Uke 46: Repetisjonsoppgaver/eksamensliknende oppgaver IN1020

LMC og tallsystemer:

Oppgave 1: Verdien 112_{10} (112 i 10-tallssystemet) kan også representeres i andre tallsystemer. Hvilke av disse verdiene er lik 112_{10}?

- ○ 1110000_2
- ○ 111_7
- ○ 70_{16}
- ○ 1012_3
- ○ 160_8
- ○ 400_5

Oppgave 2: En byte inneholder disse bitene: 10010110. Hvilke verdier kan vi representere av disse bitene?

- ○ 105
- ○ -53
- ○ 202
- ○ 150
- ○ -106

Oppgave 3: Hva skrives ut når denne koden og brukeren gir først 10 og 5 som input?

```
INP
STA 99
INP
STA 98
ADD 98
ADD 99
OUT
HLT
```

- ○ 20
- ○ 25
- ○ 15
- ○ Ingenting skrives ut
- ○ 10

Oppgave 4: Hva blir skrevet ut når brukeren gir verdiene: 10, 20, 5, 1?

```
0:      901
1:      805
2:      508
3:      902
4:      000
5:      208
6:      308
7:      600
8:      000
```

- ○ -15
- ○ -5
- ○ 5
- ○ 10
- ○ Ingenting skrives ut

Oppgave 5: Hva skrives ut når dette programmet kjøres og brukeren gir 1 som input?

```
        INP
        STA w
lok     LDA tekst
        BRZ done
        OTC
        LDA lok
        ADD one
        STA lok
        BRA lok
done    HLT
one     DAT 1
w       DAT 0
tekst   DAT 72
        DAT 101
        DAT 105
        DAT 32
        DAT 58
        DAT 125
        DAT 0
```

- ○ HEI!!
- ○ 72, 101, 105, 32, 58, 125
- ○ Hei :}
- ○ Ingenting skrives ut
- ○ 494

Oppgave 6: En byte inneholder disse bitene: 00111101. Hvilke verdier kan representeres av disse bitene?

- ○ -67
- ○ 113
- ○ 125
- ○ 61
- ○ 60

Oppgave 7:

Hvordan lagres verdien 37 i en byte (8 bit)? Skriv bitene i hver sin rute.

Hvordan lagres verdien -37 når vi lagrer tall som 2-er-komplement?

Oppgave 8: Sorter de følgende verdiene etter størrelse (det minste først og største sist).

100010_2 (binært)
66_{10} (desimalt)
$3AE0_{16}$ (heksa)
74_8 (oktalt)

Oppgave 9: Hva skrives ut når denne koden kjøres og brukeren gir 1, 2, 3, 4, 0 som input?

```
lok     INP
        BRZ ut
        STA x
        BRA lok
ut      LDA x
        ADD ti
        OUT
        HLT
x       DAT 0
ti      DAT 10
```

- ○ 10
- ○ Ingenting skrives ut
- ○ 14
- ○ 0
- ○ 1

Oppgave 10: Velg det største og det minste tallet. Alle tallene representeres med 2-er-komplement.

- ○ 11001011_2
- ○ 000001_2
- ○ 0101011_2
- ○ 10010000_2
- ○ 11111110_2

Sikkerhet:

Oppgave 11: Hvilke av følgende begrep defineres som sikkerhetsmål:

- ○ Autentisitet
- ○ Kryptografi
- ○ Konfidensialitet
- ○ Sporbarhet
- ○ Tilgangskontroll
- ○ 2-faktorautentisering
- ○ Digital signatur
- ○ Integritet

Oppgave 12: Hvilke av følgende sikkerhetstiltak kan bidra til å oppnå sikkerhetsmålet integritet?

- ○ Benytte sjekksumalgoritmer for data som skal overføres i nettverk.
- ○ Å benytte kryptografi for å gjøre informasjon uleselig for de som ikke skal ha tilgang.
- ○ Benytte endringskontroll slik at kun autoriserte brukere har tilgang til å endre data.
- ○ Å sørge for gode rutiner for sikkerhetskopiering av all informasjon.
- ○ Å sørge for god opplæring av brukere.

Oppgave 13: Phishing-attacks utnytter menneskelige svakheter. Hvilke sikkerhetstiltak kan forebygge slike angrep?

- ○ Kryptering av alle meldinger slik at disse skal være uleselige for andre
- ○ God opplæring, slik at folk klarer å identifisere potensielle farer.
- ○ Mer omfattende lovverk som gjør at de som er ansvarlig for slike angrep får konsekvenser.
- ○ Filtrering av e-poster.
- ○ E-post-autentisering.

