Revisar entrega de examen: Parcial 1

Pregunta 1

Una autoridad certificante puede certificarse a sí misma.

Pregunta 2

Cualquier criptosistema que cumpla con la propiedad de CCA-Secure garantiza directamente integridad.

Pregunta 3

Base64 es un mecanismo de encripción simétrico muy utilizado en los bancos

Pregunta 4

El algoritmo de AES se basa es las Feister-Network para cifrar simétricamente un mensaje m.

Pregunta 5

Si un criptosistema es MAC-resistant, entonces es CCA.

Pregunta 6

a) Explicar qué es el salt en las funciones de hashing y por qué su uso es importante.

b) ¿ Cómo se podría utilizar el hash en un sistema de registro de claves de acceso (passwords) en una base de datos?

Pregunta 7

Un sistema de encripción simétrico

Pregunta 8

En criptografía asimétrica, en caso de que quiera enviar un mensaje que solo una persona pueda leerlo, lo encripto con mi llave pública.

Pregunta 9

No existe ningún mecanismo para quebrar un criptosistema que tiene seguridad perfecta

Pregunta 10

Dado el siguiente protocolo de intercambio/generación de una clave simétrica (k1 || k2), y asumiendo que tanto A como B están en posesión de CertA y CertB

$1: A \rightarrow B: Sig_A(k_1)$

$2: B \rightarrow A: Sig_B(k_1 \,||\, k_2)$

← **Aceptar**