ⁱ Nytt dokument

Exam in IN1020 autumn 2017

Time

13th December 14:30
The lecturers will visit you from 15:30.

The problems

The problems are mainly multiple choice questions allowing for several answers. Some problems will have a single correct answer, while others have more than one. Every problem will have at least one correct answer. You will be awarded points for selecting a correct answer, and you will lose points when you choose an incorrect one.

Permitted aids

Any written or printed material.
A calculator (running on batteries and without any communication facilities)

1(a) Porter
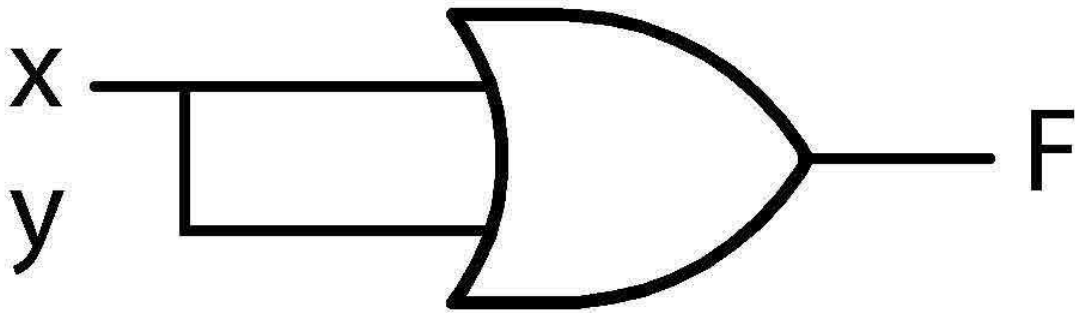
What is the function at the output:
Select one or more alternatives:

- ☐ F = x´

- ☐ F = x + y

- ☐ F = x

- ☐ F = xy

Maximum marks: 2

1(b) Teori

In the course we have talked about Flip-Flop, what is it?
Select one or more alternatives:

- ☐ Circuits that lock or latches

- ☐ Gates that opens

- ☐ Circuits that can flipp

- ☐ Sandals

Maximum marks: 2

1(c) **Teori**

Which of the following statement is true? ((Data in this context mean the information/bit that is stored in memory)

Select one or more alternatives:

☐ In memory hierarchy, the smallest data is the fastest to process so they are closest to the CPU

☐ In memory hierarchy, only the hard disk is loaded with all data, the others get just one copy

☐ In memory hierarchy, the largest data has the most power and can override any other minor data.

☐ ALU is a sequential circuit that controls the entire memory hierarchy.

☐ In memory hierarchy, it is Cache that determines what the other elements (i.e. RAM) can store as data

Maximum marks: 2

1(d)   **Kretsanalyse**
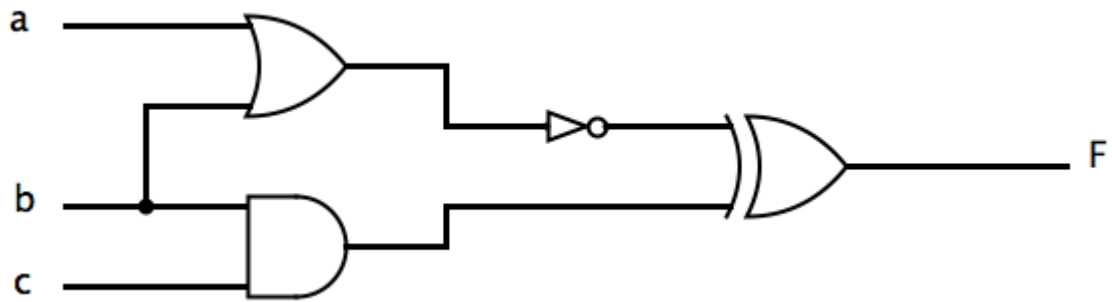
What is the output for the circuit?

