Security
1st Semester, 2013/14

1st Test
November 13, 2013

- All questions have the same value.
- The total duration is 1h30.

1. ARP poisoning attacks are possible due to the existence of vulnerabilities. Explain:
   a. Which are those vulnerabilities?
   b. Point out a consequence of a specific attack (to describe) and the advantage that comes out for the attacker.

2. XSS (Cross-Site Scripting) attacks explore several types of vulnerabilities. Explain:
   a. What is the vulnerability in the case of the Stored XSS attacks?
   b. How can this vulnerability be eliminated?

3. The following cryptogram was generated with a Vigenère cipher: **`SDTOAEGEEBPSHLEGEEDPEGEA`**
   a. Explain how the cipher works.
   b. Deduce, with a justification, what is the period of the cipher.

4. Consider the exploitation of the AES block cipher (with 128 bit blocks) in 8-bit OFB (*Output FeedBack*) mode.
   a. How does the cipher and decipher operations are performed?
   b. How many AES operations are necessary to cipher 1 KB of data?

5. Block ciphers, when applied in ECB (*Electronic Code Book*) mode, force the plaintext to be aligned to the block size of the cipher. Describe a method to do such alignment in a way that the decipher could extract from the cryptogram the alignment performed (e.g. PKCS#5).

6. Explain the generic algorithm used to implement digest functions such as MD5 or SHA-1.

7. Asymmetric ciphers can be used for two completely different purposes, depending on the key that is used to encrypt or decrypt. Explain what these purposes are and how the keys are used in each of them.

8. Asymmetric ciphers, such as RSA, when are repeatedly used to encrypt a constant value always produce different results. Explain:
   a. What causes this behavior?
   b. Which benefit comes out of this behavior?

9. Consider the management of public keys. Explain:
   a. What is a CRL (*Certificate Revocation List*)?
   b. For what reason is it necessary that a Certification Authority maintains a CRL and provides public access available to it?

10. When verifying whether a certificate has been revoked or not, this check should take into account a precise temporal notion (i.e., should take into account a particular time instant). Considering the case of the digital signature of documents, what time are we talking about? Justify your answer