



**Note:**

- During the attendance check a sticker containing a unique code will be put on this exam.
- This code contains a unique number that associates this exam with your registration number.
- This number is printed both next to the code and to the signature field in the attendance check list.

## Computer Networking and IT Security

**Exam:** INHN0012 / Endterm

**Date:** Thursday 16<sup>th</sup> February, 2023

**Examiner:** Prof. Dr.-Ing. Stephan Günther

**Time:** 14:00 – 15:30

Before we proceed with reading the processing instructions, please answer the following questions. This information helps us to examine learning success depending on participation in individual lecture components. The information is **voluntary** and **not considered for evaluation**, i. e., answers to these questions do not give credits. In order to exclude any influence, this page will not be made accessible during the correction.

a) Did you attend the lecture?

1 (regularly)

2 (sometimes)

3 (never)

b) Did you attend the tutorials?

1 (regularly)

2 (sometimes)

3 (never)

### Working instructions

- This exam consists of **12 pages** with a total of **6 problems** and the cheatsheet distributed with the exam. Please make sure now that you received a complete copy of the exam.
- The total amount of achievable credits in this exam is 90 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - one **non-programmable pocket calculator**
  - one **analog dictionary** English ↔ native language
- Subproblems marked by \* can be solved without results of previous subproblems.
- **Answers are only accepted if the solution approach is documented.** Give a reason for each answer unless explicitly stated otherwise in the respective subproblem.
- Do not write with red or green colors nor use pencils.
- Physically turn off all electronic devices, put them into your bag and close the bag.

Left room from \_\_\_\_\_ to \_\_\_\_\_ / Early submission at \_\_\_\_\_

## Problem 1 Multiple Choice (18 credits)

The following subproblems are multiple choice / multiple answer, i. e., at least one answer per subproblem is correct. Subproblems with a single correct answer are graded with 1 credit if correct. Those with more than one correct answers are graded with 0.5 credit per correct answer and  $-0.5$  credit per wrong answer. Missing crosses have no influence. The minimal amount of credits per subproblem is 0 credits.

Mark correct answers with a cross



To undo a cross, completely fill out the answer option



To re-mark an option, use a human-readable marking



a)\* Which statements regarding MLT-3 are correct?

- It is a line code                       It is a source code                       It is guaranteed to be DC-free  
 It is a channel code                       One symbols encodes 3 bit                       The spectrum is narrower than Manchester

b)\* How many broadcast domains does the network to the right contain?

- 3                       6                       1                       5                       2                       4

c)\* How many collision domains does the network to the right contain?

- 4                       2                       3                       1                       6                       5

d)\* Mark the adjacency matrix for the network to the right.

- $\begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}$                         $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$                         $\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

e)\* Given the distance matrix  $D$  for the network to the right. What is the minimum  $n$  such that  $D^n = D^{n+1}$  holds?

- $n = 1$                         $n = 4$                         $n = 3$                         $n = 6$   
  $n = 7$                         $n = 0$                         $n = 2$                         $n = 5$

f)\* Given the IP address 192.0.2.42, determine the respective PTR record in DNS.

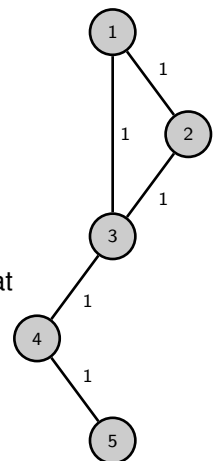
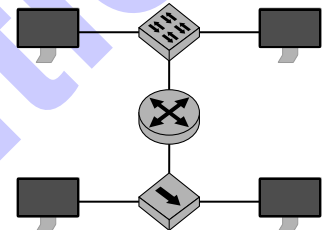
- 42.2.0.192.in-addr.arpa.                       192.0.2.42.                       There is no PTR record  
 192.0.2.42.in-addr.arpa.                       42.2.0.192.                       Something different

g)\* Which of the following syscalls are usually **only** used with datagram oriented sockets?

- sendto()                       send()                       bind()                       accept()  
 recvfrom()                       recv()                       listen()                       connect()

h)\* Given the binary value 10011100 in network byte order. Determine its representation in little endian.


- 10011100                       00111001                       11001001                       00110110






## Problem 2 TCP (15 credits)


In this problem we consider the message exchange between client and server when accessing `http://cns.net.in.tum.de`.

- 0  a)\* A server receives both a UDP datagram and a TCP segment from the same source address. Both feature the same port number as their source port. Is this a problem?

