

i Info

Eksamen IN1020 høsten 2019

Tid

9. desember kl. 9:00-13:00

Faglærerne vil gå en runde fra kl 10.00.

Oppgavene

Oppgavene er ulike varianter av flervalgsoppgaver. Noen oppgaver kan ha flere riktige svar, mens andre bare har ett. Alle vil ha minst ett korrekt svar. Man får poeng for å velge et korrekt alternativ og man mister poeng ved å velge et galt, men man vil aldri få mindre enn 0 poeng på en oppgave.

Tillatte hjelpemidler

Alle trykte og skrevne hjelpemidler.

En enkel kalkulator uten kommunikasjonsmulighet.

En kalkulator er tilgjengelig i Inspira-systemet.

1.1 Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:

Velg ett eller flere alternativer:

- Sporbarhet ✓
- Tilgjengelighet ✓
- Integritet ✓
- Brannmur
- Sikkerhetskopiering
- Tofaktor-autentisering
- Kryptering
- Uavviselighet ✓

Maks poeng: 2

1.2 Sikkerhetstiltak - konfidensialitet

Hvilke av følgende er sikkerhetstiltak som kan bidra til å oppnå sikkerhetsmålet konfidensialitet?

Velg ett eller flere alternativer:

- Benytte sjekksumalgoritmer for data som skal overføres i nettverk.
- Bruk av tofaktor-autentisering for systemer som behandler konfidensielle data. ✓ a.
- Benytte diskryptering ved lagring av data. ✓
- Benytte HTTPS framfor HTTP som protokoll i nettverkskommunikasjon. ✓
- Bevissthetstrening for alle som behandler data. ✓

Maks poeng: 2

1.3 Sikkerhetstiltak - fysisk sikring

Hvorfor er *fysisk sikring* (f.eks. å begrense fysisk tilgang til maskiner/systemer) viktig for optimal sikkerhet i kritiske datasystemer?

Velg et eller flere alternativer

- Fordi fysisk tilgang til et system gjør det enklere å autentisere seg.
- Fordi en inntrenger kan stjele biometriske identiteter.
- Fordi kritiske systemer ikke har kryptering.
- Fordi en inntrenger kan omgå så og si alle sikkerhetstiltak ved å ha fysisk tilgang til et system. ✓

Maks poeng: 2

1.4 Autentisering

Hvordan kan flerfaktor-autentisering bidra til å forbedre sikkerheten i et datasystem?

Velg et eller flere alternativer

- Flerfaktor-autentisering gjør det enkelt å begrense gjentakende forsøk på å tilegne seg ulegitimert tilgang.
- Ved å benytte biometri kan ikke uvedkommende autentisere seg ved å utgi seg for å være en annen.
- Flerfaktor-autentisering vil begrense hva brukerne har lov til å gjøre i et system.
- Ved å benytte en kombinasjon av autentikatorer vil det være vanskeligere for uvedkommende å tilegne seg ulegitimert tilgang til et system. ✓

Maks poeng: 2

1.5 Digital signatur

Et konsulentfirma har kunder over hele landet. De ønsker å erstatte den tungvinte prosessen med å signere kontrakter med med penn på papir med en digital variant av signatur som kan garantere at det er kunden og ikke en svindler som signerer avtalen. De har hørt om en metode som kalles *digital signatur*, som kanskje kan gi dem nødvendig bekreftelse på identiteten til den som signerer en kontrakt digitalt.

a) Hva kjennetegner det som i informasjonssikkerhet kalles en *digital signatur*:

Velg ett eller flere alternativer:

- Kan bekrefte avsenders identitet ovenfor mottager. ✓
- Baserer seg på symmetrisk kryptering.
- Kan bekrefte avsenders identitet ovenfor en tredjepart (uavviselighet). ✓
- Sikrer konfidensialitet for meldingen som signeres.

b) Hvilke *kryptografiske nøkler* er involvert når *digital signatur* benyttes :

Velg ett eller flere alternativer

- Mottagers private nøkkel.
- Senderens offentlige nøkkel. ✓
- Mottagers offentlige nøkkel.
- Symmetrisk nøkkel generert av sender.
- Symmetrisk nøkkel generert av mottager.
- Senderens private nøkkel. ✓

Maks poeng: 6

1.6 Behandling av personopplysninger

Institutt for informatikk ønsker å teste en nytt datasystem for gjennomføring av eksamen, som bl.a gjør det mulig for studentene å programmere Python under selve eksamenen.

