Chair of Distributed Systems and Security
Scholl 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:** | Thursday 22nd February, 2024 |
| **Examiner:** | Prof. Dr.-Ing. Stephan Günther, Leander Seidlitz M.Sc. | **Time:** | 10:00 – 11:30 |



## Working instructions

- This exam consists of **16 pages** with a total of **6 problems**.
  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 (15 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 of the following are security goals according to the lecture?

- ☐ Useability
- ☐ Performance
- ☒ Controlled Access
- ☐ Routeability
- ☐ Deployability
- ☒ Data Integrity
- ☐ Volatility
- ☒ Authenticity
- ☐ Advertisability
- ☐ Agility
- ☒ Confidentiality
- ☐ Sustainability

b)* IPv4 addresses are 4 bytes long. How long is an IPv6 address?

- ☒ 16 bytes
- ☐ 6 bytes
- ☐ 128 bytes
- ☐ 8 bytes

c)* As of today, which of the following cryptographic hash functions are considered secure?

- ☐ MD4
- ☐ SHA-1
- ☐ MD5
- ☐ MD2
- ☒ BLAKE2
- ☒ SHA-2

d)* IPsec is ...

- ☒ policy based
- ☐ only available for IPv4
- ☐ a layer 4 protocol
- ☐ insecure since the protocol was broken in 2009

e)* Which is the correct definition of **forward secrecy**?

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

f)* Which of the following is an AEAD cipher?

- ☐ AES-CBC
- ☐ AES-CTR
- ☒ AES-GCM
- ☐ AES-ECB

g)* Which factors influence the sender window of TCP?

- ☒ Timeouts
- ☐ Max. data rate on Layer 1
- ☒ Acknowledgements
- ☒ RTT
- ☒ Receive window
- ☐ Number of hops

h)* You observe the UDP datagram whose header is shown in Figure 1.1. Which service is likely being addressed?

```
0x0000    d0  2c  00  35
0x0004    00  26  a9  86
```

Figure 1.1: Hexdump of the UDP header

- [ ] DHCP
- [ ] FTP
- [ ] HTTP
- [x] DNS
- [ ] SSH
- [ ] HTTPS

i)* What is the FQDN of the PTR record for the IP address 203.0.113.42?

- [ ] 24.311.0.302.in-addr-arpa.
- [ ] 302.0.311.21.in-addr.arpa.
- [x] 42.113.0.203.in-addr.arpa.
- [ ] 203.0.113.42.in-addr-arpa.

j)* Which of the following is an exterior gateway protocol?

- [ ] EIGRP
- [x] BGP
- [ ] RIP
- [ ] OSPF
- [ ] IGRP

k)* How many L2 address types does 802.11 (WLAN) know? (Hint: source, destination, . . . )

- [ ] 3
- [x] 4
- [ ] 7
- [ ] 2
- [ ] 5

l)* What is CRC used for in Ethernet?

- [ ] Error Forwarding
- [x] Error Detection
- [ ] Error Correction
- [ ] Error Propagation

m)* What does QAM modulate?

- [ ] Density of the signal
- [x] Phase of the signal
- [x] Amplitude of the signal
- [ ] Speed of the signal

## Problem 2 Code Demos — Chat Application with UDP / TCP (14.5 credits)

In the lecture we have written several versions of a small chat application that either uses UDP or TCP as transport layer protocol. First, we consider the original UDP chat that was intended for a 1:1 communication between two clients. In particular, this version was identical on both sides, i. e., there was no server involved.

a)* On your local computer, you were able to run the client by starting it two times with the following command lines:

- `udpchat.py 6112 127.0.0.1 6113`
- `udpchat.py 6113 127.0.0.1 6112`

Briefly explain the three arguments supplied to the application.

udpchat <source port> <destination IP> <destination port>

b) We have rewritten the `udpchat.py` in the lecture to act as a relay chat server that could be started as `udpchat_server.py 6112`. Explain why this single argument is sufficient in that case.

The server listens on all its interfaces on port 6112.Clients still need to know its IP address, but the server does not need to know the IPs of its clients in advance. It will learn their addresses once messages are incoming on port 6112.

c) Argue whether or not clients need to specify a source port when communicating with the `udpchat_server`.

They do not need to specify a source port anymore:they can choose a random ephemeral port. The server will learn the necessary port number just like it does with the IP addresses of clients.

d)* How many sockets do `udpchat` and `udpchat_server` need, respectively? Give a reason for your answer.

