Forside

UNIVERSITY OF OSLO
The Faculty of Mathematics and Natural Sciences
Written examination in IN1020
FALL 2024
Duration: December 11, 15:00-19:00
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 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 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 can 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

Du er nå i seksjon 1 - Digital representasjon og assemblerkode.

Oppgave nr 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7 og 1.8 er en del av seksjon 1.

1.1 Tallsystemer

You see the following three numbers, but unfortunately, the notation telling you what number system they are written in, is gone. What number systems can these numbers be written in?

0f00d00d

- [ ] Octal numbers
- [ ] Binary numbers
- [ ] Decimal numbers
- [ ] Hexadecimal numbers

7777

- [ ] Hexadecimal numbers
- [ ] Decimal numbers
- [ ] Octal numbers
- [ ] Binary numbers

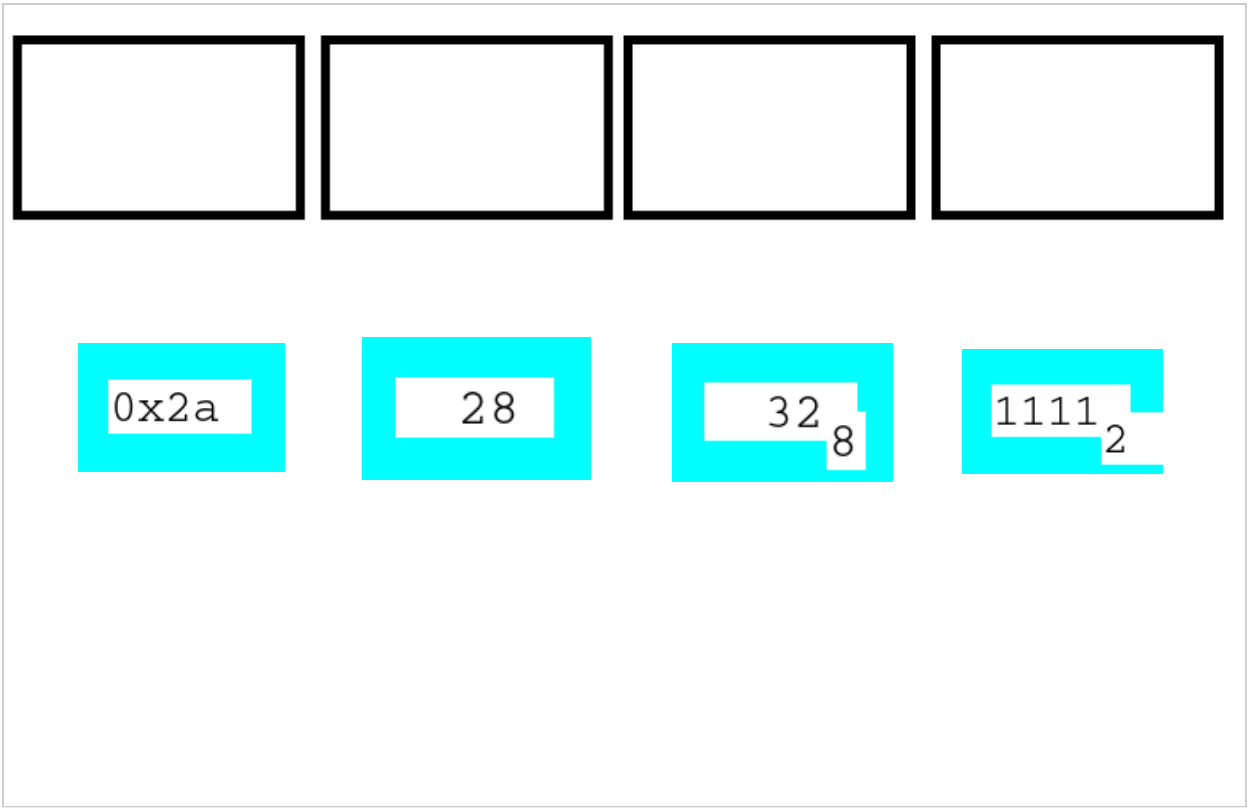
10101010

- [ ] Decimal numbers
- [ ] Binary numbers
- [ ] Hexadecimal numbers
- [ ] Octal numbers

Maximum marks: 2.4

1.2 Tallsortering

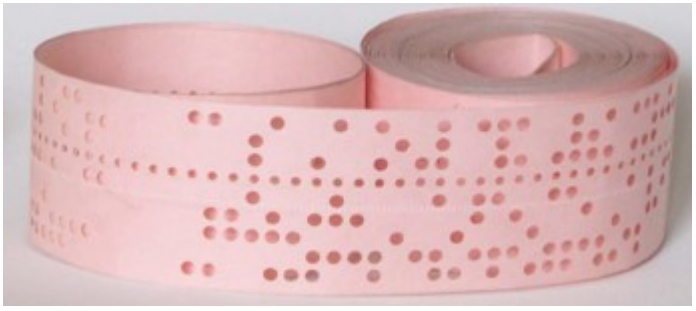
Sort the numbers in ascending order, from left to right.



