Security
1º Semester, 2010/11

1º Test
November 9, 2010

- All question have the same grade.
- Total time is 1 hour and 30 minutes

1. Consider the concept of stack smashing attack:
    a. Explain which is the vulnerability of the C language the is exploited in such attack.
    b. Give two ways for detecting its occurrence in run-time.
2. Explain the general operation model of a stream cipher, including cipher and decipher operations, and complete the explanation with a diagram.
3. CFS (*Cryptographic File System*) uses a combination of cipher modes, namely ECB (*Electronic Code Book*) and OFB (*Output Feedback*). Explain why.
4. Explain why the CTR (*Counter Mode*) cipher mode has uniform random access, the OFB (*Output Feedback*) cipher mode usually does not possesses it and the CFB (*Cipher Feedback*) cipher mode only possesses it when deciphering.
5. Explain the general exploitation model of an asymmetric cipher (e.g. RSA) in the secure communication (confidential communication) between two entities.
6. Considering the 3 properties that good digest functions should have, two of them are critical for its exploitation in the generation and validation of digital signatures. Explain:
    a. Which ones are those properties?
    b. Why are they critical?
7. Consider the MAC (*Message Authentication Code*) concept:
    a. What is the application purpose of a MAC?
    b. Give two ways for compute it.
8. Consider the concept of certification hierarchies. Explain:
    a. What are they?
    b. What is the relevance, for them, of root self-certified certificates?
9. Explain of is the added value of using the Portuguese Cartão de Cidadão for implementing an infra-structure for generating and validating digital signatures by Portuguese citizens?
10. Consider the concept of lifetime of an asymmetric key pair. Explain:
    a. Which mechanism exist to control their lifetime?
    b. Describe in a simple way the policies they may govern each of the mechanisms.