Both need only a single socket.Since UDP is stateless, one socket can be used to send data to and receive data from arbitrary remotes.

After implementing the udpchat_server, we rewrote the application again to use TCP instead of UDP as transport protocol.

e) Did anything change regarding the arguments supplied to tcpchat_server.py?

No, the server still awaits incoming messages (connection requests) on a specific port. Remote ports and addresses are learned dynamically.

f)* Argue how many sockets the server now needs to handle $N$ clients?

$N+1$, namely $N$ for the clients and one additional as listening socket for incoming connection requests.

g)* Name two **advantages** of the TCP variant compared to the UDP server. (Without reason)

1. Disconnected clients can easily be identified
2. Messages are guaranteed to be received (as long as the connection holds)

h)* Name two **disadvantages** of the TCP variant compared to the UDP server. (Without reason)

1. The server must hold more state
2. Handling disconnects by getting exceptions / errors while reading from or writing to sockets can be tricky

## Problem 3 Wireshark (16 credits)

We consider the network topology depicted in Figure 3.1. The PC tries to establish an SSH connection via IPv4 to the server SRV. The MAC and IP addresses of the devices' interfaces are given. **Assume that IP addresses are statically configured and the PC has not yet contacted its router since reboot.**

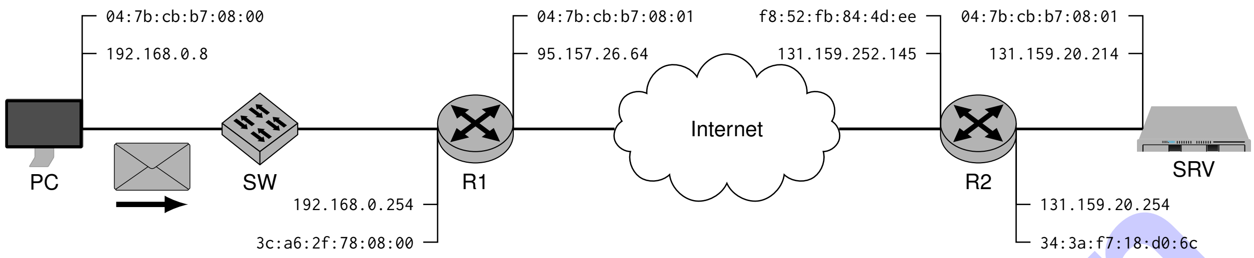


Figure 3.1: Network topology

We consider the frame sent from PC towards SW as depicted in Figure 3.1.

In the following we want to derive the **hexdump of that frame** based on the information given in Figure 3.1 and the following subproblems. Fill in the contents step by step in Figure 3.2. As an example, the L2 receiver address is already filled in as answer to some (not existing) Subproblem x).

**Note: the cheat sheet handed out together with this exam contains everything you need.**

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | (x) | | | | | | (b) | | | | | | end of L2 | | HType | |
| **0x00** | ff | ff | ff | ff | ff | ff | 04 | 7b | cb | b7 | 08 | 00 | 08 | 06 | 00 | 01 |
| | PType | | HLen | PLen | Operation | | Sender HW address | | | | | | Sender protocol address | | | |
| **0x10** | 08 | 00 | 06 | 04 | 00 | 01 | 04 | 7b | cb | b7 | 08 | 00 | $192_{10}$ | $168_{10}$ | $0_{10}$ | $8_{10}$ |
| | Target HW address | | | | | | Target protocol address | | | | end of L2 SDU | | end of frame | | | |
| **0x20** | 00 | 00 | 00 | 00 | 00 | 00 | $192_{10}$ | $168_{10}$ | $0_{10}$ | $254_{10}$ | 42 | 0a | f1 | 73 | | |
| **0x30** | | | | | | | | | | | | | | | | |
| **0x40** | | | | | | | | | | | | | | | | |
| **0x50** | | | | | | | | | | | | | | | | |
| **0x60** | | | | | | | | | | | | | | | | |

Figure 3.2: Preprint for the frame's hexdump

0
1

a) Who is (in general) being addressed by the given receiver address?

Any node on the broadcast domain.

0
1

b)* Fill in the transmitter address of layer 2 in Figure 3.2.

c)* What is the type of the L2 SDU?

