

24 timer HJEMMEEKSAMEN

TK1104 DIGITAL TEKNOLOGI

Tillatte hjelpemidler: Alle

Varighet: 24 timer

Karakterskala/vurderingsform: Bestått / Ikke bestått Dato: 13.-14. desember 2021

Oppgave 1. Generelt (15 %)

- a) Forklar hvorfor datamaskiner bruker binær logikk. Forklar kort hva binær logikk og maskinens fysiske oppbygging har å si for pålitelighet og produksjonskostnader for komponenter i en datamaskin. Tegn gjerne noen figurer som illustrerer dette.

En datamaskin bruker maskin språk som sin grunnleggende behandling og lagring av informasjon, instruksjoner og adresser og minner. Til dette har rådighet elektroniske impulser der strømmen enten på eller av. Ved «på» er notifisert med 1, ved «av» er det notifisert med 0. Maskinen har derved til rådighet å behandle alle instruksjoner med et språk bestående av 0 og 1. Dette kaller vi et binært språk. Informasjon lagres i RAM/CPU (Prosesor). Maskin bruker deretter binær logikk til utføre operasjoner. Dette er enkelt og plassbesparende.

Binærlogikk er enkelt å implementere. Maskinen har til rådighet strøm på eller strøm av (1 eller 0). Dette er et enkelt konsept, robust og mindre utsatt feil. Lagring foregår i bits/bytes bestående sekvenser av nuller og enere. I rimelig data modeller har man integrerte hovedkort som er rimelig. I det mer kostbare data maskiner har man utskiftbare komponenter på hovedkortet.



Kilde: TK1104_Leksjon_0x00_Intro

Maskinen behandler alle operasjoner, instruksjoner og adresser i CPU. Informasjon lagres binært i et mellomlager/hurtiglager for rask, sekvensiell eller parallell (Multitasking) behandling. Desto større kapasitet i CPU og tilsvarende i mellomlagret, jo raskere kan maskinen behandler instruksjonene. Samtidig øker kostanden med størrelsen på CPU og mellomlager. Fordelen med stor kapasitet i CPU og mellomlagring er at man reduserer «Overflow», «Crash», og andre feil som oppstår når maskinen pålegges flere operasjoner enn den kan behandle.

5	Applikasjonslaget	HTTP, DNS, SMTP,FTP
4	Transportlaget	TCP, UDP
3	Nettverkslaget/Internet	Ruter, IP, ICMP, RIP
2	Datalinjelaget/Lenker	Ethernet, IEEE, FDDI
1	Fysisk	Kabler, Skjerm, Mus, Tastatur osv..

b) i) Forklar forskjellen på TCP og UDP protokollene på Transportlaget.

TCP: « Transmission Control Protocol » er en standard internetmodus som håndter og organiserer overførsel av data, håndterer tap av data, håndterer «Flow Control» samt kontrollerer hastighet hos sender når kø oppstår. TCP har ingen «Timing Control»

UDP: «User Datagram Protocol» er en lett vektløsning av TCP uten garantier for feil i data transmisjon. Den er enkelt, men segmenter kan bli tapt, mulig sekvensfeil og feil i handshake.

Hvorfor UDP?:

- Ikke noe oppsett er nødvendig for transmisjon,
- Den er «Stateless»
- Lite segmenthode
- Ingen kø håndtering
- Tillater Kringkasting (Broadcasting)

ii) Gi noen eksempler på situasjoner det vil være fornuftige å velge den ene fremfor den andre.

Applications and tr-protocols:

Email	smtp / RFC 821	TCP
Terminal access	telnet / RFC 854	TCP
Web	http / RFC 2068	TCP
File Transfer	ftp / RFC 959	TCP
Streaming multimedia	proprietary	TCP / UDP
Remote file server	NES	TCP / UDP
IP telephone	proprietary	UDP

c) Forklar hva en «floppy disk» i en PC er (var), hvilket bruksområde denne har?

