Informasjon

UNIVERSITY OF OSLO
The Faculty of Mathematics and Natural Sciences
Written examination in IN1020
FALL 2023
Duration: December 11, 09:00-13:00
Permitted materials: All printed and written materials, approved calculator.
A calculator is available in Inspera (see at the bottom of the page).
It is important that you read the entire front page before you start answering the exam questions.
If you wish to zoom in on the question set, hold down ctrl and press + or - on the numeric keypad.

The lecturers will make a round from 10:00.

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 assembly code
Section 2 regards Hardware and computer architecture
Section 3 regards Security.
Section 4 regards Computer network

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

The questions

The question 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.

Available resources in Inspera

- A simple calculator
- Ascii table

Seksjon 1

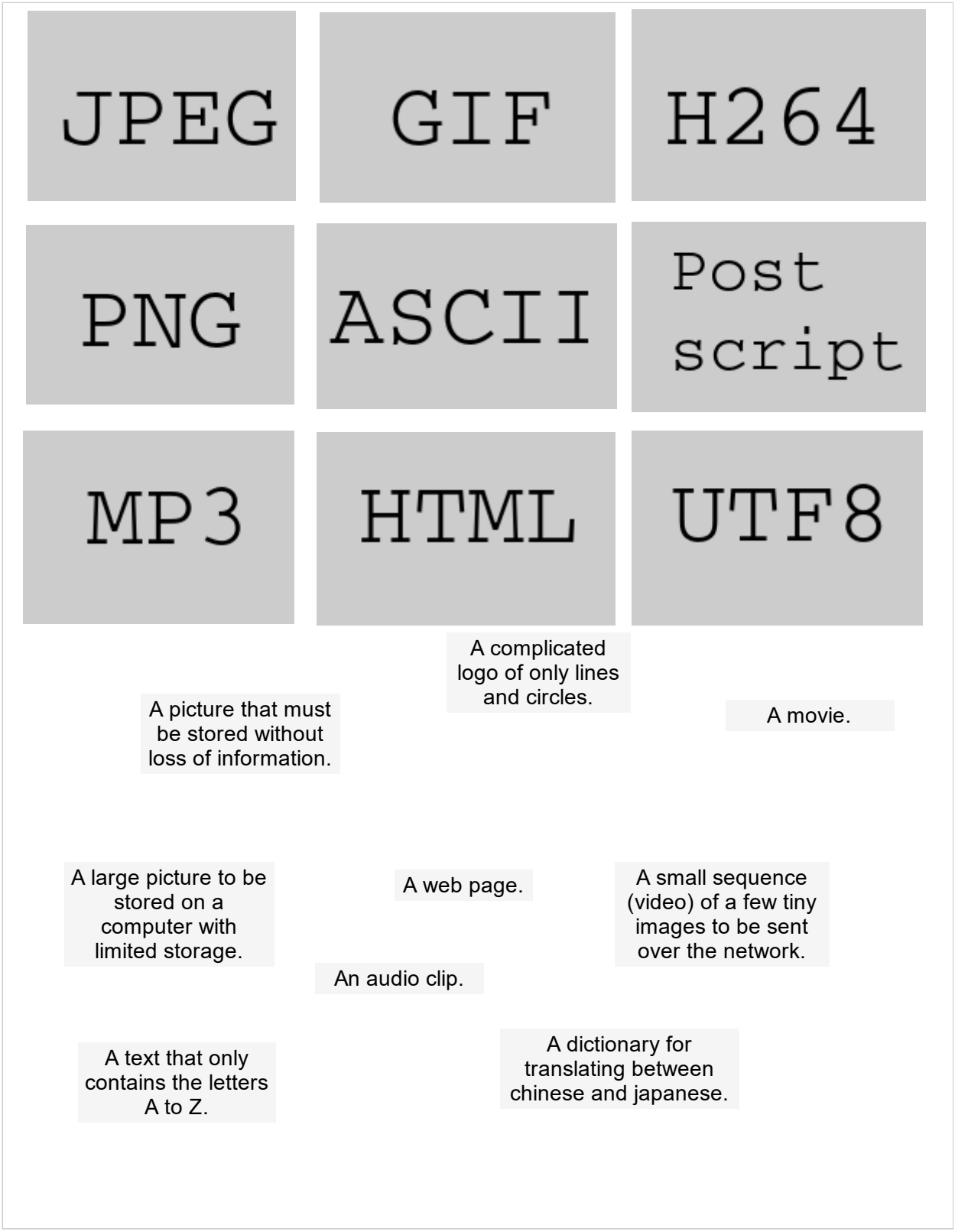
You are now in section 1 - Digital representation and assembler code.

The problem number 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8 and 1.9 are part of section 1.