Select one or more alternatives:

☐ F = a´b´ + bc

☐ F = ab + b´c´

☐ F = (a+b)´+ (bc)

☐ F = a´b´+ b´c

☐ F = abc + bc

☐ F = a XOR b

☐ F = a

☐ F = (a´+ b´) + bc

Maximum marks: 3

1(e) Teori

Which of these functions can an ALU circuit do?
Select one or more alternatives:

- ☐ Do arithmetical operations as DIV, SUB ...

- ☐ ALU stands for Aluminum and it is the material used to construct the circuit with.

- ☐ Increase the speed of the circuit by adjusting the time it takes from RAM to Cache

- ☐ Reduce HAZARDs by changing the order of the inputs

- ☐ Write data to RAM

- ☐ Do addition

- ☐ Do logic operations as AND, OR, NOT ...

Maximum marks: 4

1(f) # K-map 1

The expression for the given Karnaugh diagram is:

Select one or more alternatives:

☐ F = bd´+ c´d´+ bc + ab´

☐ F = a´c´d´ + abd´+ a´bc + ab´cd

☐ F = ab´d + bcd´+ a´c´d´+ b´d´

☐ F = c´d´+ ab´d + bd´+ a´bc

Maximum marks: 4

1(g) Forenkling av uttrykk

Show the process of simplification for $F = F(a, b, c) = \sum(0, 2, 4, 6)$

Move all possible simplifying steps into the gray rectangle.

Points will be awarded thus:

1 point per correct block

-1 point per incorrect block

You will be awarded bonus points if all answers are correct.

F = a´b´c´+ a´bc´+ ab´c´ + abc´

F = c   F = ac´   F = abc + ab´c + a´bc + a´b´c

F = c´(a XOR b) + c´(a XNOR b)   F = ab   F = a´c´(b´+b) + ac´(b+b´)

F = c´(a´+a)   F = (a´b´c) + (ab´c) + (ab´c´) + (a´b´c)

F = b´c´   F = b

F = a´c´+ ac´)(b+b´)

F = b´c´(a + a´) + ac(b + b´)   F = c´

F = (a+b+c)(a+b´+c)(a´+b+c)(a´+b´+c)

Maximum marks: 10

2(a)   **Binære tall 1**

The value 27_{10} (i.e., 27 in base 10 notation) may also be represented in other number systems. Which of these values are equal to 27_{10}?

Select one or more alternatives:

☐ 123_4

☐ 1000_3

☐ 102_5

☐ 11001_2

Maximum marks: 3

2(b)   **Binære tall 2**

The value 92_{10} (i.e., 92 in base 10 notation) may also be represented in other number systems. Which of these values are equal to 92_{10}?

Select one or more alternatives:

☐ 108_9

☐ 10102_3

☐ 134_8

☐ $7A_{12}$

Maximum marks: 3

2(c) Bit og byte

A byte contains these bits:

0	1	1	1	0	0	0	1

Which values may be represented by these bits?
Select one or more alternatives:

- [ ] 97

- [ ] 65

- [ ] 113

- [ ] -143

Maximum marks: 3

2(d) Assembler 1

```
        .globl   f1
f1:
        movq     %RDI,%RAX
        addq     %RSI,%RAX
        subq     %RDX,%RAX
        ret
```

```
 long res = f1(1, 3, 5);
```

What is the result of calling function **f1**?
Select one or more alternatives (but only one is correct):

- [ ] -1
- [ ] 3
- [ ] 5
- [ ] 1

Maximum marks: 4

2(e) Assembler 2

```
        .globl  f2
f2:
        movq    $100,%RAX
        movq    v,%R10
        cqo
        idivq   %R10
        ret

        .data
v:      .quad   7
```
```
long res = f2();
```

What is the result of calling function **f2**?

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

☐ 10

☐ 100

☐ 14

☐ 7

Maximum marks: 4

2(f) Assembler 3

```
        .globl   f3
f3:
        movq     %RDI,%RAX
        andq     $1,%RAX
        ret
```
```
long res = f3(11);
```

What is the result of calling function **f3**?

