INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre __CHACON INOSTROSA JAIME ENRIQUE_RAMIREZ OLVERA GUILLERMO_SANCHEZ MENDEZ EDMUNDO
JOSUE_BERNAL RAMIREZ ANDRE_CEDILLO HERNANDEZ JUAN DANIEL_COVARRUBIAS SANCHEZ DANIEL_

Evaluación de conocimientos del segundo parcial.

1.- Betito recibió la siguiente imagen bmp de 24 bits cifrada. Sabe que Alicia utilizó Hill m=3 cuya llave $k=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix}$ y con el modo de operación OFB. IV=(0,1,2) Ayuda a Betito a encontrar P1 [3pts]

P1			P2		
			255	255	255

C1			C2		
16	3	8	151	146	119

Procedimiento:

$$(0 \quad 1 \quad 2)\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix} = (26 \quad 23 \quad 22)$$

$$(26 \quad 23 \quad 22) \oplus (16 \quad 3 \quad 8) = (10 \quad 20 \quad 30)$$

Resultado:

P1			P2		
10	20	30	255	255	255

C1			C2		
16	3	8	151	146	119

2.-Actualmente AES es un estándar oficial para cifrado de información. [5pts]

a) Describa las diferencias de la historia de la creación y funcionalidad de AES en comparación con la de DES.

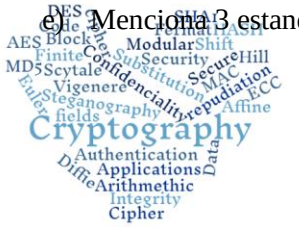
DES	AES
El plaintext con el que se trabaja es de 64 bits	El plaintext con el que se trabaja puede ser de 128, 192 o 256 bits.
En el DES se realizan 16 rondas	Se realizan: 10 rondas para 128 bits 12 rondas para 192 bits 14 rondas para 256 bits
Fue publicado en 1977 por el Instituto Nacional de Normas y Tecnología y se basa en la estructura Feisel donde el plaintext se divide en 2	Fue publicado en 1977 por el Instituto Nacional de Estándares y Tecnología, este fue publicado para reemplazar a AES ya que al DES se le consideraba muy lento y que su clave era muy pequeña
Se trabaja con las sbox para cada caso en cada operación.	Se utiliza una matriz para identificar los diferentes valores por los que hay que reemplazar.

b) ¿Cuál es el nombre original del algoritmo conocido como AES?
R.- AES= Advanced Encryption Standard (Rijndael)

c) ¿Quién desarrolló este algoritmo?
R.- El algoritmo AES fue desarrollado por Vincent Rijmen y Joan Daemen y fue asumido oficialmente el 26 de noviembre del 2001.

d) ¿Qué implica hablar de AES 192? (Qué tamaño de bloque y longitud de llave permite este algoritmo)
R.- Para AES 192 se necesita tener una llave de longitud 192, un tamaño de bloque de 128 y como numero de rondas un total de 12.

e) Menciona 3 estandáres/protocolos de seguridad que utilicen AES.



M. en C. Nidia A. Cortez Duarte

- Protocolo CCMP
- Protocolo GCMP
- Estándar SSH
- Estándar IPsec

3.- Para el Algoritmo AES, algunos calculos se realizan mediante campos finitos (Galois Field).

Considera GF(2^4), P(x) = x^4 +x +1, A(x) = x^2 +1, B(x) = x^3 +x^2 +1

a) Calcular A(x) + B(x) mod P(x) [1pts]
b) Calcular A(x) * B(x) mod P(x) [2pts]

a)

Procedimiento:

A(x) = x^2 +1 = 0101

B(x) = x^3 +x^2 +1=1101

Resultado: A(x) + B(x) mod P(x) = 1000

b)

Procedimiento:

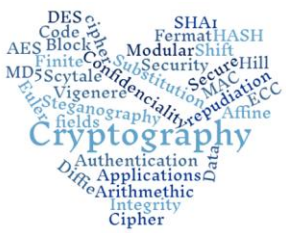
A(x) = x^2 +1 = 0101

B(x) = x^3 +x^2 +1=1101

P(x) = x^4 +x +1= 10011

A(x) * B(x) mod P(x)=

```
    0101
  * 1101
  ------
    0101
  + 010100
  --------
   0101000
  --------
  00111001
     0011
     0011
  ------
     1100
```



M. en C. Nidia A. Cortez Duarte

Resultado: A(x) + B(x) mod P(x) = 1100= 0xC

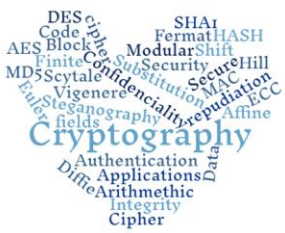
4.- Considera el AES 128, ¿Cuál es la salida de la primera ronda de AES si el bloque en plan consta de 128 unos, y la llave inicial también consta de 128 unos? Escribe tu resultado en formato de matriz [4pts]

8B	74	8B	74
8A	75	8A	75
8A	75	8A	75
8A	75	8A	75

Procedimiento:

