

i Informasjon

Exam IN1020 autumn 2018

Time

12th December, 14:30-18:30

The teachers will visit the venue from 15:30.

The problems

The problems are multiple choice problems in which you may select as many alternatives as you like. Some problems will have several correct alternatives while others will have only one. Every problem will have at least one correct alternative. You will obtain points by selecting a correct alternative, and you will lose point if you choose a wrong one. However, you will never obtain less than zero points on any problem.

Permitted aids

- Any written or printed material.
- A calculator (battery-driven, with no communication); in addition, a calculator will be available in the Inspira system.

1(a) Porter / Kretsanalyse

The functional expression for this circuit is:

Select one or more alternatives:

$F = \bar{a} \cdot \bar{b}$

$F = \bar{a} + \bar{b}$ ✓

$F = \overline{a + b}$

$F = \overline{(ab)}$ ✓

Maximum marks: 5

1(b) K-map / Funksjonsuttrykk

Which of these interpretations of the Karnaugh diagram are valid:

Select one or more alternatives:

- $F(a, b, c, d) = \sum(0, 1, 5, 7, 9, 11, 13)$ ✓
- $F(a, b, c, d) = ab\bar{c}d + \bar{a}\bar{b}\bar{c} + \bar{a}bd + \bar{a}bd$ ✓
- $F(a, b, c, d) = d(a \oplus b \oplus c) + \bar{c}d\overline{(a \oplus b)} + \bar{a} \cdot \bar{c}(b \oplus d)$ ✓
- $F(a, b, c, d) = \bar{c}d + \bar{a}bd + \bar{a}bd + \bar{a}\bar{b}\bar{c}$ ✓
- $F(a, b, c, d) = ad(b\bar{c} + \bar{b}) + \bar{a}(\bar{b}\bar{c} + bd)$ ✓
- $F(a, b, c, d) = b\bar{c}d + \bar{a}d(c \oplus b) + \bar{a}\bar{b}\bar{c} + \bar{a}bd$ ✓

Maximum marks: 10

1(c) Godt og blandet

Please match the values:

	False	True
The ALU alone decides the speed of a pipeline.	<input checked="" type="radio"/>	<input type="radio"/>
The ALU and the CPU are the same unit, but with different clock speeds.	<input checked="" type="radio"/>	<input type="radio"/>
In a ripple subtraction circuit we may only use full-adders.	<input type="radio"/>	<input checked="" type="radio"/>
The technological development enables us to create bigger registers on a microchip.	<input type="radio"/>	<input checked="" type="radio"/>
Max-term denotes the maximum numbers of expressions that may be interpreted from a Karnaugh diagram.	<input checked="" type="radio"/>	<input type="radio"/>
In case of a cache miss, data must be read from RAM.	<input type="radio"/>	<input checked="" type="radio"/>
One solution for avoiding data hazards is to connect the output of the first bit ALU to the input of the next bit ALU.	<input checked="" type="radio"/>	<input type="radio"/>

Maximum marks: 10

2(a) Binære tall 1

The value 30_{10} (i.e., 30 in the decimal system) may also be represented in other number systems. Which of the following values are equal to 30_{10} ?

Select one or more alternatives:

- 42_7 ✓
- 1000_3
- 111_5
- 11110_2 ✓

Maximum marks: 3

2(b) Binære tall 2

A byte contains these bits:

1	1	0	0	1	0	0	0
---	---	---	---	---	---	---	---

Which values may be represented by these bits?

Select one or more alternatives:

- 56 ✓
- 148
- 72
- 200 ✓
- 149

Maximum marks: 3

2(c) Maskinkode 1

start	INP	
	STA	50
	ADD	50
	ADD	50
	OUT	
slutt	HLT	

What is printed when this code is run and the user enters **7** as input?

Select one or more alternatives:

- 21
- 0
- 50
- Nothing is printed.
- 7



Maximum marks: 4

2(d) Maskinkode 2

start	LDA	x
	BRZ	slutt
	SUB	y
	STA	x
	INP	
	STA	w
	LDA	z
	SUB	w
	STA	z
	BRA	start
slutt	LDA	z
	OUT	
	HLT	
w	DAT	0
y	DAT	1
x	DAT	3
z	DAT	100

What is printed when this code is run and the user enters the three values 1, 2 and 3 as input?

