ℹ Informasjon

Exam IN1020 autumn 2022

Time

12th of December at 15:00-19:00
The lecturers will visit you some time after 16:00.

This examset

This examset consists of 4 sections, wheras each section gives upto 25 points and hence the total would be 100 points for this examset.

Section 1 regards Digital representation and assembler code
Section 2 regards Hardware and computer architecture
Section 3 regards Security.
Section 4 regards Computer network

Notice that each section has to be passed in order to pass the whole exam.

The problems

The problems are different variants of multiple choice questions. Some questions may have several correct answers, while others have only one. All will have at least one correct answer. You obtain points for each correct answer and lose points for wrong ones, but you will never get less than 0 points for any problem.

Permitted aids

Any written or printed material.
A simple calculator without possibilities for communication.
A calculator is available in the Inspera system.

ℹ Seksjon 1

You are now in section 1 - Digital representation and assembler code.

The problem number 1.1, 1.2, 1.3, 1.4, 1.5, 1.6 and 1.7 are part of section 1.

1.1 HTML Fargekoder

HyperText Markup Language (HTML) is a standard markup language used to format content in web browsers. HTML can for example be used to display text in various colors. In HTML, color is represented with a red (R), green (G) and blue (B) value - termed RGB. These are usually given in hexadecimal notation, where the first byte (from the left) is red, the second byte is green and the third byte is blue.

Consider the color 0xA07CD1. What are the values for red, green and blue?

Select one or more alternatives:

□ rød=148, grønn=124, blå=209

□ rød=148, grønn=128, blå=191

□ rød=160, grønn=124, blå=209 ✓

□ rød=160, grønn=134, blå=179

Maximum marks: 1

1.2 2'er Komplement - variant 2

Consider the following two bytes:

Byte A:

0	1	0	0	1	1	0	0

Byte B:

0	1	0	1	0	0	0	1

Calculate a new byte C that is the sum of these (C = A + B). What values can C have?

Select one or more alternatives:

- □ -67
- □ 126
- □ 157 ✓
- □ -99 ✓

Maximum marks: 3

1.3 Tallsystemer

Convert the following numbers to decimal (base 10) numbers.

a) 1101_2 Select alternative ⌄ (135, 13, Ingen av disse, 23, 51)

b) 113_4 Select alternative ⌄ (Ingen av disse, 13, 51, 23, 135)

c) 0x33 Select alternative ⌄ (23, 13, Ingen av disse, 135, 51)

d) 207_8 Select alternative ⌄ (135, 51, 13, Ingen av disse, 23)

Maximum marks: 5

1.4 Godt og Blandet

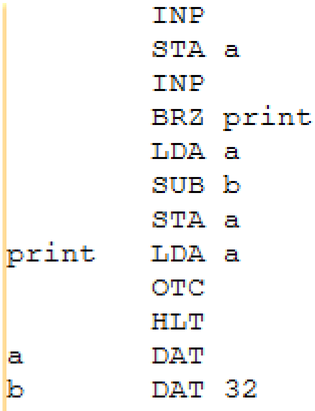
Check right or wrong for the following claims.

Please match the values:

	Riktig	Galt
A machine that is built on von neumann architecture has both code and data in the same memory.	○ ✓	○
DAT is a normal machine instruction that LMC understands.	○	○ ✓
One byte can represent a total of 512 unique values.	○	○ ✓
ASCII has room for 128 unique control- or character-symbols.	○ ✓	○
ASCII can easily be translated into UTF8 by setting the upper bit to zero.	○ ✓	○
Vector graphics is an appropriate format to store photos taken with a smart phone.	○	○ ✓
LMC has a total of three internal registers: the program counter, the instruction register and the accumulator.	○	○ ✓
LMC understands a total of 9 types of instructions.	○ ✓	○

Maximum marks: 5

1.5 LMC-1



```
        INP
        STA a
        INP
        BRZ print
        LDA a
        SUB b
        STA a
print   LDA a
        OTC
        HLT
a       DAT
b       DAT 32
```

When running this code, what will be printed when the user provides the following input data: **114** and **999**?

