**  
 -Applikasjon: Protokoller for web-browsing, epost, http, FTP, POP, SMTP  
 -Transport: Bestemmer hvilke klient- og server-programmer som skal få data, UDP, TCP  
 -Internett: Transportere data over samling av flere nettverk mellom to noder, IP  
 -Nettverk: Transportere data mellom noder på samme nettverk eller link, Ethernet, Wi-Fi  
 -Fysisk: Bestemmer hvordan signaler sendes over et medium(kabel,radio), Kabel(10 Base T), Trådløs (802, 11)

**Lokalnettverk topologier:** Layout/form på nettverk  
 -Buss: Ethernet-kabel som alle datamaskiner er koblet til. Fordel: Enkel kabling, krever lite kabel, enkelt å utvide. Ulempe: Kollisjoner, delt båndbredde  
 -Ring: Kabel mellom PC 1 og 2, en mellom PC 2 og 3 osv. i sluttet ring. Fordel: Ingen kollisjoner ettersom data sendes i ring. Høyere båndbredde enn buss. Ulempe: Alt stopper opp hvis en PC feiler, gir større forsinkelse.   
 -Mesh: Direkte kobling mellom alle datamaskiner. Fordel: Veldig robust mot feil i nettet. Raskt. Ulempe: Krever mye koblinger og kabler.  
 -Stjerne: Datamaskiner koblet sammen til sentral. Fordel Fungerer om en PC feiler, kan legge til å fjerne PC. Ulempe: Hub er flaskehals og «single point og failure».  
Chart

Description automatically generated

**Intranett;** Internett eid av en institusjon, designet så den kan brukes av institusjonens ansatte.

**Virtuelt nettverk:** Internett er et virtuelt nettverk fordi kommunikasjonssystemet er en abstraksjon. Gir illusjon at det er ett nettverk, men består egentlig av masse sammenkoblede nettverk.

**Uke 43 – Nettverk: Del 3**

**Pakke:** Blokk av data fra 7 til 65542 bytes send vha. TCP-protokollen

**Datagram:** Blokk av data send vha. UDP-protokollen

**Frame:** Data sendt over data-link laget f.eks. bruker ethernet-protokollen og ikke IP

**IP-adresser:** Alle datamaskiner og utstyr koblet til internett har en egen adresse. Er en del av IP-protokollen. Bruker to versjoner IPv4 og IPv6

**IPv4:** benytter 32 bit(4bytes). Tilbyr ca. 4,3 milliarder unike adresser (2^32)

**Subnet (IPv4):** Kan sette bits av ip-adressen samme for et nettverk og de siste bitene er unike for hver datamaskin. CIDR notasjon.

**IPv6:** 128-bit adressering. Notasjon er 8 grupper av fire heksadesimale tall med kolon mellom: 2001:0DB8:85A3:0000:0000:8A2E:0370:7334

**Quality of Service (QoS):**  Samling av retningslinjer for gi spesifikk datatrafikk prioritet over annen datatrafikk. Sikre kvalitet på sanntidstjenester på nettet.   
 -DiffServ: Markere spesifikke datapakker med høy prioritet  
 -IntServ: Gir spesifikk datatrafikk prioritet f.eks. Voice over IP

**Forsinkelse (delay/latency):** Tid en pakke bruker fra avsender til mottaker

**Jitter:** Variasjon i forsinkelse på pakker. Høy jitter = stor variasjon i forsinkelse av apkker

**Pakketap:** Antall pakker som forsvinner fra avsender til mottaker

**Throughput/Goodput:** Mengde data som kan overføres per tidsenhet

**Ulike typer forsinkelser:**   
 -Propagation: Tiden det tar for et signal å forflytte seg over et transmisjonsmedium  
 -Access: Tiden det tar å få tilgang til et transmisjonsmedium  
 -Switching: Tiden det tar å videresende en pakke  
 -Queuing: Tiden en pakke befinner seg i minnet til en switch eller ruter i vente på å bli valgt til utsending

**Cybersikkerhet:  
 -**Konfidensialitet: Kun autoriserte personer får tilgang til spesifikk data og system  
 -Integritet: Kun autoriserte personer kan bruke og endre data og system  
 -Tilgjengelighet: Autoriserte personer skal alltid har tilgang til deres data og systemer

**Tre typer autentisering:**   
 -Hva vet du?  
 -Hva har du?  
 -Hva/hvem er du?

**To-faktor autentisering:** -Brukes der sikkerhet er særdeles viktig  
 -Lite sannsynlig at hackere kan knekke begge autentiseringer  
 -Kombinerer to former for autentisering. Hva vet du? Hvem er du?