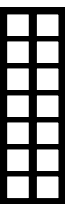
1  No, as the server and client can differentiate based on the L4 protocol.

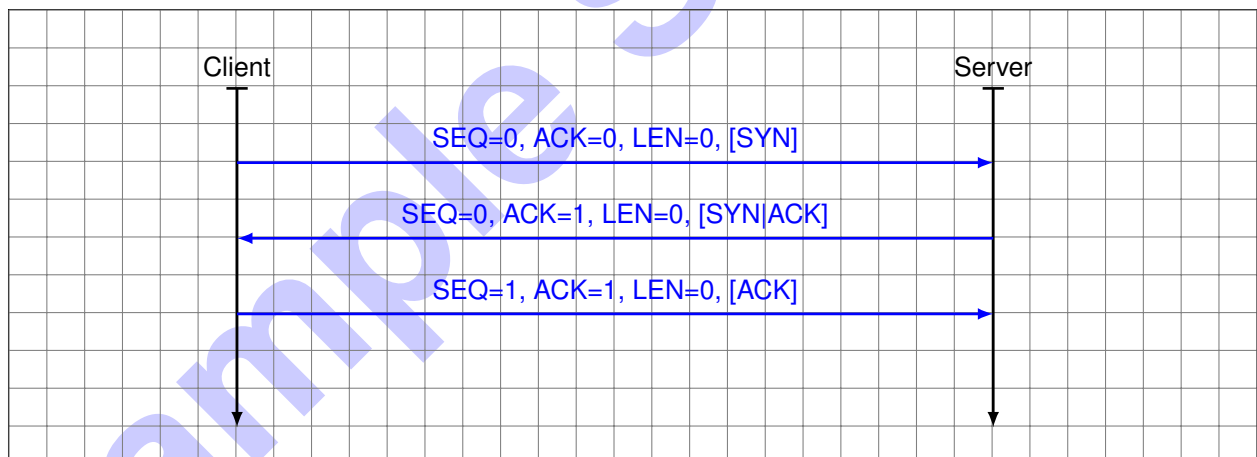
- 0  b)\* Justify which port number will be used as source port by the client? Assume the client is an unprivileged process.


1  An (unused) port number ranging from 1024 to 65 535 (ephemeral port).

- 0  c)\* Justify which port number will be used as destination port by the client?

1  Port 80 (well-known port for HTTP)

- 0  d)\* Sketch the connection establishment in the chart below. For each segment exchanged between client and server, state the SEQ and ACK numbers, the segment length (LEN), and relevant flags that are set.

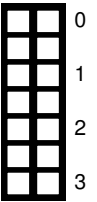
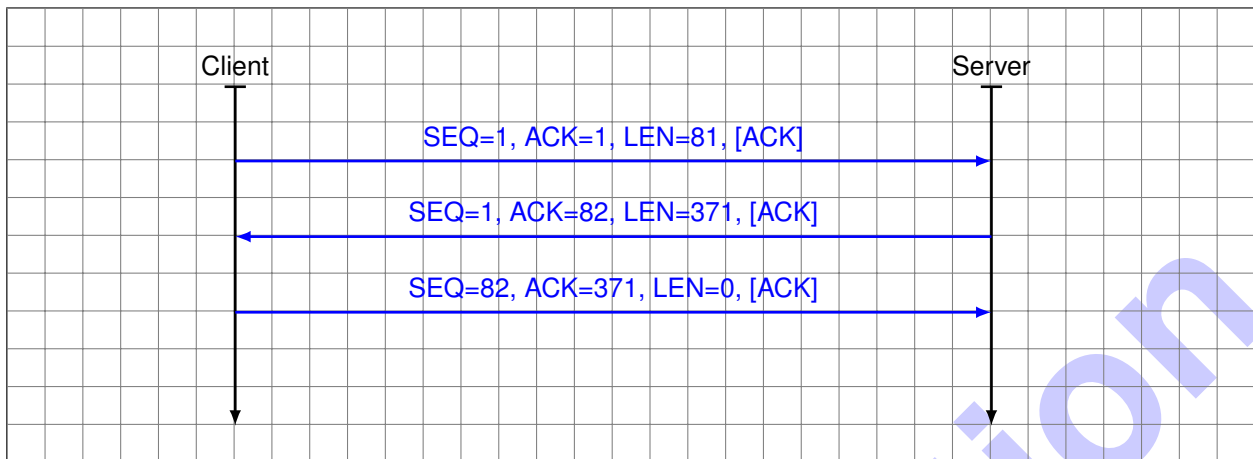


- 0  e) What is the payload (protocol and type, action, or method) of the next segment sent by the client?

