Security
1st Semester, 2009/10

1º Test
November 10, 2009

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

1. Describe the execution of a stack smashing attack.

2. Explain the generic operation of a stream cipher, including a complementary diagram.

3. The ECB cipher mode does not hide repeated, block-level plaintext patterns but it may nevertheless be interesting for some specific applications, such as secure file systems with file encryption capabilities. Explain:
   a. Why ECB is interesting for encrypting file systems?
   b. How ECB can be complemented in order to avoid the reproduction of plaintext patterns in the cryptograms (hint: the mechanisms used by CFS)?

4. Digest functions should complicate the discovery of collisions. Explain:
   a. What is a collision discovery?
   b. What is the risk of collision discovery when we are dealing with the validation of digital signatures computed over values generated by digest functions?

5. A MAC (Message Authentication Code) is a data authentication mechanism. Explain why it cannot be used to prove the authorship of data to third parties (or, in other words, why it allows origin repudiation).

6. Digital signatures are usually computed over digest of documents. Explain the rationale of such decision.

7. Consider EFS (*Encrypting File System*), an NTFS extension. Explain:
   a. The management of the keys used to encrypt each file.
   b. The integration between the key management and the access control mechanisms for each file.

8. Consider the PKCS #11 standard. Explain:
   a. What does this standard defines?
   b. What is its relevance for the exploitation of smartcards?

9. Consider the public key management. Explain:
   a. What is a public key certificate?
   b. How can we impose limits to the lifetime of the certificates issued by a Certification Authority?

10. Explain the goal of the OCSP protocol and when it should be used.