Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

M. Aguilar

CONTROL DE TRANSMISIÓN DE DATOS. 31 de Mayo de 2007

Notas Importantes:

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

Problema 1 (33%)

Sea un sistema de clave pública RSA. Considere dos usuarios A y B y una entidad certificadora CA que expende Certificados Firmados (Certificado Claro || Firma Digital). Los usuarios del sistema utilizan criptografía asimétrica RSA para autenticarse y para intercambiar una clave de sesión. Las secuencias binarias se consideran con más peso a la izquierda (MPI). **El sistema trabaja en bloques de 4 bits.**

Parámetros RSA de los usuarios:

Usuario A: 0001	p_A=13, q_A=7, e_A=7, d_A=31
Usuario B: 0010	p_B=5, q_B=11, e_B=3, d_B
CA	P_{CA}=3, q_{CA}=11, e_{CA}=13, d_{CA}=17

La función resumen o *Hash* H(M) de un mensaje M, se obtiene aplicando la operación OR-exclusiva (⊕), bit a bit, sobre los sucesivos bloques del mensaje M de entrada. El funcionamiento es el siguiente:

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden a la izquierda del mensaje tantos ceros como sea necesario para que la longitud sea múltiplo de 4.
- Se divide el mensaje resultante desde la izquierda en m bloques b_j, de n=4 bits cada uno, siendo $1 \leq j \leq m$.
- b_{ij} es el bit i-ésimo del bloque j-ésimo; $1 \leq i \leq n$
- $H(M)=C$. La función *Hash* de M es un bloque resultante $C=C_1C_2C_3\ldots C_n$ de n=4 bits, donde:
- El bit i-ésimo del bloque C es: $C_i=b_{i1}\oplus b_{i2}\oplus b_{i3}\oplus\ldots..\oplus b_{im}$.

a) Obtenga el certificado digital que CA envía a A. Expréselo en hexadecimal. Explique qué hacen ambos usuarios de modo que uno de ellos autentique al otro. ¿Quién autentica a quién, en este caso? **(1p)**

b) B desea comunicar una clave de sesión a A, $k_{sesión}$. Indique qué condiciones han de cumplir las posibles $k_{sesión}$ que B envíe a A. ¿Es válida $k_{sesión}$ = 6? **(1p)**

c) Suponga que la respuesta es afirmativa, obtenga el criptograma que B envía a A. **(0,3p)**

d) Dicha clave de sesión es el estado inicial del LFSR con polinomio de conexiones $C(D)=1+D^3+D^4$, que se utiliza para cifrar en flujo. Obtenga el criptograma que genera B para enviar codificado a A el mensaje $M=43F2A2_H$. Nota: El 1er bit generado por el LFSR cifra al bit menos significativo del mensaje. **(1p)**

Problema 2 (33%)

Sean X e Y dos variables aleatorias discretas con la siguiente función de distribución (**probabilidades conjuntas**):

Y\X	X_1	X_2	X_3	X_4
Y_1	1/18	1/18	1/9	1/9
Y_2	1/9	1/9	1/9	1/9
Y_3	0	1/9	0	1/9

a) Calcule la entropía conjunta, H(X, Y). **(0,6p)**

b) Calcule la entropía de X, H(X). **(1p)**

c) Calcule la entropía condicionada, H(Y\X). **(1p)**

d) Calcule la información mutua, I(X; Y). **(0,7p)**

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

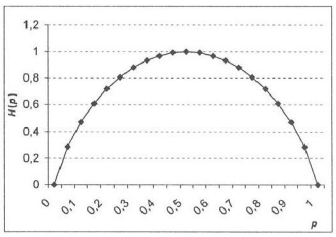
Problema 3 (34%)

Sea un canal discreto caracterizado por esta matriz de probabilidades de transición:

$$p(D \setminus F) = \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$$

a) Calcule la capacidad de canal discreto. **(1p)**
b) ¿Cómo es la fuente F que aproveche al máximo la capacidad de dicho canal? **(1p)**
c) Calcule la eficiencia del código *Huffman* para la fuente del apartado anterior. **(0,4p)**
d) Comente el resultado obtenido. **(1p)**

