Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Esolution
Place student sticker here

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:**	Tuesday 24th February, 2026
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	14:00 – 15:30

Working instructions

- This exam consists of **12 pages** with a total of **6 problems**.
- The total amount of achievable credits in this exam is 90 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - the **provided cheat sheet** inside the exam booklet
  - 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.

Additional space for solutions–clearly mark the (sub)problem your answers are related to and strike out invalid solutions.

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 answer are graded with 1 credit per correct answer and -1 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)* What is the type of the following identifier or address? `70:2e:10:af:7f:ex:81:f0`

- ☐ MAC address
- ☐ IPv4 address
- ☐ IPv6 address
- ☒ None of the listed options
- ☐ IP identifier
- ☐ Port number

b)* What is the approximate SNR when sending a signal with a power of 220 mW and a noise power of 5 mW is measured?

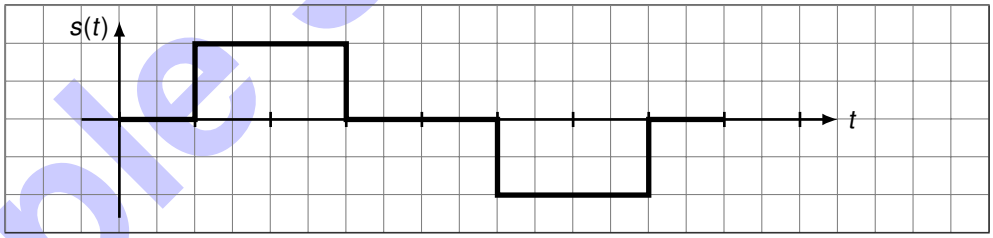
- ☐ ∼2.6 dB
- ☒ 44
- ☐ ∼0.2
- ☒ ∼16.4 dB
- ☐ 68
- ☐ ∼70.4 dB

c)* Given is an encoder, that converts code words of length 8 bit to channel words of length 10 bit. How much added redundancy is contained in 22 channel words?

- ☐ 2 bit
- ☐ 220 bit
- ☐ 22 bit
- ☐ 176 bit
- ☐ 18 bit
- ☒ 44 bit

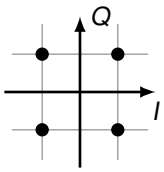
d)* Given is the baseband signal shown below, which encodes the bit sequence `0101 0101`. Which line code was used to encode the signal?

- ☐ NRZ
- ☐ Manchester
- ☐ RZ
- ☐ Rect
- ☒ MLT-3



e)* Which modulation scheme(s) does the adjacent signal constellation diagram represent?

- ☐ 2+2-AM
- ☐ 2+2-AK
- ☒ 4-QAM
- ☐ 2+2-PSK
- ☐ BPSK
- ☐ 4-ASK



f)* The header(s) of which protocol(s) can occur immediately after an Ethernet header?

- ☐ DNS
- ☐ UDP
- ☐ ICMPv6
- ☒ ARP
- ☐ ICMPv4
- ☐ NDP

g)* Which IP header fields are **guaranteed** to change when a packet is routed from one endpoint to another over multiple hops?

- ☐ Version
- ☐ Flow label
- ☒ TTL
- ☐ Fragment Offset
- ☐ Traffic Class
- ☒ Header Checksum
- ☐ Destination IP Address
- ☐ Protocol
- ☐ IHL

h)* Consider the IPv4 address range **10.8.0.0/24** that is divided into **eight** subnets with 32 addresses each. Which statements about these subnets are true?

- [ ] 10.8.0.255 is the broadcast address of the fourth subnet.
- [x] 10.8.0.224 is the network address of the last subnet.
- [ ] The prefix length of the subnets is /21.
- [x] Each subnet has 30 host-assignable addresses.
- [x] 255.255.255.224 is the subnet mask of each subnet.
- [ ] 10.8.0.32 is the first host-assignable IP address in the second subnet.

i)* What is the *Maximum Segment Size* (MSS) between two directly connected hosts if the MTU is 1 280 B? Assume that IPv6 and TCP are used without extension headers or options.

