Parcial Online

Ejercicios de opción múltiple

Ejercicio 1

Un experto en seguridad afirma que un sistema de encripción basado 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) xor m).

- La afirmación es cierta ya que el valor de E_k(r) es indistinguible de un valor al azar uniforme y su determinismo sólo depende de r.
- La afirmación es correcta ya que al ser E_k(r) 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 extraído.
- La afirmación es falsa, ya que para que sea CPA-Secure requiere además de un tag que garantice integridad.

Ejercicios de verdadero o falso

Ejercicio 2

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

- Verdadero
- Falso

Ejercicio 3

Lo importante al enciptar un mensaje con un MAC es que esté demostrado que para esta primitiva es computacionalmente complejo encontrar la preimagen, eventuales colisiones o segundas preimágenes.

- Verdadero
- Falso

Ejercicio 4

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

- Verdadero
- Falso

Ejercicio 5

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

- Verdadero

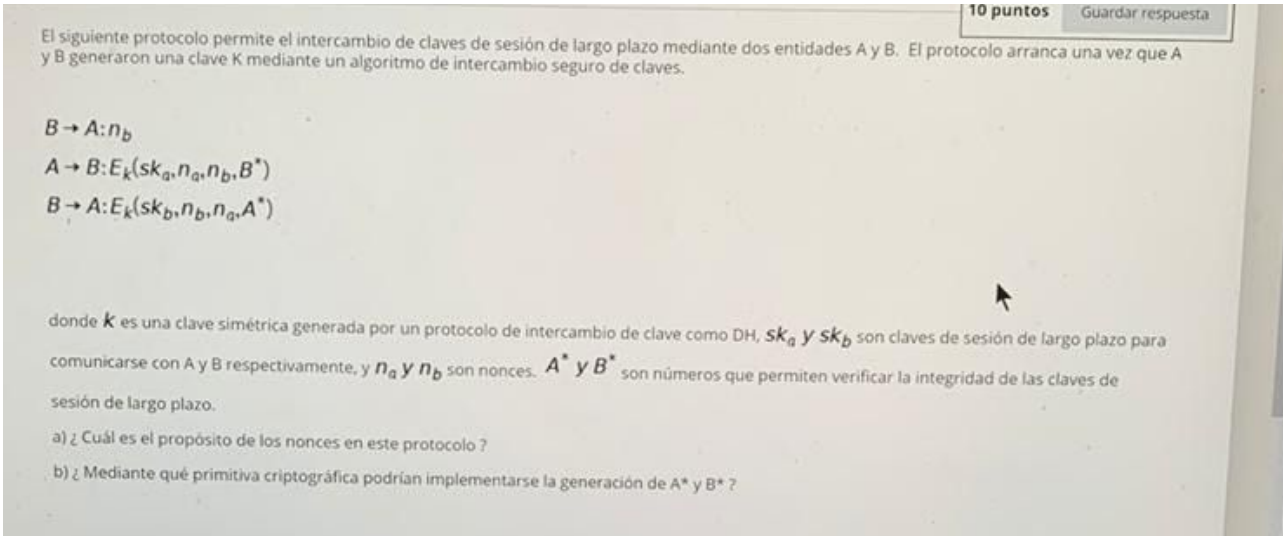
- Falso

Ejercicios de completar en box de campus

Ejercicio 6

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

Ejercicio 7



10 puntos Guardar respuesta

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* ?

Ejercicio 8

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

Ejercicio 9

Supóngase que se desea que se desea encriptar un mensaje con M€{0, 1, 2} utilizando una clave simétrica compartida K€{0, 1, 2}. Los datos se representan con dos bits (00, 01, 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.

Ejercicios de subir archivo

Ejercicio 10

Plantear un experimento $Exp_{CCA}(A, n)$ y demostrar por qué en un criptosistema basado en una función pesudoaleatoria $E_k=F_k(r)$ xor m el atacante no tiene éxito.