Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 16 de Agosto de 2005

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. Lucas y Alejandro desean jugar al ajedrez de **forma remota**. El problema es que ambos quieren jugar con las piezas blancas. Ambos acordaron decidir la cuestión jugando al piedra, papel o tijera. Para ello elegirán cada uno una de las tres opciones posibles y quien gane elegirá color de pieza.
   Se pide diseñar un protocolo criptográfico para determinar quien comenzará la partida. Una condición necesaria que se debe cumplir es que ninguno de los dos pueda saber el resultado del otro de antemano. Es decir, se deben enterar de lo que eligió la otra parte de forma "simultanea" (o paralela).

2. Supóngase la siguiente situación: Un cliente desea logearse en un servidor. ¿Que consideraciones habría que tener en cuenta para que ningún intruso pueda hacerse pasar por el cliente y conectarse al servidor en cualquier instante?. Diseñe el protocolo.

3. a. Lucas y Alejandro decidieron, de forma conjunta, utilizar criptografía asimétrica para sus comunicaciones. Pero en el momento del intercambio de claves, una tercera persona intercepto las claves (ataque por intermediario). ¿Cómo podrían darse cuenta de tal situación?
   b. Diseñe un protocolo de intercambio de claves que permita detecta el problema presentado en el ítem anterior.

4. ¿Cuanto tiempo llevaría romper por fuerza bruta el algoritmo DES?

Archivos Multimediales – 2do Cuatrimestre 2004

5. ¿Por qué no aplicaría una compresión FRACTAL a un archivo de Texto?

6. Mencionar y describir los tipos de Metadatos que contiene un archivo MP3 (como ser nombre de autor, de disco, fecha de edición, nombre del tema. duración, calidad, etc).

Archivos Multimediales – 1er Cuatrimestre 2005

5. Describir las características del algoritmo MPEG que hacen a la compresión (o ahorro de espacio en almacenamiento) de una película.

6. ¿Por qué no aplicaría una compresión JPEG a un archivo de Texto?