Computer Networks: exam

Signature

.....

Duration : 105 minutes (1h45).
Important : Strictly forbidden : any kind of communication
Important : Authorized: personal documents (slide printout, personal notes, project)
Important : Each question have at least one correct answer and may have multiple correct answers (check all that are correct). The answer "*(other)*" must be checked only when none of the other answers is correct.

NB: To "check" a box, put the corresponding letters in your .txt answer file.
Format to follow (these are just examples and not correct answers)

```
====
Q1:
EMONET
Rémi

Q2:  A

Q3:  ???

Q4:  A D
====
```

As there might be errors in the subject and it is difficult to ask questions: IF REALLY in doubt, you can explain your doubt below `Q?` in your txt file.

Question 1 About you:

LASTNAME (NOM)

FIRSTNAME (PRÉNOM)

Question 2 What is the interest of asymmetric cryptography?

- [A] it does not require a shared secret
- [B] it allows for secure communication
- [C] *(other)*
- [D] it is fast in term of processing

Question 3 What is the interest of symmetric cryptography?

- [A] it allows for secure communication
- [B] it does not require a shared secret
- [C] it is fast in term of processing
- [D] *(other)*

Question 4 About HTTP :

- [A] thanks to proxies, the external bandwidth is reduced
- [B] thanks to proxies, the bandwidth on the local network is reduced
- [C] thanks to cookies, the server associate information to clients
- [D] thanks to cookies, the client stores information about DNS servers

Question 5 The IP header contains:

- [A] the port used
- [B] the destination IP address
- [C] the transport protocol used (TCP, ...)
- [D] the source IP address

Question 6 The TCP header contains:

- [A] the MAC address
- [B] some sequence number
- [C] the port used
- [D] the source IP address

Question 7 DNS Servers are used for :

- [A] finding mail servers
- [B] transforming a name into an IP address
- [C] sending emails
- [D] reading emails

Question 8 Consider a router and an outgoing link that is a cable with capacity C and length L. The underwater cable is damaged (e.g., hit by a whale) and it is replaced in urgency by a "smaller" cable: same length L but half of the capacity ($\frac{C}{2}$). Then:

- [A] the propagation time increases
- [B] *(other)*
- [C] the bandwidth decreases
- [D] all delays remain the same
- [E] the transmission time increases
- [F] the waiting time (in the queue) increases

Question 9 Consider two hosts A and B separated by N successive links of capacities $C_{i=1..N}$. Without congestion, what is the maximal bandwidth between A and B?

- [A] $\max_i C_i$
- [B] $\sum_i C_i$
- [C] $\min_i C_i$
- [D] $\left(\sum_i \frac{1}{C_i}\right)^{-1}$

Question 10 Consider two hosts A and B separated by N successive links of capacities $C_{i=1..N}$, how long will it approximately take to transfer a huge amount Z of data from A to B:

- [A] $\left(\sum_i \frac{Z}{C_i}\right)^{-1}$
- [B] $\sum_i \frac{Z}{C_i}$
- [C] $\frac{Z}{\max_i C_i}$
- [D] $\frac{Z}{\min_i C_i}$

Consider a network with $N+1$ machines, each being able access the core of the network (supposed very fast) via a symmetric connection with rate R. At the beginning, we suppose that one of the machines (M) has a very big file of size L that it wants to distribute to all other machines.

Question 11 How long will it approximately take, at very best, for the file to be replicated on all machines, using a peer to peer approach like BitTorrent?

- [A] $\frac{L}{R}$
- [B] $\frac{NR}{L}$
- [C] $\frac{NL}{R}$
- [D] $\frac{L\log_2(N)}{R}$
- [E] $\frac{L}{NR}$

Question 12 How long will it approximately take, at best, for the file to be replicated on all machines, if M acts as a server and others as clients (client/server approach)?

- [A] $\frac{NL}{R}$
- [B] $\frac{NR}{L}$
- [C] $\frac{L\log_2(N)}{R}$
- [D] $\frac{L}{R}$
- [E] $\frac{L}{NR}$

Question 13 What mechanism(s) is(are) mandatory for making two TCP connections equally share the available bandwidth?