1  HTTP GET (requesting `cns.net.in.tum.de`)

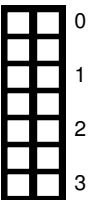
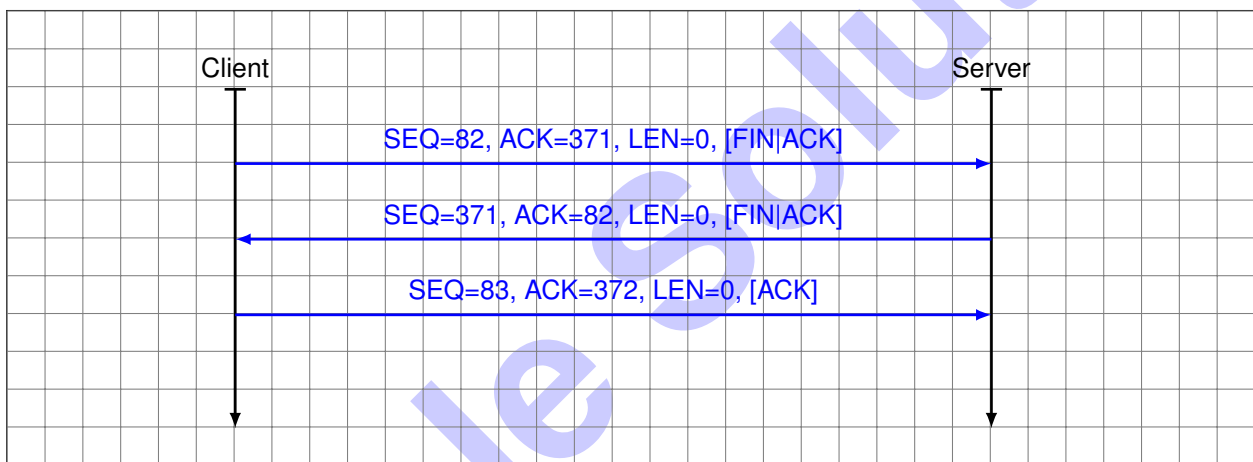
The segment sent in Subproblem e) has a payload of 81 B, followed by a response of length 370 B by the server.

f) Draw the message exchange so far assuming that the MSS is not exceeded for individual segments.



After that, the connection termination is initiated by the client and completed from both sides.

g)\* Draw the message exchange during termination.



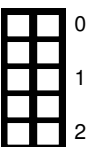
The reply from the server in Subproblem f) has the following text content:

```

HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0
Date: Thu, 02 Feb 2023 10:55:24 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: https://cns.net.in.tum.de/
(...)
  
```

h)\* What does the response mean?

In particular, the response code 301 means that the destination is no longer available but a redirect exists.  
 In that case, the redirect is simply to `https://...`, i.e., making the website reachable via unsecured HTTP by immediately redirecting to a TLS-based connection.



### Problem 3 DNS (13.5 credits)

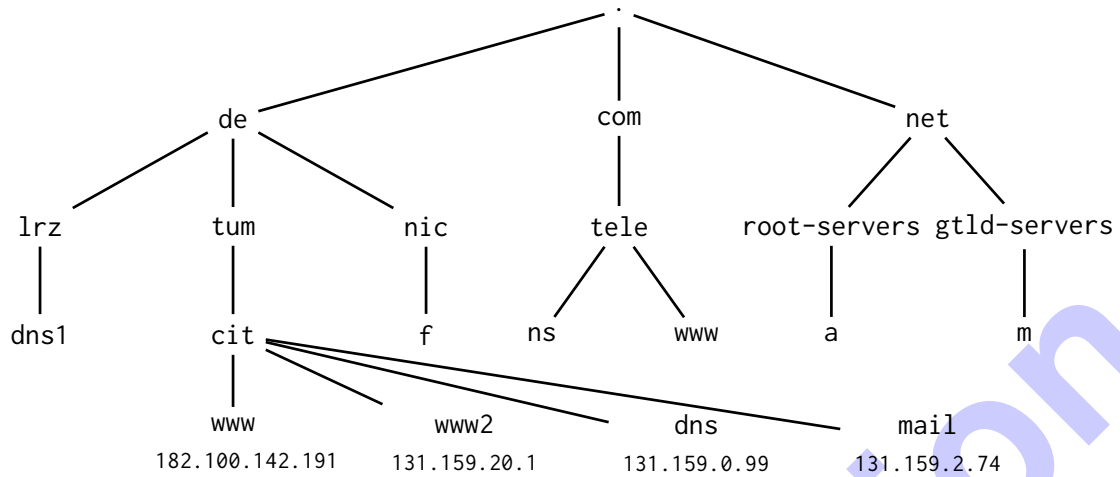


Figure 3.1: A part of the DNS.



a) Briefly describe the purpose of DNS.