Oppgave 14: Assymetrisk kryptering med nøkkelpar bestående av privat og offentig nøkkel, benyttes til både digital signatur og kryptering av innhold av en melding. Hvordan må nøkkelparet benyttes (dvs. skal avsender eller mottagers nøkkelpar benyttes? Hvem skal benytte offentlig og hvem skal benytte privat nøkkel?) ved digital signatur

- ○ Senders offentlige nøkkel
- ○ Mottakerens private nøkkel
- ○ Mottakerens offentlige nøkkel
- ○ Senderens private nøkkel

Oppgave 15: Hvilke av følgende egenskaper stemmer IKKE for en sjekksumalgoritme?

- ○ Umulig (vanskelig) å finne den opprinnelige beskjeden gitt en sjekksum.
- ○ Umulig (vanskelig) å endre en beskjed uten at sjekksummen blir endret.
- ○ Det er enkelt å regne ut sjekksummen for en gitt beskjed.
- ○ Det er mulig (og enkelt) å finne den opprinnelige beskjeden fra en sjekksum.
- ○ Umulig (vanskelig) å finne 2 ulike beskjeder med samme sjekksum.
- ○ Endrer vi en bokstav i en melding, så vil bare 1-4 symbol i koden forandres.

Oppgave 16: Til tross for at en webtjeneste for en nettbank er svært sikkert konfigurert, kan ting gå galt f.eks. når en bruker skal bruke (logge seg inn til) banken for å betale en regning. Hvilke mulige feil som truer sikkerheten kan oppstå i denne situasjonen?

- ○ Brukeren glemmer passordet sitt.
- ○ Bruker benytter et åpent trådløst nett: DNS-forfalskning i et kompromittert eller falskt aksesspunkt kan sende brukeren til en falsk nettside.
- ○ Brukeren Googler bankens navn og ikke selve adressen og havner på en falsk nettside (f.eks. www.dnb.no og www.d-nb.no).
- ○ Det er installert en tastelogger på brukerens maskin uten deres viten som registrerer innloggingsinformasjonen til brukeren.
- ○ Brukeren får en e-post om at de har ubetalte regninger i nettbanken fra e-posten thisisDNBno@epost.no og de trykker videre på lenken for å gå til bankens nettside, men de blir sendt til en falsk nettside.

Oppgave 17: I «Lov om behandling av personopplysninger (personopplysningsloven)» skilles det mellom ordinære personopplysninger og sensitive personopplysninger. Kategoriser de følgende personopplysningene som enten ordinær personopplysning eller sensitiv personopplysning.

Personopplysninger	Ordinære personopplysninger	Sensitive personopplysninger
Bilder	○	○
Genetiske opplysninger	○	○
Opplysninger om atferdsmønstre	○	○
Fødselsnummer	○	○
Fingeravtrykk	○	○
Medlemskap i fagforening	○	○
Filosofisk overbevisning	○	○
Etnisk opprinnelse	○	○

Oppgave 18: PKI er et rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater med offentlige nøkler. Hovedformålet er å sikre ektheten av offentlige nøkler, samt forenkle nøkkel-distribusjonen. Hvilke av de følgende påstandene stemmer om PKI?

- ○ PKI trenger ikke å inneholde en policy for sertifikat-håndtering.
- ○ Et sertifikat utstedes av en tiltrodd sertifikatutsteder (Certificate Authority), som går god for den offentlige nøkkelens ekthet.
- ○ Hver eneste offentlige nøkkel bakes inn i hvert sitt elektroniske sertifikat som knytter nøkkel og identitet sammen.
- ○ Sertifikatene med de private nøklene gjøres tilgjengelig for alle mottagere som skal kryptere og dekryptere meldinger.
- ○ PKI må inneholde prosedyrer for hvordan håndtere og forvalte nøklene.
- ○ MinID, BankID, Buypass og Commfides er eksempler på PKIer i Norge.
- ○ Den tilhørende private nøkkelen kan ikke oppbevares på en datamaskin, på SIM-kortet i en mobil, på et smartkort eller i banken.

Oppgave 19: Petter jobber i justisdepartementet. Han har fått beskjed om å bytte kontorplass fordi alle som jobber på et gitt prosjekt skal sitte samlet i et åpent landskap i øverste etasje. Samtidig som de flytter inn i landskapet får de utdelt nye PC-er. På disse er det et klistremerke med budskapet "Lås PC-en når du går fra den!". Petter husker at informasjonssikkerhetsansvarlig snakket om dette på nyansattkurset han deltok på for lenge siden, men har egentlig aldri forstått hvorfor han skal låse PC-en sin. Alle i landskapet jobber på det samme prosjektet.