- [ ] 1 280 B
- [ ] 1 260 B
- [x] 1 220 B
- [ ] 980 B
- [ ] 1 460 B
- [ ] 1 440 B

j)* Which of the following properties apply to link-state routing protocols?

- [ ] Routers have no information about the network topology.
- [ ] The operating principle is similar to the Bellman-Ford algorithm.
- [x] The operating principle is similar to Dijkstra's algorithm.
- [x] Routers regularly exchange status messages.
- [ ] Routers determine a minimum spanning tree from the exchanged information.
- [ ] Routers only exchange cumulative costs with each other.

k)* Which are **not** standard HTTP methods?

- [x] FETCH
- [ ] PUT
- [ ] GET
- [ ] POST
- [ ] DELETE
- [ ] HEAD

l)* What is correct regarding DNS?

- [x] The TTL specifies how long a resource record may be cached.
- [ ] A resolver contacts at most one nameserver during iterative querying.
- [ ] Every resolver is an authoritative nameserver.
- [ ] PTR records must be in the same zone as the corresponding A records.
- [ ] A nameserver sends iterative queries.
- [x] Multiple nameservers can be authoritative for the same zone.

Problem 2 Switching WiFi (16 credits)

Given is the network shown in Figure 2.1. Assume that the notebooks are associated with the access point AP and that the switching table of SW is empty.

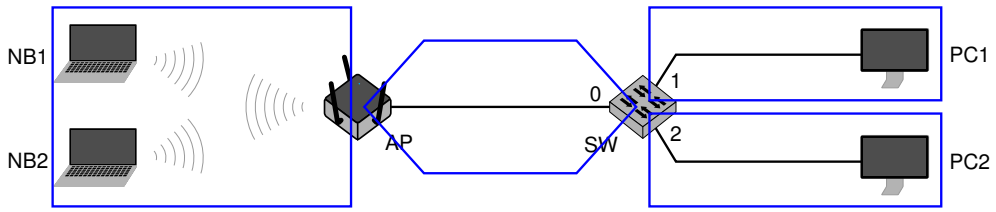


Figure 2.1: Topology

0 1 2

a)* Mark all collision domains in Figure 2.1. Make sure that interfaces are clearly associated with the respective collision domain.

b)* Briefly argue how many broadcast domains there are in this topology.

0 1

There are no routers, so this layer 2 network is one single broadcast domain.

0 1 2 3

c)* Argue for both the switch SW and the access point AP whether they have a MAC address or not.
Hint: Consider whether the device is transparent to the communication or not.

A switch is transparent and will simply forward frames according to the destination address, is not addressed and therefore does not have a MAC address.
An access point is always directly addressed by the associated wireless clients and therefore requires a MAC address.

NB1 wants to send a message **to PC2**. Assume that NB1 knows the MAC address of PC2.

0 1 2

d) Name all MAC addresses that are present in the frame on the link **from NB1 and AP** by specifying the respective device name. Additionally specify the meaning(s) of the addresses:

- SA: Source Address
- DA: Destination Address
- TA: Transmitter Address
- RA: Receiver Address

Hint: There are more rows than needed.

Address/Device	Meaning(s)
NB1	SA, TA
AP	RA
PC2	DA

The frame now reaches the switch SW.

e)* Argue to which ports (0,1,2) the switch will forward the frame to.

0
1

To all ports, except the incoming port, because the switching table is empty.

f)* Update the switching table in Table 2.1 so that it reflects the state after the frame passed the switch.

0
1

Subtask	Address/Device	Port
f)	NB1	0
i)	PC2	2

Table 2.1: Switching table of switch SW

g) Name all MAC addresses that are present in the frame on the link **from SW and PC2** by specifying the respective device name. Additionally specify the meaning(s) of the addresses.
Hint: There are more rows than needed.

0
1
2

Address/Device	Meaning(s)
NB1	SA, TA
PC2	RA, DA

PC2 responds to the request with another frame.

h) Argue to which ports (0,1,2) the switch will forward the frame **of the response** to.

