Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 08 de Marzo de 2006

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

Criptografía

> *Nota: Por protocolo criptográfico se entiende conjunto finito de pasos que deben realizar las partes involucradas para llevar a cabo un objetivo. El mismo debe ser de previo conocimiento de las partes participantes. Además debe ser completo (no existen situaciones que no abarque) y no ambiguo (para cada situación un único resultado)*

1. ¿Qué ocurre si la clave de una autoridad certificante se pierde o se encuentra comprometida? ¿Qué ocurre si una persona pierde su clave privada?
2. ¿Por qué en un sistema simétrico se obtiene la confidencialidad y la integridad al mismo tiempo protegiendo la clave?
3. Describir el proceso de desencriptación con PGP
4. ¿Explique los "pasos" que existen en una firma digital? Comente similitudes con la firma manuscrita.

Archivos Multimediales

5.