Select one or more alternatives:

□ 999

□ r

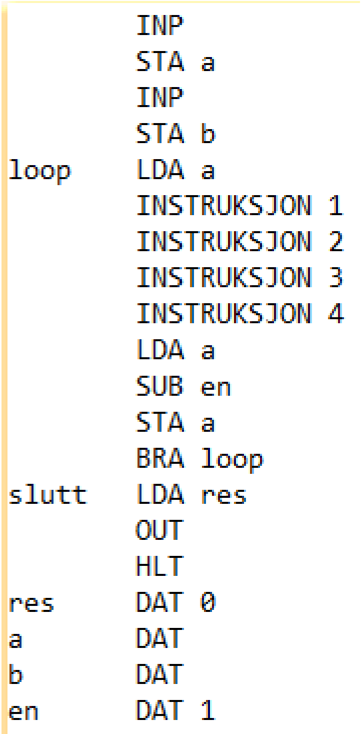
□ q

□ R ✓

□ T

Maximum marks: 3

1.6 LMC-2



```
        INP
        STA a
        INP
        STA b
loop    LDA a
        INSTRUKSJON 1
        INSTRUKSJON 2
        INSTRUKSJON 3
        INSTRUKSJON 4
        LDA a
        SUB en
        STA a
        BRA loop
slutt   LDA res
        OUT
        HLT
res     DAT 0
a       DAT
b       DAT
en      DAT 1
```

You are making a small program to multiply two numbers **a** and **b**, such that

res = a * b

You have written the program above, but some instructions are missing. Which ones?

Instruksjon 1:

Select alternative (BRZ slutt, BRP slutt, BRA slutt)

Instruksjon 2:

Select alternative (LDA b, LDA res, STA a, LDA a)

Instruksjon 3:

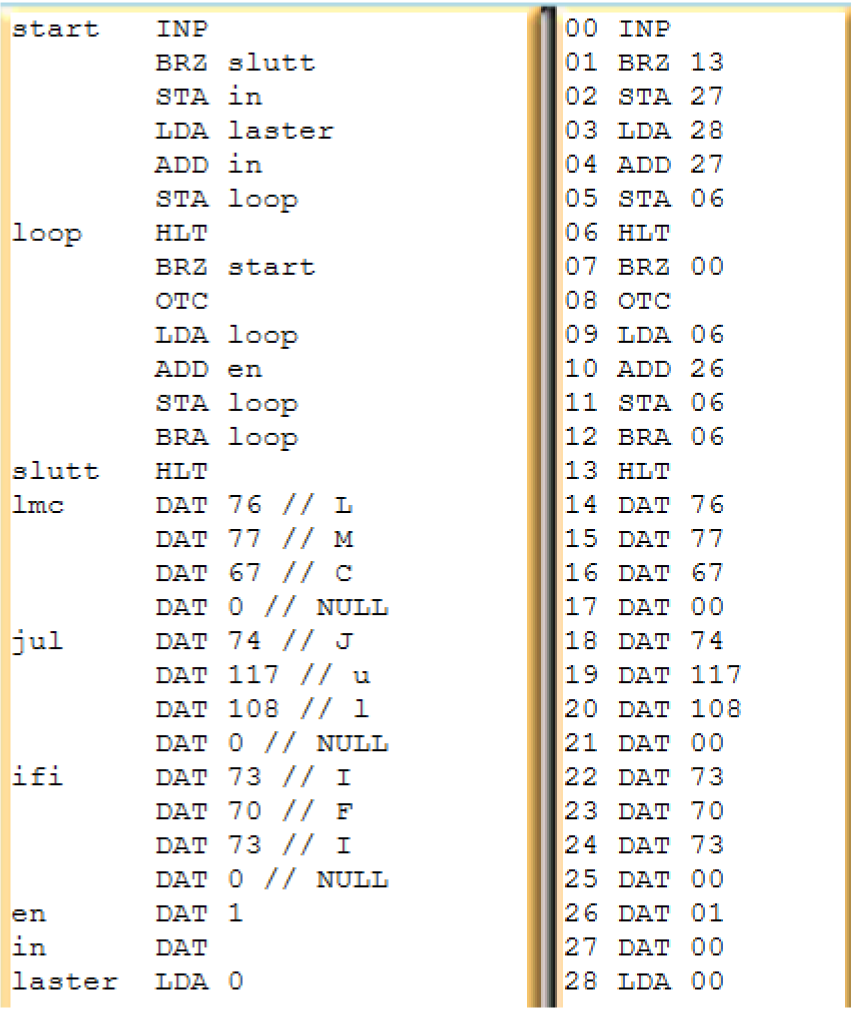
Select alternative (ADD en, ADD b, ADD a, ADD res)

