Security
1st Semester, 2014/15

1st Test
November 21, 2014

- All questions have the same grade.
- The total time is 1h30.

1. Consider the stack smashing attack using C.
   a. Explain how they work.
   b. Explain how the canary mechanism prevents their success.

2. A stream cipher can create problems when its generator has a reduced number of internal states (comparing with the length of a message to encrypt). Explain in detail why, using a diagram to illustrate your answer.

3. Padding is a usual solution for being able to encrypt messages of any length using a block cipher mode. Explain:
   a. Why is padding required?
   b. Describe a way to perform such padding, illustrating your explanation.

4. Some cipher modes allow uniform random access, both in encryptions and decryptions. Explain:
   a. What is the meaning of such quality?
   b. Identify, with a justification, 2 cipher modes with such quality.

5. Consider the properties that distinguish digest functions from other hashing functions.
   a. Explain those properties, using mathematical notation.
   b. Identify, with a justification, which of those properties (**only one!**) is the most critical for the exploitation of digest functions in digital signatures.

6. Identify 2 reasons that you may consider fundamental for exploring smartcards, such as the Portuguese Citizen Card, to perform digital signatures with legal value.

7. Consider the management of public keys. Explain:
   a. What is a certification chain?
   b. What exactly is a trusted root of the certification chain?

8. It is intended to validate a digital signature performed at date T1 with the public key present in a certificate with a validity period between T2 and T3 that was revoked at date T4. Identify, with a justification, for which values of T1 can the signature be considered as valid.

9. Within biometric evaluations it is possible that two individuals exhibit the exact same biometric characteristics. Discuss the impact of this fact in the evaluation of the effectiveness of a biometric authentication system (**beware! do not confound biometric identification with biometric authentication**).

10. Consider the authentication of people with a direct presentation of one-time passwords. Explain:
    a. What are one-time passwords?
    b. In which operational scenarios thus it make sense to use such passwords?