Floppy Disk var vanlig en lagring metode i tidligere pc. Lagring var delt opp i spor og sektorer nummerert utenfra og innover. En sektor var typisk 512 byte. Sektorene ble lest parallelt. Sammenhengende sektorer innen samme spor ble kalt for blokk. Blokkstørrelsene var på 4kb. Aksestiden var langsomt i forholdt til andre lagringsmedia i dag.

overflow

1 1 1 1 1 1
1 1 0 0 1 1 0 1₂
+ 1 1 0 0 1 1 1 1₂
= 1 0 0 1 1 1 0 0₂

$$376_{10} - 77_{10} = 0000\ 0001\ 0010\ 1011_2$$

		376 =	256 + 120																
		120 =	64 + 56																
		56 =	32 + 24																
		24 =	16 + 8																
		8 =	8																
		2 ¹⁵	2 ¹⁴	2 ¹³	2 ¹²	2 ¹¹	2 ¹⁰	2 ⁹	2 ⁸	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰		
		32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1		
✓	375 ₁₀	0	0	0	0	0	0	0	1	0	1	1	1	1	0	0	0		
		77 =	64 + 13																
		13 =	8 + 5																
		5 =	4 + 1																
		1 =	1																
		2 ¹⁵	2 ¹⁴	2 ¹³	2 ¹²	2 ¹¹	2 ¹⁰	2 ⁹	2 ⁸	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰		
		32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1		
✓	77 ₁₀	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1		
	Flippe 77 ₁₀	1	1	1	1	1	1	1	1	1	0	1	1	0	0	1	0		
	Pluss 1																1		
	Sum Flipt	1	1	1	1	1	1	1	1	1	0	1	1	0	0	1	1		
		1	1	1	1	1	0	1	1	1	1	1							
✓	375 ₁₀	0	0	0	0	0	0	0	1	0	1	1	1	1	0	0	0		
	+	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1		
	Sum 299 ₁₀ :	0	0	0	0	0	0	0	1	0	0	1	0	1	0	1	1		

d) Forklar forskjellen på UTF-8 og UTF-16, i hvilke tilfeller kan det lønne seg å velge det ene enkodingsformatet over den andre.

Unicode er et universalt kodesystem for å få med seg alle tegn, bokstaver og tall i verdens ulike språk. Det tillater 65536 kode punkter på 17plan (mens ASCII kun tillater 128 tegn.)

Unicode enkodes ved hjelp transformasjon-formater. Det kan kodes både som UTF-8 og UTF-16. UTF-8 er den vanlige standard til internett.

UTF-8 og USC-2 er sub set av UTF-16

UTF-16 = Unicode points mens USC-2 er alltid 2 bytes

UTF-16 er vanligvis 2 bytes men kan være flere.

UTF-16 er Vanlig format for strenger i Java.

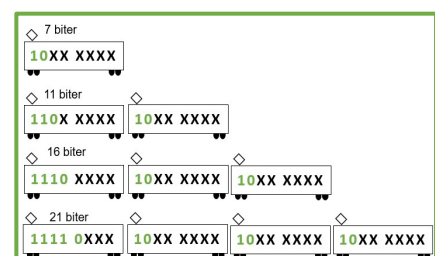
UTF-8: U+0000 til U+007F er det samme for ASCII

Plus to eller flere bytes for å kode tegn, minimum 1 byte

Over U+007F bruker UTF-8 to eller flere byte for å kode et tegn.

UFT-8 tillater koding på følgende måte:

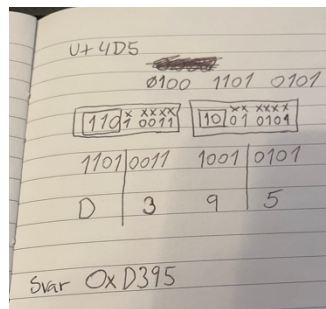
Kilde: TK1104 Leksjon 0x02 TXTmedia



Vanligvis bruker UTF-16 to byte for å kode et tegn, mens UTF-8 bruker tre eller flere tegn for å kode samme. UTF-16 sparer derfor plass på lagrings mediet.

