CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

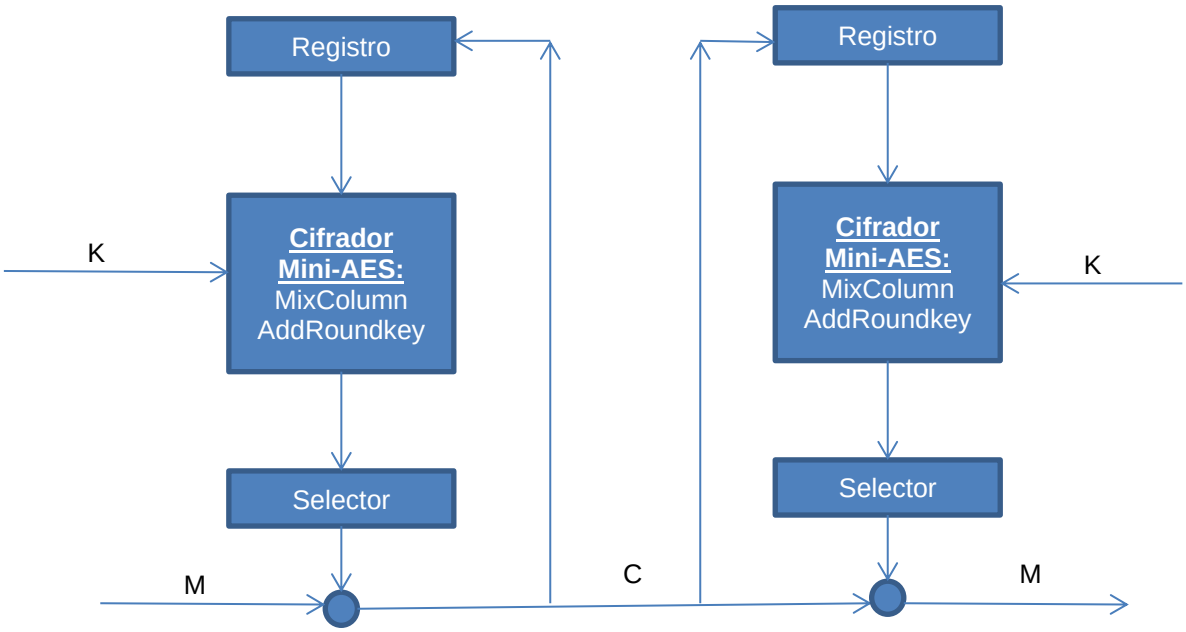
Examen Parcial 2018-2019

PROBLEMA 2 ES

Se dispone de un cifrador simétrico de bloque en modo CFB. Tanto la semilla, o valor inicial del registro, como la clave tienen una longitud de 32 bits (4 bytes). La semilla y la clave se acuerdan entre emisor y receptor del mensaje de forma segura mediante el protocolo de Diffie-Hellman.

El cifrador consistirá en un cifrado AES muy simplificado, que llamaremos Mini-AES. Las transformaciones consideradas en una ronda serán una MixColumn sobre los 4 bytes y una AddRoundKey, en ese orden. El cifrador solo tiene una única ronda. La salida del cifrador será de 4 bytes (b = 32 bits).

El tamaño del bloque de mensaje en claro (segmento) será de 1 byte (s = 8 bits).



a) Calcule el valor que se intercambian A y B mediante Diffie-Hellman a partir del cual acordarán la semilla y la clave. Los parámetros para el intercambio son g=10, p=23, la clave privada de A es x_a=4 y la clave privada de B es y_b=3

b) Sin tener en cuenta el resultado anterior, suponga que la clave de cifrado convenida expresada en hexadecimal es (A1 B2 C3 D4) y que la semilla acordada es (0C 0A 01 03). Obtenga la salida del cifrador Mini-AES. Nota: Tenga en cuenta que el byte menos significativo será la fila 0 de la transformación MixColumn y así sucesivamente

c) Si la salida del cifrador Mini-AES es (1A 2B 3C 4D), y el primer bloque de texto en claro es M_1= (FF) obtenga el primer criptograma C_1. Indique como quedaría el registro tras el cifrado de C_1