Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 14 de Diciembre 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. Explique como se puede obtener integridad de los datos en una firma digital simétrica.

2. Arturo esta diseñando un protocolo para la trasmisión de video por Internet. Un requerimiento funcional que se debe garantizar es la confidencialidad de la señal. En otras palabras, solo las personas abonadas deben poder ver la transmisión. Para ello, Arturo opto por utilizar criptografía simétrica. Además debe trasmitirse comprimida, de manera tal, de disminuir el trafico en la red. Se pide:
    a. Diseñar el protocolo. Desde que una persona se suscribe al servicio hasta que puede hacer uso del mismo.
    b. ¿Qué supone que es lo más conveniente: comprimir la señal y luego cifrarla, al revés o indistinto? Justificar adecuadamente.

3. Explique que es un cifrado por producto. Además indique y justifique si los siguientes métodos corresponden a dicha familia:
    a. DES
    b. RSA
    c. Vigenere

Archivos Multimediales

4. ¿Cómo sería la organización de un archivo de gráficos vectoriales? Describa la estructura lógica y las razones por las que debería ser así.

5. ¿Qué solución ofrece MPEG para hacer P-Frame (predictores) de una imágen que se mueve pero tiene partes que, en otro lugar de la pantalla, se ven iguales? Explique y proponga otra forma.