Hvilke vurderinger og refleksjoner bør gjøres når de ansatte vurderer om de skal låse PC-en sin eller ikke (med tanke på sikkerheten)?

- ○ Det er ikke sikkert alle skal ha tilgang til samme informasjon selv om de jobber på samme prosjekt.
- ○ Vi kan ikke sikre hvem som har endret eller slettet informasjon i prosjektet om en pc kan være brukt av hvem som helst i rommet.
- ○ Det er en fare for at noen går inn på noen andres pc og leser private e-poster og meldinger.
- ○ Alle de ansatte som jobber på prosjektet er godt kjent med hverandre og de stoler på at ingen kommer til å gjøre noe ulovlig på noen andres maskin.
- ○ Det er ikke bare ansatte som jobber på prosjektet som har tilgang til rommet, men også f.eks resepsjonister, vaktmestere etc.
- ○ Petter kan få konsekvenser om en annen kollega har brukt hans PC til å utføre handlinger som er i strid med intern sikkerhetsinstruks uten hans viten.
- ○ De trenger ikke å låse PC-ene sine, ettersom alle uansett jobber med det samme prosjektet.

Oppgave 20: Tilgjengelighet er et sikkerhetsmål. Hva kan utgjøre en trussel mot tilgjengeligheten i et system?

- ○ At mobilen din er tom for batteri og kan ikke logge inn på mobilbanken for å betale en regning.
- ○ Generelle systemfeil som fører til nedetid på systemet i løpet av en kort tidsperiode.
- ○ At systemer er tilgjengelig er ikke så viktig, så det finnes ingen trusler mot tilgjengelighet.
- ○ Manuell feilregistrering av tilganger i systemet slik at en ansatt ikke får tilgang til den informasjonen de trenger, når de trenger det.
- ○ At tjenerne som leverer tjenesten i systemet blir overbelastet med (falske) forespørsler slik at systemet er nede (DDOS-angrep).
- ○ At brukeren har glemt passordet til en tjeneste og har dermed ikke informasjonen tilgjengelig når den trengs. De må bruke ekstra, verdifull tid på å resette passordet.

Nettverk:

Oppgave 21: Hva stemmer for linjesvitsjing (circuit switching), beskjedsvitsjing (message switching) og pakkesvitsjing (package switching)?

- ○ Linjesvitsjing er det som brukes på internett i dag.
- ○ Beskjedsvitsjing er tilkoblingsorientert slik at kommunikasjonen først settes opp og gjennom hele nettet før kommunikasjonen kan begynne.
- ○ I linjesvitsjing settes det opp en dedikert linje som brukes under hele kommunikasjonen som er statisk og ikke kan endre seg.
- ○ Pakkesvitsjing er det som brukes på internett i dag og det ligner mye på beskjedsvitsjing.
- ○ Beskjedsvitsjing er tilkoblingsløs, så den trenger ikke å opprette en forbindelse med mottakeren på forhånd.
- ○ I linjesvitsjing trenger ikke meldingene å følge samme vei hver gang og det er ingen dedikert linje mellom sender og mottaker.

Oppgave 22: Hva er fordelene med å bruke CDN for distribusjon av data?

- ○ Man må på forhånd vite hvor de fleste brukerne befinner seg geografisk og plassere tjenerene ut ifra dette.
- ○ Å ha innholdet fysisk nærme brukeren reduserer round trip time (RRT) og gjør det derfor raskere å aksessere.
- ○ Ved å cache innholdet nær brukeren sparer man trafikk over backbone-nettet.
- ○ Ved å distribuere innholdet, avlaster man tjeneren som leverer dette innholdet, noe som gir en mer skalerbar tjeneste.
- ○ Det koster ekstra maskinvare og lagringsplass.

Oppgave 23: Push, Pull og Publish-subscribe er noen paradigmer for initiering og gjennomføring av kommunikasjon over Internett. Hvilke av alternativene stemmer for push, pull og publish-subscribe?

- ○ Pull: klienten initierer en forbindelse til en tjener med en forespørsel om en tjeneste.
- ○ Publish-subscribe er den vanligste forbindelsesstrategien.
- ○ Push: en tjener «dytter» innhold til en klient når den har noe interessant å levere.
- ○ Pull krever at det er en forbindelse fra før eller at klienten lytter.
- ○ Publish subscribe: «dytter» en tjeneste til klienten
- ○ Publish-subscribe: når mange klienter abonnerer på en tjeneste og tjenesten dytter innhold til abonnentene når den har noe interessant å levere.

Oppgave 24: Hvilke lag finner vi vanligvis i internett?