Instruksjon 4:

Select alternative (STA a, STA res, Ingen instruksjon, STA b)

Maximum marks: 5

1.7 LMC-3



```
start   INP
        BRZ slutt
        STA in
        LDA laster
        ADD in
        STA loop
loop    HLT
        BRZ start
        OTC
        LDA loop
        ADD en
        STA loop
        BRA loop
slutt   HLT
lmc     DAT 76 // L
        DAT 77 // M
        DAT 67 // C
        DAT 0 // NULL
jul     DAT 74 // J
        DAT 117 // u
        DAT 108 // l
        DAT 0 // NULL
ifi     DAT 73 // I
        DAT 70 // F
        DAT 73 // I
        DAT 0 // NULL
en      DAT 1
in      DAT
laster  LDA 0
```

```
00 INP
01 BRZ 13
02 STA 27
03 LDA 28
04 ADD 27
05 STA 06
06 HLT
07 BRZ 00
08 OTC
09 LDA 06
10 ADD 26
11 STA 06
12 BRA 06
13 HLT
14 DAT 76
15 DAT 77
16 DAT 67
17 DAT 00
18 DAT 74
19 DAT 117
20 DAT 108
21 DAT 00
22 DAT 73
23 DAT 70
24 DAT 73
25 DAT 00
26 DAT 01
27 DAT 00
28 LDA 00
```

The code above writes out one and one character from a provided address until a "zero" is read from memory.

After providing the input "14", the user inputs "18" and then "0". What text is printed?

Select alternative ("LMC", "Jul", and nothing else., The program crashes., "IFI", "Jul", and nothing else., "IFI" and nothing else.)

What machine-code will we find on the label **loop** after the sixth instruction has been fully executed?

Select alternative (914, 518, 500, 514, 300, 906)

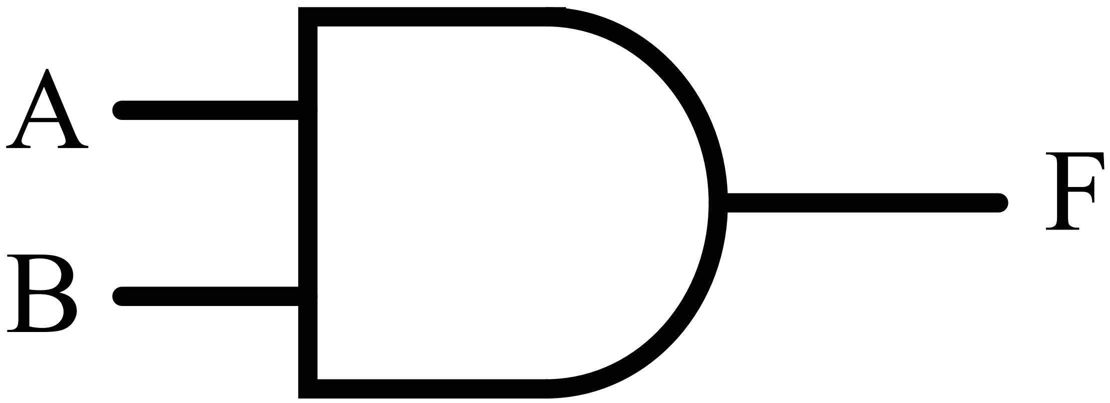
Maximum marks: 3

Seksjon 2

You are now in section 2 - Hardware and computer architecture.

The problem number 2.1, 2.2, 2.3, 2.4, 2.5 and 2.6 are part of section 2.

