Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 09 de Febrero de 2005

Resolver los ejercicios de criptografía y archivos multimediales en hojas separadas.

Criptografía

1. Diseñe un protocolo criptográfico para la celebración de contratos de locación de forma **remota**. Los actores son: el locador (dueño), el locatario (inquilino) y un escribano público que certifica.

2. Juan Carlos desea encriptar el mensaje M=ingenieria antes de enviárselo a José. Para ello utiliza el algoritmo RSA con el siguiente conjunto de claves: (d=1019) (e=79,n=3337). Se pide: encriptar el mensaje anterior (sin realizar las cuentas) e indicar como José procedería para desencriptarlo.

3. ¿Si una Autoridad de Certificación es la tercera parte de confianza, ¿actúa de forma activa o pasiva en la comunicación? Explicar.

Archivos Multimediales

4. ¿Qué diferencia existe entre una compresión de imágenes de tipo PNG (suponga que el algoritmo de este compresor es el mismo que se vio en la materia) y una JPEG? Indique características de sus algoritmos.

5. Mencione y describa qué tipos de metadatos se encuentran comúnmente en los archivos gráficos.