Select one or more alternatives:

- 106
- 100
- 94
- 6
- Something else



Maximum marks: 4

2(e) Maskinkode 3

Assume that the memory contains these values:

0:	901
1:	805
2:	508
3:	902
4:	000
5:	108
6:	308
7:	600
8:	000

Assume also that the *program counter* (also called *location counter*) contains **0**. What is printed when we start the processor and the user enters the values **10**, **1** and **-2** as input?

Select one or more alternatives:

- 11
- 2
- 0
- 2
- Nothing is printed



Maximum marks: 4

2(f) Maskinkode 4

start	INP	
	BRZ	slutt
	BRP	k
	BRA	start
k	:	
	BRA	start
slutt	LDA	x
	OUT	
	HLT	
x	DAT	0
y	DAT	1

a	LDA	x
	ADD	1
	STA	x

b	LDA	1
	ADD	x

c	LDA	x
	ADD	y
	STA	x

d	ADD	x
	STA	x

e	ADD	y
	STA	x

This program (in the thick red frame) shall read several numbers. The last number is **0**, and no other 0-s are given. The program shall count how many positive numbers (i.e., numbers >0) there are, and print that result. Negative numbers are ignored. The sequence

3 3 4 -1 -2 5 0

shall produce the answer **4** since there are 4 numbers >0.

The program is missing some instructions where there is a colon (:). Which instructions are missing?

Select one or more alternatives:

- Alternative a
- Alternative b
- Alternative c
- Alternative d
- Alternative e



Maximum marks: 4

2(g) Moores lov

Moore's law says that

Select one or more alternatives:

- The number of cores in a CPU doubles every second year.
- The size of memory (RAM) doubles every second year.
- The price of a computer is halved every second year.
- The clock frequency of computers doubles every second year.
- The number of transistors in an integrated circuit doubles every second year. ✓

Maximum marks: 3

3(a) TCP og UDP

Which of these services are offered both by TCP and UDP

Select one or more alternatives:

- Congestion control
- Flow control
- Reliability
- Multiplexing over one IP-address (ports) ✓
- Checksum (data integrity) ✓

Maximum marks: 2

3(b) Subnet - Kringkastingsadresse

A valid IP-address in a subnet is 134.1.98.45. The netmask to the subnet is 255.255.248.0. What is the broadcast address for this subnet?

Select one alternative:

- 134.1.103.255 ✓
- 134.1.99.255
- 134.1.98.255
- 134.1.111.255

Maximum marks: 2

3(c) ARP-tabell

What is an ARP table?

Select one alternative:

- A list of possible routes an IP-packet can take through the Internet.
- A list, maintained by a host on a subnet, that contains IP-addresses and MAC-addresses to other hosts on the same subnet.
- A list of IP-addresses and port numbers used to enable private addresses on a subnet to connect to other machines on the Internet (outside own LAN)
- A table that shows when different ARP-packets are ready to be sent

Maximum marks: 1

3(d) Private IP-adresser

Which of these IP-addresses are so-called "private IP-addresses" that can not be used externally on the Internet?

Select one or more alternatives:

- 192.168.12.34
- 10.0.1.15
- 129.240.171.52
- 8.8.8.8

Maximum marks: 2

3(e) IPv6

What is the primary motivation for upgrading from IPv4 to IPv6?

Select one alternative:

- More ports will be available per IP-address.
- Increase the number of globally addressable IP-addresses. ✓
- Makes it harder to do a "man-in-the-middle" attack.
- Easier to connect IP-addresses and MAC-addresses.

Maximum marks: 2

3(f) Mulige IP-adresser i subnett

A subnet is defined by 192.168.0.0/30 (CIDR notation). How many valid IP-addresses can be assigned to hosts in the subnet?

Select one alternative:

- 16
- 254
- 255
- 2 ✓

Maximum marks: 2

3(g) Klient-tjener

What characterises a client-server access model?

Select one or more alternatives:

- A server listens for requests and delivers a service when a request is received. ✓
- Many independent nodes cooperate to deliver a service.
- A client initiates the exchange by connecting to a server and request a service. ✓
- There is no centralized control over the service.

Maximum marks: 2

3(h) Pakkeswitching

What is true for a packet switched network?

Select one or more alternatives:

- A dedicated connection is established between the sender and receiver.
- Data for transmission is split into smaller parts that are sent independently in the network. ✓
- Capacity has to be reserved along the entire path.
- Different packets can take different paths from sender to receiver. ✓

Maximum marks: 2

3(i) Metningskontroll

The task of congestion control is to...