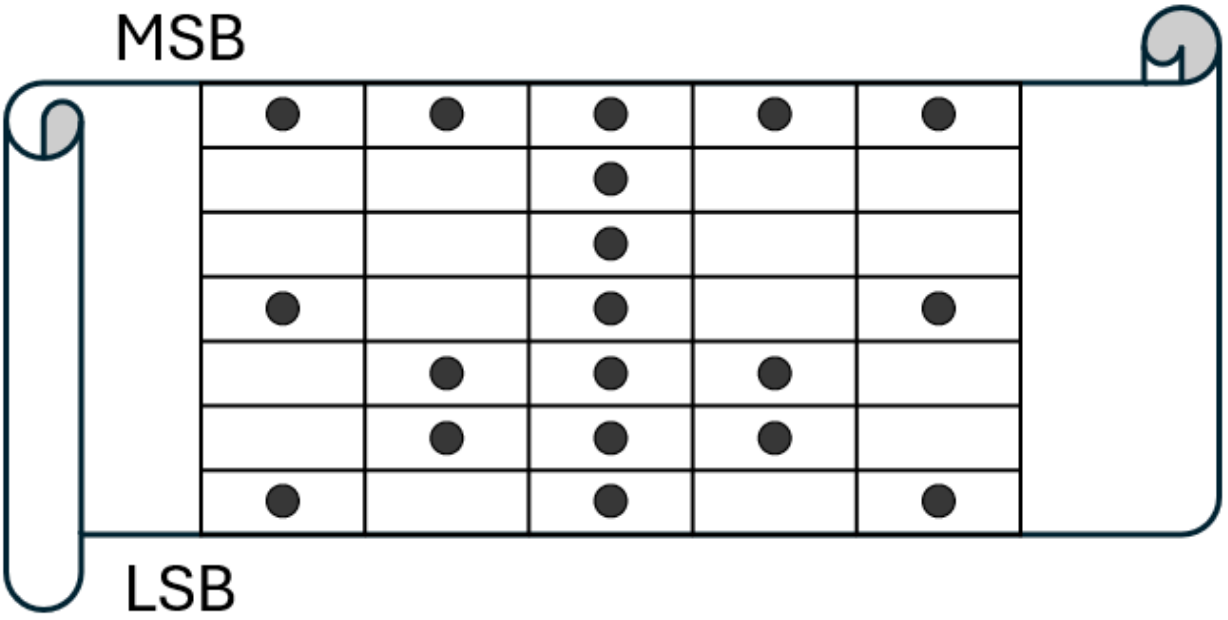
Maximum marks: 3

1.3 ASCII - Hullbånd

Early computers used punched tapes to represent information:



Imagine the following section of such a tape, where each cell contains a "1" if there is a punched hole (black circle), and "0" otherwise:



Given that data is represented in ASCII, what does this say?

Maximum marks: 3.8

1.4 Minnebruk

You have written a program for the LMC (used in the lectures) where food groceries are digitally represented in the following way:

What	Number of cells
PLU code	1
Name of the item	4
Price	1

Your program uses 43 cells. How many different food items can you represent?

Maximum marks: 3

1.5 LMC - Aritmetikk

Consider the following LMC program:

```
        INP
        STA a
        INP
        STA b
        LDA a
        SUB a
        SUB a
        ADD b
        OUT
        HLT
a       DAT
b       DAT
```

What function does the program compute?

