Pregunta 1

10 de 10 puntos

¿ En qué está basado el cifrado simétrico DES ? Explicar la idea general, que es lo que se busca en el algoritmo. Si trabajasen en un banco y alguién propone utilizar este protocolo, ¿ Que aconsejarían y cómo lo argumentarían ?

Respuesta seleccionada: DES está basado en redes Feistel. La idea general es que se parte el texto plano en 2 mitades y la clave en varias partes, Se transforma una mitad del texto con una caja Feistel y una parte de la clave, se intercambian las mitades de lugar y se repiten los pasos anteriores hasta terminar. La entrada es de 64 bits y la clave también, pero en el caso de esta útima solo 56 son efectivos.

se busca que sea computacionalmente muy dificil recuperar el mensaje por fuerza bruta.

Desaconsejaría que se utilize DES en el banco ya que el algoritmo está debilitado (se puede romper en 2^43 intentos), en su lugar usaría AES.

Respuesta correcta: [None]

Comentarios para respuesta: [No se ha dado ninguna]

Pregunta 2

10 de 10 punt

Supongase que se desea encriptar un mensaje con $M \in \{0,1,2\}$ utilizando una clave simétrica compartida $K \in \{0,1,2\}$. Los datos se representan con dos bits (00,01 y 10). El procedimiento de encripción consiste en XORear las dos representaciones.

a) Explicar si este esquema de las garantías de seguridad de One-Time Pad. Demostrar mediante la realización de un experimento $Exp_{eav}(A, n)$

b) Ofrecer una alternativa al esquema anterior que ofrezca las garantías de seguridad de One-Time Pad manteniendo los mismos espacios de M y K.

Respuesta seleccionada: a)
P(C = 10 | M = 01) = 0
P(C = 10 | M = 10) = 1/3

0 != 1/3

En un EAV:

El esquema da las garantías de seguridad de One-Time Pad si P(acierto) del atacante es 0,5 + δ (delta despreciable)

A envía m0 = 00 y m1 = 01
si C <= 2, emite 0 sino 1

M	K	C	B'	acertó?
00	00	00	0	SI
00	01	01	0	SI
00	10	10	0	SI
01	00	01	0	NO
01	01	00	0	NO
01	10	11	1	SI

P(acierto) = 4/6 > 0.5 => No tiene secreto perfecto

b) Se podría usar una matríz de encripción que para cada posible mensaje, tenga uniformemente distribuídas las posibles encripciones y de esta forma el atacante tendría una probabilidad de éxito del 0.5 aprox.

Respuesta correcta: [None]

Comentarios para respuesta: [No se ha dado ninguna]

Pregunta 3

10 de 10 puntos

Planteen un algoritmo de encripción simple basado en un algoritmo de sustitución polialfabética. ¿ Cómo y bajo qué condiciones pueden utilizarlo para implementar con el un esquema de One-Time-Pad ?

Respuesta seleccionada: Cualquier criptosistema que tenga secreto perfecto, puede reducirse a One-Time-Pad. Un ejemplo de un algoritmo de sustitución polialfabética es Vigenere, que para que tenga secreto perfecto, La clave que se utilize debe tener una longitud igual o mayor a la longitud del mensaje a encriptar.

Respuesta correcta: [None]

Comentarios para respuesta: [No se ha dado ninguna]

Pregunta 4

10 de 10 puntos

Lo importante al encriptar un mensaje con un Mac es que este demostrado que para esta primitiva es computacionalmente complejo encontrar la preimagen, eventuales colisiones o segundas preimagenes.

Respuesta seleccionada: Falso

Respuestas:
- Verdadero
- Falso

Pregunta 5

10 de 10 puntos

La ventaja del modo de encripción en bloque CBC es que puede ser paralelizable.

Respuesta seleccionada: Falso

Respuestas:
- Verdadero
- Falso

Pregunta 6 10 de 10 puntos

Un experto en seguridad afirma que un sistema de Encripción basada en una primitiva segura E_k es CPA-Secure. El emisor, al enviar un mensaje m, obtiene un número al azar r y envía $(r, E_k(r) \oplus m)$.

Respuesta seleccionada: La afirmación es cierta ya que el valor de $E_k(r)$ es inindistinguible de un valor al azar uniforme y su determinismo sólo depende de r.

