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

Criptografía y Seguridad (72.44)

PARCIAL 1 – *2017*

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: Un cilindro de Jefferson está compuesto por 36 discos, unidos sobre un eje de rotación en el interior que le permite rotar libremente. Cada disco tiene a su vez 26 letras, A-Z, en la periferia, con un orden específico para cada disco, en una configuración particular. Es decir, cada disco tiene una permutación particular de A-Z, y a su vez, el orden de los discos puede alterarse. Una barra de referencia con una ranura se coloca de manera paralela al eje por donde es posible leer la alineación de las letras.

El mecanismo de encripción procede alineando los discos hasta formar sobre la ranura el mensaje de 36 letras a encriptar y se selecciona una de las 25 alineaciones restantes para formar el texto cifrado. Ejemplo, si el mensaje a encriptar arranca con "ATAQUE…", se rota el primer disco hasta que la "A" quede visible sobre la ranura, el segundo disco hasta que quede visible la "T", y así sucesivamente. Luego se elige alguna de las 25 alineaciones restantes, y esa corresponde al texto cifrado.

Con discos con exactamente la misma configuración de letras cada uno y ordenados en la misma secuencia, se procede a la Desencripción alineando el texto cifrado con cada una de las letras de cada disco sobre la ranura y buscando en las restantes 25 alineaciones, aquella que posea algún texto plano reconocible.

Considerando por simplicidad mensajes de 36 letras,

a) **CUÁL** es el tamaño del espacio de claves.

b) **DEMOSTRAR** si este sistema admite secreto perfecto y bajo qué condiciones. Especificar claramente la estrategia de la demostración elegida.

EJERCICIO 2: Dado el siguiente esquema de intercambio de claves (Shamir's no-key protocol) entre A y B.

Gen:

Público $p\ prime$

A,B seleccionan $a, b |\ 1 \leq a, b \leq p-2, a \perp (p-1), b \perp (p-1)$ ($\perp$ coprimo).

A selecciona K, clave de sesión al azar, $1 \leq K \leq p-1$

Trans:

1) $A \rightarrow B: K^a mod\ p$

2) $A \leftarrow B: (K^a)^b mod\ p$

3) $A \rightarrow B: (K^{ab})^{a^{-1}} mod\ p$ (de forma tal que $(K^a)^{a^{-1}} mod\ p = K$)

a) **DETALLAR** cuál es el objetivo del protocolo, y dónde radica la seguridad computacional del mismo.

b) **EN QUE** se diferencia con Diffie-Hellman.

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

Criptografía y Seguridad (72.44)

PARCIAL 1 – *2017*

EJERCICIO 3: Especificar los pasos de validación que debería realizar un browser al conectarse a un homebanking para verificar que el certificado presentado por el sitio no es apócrifo.

EJERCICIO 4: Dado el siguiente algoritmo de generación de MAC, demostrar mediante la prueba Mac-Forge cómo un Atacante podría tener éxito en la ejecución del experimento.

$k \leftarrow \{0,1\}$

$$t \leftarrow Mac_k(m) := \begin{cases} t\ es\ bit\ paridad\ par\ si\ k = 0 \\ t\ es\ bit\ paridad\ impar\ si\ k = 1 \end{cases}$$

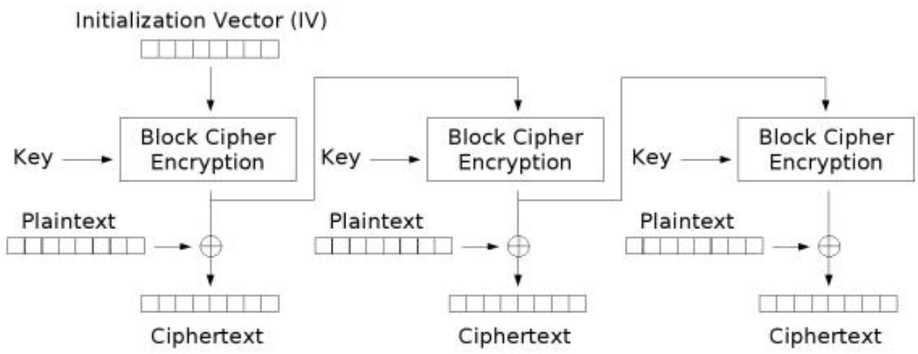
$$b \leftarrow Vrfy_k(m,t) := \begin{cases} 1 & si\ k = 0\ y\ t\ es\ bit\ paridad\ par\ de\ m \\ 1 & si\ k = 1\ y\ t\ es\ bit\ paridad\ impar\ de\ m \\ 0 & otro \end{cases}$$

Recordar que si m=1001, paridad par es agregarle un bit adicional para que la cantidad de 1(unos) en el mensaje sea par, y paridad impar es, correspondientemente, para que esa cantidad sea impar.

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

(1) EN EL MODO DE ENCADENAMIENTO PARA CIFRADOS EN BLOQUE OFB:

a) Cada bloque del texto cifrado Ci surge de Encriptar cada bloque del texto plano Pi
b) La alteración de un bit de Ci afecta toda la Desencripción a partir de ese punto.
c) La salida Oj de cada bloque de encripción se genera encriptando la salida del bloque Oj-1
d) Se aplica una operación XOR inicial sobre el IV que luego se Encripta formando Ki inicial



Output Feedback (OFB) mode encryption

(2) EL "CVV" O *CODE VERIFICATION VALUE* ES EL CÓDIGO DE VALIDACIÓN DE 3 Ó 4 DÍGITOS QUE SE USA EN LAS TARJETAS DE CRÉDITO PARA DEMOSTRAR POSESIÓN REAL DEL PLÁSTICO EN VTA. TELEFÓNICA. QUE MECANISMO CRIPTOGRÁFICO SERÍA EL MÁS CONVENIENTE PARA REALIZAR LA VALIDACIÓN DE DICHO CÓDIGO EN LOS SERVIDORES DEL BANCO EMISOR DE LA TARJETA Y ASÍ VERIFICAR QUE EL MISMO ES VÁLIDO, PERO SIN QUE EL CÓDIGO ESTÉ DIRECTAMENTE ACCESIBLE EN LAS BASES DE DATOS.

a) Un HMAC basado en una clave simétrica almacenada de manera segura en el banco emisor.
b) AES-256 basado en una clave pública distribuida públicamente de manera autenticada.
c) Un esquema de Diffie-Hellman para intercambiar ese código.
d) Una firma digital basado en una clave pública distribuida de manera autenticada.

(3) QUE MECANISMO CRIPTOGRÁFICO SERÍA MÁS CONVENIENTE UTILIZAR PARA LA DISTRIBUCIÓN DE SOFTWARE EN LOS MERCADOS DE APPS QUE SE UTILIZAN EN LOS DISPOSITIVOS MÓVILES.

a) Un mecanismo de encripción simétrica TDES con una clave secreta.
b) Un CBC-MAC basado en una Función pseudoaleatoria Fk.
c) Un esquema de firma digital sobre los binarios.
d) Una función de Hash SHA-1 aplicado sobre los ejecutables.