Select one alternative:

- -a + b
- 2a - b
- a - b
- 2a + b

Maximum marks: 3

1.6 LMC - Maskinkode

The following LMC code should read in two numbers from the user, **a** and then **b**. The code should then calculate **a + b** and print the answer. Does the code work?

```
        INP
        STA a
        INP
        STA b
        DAT 508
        ADD b
        OUT
        HLT
a       DAT
b       DAT
```

Select one alternative:

- No
- Yes

Maximum marks: 3

1.7 LMC - Programflyt

Consider the following program for the LMC:

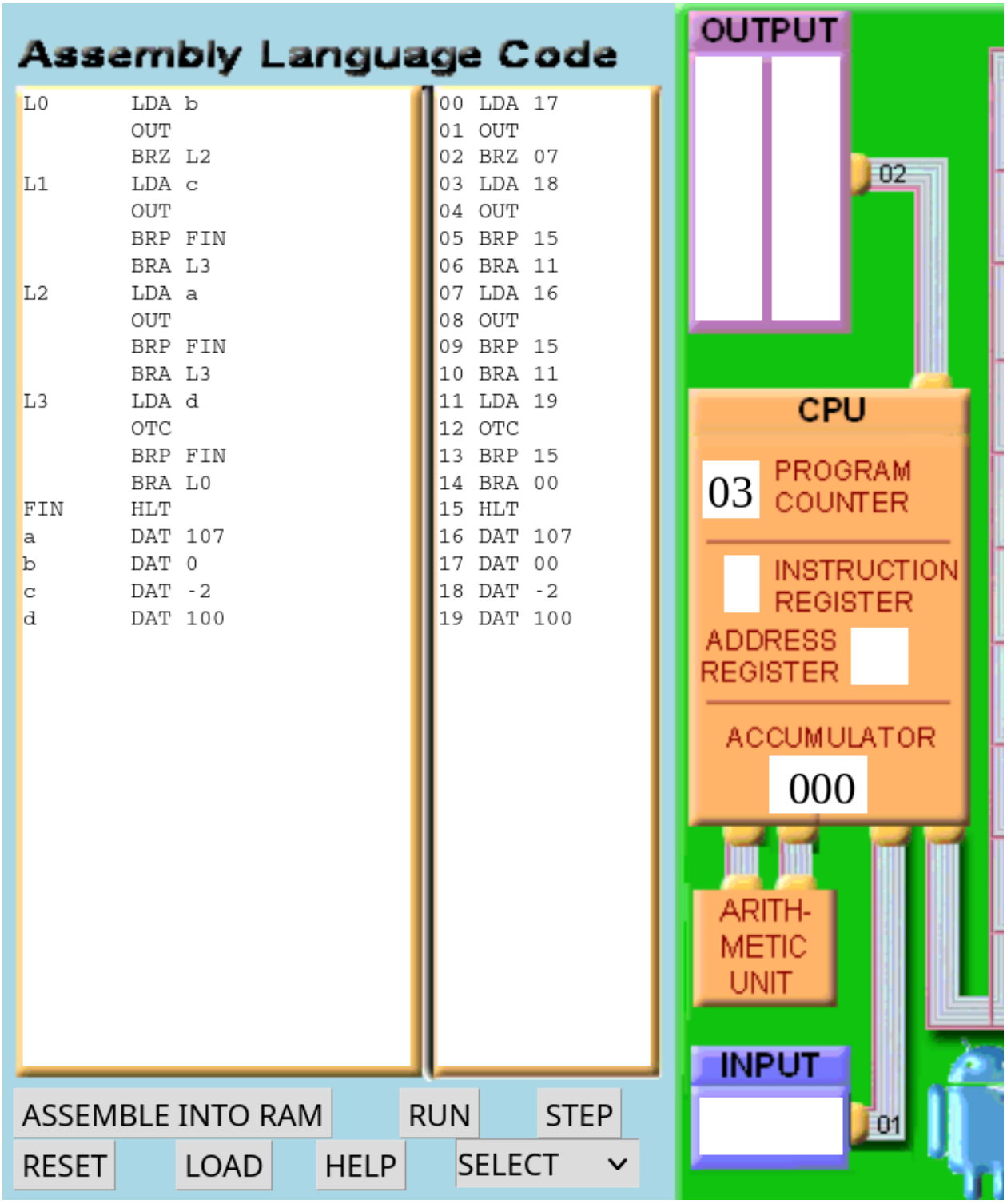
```
        INP
        STA a
        INP
        STA b
        SUB a
        STA a
        LDA b
        ADD a
        OUT
        HLT
a       DAT
b       DAT
```

What is printed when the user gives as input **2** and then **-1**?

Maximum marks: 3

1.8 LMC - Hopping

You have programmed and configured the LMC like this:



What does the LMC print when you press "RUN"?