0
1

To port 0, because it knows that NB1 is reachable on port 0.

i) Update the switching table in Table 2.1 so that it reflects the state after the frame **of the response** passed the switch.

0
1

j)* Name and explain a possible Denial of Service attack that can be performed on the wireless part of the network.

0
1

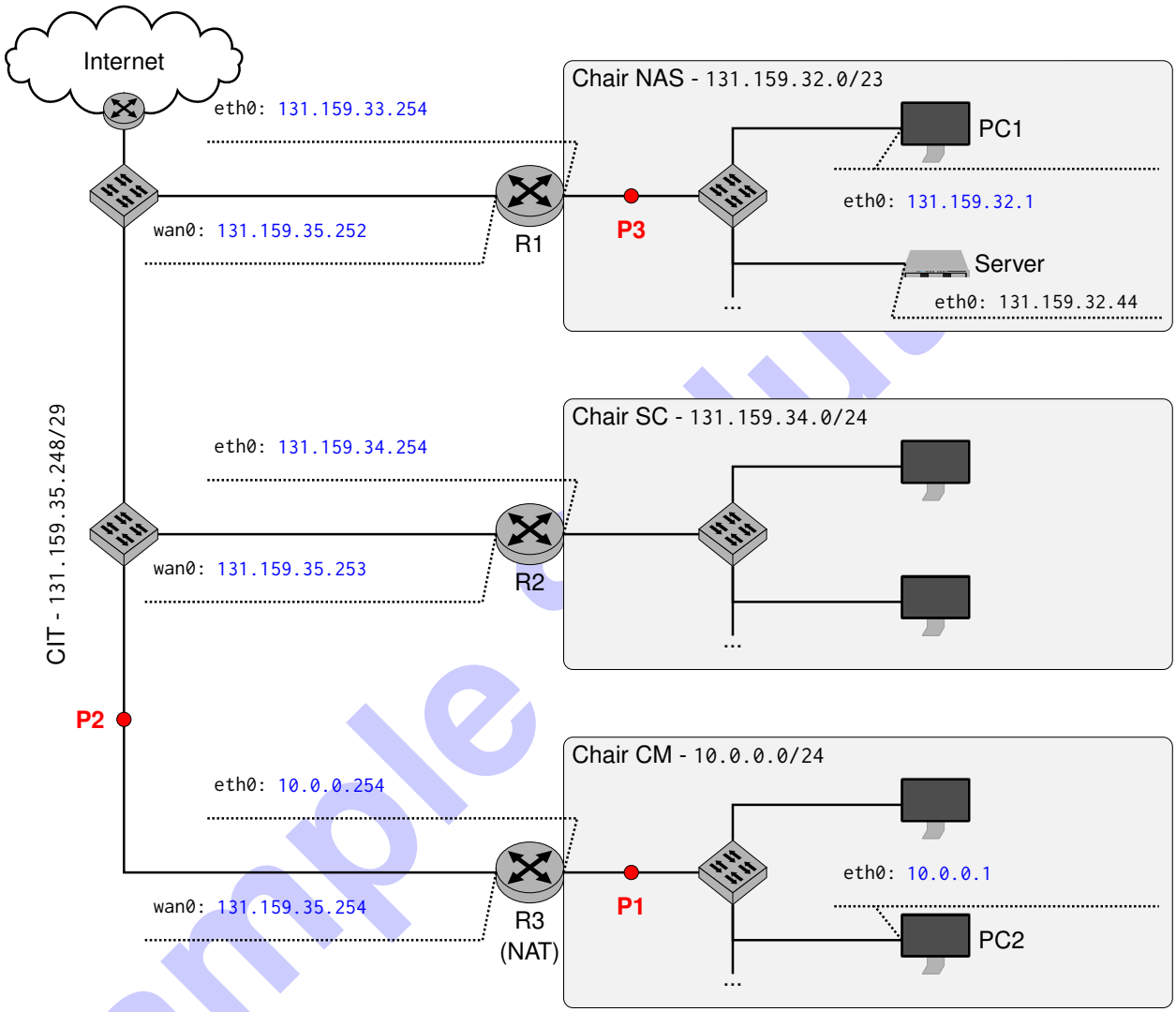
Jamming: constantly sending on the frequency band, thereby interfering with all other communication
or
Deauthentication: Deauthenticate associated clients from the network, forcing them to redo the handshake to rejoin