- ○ Linklaget
- ○ DHCP-laget
- ○ Presentasjonslaget
- ○ Nettverkslaget
- ○ Pakkelaget
- ○ Det fysiske laget
- ○ Sesjonslaget

Oppgave 25: Du ønsker å laste ned en fil på 120 megabyte og den maksimale nedlastningshastigheten på din internettforbindelse er 30 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

- ○ 4 sekunder
- ○ 2 sekunder
- ○ 32 sekunder
- ○ 15 sekunder
- ○ 3600 sekunder

Oppgave 26: Et subnett har nettverksmasken 11111111. 11111111.10000000. 00000000. Hvor mange gyldige IP adresser kan tildeles verter i subnettet?

- ○ 15
- ○ 13
- ○ 30
- ○ 32768
- ○ 32766
- ○ 131070

Oppgave 27: Hvilke utsagn er sanne om klient-tjener aksessmodellen?

- ○ Har distribuert eierskap.
- ○ Har en sentral tjener som mottar forespørsler fra mange klienter.
- ○ Klienter oppretter en forbindelse ved å be om en tjeneste og tjeneren svarer på forespørselen ved å levere tjenesten.
- ○ Alle nodene er likeverdige vertsmaskiner som samarbeider om å levere en tjeneste.
- ○ Det kan potensielt være store kostnader med å få infrastrukturen skalerbar.

Oppgave 28: Hvilke utsagn er USANNE om DHCP?

- ○ Det er en metode som brukes for at et hjemmenettverk med private IP adresser skal kunne kommunisere med internett som bruker offentlige IP adresser.
- ○ Brukes til å automatisk tildele IP-adresser til enheter som kobler seg på et lokalt nettverk.
- ○ DHCP oversetter mellom IP adresser og MAC adresser.
- ○ DHCP brukes for å oversette mellom IP adresser og domenenavn, siden IP adresser er vanskelige å huske.
- ○ I nettverket hjemme er det vanligvis ruteren som kjører en DHCP tjener.
- ○ DHCP tildeler en midlertidig IP adresse som er gyldig en viss tidsperiode når en enhet kobler seg til og så tar tilbake IP adressen når tiden har gått ut.

Oppgave 29: Et subnett er definert ved 192.168.11.13/27 (CIDR-notasjon). Hva er kringkastingsadressen i dette subnettet?

- ○ 255.255.255.255
- ○ 192.168.11.31
- ○ 192.168.11.255
- ○ 192.168.11.27
- ○ 255.255.11.13
- ○ 192.168.11.0

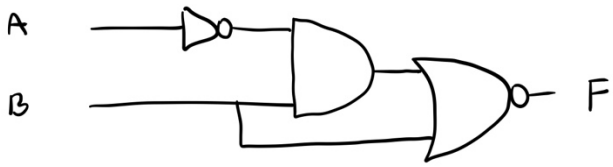
Oppgave 30: Hvilke påstander stemmer for en UDP-protokollen?

- ○ Tilkoblingsorientert forbindelse (3-way handshake).
- ○ Pakkene leveres i riktig rekkefølge.
- ○ Ingen garantier (best effort)
- ○ Feilsjekking av meldingene (sjekksum)
- ○ Bruker flytkontroll og metningskontroll.
- ○ Tilkoblingsløs forbindelse
- ○ Garanterer at pakkene kommer fram til mottakeren - pålitelighet

Hardware:

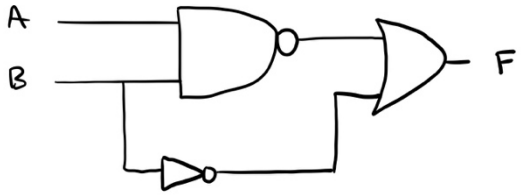
Oppgave 31: Hva er funksjonsuttrykket for denne kretsen? (Velg ett eller flere alternativer.)

- ○ A
- ○ (A'B)'
- ○ B'
- ○ A'B+B
- ○ (A'B+B)'
- ○ A+B'



Oppgave 32: Hva er funksjonsuttrykket for denne kretsen? (Velg ett eller flere alternativer.)

- ○ A'B'+B'
- ○ (AB)'+B'
- ○ A'+B'+B'
- ○ A'+B'
- ○ A'B+B'
- ○ A'+B



Oppgave 33: Anta at prosessoren har 10 000 instruksjoner å utføre, der hver instruksjon tar 3 klokkesykler å utføre. Vi regner med å ha en minneaksessering på 70% og cache-miss på 10%. En cache-hit fører til 5 ekstra klokkesykler og en cache-miss fører til 10 ekstra klokkesykler. Hvor mange klokkesykler vil det ta for prosessoren å kjøre alle instruksjonene?

