



## “Criptosistemas simétricos: Flujo”

### Test de autoevaluación

---

Seleccione la respuesta correcta.

1. Los cifradores de flujo...
  - Dividen el mensaje en fragmentos relativamente grandes y operan cada uno de forma independiente.
  - Necesitan que emisor y receptor se sincronicen externamente
  - Requieren una serie cifrante, idealmente infinita y aleatoria.
  - En la práctica, ambos comunicantes comparten una clave tan larga como el mensaje.
  
2. Los postulados de Golomb...
  - Establecen propiedades deseables que una serie cifrante debería cumplir.
  - Establecen que el secreto del cifrador debe residir en el secreto de la clave.
  - Miden la calidad (aleatoriedad) de la salida de un cifrador de flujo.
  - Establecen, entre otras cosas, que no puede haber un número grande de símbolos iguales consecutivos.
  
3. ¿Para qué sirve la complejidad lineal?
  - Para medir la impredecibilidad de una serie cifrante.
  - Para determinar la velocidad de un LFSR.
  - Para calcular el periodo de una serie cifrante.
  - Para estimar la longitud de clave necesaria para alcanzar un determinado nivel de seguridad.
  
4. Un registro de desplazamiento con realimentación lineal (LFSR, por sus siglas en inglés),
  - Permite cifrar un valor, o semilla, utilizando una combinación de XOR determinada por un polinomio.
  - Permite crear una secuencia (por ejemplo, una serie cifrante) a partir de un valor inicial.
  - Permite crear una serie binaria cifrante no periódica.
  - Son sistemas altamente seguros debido a su alta complejidad lineal.

- 
5. Al combinar varios LFSR...
- Se consigue un periodo exponencialmente mayor para la serie cifrante.
  - La serie cifrante se produce de manera más rápida y segura.
  - Se asegura el cumplimiento de los postulados de Golomb
  - Se consigue aumentar la complejidad lineal del sistema de generación de una serie cifrante.
6. ¿Cuántas celdas tendrá un LFSR descrito por el polinomio  $p(x) = x^5 + x^3 + x^2 + 1$ ? ¿Y cuántas entradas tendrá su XOR?
- 5 celdas, 3 entradas
  - 4 celdas, 4 entradas
  - 4 celdas, 3 entradas
  - 3 celdas, 3 entradas
7. En comparación con los cifradores de bloque, los cifradores de flujo...
- Son más adecuados para los sistemas basados en *streaming*.
  - Son más seguros.
  - Son, en media, más lentos.
  - Causan una mayor incertidumbre al criptoanalista pues tienen mayor difusión de la información.
8. Si se reutiliza la clave en varias operaciones de un cifrador de flujo...
- Si se conoce el texto en claro, se podría obtener la clave de cifrado.
  - Se puede descifrar cualquier mensaje si se obtienen dos o más criptogramas.
  - La clave inmediatamente queda al descubierto.
  - Se consigue mayor velocidad sin merma de las garantías de confidencialidad.
9. ¿Cuál de las siguientes afirmaciones sobre RC4 es cierta?
- Utiliza una matriz bidimensional para guardar el estado interno.
  - Es rápido incluso en sus implementaciones software.
  - Utiliza una clave fija de 255 bytes.
  - Actualmente se considera irrompible dada la baja linealidad de su resultado.
10. ¿Utiliza alguna clave el algoritmo RC4?
- No, sólo una matriz de estado interna.
  - No, por eso es tan rápido.
  - Sí, para reordenar el estado interno.
  - Sí, para generar una serie cifrante con un LFSR.