- [A] the multiplicative incr. of *cwnd* (slow start)
- [B] the additive increase of *cwnd*
- [C] the multiplicative decrease of *cwnd* (on loss)
- [D] the fact that *cwnd* is constant

Question 14 What mechanism(s) is(are) mandatory (necessary and sufficient) to ensure the reliability of the TCP connection?

- [A] the pipelining (sending multiple packets)
- [B] the use of acknowledgments
- [C] the re-emission in case of multiple ACK
- [D] the re-emission after a timeout

Question 15 10 students are in a practical session. Each uses the network 33% of the time. The probability that exactly 1 student is using the network at a given instant is roughly :

- [A] $\frac{1}{3}$
- [B] $\frac{2^9}{3^{10}}$
- [C] $10 \times \frac{2^9}{3^{10}}$
- [D] 3
- [E] $\frac{1}{3^{10}}$

Question 16 Consider a simple HTTP browser that uses a sequential persistent TCP connection. How many RTT (round-trip time, time to go to the server and back) will it take before the browser can properly display an HTML page that references 2 images, 1 CSS and 1 javascript file (each very small)?

A 10	C 5	E 6	G 8
B 3	D 2	F 4	

Important: For the following exercises, provide your answers on an exam sheet. With your answer, you must **clearly write the exercise number** but you don't need to recopy the question. Take the time to properly read the questions.

Question 17 SEE the `.txt` file and answer the section about the project.

Question 18

destination	interface
00101010 00101010 *	1
00101010 00101010 00000000 *	2
00101010 *	3
*	4

Given these forwarding rules from a router, answer the following questions (you may convert to a decimal or hexadecimal notation if you find it simpler). (`00101010 = 42 = 0x2A ; 01111111 = 127 = 0x7F`)

On which interface will be forwarded a packet for IP 00101010 00101010 00101010 00000000 ?
and for 00101010 00101010 00101010 01111111 ? and for 00101010 00101010 01111111 01111111 ? and for 00101010 00101010 00000000 00000000 ?

Question 19 Given the previous forwarding rules, what are the ranges of addresses associated to each interface?

Question 20 Explain the difference between the following Java classes: `Socket`, `ServerSocket` (or between a socket and a bound/listening socket in Python).

Question 21 Explain why (in which situation) and how you would use a Java `BlockingQueue` or Python `queue`.

Question 22 You are in the middle of your project (already hosted on github) and you have modified two files (e.g., README.md and auto-eval.md). You want to share these changes with your collaborators, using git and github. Give and explain the commands that allow you to make your changes available to your collaborators.

Question 23 In a blockchain system (not necessarily a cryptocurrency system), what is the use of the hashing function? (when is it used and for which reason?)

Question 24 Consider the following diagram where a laptop is in a network, **using NAT**, and wants to connect to a web server (on the default port). We are interested in a round trip (a packet going one way and its response coming back), for instance when a TCP connection is open.

Provide a *partial answer if you know only part of the answer.* Give a meaningful content, at the TCP, IP and MAC levels (addresses, ports, sources, destinations) of the 6 messages (2 directions, 3 links) circulating on the links during the round trip. Decide and specify any missing information (IP, port, ...).

Question 25 Supposing Atlanta and Hawaï are separated by 7500km (15000km for the round trip) and that the speed of light is about 300 000 km/s. Considering two hosts, one in Atlanta, one in Hawaï, linked by a direct optical fiber cable with a capacity of 10 Gbps. While sending a 125 MB message, how much time is due to propagation (t_{prop})? how much time is due to transmission (t_{trans})? and what is the total time?

Question 26

0	1	1	0
0	1	0	1
0	0	0	0
0	1	1	

Given the message that is received with its 2D parity codes, what was the original 2D binary message content that you can decode?

Question 27 Explain how asymmetric cryptography can be used to send a message that is guaranteed to come from the emitter and that can only be read by the person it is addressed to.

Question 28 Explain how symmetric cryptography can be used to send a message that is guaranteed to come from the emitter and that can only be read by the person it is addressed to.

Question 29 Explain how cryptography can be used in a cryptocurrency system (like BitCoin or simpler) to ensure transactions can be trusted.