Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 12 de Julio 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. Alejandro y Lucas, situados a distancia, quieren decidir algo a sorteo, pero no se tienen confianza entre sí. Uno de los dos lanza una moneda y el otro elige. Un tema importante es que, la primera persona que proporciona la información queda en desventaja frente a la intención de trampear de la otra. Se pide diseñar un protocolo criptográfico, que cumpla con la especificación mencionada anteriormente.

   Observación: El protocolo debe ser no arbitrado.

2. Describir el proceso de desencriptación con PGP
3. ¿Se puede afirmar que la criptografía asimétrica es la sustituta de la simétrica? ¿Por qué? Justificar adecuadamente.

Archivos Multimediales

4.