1.1 Dataformater

The image below contains descriptions of various objects that can be stored in a computer. Drag the descriptions to the appropriate storage format.

Select one alternative:



Maximum marks: 4.5

1.2 2'er Komplement

Consider the following byte:

1	0	1	0	1	1	0	0

What values can it represent?
Select one or more alternatives:

- [ ] -45
- [ ] 132
- [ ] -30
- [ ] -68
- [ ] 190
- [ ] 172
- [ ] -84

Maximum marks: 2

1.3 Filtillatelser

User			Group			Other		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute

Alice has created a file "vacation.py" on her Linux machine. She has given the file the following (octal) permissions:

$$774_8$$

Consider the following statements. Which are right and which are wrong?

Please match the values:

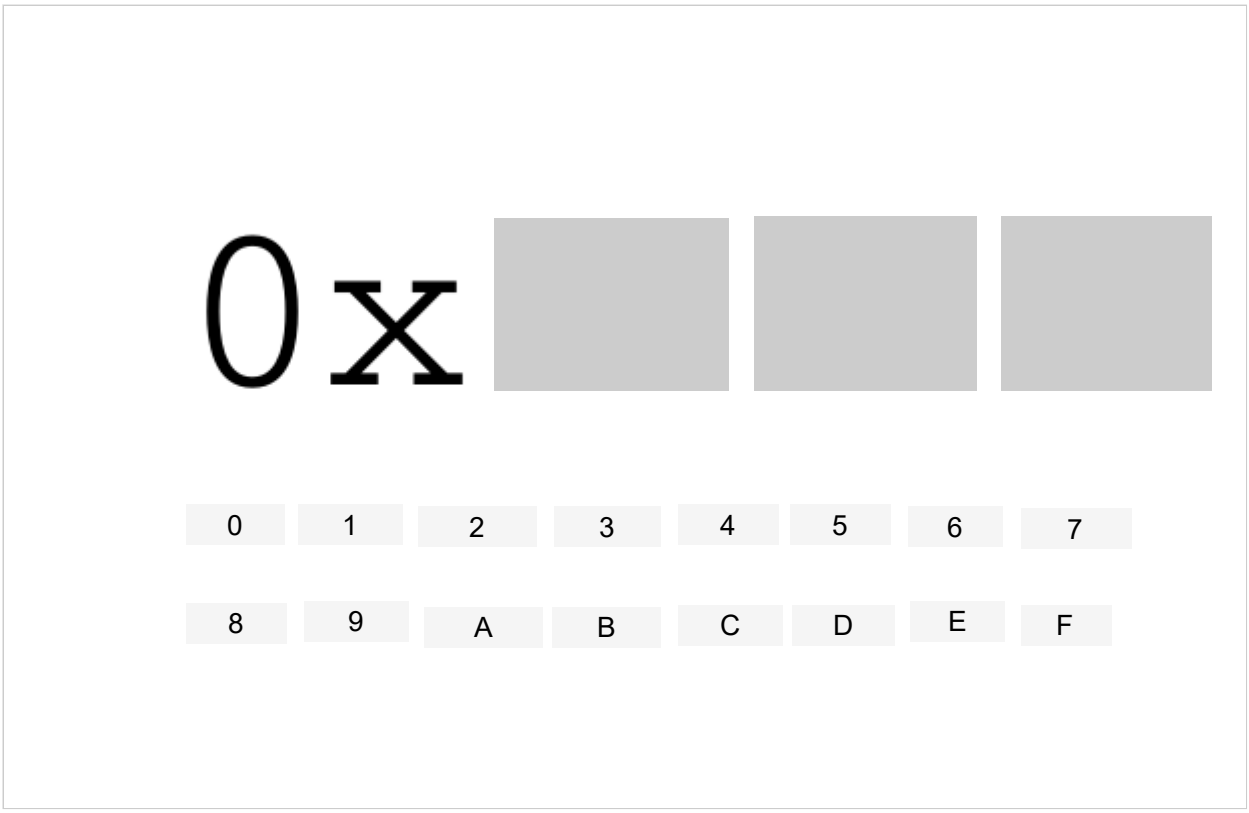
	Riktig	Galt
Group owners can read and execute the file.	○	○
The file owner can read and write, but not execute the file.	○	○
Other users can only execute the file.	○	○

Maximum marks: 1.5

1.4 Konvertering

Convert 73_{10} to hexadecimal representation.