ARP (Request), given by the Ethertype `0x0806`.

d) What is the purpose of this frame?

Determining the router's MAC address given its IP address.

Before we continue to fill in the hexdump, we want to mark the end of the L2 payload and the end of the frame.

e)* Mark **the end** of the **L2** payload as well as of the **frame itself** in Figure 3.2. As an example, the end of the L2 header is already marked.

f) Fill in the frame check sequence given as `42 0a f1 73` in Figure 3.2.

After having figured out the type of the L2 payload, it should be straight-forward now to fill in the complete frame. You do not need to name the fields – just fill it in with hex digits. If IP addresses should occur, you do not need to convert them to hex – just fill it in Byte by Byte.

g) Fill in the frame's payload.

h) Assuming IPv6 had been used instead of IPv4. To which protocol would this frame belong to in that case?

It would be a neighbor solicitation.

## Problem 4 Line codes (12 credits)

In this problem we want to compare the four line codes NRZ, RZ, Manchester, and MLT-3 by means of the example bit sequence **`0000 1101`**. Figure 6.2 gives you a template for all four different signals. You find another pre-print at the end of the exam if necessary. **Make sure to strike-out solutions that should not be graded.**

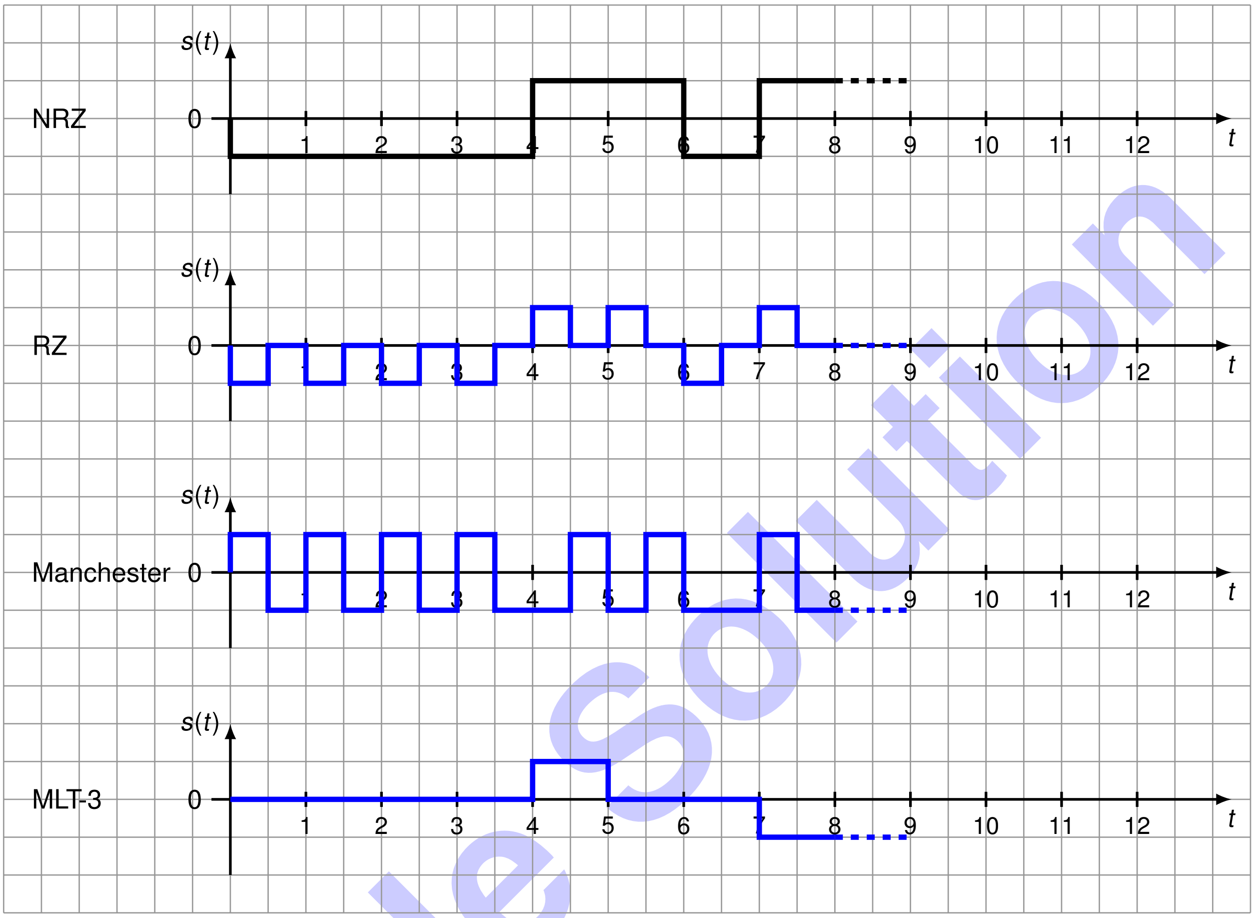


Figure 4.1: Preprint for signals



As an example we show the resulting signal for NRZ in Figure 6.2. Please use positive values (or turns from lower to higher voltages) to indicate a logical `1`, and vice versa for a logical `0`. Use $s(t) = 0$ as start value.

a)* Draw the signal for RZ in Figure 6.2.

b)* Draw the signal for Manchester in Figure 6.2.

c)* Draw the signal for MLT-3 in Figure 6.2.

d) Compare NRZ to RZ and Manchester. Reason which of the signals requires the most bandwidth.

Both RZ and Manchester have two signal changes per line code symbol and thus require more bandwidth than NRZ.

