Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
2 de diciembre de 2003

NOTAS IMPORTANTES:

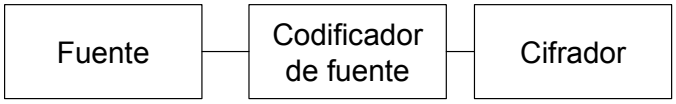
1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
2.- *Se valorará la justificación, discusión y claridad de los resultados.*
3.- ***Los resultados no reflejados en la hoja de resultados anexa no serán tenidos en cuenta.***
4.- *Un **error conceptual grave** puede anular todo el problema.*
5.- *Nótese que **los problemas constan de distintas partes que pueden resolverse por separado**. Se recomienda saltar aquellas partes que no sepan resolverse.*

Problema 1 (20%)

Encuentre, de forma razonada, el tamaño de todos los ciclos posibles en un LFSR con polinomio de conexiones irreducible arbitrario de grado 8.

Problema 2 (50%)

El emisor de un sistema de transmisión de datos está formado por los siguientes módulos:



La **fuente** emite cuatro símbolos independientes con probabilidades 0.55, 0.15, 0.15 y 0.15.
La salida del **codificador de fuente** es binaria.
El **cifrador**, para todo aquel que desconozca la clave de cifrado (atacante), se comporta como un canal binario simétrico con una probabilidad de error de 0.3.
Se define la información media por dígito codificado (**Hdc**) como la información promedio que soporta cada digito de codificación.

Se pide:

a) El valor de Hdc ¿depende de cómo se implemente el codificador de fuente? ¿Por qué? **(1 punto)**

Si el codificador de fuente realiza la codificación:

A:00, B:01, C:10, D:11

b) ¿Cuál es el valor de Hdc para un usuario que conoce la clave de descifrado. **(1.5 puntos)**
c) ¿Cuál es el valor de Hdc para un usuario que desconoce la clave de descifrado. **(2.5 puntos)**

SIGUE DETRÁS

d) Si se transmite la secuencia de fuente A, B, A, D ¿Cuál será la secuencia que debería decodificar un usuario ilegítimo (mayor probabilidad)? **(2 puntos)**

Si el codificador de fuente realiza una codificación de Huffman

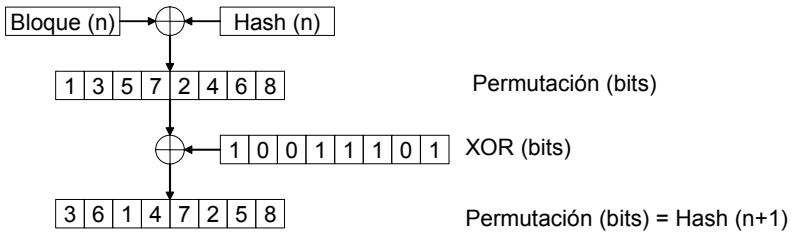
e) ¿Cuál es el valor de Hdc para un usuario que conoce la clave de descifrado. **(1.5 puntos)**

f) La tarea del atacante en este caso ¿es más fácil o más difícil? ¿Por qué? **(1.5 puntos)**

Problema 3 (30%)

Una función de hash de 8 bits se implementa de la siguiente manera:

1. Se rellena con ceros a la derecha (menor peso) hasta formar un múltiplo de 8 bits
2. Se van introduciendo los bloques del mensaje (de izquierda a derecha) según el siguiente algoritmo (Hash(0) = 0)



Se quiere formar un grupo de 16 usuarios en el cual todos usan el mismo número público e=7. Si la autoridad de certificación trabaja con el módulo Nca=13*19=247 calcule el certificado, con la mínima información posible, para el usuario 5 que trabaja módulo N5=11*17=187. (*Nota.- los datos públicos de la autoridad de certificación son conocidos por los 16 usuarios*):