Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 15 de Diciembre de 2004

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

Criptografía

1. ¿Por que decimos que un sistema asimétrico la gestión de claves es mucho mejor que en un sistema simétrico?

2. Muestre y explique mediante un ejemplo como se garantiza el no repudio en una firma digital asimétrica o pública.

3. Responder Verdadero o Falso, justificando en ambos casos la respuesta:
    a. El método de Vigénere utiliza un modo ECB (Electronic Code Book) para encriptar los bloques.
    b. Se puede demostrar matemáticamente que el método One Time Pad se puede romper mediante un criptoanálisis diferencial en un tiempo razonable.
    c. La criptografía asimétrica deja obsoleta a la criptografía simétrica

Archivos Multimediales

4. ¿Qué ventajas y desventajas tiene la Modulación Delta (Variación de DPCM) respecto del DPCM estándar?

5. ¿Por qué se pasa una imagen al dominio de frecuencia en la compactación?