Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía, 14 de Julio de 2010

1.- Explicar el esquema de encriptación y comunicación utilizado por PGP. Explicar el concepto de red de confianza y su relación con PGP.

2.- Enumerar los pasos para generar las claves pública y privada del método RSA e ilustrar con un ejemplo. Describir cómo se encripta un mensaje con este método e ilustrar con un ejemplo. ¿Por qué, para este método, es computacionalmente inviable calcular la clave privada a partir de la clave pública?

3.- Describir un ataque meet-in-the-middle. ¿Por qué el método TDES no es vulnerable a este ataque? ¿Este método tiene estructura de grupo? ¿Por qué se dice que es compatible con DES?