2.1 Gates



Which gate(s) is /are on the above figure:
Select one or more alternatives:

□ NOT-gate

□ NOR-gate

□ OR-gate

□ AND-gate ✓

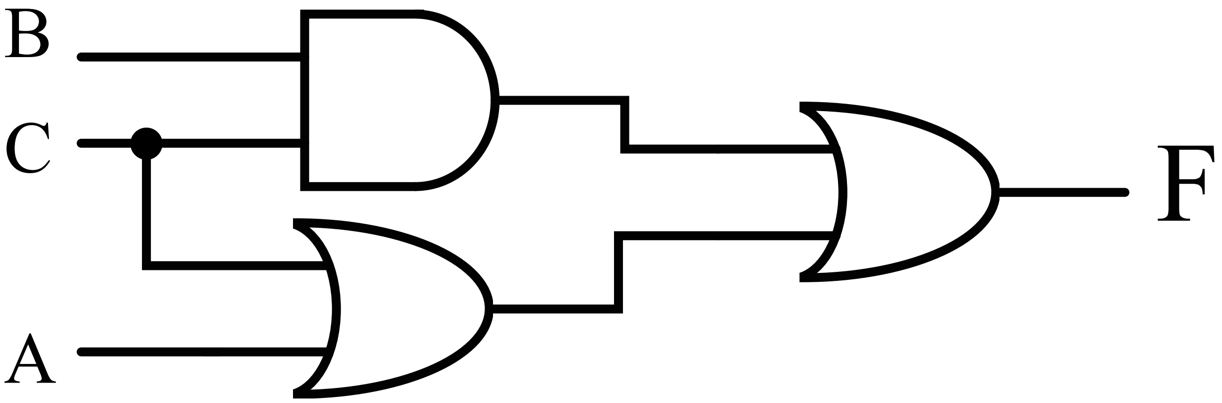
□ XOR-gate

□ XNOR-gate

□ NAND-gate

Maximum marks: 1

2.2 Kretsanalyse



The function F is given by:

Select one or more alternatives:

□ F = AC

□ F = ABC

□ F = A + BC

□ F = A + C ✓

□ F = C + AB

□ F = A + B + C

□ F = AB

□ F = C + A ✓

□ F = B + C

□ F = A + B

□ F = BC

□ F = B + AC

Maximum marks: 5

2.3 Cache

Assume that there are 3000 instructions left and that one instruction takes 1 clock cycle, except for any cache misses. Furthermore, you can assume that there will be 50% cache miss where it will take a total of 4 clock cycles for each instruction in cache miss.

What is the total time required?

Select one or more alternatives:

□ 15000

□ 8250

□ 5000

□ 9000

□ 3000

□ 10000

□ 7500 ✓

□ 13250

□ 5500

□ 6600

Maximum marks: 3

2.4 Godt og blandet H2022

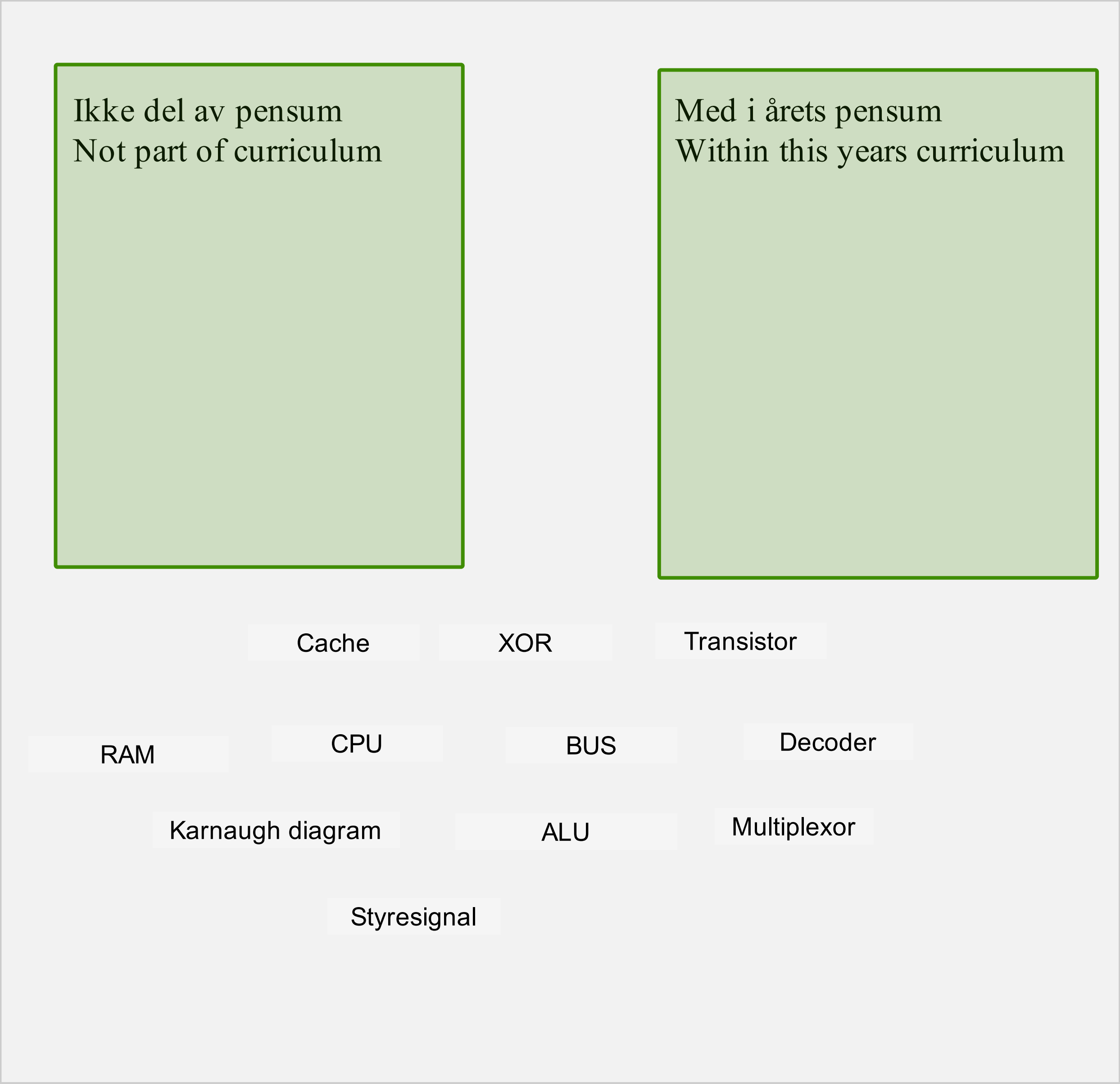
Please match the values:

	True	False
Transistor is a collection of current that makes 1 byte	○	○ ✓
Secondary memory is volatile memory	○	○ ✓
The ALU is situated right outside of the CPU	○	○ ✓
Cache-miss is when a part of the memory is broken	○	○ ✓
A register contains of many RAMs	○	○ ✓
A databus (BUS) transports information between the processor and other units	○ ✓	○
The technological evolution contributes to the fact that there will be less transistors on a chip	○	○ ✓
A full-adder can be used as a subtractor by adding a 1 to the carry-in	○	○ ✓
The clock-signal in a CPU is stored in RAM	○	○ ✓
A 64-bits ALU needs 65 elements of a 1-bit ALU	○	○ ✓

Maximum marks: 8

2.5 Pensum H2022

Which of these topics below are part of this years curriculum? Drag-and-drop the topics inn to the representative grey areas. It is possible to put the topics on top of each other.



Maximum marks: 3

2.6 Abstraksjonsnivå H2022

Place these elements in the correct order in regards to the abstraction level.

Highest level: Select alternative (Pipeline, Register, Transistor, STA 04)

Select alternative (Transistor, STA 04, Pipeline, Register)

Select alternative (Register, STA04, Pipeline, Transistor)

Lowest leve: Select alternative (Pipeline, STA 04, Register, Transistor)

Maximum marks: 5

Seksjon 3

You are now in section 3 - Security.

The problem number 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 and 3.7 are part of section 3.