Problem 3 CIT Chairlink (15 credits)

In this task, you configure internal networks of and between chairs of the *School of Computation, Information and Technology*. All networks use public IPv4 addresses, except for the one of the CM chair. Unfortunately there were not enough addresses left, so they use a private address range and R3 implements NAT. Assume that all caches of all devices are empty.

0 1 2

a)* Assign valid IP addresses to the named interfaces in the topology. Mind the respective address ranges! Routers should have the last address of a network. When there are multiple routers, addresses should be in ascending order of the router index (i.e. R3 should have the highest address).



0 1

b)* Calculate the number of usable host addresses in the NAS network.

$N = 2^{32-23} - 2 = 2^9 - 2 = 510$

After the network setup, **PC1** wants to send an HTTP request to **Server** in the same network and already knows the IP address of the server. At this point however, PC1 is not able to contact the server.

0 1 2

c)* Explain why PC1 cannot contact the server, what information is missing and how that information can be obtained.

PC1 does not know the MAC address of the server and therefore cannot build the frame.
PC1 has to send an ARP request to obtain the MAC address of the server.

Now a member from the chair CM, working on **PC2** wants to access the server. To make this work, you have to configure the routers R1 and R3 such that they forward packets correctly.

d)* Write down all necessary entries of the routing tables of R1 and R3 respectively such that traffic is routed correctly from PC2 to the server and back from the server to the NAT router of PC2.
Hint: There are more rows than necessary.

0 1 2 3 4 5

Destination	Next Hop	Iface
131.159.35.248/29	0.0.0.0	wan0
131.159.32.0/23	0.0.0.0	eth0

Routing table of R1

Destination	Next Hop	Iface
131.159.35.248/29	0.0.0.0	wan0
10.0.0.0/24	0.0.0.0	eth0
131.159.32.0/23	131.15.35.252	wan0

Routing table of R3

After the routes are configured, everything should work. To verify this, you inspect the actual HTTP request **sent from PC2 to the server** at various points in the network.

e)* Complete the table below: Note down the addresses, ports and TTL for the **request** at each of the points P1, P2 and P3. Use the notation *device.interface* to refer to the MAC or IP address of a device. You can omit the interface on devices with only one interface.
In case a value is not specifically defined in this task, choose a sensible value!

0 1 2 3 4

Field	P1	P2	P3	*Spare*
Src MAC	PC2	R3.wan0	R1.eth0	
Dst MAC	R3.eth0	R1.wan0	Server	
Src IP	PC2	R3.wan0	R3.wan0	
Dst IP	Server	Server	Server	
TTL	64	63	62	
Src Port	12345	33344	33344	
Dst Port	80	80	80	

Problem 4 Wired shark (15 credits)

You are a network administrator at a media company and maintain a part of their network infrastructure shown in Figure 4.1:

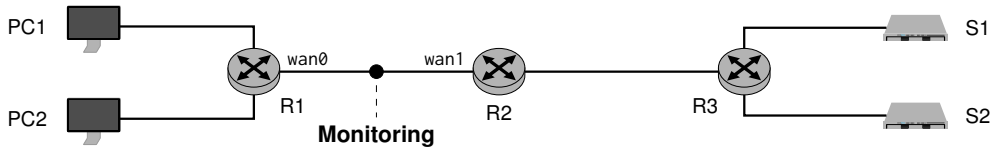


Figure 4.1: Network topology

Today, you are tasked with debugging a problem in a legacy video stream. You use Wireshark to monitor frames on the link between routers R1 and R2 and see multiple frames **from PC1 that should reach server S2**, but do not. Figure 4.2 shows such a frame.

```
                (b)                                     (a)                     (c)
0x0000  30 ee a4 4b 43 d5 e0 63   da 89 f1 ee 86 dd 60 07
                      (f)                         (d)
0x0010  45 3d 00 84 06 3f 20 01   0d b8 11 ab 00 01 32 44
            (d)
0x0020  d7 ff fe 65 dc 73 20 01   0d b8 11 ab 00 0d 00 00
                                      (g)
0x0030  00 00 00 00 00 02 c2 65   01 bb a2 77 24 07 00 00
            (h)
0x0040  00 00 80 02 fa f0 ee b8   00 00 01 01 08 0a b8 ba
                                                (x) Example
0x0050  4a 00 2b cf d4 80 a8 52   a7 c9 99 1d 82 10 37 ..
```

Figure 4.2: Ethernet frame (truncated)

First, you decide to gather some information about the involved devices and protocols.
Please note: Depending on the subproblem you must or should mark relevant parts of the hexdump—ensure that the markings are clearly associated with the subtask. Answers where the solution approach is not documented sufficiently **will not be graded**. Note down MAC and IP addresses in their respective formats and, in case of IPv6, their shortened form.

0 1

a)* What is the MAC address of R1.wan0? Only name and mark the respective header field.

Address: `e0:63:da:89:f1:ee` Field: Source MAC

0 1

b)* What is the MAC address of R2.wan1? Only name and mark the respective header field.

Address: `30:ee:a4:4b:43:d5` Field: Destination MAC

0 1

c)* Which network layer protocol is used?

Protocol: IPv6 Reasoning: EtherType = `0x86dd`

0 1 2

d) What is the IP address of PC1? Only name and mark the respective header field.

Address: 2001:db8:11ab:1:3244:d7ff:fe65:dc73 Field: Source IP

e) Through which mechanism was the IP address of PC1 most likely obtained? Explain shortly.

0 1

SLAAC, because of the clearly distinguishable 64bit EUI-64 Identifier with the constant value `ff:fe` in the middle

f) Which transport layer protocol is used?

0 1

Protocol: TCP Reasoning: IPv6 Next Header = `0x06`

g) Which application layer protocol is most likely used?

0 1

Protocol: HTTPS Reasoning: TCP Destination Port = 443

h) At what index (e.g. `0x0065`) in the frame does the PDU of layer 5 start?

0 1 2

Index: 0x0056 Reasoning: TCP Offset is `8` → TCP header is 32 B long

Then, you see another packet on the monitored link with an ICMPv6 message that provides additional information about the underlying problem. Figure 4.3 shows only the header and payload of the ICMP message.

```
                (i)
0x0000  01 00 ff ff 00 00 00 00   60 07 45 3d 00 84 06 3f
0x0010  20 01 0d b8 11 ab 00 01   32 44 d7 ff fe 65 dc 73
0x0020  20 01 0d b8 11 ab 00 0d   00 00 00 00 00 00 00 02
0x0030  c2 65 01 bb a2 77 24 07   00 00 00 00 80 02 fa ··
```

Figure 4.3: ICMPv6 message (truncated)

i)* What is the underlying cause of the ICMP message? Remember to name and mark respective fields.

0 1

Message cause: Destination Unreachable, no route to destination

Reasoning: ICMP type `0x01` and code `0x00`

j) Argue which device in the topology created this ICMP message.

0 1

R2: The TTL in the original datagram's IPv6 header contained in the ICMP message is still `0x3f`, therefore the original packet has not been forwarded by R2.

k) Explain what you might need to change in your network such that the packets are successfully received.

0 1

Update the routing table of R2 to successfully forward packets toward the servers.

Problem 5 Sampling and Quantization (13 credits)

Given is the analog signal of a sensor, shown in Figure 5, that represents the current draw of a motor. In order to process the signal in a controller, it must be converted to a digital signal through sampling and quantization.