First print:

Second print:

Maximum marks: 3.8

24-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 24-Minne/Cache

A cache hierarchy with two-level cache has the following properties:
30% of the instructions require access to Cache L1. 10% of the instructions require access to Cache L2. 4% of the instructions require access to RAM. The remaining instructions require no memory access.

Each instruction takes: 1 clock cycle without memory access. 20 clock cycles for each cache level. 400 clock cycles for RAM.

How many clock cycles does it take to execute 100 instructions?

Select one alternative:

- 2656
- 2456
- 2600
- 3056
- 2256
- 3456

Maximum marks: 5

2.2 24-datapath

Choose the correct alternatives for how a processor handles instructions.
HINT! recall the lecture of "Pipeline" and "kretser som driver koden"?

The instruction format is determined by Select alternative (Operating system, Processor Architecture, Compiler, Memory).

The result of a calculation is temporarily stored in

Select alternative (Cache, Hard drive, Clock, Register).

Instruction decoding is done by

Select alternative (DMA, Instruction Decoder, Memory Controller, ALU) i

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

Control signals from decoding are sent to Select alternative (Memory, Hard drive, ALU, PC)to determine

Select alternative (Synchronization, Voltage, Operation, Address).

Maximum marks: 6

2.3 24-Godt og blandet

Which of these are true?

- [ ] All logic gates must have at least two inputs
- [ ] A synchronous circuit always needs a clock pulse
- [ ] A CPU can only execute instructions stored in RAM
- [ ] In a pipeline, all stages must take the same amount of timed
- [ ] Cache memory is slower than main memory (RAM)
- [ ] A pipeline with 5 stages always executes 5 instructions simultaneously
- [ ] A NAND gate can be used to create all other logic gates
- [ ] A Half Adder cannot handle carry in

Maximum marks: 4

2.4 24-Abstraksjonnivå

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

Highest	Select alternative (ALU, Transistor, Register, CPU, Inverter)
	Select alternative (Register, CPU, Inverter, ALU, Transistor)
	Select alternative (CPU, Transistor, Inverter, Register, ALU)
	Select alternative (ALU, Inverter, Transistor, CPU, Register)
Lowest	Select alternative (Inverter, Transistor, Register, CPU, ALU)