3.1 Sikkerhetsmål

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

Select one or more alternatives:

□ Worm

□ Availability ✓

□ Integrity ✓

□ Two-factor authentication

□ Non-repudiation ✓

□ Access control

□ Firewall

□ Authorization

Maximum marks: 2

3.2 Sikkerhetstiltak: Konfidensialitet

Confidentiality is an essential requirement in Norwegian Privacy Act. Which of the following security services will ensure the confidentiality of personal data processed in an IT system:
Select one or more alternatives:

- □ Use of cryptography for data stored in the system ✓
- □ Provide for redundant services.
- □ Provide a backup of your data
- □ Provide a backup of your hardware
- □ Identify all the users of the IT system
- □ Use of perimeter defense ✓

Maximum marks: 2

3.3 Sikkerhetstiltak: Integritet

Integrity is an essential requirement in Norwegian Privacy Act. Which of the following security services will ensure the integrity of personal data processed in an IT system:
Select one or more alternatives:

- □ Encrypt all network traffic to, from and internally in the computer system. ✓
- □ Provide for redundant services.
- □ Keep all software well security updated ✓
- □ Ensure a backup copy of all the hardware
- □ Have good routines for access control in the IT-system ✓
- □ Identify all the users of the IT system

Maximum marks: 2

3.4 Autentisering

How can two-factor authentication with a combination of the authentication factors *Something you know* and *Something you have* for logging in help improve the security of an IT system?

Select one or more alternatives:

- □ It makes it more difficult for attackers to exploit user information leaked in e.g. phishing attacks. ✓
- □ This makes it unnecessary to further secure data stored in the IT system.
- □ It makes it difficult to succeed with so-called brute-force attacks. ✓
- □ It restricts what users are permitted to do in an IT system.

Maximum marks: 3

3.5 Symmetrisk kryptering

Symmetric encryption is one of several categories of encryption used in computer-based cryptography.

Which of the following statements about symmetric encryption are true and which are false?

	True	False
Can be used to ensure data confidentiality.	○ ✓	○
Can be used to ensure non-repudiation.	○	○ ✓
Is based on the use of a pair of cryptographic keys known as a public and a private key.	○	○ ✓
Safe exchange of the secret cryptographic key is a common security challenge.	○ ✓	○
Is used for encryption of secret messages.	○ ✓	○
Is used for so-called digital signature.	○	○ ✓
The sender and the receiver share one secret cryptographic key.	○ ✓	○
Symmetric encryption destroys the message so that it can never be decrypted.	○	○ ✓

Maximum marks: 4

3.6 Asymmetrisk kryptering

The company where you are employed has the need for strong security and authenticity for data and messages, and has introduced a separate, local public-key infrastructure (PKI). All employees have been assigned a cryptographic key pair, consisting of a private and a public key. Since you have passed the course IN1020, it will be your task to explain to your colleagues which keys are to be used for which operations.

For each operation below enter the correct key:

Key sender uses for signing (digital signature): Select alternative ⌄ (The recipient's public key, The sender's private key, The sender's public key, The recipient's private key).

Key recipient uses for validation (digital signature): Select alternative ⌄ (The sender's public key, The recipient's private key, The sender's private key, The recipient's public key)

Key sender uses for encryption (secret message exchange): Select alternative ⌄ (The recipient's public key, The sender's public key, The recipient's private key, The sender's private key)

Key recipient uses for decryption (exchange of secret message): Select alternative ⌄ (The sender's private key, The recipient's public key, The sender's public key, The recipient's private key)

Maximum marks: 3

3.7 Personvern og trusselmodellering

Viken County Council plans to introduce a new digital system for conducting and examining final written exams for upper secondary school students.

One of the solutions they are considering is a cloud service from an external IT provider, available to students, examiners and the school administration as a web application. Both the storage of data and the execution of the application take place on the supplier's computer equipment which is physically located in an EU country, while the exam itself is carried out in a browser on the schools' computers on the school's premises.

The examination system have to contain enough information to uniquely identify students and examiners (social security number, name, candidate id), the students' examianion answers, as well as the examination justification and grade for each individual exam answer the examinators give.

Task A)
The county council have to assess requirements for *personal data protection* (GDPR), and you are going to help them on their way. Consider the following statements, and mark the correct ones based on the use of an examination system as described above:

Select one or more alternatives:

□ The Personal Data Act sets requirements for information security; Confidentiality, integrity and availability. ✓

□ The county council is not legally responsible for information about pupils being processed in accordance with the Personal Data Act, as the examination system in its entirety is provided by an external company.

