Info

Exam IN1020 autumn 2019

Time

9th December 9:00-13:00
The lecturers will visit you some time after 10 o'clock.

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.

1.1 Sikkerhetsmål

Security services are essential in information security. Which of the following is defined as a security service:
Select one or more alternatives:

- [ ] Backup
- [ ] Two-factor authentication
- [ ] Firewall
- [ ] Availability ✔
- [ ] Encryption
- [ ] Accountability ✔
- [ ] Integrity ✔
- [ ] Non-repudiation ✔

Maximum marks: 2

1.2 Sikkerhetstiltak - konfidensialitet

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

Select one or more alternatives:

- [x] Use HTTPS over HTTP as a protocol in network communication. ✔
- [ ] Using checksum algorithms when transmitting data in computer networks.
- [x] Use of two-factor authentication for systems which process data of confidential art. ✔
- [x] Use disk encryption when storing data. ✔
- [x] Awareness training for everyone who processes data. ✔

Maximum marks: 2

1.3 Sikkerhetstiltak - fysisk sikring

Why is physical security (such as limiting physical access to computers/computersystems) important for optimal security in critical computer systems?

Select one or more alternatives:

- [x] Because an intruder can bypass virtually all security measures by getting physical access to a system. ✔
- [ ] Because an intruder may steal biometric identities.
- [ ] Because critical computer system does not have encryption.
- [ ] Because physical access to a system makes it easier to authenticate.

Maximum marks: 2

1.4 Autentisering

How can multi-factor authentication help improve the security of a computer system?

Select one or more alternatives:

- [x] By using a combination of authenticators, it will be more difficult for unauthorized persons to acquire illegitimate access to a system.
- [ ] By using biometrics, unauthorized persons cannot authenticate themselves by pretending to be someone else.
- [ ] Multi-factor authentication will limit what users are allowed to do in a system.
- [ ] Multifactor authentication makes it easy to limit repeated attempts to acquire unauthorized access.

Maximum marks: 2

1.5 Digital signatur

A consultancy company has customers all over the country. They wish to replace the awkward process of signing contracts using pen and paper with a digital variant of signature which can guarantee that a customer and not a swindler signed the contract. They have heard of a method called *digital signature*, which may provide them with sufficient confirmation of the signer's identity.

a) What characterises that which is known in information security as a *digital signature*:
Select one or more alternatives:

- [ ] Secures confidentiality for the signed message.
- [ ] It may confirm sender's identity to a third party (non-repudiation). ✔
- [ ] It may confirm sender's identity to recipient. ✔
- [ ] Is based on symmetric encryption.

b) Which *cryptographic keys* are involved when *digital signatures* are being used:
Select one or more alternatives:

- [ ] Recipient's public key.
- [ ] Sender's public key. ✔
- [ ] Sender's private key. ✔
- [ ] Recipient's private key.
- [ ] Symmetric key generated by sender.
- [ ] Symmetric key generated by recipient.

Maximum marks: 6

1.6 Behandling av personopplysninger

The Department of Informatics wants to test a new computer system for conducting the exam, which allows students to program Python during the examination.

The computer system the department will adopt is a cloud service from an external provider, available through a web application. Both data storage and application execution are done on the supplier's computer equipment, which is physically located in an EU country. The exam itself is facilitated/conducted via a browser on UiO's computers in UiO's exam locations.

Each student is given a unique candidate number and password, which they use when logging into the system to take the exam. A written exam delivery is linked to a student through the student's candidate number.

Consider the following statements and select the ones you think are correct, based on the information given above.

Select one or more alternatives:

- [ ] Students have the right to know which information about themself is being processed in the system. ✔
- [ ] The Department of Informatics is legally responsible for ensuring that information about students and their exam answers is processed in accordance to the Privacy regulations. ✔
- [ ] Names or social security numbers are not stored in the system, so there is no need to comply with the Privacy regulations.
- [ ] Because the service is provided entirely by others, the Department of Informatics is not legally responsible that the information about students and their exam answers is being processed in accordance to the Privacy regulations.