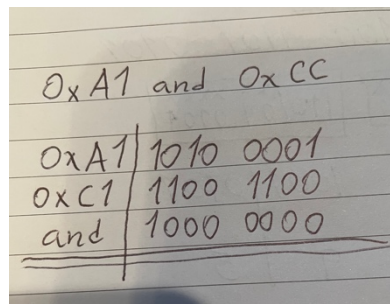
Når meste parten av kodingen greier seg med ASCII tegn er det fordel å bruke UTF-8.

e) Utfør UTF-8 enkoding av Unicode-punktet U+4D5 (et tegn fra Kyrillisk alfabet – som ser likt ut som en bokstav i vårt latinske alfabet). Oppgi svaret i hex.

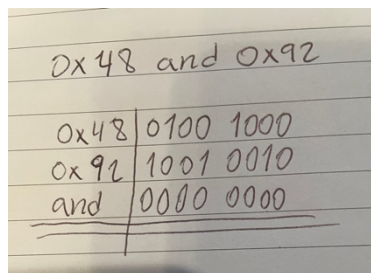


f) Utfør følgende boolske operasjoner. (Vis utregning.)

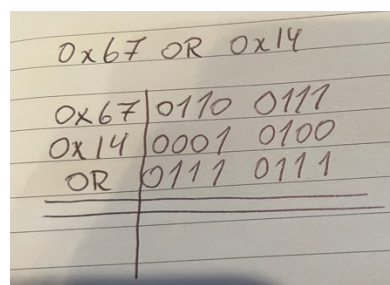
$$0xA1 \text{ AND } 0xCC = 1000 \ 0000$$



$$0x48 \text{ AND } 0x92 = 0000 \ 0000$$



$$0x67 \text{ OR } 0x14 = 0111 \ 0111$$



$$0xF0 \text{ OR } 0x89 = 1111\ 1001$$

Handwritten calculation showing the OR operation between 0xF0 and 0x89. The binary representations are aligned and the result is calculated bit by bit.

0xF0	1111	0000
0x89	1000	1001
OR	1111	1001

$$0x51 \text{ XOR } 0x95 = 1100\ 0100$$

Handwritten calculation showing the XOR operation between 0x51 and 0x95. The binary representations are aligned and the result is calculated bit by bit.

0x51	0101	0001
0x95	1001	0101
XOR	1100	0100

g) Hva er bitstyrken til et passord med 8 tegn hvor passordet består av små bokstaver (a-z) og tall? (Vis utregning.)

Bit styrke måler kvaliteten på et passord og uttrykker hvor mange forsøk en angriper trenger for å finne passordet (Brute Force)

Bit styrke = \log_2 (forskjellige tegn i passordet) * antall tegn i passordet.

$$\text{Bit styrke} = \log_2 (26+10)*8 = \log_2(36)*8 = 5.169925 = \underline{\underline{41.3594}}$$

Oppgave 3. Praktiske oppgaver (30 %)

- a) Hva gjør kommandoen "nslookup -query=ns . > table" på kommandolinje/terminal? (Du kan svare for det operativsystemet du kjenner best; Windows, Linux eller OSX, men du må oppgi hvilket operativsystem du har brukt i besvarelsen.)

Jeg buker OSX som er bygget på toppen av UNIX. Jeg buker Terminal for spørring.

```

Dante@Dante: ~$ nslookup -query=ns . > table
> table
Server: 127.0.0.1
Address: 127.0.0.1#53
Do you use UNIX commands on a Mac?
** server can't find table: NXDOMAIN
  
```

Av sikkerhetshensyn har jeg overstrøket med gult:

User navn

Min Server adresse

Min Router adresse

- b) Demonstrer kommandoen «ftp» på kommandolinje/terminal, bruk domenet ftp://speedtest.tele2.net og last ned noen testfiler fra serveren. Hvilke nedlastingshastigheter oppnår du? Dokumenter kommandoer du har brukt og resultater enten med tekst eller screenshot.

```
$ telnet speedtest.tele2.net 80
Trying 90.130.70.73...
Connected to speedtest.tele2.net.
Escape character is '^]'.
POST /upload.php HTTP/1.1
Host: speedtest.tele2.net
Content-Length: 3

abc
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 13 Dec 2021 19:12:41 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

8
size=500
0
```

- c) I denne oppgaven skal du både demonstrere forståelse av bruk av verktøyet Wireshark og web browser, og generell forståelse av URL og web sider.