The mapping between FQDN and IP addresses.



b) Briefly describe the difference between a fully and non-fully qualified domain name.

A fully qualified domain name starts at the root, denoted by the ".".  
A non-fully qualified domain name starts at an intermediary node of the DNS.

Figure 3.1 shows the zone file of the authoritative name server for `cit.tum.de`.

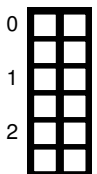
```

1 $ORIGIN cit.tum.de.
2 $TTL 1H
3
4 @ IN SOA dns.cit.tum.de. hostmaster.cit.tum.de. (...)
5
6 cit.tum.de.      IN      NS      dns.cit.tum.de.
7 cit.tum.de.      IN      MX      20 mail.cit.tum.de.
8
9 dns.cit.tum.de.  IN      A      131.159.0.99
10 mail.cit.tum.de. IN      A      131.159.2.74
11 www.cit.tum.de.  IN      A      182.100.142.191
12 www2.cit.tum.de. IN      A      131.159.20.1

```



Figure 3.2: DNS zone file on nameserver `dns.cit.tum.de`



c)\* Add the mail server `mail.in.tum.de` to the zone file given in Figure 3.2 based on the information from Figure 3.1 and assign it preference **20**.

d)\* Add all other missing records in Figure 3.2 based on the information from Figure 3.1.

e)\* What purpose does the TTL of 1 h in the DNS zone file serve?

A resolver might cache the result for the amount of time specified in the TTL. After the time has expired it must query the authoritative nameservers again.



f)\* What purpose does a zone transfer serve?

The zone file is synchronized onto secondary nameservers, which are authoritative for the same zone so that the latter have the up to date information.



g)\* What does "authoritative" mean in the context of DNS?

An authoritative nameserver for a zone holds the zone records for this zone and answers queries it.



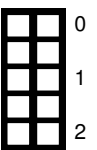
h)\* When does DNS use TCP instead of UDP?

When the request is larger than 512 B.



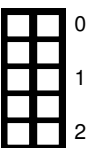
i)\* How is the administrator of dns.cit.tum.de. ensured that no malicious server answers the requests for their zone, assuming that man-in-the-middle attacks are not possible.

The root nameservers serve as a root of trust, as a resolver knows their IP addresses without querying the DNS. Starting at the root nameservers, only nameservers that are contained in the zone files will be contacted. Therefore, assuming the root is trusted, only trusted servers are contacted. An untrusted nameserver is therefore never contacted as no server points to it.



j) Explain the difference between recursive and iterative name resolution.

With recursive resolution, only one request for a resource record is made to a configured resolver, which returns the final response.  
With iterative resolution, the FQDN is instead resolved starting at the root zone (or the last known SOA) by querying the authoritative name servers for the respective zones. Their answers contain either the FQDN of an authoritative name server of the next lower zone or the final resource record if the queried name server is authoritative for it.



## Problem 4 Wireshark (15.5 credits)

Consider the Ethernet frame depicted in Figure 4.1. In the following, we will analyze this frame step by step.

