Control Aguilar

CONTROL DE TRANSMISIÓN DE DATOS. 13 de Diciembre de 2007

Notas Importantes:

1h 30min

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Ponga su nombre y apellidos en cada hoja, enumerándolas.
3. Un error conceptual grave, puede anular todo el problema.

Nota: Lista de los números primos menores que 230: 1 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229.

Pregunta 1 (1p)

Un atacante ha conseguido que dos usuarios RSA A y B cifren un mismo mensaje desconocido. El atacante conoce sus claves públicas $(e_A, N_A)=(5, 119)$ y $(e_B, N_B)=(11, 119)$ y los criptogramas que se intercambian $C_{A\to B}=108$ y $C_{B\to A}=3$. Averigüe cuál es el mensaje.

Pregunta 2 (1p)

Sea F={A, B, C} un fuente que emite sus símbolos con probabilidades p(A)=0'8, p(B)=0'1 y p(C)=0'1.

a) Calcule la eficiencia del código Huffman binario. **(0'5p)**

Para aumentar esta eficiencia se extiende la fuente de tal manera que se concatenan los símbolos de dos en dos.

b) Calcule la eficiencia del código Huffman binario para la fuente extendida resultante de concatenar los símbolos de la fuente sencilla de dos en dos. **(0'5p)**

Pregunta 3 (1p)

Se dispone de un texto de 1000 símbolos utilizando un alfabeto inventado cuyos elementos son independientes y equiprobables. El texto se emite a 500 bps durante 10 seg. ¿Cuántos elementos como máximo tiene el alfabeto?

Pregunta 4 (1p)

Se dispone de un codificador aritmético para una fuente de alfabeto {A, B, C, D, E}. Las probabilidades asociadas a los símbolos fuente son p(A)=p(B)=p(C)=p(D)=p(E)=0'2. Decodifique el valor 0'0675 si procede de una secuencia de 4 caracteres.

Pregunta 5 (1p)

Dos tenistas T1 y T2 se reúnen a menudo y juegan dos partidos consecutivos. Sea X la variable aleatoria resultado del primer partido e Y la variable aleatoria resultado del segundo partido. Se ha observado que si el primer partido lo gana T1, el segundo partido lo gana T1 o T2 al 50%. Y si el primer partido lo gana T2 el segundo siempre lo gana T2 de nuevo. El primer partido lo gana T2 con probabilidad 1/3.

a) Calcule H(Y\X). **(0'5p)**

b) Calcule I(X;Y). **(0'5p)**

Pregunta 6 (1p)

Sea un LFSR caracterizado por el polinomio de conexiones completo de grado 17. Puede asegurarse que:

a) El período no depende del estado inicial.

b) Si el estado inicial es D^5, el período es 18.

c) El período es 131071.

d) Ninguna de las anteriores

Pregunta 7 (1p)

Una fuente que emite dos símbolos independientes con probabilidades 0'6 y 0'4 atraviesa un canal BSC (*Binary Symmetric Channel*). La BER (*Bit Error Rate*) del canal es de 0'1.

a) ¿Cuánto vale la entropía a la salida del canal? **(0'5p)**

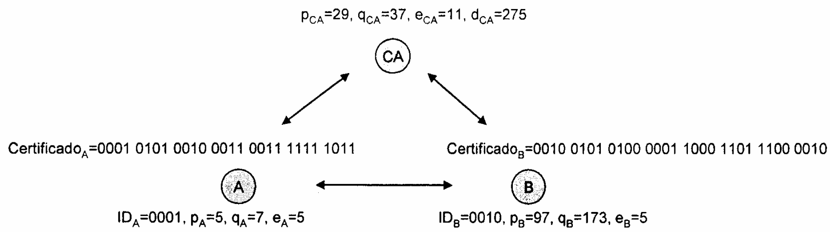
b) ¿Cuánto vale la información mutua de la fuente a la entrada del canal y la fuente a la salida del canal? **(0'5p)**

Pregunta 8 (1p)

Sean A y B dos usuarios de un sistema RSA en que se trabaja con secuencias binarias de longitud mínima 4 bits. CA es la autoridad certificadora. A y B solicitan a CA sus certificados digitales.

La función resumen H(M) tiene 4 bits de longitud. Consiste en añadir ceros a la izquierda de la secuencia M hasta que ésta tenga longitud múltiplo de 4 y hacer bloques de 4 bits. El primer bit de H(M) es la suma de todos los primeros bits de cada bloque; el segundo bit de H(M) es la suma de todos los segundos bits de cada bloque; y así sucesivamente hasta llegar al cuarto bit de H(M).

A y B se intercambian sus certificados. Haga las operaciones que hace B para autenticar la procedencia del certificado de A. ¿La clave pública de A es auténtica?



Pregunta 9 (1p)

En relación al ejercicio anterior, obtenga el criptograma C_{BA} que B envía a A correspondiente al mensaje M_{BA}=100.

