Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 22 de Diciembre de 2004

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

Criptografía

1. ¿Por qué cree que un escenario de integridad en la que hay siempre una tercera parte de confianza **activa** no sería adecuado en Internet?

2. ¿Cuál es la principal debilidad de los métodos de cifrados por sustitución monoalfabéticos? ¿Cómo los criptoanalizaría?

3. Con el crifrado de Hill obtenga el criptograma para el siguiente mensaje plano: “hola que tan”, sabiendo que el alfabeto esta formado por letras (sin la “ñ”) más el símbolo de espacio. Las posibles claves a utilizar son: ceca, coca, caco, coco. ¿Cual utilizaría y por qué?

4. ¿El algoritmo TDES posee estructura de grupo? ¿Por qué? ¿Tiene compatibilidad con su antecesor? ¿Qué tamaño de clave utiliza? Justifique sus respuestas adecuadamente.

Archivos Multimediales

5. ¿Si se tiene una imagen de 200 por 200 pixels con una definición de 100ppi y otro de 1000 por 1000, cuál tiene mejor relación de compresión JPEG? Suponga que las demás características son idénticas, misma imagen.

6. ¿Qué utilidad tiene guardar imágenes en meta-archivos?