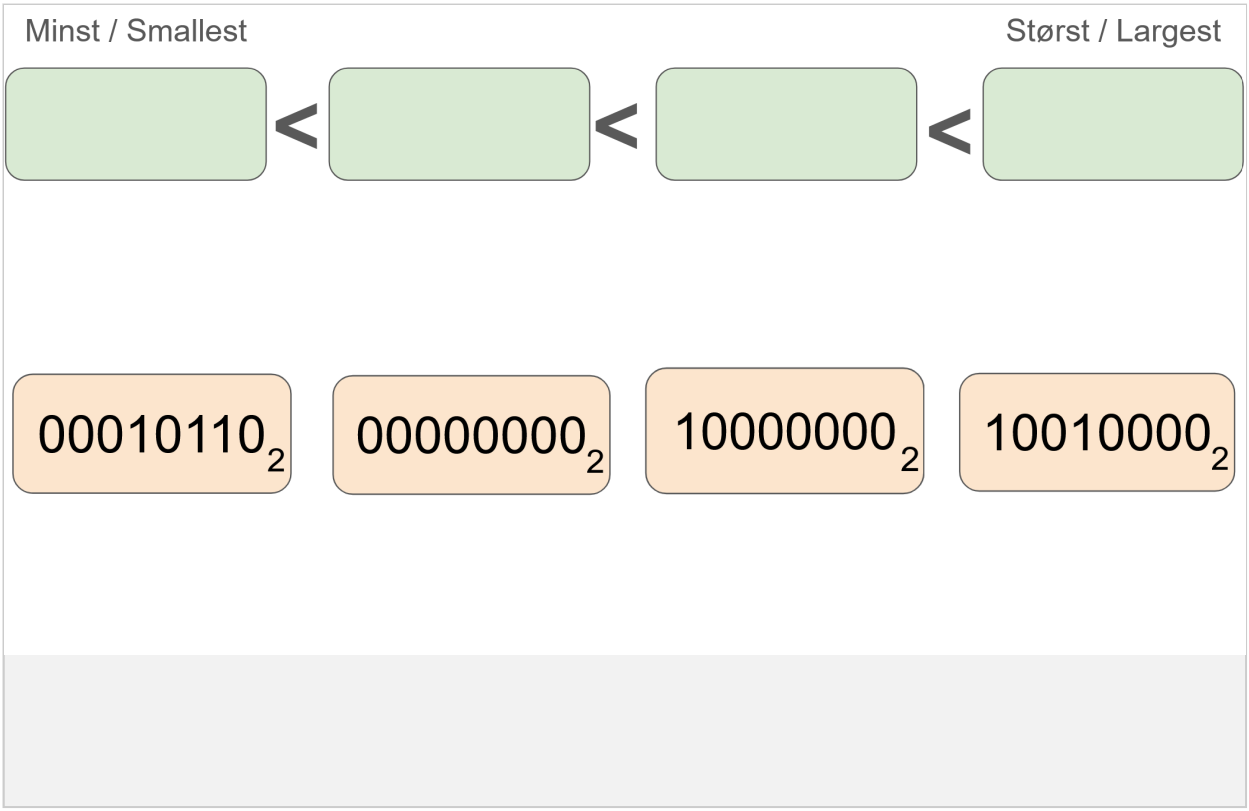
Drag the hexadecimal numbers to the right location.



Maximum marks: 3

1.5 Tallsortering

Arrange the following numbers in ascending order (from the smallest to the biggest):



Maximum marks: 5

1.6 LMC - Aritmetikk

What will LMC write to its output if the user gives as input the number **5** and then **1**?

```
          INP
          STA a
          INP
          ADD a
          SUB v
          OUT
          HLT
a         DAT
v         DAT 2
```

Select one alternative:

- 5
- 4
- -1
- 2
- -2

Maximum marks: 2

1.7 LMC - ASCII

Consider the following program for the LMC:

```
        LDA 90
        OTC
        LDA 91
        OTC
        LDA 90
        OTC
        LDA 92
        OTC
        HLT
```

Initialise the memory such that "**IFI2**" is printed when the code runs.



Maximum marks: 3

1.8 LMC - Programflyt

```
        INP
        BRP fin
        STA v
        SUB v
        SUB v
fin     OUT
        HLT
v       DAT
```

When this code is run on the LMC, the number **2** is written to the output. What can the user have provided as **input** to the LMC?

Select one or more alternatives:

- [ ] 2
- [ ] 4
- [ ] 3 and then 1
- [ ] -1
- [ ] -2
- [ ] 5

Maximum marks: 3

1.9 LMC - Selvmodifiserende kode

Consider the following code for the LMC:

```
start   INP                 00 INP
        ADD jump            01 ADD 03
        STA jump            02 STA 03
jump    DAT 600             03 DAT 600
        LDA a               04 LDA 10
        OTC                 05 OTC
        BRA start           06 BRA 00
        LDA b               07 LDA 11
        OTC                 08 OTC
        BRA start           09 BRA 00
a       DAT 35 // '#'       10 DAT 35
b       DAT 94 // '^'       11 DAT 94
```

What must the user provide as input to print out "**^^**" and then halt?

