CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

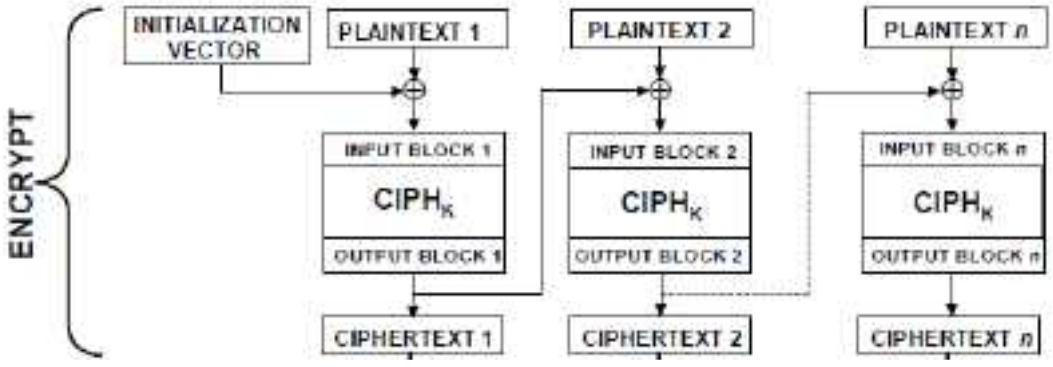
Examen Parcial 2018-2019

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