Først må bruke terminal for finne www.eastwillsecurity.com sever.
Kommandoen er nslookup www.eastwillsecurity.com
Deretter brukte jeg wireshark for å spore (Sniffe) web browser ved å bruke ip.addr == 77.111.240.75
Den blå linjen viser informasjonen.

```
$ nslookup www.eastwillsecurity.com
Server: 0.1
Address: #53

Non-authoritative answer:
Name: www.eastwillsecurity.com
Address: 77.111.240.75
```

```
ip.addr == 77.111.240.75
No. | Time | Source | Destination | Protocol | Length | Info
--+--+
84 2021-12-13 20:26:34.777411 77.111.240.75 192.168.10.142 TCP 74 80 → 55134 [SYN, ACK] Seq=0 Ack=1 Win=
85 2021-12-13 20:26:34.477576 192.168.10.142 77.111.240.75 TCP 66 55133 → 80 [ACK] Seq=1 Ack=1 Win=1317
86 2021-12-13 20:26:34.477577 192.168.10.142 77.111.240.75 TCP 66 55134 → 80 [ACK] Seq=1 Ack=1 Win=1317
87 2021-12-13 20:26:34.478114 192.168.10.142 77.111.240.75 HTTP 643 GET / HTTP/1.1
88 2021-12-13 20:26:34.489990 77.111.240.75 192.168.10.142 TCP 66 80 → 55133 [ACK] Seq=1 Ack=578 Win=64
89 2021-12-13 20:26:34.489996 77.111.240.75 192.168.10.142 HTTP 397 HTTP/1.1 304 Not Modified

> Frame 87: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface en0, id 0
> Ethernet II, Src: Apple_b1:9a:c9 (98:01:a7:b1:9a:c9), Dst: ZyxelCom_dd:83:b3 (e4:18:6b:dd:83:b3)
> Internet Protocol Version 4, Src: 192.168.10.142, Dst: 77.111.240.75
> Transmission Control Protocol, Src Port: 55133, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
> Hypertext Transfer Protocol

0000 e4 18 6b dd 83 b3 98 01 a7 b1 9a c9 08 00 45 00 ..K...x...E
0010 02 75 00 00 40 00 00 2f 92 c0 a8 0a 8e 4d 6f ..u..@./....Mo
0020 f0 4b d7 5d 00 50 a4 22 d1 ef 90 45 58 b2 80 18 .K.J.P."...EX...
0030 00 0a a3 49 00 00 01 01 08 0a 7a 00 06 f8 9a 37 ..I...z...
0040 e7 3d 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..=GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 61 73 74 ..Host: www.east
0060 77 69 6c 6c 73 65 63 75 72 69 74 79 2e 63 6f 6d willsecu rity.com
0070 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 ..Connec tion: ke
0080 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d ep-alive Cache-
0090 43 6f 6e 74 72 6f 6e 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00a0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0 Upgr ade-Inse
00b0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00c0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo
```

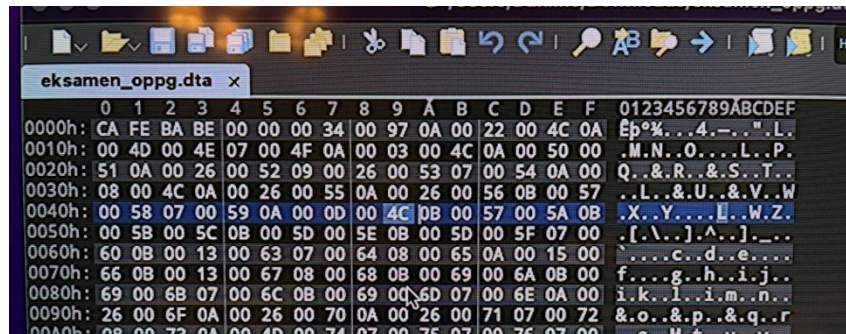
d) I denne oppgaven skal du demonstrere forståelse for filer og filformater, og praktisk bruk av en hexeditor. Først last ned denne filen:

http://www.eastwillsecurity.com/tk1104/oppgave3d/eksamen_oppg.dta

Magic Number i denne filen er CAFE BABE

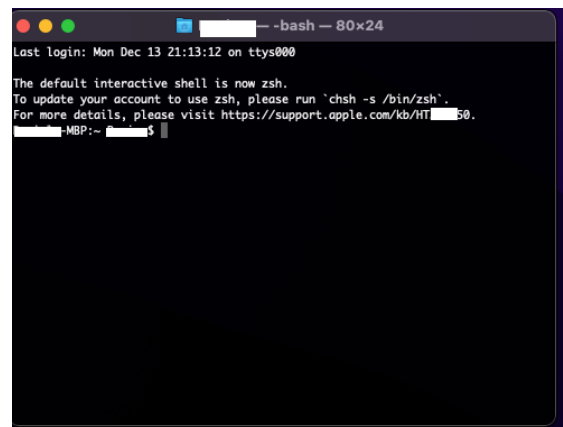
Fil tabellen er type Unicode

0x4C = 0100 1100 som skrive ut alfabet L

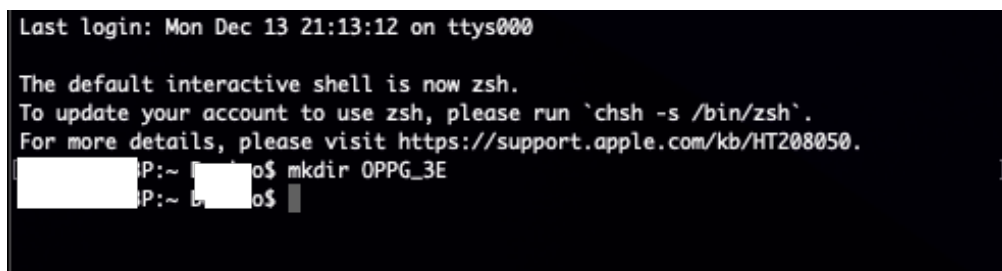


e) I denne oppgaven skal du demonstrere grunnleggende ferdigheter i shell/terminal, oppgaven består av 6 små deler som skal utføres i rekkefølge.

Del 0: Åpne terminal (Linux/OSX) eller kommandolinje (Windows)



Del 1: Opprett en ny mappe/katalog som heter 'OPPG_3E'



Del 2: Gå inn i mappen du opprettet

```
MBP:~ [redacted]$ cd OPPG_3E/  
MBP:OPPG_3E [redacted]$
```

Del 3: Opprett en fil som heter 'TEST.TXT' med innholdet 'TESTTESTTEST'

DEL 4: Skriv ut innholdet av filen på skjermen (ut i terminal/kommandolinje)

```
MBP:OPPG_3E [redacted]$ echo TESTTESTTEST > TEST.txt  
MBP:OPPG_3E [redacted]$
```

Del 5: Slett filen du opprettet

```
MBP:OPPG_3E [redacted]$ rm TEST.txt  
MBP:OPPG_3E [redacted]$
```

Del 6: Slett mappen/katalogen du opprettet

```
MBP:~ [redacted]$ rmdir OPPG_3E/  
MBP:~ [redacted]$
```

Oppgave 4. Forståelse av nettverk (20 %)

- a) Forklar forskjellen på en Hub, en Switch og en Router i et nettverk. Forklar hvordan de fungerer, hvilket TCP/IP lag de opererer på, og hvor i et nettverk de typisk brukes.

Hub:

- Hver mottatt byte bli omdirigert til andre lenker.
- Ingen buffering
- Ingen CSMA/CD – NIC oppdager kollisjoner.

Switch:

- Linker lang segmenter
- Utvider distansen mellom HUBene
- 10 BaseT og 100 BaseT er kompatible for linkup:
 - Slike koblinger krever en bro (brigde)
- Link Layer box: Mellomlagrer og transmisjoner av rammer (frames).
- Sjekker hoder (heads) når det er nødvendig
- Gjennomsiktig (Transperent)
- Plug and play
- Switch har en Switch tabell

Router:

- Router har lagring og videre sender
- Router er «Net layer units» (3. lag).
- Router bruker ruter tabeller / implementere ruter algoritmer

Routers vs. Switches:

- Router er net layer units (3. lag) / Switches er link layer units (2.lag).
- Router bruker routing tables / Switches bruker switch tables.
- Router implementerer router algoritmer / Switches filtrer + plug & play.