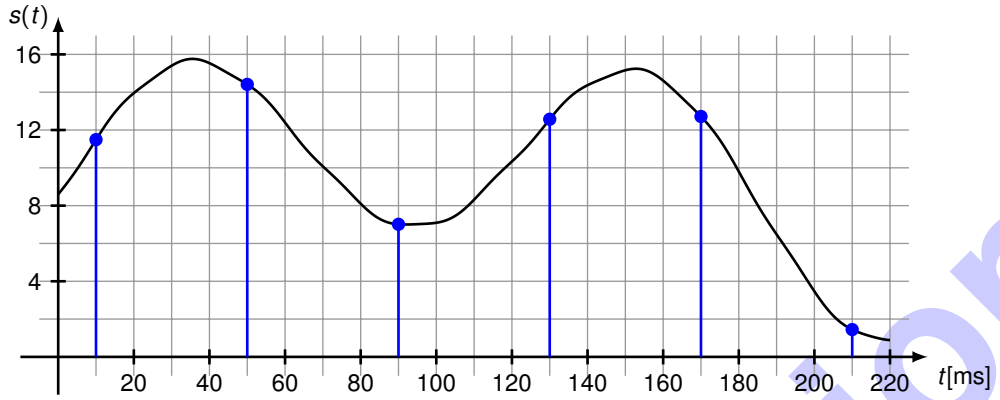


Figure 5.1: Signal

The signal should be sampled with frequency $\mathbf{f_s = 25\,Hz}$ and quantized with **8 steps** in the interval $\mathbf{I_q = [0; 16]}$. Each quantization step is mapped to a binary codeword for digital processing. The codewords are assigned consecutively in ascending order, meaning the lowest step gets the lowest codeword.

0 1 2

a)* Enter the numerical values of the quantization steps in the first row of Table 5.1. Choose the quantization steps linearly with minimal quantization error in I_q.
Hint: there are more columns than necessary.

b)* Enter the binary code words corresponding to the quantization steps in the second row of Table 5.1.

0 1

Subtask a) **Quantization step**	1	3	5	7	9	11	13	15
Subtask b) **Binary code word**	000	001	010	011	100	101	110	111

Table 5.1: Quantization steps and their code words

0 1

c)* Determine the sampling interval T_s.

$T_s = 1/f_s = 40\,\text{ms}$

0 1 2

d) Sample the signal with frequency f_s in the domain $\mathbf{t} \in [\mathbf{0ms}; \mathbf{220ms}]$ using $\mathbf{t_0 = 10\,ms}$ as the first sampling point. Draw the time discrete signal in Figure 5 and enter the time values in the first row of Table 5.2.
Hint: there are more columns than necessary.

Subtask d) **Time [ms]**	10	50	90	130	170	210		
Subtask e) **Value (quantized)**	11	15	7	13	13	1		
Subtask f) **Code word (mapped)**	101	111	011	110	110	000		

Table 5.2: Sample points, quantized values, and code words

0 1

e) Do the quantization for the sampled values according to the previously defined quantization steps in the second row of Table 5.2.

0 1

f) Map the quantized values back to the respective code words and enter the code words in the third row of Table 5.2.

g)* Calculate the maximum quantization error inside I_q.

0 1

$$q_{max} = \frac{\Delta}{2} = \frac{\frac{b-a}{M}}{2} = \frac{\frac{16}{8}}{2} = 1$$

The current resolution is too coarse for the intended application. Instead, a much lower quantization error of $q'_{max} = 0.1$ should be achieved.

h)* Determine the number of quantization steps M' required to achieve the maximum error q'_{max}.

0 1

$$M' = \frac{b-a}{2 \cdot q'_{max}} = \frac{16}{0.2} = 80$$

i) Determine the code word length if M' code words are used.

0 1

$$N = \lceil \log_2(M') \rceil = 7\,\text{bit}$$

Problem 6 HTTP Security (13 credits)

A friend of yours, Bob, wants to get into self-hosting a server with a webservice, but is unfortunately quite inexperienced. Luckily you have advanced knowledge about networking and IT security to help Bob out. Initially he asks you some questions about how he can set up user accounts on his web server.

a) Differentiate the terms Authentication and Authorization.

