



## “Distribución y establecimiento de clave”

### Test de autoevaluación

Seleccione la respuesta correcta.

1. El concepto de envoltura de clave (*key wrapping*) implica:
  - Cifrar una clave simétrica con una clave asimétrica pública.
  - Cifrar una clave simétrica con otra clave simétrica**
  - Cifrar una clave asimétrica privada con una clave asimétrica pública.
  - Cifrar una clave asimétrica pública con una clave asimétrica privada.
2. El concepto de encapsulación de clave (*key encapsulation*) implica:
  - Cifrar una clave simétrica con una clave asimétrica pública.**
  - Cifrar una clave simétrica con otra clave simétrica
  - Cifrar una clave asimétrica privada con una clave asimétrica privada.
  - Cifrar una clave asimétrica pública con una clave simétrica.
3. La mejor opción en cuanto a rapidez y facilidad de gestión de las claves es:
  - Cifrado simétrico.
  - Cifrado asimétrico.
  - Cifrado híbrido.**
  - Cifrado jerárquico.
4. Asuma que B posee la siguiente clave pública RSA:  $(e,n)=(5,69)$ . A cifra para B el mensaje  $M=218$  y clave  $K=57$ , utilizando un mecanismo de encapsulación de clave basado en el algoritmo de cifrado simétrico  $E(K, M) = M + K \pmod{256}$ . Elija de entre las siguientes opciones cuál es el mensaje cifrado que recibe B:
  - 5.
  - (223,17).
  - 19.
  - (19,51)**

- 
5. Tras ejecutar dos interlocutores el algoritmo de Diffie-Hellman:
- **Ambos han convenido una clave simétrica a través de un canal público**
  - Uno ha cifrado un mensaje para el otro con criptografía simétrica y el otro lo ha descifrado.
  - Uno ha cifrado un mensaje para el otro con criptografía asimétrica y el otro lo ha descifrado.
  - Ambos han convenido una clave asimétrica a través de un canal público.
6. A y B ejecutan el algoritmo de Diffie-Hellman con los siguientes parámetros:  $g=2$ ,  $p=19$ ,  $x_A=7$ ,  $x_B=6$ . EL resultado del algoritmo es:
- B obtiene como resultado final  $Y_B=12$
  - A envía a B el mensaje cifrado  $Y_A = 14$ , y B lo descifra como  $M=7$ .
  - **A obtiene como resultado final  $K=7$**
  - B envía a A el mensaje en claro  $M=2$ , y A lo cifra con la clave  $x_B=6$ .