TCP/IP hadde fire nivåer: Application, Transport, Internet og Network Interface. Dagens TCP/IP har fem lag: Application, Transport, Network, Datalink og fysisk. TCP/IP headeren 20 bytes stor.

TCP brukes i transport lageret / IP i netverk routing.

- b) Forklar hvordan Linklagsprotokoller basert på Multiple Access (MA) fungerer, forklar også hvordan CSMA protokoller løser utfordringene med Multiple Access.

MA er en delt kanal (one shared chanel) som kan motta «broadcasting». Den er «half-duplex» for å hindre interferens. Den benytter en distribuert algoritme som bestemmer hvordan nodene deler trafikken.

CSMA lytter (listens) før sending. Hvis kanalen er fri; send. Hvis den er opptatt; vent til den er ledig. Der er imidlertid et problem hvis nodene er for langt fra hverandre siden det øker fare for kollisjoner. Konsekvensen er at man deler mediet hvilket gjør det mulig å dele kapasiteten.

CSMA/CD (Colisions Control) Det er en videreutvikling av CSMA med kollisjons kontroll. Den lytter før sending; hvis ledig: send. Hvis opptatt; venter + lytter mens sending pågår; hvis kollisjon inntreffer: sendingen stoppes. Den oppdager kollisjoner på følgende måte: måler signalstyrken i enkle kablede nettverk. Dette er mere komplisert i wifi nettverk.

- c) Forklar hvordan DHCP fungerer, og hvilken oppgave denne protokollen har i et nettverk. Hva skjer hvis en maskin som skal bruke en DHCP server ikke får svar fra den – kan man sette opp et nettverk uten å bruke DHCP?

DHCP gjennomfører adressering med Plug & Play.

- Host: oppdager DHCP
- Server: DHCP tilbyr (offer),
- Host: DHCP forespørsel (query),
- Server: IP adr. + nettverk parametere + DHCP ack
- Host: Aksepterer verdiene som er sendt.
 - C:\User\blis og > ipconfig / frislipp – fornyelse

DHCP finner nettverk parameterne:

- Klienten spør nettverket om IP, nw.maske, std. Gateway, DNS ved å utstede FF-FF-FF-FF-FF-FF i LAN (for oppdagelse)
- Ledig DHCP server svarer med tilbud (oppbevares in nettverket)
- Når «leien» slutter, blir prosessen fornyet.

Hvis ikke noe svar fra Server foreligger, vil Host fortsette å tilby DHCP til svar oppnås. Hvis ikke noe svar foreligger etter x antall forsøk, brytes forbindelsen.

Det er vanskelig å sette opp et nettverk uten DHCP, men man kan tilordne statiske adresser.

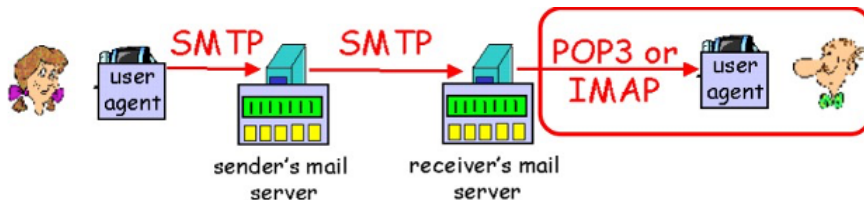
- d) Forklar hvordan SMTP protokollen (for sending av epost) fungerer. Illustrer forklaringen med en skjematisk tegning som viser dataflyt mellom klient og server.

SMTP bruker TCP for å sende email fra klient til server; port 25 (587)

Protokollen etablerer direkte transmisjon av data server til server;

- Gjennomfører «handshake»
- Overføring av data finner sted
- Avslutter transmisjon.

Transmisjon av data foregår ved ASCII tekst. Meldingen sendes med 7-bits ASCII. Sendingen avsluttes med '.'



Kilde: TK1104_Leksjon_0x07_ApplikasjonsLaget