Apellido y Nombre:……..... *Legajo:*.....

Criptografía y Seguridad (72.44)

PARCIAL 1 – *2016*

Ej. 1	*Ej. 2*	*Ej. 3*	*Ej. 4*	*Ej. 5*	*Nota*
3 puntos	2 puntos	1,5 puntos	2 puntos	1,5 puntos	

IMPORTANTE:
- **Las respuestas no se ajusten estrictamente al enunciado, no serán aceptadas.**
- **La condición de aprobación es sumar 5 puntos.**

EJERCICIO 1: En un esquema de **transposición por columnas**, el texto del mensaje se distribuye en una matriz de k columnas (siendo k la clave) y lueo se obtiene el texto cifrado concatenando las letras de cada fila empezando por la columna 1, luego la columna 2, hasta la columna k. (Es decir, leyendo las filas de la matriz traspuesta de la que contiene el mensaje)

Ejemplo: **m = "ESTEMENSAJEESCLARO", k = 3**

E	**S**	**T**
E	**M**	**E**
N	**S**	**A**
J	**E**	**E**
S	**C**	**L**
A	**R**	**O**

Entonces el cifrado es **c = "EENJSASMSECRTEAELO"**

Considerar un **esquema de transposición por columnas**, tal que:

Gen: elige aleatoriamente y en forma uniforme $k \in K = \{2,3\}$

Enc: Si el texto plano es $m = m_1 m_2 ... m_6$, entonces el cifrado c es $c = c_1 c_2 ... c_6$, donde m se distribuyó en una matriz M_{enc} de k columnas y $6/k$ filas y c corresponde a la lectura por filas de la matriz traspuesta de M_{enc}.

Dec: Si el cifrado es $c = c_1 c_2 ... c_6$, entonces el texto plano es $m = m_1 m_2 ... m_6$, donde c se distribuyó en una matriz M_{dec} de k filas y $6/k$ columnas y m corresponde a la lectura por filas de la matriz traspuesta de M_{dec}.

DEMOSTRAR de manera formal si el esquema de cifrado propuesto tiene secreto perfecto para los siguientes espacios de mensajes, indicando en cada caso qué definición de secreto perfecto se utilizó.

a) $M = \Sigma^6 / \Sigma = \{'a','b','c','d','e','f'\}$ (es decir $|m| = 6$)

b) $M \subset \Sigma^6 / \Sigma = \{'a','b','c','d','e','f'\} \wedge \left(m \in M \Leftrightarrow m = m_0 ... m_5 \wedge m_i \neq m_j\right)$

EJERCICIO 2: Se tienen dos protocolos en los cuales un participante (A) envía a otro (B) un mensaje y.

Protocolo 1: $y = Enc_{k1}\left(x \parallel H\left(k_2 \parallel x\right)\right)$

Donde x es un mensaje, H es una función de hash, Enc es un algoritmo de encripción simétrico, || denota una concatenación y k1 y k2 son claves secretas compartidas y conocidas únicamente por el emisor y el receptor.

Protocolo 2: $y = Enc_k\left(x \parallel Sign_{kprA}\left(H(x)\right)\right)$

Donde x es un mensaje, H es una función de hash, Enc es un algoritmo de encripción mediante clave secreta compartida k, || denota una concatenación y kprA es la clave privada de A (emisor del mensaje y)

a) EXPLICAR qué pasos efectúa B (el receptor) con el mensaje recibido en cada protocolo.

b) ESTABLECER, para cada protocolo, si los siguientes aspectos se preservan:

- **CONFIDENCIALIDAD**

- **INTEGRIDAD**
- **NO REPUDIO**
- **SEGURIDAD ANTE ATAQUE DE REPLAY**

EJERCICIO 3: Considere el modo de cifrado de bloque llamado **"Fischer Spiffy Mixer" (FSM)**
En este modo, la encripción de una secuencias de bloques de mensaje $m_1 ... m_n$ resulta en una secuencia $c_1 ... c_n$, donde:

$c_0 = IV_1$

$m_0 = IV_2$

$c_i = m_{i-1} \oplus F_k(m_i \oplus c_{i-1}), \forall i \geq 1$

Los vectores de inicialización IV son acordados y conocidos por emisor y receptor.
F_k es una función seudoaleatoria.

A) **DESCRIBIR** cómo se hace la desencripción.

B) Si un bit en el bloque cifrado c_j se daña en la transmisión, ¿qué bloques de texto se descifrarán mal? ¿Por qué?

EJERCICIO 4:

A) EXPLICAR qué significan las siglas PKI Y KDC.

B) COMPARAR PKI Y KDC (Encontrar por lo menos una similitud o punto en común y una diferencia)

EJERCICIO 5: Elegir, en cada caso, la única opción correcta.

(1) EL SIGUIENTE PROTOCOLO:

1. Alice ejecuta $G(1^n)$ para obtener (G, q, g) (Grupo cíclico, orden, generador)
2. Alice elige $x \leftarrow Z_q$ de manera aleatoria y uniforme, y calcula $h_1 := g^x$
3. Alice envía (G, q, g, h_1) a Bob.
4. Bob recibe (G, q, g, h_1). Elige $y \leftarrow Z_q$ de manera aleatoria y uniforme, y calcula $h_2 := g^y$. Bob envía h_2 a Alice y emite la clave $k_B := h_1^y$

a) Es un protocolo de etiquetado de mensajes (MAC).
b) Es un protocolo de Firma asimétrico.
c) Es un protocolo de intercambio de claves.
d) Es un protocolo de encripción asimétrico.

(2) UN CRIPTOSISTEMA (GEN, ENC, DEC), CON:

- **GEN:** elige en forma uniforme y aleatoria $k \leftarrow \{0,1\}^n$
- **ENC:** obtiene c a partir de $m \in \{0,1\}^n$ y $F_k(x)$ una función seudoaleatoria.

Es seguro frente a ataque de texto plano conocido (CPA) si:

a) $c := \langle F_k(m) \oplus k \rangle$

b) $c := \langle r, m \oplus r \rangle, r \leftarrow \{0,1\}^n \; seudoaleatorio$

c) $c := \langle r, F_k(r) \oplus m \rangle, r \leftarrow \{0,1\}^n \; seudoaleatorio$

d) $c := \langle F_k(m) \rangle$

(3) LA CONSTRUCCIÓN CBC-MAC ES UNA CONSTRUCCIÓN SEGURA PARA MAC:

a) si los mensajes son de longitud fija y el vector IV es aleatorio
b) si los mensajes son de longitud variable y el vector IV es aleatorio
c) si los mensajes son de longitud fija y el vector IV es constante
d) si los mensajes son de longitud variable yel vector IV es constante