Nota:



$$H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{(1-p)}$$

p	H(p)
0	0,00000
0,001995	0,02077
0,00399	0,03754
0,005985	0,05280
0,00798	0,06708
0,009975	0,08063
0,01197	0,09359
0,013965	0,10606
0,01596	0,11811
0,017955	0,12980
0,01995	0,14116
0,021945	0,15223
0,02394	0,16302
0,025935	0,17358
0,02793	0,18390
0,029925	0,19402
0,03192	0,20393
0,033915	0,21366
0,07	0,36592
0,08	0,40218
0,09	0,43647
0,1	0,46900
0,11	0,49992
0,12	0,52936
0,13	0,55744
0,14	0,58424
0,15	0,60984
0,16	0,63431
0,17	0,65770
0,18	0,68008
0,19	0,70147
0,2	0,72193
0,21	0,74148
0,22	0,76017
0,23	0,77801
0,24	0,79504
0,25	0,81128
0,26	0,82675
0,27	0,84146
0,28	0,85545
0,29	0,86872
0,3	0,88129
0,31	0,89317
0,32	0,90438
0,33	0,91493
0,34	0,92482
0,35	0,93407
0,36	0,94268
0,37	0,95067
0,38	0,95804
0,39	0,96480
0,4	0,97095
0,41	0,97650
0,42	0,98145
0,43	0,98582
0,44	0,98959
0,45	0,99277
0,46	0,99538
0,47	0,99740
0,48	0,99885
0,49	0,99971
0,5	1,00000
0,51	0,99971
0,52	0,99885
0,53	0,99740
0,54	0,99538
0,55	0,99277
0,56	0,98959
0,57	0,98582
0,58	0,98145
0,59	0,97650
0,6	0,97095
0,61	0,96480
0,62	0,95804
0,63	0,95067
0,64	0,94268
0,65	0,93407
0,66	0,92482
0,67	0,91493
0,68	0,90438
0,69	0,89317
0,7	0,88129
0,71	0,86872
0,72	0,85545
0,73	0,84146
0,74	0,82675
0,75	0,81128
0,76	0,79504
0,77	0,77801
0,78	0,76017
0,79	0,74148
0,8	0,72193
0,81	0,70147
0,82	0,68008
0,83	0,65770
0,84	0,63431
0,85	0,60984
0,86	0,58424
0,87	0,55744
0,88	0,52936
0,89	0,49992
0,9	0,46900
0,91	0,43647
0,92	0,40218
0,93	0,36592
0,94	0,32744
0,95	0,28640
0,96	0,24229
0,97	0,19439
0,98	0,14144
1	0,00000

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

(2) a) $H(X,Y) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)} =$

$= 2 \cdot \frac{1}{18} \log_2 \frac{1}{1/18} + 8 \cdot \frac{1}{9} \cdot \log_2 \frac{1}{1/9} = 3'2810 \frac{\text{bits}}{\text{símbolo}}$

b) $H(X) = \sum_i p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = \frac{1}{6} \log_2 6 + \frac{5}{18} \log_2 \frac{18}{5} + \frac{2}{9} \log_2 \frac{9}{2} + \frac{1}{3} \log_2 3$

$p(x_1) = \sum_j p(x_1, y_j) = \frac{1}{18} + \frac{1}{9} = \frac{1}{6}$

$p(x_2) = \sum_j p(x_2, y_j) = \frac{1}{18} + 2 \cdot \frac{1}{9} = \frac{5}{18}$

$p(x_3) = \sum_j p(x_3, y_j) = 2 \cdot \frac{1}{9} = \frac{2}{9}$

$p(x_4) = \sum_j p(x_4, y_j) = 3 \cdot \frac{1}{9} = \frac{1}{3}$

$H(X) = 1'9547 \frac{\text{bits}}{\text{símbolo}}$

c) $H(Y \backslash X) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(y_j \backslash x_i)}$

