CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen Parcial 2018-2019

PROBLEM 3 ES

Alice y Bob han convenido utilizar cifrado híbrido para intercambiarse mensajes confidenciales. Ambos conocen las claves públicas RSA del otro, que usan para intercambiarse las claves de sesión. Para cifrar los mensajes, utilizan una función de cifrado *CIPH(Key, Input)* operado en modo CTR sobre bloques de 4 bits.

a) Considere que Alice selecciona la clave de sesión K = 7. La clave pública de Alicia es $(e_A, n_A) = (9, 85)$ y la clave pública de Bob es $(e_B, n_B) = (7, 77)$. Calcule la clave de sesión cifrada que Alicia envía a Bob.

b) Ignore los resultados del apartado anterior. A partir de la clave *Session Key* ambas partes derivan la clave de cifrado *Encryption Key* y el *Nonce* que se utilizarán para cifrar simétricamente en modo CTR. Considerando los siguientes parámetros y función de derivación, calcule la clave de cifrado *Encryption Key* y el nonce *Nonce* que se utilizará en esta sesión:
   - Session Key (seleccionada por Alice y que Bob ha recibido de Alice) = $8_{(16}$
   - Tamaño de las claves y de los bloques: 4-bits
   - Encryption Key = (Session Key) $\cdot\ 3_{(16}$ mod p(x)
   - $p(x) = x^5 + x^2 + 1$
   - Nonce = NOT(Session Key)

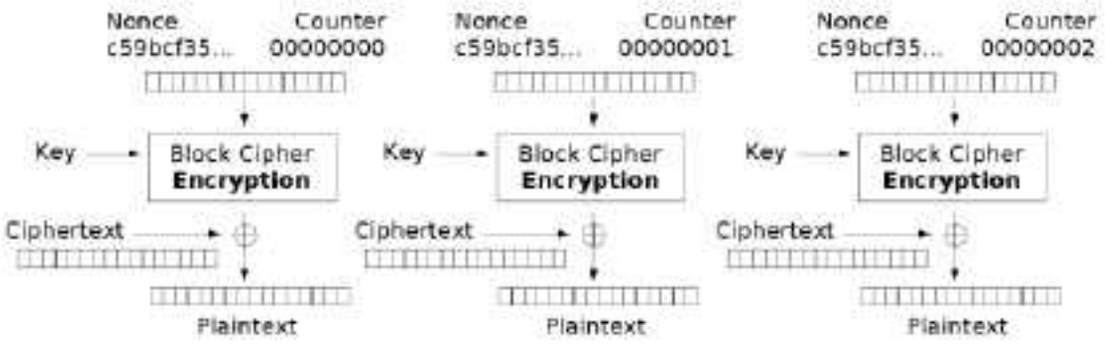
   Nota 1: La función de derivación de la clave de cifrado *Encryption key* se calcula en el cuerpo de Galois $GF(2^5)$ con polinomio primitivo $p(x) = x^5 + x^2 + 1$.

   Nota 2: Relación de HEX a BIN (valores superiores a 9):
   A= 1010; B= 1011; C= 1100; D= 1101; E= 1110; F= 1111

NOTE QUE HAY OTRA PREGUNTA EN EL REVERSO

c) Ignore los resultados obtenidos en b). Considerando los siguientes parámetros, detalle los pasos y calcule el mensaje <u>en claro</u> que Alice ha enviado a Bob, utilizando el criptosistema simétrico en modo CTR definido como sigue:

- Mensaje cifrado (*Encrypted Message*) C = A 7 1 B $_{(16}$ (el dígito hexadecimal menos significativo es el que primero se transmite y procesa)
- *Encryption Key* = $4_{(16}$
- *Nonce* = $A_{(16}$.



CIPH (KEY, INPUT)

		KEY															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INPUT	0	7	3	A	1	0	5	6	4	0	D	9	2	1	3	7	4
	1	3	0	F	4	5	7	2	2	7	F	B	7	6	F	2	5
	2	1	6	D	2	7	1	4	5	1	9	D	5	2	A	5	F
	3	6	1	B	0	2	3	7	6	3	B	F	3	0	1	3	B
	4	2	5	9	7	3	2	1	0	C	2	A	A	4	5	1	9
	5	0	4	8	3	1	6	5	7	A	6	E	F	5	4	0	E
	6	4	7	C	6	6	4	3	1	D	4	C	D	F	B	4	7
	7	5	2	E	5	4	0	0	3	E	0	8	B	B	8	6	3
	8	F	B	7	9	8	D	E	C	4	A	5	1	7	7	A	1
	9	B	8	2	C	D	F	A	A	2	E	7	0	3	2	F	6
	A	9	E	5	A	F	9	C	D	5	C	1	4	9	E	D	2
	B	E	9	3	8	A	B	F	E	6	8	3	6	E	9	B	0
	C	A	D	1	F	B	A	9	8	8	5	2	9	A	D	9	A
	D	8	C	0	B	9	E	D	F	F	7	6	8	8	C	8	8
	E	C	F	4	E	E	C	B	9	9	1	4	C	C	0	C	C
	F	D	A	6	D	C	8	8	B	B	3	0	E	D	6	E	D

RSA intercambiar claves sesión

Cifrar mensaje con CIPH(key, Input) modo CTR de 4bits

a) Alicia $k=7$ $(e_A, n_A)=(9,85)$

Bob $(e_B, n_B)=(7,77)$ Calcular la clave de sesion cifrada A→B

$C_k = M^{e_B} \bmod n_B = 7^7 \bmod 77 = \boxed{28}$

b)

Session key = $8_{(16} = 1000_{(2}$

Tamaño clave y bloque = 4 bits

Encryption key = $Sk \cdot 3_{(16} \bmod p(x) = \overset{x^3 \cdot (x+1)}{1000 \cdot 0011} \bmod 100101 = 11000 = \boxed{x^4+x^3}$

$p(x) = x^5+x^2+1$ 100101

Nonce = NOT(Sk) = $\boxed{0111}$

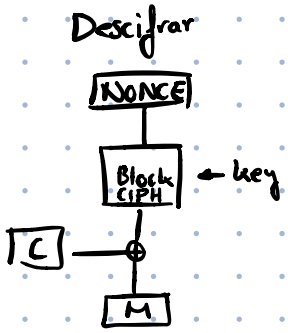
c) Detallar pasos y calcular el mensaje <u>enclaro</u>. El orden es de menor a mayor (←)

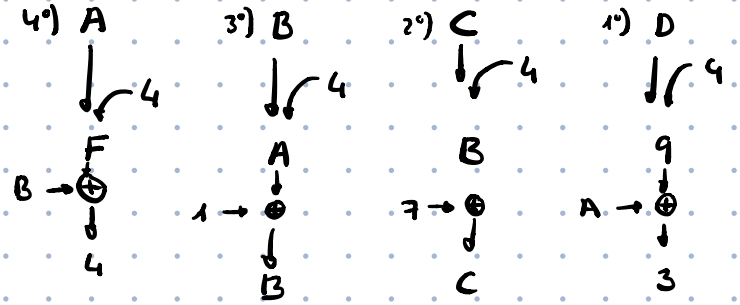
CTR:

Mensaje Cifrado $C = A71B_{(16} = 1010\ 0111\ 0001\ 1011$

Encryption key = $4_{(16} = 0100_{(2}$

Nonce = $A_{(16} = 1010_{(2}$





$\boxed{D(C) = 3\ C\ B\ 4}$