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

☐ 12

☐ 11

☐ 1

☐ 0

Maximum marks: 4

2(g) Assembler 4

```
        .globl   f4
f4:
        movq     $1,%RAX
        subq     %RSI,%RDI
        jz       f4x
        movq     $0,%RAX
f4x:
        ret
```

```
long res = f4(2, 5);
```

What is the result of calling function **f4**?

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

☐ 2

☐ 0

☐ 5

☐ 1

Maximum marks: 4

3(a) Lagdeling

Why do we have layers in the Internet architecture?
Select one or more alternatives:

☐ To save energy.

☐ To allow for changing components that offers specific services without changing the entire system.

☐ To make sure that all the components in the architecture does not need to support the functionality of all the layers.

☐ Because it took too long time to standardize all the protocols.

Maximum marks: 3

3(b) TCP/IP-modellen

Which layers do we have in the TCP/IP-model?
Select one or more alternatives:

- ☐ The bit layer, the ARP layer, the DHCP layer, the UDP layer and the FTP layer.

- ☐ The Physical layer, the Link layer, the Network layer, the Transport layer and the Application layer

- ☐ The TCP-layer and the IP-layer.

- ☐ The physical layer, the link layer, the network layer, the transport layer, the session layer, the presentation layer and the application layer.

Maximum marks: 1

3(c) Peer-to-peer

Which statements are true?
A peer-to-peer access model...
Select one or more alternatives:

- ☐ can help to avoid that a company or government has control over the service.

- ☐ has a central server that receives requests from many clients.

- ☐ has a distributed ownership.

- ☐ is only used for illegal services.

- ☐ has equal host machines that cooperate to deliver a service.

Maximum marks: 4

3(d) Subnett

A subnet has the netmask 11111111.11111111.11100000.00000000
How many valid IP-addresses can you assign to hosts in the subnet?
Select one or more alternatives:

- ☐ 65535

- ☐ 2046

- ☐ 254

- ☐ 2047

- ☐ 65534

- ☐ 255

Maximum marks: 2

3(e) Overføring

You want to download a 50 megabyte file, and the maximum download speed on your internet connection is 20 megabit per second. What is the theoretical shortest transfer time?
Select one or more alternatives:

- ☐ 10 seconds

- ☐ 50 seconds

- ☐ 20 seconds

- ☐ 2.5 seconds

Maximum marks: 2

3(f) UDP

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

- ☐ Connection-oriented

- ☐ Flow control

- ☐ Congestion control

- ☐ Multiplexing over IP-addresses (ports)

- ☐ None of these

- ☐ Bytes are delivered in the order transmitted

- ☐ Checksum

Maximum marks: 3

3(g) Switch

What is a "switch" in a computer network?
Select one or more alternatives:

- ☐ A service that assigns IP-adresses to computers in a local area network (LAN).

- ☐ A toggle for turning the computer on and off.

- ☐ A unit that forwards packets to other subnets on the Internet.

- ☐ A unit that forwards packets in the link layer.

- ☐ A unit that forwards packets within a local area network (LAN)

Maximum marks: 3

3(h)   Broadcast

Why should a broadcast domain not be configured to be too large?
Select one or more alternatives:

☐ Lookups in the ARP-table takes too long.

☐ It takes too long to route the traffic via all the hosts.

☐ It is no problem as long as the network topology is a star network.

☐ The noise from broadcast traffic (like DHCP and ARP) might grow too large and affect other traffic negatively.

Maximum marks: 1

3(i)   HTTP - Del 1

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

☐ The TCP connection will continue to try to connect, even if it is closed or interrupted.

☐ 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.

Maximum marks: 1

3(j) NAT

Which service is offered by Network Address Translation (NAT)?
Select one or more alternatives:

- It enables many units on a local area network to share one externel/public IP address.

- It makes it easier for hosts on the Internet to connect to machines in the local area network.

- It translates between MAC adresses and IP addresses.

