Security
1st Semester, 2010/11

2nd Test / 1st Exam
January 14, 2010

- All questions have the same grade.
- Total duration time of test is 1 hour and 30 minutes (last 10 questions).
- Total duration time of exam is 3 hours (20 questions).

1. Consider the *stack smashing attack*s. Discuss their suitability if there were two stacks, and not jus tone: one for parameters and local variables, another for return addresses and stack frame pointers.
2. Consider the triple cipher concept. Explain:
    a. What motivates its use?
    b. Why is triple cipher used with the EDE policy?
3. The security of RSA cipher is based on two properties: difficulty in the factorization of large numbers and difficulty in the computation of discrete logarithms of large numbers. Explain why?
4. Explain the applicability of the Birthday Paradox to the collision resistance of digest functions.
5. Describe the general operation model of digest functions (i.e. how they are built).
6. Consider the concept of digital signature. Explain:
    a. How is it build? Illustrate with a diagram.
    b. How is it validated? Illustrate with a diagram.
7. Consider the PKCS #11 *de facto* standard. Explain:
    a. What does it mean?
    b. Why doesn't it encompass all the functionalities of Cartão de Cidadão?
8. Explain, as completely as possible, why public key certificates are used.
9. Why is it fundamental to generate the signature private key inside the Cartão de Cidadão and to prevent it from leaving the card?
10. Explain the advantages of using the international GTE Cyber Trust Global Root self-signed certificate at the root of the Cartão de Cidadão certification hierarchy?

11. Consider the authentication paradigms with direct presentation of credentials and challenge-response. Explain:
    a. What is the fundamental difference between them?
    b. In which circumstances can (should) each be explored?
12. Consider the concept of one-time authentication. Explain:
    a. What dos it mean?
    b. Explain its advantages and disadvantages
13. Consider the GSM authentication model. Explain:
    a. How does it work?
    b. Which risks can be created by a BTS (*Base Transceiver Station*) personification by an attacker?
14. Consider the concept of access control monitor Explain:
    a. What is it good for?
    b. Give two practical examples of its exploitation
15. Consider the concept of Access control matrix. Explain:
    a. How is it decomposed in Access Control Lists, (ACLs)?
    b. How is it decomposed in capabilities?
16. Consider the concept of Role-Based Access Control (RBAC). Explain:
    a. How does it work?
    b. Why it cannot be implemented with group-based access controls, using a group per role?
17. Consider flow control models. Explain:
    a. How do they work?
    b. Which information is used by the access control monitor in order to make a decision?
18. Consider the Clark-Wilson integrity model. Explain what is:
    a. A CDI (*Constrained Data Item*) and an UDI (*Unconstrained Data Item*)
    b. An IVP (*Integrity Verification Procedure*) and a TP (*Transformation Procedure*).
19. Consider the concept de sensitive information. Explain:
    a. What does it means to be inherently sensitive? Give an example.
    b. What does it means to be sensitive because provides from a sensitive source? Give an example.
20. Consider the public CVE (*Common Vulnerabilities and Exposures*) index. Explain:
    a. Which advantages does it provide to potential victims?
    b. Which risks can we face by leaking all that information to potential attackers?