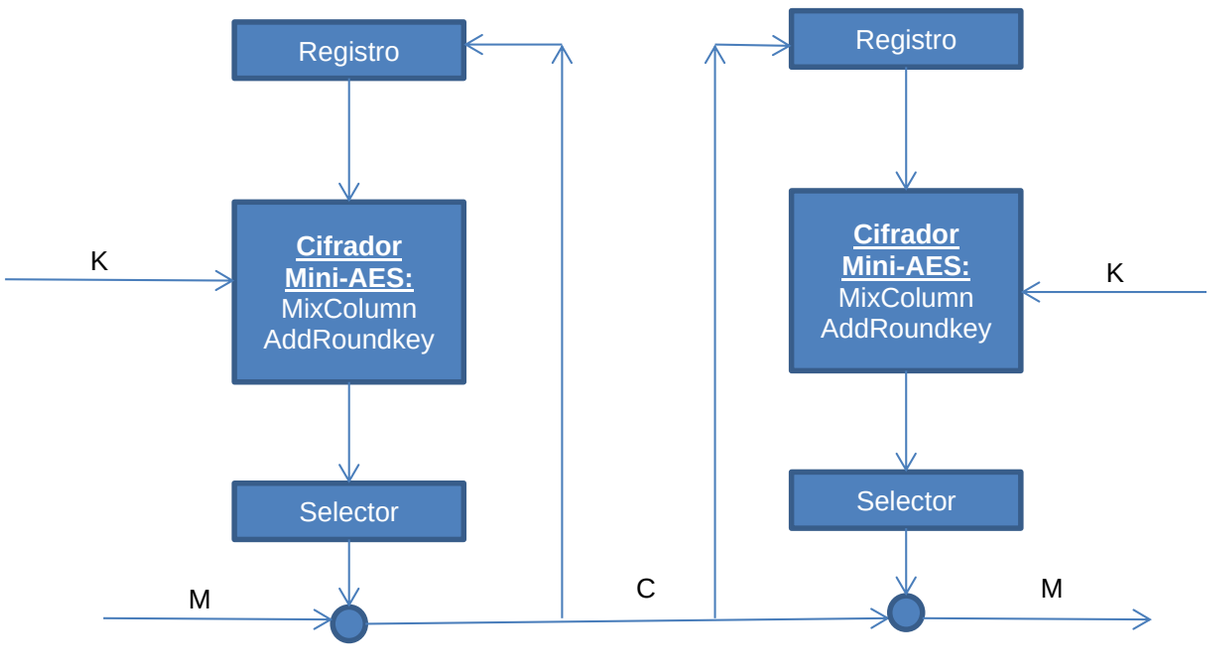
CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen Parcial 2018-2019

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

a.) $q = 10 \quad p = 23 \quad A \ x_a = 4 \quad B \ y_b = 3$

$A = 10^4 \bmod 23 = 18$ $\qquad A \xrightarrow{q,p,A} B \qquad B$

$B = 10^3 \bmod 23 = 11$

$K_A = 11^4 \bmod 23 = 13$

$K_B = 18^3 \bmod 23 = 13$ } Clave.

b.) Clave A1 B2 C3 D4 $\qquad$ 10100001 10110010 11000011 11010100

Semilla 0C 0A 01 03 $\qquad$ 00001100 00001010 00000001 00000011

MixColumn

$$\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 03 \\ 01 \\ 0A \\ 0C \end{pmatrix} = \begin{pmatrix} 03 \\ 13 \\ 02 \\ 1C \end{pmatrix}$$

AddRandkey

16 02 13 03
A1 B2 C3 D4
B7 B0 D0 D7

00000011
00000010
00000
00000011

1010 A
1011 B
1100 C

$00000110 \oplus 00000011 \oplus 00001010 \oplus 00001100 = 00000011 \Rightarrow 3$

$00000011 \oplus 00000010 \oplus 00001010 \oplus 00001101 = 00010011 \Rightarrow 13$

00000011
00001010
00001010
00011110

$00000011 \oplus 00000001 \oplus 00001010 \oplus 00001101 = 00000010 \Rightarrow 02$

00000010
00010100

00000011
00001101
00001101
00010111

00000011
00000011
00000011
00000011

00001100
00000010

$000000101 \oplus 00000001 \oplus 00001010 \oplus 00011000 = 00010110 \Rightarrow 16_{(16}$

c) Salida Mini-AES $\underset{\oplus}{1A}$ 2B 3C 4D

Texto claro $M_1 = \overline{FF}$

$C_1 = 1A \oplus FF = 0001\,1010 \oplus 1111\,1111 = 1110\,0101 = E5$

El registro se desplaza para introducir el bloque $C1 = E5$, por lo tanto el registro es: ~~DD~~ 0A 01 03 E5

Registro