Select one or more alternatives:

- ... make sure that the resources in the network are shared equally between the data flows. ✓
- ... count the number of data streams over a network interface.
- ... prevent that the receiver gets more data than it can accept.
- ... prevent that the network traffic stops because of overload (congestion collapse). ✓
- ... send data packets from the correct port in a router.

Maximum marks: 2

3(j) Content Delivery Network

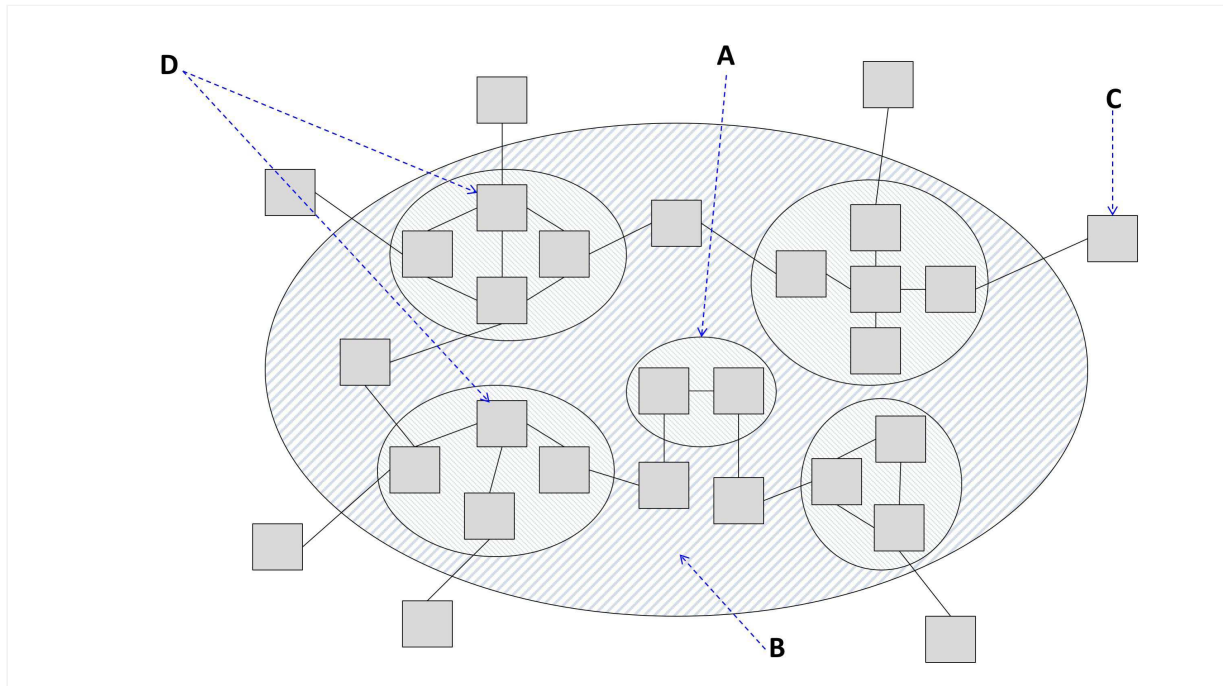
Which alternatives are positive effects of a Content Delivery Network?

Select one or more alternatives:

- Can prevent data breaches.
- Reduces the latency for accessing content by moving the data closer to the user. ✓
- More machines lead to increased power consumption.
- Prevents overload on the server by distributing the workload on multiple machines. ✓
- Saves resources in the backbone network. ✓
- Makes sure that a government or company can not control the network.

Maximum marks: 3

3(k) Topologi i Internett



What is the correct name on the labels?

Select one alternative:

- A) Server, B) Gateway, C) Intermediate system, D) Subnet
- A) Repeater, B) Bridge, C) Gateway, D) Gateway
- A) Subnet, B) Network C) End system D) Intermediate system
- A) Gateway, B) Intermediate system, C) Router, D) End system



Maximum marks: 2

3(l) Linklaget

Which claims about the link layer are true?

Select one or more alternatives:

- Responsible for interpreting every bit at the receiver.
- The Link layer enables reliable communication between two devices on the local network. ✓
- Handles routing of the data traffic.
- Data units sent on the link layer is called packets.
- Responsible for dividing a bit stream into data frames. ✓
- Does error checking on data ✓

Maximum marks: 3

4(a) Sikkerhetsmål

Security services are essential in information security. Which of the following is defined as a security service:

Select one or more alternatives:

- Data origin authentication ✓
- Intrusion detection
- Biometrics
- Disk encryption
- Non-repudiation ✓
- Logging
- Availability ✓

Maximum marks: 1.5

4(b) Sikkerhetstiltak 1

Security controls may be categorized according to the *phase* a control is intended to work within. We may distinguish between *preventing* attacks, *detecting* ongoing attacks, or *correcting* for an attack that has occurred.