Maximum marks: 4

1.7 Trusselmodellering - tilgjengelighet

After an evaluation of Personal Data Protection, the Department of Informatics is planning to start to use the following computer system for conducting the examination (same as in the previous assignment):

The computer system the department will adopt is a cloud service from an external provider, available through a web application. Both data storage and application execution are done on the supplier's computer equipment, which is physically located in an EU country. The exam itself is facilitated/conducted via a browser on UiO's computers in UiO's exam locations.

Each student is given a unique candidate number and password, which they use when logging into the system to take the exam. A written exam delivery is linked to a student through the student's candidate number.

Availability of the system is of course of high importance, as students have to be able to log in and use the system when they show up to take the exam. Your task is therefore to make an evaluation of what might be a threat to availability, given the information above.

Select one or more alternatives:

- [x] Lack of security updates of the software and operating system used by the system.
- [x] Unavailable attacks (DDoS) done by outside attackers with malicious inte
- [x] Failur in the system performing access control in the computer system.
- [ ] Someone placed a keylogger between keyboard and the computer.
- [ ] Error in the storage routines that allows students to see each other's examination answers.

Maximum marks: 5

1.8 Trusselmodellering

Why can the use of USB memory sticks pose a security threat to the security service of confidentiality?

Select one or more alternatives:

- [ ] They may carry with them malware that bypass other security mechanism ✔
- [ ] They may be stolen. ✔
- [ ] They can use too much power and thus adversely affect a computer.
- [ ] They may be unintentionally encrypted by, for example, ransomware.

Maximum marks: 2

2.1 Nettverksprotokoller

What is a network protocol?

Select one or more alternatives:

- [ ] A log where all data communication is stored.
- [ ] A detailed description about your Internet subscription.
- [ ] A file with drivers for your network card.
- [ ] Rules on how data is transferred between two machines. ✔

Maximum marks: 1

2.2 Nettverkstopologi

Which of the alternatives are not a network topology:
Select one or more alternatives:

- [ ] Client/server ✔
- [ ] Hash ✔
- [ ] Star
- [ ] Full mesh
- [ ] Ring

Maximum marks: 2

2.3 WiFi

WiFi is typically used in a:
Select one or more alternatives:

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

Maximum marks: 1

2.4 TCP/IP-modellen

What layer in the TCP/IP model is the lowest layer that only cares about end-to-end communication?

Select one alternative:

- Transport layer
- Physical layer
- Application layer
- Link layer
- Nettverkslaget ✔

Maximum marks: 1

2.5 Overføringshastighet

You want to download a file at 200 megabytes, and the maximum download speed of your Internet connection is 20 megabits per second. What is the theoretical shortest transfer time?

Select one alternative:

- 10 seconds
- 100 seconds
- 20 seconds
- 80 seconds ✔
- 5 seconds

Maximum marks: 2

2.6 IP-adresser

A subnet has the network mask 11111111.11111111.00000000.00000000
How many valid IP-addresses can be allocated to hosts in the subnet?
Select one alternative:

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

Maximum marks: 3

2.7 TCP

Which of these services are offered by TCP:
Select one or more alternatives:

- Flow control. ✔
- Routing of packets in the Internet.
- Congestion control ✔
- Encrypted transfers.
- All of these services.
- Connectionless communication.
- Checksum. ✔