- It broadcasts which port number that is used by a specific service.

Maximum marks: 2

3(k) HTTP - Del 2

Which statements are true?
Multiplexing in HTTP...
Select one or more alternatives:

- ...means that the client sends several requests, and the server must reply to them in the order they arrived from the client.

- ...means that the server can "guess" which requests will arrive from the client and send replies before it has received the actual request.

- ...means that the client sends several requests, and the server can send replies to all of them in an order determined by the server.

- ...means that for each request sent by the client, it has to wait for a reply to that specific request before sending the next one.

Maximum marks: 2

3(l)   DNS - Del 1

A root server in the DNS hierarchy keeps this information:
Select one or more alternatives:

- ☐ A list of free IP addresses in the Internet.

- ☐ Information about DNS servers of the the top level domains (TLDs).

- ☐ A list of all the IP addresses in an organisation (like uio.no).

- ☐ A list of IP-addresses and their corresponding MAC addresses.

Maximum marks: 1

3(m)   DNS

What is DNS-prefetching?
Select one or more alternatives:

- ☐ 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.

- ☐ A service caches the MAC addresses of webservers for fast lookups.

Maximum marks: 1

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:

☐ Access control

☐ Identification

☐ Non-repudiation

☐ Biometrics

☐ Authorization

☐ Data encryption

☐ Availability

☐ System authentication

Maximum marks: 2

4(b) Sikkerhetstiltak 1

A) Which of the following security controls may be used to ensure the security service confidentiality?
Select one or more alternatives:

☐ Encryption

☐ Identify and authenticate users

☐ Logging of system events

☐ Redundancy of resources

☐ Access control

☐ Training of users

B) Which of the following security controls may be used to ensure the security service accountability?
Select one or more alternatives:

☐ Encryption

☐ Access control

☐ Training of users

☐ Redundancy of resources

☐ Logging of system events

☐ Identify and authenticate users

Maximum marks: 3

4(c)   Sikkerhetstiltak 2
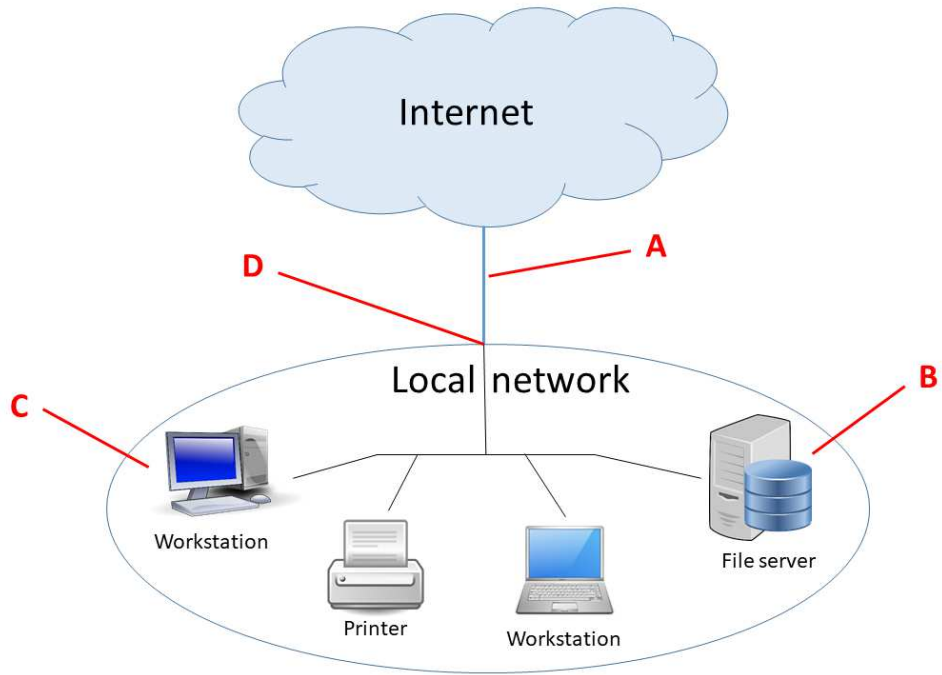
This figure illustrates a local network connected to the internet.

