Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía, 8 de Febrero de 2010

1. Para cada uno de los métodos enumerados a continuación indicar (no es necesario justificar) si pueden romperse mediante la resolución de un problema matemático considerado como computacionalmente intratable. Para el o los métodos que tengan respuesta afirmativa, explicar (o mostrar con un ejemplo) cómo la resolución de ese problema matemático haría trivial desencriptar un criptograma cifrado con ese método.
    a. RSA
    b. Knapsack
    c. TDES
2. Mostrar un ejemplo de encriptación y desencriptación utilizando cifrado de Hill con bloque de tamaño 2. Indique si la clave debe cumplir con algún criterio. ¿Por qué se dice que es un cifrado poligráfico y cuál es la diferencia con un cifrado polialfabético?
3. Un ataque de denegación de servicio (DoS) sobre un servidor consiste en saturarlo con más flujo de datos del que puede manejar, con el objetivo de que se sobrecargue y no pueda seguir prestando servicios. Analice la robustez de los esquemas de firma mencionados a continuación ante este tipo de ataques:
    a. Firma digital de clave privada
    b. Firma digital de clave pública con resumen de mensaje y certificados digitales