First input:

Second input:

Third input:

Maximum marks: 4

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 Kretsanalyse 23

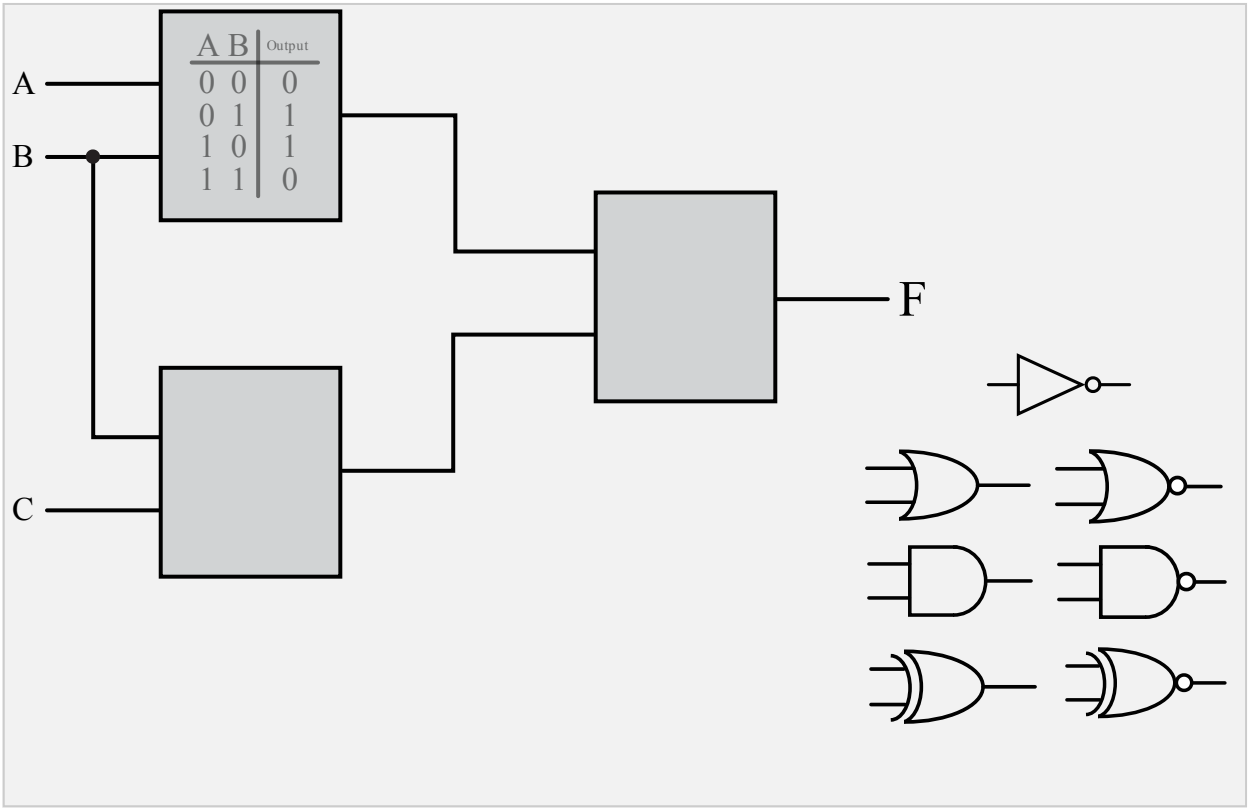
The circuit has the function

$$F = \overline{A'B + \overline{BC} + AB'}$$

Use the figure below to drag the correct gates into the gray boxes.

Hint! Do you remember the different symbols for a function expression that is inverted?
Hint! In one of the gray boxes, the truth table for the gate is provided.

Select one alternative:



Maximum marks: 5

2.2 Minne 23

In this task, you will work with a specific computer that has a hierarchy of memory elements consisting of registers, a four-level cache, RAM, and a flash drive. The machine's memory hierarchy is designed to handle various data access and write operations with varying speeds.

According to information provided by the manufacturer, the cache hierarchy has the following characteristics:

- Read operations take 5 clock cycles per level in the cache.
- Write operations take 10 clock cycles per level in the cache.

Furthermore, you have information about the other memory elements:

- Read operations from RAM have an access time of 50 clock cycles.
- Write operations to RAM have an access time of 100 clock cycles.
- Read operations from the Flash-drive take 760 clock cycles.
- Write operations to the Flash-drive take 1120 clock cycles.

HINT! For each memory access operation, note that the given values are an 'increased' access time.