Datasystemet instituttet vil benytte er en ren sky-tjeneste fra en ekstern leverandør, tilgjengelig gjennom en web-applikasjon. Både lagring av data og kjøring av applikasjonen skjer på leverandørens datautstyr som står fysisk plassert i et EU-land, mens selve eksamen gjennomføres/avlegges via en nettleser på UiOs datamaskiner i UiOs lokaler.

Den enkelte student får utdelt et unikt kandidatnummer og et unikt passord, som de bruker når de skal logge inn i systemet for å avlegge eksamen. En levert besvarelse knyttes til en student gjennom studentens kandidatnummer.

Vurder følgende utsagn, og velg de du mener er korrekte med utgangspunkt i opplysningene gitt over.

Velg ett eller flere alternativer:

- Institutt for informatikk er juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket. ✓
- Navn eller fødselsnummer lagres ikke i systemet, og det er dermed ikke nødvendig å forholde seg til personvernregelverket.
- Studentene har rett til å få vite hvilke opplysninger om dem som behandles i systemet. ✓
- Fordi tjenesten helt og holdent er levert av andre, er Institutt for informatikk er ikke juridisk ansvarlig for at informasjon om studentene og deres eksamensbesvarelse behandles i samsvar med personvernregelverket.

Maks poeng: 4

1.7 Trusselmodellering - tilgjengelighet

Etter en vurdering av personopplysningsvern, skal Institutt for informatikk nå ta i bruk følgende datasystem for gjennomføring av eksamen (samme som i foregående oppgave):

Datasystemet er en ren sky-tjeneste fra en ekstern leverandør, tilgjengelig gjennom en web-applikasjon. Både lagring av data og kjøring av applikasjonen skjer på leverandørens datautstyr som står fysisk plassert i et EU-land, mens selve eksamen gjennomføres/avlegges via en nettleser på UiOs datamaskiner i UiOs lokaler.

Den enkelte student får utdelt et unikt kandidatnummer og et unikt passord, som de bruker når de skal logge inn i systemet for å avlegge eksamen. En levert besvarelse knyttes til en student gjennom studentens kandidatnummer.

Tilgjengeligheten til systemet er selvfølgelig svært viktig, da studentene må kunne logge inn og bruke systemet når de møter opp for å avlegge eksamen. Din oppgave er derfor å gjøre en vurdering av hva som kan være en trussel mot *tilgjengelighet*, gitt opplysningene over.

Velg ett eller flere alternativer:

- Manglende sikkerhetsoppdateringer av programvaren og operativsystemet[†] systemet benytter. ✓
- Utilgjengelighetsangrep (DDoS) fra utenforstående med ondsinnede hens . ✓
- Tastelogger plassert i overgangen mellom tastatur og datamaskin.
- Feil i systemet som utfører tilgangskontroll i datasystemet. ✓
- Svikt i lagringsrutinene som fører til at studenter kan se hverandres eksamensbesvarelser.

Maks poeng: 5

1.8 Trussellmodellering

Hvorfor kan bruk av USB minnepinner utgjøre en *sikkerhetstrussel* mot sikkerhetsmålet konfidensialitet?

Velg ett eller flere alternativer

- De kan bruke for mye strøm og på den måten påvirke en datamaskin negativt.
- De kan bringe med seg skadevare som omgår andre sikkerhetsmekanisr ✓
- De kan utilsiktet bli kryptert av for eksempel løsepengevirus.
- De kan stjeles. ✓

Maks poeng: 2

2.1 Nettverksprotokoller

Hva er en nettverksprotokoll?

Velg et eller flere alternativer

- En logg hvor all datakommunikasjon registreres.
- En detaljert beskrivelse av ditt Internettabonnement.
- En fil som inneholder drivere til ditt nettverkskort.
- Regler om hvordan data skal overføres mellom to maskiner. ✓

Maks poeng: 1

2.2 Nettverkstopologi

Hvilke av alternativene er ikke en nettverkstopologi:

Velg et eller flere alternativer

- Stjerne
- Ring
- Hash
- Klient/server
- Full mesh



Maks poeng: 2

2.3 WiFi

WiFi brukes typisk i et:

Velg et eller flere alternativer

- Storage-area Network (SAN)
- Metropolitan-area network (MAN)
- Wide-area network (WAN)
- Local-area network (LAN)



Maks poeng: 1

2.4 TCP/IP-modellen

Hvilket lag i TCP-IP modellen har ansvaret for ruting av pakker i Internett?

