Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía, 26 de Julio de 2010

1.- Alice le quiere enviar a Bob un mensaje de tres bytes, encriptado con RSA. El resultado de la encriptación es: 0xC7 0xF3 0xB2. El tamaño de bloque es un byte. Claves públicas:
Alice: n=1763, e=21 Bob: n=629, e=13 (números en base 10)
Eva intercepta el mensaje e intenta decodificarlo por fuerza bruta, aprovechando que la longitud elegida para la clave es muy corta. ¿Cuál es el mensaje descifrado por Eva?

2.- Describa, para SSH, los pasos del intercambio de mensajes al establecer una conexión segura y al autenticar al cliente con clave pública. ¿Este intercambio incluye una autenticación de tipo challenge-response?

3.- ¿Qué tipos de criptoanálisis conoce? Describa en cada caso, qué datos o artefactos necesita un atacante para actuar. ¿Qué diferencias tiene con un ataque? ¿Tiene utilidad criptoanalizar un algoritmo asimétrico cuando éste se utiliza para firmar sin buscar confidencialidad?