



## “Introducción a los criptosistemas y conceptos relacionados”

### Test de autoevaluación

---

Seleccione la respuesta correcta.

1. Señale la afirmación correcta:
  - La definición clásica de criptografía incluye los métodos y técnicas para prevenir la modificación no autorizada de la información.
  - La definición clásica de criptografía se preocupaba por la disponibilidad de la información.
  - La definición moderna de criptografía incluye formas de evitar el repudio de los datos.**
  - Las definiciones (clásica y moderna) de criptografía hablan de proteger los datos, no de transformarlos.
2. En un criptosistema...
  - No existen claves.
  - Hay dos claves, necesariamente diferentes.
  - Hay una clave, que comparten ambos comunicantes.
  - Hay dos claves, que pueden ser iguales.**
3. Los sistemas criptográficos se clasifican según...
  - El tipo de operaciones: de contracción y de expansión.
  - El número de claves: básicos y extendidos.
  - El tipo de procesamiento de la información a cifrar: por bloques y en flujo.**
  - Su reversibilidad: reversibles o irreversibles.
4. Según el principio de Kerckoffs,
  - La seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave.**
  - La seguridad del cifrado debe residir en el secreto de su diseño.
  - La seguridad del cifrado debe depender de la aleatoriedad del mensaje en claro.
  - La seguridad del cifrado debe residir en la complejidad de sus operaciones.

- 
5. El objetivo del criptoanalista es:
- Descifrar un texto concreto.
  - Suplantar al emisor legítimo.
  - **Recuperar la clave de descifrado.**
  - Obtener fama y reconocimiento, exclusivamente.
6. En lo que se refiere a los ataques de criptoanálisis al algoritmo:
- El más fácil es el del texto en claro escogido.
  - **En el ataque de texto en claro escogido, los mensajes se cifran con la misma clave.**
  - El ataque de texto escogido es el más fácil, pues es el único en el que el atacante conoce el algoritmo.
  - En el ataque de texto en claro conocido, el atacante escoge uno o más criptogramas y los cifra con diferentes claves.
7. El cifrador de Vernam:
- **Es incondicionalmente seguro si, entre otras cosas, se utiliza una clave de cifrado aleatoria.**
  - Es computacionalmente seguro, pero no incondicionalmente seguro.
  - Es irrompible si la clave de cifrado es aleatoria y se usa una única vez.
  - No es práctico porque cifra bit a bit y por tanto sería extremadamente lento.
8. En un ataque de fuerza bruta:
- **Para tener éxito, en media se deben probar la mitad de las claves posibles.**
  - Si la clave es de 128 bits, el ataque se puede realizar en menos de una hora con un ordenador convencional.
  - La ruptura de una clave de 26 caracteres es factible en unos pocos años utilizando procesamiento paralelo.
  - Incluso si la clave es de 32 bits, resulta imposible llevar a cabo un ataque de fuerza bruta.

---

9. En lo que se refiere a la teoría de la información:

- **Un cifrador incondicionalmente seguro no filtra información al criptoanalista, incluso si el criptograma es muy largo.**
- Un cifrador matemáticamente vulnerable siempre filtra al criptoanalista la misma cantidad de información.
- Mide cómo de interesante es un mensaje para un criptoanalista.
- Mide la cantidad de información que puede procesar un cifrador en una misma operación criptográfica, considerando un equipo computacional estándar.

10. Acerca de la entropía:

- Si una fuente produce cuatro mensajes, la entropía máxima es 4.
- Es nula si todos los mensajes producidos por una fuente son equiprobables.
- Puede ser positiva o negativa.
- **Mide la incertidumbre que tiene un observador al aparecer un mensaje m.**

11. Sea una fuente M de mensajes que produce cuatro mensajes ( $m_1$ ,  $m_2$ ,  $m_3$  y  $m_4$ ), siendo la probabilidad p de cada uno:  $p(m_1) = p(m_3) = 40\%$ ,  $p(m_2) = 15\%$ ,  $p(m_4) = 5\%$ . La entropía de M es...:

- 0
- **2,73**
- -0,51
- 0,51

12. La aleatoriedad de una secuencia...

- Se puede confirmar utilizando una serie de pruebas.
- Si tiene una racha muy larga de valores consecutivos, se puede afirmar que no es aleatoria.
- **Impide que se pueda inferir una subsecuencia a la vista de otras.**
- Se puede producir una secuencia aleatoria utilizando un algoritmo de ordenador.

13. Los problemas computacionales pueden ser clasificados en...

- Tratables o Intratables, en función de si tienen o no un algoritmo para su resolución.
- Decidibles o Indecidibles, según el tiempo que se tarde en resolverlo.
- Deterministas o aleatorios, en función de si su solución es siempre la misma o varía con el tiempo.
- **Clase P o NP, según si el tiempo necesario para resolverlos crece polinomialmente o no, respectivamente, en función del tamaño del problema.**