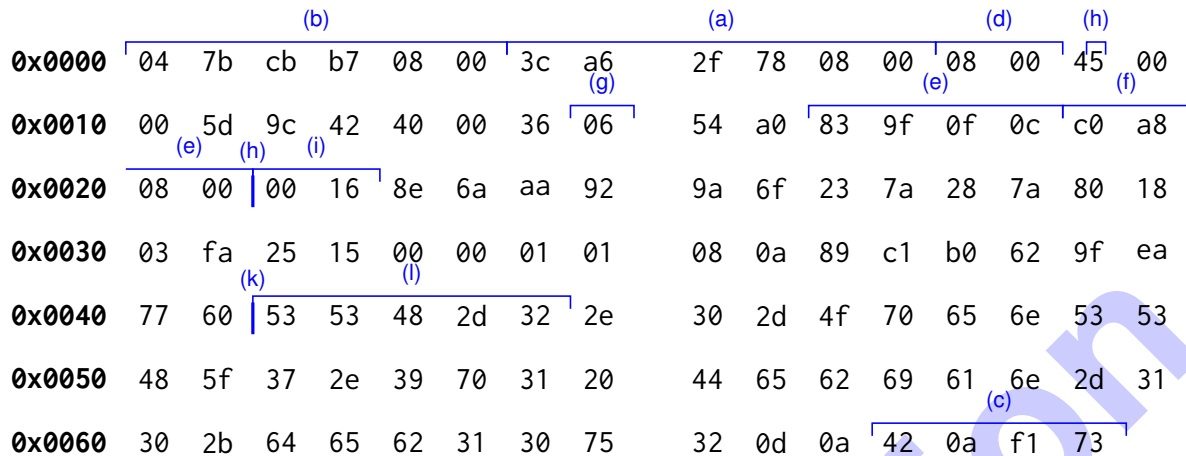


Figure 4.1: Ethernet frame including checksums.

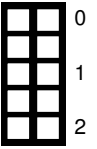
For each of the following subproblems, clearly mark the respective header fields in Figure 4.1. **Take care that markings can uniquely be related to individual subproblems**, i. e., note the subproblem above markings. Answers that cannot be followed **are not graded**.

- 0  a)\* Mark the transmitter address of layer 2 in Figure 4.1.
- 0  b)\* Mark the receiver address of layer 2 in Figure 4.1.
- 0  c)\* Mark the frame check sequence in Figure 4.1.
- 0  d)\* What protocol is used as L3 PDU? Mark the respective header field in in Figure 4.1.
- IPv4
- 0  e) State the layer 3 source address in its usual and fully abbreviated form.
- 131.159.15.12
- 1  f) State the layer 3 destination address in its usual and fully abbreviated form.
- 192.168.8.0
- 0  g) What protocol is used as L4 PDU? Mark the respective header field in in Figure 4.1.
- TCP
- 0  h) At which offset does the layer 4 PDU start? Give an explicit reason how you determine this offset.
- Offset: 0x0022                      Reason: IHL = 0x5 ⇒ 20 B IP header / no options



i) What type is the layer 7 protocol probably?

The destination port is an ephemeral port. However, the source port 22 suggests that it is SSH.



j) For what purpose is that protocol used?

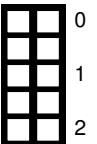
Encrypted remote control of computers.



k) Determine the offset where the L7 PDU starts. Give an explicit reason how you determine this offset.

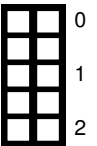
Offset:  $0x0042$

Reason:  $\text{Offset} = 0x8 \Rightarrow 32 \text{ B TCP header}$



l) Decode the first 5 B of the L7 SDU.

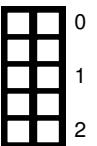
ASCII coded string starting at offset  $0x0042$ :  $0x53 \ 0x53 \ 0x48 \ 0x2d \ 0x32 = \text{SSH-2}$



## Problem 5 Short Questions: Security (20 credits)

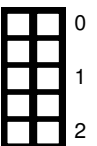
a)\* Differentiate Authentication from Authorization.

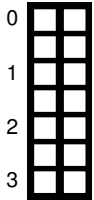
Authentication is the process of proving an entities identity.  
Authorization determines which privileges an entity has.



b)\* Why are so-called hybrid encryption schemes employed? Describe the function of such scheme, and why each component is used.

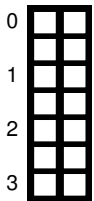
In such scheme, an asymmetric scheme is used to establish a secret. This solves the problem of not having a shared secret in the beginning as a key can be encrypted with the receiver's public key and only the receiver can decrypt it using its private key.  
After key establishment, a symmetric scheme is used. This is as symmetric ciphers have a higher throughput as they are cheaper to calculate.





c)\* Name and describe the three properties of a cryptographic hash function.

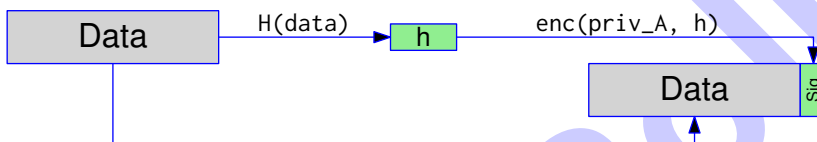
1. **Pre-Image Resistance:**  
Given a hash value, it is hard to find an input that results in the same hash.
2. **Second Pre-Image Resistance:**  
Given a message, it is difficult to find another input that results in the same hash.
3. **Collision Resistance:**  
It is difficult to find a pair of two different messages that result in the same hash.



