CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

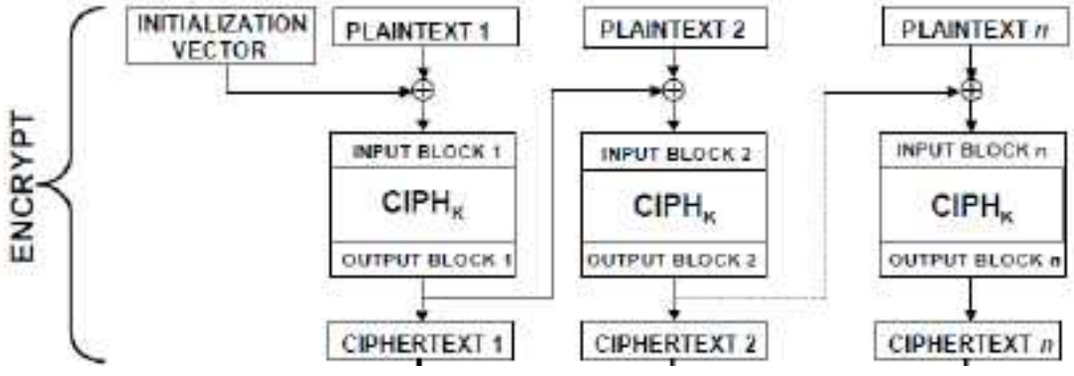
Examen Parcial 2018-2019

PROBLEMA 1 ES

- P1: Alicia y Bob han acordado un sistema de cifrado (byte a byte) que consiste en un esquema basado en el modo de operacióon CBC (Cipher Block Chaining) y una función de cifrado *CIPH(Key, Input)*.

  a) Considerar que la clave de cifrado K (de 1 byte) es intercambiada mediante Diffie-Hellman. Calcular la clave K obtenida considerando los siguientes parametros: g=5; p=23; Alicia X_A=15 (privado); Bob X_B=12 (privado).

  b) Ignorar la clave obtenida in a). Considerando los siguientes parametros, detallar los pasos y calcular los datos cifrados C1 y C2 resultantes del sistema de cifrado CBC:
     - Mensaje M = $B17A_{)16}$
     - Vector de Inicialización = $3F_{)16}$
     - Block size b = 8 bits
     - Clave K = $04_{)16}$
     - *CIPH(Key, Input) = (Key)* ***XOR*** *(Input)* ***XOR*** *($A5_{)16}$)*



REMARK: HEX to BIN translation:
A= 1010; B= 1011; C= 1100; D= 1101; E= 1110; F= 1111

a.) D-H Calcular K

$g = 5 \quad p = 23 \quad$ Alicia $X_A = 15 \quad$ Bob $X_B = 12$

$$A = 5^{15} \bmod 23 = (5^5)^3 \bmod 23 = (20)^3 \bmod 23 = 19$$

$$k = A^{12} \bmod 23 = 19^{12} \bmod 23 = (19^6)^2 \bmod 23 = 2^2 \bmod 23 = 4 \Rightarrow 0000\ 0100$$

b.) Mensaje = $B17A_{(16)} = 1011\ 0001\ 0111\ 1011$

Vector = $3F_{(16)} = 0011\ 1111$

Clave $k = 04_{(16)} = 0000\ 0100$

$CIPH(k, In) = k \underline{XOR}\ In \underline{XOR}\ 1011\ 0101$ ($AS_{(16)}$)

$$C_1 = \underbrace{0000\ 0100}_{k} \oplus (\underbrace{1011\ 0001}_{V} \oplus \underbrace{0011\ 1111}_{M}) \oplus \underbrace{1011\ 0101}_{AS_{(16)}} = 0010\ 1111 \Rightarrow 2F_{(16)}$$

($1000\ 1110$)

$$C_2 = 0000\ 0100 \oplus (0010\ 1111 \oplus 0111\ 1010) \oplus 1011\ 0101 = 1111\ 0100 \Rightarrow F4_{(16)}$$

($0101\ 0101$)