



## “Códigos de autenticación de mensajes”

### Test de autoevaluación

Seleccione la respuesta correcta.

1. ¿Qué diferencia un código de autenticación del mensaje de una función resumen?
  - ☐ El tamaño de los mensajes (pueden ser más grandes en las funciones resumen).
  - ☒ **El uso de una clave secreta.**
  - ☐ Nada, son lo mismo.
  - ☐ La aleatoriedad de la salida (los códigos de autenticación son más aleatorios).
  
2. ¿En qué se parecen los códigos de autenticación del mensaje y las funciones resumen?
  - ☐ Las funciones resumen son no invertibles y las MAC pueden no serlo.
  - ☐ Ambas pueden sufrir colisiones.
  - ☐ La probabilidad de encontrar dos mensajes que ofrezcan el mismo resultado es  $2^{-n}$  en ambos casos
  - ☒ **Todas las anteriores son ciertas.**
  
3. ¿Qué propiedad de seguridad permiten verificar los códigos de autenticación del mensaje?
  - ☐ Confidencialidad.
  - ☐ Integridad.
  - ☐ Disponibilidad.
  - ☒ **No repudio.**
  
4. La complejidad de un ataque de fuerza bruta a una función MAC vendrá determinado por:
  - ☒ **El mínimo entre el tamaño del espacio de claves y el de mensajes.**
  - ☐ El máximo entre el tamaño del espacio de claves y el de mensajes.
  - ☐ El tamaño de la salida de la función MAC.
  - ☐ El tamaño del espacio de mensajes, exclusivamente.

- 
5. Para diseñar una función MAC se puede optar por:
- Utilizar como base una función resumen, añadiendo bits al mensaje basados en la clave.
  - Utilizar un cifrador simétrico.
  - Realizar un diseño nuevo, independiente de cualquier otro mecanismo criptográfico.
  - **Todas las anteriores son ciertas.**