Organización de Datos – Curso Servetto

Evaluación Criptografía-Multimediales, 12 de Febrero del 2007

Resolver los ejercicios de Criptografía y Multimediales en hoja separadas.

Criptografía

2006 2C

1. Explique cuales son las características de un algoritmo de clave pública. Compare con uno de clave privada.

2. Responder Verdadero o Falso, justificando en ambos casos la respuesta:
    a. Si una clave tiene caracteres repetidos es imposible utilizarla en el método de transposición por columnas.
    b. El cifrado por sustitución reemplaza símbolos del mensaje plano por otros símbolos pertenecientes al mismo alfabeto.
    c. Una condición suficiente para que un criptosistema sea seguro es que el algoritmo de encriptación sea extremadamente complejo o de alto nivel de seguridad.

Cuatrimestres anteriores

1. Muestre y explique mediante un ejemplo como se garantiza la integridad de los datos en una firma digital pública o asimétrica.

2. El emisor se quiere comunicar con el receptor, utilizando criptografía de clave pública. Para el ello, el emisor establece una conexión con alguien que espera sea el receptor. Le pide su clase pública y él se la envía en texto plano junto con un certificado digital firmado por una autoridad de certificación (AC). ¿Qué pasos debe el emisor realizar para verificar que esta hablando con el receptor deseado. Suponer que al receptor no le importa con quién está hablando.

Multimediales

1. Describa las consideraciones a tomar en cuenta para almacenar películas en un servidor de vídeo. Tenga en cuenta que este equipo provee muchas películas.

2. Describa los pasos de un proceso de digitalización JPEG (el algoritmo).