Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

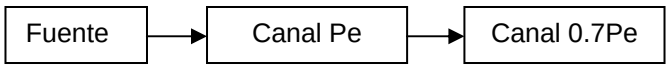
CONTROL DE TRANSMISIÓN DE DATOS
18 de mayo de 2007

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 (40%)

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



La **fuente** emite dos símbolos con probabilidades P(A/A)=0.6 P(B/B)=0.4

Se pide:

a) La memoria de la fuente **(1.5 puntos)**
b) El valor H_F de la entropía de la fuente **(1.5 puntos)**

Si el codificador de fuente realiza la codificación:

A:0 B:1

a la salida del canal se tiene un 54.32% de ceros.

c) ¿Cuál es la capacidad del canal conjunto? **(3 puntos)**
d) ¿Cuál es la capacidad de cada canal? **(2 puntos)**
e) ¿Cuál es el valor de la entropía a la salida del canal? **(2 puntos)**

Problema 2 (20%)

Sabiendo que:

$$7^{201} = 2 \; mod \; 997$$
$$7^{6} = 3 \; mod \; 997$$
$$7^{817} = 11 \; mod \; 997$$
$$7^{x} = 792 \; mod \; 997$$

encuéntrese el valor de *x* (logaritmo discreto en base 7 de 792 módulo 997)

SIGUE DETRÁS

Problema 3 (40%)

Se dispone de un cifrador de cuatro bits de entrada y cuatro bits de salida que, para la clave **k=158** tiene la siguiente relación entrada salida [M,E_{158}(M)]

M	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
C=E_{158}(M)	7	4	1	E	B	8	5	2	F	C	9	6	3	0	D	A

- El tamaño de **k** es el mínimo necesario para que el cifrador pueda suponerse perfectamente aleatorio
- El usuario **A** tiene un sistema RSA caracterizado por *p=13, q=43, e=5*
- El usuario **B** tiene un sistema RSA caracterizado por *p=17, q=41, e=3*
- El mensaje **M** =44F578 tiene un valor de hash de 5F84

¿Cuál sería el criptograma resultante de enviar el fichero M de A hacia B en secreto y firmado?

PROBLEMA 1

a)

$p(A/A) = 0'6 \rightarrow p(B/A) = 0'4$
$p(B/B) = 0'4 \rightarrow p(A/B) = 0'6$
} El sistema se comporta igual en ambos estados ⇒ SIN MEMORIA

b) Puesto que es una memoria $p(A) = p(A/A) = 0'6 \Rightarrow p(B) = 0'4$

$$H_F = 0'6 \cdot \log_2 \frac{1}{0'6} + 0'4 \log_2 \frac{1}{0'4} = 0'971 \text{ bits/símb.}$$

c) 54'32 % de veces a la salida → $p_S(0) = 0'5432$.

Sea P_E la probabilidad de error del canal conjunto

$$p_S(0) = p(1) P_E + P(0)(1-P_E) \Rightarrow 0'5432 = 0'4 P_E + 0'6 \cdot (1-P_E) = 0'6 - 0'2 P_E$$

$$\Rightarrow P_E = \frac{0'6 - 0'5432}{0'2} = 0'284$$

$$C_{CONJUNTO} = 1 - \left[0'284 \log_2 \frac{1}{0'284} + 0'716 \log_2 \frac{1}{0'716}\right] = \underline{0'14 \text{ bits/símb.}}$$

d) $P_E = P_e (1-0'7P_e) + (1-P_e) 0'7 P_e = 0'284 \Rightarrow$

$0'284 = P_e - 0'7 P_e^2 + 0'7 P_e - 0'7 P_e^2 = -1'4 P_e^2 + 1'7 P_e \Rightarrow$

$1'4 P_e^2 - 1'7 P_e + 0'284 = 0 \Rightarrow P_e = \begin{cases} 0'2 \\ 1'014 \Rightarrow \text{No tiene sentido} \end{cases}$

$\underline{P_{e_1} = 0'2}$ $\underline{P_{e_2} = 0'7 P_{e_1} = 0'14}$

$$C_1 = 1 - \left[0'2 \log_2 \frac{1}{0'2} + 0'8 \log \frac{1}{0'8}\right] = 0'278 \text{ bits/símb.}$$

$$C_2 = 1 - \left[0'14 \log_2 \frac{1}{0'14} + 0'86 \log_2 \frac{1}{0'86}\right] = 0'416 \text{ bits/símb.}$$

e) $H_S = 0'5432 \log_2 \frac{1}{0'5432} + 0'4568 \log_2 \frac{1}{0'4568} = 0'994 \text{ bits/símb.}$

PROBLEMA 2

$$792 = 2^3 \cdot 3^2 \cdot 11$$

$$7^x = 792 = (7^{201})^3 \cdot (7^6)^2 \cdot 7^{817} \mod 997$$

$$\Rightarrow \quad x = 201 \cdot 3 + 6 \cdot 2 + 817 \mod 996 \Rightarrow x = 436$$

PROBLEMA 3

Envío de la clave de sesión $158^3 \mod_{697} = 686 = 2AE$

Cifrado del mensaje (CBC)

$4 \rightarrow B$

$4+B = 0100 + 1011 = 1111 = F \rightarrow A$

$F+A = 1111 + 1010 = 0101 : 5 \rightarrow 8$

$5+8 = 0101 + 1000 = 1101 = D \rightarrow 0$

$7+0 = 0111 + 0000 = 0111 = 7 \rightarrow 2$

$8+2 = 1000 + 0010 = 1010 = A \rightarrow 9$

} BA029

Firma del hash: 5F

$d_A = 5^{-1} \mod 504$

	504	5	4	1
0	1	-100	101	
	100	1		

$\Rightarrow d_A = 101$

$5F84_H = 24452 \mod_{559} = 415$

Hash firmado $= 415^{101} \mod_{559} = 519 = 207_H$

CRIPTOGRAMA

2AE BA029 207