□ The county council can disregard the Personal Data Act for the processing of personal data, since it is absolutely necessary to process data about students in order to complete the exam.

□ Students have the right to gain insight in the personal data stored about them. ✓

Task B)
The county council's next concern is the *integrity* of the data stored and processed in the examination system. That e.g. exam answers or grades are changed by unauthorized persons. Which of the following might be a threat to integrity, given the information above:

Select one or more alternatives:

- □ Poor information security expertise at the company that supplies the exam solutio ✓
- □ *Man-in-the-middle attacks* on network traffic. ✓
- □ Unavailability attacks from outsiders with malicious intent.
- □ *Rootkit* installed on an exam examiner's computer. ✓
- □ Use of passwords as the only authentication factor. ✓
- □ Lack of redundant services.

Maximum marks: 9

i Seksjon 4

You are now in section 4 - Computer network.

The problem number 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 and 4.9 are part of section 4.

4.1 Klient-tjener

What characterises the access model client-server?
Select one or more alternatives:

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

Maximum marks: 2

4.2 Linjeswitching

What is true for a circuit-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.

□ Different packets can take different paths from sender to receiver.

□ Capacity has to be reserved along the entire path. ✓

Maximum marks: 2

4.3 Overføringshastighet

You want to download a 150 megabyte file, and the bandwidth on your Internet connection is 50 megabit per second down and 20 megabit per second up. What is the theoretical transfer time?

Select one alternative:

○ 3 seconds

○ 24 seconds ✓

○ 60 seconds

○ 150 seconds

○ 7,5 seconds

Maximum marks: 3

4.4 Punktnotasjon til CIDR

A computer has the IP-address: 172.16.100.18
The netmask is: 255.255.255.248
What is the IP-address to the machine written in CIDR notation?
Select one alternative:

○ 172.16.100.1/26

○ 172.16.100.18/26

○ 172.16.100.1/29

○ 172.16.100.18/29 ✓

Maximum marks: 3

4.5 Antall IP-adresser

A subnet as the network mask 11111111.11111111.11111111.11111000
How many valid IP-addresses can be allocated to hosts in the subnet?
Select one alternative:

○ 30

○ 32

○ 8

○ 6 ✓

○ 256

Maximum marks: 2

4.6 Broadcast-adresse

You have a machine with the following IP-address written in CIDR-notation: 172.16.10.112/26
What is the broadcast-address in this subnet?
Select one alternative:

○ 172.16.10.64

○ 172.16.10.63

○ 172.16.10.1

○ 172.16.1.255

○ 172.16.10.127 ✓

○ 172.16.10.255

Maximum marks: 5

4.7 IPv6

What is the primary motivation for upgrading from IPv4 to IPv6?
Select one alternative:

○ Makes it harder to do a "man-in-the-middle" attack.

○ More ports will be available per IP-address.

○ Easier to connect IP-addresses and MAC-addresses.

○ Increase the number of globally addressable IP-addresses. ✓

Maximum marks: 2

4.8 Transportlagsprotokoller

The transport layer in the TPC/IP stack contains mainly two protocols: TCP and UDP.

Which of the following statements about protocols in the transport layer are true and which are false?

	False	True
The transport layer only works on end-to-end and has no knowledge on how data is transmitted over the network.	○	○ ✓
Both TCP and UPD makes sure that data is delivered in-order.	○ ✓	○
TCP is a connection-oriented protocol.	○	○ ✓
TCP is the most used of the two protocols in the transport layer.	○	○ ✓
Congestion Control makes sure that the capacity in the network is shared on all connections.	○	○ ✓
UDP is a lightweight protocol and is therefore well suited to transfer large files.	○ ✓	○
Flow control makes sure that TCP does not transmit data faster than capacity in the network.	○	○ ✓
It is not possible to use encryption on the application layer when UDP is used.	○ ✓	○

Maximum marks: 4

4.9 HTTP-streaming

Which statements are correct with regards to streaming over HTTP?
Select one or more alternatives:

□ Streaming over HTTP only uses UDP to transfer the video.

□ With HTTP-streaming you must buffer the entire video before playback can start.

□ It is the client that descides which qualirt layer to download, not the server. ✓

□ Video is divided in small segments and different quality layers. ✓

Maximum marks: 2