$p(y_j \backslash x_i) = \frac{p(y_j, x_i)}{p(x_i)}$

$Y \backslash X$	x_1	x_2	x_3	x_4
Y_1	1/3	1/5	1/2	1/3
Y_2	2/3	2/5	1/2	1/3
Y_3	0	2/5	0	1/3

$H(Y \backslash X) = \frac{1}{18} \log_2 3 + \frac{1}{9} \log_2 \frac{3}{2} + \frac{1}{18} \log_2 5 + \frac{1}{9} \log_2 \frac{5}{2} + \frac{1}{9} \log_2 \frac{5}{2} + \frac{1}{9} \log_2 2 + \frac{1}{9} \log_2 2 +$

$+ 3 \cdot \frac{1}{9} \cdot \log_2 3 = 1'3263 \frac{\text{bits}}{\text{símbolo}}$

O bien: $H(Y \backslash X) = H(X,Y) - H(X) = 3'2810 - 1'9547 = 1'3263 \frac{\text{bits}}{\text{símbolo}}$

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

$H(Y) = \sum_j p(y_j) \cdot \log_2 \frac{1}{p(y_j)}$

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

$$p(y_1) = \sum_i p(x_i, y_1) = 2\cdot\frac{1}{18} + 2\cdot\frac{1}{9} = \frac{1}{3}$$

$$p(y_2) = \sum_i p(x_i, y_2) = 4\cdot\frac{1}{9} = \frac{4}{9}$$

$$p(y_3) = \sum_i p(x_i, y_3) = \frac{2}{9}$$

$$H(Y) = \frac{1}{3}\cdot\log_2 3 + \frac{4}{9}\cdot\log_2\frac{9}{4} + \frac{2}{9}\cdot\log_2\frac{9}{2} = 1'5305 \ \frac{\text{bits}}{\text{símbolo}}$$

$$\boxed{I(X;Y) = 1'5305 - 1'3263 = 0'2042 \ \frac{\text{bits}}{\text{símbolo}}}$$

(3)

$$p(D\setminus F) = \begin{array}{c} \\ A_i=1 \\ A_i=2 \end{array}\begin{array}{c} \begin{array}{ccc} B_j=1 & B_j=2 & B_j=3 \end{array} \\ \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 1/3 & 1/3 \end{pmatrix} \end{array} \qquad p(A_1) + p(A_2) = 1$$

a)

$$H(D\setminus F) = \sum_i p(A_i)\cdot H(D\setminus A_i) = p(A_1)\cdot 1'5 + \left(1-p(A_1)\right)\cdot 1'5849 = 1'5849 - 0'0849\cdot p(A_1)$$

$$H(D\setminus A_1) = \frac{1}{2}\log_2 2 + \frac{1}{4}\cdot\log_2 4\cdot 2 = \frac{1}{2} + 1 = \frac{3}{2} = 1'5$$

$$H(D\setminus A_2) = 3\cdot\frac{1}{3}\log_2 3 = 1'5849$$

$$H(D) = \sum_j p(B_j)\cdot\log_2\frac{1}{p(B_j)}$$

$$p(B_1) = \frac{1}{2}\cdot p(A_1) + \frac{1}{3}\cdot p(A_2) = \frac{1}{2}\cdot p(A_1) + \frac{1}{3}\cdot\left(1-p(A_1)\right) = \frac{1}{3} + 0'167\cdot p(A_1)$$

$$p(B_2) = \frac{1}{4}\cdot p(A_1) + \frac{1}{3}\,p(A_2) = \frac{1}{4}\cdot p(A_1) + \frac{1}{3}\left(1-p(A_1)\right) = \frac{1}{3} - 0'083\cdot p(A_1)$$

