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)

"Key distribution and management"

Self-assessment test

Select the correct answer.

1. Key wrapping is:
   - Encrypting a symmetric key using a public asymmetric key.
   - **Encrypting a symmetric key using another symmetric key.**
   - Encrypting a private asymmetric key using a public asymmetric key.
   - Encrypting a public asymmetric key with a private asymmetric key.

2. Key encapsulation is:
   - **Encrypting a symmetric key using a public asymmetric key**.
   - Encrypting a symmetric key using another symmetric key.
   - Encrypting a private asymmetric key using a private asymmetric key.
   - Encrypting a public asymmetric key with a symmetric key.

3. The best option regarding speed and ease of key management is:
   - Symmetric encryption.
   - Asymmetric encryption.
   - **Hybrid encryption.**
   - Hierarquical encryption.

4. B's RSA public key is (e,n)=(5,69). A encrypts message M=218 for B using the symmetric key K=57, and the encryption algorithm E(K, M) = M + K mod. 256. K is sent to B using key encapsulation. Select from the following options which one corresponds to the message B receives:
   - 5.
   - (223,17).
   - 19.
   - **(19,51)**

5. After two parties execute the Diffie-Hellman protocol:
   - **Both have agreed on a symmetric key over a public channel**
   - One party has encrypted a message for the other party using symmetric encryption and the other one has decrypted it.
   - One party has encrypted a message for the other party using asymmetric encryption and the other one has decrypted it.
   - Both have agreed an asymmetric key over a public channel.

6. A and B execute the Diffie-Hellman protocol with the following parameters: g=2, p=19, x_A=7, x_B=6. The result is:
   - B gets as a final result Y_B=12
   - A sends to B the encrypted message Y_A = 14, and B decrypts it as M=7.
   - **A gets as a final result K=7**
   - B sends to A the cleartext message M=2, and A encrypts it with the key x_B=6.