Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía, 1 de Febrero de 2010

1. Resolver lo siguiente:
    a. Alice le quiere enviar a Bob un mensaje de un byte: 01101010, garantizando la **confidencialidad**. Utilizando el método Merkle-Hellman. Si esto es posible, se pide:
        - Generar una clave privada válida y su clave pública correspondiente
        - Encriptar el mensaje y mostrar el resultado
        - Desencriptar el criptograma y mostrar que se llega al mensaje original

    Es importante indicar quién ejecuta cada paso, y qué clave está involucrada en la encriptación y en la desencriptación. Si no es posible, explicar por qué.

    b. Idem a., pero garantizando **autenticación** en vez de confidencialidad.

2. Responda verdadero o falso, justificando las respuestas:
    a. El cifrado One Time Pad es incondicionalmente seguro, pero durante el intercambio de claves es vulnerable a ataques de intermediario.
    b. Puede existir un criptosistema que garantice el no repudio pero no garantice autenticación.
    c. Un esquema de firma de clave pública puede seguir funcionando (emisor y receptor se pueden seguir comunicando) aunque el servidor de la autoridad certificante quede fuera de servicio.
    d. El modo de operación ECB (Electronic Code Book) se utiliza para eliminar patrones que surgen al encriptar bloques iguales. El problema surge porque sin un sistema que encadene los bloques, dos bloques iguales se encriptarán igual, generando patrones distinguibles por más que el sistema de cifrado sea excelente.
    e. El método de Vigénere tiene estructura de grupo si y sólo si K1 y K2 son tales que la longitud de una es múltiplo de la longitud de la otra.
    f. Con conocer la clave pública y *uno, cualquiera*, de los siguientes valores en un cifrado RSA, alcanza para desencriptar un mensaje: $\varphi(n)$, p, q, d.
    g. El protocolo TLS, siempre requiere que el servidor tenga certificado digital, y en algunos casos requiere que el cliente también.
    h. En el protocolo Kerberos, todos los servidores pueden validar la contraseña de los usuarios.
    i. En un esquema de firma digital simétrica, se puede engañar al Big Brother haciéndose pasar por otra persona, pero el receptor del mensaje descubrirá el engaño en la firma del Big Brother.