Criptografía

1. La criptografía puede definirse como "El conjunto de conocimientos científicos, métodos y técnicas que hacen posible la transformación de los datos para:":
   1. Ocultar su información (confidencialidad)
   2. Garantizar su integridad
   3. Garantizar su autenticidad
   4. **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):
   1. Confidencialidad: Garantizar que personas no autorizadas no accedan a la información
   2. **Eficiencia: Garantizar la máxima velocidad de enlace.**
   3. Integridad: Garantizar que la información no sea alterada por personas no autorizadas de forma que no sea detectable por los usuarios autorizados
   4. 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)
   1. **Verdadero**
   2. Falso
4. Indicar cuál de los siguientes se corresponden con métodos clásicos de sustitución:
   1. Monoalfabéticos, como el Cifrado César
   2. Sustitución por dígrafos, como Playfair
   3. Sustitución polialfabéticos, como Vigenere
   4. **Todas las respuestas son correctas.**
5. Indicar cuál de los siguientes se corresponden con técnicas de criptoanálisis:
   1. Análisis de frecuencias
   2. Detección de patrones de repetición idiomáticos
   3. Método Kasisky
   4. **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)
   1. **Verdadero**
   2. Falso
7. Indicar cuál de las de la siguientes no es una función implementada en el del algoritmo AES:
   1. SubBytes
   2. ShiftRows
   3. **Esquema Feistel**
   4. MixColumns
8. Indicar cuál de los de las siguientes se corresponde con modos de operación definidos por el NIST:
   1. ECB: Electronic Code Book
   2. CBC: Cipher Block Chaining
   3. CTR: Counter
   4. **Todas las respuestas son correctas (buscar)**
9. Indicar cuál de los de las siguientes afirmaciones es falsa en relación a las funciones Hash:
   1. Son un elemento fundamental para asegurar y verificar la integridad de la información.
   2. Admiten textos de entrada de cualquier longitud, y generan un hash de longitud fija.
   3. **Son una función ampliamente utilizada en la criptografía clásica pero actualmente en desuso.**
   4. 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.
    1. **Verdadero**
    2. Falso
11. Indicar cuál de los siguientes campos se incluye habitualmente en los certificados digitales conformes a la norma X-509:
    1. Clave privada del sujeto
    2. **Clave pública del sujeto**
    3. Clave privada del emisor
    4. Firma digital generada con la clave privada del sujeto