Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 16 de Agosto de 2006

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

Criptografía

1. Suponga que se esta utilizando un esquema de firma asimétrico utilizando resumen del mensaje (digest). Explicar que ocurre en las siguientes situaciones:
   a. Un intruso reemplaza el mensaje de emisor. ¿El receptor puede detectarlo?
   b. Un intruso reemplaza tanto el mensaje como la firma del emisor. ¿El receptor puede detectarlo?

2. Utilizar el algoritmo RSA para firmar digitalmente sabiendo p, q, phi(n), n, e y d, el siguiente documento: AGOSTO. Responder detalladamente y algebraicamente los pasos necesarios.

3. Dado el siguiente algoritmo de cifrado:

   - Dividir la fuente en bloques de longitud b
   - Para cada bloque, se realiza la siguiente transformación

   $S_i \rightarrow S_{b-i}$, donde $i = \{0,\ldots, \text{Piso } (b/2) \}$

   S_i = i-nésimo símbolo del bloque

   Se pide:
   a. Determinar si se trata de un cifrado por sustitución o transposición.
   b. Clasificar el método según las categorías vistas en clase, respondiendo con la más especifica posible.

Archivos Multimediales

4. ¿Cómo puede guardar un archivo de vídeo MPEG para que se reproduzcan todos los tipos de “frames” de una pasada? Explique la respuesta.

5. ¿Qué condiciones deben tenerse en cuenta para permitir una reproducción simultánea a dos observadores independientes?