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)

"Symmetric block cryptosystems"

Self-assessment test

Select the correct answer.

1. Regarding the block cipher modes:
   - In all block cipher modes, each block is encrypted separately and independently from the others
   - In ECB mode, each block encrypted depends on the previous encrypted block.
   - In CBC mode, both encryption and decryption depends on the previous encrypted block.
   - In CFB mode, an error in one bit from the ciphertext affects only one block of the decrypted text.

2. In a CFB block cipher, the cleartext is divided in blocks of m=16 and a cipher that accepts blocks of 48 bits. An error in one of the blocks during the transmission:.
   - Will affect 16 blocks from the decrypted text
   - Will affect 3 blocks from the decrypted text
   - Will affect 4 blocks from the decrypted text
   - Will affect 2 blocks from the decrypted text

3. Regarding the block cipher modes:
   - In CBC mode the sizes of the encrypted block and the register are the same.
   - In CFB mode, the sizes of the encrypted block and the register are different.
   - In all methods, the sizes of the message block message and encrypted block are the same.
   - All the remainder answers are valid.

4. In block ciphers:
   - A DES encryption in CBC mode implies that after encryption of each block M, the ciphertext C obtained is operated "or-exclusive" again with M, and the result is again encrypted with DES.

- One of the reasons to adopt a new american standard, i.e. AES, was the high number of vulnerabilities found in its predecessor, i.e., DES. .
- Upon receiving an encrypted message C, using AES in ECB mode, the receiver could decrypt first the first and last blocks, without needing to decrypt the intermediate blocks
- In CBC mode, the sizes of the encrypted block and the register are different.

5. Regarding the block cipher modes:
   - During the reception of an encrypted message in various blocks using AES in CBC mode, the receptor cannot start decryption until all messages have been received
   - During the reception of an encrypted message in various blocks using AES in CBC mode, the receptor cannot decrypt one block without decrypting the previous ones
   - During the reception of an encrypted message in various blocks using AES in ECB mode, the receptor cannot decrypt one block without decrypting the previous ones
   - None of the others is correct

6. In DES
   - DES uses an external key of 64 bits, used to generate 16 internal keys of 64 bits each.
   - DES uses an external key of 64 bits, being the total number of keys 264.
   - One of the weaknesses of DES is the high amount of weak keys it uses.
   - DES divides cleartext messages in blocks of 64 bits, and uses external keys of 64 bits and internal keys of 48 bits.

7. Select the correct answer
   - If A and B share to secret keys K1 and K2, a third party C, knowing one of the keys (e.g. K1), can decrypt the messages interchanged between A and B, since they are using a symmetric encryption scheme and one can obtain K2 knowning K1
   - An unsecure channel allows the exchange of secret keys.
   - One of the reasons to adopt a new american standard, i.e. AES, was the high number of vulnerabilities found in its predecessor, i.e., DES. .
   - None of the above are correct