Fill in the correct value in the fields (integers only):

(a) What is the total number of clock cycles in delay when you get a cache-hit on level 3?

clock cycles

(b) What is the total number of clock cycles it takes to write back a modified value in the pipeline to the RAM? clock cycles

(c) Assume that an optimization allows cache level 1 and 2 to be updated in parallel, while the remaining levels still require sequential updating. What will be the new total clock cycle delay for writing a value to RAM? clock cycles

(d) You are to calculate how many clock cycles it will take in total to execute 100 instructions where it takes 1 clock cycle per instruction without memory accessing. Since you are an expert in making good programs and know a lot about memory hierarchy, you have managed to arrange your instructions so that those accessing memory will always have a cache-hit at level 1. How many clock cycles will it all take when you expect 20% memory accessing? clock cycles

---

Maximum marks: 5

2.3 Abstraksjonnivå 23

Rank these 5 according to the abstraction levels they belong to relative to each other.

Highest	Select alternative (2 Inverters, Register, Logical values, Pipeline, Volt)
	Select alternative (2 Inverters, Pipeline, Volt, Register, Logical values)
	Select alternative (Logical values , Pipeline, 2 Inverters, Register, Volt)
	Select alternative (Logical values , Volt, 2 Inverters, Register, Pipeline)
Lowest	Select alternative (2 Inverters, Pipeline, Volt, Logical values , Register)

Maximum marks: 3

2.4 Godt og blandet 23

Which of these statements are true?

- [ ] The input and output of an inverter are physically connected.
- [ ] An XNOR is the inverted of an XOR.
- [ ] The output of a gate can be an input to several gates.
- [ ] You can create any function with only having INV and OR.
- [ ] ALU stands for Adder-Logic-Unit.
- [ ] It’s not possible to have an odd number of stages in a pipeline.
- [ ] There is only one output on a gate.
- [ ] There is only one type of transistors.

Maximum marks: 4

2.5 Datapath 23

Select the correct options for how an instruction is processed.
HINT! Do you remember the lecture on "Pipeline" and "circuits that drive the code"?

It is Select alternative (BUS, Cache, PC, ALU) that holds the address to the next instruction.

The current instruction is Select alternative (divided up, stored, added together, changed) in the decode phase.

The control signal to Select alternative (GPU, CPU, ALU, RAM, PC) comes from

Select alternative (WB-step, EX-step, IF-step, DE-step).

In the WB step, the result is sent through Select alternative (BUS, Clock, Inverter, CPU).

Maximum marks: 5

2.6 ALU 23

Given an ALU that is supposed to perform the following operations:

Add,
NAND,
XOR,
NOR,
XNOR

(a) How many bit(s) must the control signal be? ☐ **bit(s).**

(b) How confident are you with your answer in (a)?
Here you have 100% confidence to distribute among these alternatives. NOTE! You must fill out a number in all the alternatives. Where you are absolutely sure it is incorrect, you fill out 0, whereas where you are sure (or in doubt) you can fill out with a number between 1-100.

☐ **svaret er 1 bit**

☐ **svaret er 2 bit**

☐ **svaret er 3 bit**

☐ **svaret er 4 bit**

☐ **svaret er 5 bit**

Maximum marks: 3

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 Brudd på sikkerhetsmål

Specify which security service is typically violated as a result of each of the following attacks:
Please match the values:

	Confidentiality	Integrity	Availability	Authenticity
Ransomware	○	○	○	○
Identity theft	○	○	○	○
Forgery of website	○	○	○	○
DNS modification	○	○	○	○
DDoS attack	○	○	○	○
Spyware	○	○	○	○

Maximum marks: 3

3.2 Sikkerhetsmål og sikkerhetstiltak

You participate in an IT project that develops a new digital patient system for a group of private practicing psychologists. The system will contain patient information. Your task is to advise the project management on necessary security goals for the patient system.

a) First of all, you must identify security goals beyond CIT that must be taken care of in the patient system. Which of the following are security goals as defined in IN1020:
Select one or more alternatives:

- [ ] Authorization
- [ ] Intrusion detection
- [ ] Accountability
- [ ] Fire safety
- [ ] Privacy

b) Select the security controls you would recommend to ensure the confidentiality of data processed in the patient system:
Select one or more alternatives:

- [ ] Require two-factor authentication for login
- [ ] Log all activity which is performed in the patient system
- [ ] Use checksum algorithms for data transmitted over networks
- [ ] Training of all data processors
- [ ] Encrypt all data stored in the system
- [ ] Use of secure network protocols for data transfer
- [ ] Use different attack vectors
- [ ] Ensure proper procedures for data backup

c) Select the security goals you would recommend to ensure the best possible availability of data processed in the patient system:

Select one or more alternatives:

- [ ] Ensure proper procedures for data backup
- [ ] Use of secure network protocols for data transfer
- [ ] Log all activity which is performed in the patient system
- [ ] Use different attack vectors
- [ ] Conduct safety drills
- [ ] Install antivirus software
- [ ] Encrypt all data stored in the system
- [ ] Follow up on notifications about new vulnerabilities

Maximum marks: 5

3.3 Begrepsforståelse

Place the terms below together with the correct text. Note: Half of the terms will be left over.

