Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 01 de Julio de 2005

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

Criptografía

1. Alejandro y Lucas decidieron utilizar el cifrado de Vigénere como método de encriptación para evitar que sus mensajes puedan ser interpretados por terceros. Previamente acordaron que la clave a utilizar por Alejandro es ALEEE y la clave de Lucas es NULL.
   Suponga que Alejandro le envía a Lucas el mensaje INGENIERIA utilizando el método de encriptación mencionado anteriormente. Para ello utiliza un alfabeto que contiene los siguientes símbolos: GARNEILU. Se pide:
   a. Mostrar todo lo que le envía Alejandro a Lucas
   b. Indicar qué tipo de cifrado es el método del punto anterior. Justifique sobre su respuesta del ítem anterior.

2. 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 emisor puede detectarlo?
   b. Un intruso reemplaza tanto el mensaje como la firma del emisor. ¿El emisor puede detectarlo?

3. 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 realizar el emisor para verificar que esta hablando con el receptor deseado?. Suponer que a el receptor no le importa con quién está hablando.

Archivos Multimediales

4.