Select the correct category for each of the listed security controls:

	Detective contols	Corrective controls	Preventive controls
Restore from backup	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Network encryption	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Intrusion detection systems	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>

Maximum marks: 1.5

4(c) Sikkerhetstiltak 2

Which of the following are security controls that may help achieve confidentiality?

Select one or more alternatives:

- To provide good procedures for backing up all information.
- To ensure training of users to gain knowledge of how confidential information is to be processed. ✓
- To use cryptography to make information illegible for those who shall not have access. ✓
- To use access control to limit who and what is given access to a resource ✓

Maximum marks: 3

4(d) Brukerautentisering og passord

The IT department of the Parliament of Norway is about to prepare a new, common system for user authentication for all the Parliament's IT systems. They have decided to use passwords as authentication factor.

Developing a safe system and proper routines for managing and storing passwords is important in any system that involves user authentication with passwords. Below are four requirements that the Parliament have set for how passwords are managed in the system.

For each requirement, choose the most appropriate security control to make sure that you meet the requirement:

	Access control	Salting	Complex passwords	Hashing
Only authorized entities/individuals can read the password database.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Passwords are not readable in plain text form in the database.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
It should be difficult for attackers to crack passwords stored in the database, even when passwords are both salted and hashed.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Pre-computed hash tables can not be used for easy password cracking.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maximum marks: 4

4(e) Asymmetrisk kryptering og nøkkelutveksling

Erna and Siv are in the middle of the budget negotiations and collaborate on several digital documents. They have recently attended a course in information security, where they learned about asymmetric encryption (public key encryption). They agree to use asymmetric encryption for secure document exchange, and each of them holds a set consisting of a private and a public key.

A. Erna is going to send Siv a confidential document, which must be protect against access from others. Which key do Erna have to use to encrypt the document before sending it to Siv?

Select one alternative:

- Ernas's public key
- Ernas's private key
- Siv's public key
- Siv's private key

B. Siv has prepared a document to be approved and digitally signed by Erna before it is valid. Erna has been sent the digital document and will sign it using asymmetric encryption. Which key should Erna use when she does what is called *digital signing*?

Select one alternative:

- Ernas's private key
- Ernas's public key
- Siv's private key
- Siv's public key

C. In practical use of asymmetric encryption, there is a need for what we call *digital certificates*. What is the purpose of a digital certificate?

Select one alternative:

- To associate a public and a private key.
- To associate a user's identity with a certificate issuer.
- To associate a public key with the identity of its owner.
- To associate a certificate issuers and a public key.



Maximum marks: 6

4(f) Trusselmodellering

For simplicity, a small group of employees in a subdivision of the Ministry of Defense uses the same user ID and password to authenticate in a system for administrative procedures.

This group of employees has the superuser role in the system, which means they have extended privileges compared to the regular employee in the ministry. Among other things, they have the privilege to change and delete *all* stored documents and cases in the system.

Select the correct statements based on this scenario:

- As long as all the employees have the same privileges, there is no need of equipping each employee with an individual user identity.
- When events in the administrative procedure system can not be linked to an individual, it can be difficult to find and correct changes in the system due  for example, human errors.
- Even though employees have the same privileges, it is necessary to be able to associate events with individuals, and thus single users, to ensure accountability. 
- It is less likely that a password will be lost when there is only one common password to handle.

Maximum marks: 4

4(g) Tastelogger

The purpose of a *key logger* is to capture every keystroke a user is typing on a corresponding computer's keyboard. Below you find a number of statements about key loggers, where your task is to select the correct ones.

Select one or more alternatives:

- A key logger is a form of malicious spyware, which is usually spread as e-mail attachments. ✓
- A key logger is a common security control that is used to restore a user's history in a Unix shell.
- Laptops with integrated keyboard are not exposed to key loggers.
- Publicly available computers, with possible physical access from many different people, are exposed to key loggers. ✓
- Physical protection of computers is a suitable security control against key loggers. ✓

Maximum marks: 3

4(h) Risikoanalyse

Which **two key elements** are central when carrying out a risk analysis of an IT system?

Select two options:

- Attack vector used
- Likelihood of an event ✓
- Value-based threat identification
- Impact of an event ✓
- Possible rootkits

Maximum marks: 2