Security
1st Semester, 2015/16

Intermediate Test
11 de November de 2015

- All questions have the same weight.
- All answers must be properly explained, including the reasoning.
- The test has the duration of 1h 30.

1. Distinguish *ARP Spoofing* from *ARP Poisoning* and demonstrate its use in the execution of a *Man in The Middle* attack.

2. Describe a *Stack Smashing* attack and the impact of overwriting the address of the *Instruction Pointer* (IP) stored in the stack.

3. In a stream cipher, explain what diffusion process is applied to the text.
   a. What is the relation of this fact with the need of integrity control?

4. Identify and describe an appropriate and an inappropriate cipher mode to provide random read and write access to a ciphered hard disk.
   a. Which characteristics of these modes are relevant to the selection of the correct cipher mode?
   b. Present an example of the encode and decode process of each mode, and present their diagrams of operation.

5. Describe with detail a way of converting a block cipher into a stream cipher.

6. Describe what is the *Ciphertext Stealing* method, how it is applied and what is its purpose.

7. Describe and present examples of three methods of enhancing the security of a cipher.

8. Describe the concepts of *Digest* and *Message Authentication Code (MAC)*, their main differences, and scenarios where its use is most appropriate.

9. Considering a X.509 certificate, what are the main mandatory fields and what is their function in the validation of an email message?
   a. Consider a signed message created at a time instant t_0, which respective public key certificate was revoked at t_1 and the message verified at t_2 ($t_0 < t_1 < t_2$).

10. In the management of asymmetric keys why the temporal restrictions are insufficient to restrict the temporal use of a key, imposing the need for additional mechanisms?
    a. Consider the revocation mechanisms studied, and explain the need of multiple alternatives.