# Organización de Datos – Curso Servetto

*Evaluación Módulo Criptografía, 7 de Julio de 2010*

1. Explicar el handshake en TLS. Asumir que el cliente y el servidor tienen una clave pública avalada por un certificado digital.

2. Determine si el esquema de firma digital asimétrica utilizando resumen de mensaje garantiza el no repudio. ¿Y la confidencialidad? Explique por qué. Enumere las características que debe tener una función de resumen para ser útil en una firma digital.

3. ¿Qué es un modo de encriptación? Compare los siguientes pares de modos, enunciando las ventajas de cada uno con respecto al otro:

    a. Electronic Code Book (ECB) vs. Cipher-block chaining (CBC)
    b. Output feedback (OFB) vs. Cipher-block chaining (CBC)