

Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 02 de Marzo de 2005

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

Criptografía

1. Encriptar el mensaje M=facultad con el algoritmo de Merkle-Hellman. Para ello utilizar el siguiente subconjunto {2,3,7,13,26,55}. Indicar la(s) o las clave(s) involucradas.
2. Explique el esquema de encriptación que utiliza PGP.
3. Muestre y explique mediante un ejemplo como se garantiza la integridad de los datos en una firma digital privada o simétrica.

Archivos Multimediales

4. *Discretización Vectorial*: ¿qué es? ¿cómo se aplicaría si tengo una imagen con dos círculos, uno pequeño y otro grande?
5. *Metadatos*: ¿qué tipo de metadatos serían los generados por los TAG de XML? Obs.: Sólo para el caso general. Ejemplo: "<Padre>" interesa qué función de metadato tiene el TAG para cualquier documento, no que sea padre de alguien.