Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 12 de Julio de 2005

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

Criptografía

1. Muestre y explique mediante un ejemplo como se garantiza la integridad de los datos en una firma digital privada o simétrica

2. Encriptar el mensaje M=computadora con el algoritmo de Merkle-Hellman (knapsack). Para ello utilizar el siguiente subconjunto {1,5,9,21,37}. Indicar la(s) o las clave(s) involucradas.

3. Responder Verdadero o Falso, justificando en ambos casos la respuesta:
   a. La seguridad de los criptosistemas de clave pública reside íntegramente en la dificultad computacional de problemas numéricos y algebraicos.
   b. La criptografía asimétrica es más eficiente que la simétrica
   c. Una condición suficiente para que un criptosistema sea seguro es que el algoritmo de encriptación sea extremadamente complejo o de alto nivel de seguridad.

Archivos Multimediales

4. ¿Qué ventajas/desventajas tiene la transformación DCT en dos dimensiones contra la lineal en una digitalización de imágenes?

5. ¿Si tuviera que digitalizar un archivo vectorial (se conforma de figuras geométricas escaladas), cómo lo haría?