Chair of Distributed Systems and Secuirty
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:**	Friday 2nd December, 2022
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	19:30 – 19:45

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 **4 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 15 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - everything **except the help of others and plagiarism**
- 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 chouce / 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)* Let be given a signal with power 8 mW and noise power of 5 mW. Determine the SNR.

☒ 2.04 dB ☐ 6.78 dB ☐ 0.20 dB ☐ 4.70 dB ☐ 1.36 dB ☒ 1.60

b)* Given a packet of length 1200 B to be transmitted in a wired network over a distance of 200 km at a data rate of 1000 Mbit/s. Determine the time until the packet is fully received at the destination.

☐ 0.67 ms ☐ 0.68 ms ☐ 1.00 ms ☒ 1.01 ms ☐ different value

c)* Which statements about token passing are true?

☒ It resembles a logical ring
☒ It is deterministic
☐ Collisions may occur
☐ A station may only transmit after it has forwarded the token

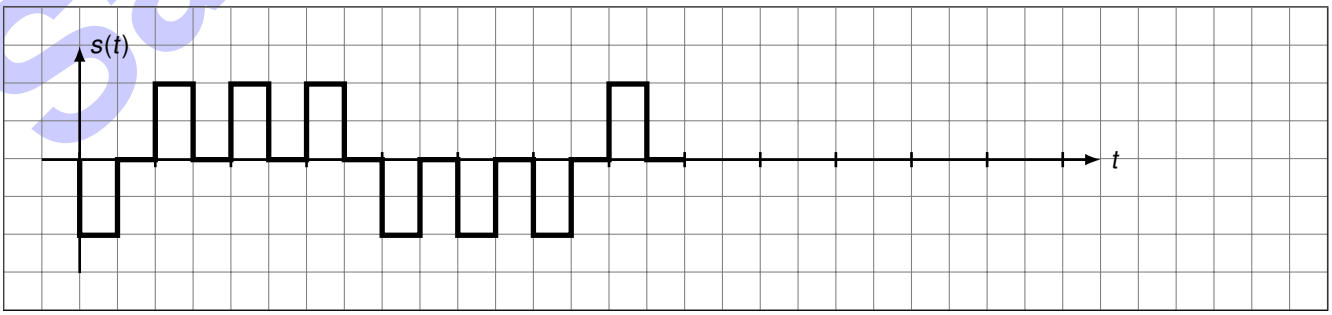
d)* Which of the following factors can affect a signal in a transmission channel?

☒ Interference ☐ Gaussian sum factor ☐ Sieve filter
☐ Binomial factors ☒ Noise ☐ Antifactor

e)* Given is a channel with independent and equally distributed bit error probability $p_e = 0.6\,\%$. Determine the probability that a codeword of length 4 bit is transmitted without error.

☐ 12.96 % ☐ different value ☒ 97.62 % ☐ 0.00 % ☐ 2.56 %

f)* Given is the baseband signal shown below, which encodes the bit sequence `0111 0001`. What is the line code presented in the lecture?



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

Problem 2 CRC (7 credits)

In the following, we consider CRC as introduced in the lecture with the reduction polynomial $r(x) = x^2 + 1$. Give answers in **your own words**, i. e., copy & paste from the internet, lecture slides, tutorials, and old exams is probhibited.

a)* For what purpose is $r(x)$ needed?

0 1

A message of arbitrary length is mapped to a checksum of fixed length (here 2 bit).

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

0 1

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.

0 1

$(x + 1)^2 = „x^2 + 2x + 1“ = x^2 + 1 = r(x)$

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

0 1

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 $r(x) = x^2 + 1$.

e)* Derive the CRC checksum.

0 1 2

```
00100101 00 : 101
  101
  ---
  00110
    101
    ---
    0111
     101
     ---
     010 0
      10 1
      00 10
```

f)* Explicitly state the message that is transmitted.

0 1

`00100101 10`

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