Pregunta 10 (1p)

Se ha encontrado un criptograma antiguo cifrado con una *Escítala lacedemonia de Esparta* (bara de madera en la que se enrollaba el texto que se quería enviar cifrado). Se sabe que esta escítala equivale a una matriz 8x3. El criptograma es **UNSNOCACAGASUZWIAWLMWAOW**. ¿Cuál es el mensaje?

(1) Ataque por módulo común.

(A)	(B)
$e_A = 5$	$e_B = 11$
$N = 119$	$N = 119$
$C_{AB} = M^{e_B} \bmod N$	$C_{BA} = M^{e_B} \bmod N$

Si $mcd(e_A, e_B) = 1$, $\exists\, r, s$ enteros $\mid r \cdot e_A + s \cdot e_B = 1$.

$mcd(5, 11) = 1$. $\Rightarrow \left(C_{AB}^{\,s} \cdot C_{BA}^{\,r}\right)_N = M^{s \cdot e_B} \cdot M^{r \cdot e_B} = M^{s \cdot e_B + r \cdot e_B} = (M)_N$

$r \cdot 5 + s \cdot 11 = 1 \longrightarrow r = -2,\ s = 1$

$M = 108^1 \cdot 3^{-2} \bmod N = 108 \cdot (3^2)^{-1} \bmod N = (108 \cdot 9^{-1}) \bmod 119$

$9^{-1} \cdot 9 = 1 \bmod 119 = 1 + k \cdot 119$

$9^{-1} = \dfrac{1 + k \cdot 119}{9} = \dfrac{1 + k(13 \cdot 9 + 2)}{9} = 13k + \dfrac{2k+1}{9} \underset{k=4}{\uparrow} = 53$

$119 \,\lfloor 9$; $2\ \ 13$

$M = (108 \cdot 53) \bmod 119 = 5724 \bmod 119 = 12$

$$\boxed{M = 12}$$

(2)

F	p(F)	Código
A	0'8	0
B	0'1	10
C	0'1	11

a)

$H(F) = 0'8 \log_2 \dfrac{1}{0'8} + 2 \cdot 0'1 \cdot \log_2 \dfrac{1}{0'1} = 0'9219$ bits/símbolo

$\bar{L} = 1 \cdot 0'8 + 2 \cdot 0'1 \cdot 2 = 1'2$ bits/símbolo

$E = \dfrac{H}{\bar{L}} = \dfrac{0'9219}{1'2} \rightarrow \boxed{E = 0'7683}$

b)

F^m	$p(F^m)$
AA	$0'8^2 = 0'64$
AB	$0'8 \cdot 0'1 = 0'08$
AC	$0'8 \cdot 0'1 = 0'08$
BA	$0'1 \cdot 0'8 = 0'08$
BB	$0'1^2 = 0'01$
BC	$0'1^2 = 0'01$
CA	$0'1 \cdot 0'8 = 0'08$
CB	$0'1^2 = 0'01$
CC	$0'1^2 = 0'01$

$H(F^m) = m \cdot H(F) = 2 \cdot 0'9219 = 1'8438$ bits/símbolo

o bien:

$H(F^m) = 0'64 \cdot \log_2 \dfrac{1}{0'64} + 4 \cdot 0'08 \cdot \log_2 \dfrac{1}{0'08} + 4 \cdot 0'01 \cdot \log_2 \dfrac{1}{0'01}$

$= 1'8438$ bits/símbolo

Código

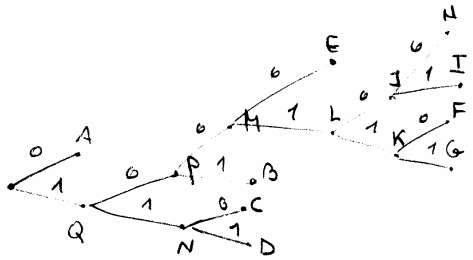
AA → A 0'64
AB → B 0'08
AC → C 0'08
BA → D 0'08
BB → E 0'08
BC → F 0'01
CA → G 0'01
CB → H 0'01 }
CC → I 0'01 } J 0'02

A 0'64
B 0'08
C 0'08
D 0'08
E 0'08
J 0'02
F 0'01 }
G 0'01 } K 0'02 } L 0'04 } M 0'12

A 0'64
M 0'12
B 0'08
C 0'08 }
D 0'08 } N 0'16

A 0'64
N 0'16
M 0'12 }
B 0'08 } P 0'2

A 0'64
P 0'2 }
N 0'16 } Q 0'36 //



F^m	Código
A	0
B	101
C	110
D	111
E	1000
F	100110
G	100111
H	100100
I	100101

$$\bar{L} = 1 \cdot 0'64 + 3 \cdot 0'08 \cdot 3 + 4 \cdot 0'08 + 6 \cdot 0'01 \cdot 4 = 1'92 \text{ bits/símbolo}$$

$$E = \frac{H}{\bar{L}} = \frac{1'8438}{1'92} \rightarrow \boxed{E = 0'9603}$$ Aumenta.

