Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales , 30 de Junio de 2006

Criptografia

1. Explique qué significa que en un sistema de cifra asimétrica se obtengan la confidencialidad y la integridad por separado.

2. Si se desea enviar un mensaje garantizando confidencialidad y reduciendo su tamaño. ¿Qué es lo más conveniente: comprimir el mensaje y luego cifrarlo, al revés o indistinto? Justificar adecuadamente

3. Alejandro desea encriptar el mensaje M=psapeugeot antes de enviárselo a Lucas. Para ello utiliza el algoritmo RSA con el siguiente conjunto de claves: (d=1019) (e=79,n=3337). Se pide: encriptar el mensaje anterior (sin realizar las cuentas) e indicar como Lucas procedería para desencriptarlo.

Archivos Multimediales