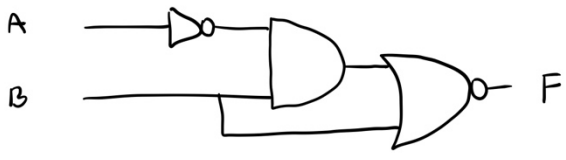
- ○ 38 500
- ○ 66 500
- ○ 47 500
- ○ 75 000
- ○ 7000
- ○ 31 500

Oppgave 34: Hvilke av påstandene under er sanne og hvilke er usanne? Kryss av på rett plass.

Påstand	Sant	Usant
Fetch er en av stegene i en pipeline	○	○
Harddisken er det eneste minneelementet som ikke mister data når datamaskinen skrus av	○	○
Binær addisjon av 1+1+1 gir 0 i sum og 1 i mente	○	○
ALUen kan ikke utføre logiske operasjoner	○	○
En AND port kan ha 4 inputs	○	○
En buss er en kommunikasjonskanal for å frakte data mellom komponenter	○	○
A'B+AB' er funksjonen til en NOR-port	○	○
En hazard er en type komplikasjon som kan oppstå når vi bruker pipeline	○	○

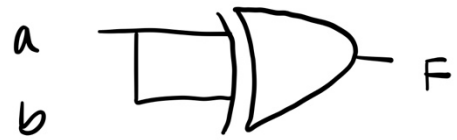
Oppgave 35: Gitt en portforsinkelse på 5ps per port, hvilken frekvens vil denne kretsen kunne operere på? Anta at klokkesignalet er 50%-50% av.

- ○ 15 Hz
- ○ 66.6 GHz
- ○ 33.3 GHz
- ○ 33.3 Hz
- ○ 200 GHz



Oppgave 36: Hva er portens funksjon?

- ○ (a+b)(a'+b')
- ○ aa'
- ○ a⊗b
- ○ 0
- ○ ab'+a'b
- ○ 1
- ○ a⊗a



Oppgave 37: Hvilke av følgende begrep beskriver minneelementer i en datamaskin?

- ○ L1-Cache
- ○ ROM
- ○ OS
- ○ Harddisk
- ○ Registre
- ○ ALU
- ○ FA

Oppgave 38: Hvilke av påstandene stemmer for en adde-kretser?

- ○ En halvadder har mente inn og to binære tall som inputs og mente ut og resultat som output.
- ○ En halvadder adderer sammen kun to 1-bits binære tall.
- ○ ALUen inneholder (vanligvis) en seriell adder.
- ○ En fulladder tar både mente inn og mente ut.
- ○ En seriell adder blir brukt for å addere sammen tall på flere bits.
- ○ Vi kan ikke kombinere en halvadder og en fulladder for å lage en seriell adder.
- ○ Vi kan bruke porter for å bygge opp de ulike adderene.

Oppgave 39: Hvilke av påstandene stemmer for pipeline?

- ○ Når vi bruker pipeline deler vi en instruksjon opp i 4: fetch, decode, execute og write-back.
- ○ Instruksjonene blir ikke raskere utført med pipeline (enn uten) fordi det oppstår komplikasjoner underveis.
- ○ Når vi bruker pipeline kan CPUen jobbe med flere instruksjoner samtidig, fordi det er ulike deler av CPUen som jobber med ulike deler av instruksjonen.
- ○ Bruker vi pipeline så vil utførelsen av 4 instruksjoner ta 4 ganger mindre tid enn å utføre instruksjonene en etter en.
- ○ Structural hazard, data hazard and control hazard er typer komplikasjoner som kan skje.

Oppgave 40: Hvilke av påstandene stemmer for minnet i en datamaskin?

- ○ Minnet er strukturert i flere nivåer der registrene er øverst og sekundærminnet er nederst.
- ○ Datamaskinen kan selv velge om den vil lagre data i cache, RAM eller på harddisken.
- ○ Cache henter ut bolker med informasjon direkte fra sekundærminnet slik at CPUen har informasjonen den trenger klart.
- ○ Cache deles opp i flere lag: L1, L2 og L3, der L1 vanligvis er på prosessoren mens L2 og L3 cache ligger ikke på prosessoren, men veldig nært.
- ○ Cache miss er når CPUen ikke finner informasjonen den trenger i cache og må lete i RAM, noe som gjør at instruksjonen tar litt lenger tid å utføre.
- ○ Registrene er billige og store minnekomponenter som brukes internt inn i CPUen.
- ○ Det tar lenger tid å aksessere cache enn RAM.