e) Reason which of the four line codes allow(s) for clock recovery / automatic synchronization?

RZ and Manchester since they require a voltage change per symbol.

f) Name an approach that can be used to allow for clock recovery even if the underlying line code does not support it on its own.

0 1 2

For instance, 4B5B encoding can be used together with MLT-3 to guarantee a change in the signal every several bits.

## Problem 5 Dynamic Routing (19 credits)

We consider the network shown in Figure 5.1. The routers are using RIP as dynamic routing protocol. The tables next to the routers represent the (simplified) routing table of the respective router containing the destination **Dst**, next hop **NH**, and the costs.

| Dst | NH | Cost |
|---|---|---|
| B | B | 0 |
| C | C | 0 |
| D | C | 1 |
| E | C | 2 |

| Dst | NH | Cost |
|---|---|---|
| A | A | 0 |
| C | C | 0 |
| D | C | 1 |
| E | C | 2 |

| Dst | NH | Cost |
|---|---|---|
| A | A | 0 |
| B | B | 0 |
| D | D | 0 |
| E | D | 1 |

| Dst | NH | Cost |
|---|---|---|
| A | C | 1 |
| B | C | 1 |
| C | C | 0 |
| E | E | 0 |

| Dst | NH | Cost |
|---|---|---|
| A | D | 2 |
| B | D | 2 |
| C | D | 1 |
| D | D | 0 |

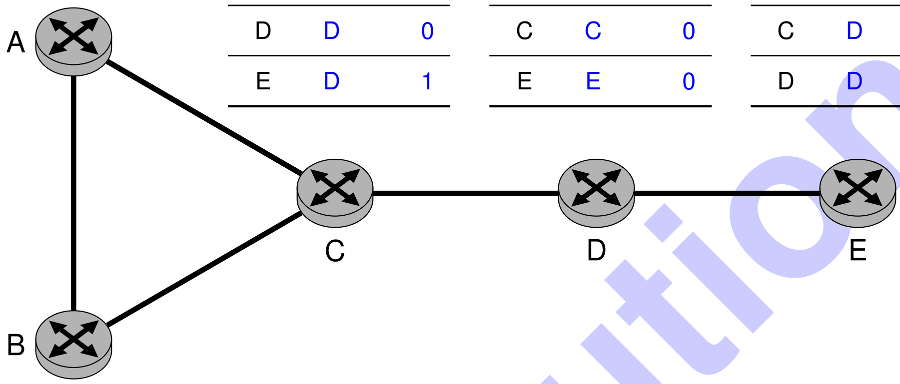


Figure 5.1: Topology and initial routing tables at boot time



0 1

a)* Which metric is used by RIP? (Without reason)

Hop Count

0 1 2

b)* RIP is a distance vector protocol. Explain the difference to link state protocols.

The routers only know the next hop and distance for a destination whole link state protocols have detailed view of the network (or parts of it).

0 1 2

c)* RIP is an interior gateway protocol. Explain the difference to exterior gateway protocols.

IGPs are used within a single autonomuous system while EGPs are used between autonomuous systems.

0 1

d)* To what extent are networks limited that use solely RIP as routing protocol?

