Diego Viñals Lage

Criptografía

1. La criptografía puede definirse como "El conjunto de conocimientos científicos, métodos y técnicas que hacen posible la transformación de los datos para:":
    a. Ocultar su información (confidencialidad)
    b. Garantizar su integridad
    c. Garantizar su autenticidad
    d. Todas las respuestas son correctas

2. Los objetivos de la criptografía desde el punto de vista de la seguridad informática son (señala la opción incorrecta):
    a. Confidencialidad: Garantizar que personas no autorizadas no accedan a la información
    b. Eficiencia: Garantizar la máxima velocidad de enlace.
    c. Integridad: Garantizar que la información no sea alterada por personas no autorizadas de forma que no sea detectable por los usuarios autorizados
    d. Autenticidad: Garantizar que los usuarios son las personas que dicen ser

3. En los métodos clásicos de transposición por filas / columnas, los elementos se introducen según un patrón geométrico (por ejemplo por filas) y se extraen según otro patrón (por ejemplo, por columnas)
    a. Verdadero
    b. Falso

4. Indicar cuál de los siguientes se corresponden con métodos clásicos de sustitución:
    a. Monoalfabéticos, como el Cifrado César
    b. Sustitución por dígrafos, como Playfair
    c. Sustitución polialfabéticos, como Vigenere
    d. Todas las respuestas son correctas.

5. Indicar cuál de los siguientes se corresponden con técnicas de criptoanálisis:
    a. Análisis de frecuencias
    b. Detección de patrones de repetición idiomáticos
    c. Método Kasisky
    d. Todas las respuestas son correctas.

6. ¿Verdadero o Falso? El algoritmo AES es un algoritmo simétrico de bloque que emplea una base matemática de álgebra polinomial modular (Cuerpos de Galois)
    a. Verdadero
    b. Falso

7. Indicar cuál de las de la siguientes no es una función implementada en el del algoritmo AES:
    a. SubBytes
    b. ShiftRows
    c. Esquema Feistel
    d. MixColumns

8. Indicar cuál de los de las siguientes se corresponde con modos de operación definidos por el NIST:
    a. ECB: Electronic Code Book
    b. CBC: Cipher Block Chaining
    c. CTR: Counter
    d. Todas las respuestas son correctas (buscar)

9. Indicar cuál de los de las siguientes afirmaciones es falsa en relación a las funciones Hash:
    a. Son un elemento fundamental para asegurar y verificar la integridad de la información.
    b. Admiten textos de entrada de cualquier longitud, y generan un hash de longitud fija.
    c. Son una función ampliamente utilizada en la criptografía clásica pero actualmente en desuso.
    d. En combinación con el empleo de la clave privada, son la base de las firmas digitales.

10. ¿Verdadero o Falso? Los certificados digitales, entre otra información, vinculan la clave privada de un sujeto con su identidad real, y van firmados digitalmente con la clave pública de la autoridad de certificación que lo ha emitido.
    a. Verdadero
    b. Falso

11. Indicar cuál de los siguientes campos se incluye habitualmente en los certificados digitales conformes a la norma X-509:
    a. Clave privada del sujeto
    b. Clave pública del sujeto
    c. Clave privada del emisor
    d. Firma digital generada con la clave privada del sujeto