# Organización de Datos – Curso Servetto

*Evaluación Módulo Criptografía-Archivos Multimediales , 19 de Julio de 2005*

*Criptografía*

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

2. Diseñe un protocolo criptográfico para el voto electrónico de **forma remota**. Indique todas las hipótesis que utilizo.

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*

4. Arturo quiere ver una película MPEG y arrancar en un cuadro en particular pero el reproductor lo posiciona uno antes o uno después, ¿por qué es esto?

5. ¿Qué parte del algoritmo de digitalización JPEG comprime el archivo?