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

Esolution
Sticker will be generated

Compliance to the code of conduct
I hereby assure that I solve and submit this exam myself under my own name by only using the allowed tools listed below.

_____
Signature or full name if no pen input available

Computer Networking and IT-Security

Exam:	INHN0012 / Quiz 1	**Date:**	Thursday 30th November, 2023
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	12:30 – 12:45

Working instructions

- **Do not forget to sign the rules of conduct at the top of this page (or to enter yout name in the field in case you do not use a tablet device).**
- This exam consists of **6 pages** with a total of **2 problems**.
  Please make sure now that you received a complete copy of the exam.
- The total amount of achievable credits in this exam is 18 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - everything **except group work, plagiarism and any kind of AI (e. g. ChatGPT**)
- 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.

Problem 1 Multiple Choice (8 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 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)* Given a Signal with Power 16 mW and Noise Power 8 mW. What is the signal-to-noise ratio in this case?

☒ 3.01 dB ☐ 10.00 dB ☐ 0.30 dB ☐ 6.93 dB ☐ 2.00 dB ☒ 2.00

b)* Which statements about the Fourier transform are correct?

☒ Used to analyze non-periodic signals.
☐ The spectrum is discrete.
☒ The spectrum is continuous.
☐ The spectrum is always bounded.
☐ The spectrum is always complex.

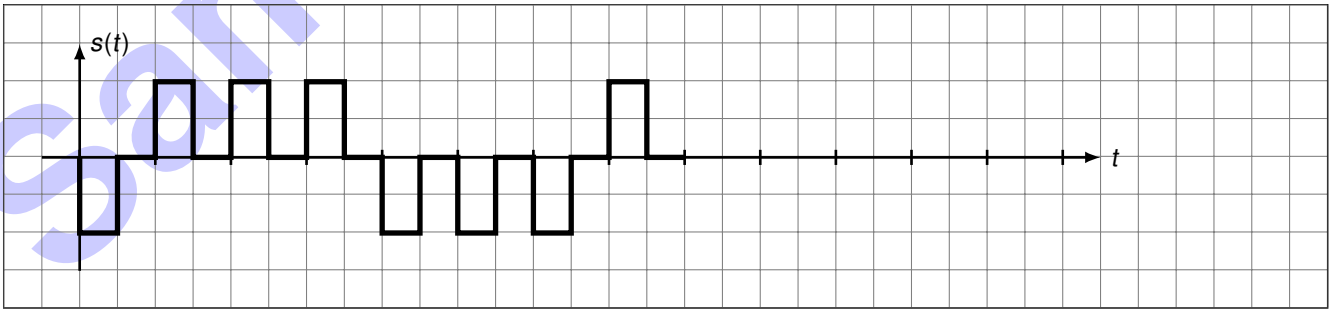
c)* You are given a packet of length 1000 B which is to be transmitted in a cabled network over the distance 2000 km using a data rate of 1000 Mbit/s. Determine the time until the parcel is fully received at its destination.

☐ 6.67 ms ☐ 10.00 ms ☒ 10.01 ms ☐ anderer Wert ☐ 6.67 ms

d)* Which statements about 4B5B coding are correct?

☒ It provides control characters.
☐ It is a code for error correction.
☒ Long inputs are mapped to 4 bit long code words.
☐ It is a code for error detection.

e)* Given the baseband signal shown below, which encodes the bit sequence `0111 0001`. Which of the line codes presented in the lecture was used?

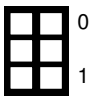


☒ RZ ☐ Manchester ☐ NRZ ☐ MLT-3 ☐ PAM-4

Problem 2 CRC (10 credits)

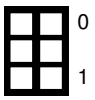
In the following, we consider CRC as introduced in the lecture with the reduction polynomial $r(x) = x^3 + x + 1$.

a)* Explain what a reduction polynomial is being used for.



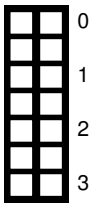
A message of arbitrary length is mapped to a checksum of fixed length (here 3 bit).

b)* Under which condition is $r(x)$ irreducible?



If it cannot be represented as product of two polynomials with degree strictly less than the degree of $r(x)$.

c) Show whether or not $r(x)$ is irreducible.

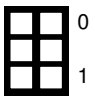


To create a polynomial of degree 3, the only factors in question are:

- $x^2 \cdot x = x^3$
- $(x^2 + 1) \cdot x = x^3 + x$
- $(x^2 + 1) \cdot (x + 1) = x^3 + x^2 + x + 1$

Oviously, $r(x)$ cannot be represented by polynomials of smaller degree
$\Rightarrow$ It is irreducible

d)* Explain briefly why one often chooses a polynomial that is **not** irreducible as reduction polynomial for CRC.



By special choice of polynomial, certain error patterns can be reliably detected, e. g. if the CRC32 polynomial is chosen, all odd errors are detected, even if they are longer than the reduction polynomial.

Let be given the binary message `00100101` and the reduction polynomial $r(x) = x^3 + x + 1$.

0 1 2

e)* Derive the CRC checksum.

```
00100101 000 : 1011
  1011
  ----
  001001
    1011
    ----
    0010 00
      10 11
      -----
      00 110
```

The remainder and thus the checksum is `110`.

0 1

f)* Explicitly state the message that is transmitted.

`00100101 110`

0 1

g)* Give an error pattern that cannot be detected.

Any error that is a multiple of the reduction polynomial itself cannot be detected.

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