Instituto Superior de Engenharia de Lisboa
MEIC, MEIM, MEETC
Cybersecurity
Example questions for each group

Group 1 - Information protection mechanisms [6 points]

1. [2] Consider a 2-byte block round cipher defined by the composition of the ciphers: C1, 2-byte block cipher defined by swapping the left and right byte positions; C2, substitution cipher that consists of identifying each byte with a pair of elements (x,y) in Z16 and performing the transformation (x,y)->(5x,x+y) in Z16. Determine the ciphertext with this round cipher, using an ECB mode of operation and, if necessary, a padding of type OneAndZeroes, obtained from the plaintext F1FB33A0.
2. [1] Cipher the plaintext:

   `boasorte`

   using the Vigenere auto-key cipher with initial key A.
3. [2] (ElGalmal Cipher) Consider the prime p=11.
   a. Check that 6 is a multiplicative generator of Z11*.
   b. Determine a public key and a private key for the El Gamal cipher with p=11 and alpha=6
   c. Encrypt the plaintext x=3 with the previously obtained public key and verify, from the ciphertext, that the private key decrypts it properly.
4. [1] Consider the recurrence relation ki=ki-1+ki-2 and the initial values k0=0 and k1=1. Determine the first 5 terms of the keystream defined by this LFSR and use it to encrypt the plaintext 00011 using the ONE-PAD cipher.

Grupo 2 - Security in Software [6 valores]

1. In the context of security vulnerabilities:
   a. [1.5] Describe the two main factors that determine the risk calculation in an application.
   b. [1.5] Distinguish between design and programming vulnerabilities.
   c. [1.5] One of the most common vulnerabilities is not properly separating data from control statements. Give an example of two vulnerabilities that are based on this problem.
2. [1.5] Distinguish between static code analysis and data flow analysis.

Group 3 - Security in Hardware [4 valores]

1. [2] Explain the advantages of using a TPM to verify the integrity of a PC-type computer during its start-up procedure (secure boot).
2. [2] Explain how confidentiality and data integrity of an enclave can be ensured by using the Intel SGX technology.

Group 4 - Security in Communications / Regulations [4 valores]

1. [2] What is the difference between an Intrusion Detection System and an Intrusion Prevention System?
2. [2] What are the main differences between a Normative Framework (e.g. the National Framework of Reference for Cybersecurity) and a Regulation (e.g. the General Data Protection Regulation)?