Sistemas Distribuídos - MEEC **2022/11/22**

Test (with handwritten cheat sheet) **Duration: 90 min**

1. **Justify all your answers.**
2. **Please answer to questions 1 and 2 in one sheet, and to the remaining questions in another sheet.**
3. **Please answer to all questions either in Portuguese or in English.**

1 [3v] - Concerning Distributed Systems:

1.1- Explain what is and how it works the **Gossip epidemic algorithm**.

1.2- Explain the trade-off between **reliable and non-reliable** communication channels.

2 [7v] - An electrical substation uses a **distributed system** based on Ethernet technology to control the energy lines and associated protections. In particular, line voltages and currents need to be measured with a **high precision** so that they can be properly correlated. The same applies to the actuation of protections to avoid over-voltage in the energy lines.

2.1- To achieve high precision the system uses **clock synchronization** with **PTP**. Which are the distinguishing features of this protocol when compared to **NTP**?

2.2- Knowing that PTP protocol is **centralized** and that the clock synchronization in place achieves an **accuracy of** $1\mu s$, can anything be inferred concerning the **precision** of the set of all clocks in the system?

2.3- Consider that the sensor messages suffer a **variable network delay** (from transmission to reception) between $8\mu s$ and $12\mu s$ and that the **precision** of the set of all clocks is $1\mu s$. Which is the minimum latency (counted from the earliest expected reception instant) that allows the receiver to detect an omission (sensor message loss)?

2.4- The substation has a **server** that records and classifies all substation events. The server is implemented with a common **thread-based** approach to handle concurrent requests. Which are the **limitations** of this architecture when facing event showers (long burst of concurrent events)?

2.5- The substation **communicates with other** substations to share its state and allows distributed actuation in the energy grid. This communications is achieved using an **overlay network** over the Internet. What is an overlay network and how would you **implement it**?

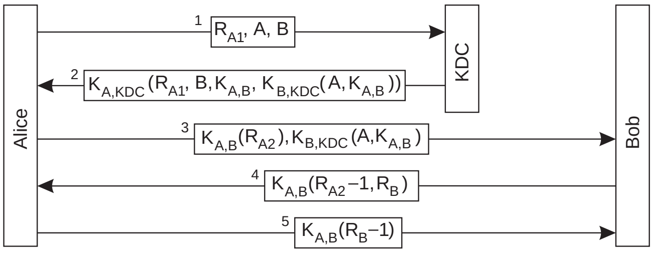
3 [3v]- About security.

3.1- Consider a hash-based Message Authentication Code (MAC). A fundamental property that the hash function, $\mathbf{h}$, used by a MAC must satisfy is known as Computational Resistance:

> For any unknown key, k , given the values x and $h(k, x)$, it is computationally infeasible to compute $h(k, y)$ for a different value y

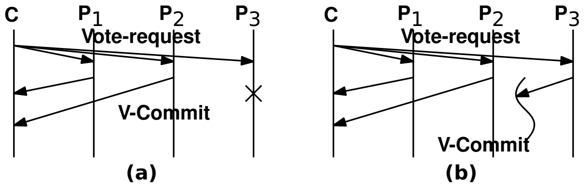
Explain what can go wrong if a MAC uses a hash function that is not computational resistant.

3.2- Consider the Needham-Schroeder authentication protocol published in 1978, shown in the figure on the right. Explain how Eve could break it, if she discovers the key shared between Alice and the KDC, even if that key has been revoked.


Alice
KDC
Bob
1 R_{A1}, A, B
2 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}))$
3 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B})$
4 $K_{A,B}(R_{A2}-1, R_B)$
5 $K_{A,B}(R_B-1)$

Hint: Draw a time diagram and explain it.

4 [3,5v]- Consider the following partial executions of the two-phase commit protocol.



(a)

(b)

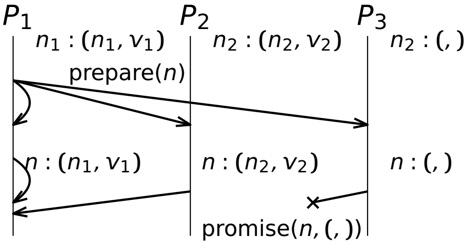
In execution (a) process P_3 crashes, whereas in execution (b) it becomes isolated from the remaining processes because of a network partition and its vote is lost.

4.1- Complete each of the executions for all processes but process P_3. Explain.

4.2- For each execution, explain how does P_3 make the same decision as the other processes, when the respective failure is repaired.

5 [3,5v]- About Paxos and state machine replication.

5.1- Consider the execution of the 1st phase of Paxos on the right. Assuming that $n_2 > n_1$, complete this time diagram. Explain.



5.2- Could this time diagram correspond to a partial execution of state machine replication (SMR) based on Paxos? Justify.