$$p(B_3) = \frac{1}{4}\cdot p(A_1) + \frac{1}{3}\cdot p(A_2) = \frac{1}{4}\,p(A_1) + \frac{1}{3}\left(1-p(A_1)\right) = \frac{1}{3} - 0'083\cdot p(A_1)$$

$$H(D) = \left(\frac{1}{3} + 0'167\cdot p(A_1)\right)\cdot\log_2\frac{1}{\frac{1}{3}+0'167\,p(A_1)} + \left(\frac{1}{3} - 0'083\cdot p(A_1)\right)\cdot\log_2\frac{1}{\frac{1}{3}-0'083\cdot p(A_1)} +$$

$$+\left(\frac{1}{3} - 0'083\cdot p(A_1)\right)\cdot\log_2\frac{1}{\frac{1}{3}-0'083\cdot p(A_1)}$$

$$C_1 = \max_{\{p(A_i)\}}\left[H(D) - H(D\setminus F)\right] \underset{p(A_1)=x}{=} \max_x\left\{\left(\frac{1}{3}+0'167x\right)\cdot\log_2\frac{1}{\frac{1}{3}+0'167x} + \left(\frac{1}{3}-0'083x\right)\cdot\log_2\frac{1}{\frac{1}{3}-0'083x}\right.$$

$$\left.+\left(\frac{1}{3}-0'083x\right)\cdot\log_2\frac{1}{\frac{1}{3}-0'083x} - 1'5849 + 0'0849x\right\}$$

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

$$G'(x) = 0'167 \cdot \log_2 \frac{1}{\frac{1}{3}+0'167x} + \left(\frac{1}{3}+0'167x\right)^2 \cdot \frac{1}{\ln 2} \cdot \frac{-1 \cdot 0'167}{\left(\frac{1}{3}+0'167x\right)^2} -$$

$$2 \cdot \left(-0'083 \cdot \log_2 \frac{1}{\frac{1}{3}-0'083x}\right) + \left(\frac{1}{3}-0'083x\right)^2 \cdot \frac{1}{\ln 2} \cdot \frac{+1 \cdot 0'083}{\left(\frac{1}{3}-0'083x\right)^2} \cdot 2 + 0'0849$$

$$G'(x) = \phi \rightarrow 0'167 \cdot \log_2 \frac{1}{\frac{1}{3}+0'167x} - \frac{0'167}{\ln 2} - 0'083 \cdot \log_2 \frac{1}{\frac{1}{3}-0'083x} \cdot 2$$

$$+ \frac{0'083}{\ln 2} \cdot 2 + 0'0849 = \phi$$

$$0'167 \cdot \log_2 \frac{1}{\frac{1}{3}+0'167x} - 0'167 \cdot \log_2 \frac{1}{\frac{1}{3}-0'083x} = -0'0849$$

$$\log_2 \frac{1}{\frac{1}{3}+0'167x} - \log_2 \frac{1}{\frac{1}{3}-0'083x} = \frac{-0'0849}{0'167} = -0'5084$$

$$\log_2 \frac{\frac{1}{3}-0'083x}{\frac{1}{3}+0'167x} = -0'5084$$

$$2^{-0'5084} = \frac{\frac{1}{3}-0'083x}{\frac{1}{3}+0'167x}$$

$$0'7030 = \frac{1-0'249x}{1+0'501x} \quad // \quad 0'7030 + 0'3522x = 1 - 0'249x$$

$$0'599x = 0'297 \quad // \quad x_{MAX} = 0'4958 = p(A_1)$$

$$\boxed{C = G(x_{MAX}) = 0'4161 \cdot \log_2 \frac{1}{0'4161} + 0'2922 \cdot \log_2 \frac{1}{0'2922} \cdot 2 - 1'5428}$$

$$= \boxed{0'02086 \ \frac{\text{bits}}{\text{símbolo}}}$$

b) La fuente emite dos símbolos. Para $p(A_1) = p$, $p(A_2) = 1-p$

$$H(F) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$$

$\boxed{H(F) \leq C}$ $\quad H(F) = C \rightarrow 0'02086 = H(p) \rightarrow \boxed{p \simeq 0'001995}$