③ Se emiten 1000 símbolos.
Se emiten $500 \frac{\text{bits}}{\text{seg}} \cdot 10\,\text{seg} = 5000$ bits.

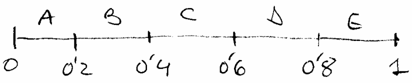
$$\bar{L} = \frac{5000 \text{ bits}}{1000 \text{ símbolo}} = 5 \text{ bits/símbolo}$$

$H(F) = \log_2 F$
↑
símbolos equiprobables independientes

$$5 = \bar{L} \geq H(F) = \log_2 F$$

$$\boxed{32 \geq F}$$

4



$0'0675 \rightarrow A$

$\dfrac{0'0675-0}{0'2} = 0'3375 \longrightarrow B$

$\dfrac{0'3375-0'2}{0'2} = 0'6875 \rightarrow D$

$\dfrac{0'6875-0'6}{0'2} = 0'4375 \rightarrow C$

$\boxed{ABDC}$

5

Y\X	T1	T2
T1	1/2	0
T2	1/2	1

a) $H(Y \backslash X) = H(Y \backslash X=T1) \cdot P(X=T1) + H(Y \backslash X=T_2) \cdot P(X=T_2)$

$P(X=T_2) = 1/3$

$P(X=T_1) = 2/3$

$H(Y \backslash X=T_1) = 0'5 \cdot \log_2 \dfrac{1}{0'5} \cdot 2 = 1$ bit/símbolo

$H(Y \backslash X=T_2) = 0 + 1 \cdot \log_2 1 = 0$

$H(Y \backslash X) = 1 \cdot \dfrac{2}{3} + 0 \cdot \dfrac{1}{3} = \dfrac{2}{3} \longrightarrow \boxed{H(Y \backslash X) = 0'6667 \ \dfrac{\text{bits}}{\text{símbolo}}}$

b) $I(X;Y) = H(X) - H(X \backslash Y) = H(Y) - H(Y \backslash X)$

Y, X	T_1	T_2
T_1	1/3	0
T_2	1/3	1/3

$P(y_j, x_i) = P(y_j \backslash x_i) \cdot P(x_i)$

$P(Y=T_1) = 1/3 + 0 = 1/3$

$P(Y=T_2) = 1/3 + 1/3 = 2/3$

$H(Y) = \dfrac{1}{3} \log_2 3 + \dfrac{2}{3} \log_2 \dfrac{3}{2} = 0'9183$

$I(X;Y) = 0'9183 - 0'6667 \longrightarrow \boxed{I(X;Y) = 0'2516 \ \dfrac{\text{bits}}{\text{símbolo}}}$

(6) $C(D)$ completo grado $m=17$

a) Sí que depende. No depende para $C(D)$ primitivo, en que $L = L_{max} = 2^m - 1 = 2^{17} - 1 = 131071$

(b) $P^{(0)}(D) = D^5 \equiv 00000100000000000$
Todos los estados con un solo Uno, pertenecen al subconjunto de estados en se $L = L_{max} = m+1 = 18$

c) No, sería el primitivo

(7)

F	p(F)	Código	BSC	F'
A	0'6	0	$\xrightarrow{1-p}$; $\xrightarrow{p}$	0'
B	0'4	1	$\xrightarrow{p}$; $\xrightarrow{1-p}$	1'

a) $p = 0'1$

$p(0') = p(0)\cdot(1-p) + p(1)\cdot p = 0'6\cdot 0'9 + 0'4\cdot 0'1 = 0'58$

$p(1') = p(0)\cdot p + p(1)\cdot(1-p) = 0'6\cdot 0'1 + 0'4\cdot 0'9 = 0'42$

$H(F') = 0'58\cdot \log_2 \frac{1}{0'58} + 0'42\cdot \log_2 \frac{1}{0'42} = 0'9814$ bits/símbolo

b) $I(F;F') = H(F') - H(F'\backslash F)$

$p(F'\backslash F) = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$

$H(F'\backslash F) = p(F=0)\cdot H(F'\backslash F=0) +$
$+ p(F=1)\cdot H(F'\backslash F=1) =$
$= 0'6\cdot\left((1-p)\log_2 \frac{1}{1-p} + p \log_2 \frac{1}{p}\right) +$
$+ 0'4\cdot\left(p \log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}\right) =$
$= p\cdot \log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p} =$
$= 0'1\cdot \log_2 \frac{1}{0'1} + 0'9\cdot \log_2 \frac{1}{0'9} = 0'4689$ bit/símbolo

$I(F;F') =$
$= 0'9814 - 0'4689$

$$\boxed{I(F;F') = 0'5124 \text{ bit/símbolo}}$$