Help

Computer worm	PKI	Risk
Digital certificates	Supply chain attacks	Asymmetric encryption
Zero-day vulnerability	Personal data	Hash-algorithm
Trojan	Values	Threat modeling

[ ] is a weakness that is not known to the provider of a service.

[ ] used to check data integrity.

[ ] is used to ensure the authenticity of public keys, as well as secure key distribution.

[ ] has both a useful and a harmful function.

[ ] has claims for confidentiality, integrity and/or availability, required by law

[ ] is a combination of the probability of an event and the consequence of the event.

Maximum marks: 3

3.4 Nettverkssikkerhet

During the development of a new website for a business, you are asked for advice as to whether it makes the most sense to use the protocol HTTP or HTTPS for communication over the network between the user and the business website.

Which of the following statements are true if you choose **HTTP** as the protocol:
Select one or more alternatives:

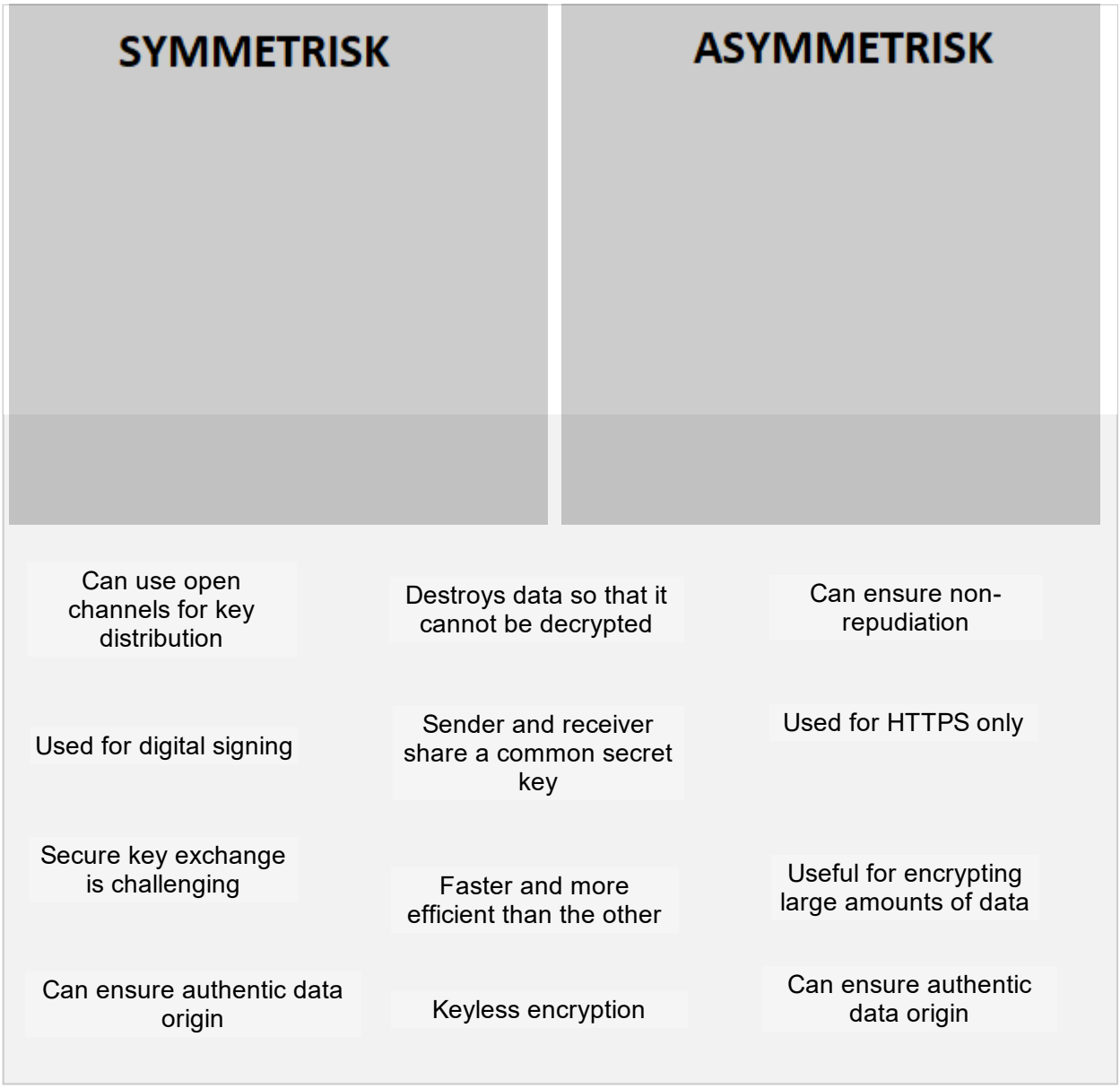
- [ ] If a user uses an encrypted connection from her computer to her wireless home router, both eavesdropping and modification of the data traffic between the user's browser and the company's web server is prevented.
- [ ] An unauthorized person will be able to manipulate data traffic between the company's web server and a user's browser.
- [ ] Integrity of data sent between the company's web server and a user's browser is ensured.
- [ ] An unauthorized person will be able to eavesdrop and read data traffic between the company's web server and a user's browser.

