



## “Esquemas de firma digital”

### Test de autoevaluación

---

Seleccione la respuesta correcta.

1. Los esquemas de firma digital se basan en:
  - La criptosistemas mixtos
  - La criptografía de clave simétrica
  - La criptosistemas híbridos
  - La criptografía de clave asimétrica
  
2. La firma digital proporciona las siguientes propiedades:
  - Integridad del mensaje, y no repudio y confidencialidad del firmante.
  - Confidencialidad y autenticación del firmante, e integridad del mensaje.
  - Autenticación y no repudio del firmante, e integridad del mensaje.
  - Autenticación del firmante, y no repudio y confidencialidad del mensaje.
  
3. En los esquemas de firma digital:
  - El firmante usa su clave pública para firmar.
  - El firmante usa su clave privada para firmar.
  - El firmante usa la clave pública del destinatario para firmar.
  - El firmante usa la clave privada del destinatario para firmar.
  
4. Si un esquema de firma es determinista y con apéndice:
  - Para mensajes iguales, la firma es la misma, y ésta se adjunta separada del mensaje.
  - Para mensajes iguales, la firma es distinta, y ésta se adjunta separada del mensaje
  - Para mensajes iguales, la firma es la misma, y ésta está integrada en el propio mensaje.
  - Para mensajes iguales, la firma es distinta, y ésta está integrada en el propio mensaje.

- 
5. Suponga que A está firmando un mensaje con RSA combinado con una función resumen. Sabiendo que el resumen del mensaje es  $H(M)=6$ , y que la clave pública de A es  $(e,n)=(13,77)$ , indique cuál es la firma que calcula A:
- 12.
  - 74.
  - 41.
  - 37.
6. A recibe de B el siguiente mensaje firmado con el algoritmo El Gamal:  $(\{m_i\}; r,s)=(\{9,10,11,12,8,13,1\}; 5,3)$ . Si los datos públicos de B son  $p=17$ ,  $g=3$ , e  $Y=14$ , y la función resumen aplicada sobre una lista de mensajes se define como  $H(\{m_i\})= \sum_i m_i \text{ mód. } 13$ , elija la respuesta correcta:
- La firma digital no es válida  $V_1 \neq V_2=4$ .
  - La firma digital es válida,  $V_1=V_2=4$ .
  - Ninguna de las anteriores es correcta.
  - Todas las anteriores son correctas.