Maximum marks: 4

2.8 DHCP

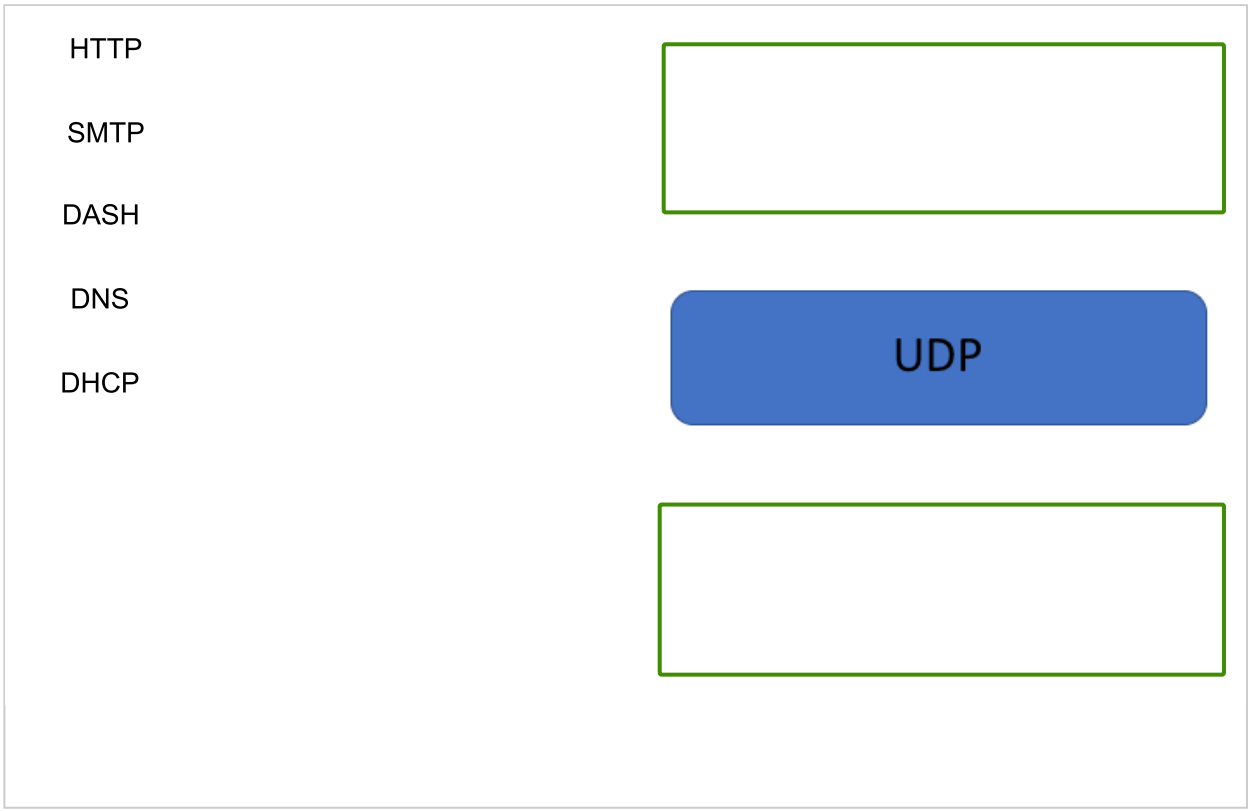
How many DHCP-servers should you have in a LAN (broadcast-domain)?
Select one or more alternatives:

- [ ] 1 ✔
- [ ] As many as you wish
- [ ] Depending on machines in the network
- [ ] Depends if NAT is used

Maximum marks: 1

2.9 Protokoller

Which protocol(s) is used by the service?
Select one alternative:



Maximum marks: 5

2.10 NAT

Which service is offered by Network Address Translation (NAT)?

Select one or more alternatives:

- [ ] It makes it easier for hosts on the Internet to connect to machines in the local area network.
- [ ] It broadcasts which port number that is used by a specific service.
- [x] It enables many units on a local area network to share one externel/public IP address.
- [ ] It translates between MAC adresses and IP addresses.

Maximum marks: 2

2.11 Content Delivery Network

Which of these statements are correct for a Content Delivery Network (CDN)?

Select one or more alternatives:

- [ ] It saves hardware and energy by virtualizing the network service.
- [x] It can reduce latency by moving data closer to the user.
- [x] It can offload the server that has the original data if you have many concurrent users.
- [ ] It increases security because it works as a firewall for the server that has the original data.

Maximum marks: 2

2.12 DNS

What is DNS-prefetching?