Maximum marks: 3

3.5 Egenskaper ved ulik type kryptering

Symmetric and asymmetric encryption are two types of encryption used in computer-based cryptography. In this task, you must associate the correct property with the correct encryption type.

Drag and drop statements about symmetric and asymmetric encryption to the correct frame. Note that not all statements fit into one of the frames, leave the ones you think don't fit.



Maximum marks: 4

3.6 Digitale signaturer

Jonas would like to conclude an digitally signed agreement (a document) with Trygve in such a way that there is no doubt that the agreement has been signed by him, not even before a 3rd party such as the press or Stortinget.

a) The desired security goal is achieved by using digital signature as given above is referred to

as Select alternative (inegrity, accountability, security control, non-repudiation, authentication, authorization) .

b) Select the correct owner and type of key for signing and validation.

In order to sign the agreement, Jonas must use Select alternative (3rd party's, his own,

Trygves's) Select alternative (public, private, symmetric) key.

To validate the digital signature Trygve have to use Select alternative (3rd party's, Jonas',

his own) Select alternative (public, symmetric, private) key.

c) Will digital signing of a document ensure confidentiality of its content?
Select one alternative:

- No
- Yes

d) Electronic certificate is often mentioned together with digital signature. Which of the following statements is correct for the use of digital certificates?
Select one or more alternatives:

- prevents fraudsters from creating a valid internet domain.
- connects a public key and the owner's identity.
- binds together an asymmetric and a symmetric key.
- prevents fake keys and fake services.

Maximum marks: 4

3.7 Personopplysningsvern

Processing of personal data is strictly regulated in Norwegian and European legislation, through the Personal Data Act.

a) Which statement best matches the legal requirements for *the processing of personal data*?
Select one alternative:

- Personal data must be processed legally, fairly and openly, and with requirements for correctness, data minimization and limitation of purpose.
- Processing of personal data must take place with appropriate technical and organizational controls so that confidentiality, integrity and availability are safeguarded.
- Personal data must be processed legally, fairly and openly, and with requirements for correctness, data minimization and limitation of purpose. The processing must take place with appropiate technical and organizational controls so that confidentiality, integrity and availability are safeguarded.
- Processing of personal data requires consent from the data subject for all processing.

b) For which group does the Personal Data Act have the greatest impact?
Select one alternative:

- Criminals
- Businesses
- Individuals (the data subjects)

Maximum marks: 3

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 Operativsystemer

Which statements about operating systems are true and which are false?

	True	False
The operating system ensures that several users can share a computer	○	○
It is the operating systems task to allocate resources to the programs that will run.	○	○
Mobile phones only run one program at a time, and therefore do not need an operating system.	○	○
The operating system ensures that several programs can run simultaneously.	○	○
An operating system provides APIs for programs to use services such as storage and networking.	○	○
The operating system hides complicated hardware details to make developing software easier.	○	○
Common programs run in kernel mode because it is more efficient.	○	○
In the operating system layer, it is the Device Control module that has all the responsibility for security.	○	○

Maximum marks: 4

4.2 IPv6

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

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

Maximum marks: 1

4.3 Overføringshastighet

You want to download a file of 800 megabytes, and the speed of your Internet line is 50 megabits per second down and 25 megabits per second up. What is the theoretically shortest transfer time?