Velg ett alternativ

- Det fysiske laget
- Nettverkslaget 
- Applikasjonslaget
- Linklaget
- Transportlaget

Maks poeng: 1

2.5 Overføringshastighet

Du ønsker å laste ned en fil på 200 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 20 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ

- 100 sekunder
- 10 sekunder
- 5 sekunder
- 80 sekunder 
- 20 sekunder

Maks poeng: 2

2.6 IP-adresser

Et subnett har nettverksmasken 11111111.11111111.00000000.00000000
Hvor mange gyldige IP-adresser kan tildeles verter i subnettet?

Velg ett alternativ

- 254
- 255
- 65534
- 8190
- 8191
- 65535



Maks poeng: 3

2.7 TCP

Hvilke av disse tjenestene tilbys av TCP?

Velg et eller flere alternativer

- Sjekksum.
- Kryptert overføring.
- Metningskontroll.
- Alle disse.
- Tilkoblingsløs overføring.
- Flytkontroll.
- Ruting av pakker i Internett.



Maks poeng: 4

2.8 DHCP

Hvor mange DHCP-tjenere bør du ha i et LAN (kringkastingsdomene)?

Velg et eller flere alternativer

- Avhengig av vertsmaskiner i nettverket.
- Kommer an på om NAT brukes.
- 1
- Så mange du vil.



Maks poeng: 1

2.9 Protokoller

Hvilke protokoll(er) bruker tjenesten?

Flytt hver tjeneste til riktig protokoll.

HTTP	
IMAP	
DASH	
DNS	UDP
DHCP	

Maks poeng: 5

2.10 NAT

Hvilken tjeneste tilbyr Network Address Translation (NAT)?

Velg et eller flere alternativer

- Den gjør det mulig for mange enheter på et lokalt nettverk å dele én ekstern/offentlig IP-adresse. ✓
- Den kringkaster hvilket portnummer som benyttes av en bestemt tjeneste.
- Den gjør det lettere for maskiner på Internett å koble seg på maskiner i det lokale nettverket.
- Den oversetter mellom MAC-adresser og IP-adresser.

Maks poeng: 2

2.11 Content Delivery Network

Hvilke av disse påstandene er riktige for et Content Delivery Network (CDN)?

Velg et eller flere alternativer

- Den øker sikkerheten siden den virker som en brannmur mot tjeneren som har originaldata.
- Den kan redusere forsinkelsen for brukeren ved å flytte data nærmere brukeren. ✓
- Den kan avlaste tjeneren som har originaldataene dersom det er mange samtidige brukere. ✓
- Den sparer maskinvare og energi ved å virtualisere nettverkstjenestene.

Maks poeng: 2

2.12 DNS

Hva er DNS-prefetching?

Velg et eller flere alternativer

- En tjeneste mellomlagrer MAC-adressen til webtjenere for raskt oppslag.
- En nettleser slår opp IP-adressen på alle domenenavn (URLer) den finner i et webdokument for å spare tid i tilfelle brukeren trykker på linken. ✓
- En hjemmerouter lagrer DNS-oppslag slik at brukeren ikke behøver å kontakte en rot tjener.
- En tjener mellomlagrer hjemmesider, slik at forespørselen ikke trenger å gå helt til kilden.

Maks poeng: 1

3.1 Tall på ulike former

Til venstre er vist fire ulike tall og de er gitt på ulike former. Sorter disse verdiene etter størrelse og bruk datamusen til å flytte dem til riktig plass til høyre.

2013 (oktalt)	<input type="text"/>	størst
40E (hex)	<input type="text"/>	nest størst
1031 (desimalt)	<input type="text"/>	nest minst
10000001001 (binært)	<input type="text"/>	minst

Maks poeng: 4

3.2 Binærtall

Hvordan lagres verdien **57** i én byte (dvs 8 bit)? Skriv bit-ene i hver sin rute.

<input type="text"/>	(0)	<input type="text"/>	(0)	<input type="text"/>	(1)	<input type="text"/>	(1)	<input type="text"/>	(1)	<input type="text"/>	(0)	<input type="text"/>	(0)	<input type="text"/>	(1)
----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----

og hvordan lagres verdien **-57** når vi lagrer tall som **2-er-komplement**?

<input type="text"/>	(1)	<input type="text"/>	(1)	<input type="text"/>	(0)	<input type="text"/>	(0)	<input type="text"/>	(0)	<input type="text"/>	(1)	<input type="text"/>	(1)	<input type="text"/>	(1)
----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----	----------------------	-----

Maks poeng: 4

3.3 Assemblerkode 1

	start	INP	
		STA	x
		INP	
		STA	y
		LDA	x
		SUB	y
		OUT	
	slutt	HLT	
	x	DAT	0
	y	DAT	0

Hva skrives ut når denne koden kjøres og brukeren gir 7 og 11 som input?