0 1 2

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

To make the user accounts work, Bob has to store user names and passwords. You tell him that he must never store passwords in plain text, but that he should hash and salt them.

b) Explain what a rainbow table is.

0 1

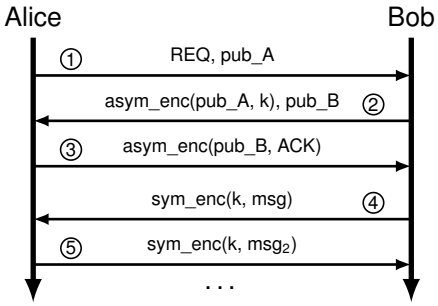
Precomputed table, mapping a string (typically password) to the corresponding hash. Facilitates reverse lookup of hashes.

c) Explain how salting a password protects against attacks using rainbow tables.

0 1

Lookup of stolen passwords no longer possible in precomputed rainbow tables, because the salt changes the hash.

Initially Bob wanted to implement his own protocol to secure the web traffic of his server. He came up with a simple key exchange between a user (Alice) and his self-hosted server (Bob).
In the first two messages Alice and Bob exchange public keys. Then, Bob generates a symmetric key and sends it to Alice. All further communication is symmetrically encrypted. That way, no one can access the secret key and all communication is safe... at least thats what Bob thinks.



0 1 2 3

d)* Point out the flaw of Bobs encryption strategy. Explain how a malicious actor *Mallory* can gain access to the exchanged data.

MitM Attack possible
Mallory can inject her own public keys into the initial exchange in messages ① and ②. Neither Bob nor Alice will notice that, since they get Mallorys keys served and there is no authentication of the public keys.
Then, Mallory can decrypt the shared secret k using her own private key and listen to all further communication.

Through your explanation, you successfully convinced Bob to stick to tried and tested implementations like HTTPS with TLS. The following figures show the encryption process of the two AES variants Electronic Codebook (ECB, Fig. 6.1) and Cipher Block Chaining (CBC, Fig. 6.2) that can be part of a TLS cipher suite.

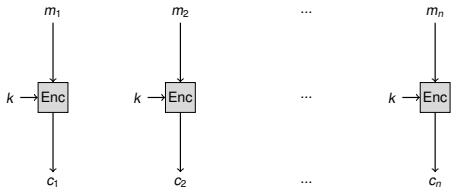


Figure 6.1: Electronic code book (ECB) mode

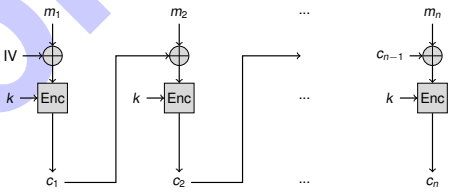


Figure 6.2: Cipher Block Chaining (CBC) Mode

0 1

e)* Why should ECB mode not be used in practice? Briefly describe what might happen.

Identical plaintext blocks will produce identical ciphertext blocks. This allows attacker to identify patterns in the ciphertext.

0 1

f) Explain how CBC mode fixes the problem described in e).

CBC mode uses the previous ciphertext block as the input for the next block. This means that identical plaintext blocks will produce different ciphertext blocks.

Another important feature of TLS is authentication of the server using certificates. When Alice connects to Bobs server, the server returns a certificate in the TLS handshake. Obtaining the certificate itself is however not sufficient to prove authenticity. Instead, two verification steps have to be performed.

0 1 2 3 4

g)* Explain the two verification steps Alice has to do with the certificate.

Verify Handshake Signature: Alice must verify all data exchanged in the handshake (including ephemeral keys of e.g. the Diffie-Hellman key exchange) with the served certificate
Verify Trust: resolve the certificates chain of trust through intermediate certificates to a trust anchor that is in Alice's trust store and therefore trusted.