Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía, 21 de Diciembre de 2009

1. 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.

2. ¿Qué significa que un método tiene estructura de grupo? ¿El método TDES tiene esta estructura? Enumere los pasos que sigue dicho método, y explique por qué es compatible con el método DES.

3. Enumere los pasos para generar las claves pública y privada del método RSA. ¿Cómo se desencripta un mensaje con este método? ¿Por qué, para este método, es computacionalmente inviable calcular la clave privada a partir de la clave pública?

4. Responder a las siguientes cuestiones:
    a. ¿Qué problema es resuelto por los certificados digitales?
    b. ¿Qué información básica debe contener un certificado digital?
    c. ¿Cómo puede un usuario asegurarse de que un certificado digital es verdadero?
    d. ¿Qué pasa si cuando dos usuarios quieren iniciar una comunicación autenticada por certificados digitales, el servidor de la autoridad certificante está caído?