Select one alternative:

- 256 seconds
- 128 seconds
- 60 seconds
- 10 seconds
- 32 seconds

Maximum marks: 2

4.4 Punktnotasjon til CIDR

A computer has the IP-address: 213.58.192.58
The netmask is: 255.255.255.224
What is the IP-address to the machine written in CIDR notation?
Select one alternative:

- 213.58.192.1/26
- 213.58.192.58/26
- 213.58.192.58/27
- 192.168.1.1/24
- 213.58.192.1/27

Maximum marks: 4

4.5 Subnett-adresse

Given a machine with IP address 213.58.192.58 and netmask 255.255.255.224.
What is the address of the machine's subnet?
Select one alternative:

- 192.168.1.1
- 213.58.192.1
- 213.58.0.255
- 213.58.192.255
- 213.58.192.32
- 213.58.0.1

Maximum marks: 2

4.6 Broadcast-adresse

Given a machine with IP address 213.58.192.58 and netmask 255.255.255.224.
What is the broadcast address in this subnet?

Select one alternative:

- 213.58.1.255
- 192.168.1.255
- 213.58.192.63
- 213.58.192.1
- 213.58.192.32
- 213.58.192.255

Maximum marks: 2

4.7 Antall IP-adresser

The subnet has the subnet mask 255.255.255.224
How many valid IP addresses can be assigned to hosts on the network?

Select one alternative:

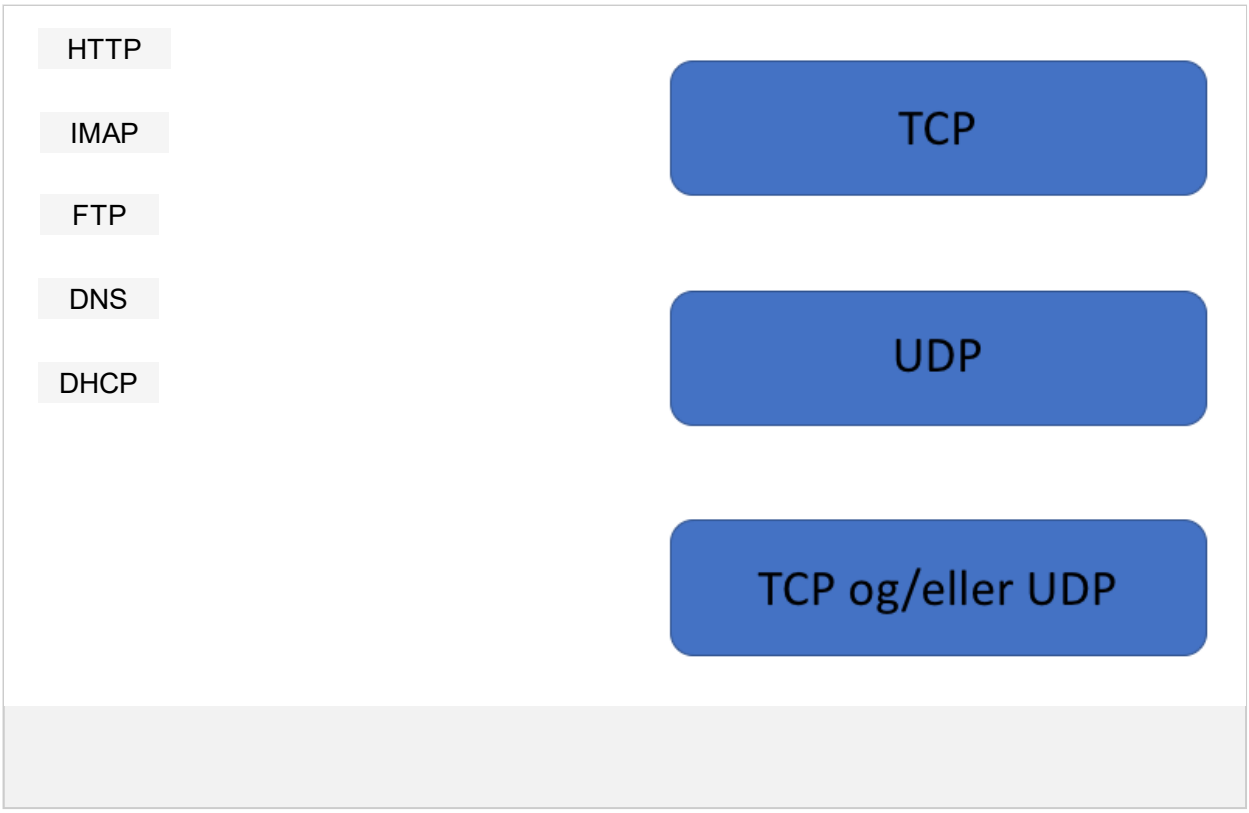
- 30
- 256
- 126
- 128
- 32

Maximum marks: 2

4.8 Transportprotokoller

Which protocol(s) in the transport layer do the services use?

Select one alternative:



Maximum marks: 5

4.9 Content Delivery Network

Which alternatives are positive effects of a Content Delivery Network?
Select one or more alternatives:

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

Maximum marks: 3