Maximum marks: 3

2.5 24-Kretsanalyse

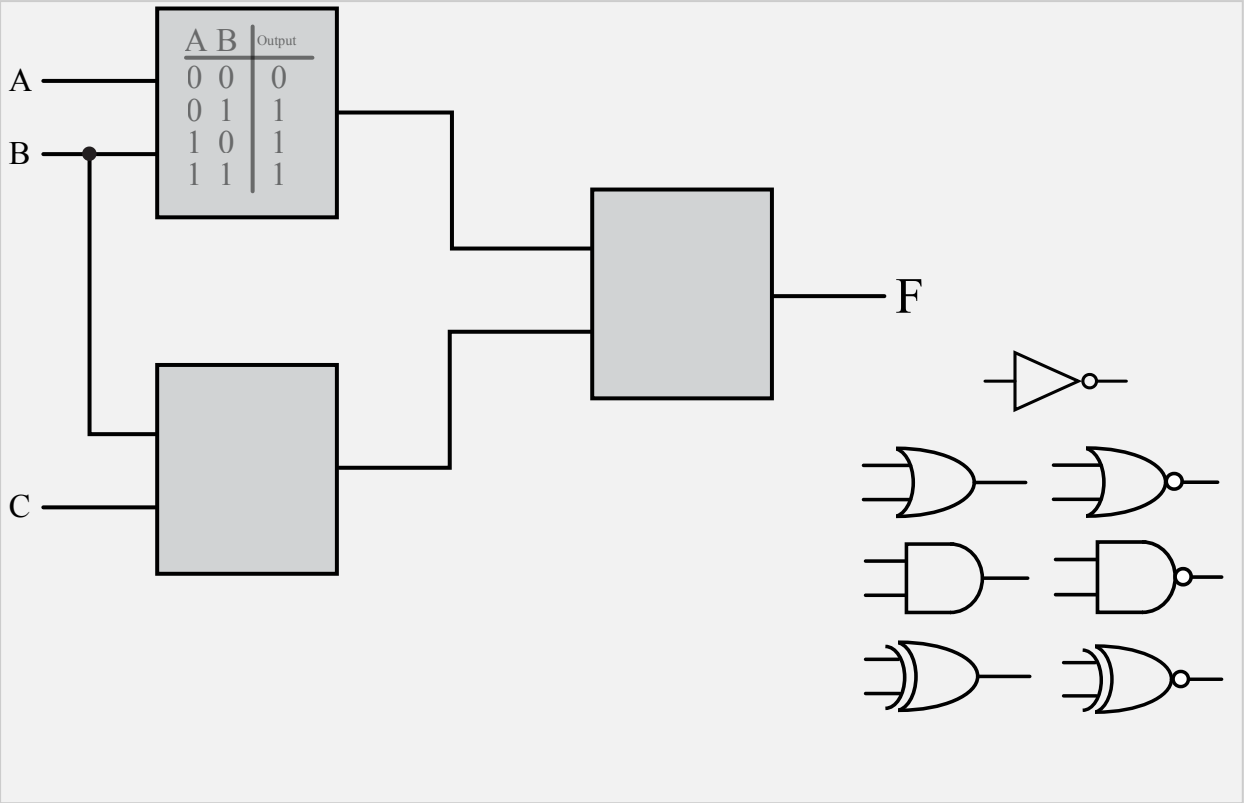
The circuit has the function

$$F = \overline{A'C' + B + AC + A}$$

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

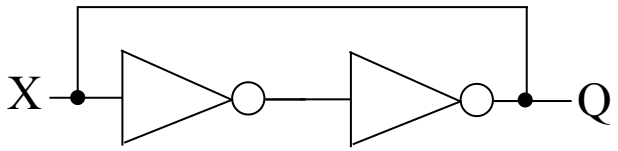
Hint! Do you remember the different symbols for a function expression that is inverted?
Hint! In one of the gray boxes, the truth table for the gate is provided.

Drag and drop correct gates into the gray area



Maximum marks: 5

2.6 24-Undring



How to answer this question:

For each alternative, indicate how likely you think it is to be correct, expressed as a percentage (%).

Examples:

- If you are completely certain that alternative 1 is correct and all others are wrong:
  - Alternative 1: 100%
  - All other alternatives: 0%
- If you think both alternatives 1 and 2 might be correct, but you are more confident about alternative 1:
  - Alternative 1: 75%
  - Alternative 2: 25%
  - All other alternatives: 0%
- If you are uncertain between three alternatives:
  - Alternative 1: 50%
  - Alternative 2: 25%
  - Alternative 3: 25%
  - Other alternatives: 0%

The sum of all percentages must equal 100%.

What is the function of the circuit above?

	0 %	25 %	50 %	75 %	100 %
Memory	○	○	○	○	○
Amplifier	○	○	○	○	○
Inverter	○	○	○	○	○
NAND	○	○	○	○	○

Maximum marks: 2

Seksjon 3

You are now in section 3 - Security.

The problem number 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 and 3.8 are part of section 3.

3.1 Brudd på sikkerhetsmål

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

	Availability	Integrity	Confidentiality	Authenticity
Eavesdropping on data traffic	○	○	○	○
SQL injection modifying content	○	○	○	○
Data traffic modification	○	○	○	○
Signal disturbance in the wireless network	○	○	○	○
Fake DNS server	○	○	○	○
Cracking file encryption	○	○	○	○

Maximum marks: 3

3.2 Sikkerhetsmål refleksjon

Security objectives are characteristics that are desired to be maintained in IT systems, and are not exact values. The objectives are closely intertwined, influenced by each other, and may even conflict with each other.

Select the correct safety measure in the two statements below:

Increased need for confidentiality may come at the expense of Select alternative (integrity, privacy, authenticity, availability).

The need for detailed accountability may come at the expense of Select alternative (privacy, authenticity, availability, integrity).

Maximum marks: 2

3.3 Begrepsforståelse

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

Help

Intrusion detection	Data minimization	Authorization	Firewall
Vulnerability	Consequence	Phishing	Hash functions
Spoofing	Storage limitation	Risk analysis	Digital certificates
Threat	Threat actor	Data processor	Access control

[ ] is to create a policy for access to resources.

[ ] is used to avoid storing passwords in clear text.

[ ] can detect attempts of digital intrusions into a computer network.

[ ] is to falsify a sender in communications.

[ ] is to collect and process only personal data that is necessary for a purpose.

[ ] is to assess the probability and consequence of potential security incidents.

[ ] can be loss of reputation due to data leakage from a company's customer register.

[ ] is the term for someone who wants to carry out harmful activity.