Select one or more alternatives:

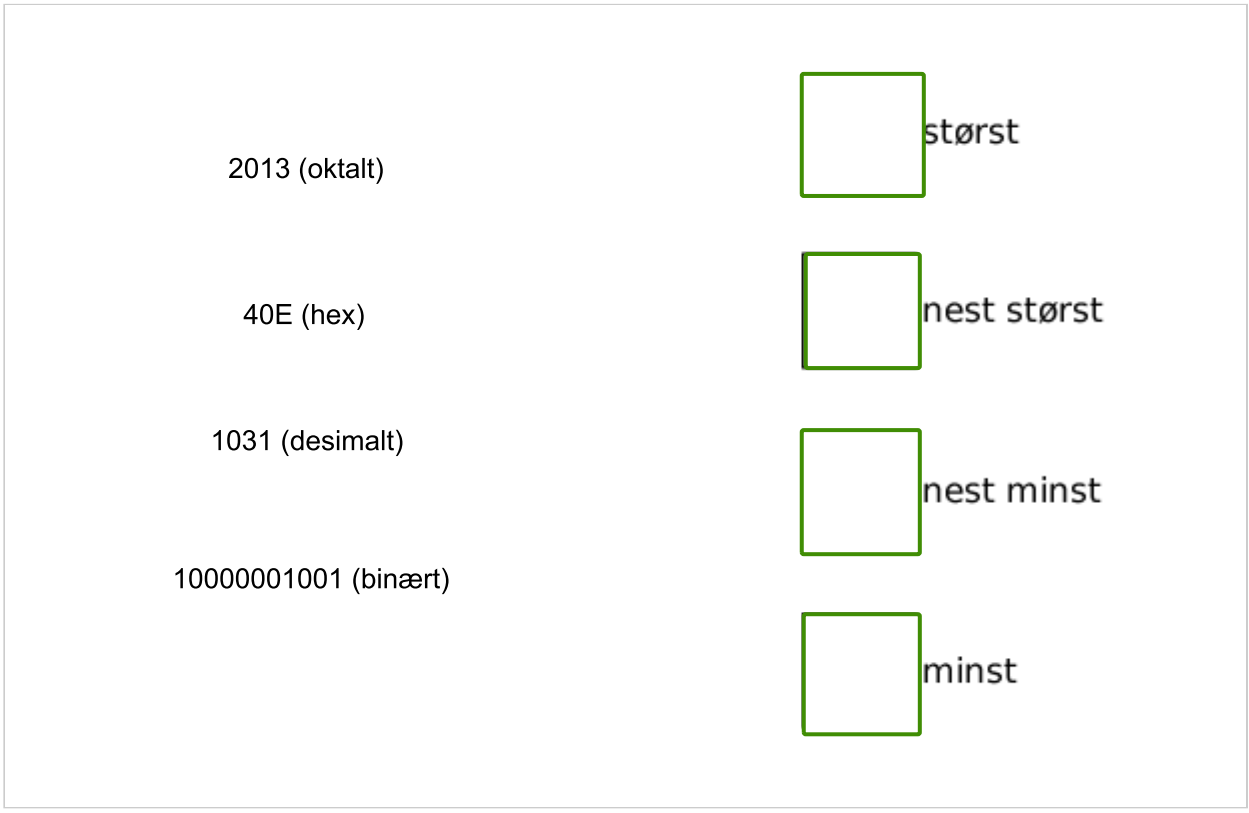
- [ ] A service caches the MAC addresses of webservers for fast lookups.
- [ ] A home router caches DNS-entries so that the client machine does not have to contact a root server.
- [ ] A server caches homepages so that the next request does not have to go the entire way to the source server.
- [ ] A browser makes DNS lookups for all the domain names (URLs) it can find in a web document to save time in case the user presses one of the links. ✔

Maximum marks: 1

3.1 Tall på ulik form

To the left are four different numbers given in different form. Sort these numbers and use the computer mouse to move them to their correct position to the right.