Please match the values:

	D	B	A	C
Intrusion detection	○	○	○	○
Backup	○	○	○	○
User training	○	○	○	○
Encrypted networktraffic	○	○	○	○
Firewall	○	○	○	○

Maximum marks: 3

4(d) Tilgangskontroll

Which is the fundamental elements in a system for access control:
Select one or more alternatives:

☐ Identification, authentication and authorization.

☐ Shared keys, authorization and user identity.

☐ Authentication, privileges and user identity.

☐ Passwords, access and encryption.

Maximum marks: 2

4(e) Autorisering

Authorization is a term within information security. Which of the following characterizes authorization?
Select one or more alternatives:

☐ If an identity is authenticated in a system the identity is also authorized in the same system.

☐ Authorization is to to specify access and user privileges for entities, roles and processes.

☐ Authorization follows a predifined policy.

☐ Passwords are used as authenticators for authorizing entities, roles, and processes.

Maximum marks: 3

4(f)   **Skadevare**

Malware is a term for software designed to intentially harm a computer system.
Match the correct functionality to the listed malware

	Keylogger	Worm	Virus	Logic bomb	Backdoor
Monitor all keyboard input from the user	○	○	○	○	○
Runs when spesific conditions occur	○	○	○	○	○
Access to a computer system trough hidden entry	○	○	○	○	○
Replicates when accessed	○	○	○	○	○
Replicates itself in order to spread to other computers	○	○	○	○	○

Maximum marks: 3

4(g) **Personvern**

The Norwegian "Lov om behandling av personopplysninger" (Personal Data Act) distinguishe between ordinary personal data and sensitive personal data.

Note: All <u>sensitive</u> personal data is basically also personal data, but in this assignment you are asked to categorize the sensitive personal data as sensitive.

Please match the values:

	Ordinary personal data	Sensitive personal data
Convicted of criminal act	○	○
Suspected of crime	○	○
Membership in sports club	○	○
Iris pattern	○	○
Head shape	○	○
IP address	○	○
Email address	○	○
Membership in trade union	○	○

Maximum marks: 2

4(h)   Kryptografi og nøkkelutveksling

Cryptography is used to protect information against transparency and modification. To encrypt and decrypt information, cryptographic keys are used. Assymetric encryption uses a key pair consisting of a private and a public key.

Which security services should be used to ensure safe storage of a public assymetric key?

Select one or more alternatives:

☐ The public key is public available and therefore need no protection.

☐ The public key must be stored in a manner that ensures confidentiality and the key's integrity and authenticity

☐ It is important to know who uses a public key, and users and systems therefore have to authenticate before use of the key to ensure accountability.

☐ The public key must be stored in a manner that ensures the key's integrity and authenticity.

Maximum marks: 2.5

4(i) Trusselmodellering 1

A healthcare business processes and stores a wide range of patient information, partly of a sensitive nature. The system is closed and not connected to networks other than the internal network for this particular system.

Which of the following statements will you represent as true on the basis of this information?

Select one or more alternatives:

- Ensuring accountabillity is not important if you provide proper mechanisms for authentication, such as two-factor authentication.

- Since the system is closed, there is no risk of external attacks, and it is therefore not necessary to prioritize the security of information highly.

- The healthcare business should have a carefully prepared policy describing which employees have access to read, change and delete information about which patients.

- Physical protection of end nodes in the system (such as the employee's workplace computers) is particularly important.

Maximum marks: 3

4(j) Trusselmodellering 2

Ransomware is a malware which infected a large number of computers around the world during the spring 2017.

Mark the action(s) which are useful to minimize the risk of beeing hit and hurt by a ransomware attack:

- File encryption

- Antivirus

- Backup

- Security patches

- Strong access control

Maximum marks: 1.5