Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Criptosistemas simétricos: Bloque"

Test de autoevaluación

Seleccione la respuesta correcta.

1. En los modos de cifrado de bloque:
   - En todos los modos de cifrado de bloque cada bloque se cifra separadamente de los demás sin dependencia de otros bloques.
   - En el modo ECB cada bloque cifrado depende del bloque cifrado anteriormente.
   - En el modo CBC tanto el cifrado como el descifrado dependen del bloque cifrado anteriormente.
   - En el modo CFB un error en un bit del criptograma afectará sólo a un bloque del texto en claro recuperado.

2. En un cifrador de bloque CFB, el texto en claro se dispone en bloques de m = 16 y un cifrador que maneja bloques de 48 bits. Si un bloque de código se recibe mal en el receptor.
   - Afecta a 16 bloques del texto en claro descifrado
   - Afecta a 3 bloques del texto en claro descifrado
   - Afecta a 4 bloques del texto en claro descifrado.
   - Afecta a 2 bloques del texto en claro descifrado.

3. En los métodos de cifrado de bloque:
   - En el método CBC el tamaño del bloque de cifrado y del registro son iguales.
   - En el método CFB el tamaño del bloque de cifrado y del registro son diferentes.
   - En cualquiera de los métodos, el tamaño del bloque del mensaje y de cifrado son iguales.
   - Todas las respuestas anteriores son correctas.

4. En los cifradores de bloque:
   - Un cifrado con DES en modo CBC significa que tras cifrar cada bloque M, el criptograma C obtenido opera "or-exclusivo" de nuevo con M y a su resultado se le vuelve a aplicar DES.
   - Entre las razones para adoptar un nuevo estándar americano, el AES, se hallan las enormes vulnerabilidades encontradas a su antecesor, el DES.

- Recibido un mensaje cifrado, C, mediante AES en modo ECB, el receptor puede, si así lo desea, descifrar los bloques primero y último, sin necesidad de descifrar los bloques intermedios.
- En el método CBC el tamaño del bloque de cifrado y del registro son distintos.

5. Sobre los modos de operación de los cifrados de bloque
   - Recibido un mensaje cifrado en varios bloques mediante AES en modo CBC (cipher-block chaining), el receptor no puede comenzar el descifrado hasta que no se han recibido todos los bloques del criptograma.
   - Recibido un mensaje cifrado en varios bloques mediante AES en modo CBC (cipher-block chaining), el receptor no puede descifrar un bloque sin descifrar previamente los bloques anteriores.
   - Recibido un mensaje cifrado en varios bloques mediante AES en modo ECB (electronic code book), el receptor no puede descifrar un bloque sin descifrar previamente los bloques anteriores.
   - Ninguna de las respuestas anteriores es correcta

6. En DES
   - DES maneja una clave externa de 64 bits, a partir de la cuál se generan 16 claves internas de 64 bits cada una.
   - DES maneja una clave externa de 64 bits, siendo el número total de claves 264.
   - Una de las desventajas del DES es el alto número de claves débiles que presenta.
   - DES maneja bloques de texto en claro de 64 bits, claves externas de 64 bits y claves internas de 48 bits.

7. Indique la afirmación correcta.
   - Si A y B comparten dos claves secretas, K1 y K2, un tercero, C, que conozca una de las claves, pongamos que K1, puede descifrar cualquiera de los cifrados que se intercambien A y B, ya que al tratarse de un criptosistema simétrico puede deducir K2 sabiendo K1.
   - Por un canal inseguro es posible el intercambio de claves secretas.
   - La razón por la que A y B acuden a una AC como tercero de confianza es para que, mediante certificados, A y B tengan a buen recaudo sus claves públicas, sólo conocidas por la AC.
   - Entre las razones para adoptar un nuevo estándar americano, el AES, se hallan las enormes vulnerabilidades encontradas a su antecesor, el DES