Note: "størst" = biggest, "nest størst" = biggest but one, "nest minst" = smallest but one, "minst" = smallest.



Maximum marks: 4

3.2 Binærtall

How is the value **57** stored in one byte (i.e., 8 bits)? Write each bit in its box.

( ) (0) ( ) (0) ( ) (1) ( ) (1) ( ) (1) ( ) (0) ( ) (0) ( ) (1)

and how is the value **-57** stored when we use **2's-complement**?

( ) (1) ( ) (1) ( ) (0) ( ) (0) ( ) (0) ( ) (1) ( ) (1) ( ) (1)

Maximum marks: 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
```

What is printed when this code is run and the user gives **7** and **11** as input?
Select one or more alternatives (but only one is correct):

- [ ] -4 ✔
- [ ] 4
- [ ] 11
- [ ] 18
- [ ] 0
- [ ] Nothing is printed

Maximum marks: 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
```

What is printed when this program is run and the user give the values **5 3 3 1 0** as input?

Select one or more alternatives (but only one is correct):

- [ ] 4 ✔
- [ ] 0
- [ ] 7
- [ ] 5
- [ ] 12
- [ ] Nothing is printed

Maximum marks: 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'
```

What is printed by this program when the user gives **6** as input?

Select one or more alternatives (but only one is correct):

- [ ] Nothing is printed
- [ ] 6
- [ ] 512
- [ ] S
- [ ] 83
- [ ] L ✔

Maximum marks: 4

3.6 Maskinkode

Assume that the memory of the LMC computer contains these values

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

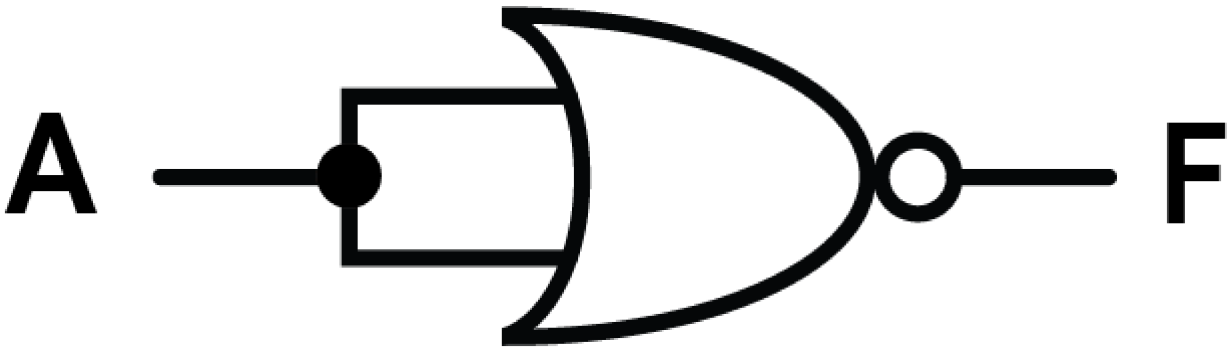
and that the program counter er **0**. What is printed when the code is run and the user gives **8** as input?

Select one or more alternatives (but only one is correct):

- [ ] Nothing is printed
- [ ] 0
- [ ] 8
- [ ] 64
- [ ] 56 ✔
- [ ] 24

Maximum marks: 5

4.1 Portanalyse



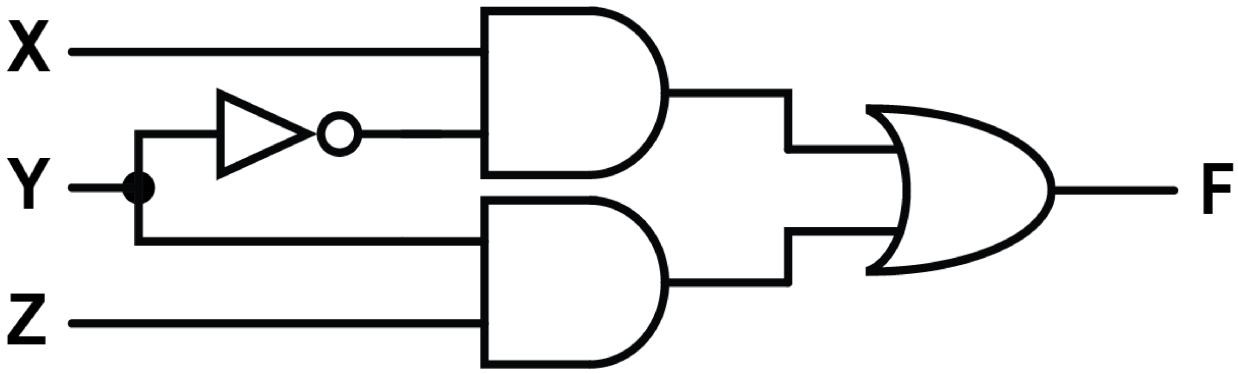
What is the function for the gate above?

Select one or more alternatives:

- [ ] F = AB´
- [ ] F = 1
- [ ] F = A´ ✔
- [ ] F = AA
- [ ] F = AA´
- [ ] F = 0
- [ ] F = (A+A)´ ✔
- [ ] F = A+B

Maximum marks: 3

4.2 Kretsanalyse



What is the function for the circuit above?

Select one or more alternatives:

- [ ] F = x´ + z´
- [ ] F = x´+ y + z´
- [ ] F = xz + y´
- [ ] F = xy + yz
- [ ] F = xy´ + zy ✔