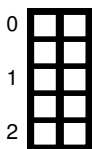
d)\* Sketch a simple scheme for signing data. **Sketch only the signature generation!**

Use the block diagrams you know from the lecture. **You do not need to reason your answer.**

You can use the cryptographic hash function  $H(x)$  and assume the signing party to possess a key pair  $(key_{priv}, key_{pub})$ . For encrypting and decrypting you may use  $aenc(key, msg)$ ,  $adec(key, msg)$  as well as  $enc(key, msg)$  and  $dec(enc, msg)$ .



- General idea makes sense and reflects a signature scheme
- Signature cannot be forged without secret (= not a checksum)
- Signature is only over the hash of the message (= efficient to calculate)



e)\* Describe the tasks and responsibilities of a Certification Authority (CA) and Registration Authority (RA).

A CA is responsible to issue the certificate for the requesting entity after the RA has checked the entities identity and relayed the request to the CA.

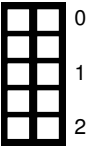


f)\* Why is the usage of true randomness for cryptographic purposes important.

A predictable random number generator results in lower entropy, leading to weaker or even broken keys/encrypted material. Keys and cypher streams might thus become predictable.

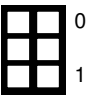
g)\* Differentiate AH from ESP in the context of IPsec.

ESP offers confidentiality, authenticity as well as integrity protection for its own headers and the IPsec payload.  
AH only offers authenticity and integrity protection, but additionally for the preceding IP header.



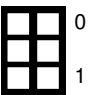
h)\* What problem does IPsec pose to NAT, and how does NAT-T solve it?

Since IPsec encrypts the layer 4 header, the port numbers cannot be used for NAT. Therefore, a dummy UDP header is inserted which only serves the purpose of traversing the NAT.



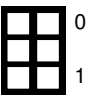
i)\* Describe the properties offered by a cryptographic scheme implementing Perfect Forward Secrecy (PFS).

A cryptography scheme provides Perfect Forward Secrecy (PFS) if previously encrypted sessions maintain their confidentiality in the scenario that the long-term secret, the current session keys, and all sessions' traffic become known to an attacker.



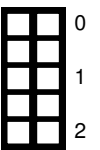
j)\* What main drawback does the usage of AES-ECB come with?

The same plain text results in the same cipher text. Therefore, patterns in the plain text propagate into the cipher text.



k)\* Describe how a length-extension attack against Merkle-Damgård-based hash functions works.

A Merkle-Damgård based scheme outputs the entire internal state of the hash function as digest. Therefore, the digest can be loaded back into the hash function, and further blocks be hashed. This allows breaking e.g. the signature scheme  $\text{sig}=\text{hash}(\text{key}|\text{msg})$ .



## Problem 6 Short Questions: General Knowledge (8 credits)



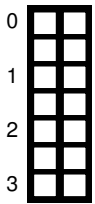
a)\* What are well-known ports?

TCP/UDP ports with port numbers smaller than 1024.



b)\* What is a major advantage of OSPF over RIP?

OSPF has knowledge of the network topology, therefore it can detect loops.



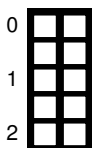
c)\* Assume a channel with a bandwidth of 35 MHz. Calculate the maximum data rate given a signal to noise ratio of 45 dB.

$$\begin{aligned} SNR_{dB} = 10 \log_{10} SNR &\Rightarrow SNR = 10^{\frac{45}{10}} = 10^{4.5} \\ r_{max} = B \log_2 (1 + SNR) \text{ bit} \\ &= 35 \cdot 10^6 \text{ Hz} \log_2 (1 + 10^{4.5}) \text{ bit} \\ &\approx 523.2 \text{ Mbit/s} \end{aligned}$$



d)\* Which purpose does ARP serve?

Resolution of layer 2 addresses to layer 3 addresses.



e)\* A time-continuous signal with unknown properties, whose signal level varies in the interval  $[-3, 3]$ , shall be digitized such that the quantization error is minimal. The resulting signal levels are encoded using 2 bit. Determine the signal levels and the maximum quantization error in the given interval.

- 2 bit  $\Rightarrow N = 4$  signal levels
- Level width  $\Delta = \frac{b-a}{N} = \frac{3}{2}$
- Maximum quantization error  $e_{max} = \frac{\Delta}{2} = \frac{3}{4}$
- Signal levels:  $-2.25, -0.75, 0.75, 2.25$