**Uke 44 – Nettverk: Del 4**

**Nettverksikkerhetens viktig:  
 -**Tap av omdømme  
 -Tap av tillit blant brukere eller kunder  
 -Tap av åndsverk

**Sikkerhetsutfordringer:**   
 -Scams: Lure nettsted-brukere til å investere eller bruke penger  
 -Denial of service: Bevist blokkere lovlig tilgang til nettsted/tjeneste  
 -Mis-representasjon: Oppgi feilaktig/falsk opplysninger om produkt/tjeneste på nett  
 -Phising: Opptre som kjent nettside for å få tak i personlig informasjon  
 -Loss of control: Uvedkommende tar kontroll over en brukers datamaskin  
 -Loss of data: Tap av åndsverk eller annen verdifull informasjon

**Sikkerhetsangrep:**   
 -Wiretapping: Kopiere datapakker under overføring for å få tak i informasjon  
 -Replay: Sende pakker fanget opp fra tidligere sesjoner  
 -Buffer overflow: Oversende mer data en hva mottaker forventer for å utnytte svakheter i systemet og få tilgang  
 -Adress spoofing: Lure mottaker til å kjøre/prosessere pakke vha. falsk IP-adresse.  
 -Denial of Service: Overøse en server med datapakker for å hindre lovlige brukere tilgang/tjenester.  
 -Password breaking: Automatiserte systemer for å “knekke” passord og kryptering  
 -Port scanning: Prøve å kople til åpne porer på datamaskin for å finne svakheter og få tilgang.  
 -Packet Interception: Modifisering av pakker på vei fra avsender til mottaker.

**SYN flooding:** Form for Denial of Service(DoD)-angrep. Sender en serie med synkroniseringsforespørsler uten å returnere kvittering til server.

**Sikkerhetsteknologier:**   
 -Hashing: Sikre at data ikke blir tuklet med   
 -Aksesskontroll/passord: Sikrer hvem som har tilgang til hva  
 -Digital signatur: Autentisering av avsender. Sikrer hvem avsender faktisk er.   
 -Brannmur: unngå uønsket trafikk   
 -Kryptering: Endre data slik at kun rett person kan lese den  
 -Digital sertifikater: Bekreftelse av avsender  
 -Intrusion Detection System: Vite hva som skjer ved data innbrudd  
 -VPN: Sikker tilgang til lokalt nettverk utenfra.   
 -SSH: Applikasjonslag protokoll for fjern-pålogging som garanterer konfidensialitet vha. kryptering over internet  
 -SSL: Mellom applikasjon og socket API, som krypterer overføring over internett. Brukes på web-forbindelser til å gjøre sikre finansielle transaksjoner  
 -IPSec: Sikkerhetsstandard bruk med IP datagram som gjør det mulig å velge autentisering eller konfidensialitet  
 -WPA: Wired Equivalent Privacy/Wi-Fi Protected Access: Sikrer konfidensiell trådløs overføring  
 -PGA: Pretty Good Privacy: Kryptografisk system til å kryptere data før overføring  
 - (Transport Layer Security): Etterfølger av SSL  
 -HTTPS: Kombinerer HTTP med enten SSL eller TSL  
 -RADIUS (Remove Authentication Dial-In User Service): Protokoll for sentralisert autentisering, autorisering og kontering

**Kryptografi:** Bruker en algoritme som gjør om lesbar tekst til ulesbar kryptert tekst.

**Kryptering med offentlig nøkkel:**   
 -Hver part får en hemmelig privat og en offentlig nøkkel  
 -Melding kun kryptert med offentlig nøkkel kan kun de-krypteres med korresponderende privat nøkkel  
 -Melding kryptert med privat nøkkel kan kun de-krypteres med korresponderende offentlig nøkkel  
 -Sikrere kondfidensialitet: kun tiltenkt mottaker får tilgang til meldingen  
 -Offentlige nøkler kan deles over nett ettersom man trenger privat nøkkel for å åpne kryptert melding

**Privatnøkkel kryptering:**   
 -Samme nøkkel (K) bruker til å kryptere ( C ) og de-kryptere melding (M)   
 -Nøkkel må holdes hemmelig og kan ikke deles

**Digitale sertifikater og utstedere:** For å sikre at webserver er «legit», kan man bruke digitale sertifikater via en nøkkelutsteder (key authorithy)  
 1. User spør Key Authorithy om Web Site offentlige nøkkel kryptert med KA`s offentlige   
 2. KA returnerer WS offentlige nøkkel vha. KA`s private nøkkel  
 3. U sender forespørsel til WS vha. WS offentlige nøkkel  
 4. WS returnerer resultatet vha. WS private nøkkel

**Brannmur:** - Overvåker og kontrollerer trafikk inn og ut av et internt nettverk  
 -Typisk innebygd i switcher og rutere  
 -Sentraliserer kontroll over nettverkstrafikken som går inn og ut  
 -Implementerer sikkerhetsretningslinjene til en organisasjon  
 -Kan filtrere IP avsender og mottaker, Port nummer, Type protokoll, rammetype osv.

**Sende pakker kryptert over internett for VPN:**   
 -Payload encryption: Krypterer kun meldingsinnholdet i pakke, ikke header.   
 -IP-in-IP tunneling: Krypterer både meldingsinnhold og header og plasserer resultatet i en ny pakke som sender over internett  
 -IP-in-TCP tunneling: To parter etablerer en TCP forbindelse der det sendes en strøm av krypterte datapakker.

**Utfordringer med VPN:**   
 -Latens: Pakker får for mange ganger mellom bruker og LAN  
 -Throughput: Dataraten over nettet kan være en begrensing  
 -Overhead/fragmentering: Tunnelig øker data som sender og mottas