The maximum hop count for RIP is 15, thus the “diameter” of those networks cannot be larger than that.

e)* Which information is contained in a routing update sent by RIP?

Solely the reachable destinations and the cost.(In particular not the next hop.)

f)* Reason whether or not RIP always chooses the shortest path in based on the hop count.

Yes, hop count is RIP's sole metric.

g)* Reason whether or not RIP always chooses the fastest route in terms of bandwidth.

No, the number of hops does not tell anything about available bandwidth.

h) Fill in the routing tables in Figure 5.1 (without intermediate steps) such that the tables represent a converged state.

Assume the link between routers D and E fails. Router D obviously recognizes the fail. Answer the following questions in the given order.

i) Router D sends a periodic update. Describe its immediate effect on the other routers.

C is informed about the fail and will remove the route to E via D.A and B do not receive the update from D.

j) Now, router A sends a periodic update. Describe its immediate effect on the other routers.

Since A still assumes there is a route to E via C, it is included in the update.B will ignore that since it also thinks there is still a route to E via C.
However, C now wrongly assumes that there is a route to E via A with cost 3 and installs this new route.

k) Describe the problem that will now arise and how it can be solved.

Count-to-Infinity: the non-existing route to E will circulate between A, B, and C until the tombstone of 15 is reached.
Possible solutions include split horizon, poison reverse, and triggered updates (where the latter only speed up the process at cost of network traffic).

## Problem 6 DNS (13.5 credits)

You are the administrator of the notorious darknet site “The Visible Wiki”, which hosts a collection of darknet links. Recently, all your servers were seized by dollarpol. You could barely escape the authorities, and are now in the process of rebuilding the site. As a first step, you set up a new nameserver at `dns.visiblewiki.what.` You start by writing a zone file.

visiblewiki’s logo

0 1 2 3 4 5 6 7

a)* You start with the basics of a DNS zone file. In the zone file below (Listing 1), add entries fulfilling the following tasks. **Do not use any record type twice!**

1. A record `visiblewiki.what.` referencing `131.159.122.12`
2. Make the website at `www.visiblewiki.what.` reachable. It is hosted on the server at `131.159.122.12`
3. Mail for `visiblewiki.what.` is also handled by the server at `visiblewiki.what.` with priority 1.

```
$TTL              14400
$ORIGIN           visiblewiki.what.

visiblewiki.what.     IN SOA  dns.visiblewiki.what.  visiblewiki.what. (
                      2024022501       ; serial YYYYMMDDxx
                      7200             ; refresh = 4 hrs
                      1800             ; retry   = 30 min
                      604800           ; expire  = 7 days
                      3600             ; neg cache time = 1 hr
                  )

;The CLASS of a record is set to IN (for Internet) for common DNS records
;involving Internet host names, servers, or IP addresses.

visiblewiki.what.     IN NS            dns.visiblewiki.what.
dns.visiblewiki.what. IN A             131.159.122.1


visiblewiki.what.     IN A             131.159.122.12
www.visiblewiki.what. IN CNAME         visiblewiki.what.
visiblewiki.what.     IN MX 1          visiblewiki.what.
```

Correction: 1pt for left column, 0.5pt for type(+prio), 1pt for right column. If trailing dot (fqdn) is missing, -0.5pt for each occurrence

Listing 1: Zone file for `visiblewiki.what`

As you know, the DNS follows a tree structure. Your domain is part of the `what` TLD. The zone file of `what.` therefore has to reference your name server. It contains the following entries:

```
[...]

visiblewiki.what.     IN NS            dns.visiblewiki.what.
dns.visiblewiki.what. IN  A            131.159.122.1

[...]
```

Listing 2: Part of the `what` TLD zone file b)* Why are the entries of Listing 2 necessary? Explain the purpose of the `A` record of Listing 2.

0 1 2

The A record is a glue record. It is necessary as the name server's IP is listed in the `visiblewiki.what.` zone file, but to reach that zone file, we have to query the nameserver that holds it. To break the bootstrapping cycle, the name server's IP is listed in the zone above (`what.`).

c)* At this point, you are concerned about the resolvers that query your name server. Describe how a resolver differs from a name server and how it interacts with name servers.

0 1 2

A resolver extracts information from the DNS by iteratively querying name servers. It interacts with our name server as soon as information from the zones it is authoritative for is to be extracted.

d)* As an operator of "The Visible Wiki" you are naturally afraid of the authorities. Can a client querying the DNS trust the resolver's response to be the actual contents of your zone file? Justify your answer!