Maximum marks: 4

3.4 Trusselmodellering

A small company is working on research and development of new and climate-friendly solutions for power delivery. The company is afraid that competitors will steal ideas, documents and other digital material relating to their work (i.e. company secrets), and e.g. get ahead of them with patents on new solutions. You are hired as a security consultant to help the company with threat modeling to avoid leakage of this type of information.

a) Protecting the company secrets is to ensure Select alternative (confidentiality for, access to, integrity for, availability to)information.

b) The company uses wireless internet in its office premises. What would be reasonable security measures against eavesdropping on network traffic?
Select one or more alternatives:

- [ ] Having redundant IT systems.
- [ ] Ensure signal interference.
- [ ] Use secure network protocols.
- [ ] Ensure that wireless access points have updated software.
- [ ] Back up all data.
- [ ] Use authentication mechanisms for connecting to wireless networks.

c) Another obvious threat is data leakage due to social engineering. What would be sensible security measures to avoid this type of incident?
Select one or more alternatives:

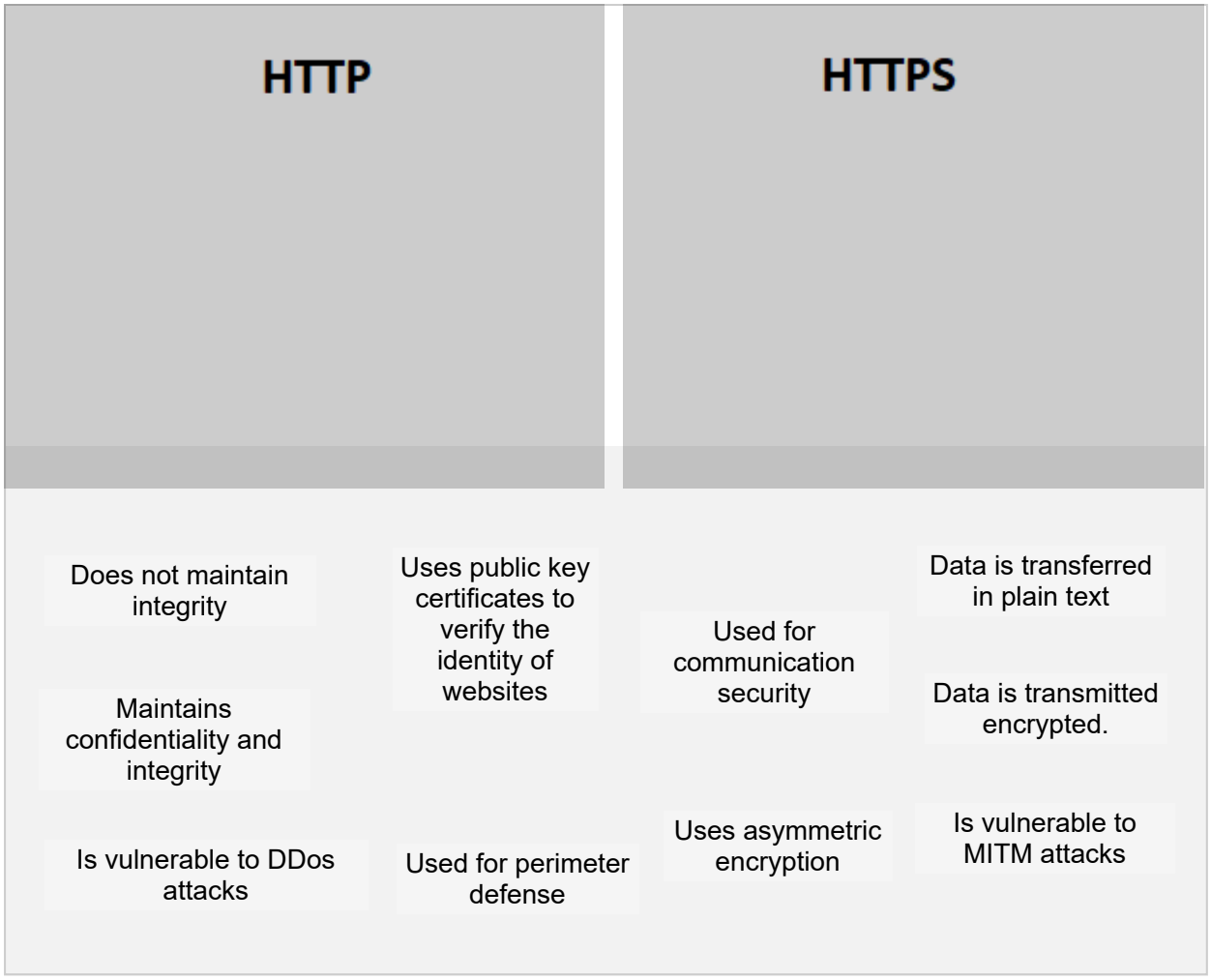
- [ ] Having redundant IT systems.
- [ ] Provide employees with information security training.
- [ ] Have sufficient financial management.
- [ ] Ensure that all employees have access to all company secrets.
- [ ] Make sure that no employees have access to more information than they strictly need.
- [ ] Have good procedures for the recovery of the IT systems.