Velg ett eller flere alternativer (men bare ett er riktig):

- Ingenting skrives ut
- 4
- 11
- 0
- 4
- 18



Maks poeng: 4

3.4 Assemblerkode 2

start	INP		
	BRZ	b	
	LDA	x	
	ADD	y	
	STA	x	
	BRA	start	
b	LDA	x	
	OUT		
slutt	HLT		
x	DAT	0	
y	DAT	1	

Hva skrives ut når dette programmet kjøres og brukeren gir verdiene **5 3 3 1 0** som input?

Velg ett eller flere alternativer (men bare ett er riktig):

- 4
- 0
- 7
- 12
- Ingenting skrives ut
- 5



Maks poeng: 4

3.5 Assemblerkode 3

start	INP			
	ADD	b		
	STA	b		
b	LDA	u		
	OTC			
	HLT			
u	DAT	83	# ASCII	'S'
	DAT	77	# ASCII	'M'
	DAT	84	# ASCII	'T'
	DAT	79	# ASCII	'O'
	DAT	84	# ASCII	'T'
	DAT	70	# ASCII	'F'
	DAT	76	# ASCII	'L'

Hva skrives ut i dette programmet når bruker gir **6** som input?

Velg ett eller flere alternativer (men kun ett er riktig):

- 83
- S
- 6
- L
- Ingenting blir skrevet ut
- 512



Maks poeng: 4

3.6 Maskinkode

Anta at minnet i LMC-maskinen inneholder disse verdiene

0	901
1	310
2	110
3	311
4	111
5	311
6	111
7	210
8	902
9	0
10	0
11	0

og at programtelleren («Program counter») er **0**. Hva skrives ut når koden kjøres og brukeren angir **8** som input?

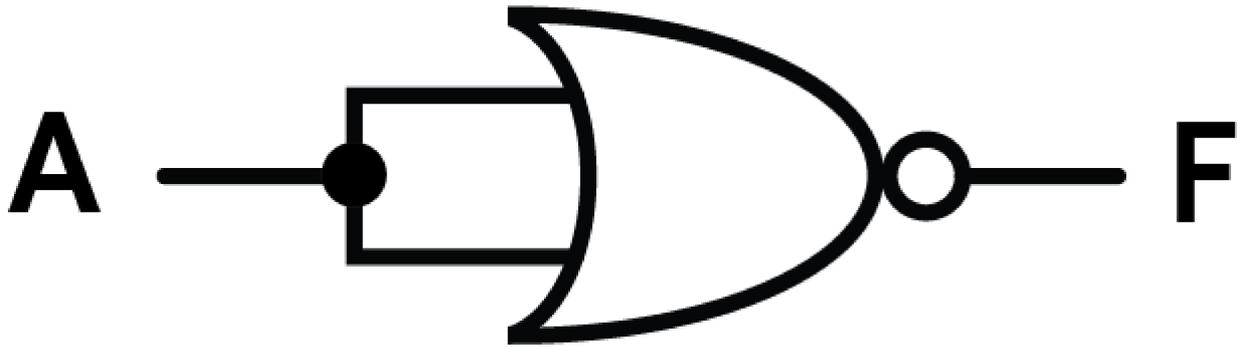
Velg ett eller flere alternativer (men bare ett er riktig):

- 56
- 24
- 64
- 8
- Ingenting blir skrevet ut
- 0



Maks poeng: 5

4.1 Portanalyse



Hva er funksjonsuttrykket til porten over? (Det kan være flere riktige svar.)

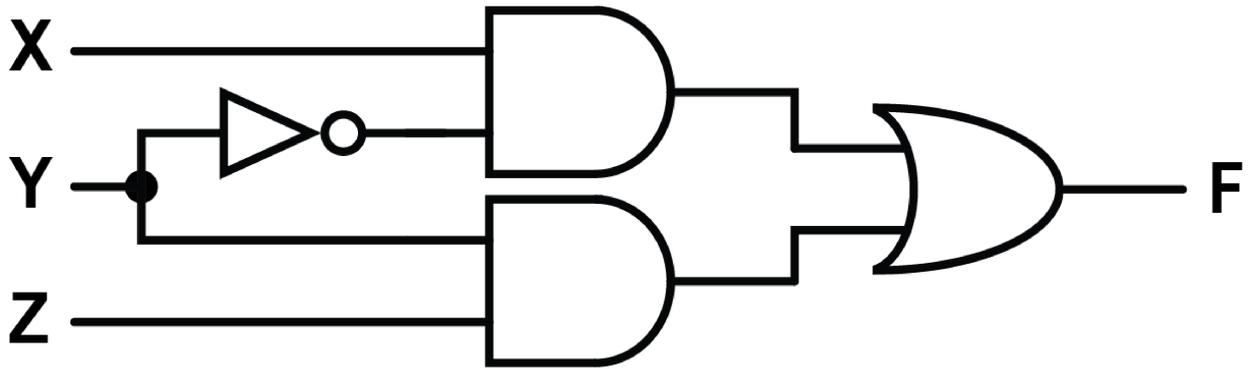
Velg ett eller flere alternativer:

- $F = 1$
- $F = 0$
- $F = A+B$
- $F = AB'$
- $F = A'$
- $F = AA'$
- $F = (A+A)'$
- $F = AA$



Maks poeng: 3

4.2 Kretsanalyse



Hva er funksjonsuttrykket for kretsen over?

Velg ett eller flere alternativer

- $F = x + y + z$
- $F = xyz$
- $F = x' + y + z'$
- $F = x' + z'$
- $F = xy + yz$
- $F = xz + y'$
- $F = xy' + zy$
- $F = xy' + yz$



Maks poeng: 7

4.3 Cache-miss

Anta at prosessoren har 100 instruksjoner igjen å utføre. Det tar én klokkesykel pr instruksjon, og man regner med å ha en minneaksessering på 80% og med cache-miss på 50%. En cache-miss fører til en total tidsbruk på 20 klokkesyklar. Cache-hit bruker total én klokkesykel. Hva er total antall gjenstående klokkesyklar?

Velg ett alternativ:

- 1000
- 860
- 950
- 800
- 1050
- 840
- 1620
- 820



Maks poeng: 7

4.4 Godt og blandet

Merk av hvilke utsagn som er sant eller usant.

NB! Det er ikke mulig å fjerne avkrysning, kun omgjøre mellom sant og usant når du først har krysset av. Så vær sikker på at du vil svare før du krysser av.

Er utsagnene sant eller usant?

	Sant	Usant
Kan man ha to innganger på en inverter?	<input type="radio"/>	<input checked="" type="radio"/>
Kan man dele en instruksjon inn i flere enn fire subinstruksjoner?	<input checked="" type="radio"/>	<input type="radio"/>
$F = xy$ er en NOR-funksjon	<input type="radio"/>	<input checked="" type="radio"/>
Klokkeperioden bestemmer frekvensen	<input checked="" type="radio"/>	<input type="radio"/>
Teknologisk utvikling bidrar til at man kan lage mindre transistorer	<input checked="" type="radio"/>	<input type="radio"/>
Det er register i CPU som lager klokkesignalene	<input type="radio"/>	<input checked="" type="radio"/>
Er $a'b'$ lik $(ab)'$?	<input type="radio"/>	<input checked="" type="radio"/>
Kan man ha fem innganger på en XOR port?	<input checked="" type="radio"/>	<input type="radio"/>
Det er mer effektivt å bruke RAM enn Cache	<input type="radio"/>	<input checked="" type="radio"/>
Kan man ha tre innganger på en AND-port?	<input checked="" type="radio"/>	<input type="radio"/>
Kan man ha to enere i mente ut av en-bits full-adder?	<input type="radio"/>	<input checked="" type="radio"/>
En sannhetsverditabell kan ha flere riktige funksjonsuttrykk	<input checked="" type="radio"/>	<input type="radio"/>
Komplikasjoner i en 4-trinns pipeline gjør at vi ikke kan få 4 ganger så rask prosessering	<input checked="" type="radio"/>	<input type="radio"/>
Binær (halvadder) addisjon av $0+1$ gir 1 i mente-ut	<input type="radio"/>	<input checked="" type="radio"/>

4.5 ALU

Hvilke av disse utsagnene stemmer for en ALU?

Velg ett eller flere alternativer

- ALU kan utføre matematiske operasjoner ✓
- ALU bestemmer antall trinn i pipeline
- ALU er en del av RAM
- ALUen er en del av CPUen ✓
- ALU kan kunn utføre logiske operasjoner
- ALU bestemmer klokkehastigheten til en CPU
- 1-bits ALU inneholder en seriell-adder
- Styresignalet i ALU kommer direkte fra instruksjonen ✓
- ALU er forkortelse for ALUminium som er neste generasjons superdatamaskiner
- Pipeline ligger i ALUen

Maks poeng: 3