

**Pregunta 1****3 / 3 puntos**

A envía a B lo siguiente:  $M, \text{HMAC}(K_{AB}, M)$ .  $\text{HMAC}(K_{AB}, M)$  es el código calculado sobre  $M$  con la llave simétrica compartida  $K_{AB}$ . Esta construcción ofrece:

- ✓☒ Autenticación del mensaje
- ✓☐ Confidencialidad del mensaje
- ✓☐ No-repudio del mensaje
- ✓☒ Integridad de mensaje

**Pregunta 2****0 / 2 puntos**

Empareje la problemática con la solución

- |                               |                 |
|-------------------------------|-----------------|
| ✗ <u>2</u> (3) Firma digital  | 1. Espionaje    |
| ✓ <u>1</u> Cifrado            | 2. Adulteración |
| ✗ <u>3</u> (2) Código de hash | 3. Repudio      |