Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 02 de Agosto de 2006

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. Si una Autoridad de Certificación es la tercera parte de confianza, ¿actúa de forma activa o pasiva en la comunicación? Explicar de forma concisa y clara.

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.

3. Arturo desea hacer una donación a una Asociación sin fines de lucro. Para ello le envía digitalmente un cheque del Banco del cual es cliente. Se pide mostrar y explicar claramente el protocolo diseñado (esquema, mensajes enviados, claves a utilizar y modo de uso) para cada una de las siguientes interacciones:
   a. Arturo le solicita el cheque al Banco.
   b. Arturo realiza la donación con ese cheque.
   c. La Asociación cobra el cheque en el Banco.

   Observaciones:
   - Tanto Arturo como la Asociación son clientes del Banco.
   - Todas las interacciones se realizan digitalmente, es decir, sin contacto físico y sobre un **canal inseguro**.
   - El protocolo debe ser **no arbitrado**.

Archivos Multimediales

4. Describa algunas soluciones (buenas) para el problema de la organización del espacio en disco para reproducir Videos.
5. Describa los datos necesarios para permitir el avance rápido y el retroceso en un CD de música. ¿Debería cambiar algo para lograr lo mismo en un video MPEG? Explique sus respuestas.