Respuestas: La afirmación es cierta ya que el valor de $E_k(r)$ es inindistinguible de un valor al azar uniforme y su determinismo sólo depende de r.

La afirmación es correcta ya que al ser $E_k(\cdot)$ una primitiva de encripción segura, el sistema será también CPA-Secure.

La afirmación es falsa ya que al utilizar el XOR se corre el riesgo de que ese valor sea reversado y el valor m pueda ser exraído.

La afirmación es falsa, ya que para que sea CPA-Secure requiere además de un tag que garantice integridad.

Comentarios para respuesta: Este es el esquema más básico para implementar un algoritmo CPA-Secure.

Pregunta 7 10 de 10 puntos

Una firma digital basada en un algoritmo simétrico requiere utilizar primitivas de hash.

Respuesta seleccionada: Falso

Respuestas: Verdadero

Falso

Pregunta 8 10 de 10 puntos

El siguiente protocolo permite el intercambio de claves de sesión de largo plazo mediante dos entidades A y B. El protocolo arranca una vez que A y B generaron una clave K mediante un algoritmo de intercambio seguro de claves.

$$B \rightarrow A: n_b$$
$$A \rightarrow B: E_k(sk_a, n_a, n_b, B^*)$$
$$B \rightarrow A: E_k(sk_b, n_b, n_a, A^*)$$

donde k es una clave simétrica generada por un protocolo de intercambio de clave como DH, sk_a y sk_b son claves de sesión de largo plazo para comunicarse con A y B respectivamente, y n_a y n_b son nonces. A^* y B^* son números que permiten verificar la integridad de las claves de sesión de largo plazo.

a) ¿ Cuál es el propósito de los nonces en este protocolo ?

b) ¿ Mediante qué primitiva criptográfica podrían implementarse la generación de A* y B* ?

Respuesta seleccionada: a) El propósito de los nonces en este protocolo es fundamentalmente para evitar los ataques de Replay, ya que sin ellos un atacante podría enviar varias veces un mismo mensaje y el receptor no tendría forma de identificar el ataque.

b) Podría implementarse una primitiva de Hash (hasheando las claves de sesión de largo plazo)
Ej:
B* = Hash(sk_a || n_b)
A* = Hash(sk_b || n_a)

Respuesta correcta: [None]

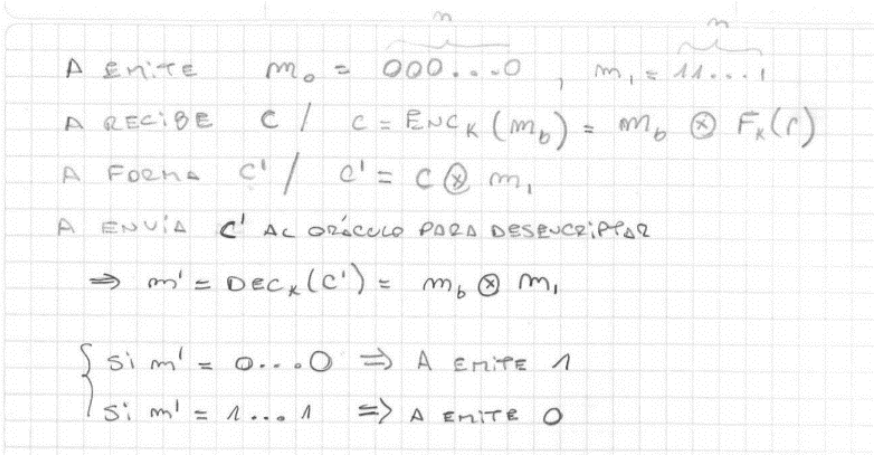
Comentarios para respuesta: [No se ha dado ninguna]

Pregunta 9 10 de 10 puntos

Plantear un experimento $Exp_{cca}(A, n)$ y demostrar por qué en un criptosistema basado en un función pseudoaleatoria $E_k = F_k(r) \oplus m$ el atacante no tiene éxito.

Respuesta seleccionada: ej9.pdf

Comentarios para respuesta: Bien



Pregunta 10

10 de 10 puntos

El algoritmo de ElGamal permite la generación entre Alice y Bob de una clave de sesión por un canal inseguro.

Respuesta seleccionada: Falso

Respuestas:

Verdadero

Falso