Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Asymmetric encryption"

Self-assessment test

Select the correct answer.

1. In asymmetric or public key cryptosystems:
   - Both parties share a symmetric key that is used to encrypt and decrypt.
   - Each party knows his private key, and everyone knows the public keys of all parties.
   - Each party knows his public key, and everyone knows the private keys of all parties.
   - Both parties share an asymmetric key that is used to encrypt and decrypt.

2. In asymmetric or public key cryptosystems, when A sends an encrypted message to B:
   - She uses B's private key to encrypt the message
   - She uses A's private key to encrypt the message
   - She uses B's public key to encrypt the message
   - She uses A's public key to encrypt the message

3. Security of asymmetric or public key cryptosystems is based on:
   - In complex problems solvable with polynomial algorithms.
   - In hard problems based on bijective functions that are not trapdoor ones
   - They are based on the discrete logarithm hard problem
   - Some systems are based on the difficulty of factorizing large integers

4. Comparing with symmetric cryptosystems:
   - For similar key size, asymmetric systems are faster.
   - For similar key size, symmetric systems are faster.
   - Recommended asymmetric key size is larger than the one recommended for symmetric key size.
   - Recommended asymmetric key size is smaller than the one recommended for symmetric key size.

5. If A has chosen e=23 with n=143, choose the value of her private exponent d in RSA:
   - 49
   - 47

- 23
- 1

6. B's RSA keys are e=(13,33), d=(17,33). If A wants to encrypt the message M=2 for B, chose which of the following values corresponds to the ciphertext:
   - 8
   - 4
   - 29
   - 12

7. If A has chosen p=13 as modulo in El Gamal (encryption), choose which of the following values she can use as generator g:
   - 2
   - 3
   - 4
   - 5

8. B has chosen the following El Gamal (encryption) keys and parameters: p=17, g=7, x=5, y=11. If A encrypts message M=6 for B, using ephemeral key k_e=9, chose the value that corresponds to the encrypted message:
   - (15,2)
   - (3,12)
   - (10,5)
   - (12,11)