M2 CyberSecurity 2021-2022

Physical Security (WMM9SY05)

Hardware and Embedded Systems

Paolo MAISTRI, Ioana VATAJELU

No documents allowed

Three different sheets (or groups of sheets) for each part
(Smart Card/Embedded/Quantum)

Write clearly your name on each sheet

Estimated 50 minutes

1. Why is security in embedded system important? Cite a few domains where embedded systems should be secured, and cite at least an example of an embedded system that was compromised.

2. Describe briefly a few side channel attacks that can be mounted against digital systems.

3. Describe a countermeasure against side channel attacks that can be applied at architectural level, why it works, and what is the additional protection that is expected against these attacks.

4. Describe the similarities and differences between the Power Consumption and the EM emission with respect to Side Channel Attacks, and the respective countermeasures that can be used to protect against them

5. AES can be vulnerable to fault attacks. Describe briefly how Differential Fault Analysis can allow recovering the secret key, and suggest a (few) countermeasure(s) that could be adopted. Which are the pros and against of the solution(s) you proposed?

6. Describe an effective solution to block the access to the internal test structures to malicious users.

7. In microelectronics industry, which are the main counterfeiting type and how are they defined? Which are the main actions for each of their prevention?

8. What are the physically unclonable functions, how are they use for circuit trust and which are their performance metrics?