- [ ] F = xy´ + yz ✔
- [ ] F = xyz
- [ ] F = x + y + z

Maximum marks: 7

4.3 Cache-miss

Assume that the processor has 500 instructions left to execute. It takes one clock cycle per instruction, and one expects to have a memory access with cache miss of 50%. A cache miss results in an total time consumption of 20 clock cycles. What is total remaining number of clock cycles?

Select one alternative:

- 2.350
- 10.000
- 5.250 ✔
- 55
- 250
- 5.000
- 500
- 500.000

Maximum marks: 7

4.4 Godt og blandet

Which statements are true or false?

NB! It is not possible to remove tick, only to switch between true and false once you have ticked off. So be sure to answer before you tick-off.

Are the statements true or false?

	False	True
Due to the technological development its possible to have smaller transistors.	○	✔
Is it possible to have five inputs for an XOR-gate?	○	✔
Is a´b´ equal to (ab)´ ?	✔	○
It is the Register in the CPU, which generates the clock signals.	✔	○
The clock period determines the frequency	○	✔
Is it possible to have three inputs for an AND-gate?	○	✔
Is it possible to get two carry bits out of a 1-bit full-adder?	✔	○
It is more efficient to use RAM rather than Cache	✔	○
Complications in a 4-step pipeline limits the possibility to obtain 4 times faster processing.	○	✔
F = xy is an NOR-gate	✔	○
Binary (half-adder) addition of 0+1 produce a Carry-out = 1	✔	○
Is it possible to divide an instruction into more than four subinstructions?	○	✔
Is it possible to have two inputs for an INVERTER-gate?	✔	○
A truth-table can have multiple expressions	○	✔

Maximum marks: 8

4.5 ALU

Which of these statements are valid for an ALU?
Select one or more alternatives:

- [ ] The Pipeline is a part of the ALU.
- [ ] A 1-bit ALU contains a ripple-adder.
- [ ] The ALU can only execute logical operations.
- [ ] The ALU can execute mathematical operations. ✔
- [ ] The control signal in an ALU comes directly from the instruction. ✔
- [ ] The ALU is a part of the CPU. ✔
- [ ] The ALU determines the clock frequency.
- [ ] ALU is short for ALUminium, which is the next generation supercomputer.
- [ ] The ALU is a part of RAM.
- [ ] The ALU determines the number of steps in a pipeline.

Maximum marks: 3