0 1 2

As DNS in its basic form does not provide any authentication or integrity, a client cannot trust the responses. If a malicious name server delegates to another malicious name server, the query queries a malicious subtree and returns attacker controlled information. Additionally, responses can be modified in-flight by a man-in-the-middle since the messages are unencrypted and unauthenticated. Points awarded for any reasonable explanation that is correct. Students might go into details about the hierarchy of trust here, or about DNSsec, ...

**Additional pre-print for Problem 4:**

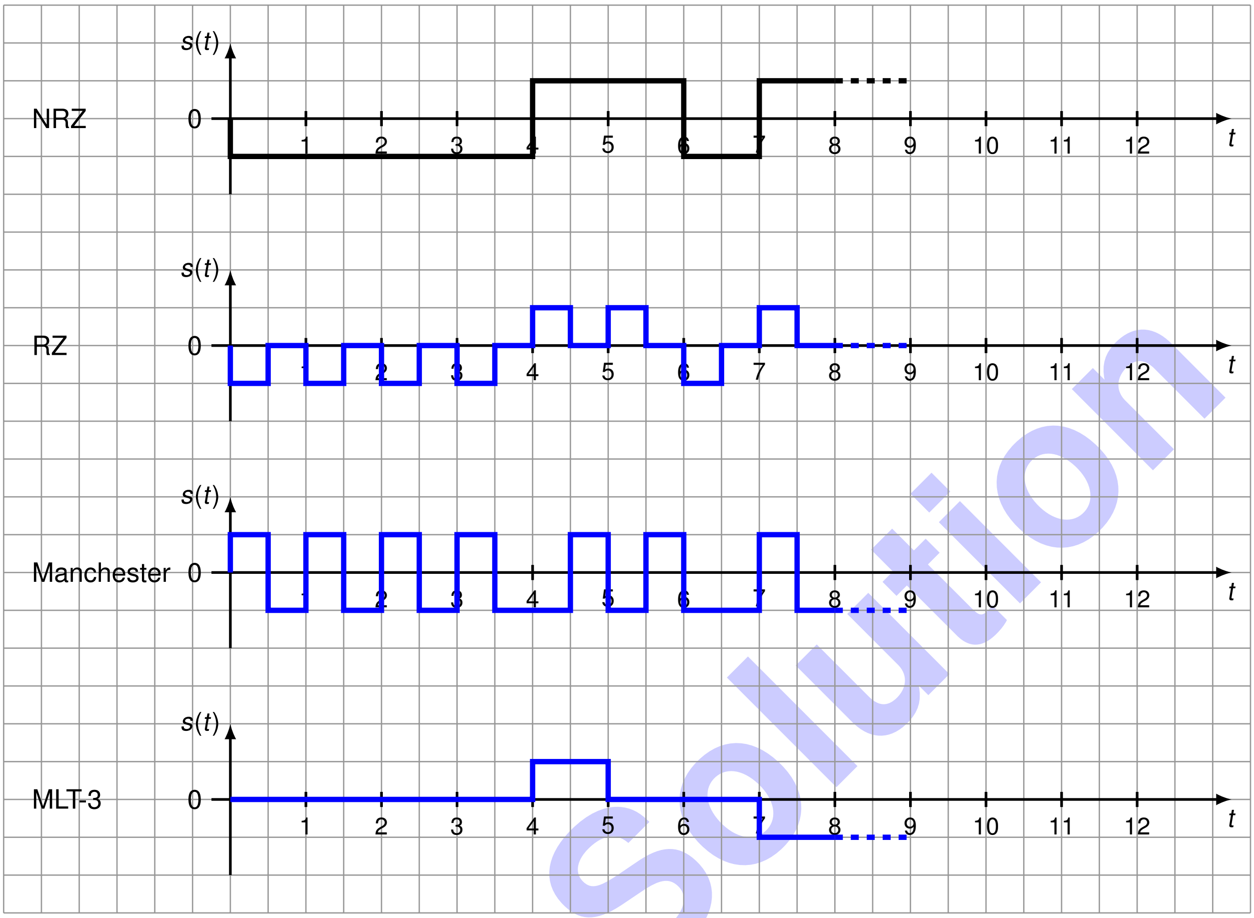


Figure 6.2: Preprint for signals

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