Llave Inicial			
FF	FF	FF	FF
FF	FF	FF	FF
FF	FF	FF	FF
FF	FF	FF	FF

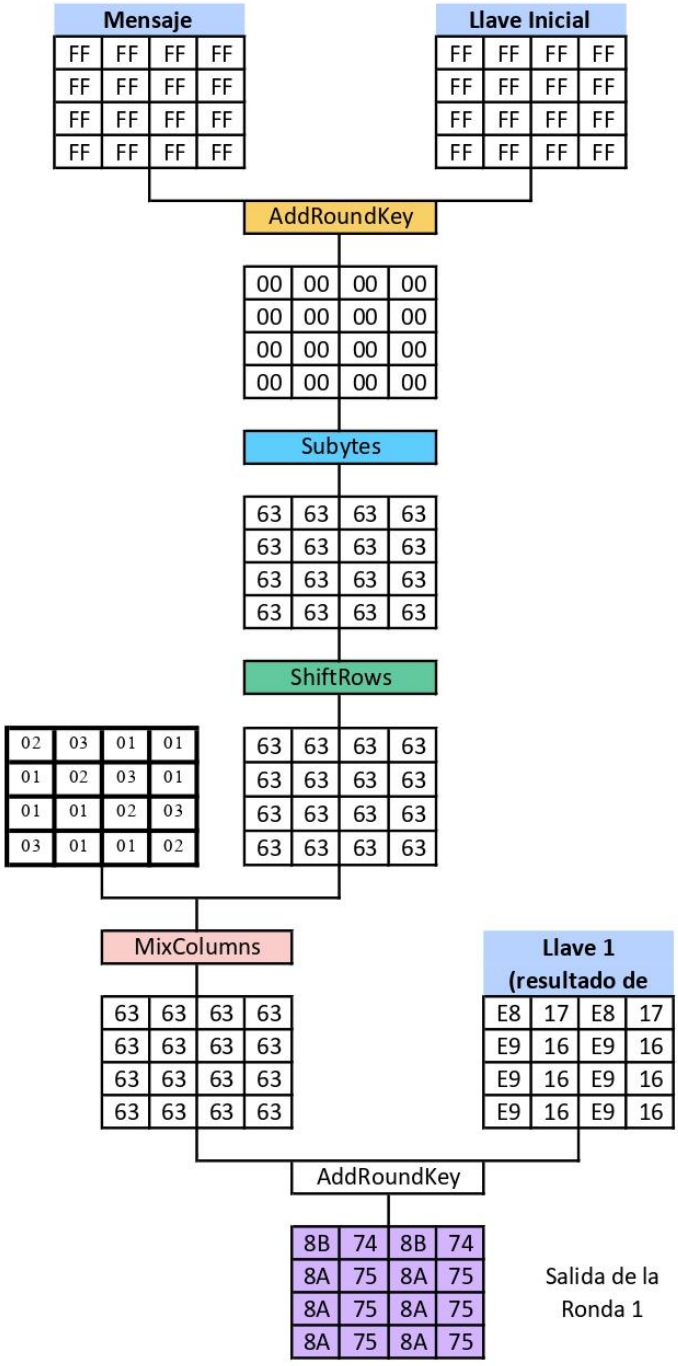
Subllave 1						
FF		16		01	E8	
FF	XOR	16	XOR	00	-> E9	FILA 1
FF		16		00	E9	
FF		16		00	E9	
E8		FF		17		
E9	XOR	FF	->	16		FILA 2
E9		FF		16		
E9		FF		16		
17		FF		E8		
16	XOR	FF	->	E9		FILA 3
16		FF		E9		
16		FF		E9		
E8		FF		17		
E9	XOR	FF	->	16		FILA 4
E9		FF		16		
E9		FF		16		



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre __CHACON INOSTROSA JAIME ENRIQUE_RAMIREZ OLVERA GUILLERMO_SANCHEZ MENDEZ EDMUNDO JOSUE_BERNAL RAMIREZ ANDRE_CEDILLO HERNANDEZ JUAN DANIEL_COVARRUBIAS SANCHEZ DANIEL_

Evaluación de conocimientos del segundo parcial.

Message:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
Key:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF



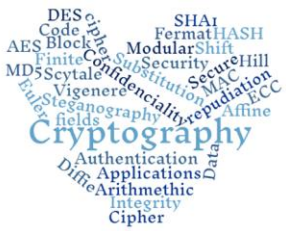
INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre __CHACON INOSTROSA JAIME ENRIQUE_RAMIREZ OLVERA GUILLERMO_SANCHEZ MENDEZ EDMUNDO JOSUE_BERNAL RAMIREZ ANDRE_CEDILLO HERNANDEZ JUAN DANIEL_COVARRUBIAS SANCHEZ DANIEL_

Evaluación de conocimientos del segundo parcial.

Nota: Los procedimientos deben realizarse a mano, deben escanear sus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

Ejercicios sin procedimientos a mano valen 0 puntos, excepto ejercicio 2.

Al finalizar guardar un sólo archivo como PDF para subirlo a Classroom.



M. en C. Nidia A. Cortez Duarte