CONTROL DE TRANSMISIÓN DE DATOS
24 de mayo de 2002
GRUPO 10

NOTA IMPORTANTE:

- *Un **error conceptual grave** puede anular todo el problema.*

PROBLEMA 1

Sea una función de hash H(M), con una salida de k bits, que se calcula de la siguiente forma:

1. Se añade al final del mensaje el número de ceros necesario para que la longitud el mensaje sea múltiplo de k
2. Se divide el mensaje en n bloques de k bits, $m_i \; 0 \le i \le n-1$
3. H(M) se calcula iterativamente de la siguiente manera:

$$h_0 = m_0$$
$$h_{i+1} = h_i \oplus m_{i+1} \; 0 \le i \le n-2 \text{ (XOR bit a bit)}$$
$$H(M) = h_{n-1}$$

a) Indique las propiedades que debe cumplir una función de hash criptograficamente robusta, y diga cuales de ellas cumple la función propuesta.

b) Sea el mensaje M= 10101010101010101010. Calcule H(M) para k=6.

c) Sea un sistema de RSA en el que todos los usuarios usan e=23. Genere un par de claves RSA con p=11, q=13. Indique cual sería la clave privada y la pública.

d) Firme digitalmente el mensaje del apartado b con el sistema de claves generado en el apartado c y la función de hash propuesta (considere siempre que los bits de menor peso son los de la derecha). Indique que servicios de seguridad ofrece la firma digital.

e) Suponga que es un atacante que quiere modificar un mensaje firmado digitalmente con el sistema anterior. Indique la forma más eficiente de hacerlo y genere un mensaje que genere la misma firma que M.

PROBLEMA 2

Sea una fuente de información sin memoria cuyo alfabeto es de 3 símbolos {A, B, C} con p(A)=0,5; p(B)=p(C)=0,25.

a) Calcule el tiempo mínimo necesario para transmitir 10.000 símbolos de fuente a través de un canal (W= 3 KHz) cuya relación señal a ruido a la entrada del receptor es S/N=7 (en escala lineal).

b) Codifique la secuencia ABACAAA mediante un codificador de Huffman.

c) Codifique la secuencia ABACA mediante un codificador de aritmético.

d) Decodifique la secuencia 0011426 mediante un codificador de LZW, con un diccionario cargado inicialmente con A en la posición 0, B en la 1 y C en la 2.

e) ¿Cuál de las codificaciones anteriores considera más apropiada para la fuente en cuestión? Razone la respuesta.