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

Será una F con $p(A_1) = 0'001995$ y $p(A_2) = 1 - p(A_1) = 0'998$

c) $E = \frac{H}{\bar{L}}$ El código Hoffman es

F	→ Código Hoffman
A_1	0
A_2	1

$\bar{L} = 1$ bit/símbolo

$E = \frac{0'02086}{1} = 0'02086$

d) Es muy bajo, debido a la fuerte dispersión de probabilidades.
Se podría aumentar E extendiendo la fuente, $H(F^m) = m \cdot H(F)$.

P1

a) $A \rightarrow CA \quad (A, e_A, N_A) = (0001 | 0111 | 0101 | 1011)$

$N_A = p_A \cdot q_A = 13 \cdot 7 = 91 \equiv 01011011$

$CA \rightarrow A \quad (\underbrace{A, e_A, N_A}_{M}, FD(M))$

$H(M) = 0+0+0+1, 0+1+1+0, 0+1+0+1, 1+1+1+1 = 1000 \equiv 8$

$FD(M) = H(M)^{d_{CA}} \bmod N_{CA} = 8^{17} \bmod 33 = 2 \equiv 0010$

$d_{CA} = 17$

$N_{CA} = p_{CA} \cdot q_{CA} = 3 \cdot 11 = 33$

$CA \rightarrow A \quad (\underbrace{0001}_{A} | \underbrace{0111}_{e_A} | \underbrace{0101 | 1011}_{N_A} | 0010)$ FD(M)

M

b) $C_{K_{sesión}} = K_{sesión}^{e_A} \bmod N_A$, $0 < K_{sesión} < N_A = 91$ OK.

c) $C_{K_{sesión}} = 6^7 \bmod 91 = 20$

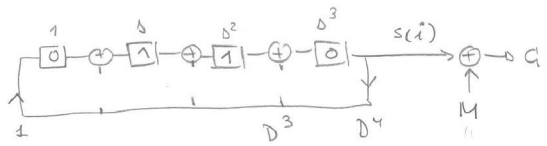
LFSR → (+) → C'

$P^{(0)}(b) = K_{sesión} = 6 \equiv 0110$

$M = 43F2A2_H \equiv 10000111111100101010010$

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

d)



$c(D) = 1 + D^3 + D^4$ es primitivo. $\Rightarrow$ $L = 2^m - 1 = 2^4 - 1 = 15$

$P^{(0)}(D) = P^{(15)}(D) = P^{(30)}(D)$ ....

m	1	D	D^2	D^3	
0	0	1	1	0	
1	0	0	1	1	$\equiv D^2 + D^3$
2	1	0	0	0	
3	0	1	0	0	
4	0	0	1	0	
5	0	0	0	1	$\equiv D^3$
6	1	0	0	1	
7	1	1	0	1	
8	1	1	1	1	
9	1	1	1	0	
10	0	1	1	1	
11	1	0	1	0	
12	0	1	0	1	
13	1	0	1	1	
14	1	1	0	0	
15	0	1	1	0	

s(i)

$P^{(n)}(D) = D \cdot P^{(n-1)}(D) \bmod c(D)$

$D^4 + D^3 \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1

$D^4 \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^3 + 1$

$D^4 + D \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^3 + D + 1$

$D^4 + D^2 + D \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^3 + D^2 + D + 1$

$D^4 + D^3 + D^2 + D \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^2 + D + 1$

$D^4 + D^3 + D^2 \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^2 + 1$

$D^4 + D^2 \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D^3 + D^2 + 1$

$D^4 + D^3 + D \;\big|\; D^4 + D^3 + 1$ — $D^4 + D^3 + 1$ — 1 — $D + 1$

HPI

→ bit menos significativo

M =	100	0011	1111	0010	1010	0010
s(i) =	110	0010	0011	0101	1110	0010
	010	0001	1100	0111	0100	0000 = d