Maximum marks: 3

3.5 Sikker nettverkskommunikasjon

HTTP and HTTPS are both protocols used to transfer data over the internet.

Drag and drop the different statements to fit the HTTP and HTTPS properties. Note: Not all alternatives will fit.



Maximum marks: 2

3.6 Ulike typer kryptering

Hash functions, symmetric and asymmetric encryption are three different forms of cryptography. In this task, you must link the correct property to the correct encryption type.

Please match the values:

	Neither part	Hash functions	Symmetric encryption	Asymmetric encryption
Can be used without an encryption key	○	○	○	○
The result cannot be decrypted	○	○	○	○
Should be collision resistant	○	○	○	○
Constitutes an important element in a PKI	○	○	○	○
Also known as checksum algorithm	○	○	○	○
Is used for authorization	○	○	○	○
Also known as cryptovirus	○	○	○	○
Also known as secret key encryption	○	○	○	○
Uses one key for encryption and another for decryption	○	○	○	○

Maximum marks: 3

3.7 PKI og kryptering

Jonas, Trygve and Sylvi communicate digitally using a public key infrastructure (PKI).
Jonas has been given a key pair consisting of a private key that is known only to Jonas, and a public key that is made known to several people, including both Trygve and Sylvi.

a) Which statements are correct when this key pair is used for digital signatures?
Select one or more alternatives:

- [ ] Trygve can validate the digital signature Jonas has signed with his private key.
- [ ] Trygve can validate the digital signature Jonas has signed with his public key.
- [ ] Sylvi can validate the digital signature Jonas has signed with his private key.
- [ ] Jonas can validate the digital signature Sylvi has signed with Jonas's public key.

b) Which statements are correct when this key pair is used to encrypt messages/documents?
Select one or more alternatives:

- [ ] Trygve can read (decrypt) the message Sylvi encrypts with Jonas's public key.
- [ ] Jonas can read (decrypt) the message Sylvi encrypts with Jonas's public key.
- [ ] Only Sylvi can read (decrypt) a message Jonas encrypts with his private key.
- [ ] Only Jonas can read (decrypt) a message Sylvi or Trygve encrypts with Jonas's public key.

c) What is the main purpose of a PKI?
Select one alternative:

- ( ) To store all users' private keys in a secure location.
- ( ) Preventing threat actors from reading encrypted messages.
- ( ) To encrypt all communication on the internet.
- ( ) To ensure the authenticity of public keys and secure key distribution.

d) Which of the following statements about digital certificates for a PKI are correct?

Select one or more alternatives:

- [ ] A digital certificate contains all of the owner's private keys.
- [ ] A digital certificate associates a public key with an identity.
- [ ] A digital certificate is signed by a certificate authority (CA).
- [ ] A digital certificate encrypts all messages sent between users.

e) What is the role of a Certificate Authority (CA) in a PKI?
Select one alternative:

- ( ) They are developing new encryption algorithms.
- ( ) They store the private keys of all users.
- ( ) They encrypt all messages sent between users.
- ( ) They issue and sign digital certificates.

Maximum marks: 4

3.8 Personopplysningsvern

You are employed as a developer in a technology company, and have been assigned to help develop a new IT system for a healthcare institution. The system will process personal data.

a) The Personal Data Act says something about *Processing of special categories of personal data.* Which of the following types of personal data fall under this category?

Select one or more alternatives:

- [ ] Phone Number
- [ ] Racial or ethnic origin
- [ ] IP address
- [ ] Data concerning health
- [ ] Trade union membership
- [ ] Name

b) In the development process, one of the tasks is to implement *Privacy by Design*. Why is it important to facilitate Privacy by Design in software development?

