Highly Dependable Systems – Sistemas de Elevada Confiabilidade – MEIC/METI
1st Exam – May 5, 2022 – Duration of the exam: 2 hours
Your answers must only use the number of lines in the boxes provided next to each question. If necessary, for instance to correct a previous answer, you can use the space at the end of the exam sheet but you cannot use more lines than in the original box. Answers can be in English or Portuguese.
Justify all answers.

Number		Name	

Dependability fundamentals

1. Is it possible to increase the availability of a system without incurring the costs of equipping the system with some form of redundancy? If yes, how?

2. Illustrate with a concrete example the relations among the concepts of failure, fault and error.

Security Fundamentals.

3. Discuss a property ensured by Digital Signatures but not provided by Message Authentication Codes. Justify the answer.

4. What additional properties should a robust cryptographic hash function have with respect to a regular hash function? Justify the answer.

Fault tolerance.

5. Assume a computer system whose reliability is estimated to be 70%. What is the reliability achievable by using a triple modular redundancy (TMR) scheme with an ideal voter?

6. Consider a system with 5 redundant modules. How many sequential faults can be tolerated using, respectively, the NMR or Hybrid with Spares techniques? Justify.

Number		Name	

Smartcards

7. What is the bus scrambling technique and what type of threats is it aimed at addressing?

8. What differentiates a Simple and a Differential Power Analysis technique? What advantages do Differential Power Analysis have over Simple Power Analysis techniques (from the attacker's perspective)?

Fault tolerant distributed algorithms.

9. Consider the specification of Fair-Loss links.

- *FLL1.* If a message is sent infinitely often by pi to pj , and neither pi or pj crashes, then m is delivered infinitely often by pj
- *FLL2.*If a message m is sent a finite number of times by pi to pj, m is delivered a finite number of times by pj
- *FLL3.* No message is delivered unless it was sent

For each of property, indicate whether it is a liveness or safety property. Justify.

10. Discuss how to implement Perfect Links on top of Fair-Loss Links.

Byzantine fault tolerance

11. What properties are ensured by the use of regular quorums and byzantine quorums? What is their size?

12. Consider the Authenticated Echo Broadcast algorithm which implements the Byzantine Consistent Broadcast specification. What conditions are necessary for a correct process to deliver a message?

Number		Name	

13. Consider the Double Authenticated Echo Broadcast algorithm which implements the Byzantine Reliable Broadcast specification. What conditions are necessary for a correct process to deliver a message?

Blockchain.

14. Discuss the main differences, in terms of safety and liveness properties, between Proof-of-Work consensus and classical Byzantine consensus.

15. How can a trusted computing technology, such as the TPM platform, be used in a blockchain to dela with Sybil Attacks?

Trusted computing.

16. Among other services, the Trusted Platform Module provides data Binding and Sealing. In which scenarios do you recommend using one over the other?

17. To attest a given service, a TPM user must first issue an Attestation Identity Key. What is the role of the Attestation Identity Key? Could the user use the Endorsement Key instead?

Question	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Grade	1	1	1	1	1	1	1	1	1,5	1,5	1,5	1,5	1,5	1,5	1	1	1