Organización de Datos – Curso Servetto

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

Criptografía

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).

   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)

2. ¿Cuál es la principal debilidad de los métodos de cifrados por sustitución monoalfabéticos? ¿Cómo los criptoanalizaría de manera no trivial?

3. Desencriptar el criptograma dado, sabiendo que se utilizo para su encriptación el algoritmo de Merkle-Hellman (Knapsack). Las claves involucrados son:
   - clave pública = {1864,872,177,1921,1422} + módulo = 2003
   - clave privada = {3,10,25,45,99} + módulo = 2003 + coeficiente multiplicador = 317

   Criptograma = 1025125412

Archivos Multimediales

4. Hernán quiere ver en su laptop un partido de la Davis. Si la transmisión es en vivo y en directo (según estándar MPEG). ¿Qué es lo más importante (puntos) a tener en cuenta para permitir que disfrute del partido sin cortes?

5. ¿Qué partes de una imagen JPEG tienen una mayor/menor nivel de compresión?