Select one or more alternatives:

- [ ] Because there is no built-in security.
- [ ] To ensure that the systems comply with the data protection principles.
- [ ] To protect the rights of the data subjects in processing personal data.
- [ ] To make the systems more complex.

c) The healthcare institution has chosen to use an external provider's cloud solution to store patient data. All data (including personal data) is stored on the external provider's computer equipment that is physically located in an EU country, and data is transferred over the internet. Which of the following statements is consistent with the guidelines in the Norwegian General Data Protection Regulation (GDPR) for the healthcare institution's processing of personal data?

Select one or more alternatives:

- [ ] When personal data is stored with an external company, the health institution can disregard the Personal Data Act for its processing of personal data.
- [ ] A patient never has the right to view or access the health information that is stored about him.
- [ ] The Personal Data Act sets requirements for information security.
- [ ] All processing of personal data must be carried out with appropriate technical and organizational measures.
- [ ] The health institution is legally responsible for processing data on patients in accordance with the Personal Data Act.

Maximum marks: 4

Seksjon 4

You are now in section 4 - Operating Systems and Data Communication.

Tasks 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 and 4.8 are part of section 4.

4.1 Lett blanding - Nettverk

Which statements about data networks are true and which are false?

	Sann	Usann
Only servers can be considered end systems in data networks.	○	○
The Internet is many interconnected networks.	○	○
The Peer-to-Peer model is the most common access model in data networks.	○	○
Modern wireless networks (WiFi) use the point-to-point communication model.	○	○
A modern wired network (Ethernet) with a switch uses a star or tree topology.	○	○
Network protocols are a set of rules that define how communication should occur.	○	○
IPv4 is a connection-oriented protocol.	○	○
The primary motivation behind IPv6 is to increase the number of globally addressable IP addresses.	○	○

Maximum marks: 4

4.2 Operativsystemer

Which of the statements about operating systems are true?
Select one or more alternatives:

- [ ] Modern smartphones do not use the operating system's services for scheduling programs.
- [ ] One of the main tasks of an operating system is to hide hardware details to make it easier to develop programs.
- [ ] An operating system will only ensure fair distribution of the processor. It is the programs themselves that are responsible for ensuring fair distribution of memory (RAM).
- [ ] All modern programs run in kernel mode for faster access to resources.
- [ ] Computers that control components such as an autopilot in an airplane have high reliability requirements and therefore do not have an operating system.
- [ ] One of the main tasks of an operating system is to allocate the resources of the computer.
- [ ] Operating systems such as newer versions of Windows and Linux are built based on the monolithic kernel model.

Maximum marks: 3

4.3 Antall IP-adresser

You are tasked with setting up a private network for a small business, and you are informed that the network provider has configured a /28 network (CIDR notation: /28).

How many IP addresses can the DHCP server allocate in this network? [ ]

Maximum marks: 3

4.4 CIDR til punktnotasjon

When you connect a device to the network, you receive the following IP address: *192.168.100.164*

As mentioned in the previous task, you were informed by the network provider that a /28 network has been reserved. Your IP address in CIDR notation is therefore: *192.168.100.164/28*.

What is the subnet mask of your device in dot-decimal notation:

Maximum marks: 4

4.5 Subnet + Broadcast

As mentioned in the previous task, you have connected a computer to the network and received the IP address: *192.168.100.164*.
The network is still a /28 network, and the IP address in CIDR notation is: *192.168.100.164/28*.

What is the subnet address of the network?

What is the broadcast address of the network?

Maximum marks: 6

4.6 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
Both TCP and UDP support multiplexing using ports.	○	○
The transport layer only works on end-to-end and has no knowledge on how data is transmitted over the network.	○	○
UDP is the most used of the two protocols in the transport layer.	○	○
UDP is a lightweight protocol and is therefore well suited to transfer large files.	○	○
Congestion Control makes sure that the capacity in the network is shared on all connections.	○	○
It is not possible to use encryption on the application layer when UDP is used.	○	○
TCP is a connection-oriented protocol.	○	○
Both TCP and UPD makes sure that data is delivered in-order.	○	○

Maximum marks: 2

4.7 HTTP

Which of these statements are correct for a persistent connection in HTTP?
Select one or more alternatives:

- [ ] The same TCP connection is reused for several rounds of HTTP requests.
- [ ] The payload will be sent many times, regardless of network conditions, to make sure that it arrives successfully.
- [ ] HTTP requests cannot be multiplexed over a persistent connection.
- [ ] The TCP connection will continue to try to connect, even if it is closed or interrupted.

Maximum marks: 1

4.8 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.
- [ ] Video is divided in small segments and different quality layers.
- [ ] 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.

Maximum marks: 2