CONTROL DE TRANSMISIÓN DE DATOS. 12 de Diciembre de 2008

MONICA AGUILAR

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.
4. Las secuencias binarias tienen MPI (Más Peso a la Izquierda).
5. Lista de los 101 primeros números primos: 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

Problema 1 (20%)

Antonio (A) y Berta (B) se comunican mediante un sistema de cifrado RSA. Sus claves públicas son, respectivamente: $Kp_A=(e_A, N_A)= (23, 403)$ y $Kp_B=(e_B, N_B)= (97, 403)$. Ambos se intercambian un mismo mensaje **M** cifrado. Averigüe el mensaje **M**, sin factorizar el módulo. El criptograma que emite Antonio es 41. El criptograma que emite Berta es 59.

Problema 2 (15%)

Ana (A) y Bruno (B) se comunican mediante un sistema de cifrado de Vernam que trabaja en bloques de 12 bits. Los primeros (izquierda) 6 bits de la clave de cifrado los elige Ana y los segundos 6 bits los elige Bruno. Ambas subclaves las intercambian mediante cifrado RSA. Sus parámetros RSA son, respectivamente:

$p_A=7$, $q_A=11$, $e_A=7$, $\mathbf{d_A}$

$p_B=3$, $q_B=11$, $e_B=3$, $\mathbf{d_B}$

Los criptogramas que se intercambian son $C_{AB}=19$ y $C_{BA}=53$. Ana desea transmitir a Bruno el mensaje $M_{AB}=$ "#%" codificado en ASCII. ¿Qué envía Ana a Bruno?

Problema 3 (7,5%)

Para un sistema de cifrado RSA, factorice N=387833 sabiendo que $\Phi(N)=386448$.

Problema 4 (7,5%)

a) Hallar la entropía de un dado trucado en que la probabilidad de salir 6 es doble que el resto de resultados.

b) Comparar con la entropía de un dado normal.

c) Comentar qué entropía tendría un dado trucado en que la probabilidad de salir 6 fuera mucho mayor que el resto de resultados.

Problema 5 (25%)

Se han analizado los resultados del tenista Rafael Nadal en función del tiempo que hace, contra un contrincante dado. La probabilidad de que gane si hace sol es del 70% y de que gane si no hace sol es del 30%. Los pronósticos del tiempo de hoy son del 20% de que haga sol, por lo que la probabilidad de que no haga sol es del 80%.

a) Halle la entropía asociada al resultado del tenista, H(N).

b) Halle la entropía condicionada al tiempo que hace, H(N/t). Comente el resultado.

c) Halle la información mutua entre el resultado del tenista y el tiempo que hace, I(N; t).

Problema 6 (25%)

Sea un canal binario de borrado tal que los datos o llegan correctamente con probabilidad p o se marcan como borrados.

a) Halle la matriz de probabilidades de transición

b) Calcule la capacidad de canal discreto, en función de p

Nota: Por comodidad, llame $H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p}$

Tabla ASCII

Byte	Carácter	Byte	Carácter	Byte	Carácter
0010 0000	Espacio	0100 0000	@	0110 0000	`
0010 0001	!	0100 0001	A	0110 0001	a
0010 0010	"	0100 0010	B	0110 0010	b
0010 0011	#	0100 0011	C	0110 0011	c
0010 0100	$	0100 0100	D	0110 0100	d
0010 0101	%	0100 0101	E	0110 0101	e
0010 0110	&	0100 0110	F	0110 0110	f
0010 0111	'	0100 0111	G	0110 0111	g
0010 1000	(	0100 1000	H	0110 1000	h
0010 1001	)	0100 1001	I	0110 1001	i
0010 1010	*	0100 1010	J	0110 1010	j
0010 1011	+	0100 1011	K	0110 1011	k
0010 1100	,	0100 1100	L	0110 1100	l
0010 1101	-	0100 1101	M	0110 1101	m
0010 1110	.	0100 1110	N	0110 1110	n
0010 1111	/	0100 1111	O	0110 1111	o
0011 0000	0	0101 0000	P	0111 0000	p
0011 0001	1	0101 0001	Q	0111 0001	q
0011 0010	2	0011 0010	R	0111 0010	r
0011 0011	3	0101 0011	S	0111 0011	s
0011 0100	4	0101 0100	T	0111 0100	t
0011 0101	5	0101 0101	U	0111 0101	u
0011 0110	6	0101 0110	V	0111 0110	v
0011 0111	7	0101 0111	W	0111 0111	w
0011 1000	8	0101 1000	X	0111 1000	x
0011 1001	9	0101 1001	Y	0111 1001	y
0011 1010	:	0101 1010	Z	0111 1010	z
0011 1011	;	0101 1011	[	0111 1011	{
0011 1100	<	0101 1100	\	0111 1100	|
0011 1101	=	0101 1101	]	0111 1101	}
0011 1110	>	0101 1110	^	0111 1110	~
0011 1111	?	0101 1111	_	0111 1111	

Control Mónica Aguilar. TD. 12/12/08

① **A**

$e_A = 23$

$N_A = 403 = N$

$C_{AB} = M^{e_B} \bmod N = 41$

B

$e_B = 97$

$N_B = 403 = N$

$C_{BA} = M^{e_A} \bmod N = 59$

5 { * e_A y e_B son primos, por tanto coprimos o primos relativos.

* Para $\text{mcd}(e_A, e_B) = 1$, $\exists\ r, s \in \mathbb{Z} \mid r \cdot e_A + s \cdot e_B = 1$ (Identidad de Bézout.)

5 * Además, como $N_A = N_B$, $M_{AB} = M_{BA}$ → Ataque por módulo común. $\text{mcd}(e_A, e_B)$

$$C_{AB}^{s} \cdot C_{BA}^{r} = M^{s \cdot e_B + r \cdot e_A} = M^1 \bmod N$$

5 * Para hallar r y s aplicamos el algoritmo de Euclides:

97 | 23 / 5 | 4	$97 = 23 \cdot 4 + 5$	$5 = 97 - 23 \cdot 4$	(1)
23 | 5 / 3 | 4	$23 = 5 \cdot 4 + 3$	$3 = 23 - 5 \cdot 4$	(2)
5 | 3 / 2 | 1	$5 = 3 \cdot 1 + 2$	$2 = 5 - 3 \cdot 1$	(3)
3 | 2 / 1 | 1	$3 = 2 \cdot 1 + 1$	$\boxed{1 = 3 - 2 \cdot 1}$	(4)
① 2 | 1 / 0 | 2	$\text{mcd}(97, 23) = 1$		

Nota:
También se puede hallar así → $r = e_A^{-1} \bmod e_B$

$$1 = 3 - 2 \cdot 1 \underset{(3)}{=} 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \underset{(2)}{=} (23 - 5 \cdot 4) \cdot 2 - 5 = 23 \cdot 2 - 5 \cdot 9 \underset{(1)}{=}$$

$$= 23 \cdot 2 - (97 - 23 \cdot 4) \cdot 9 = \underbrace{23 \cdot 38}_{e_A} - \underbrace{97 \cdot 9}_{e_B} \Rightarrow \begin{matrix} r = 38 \\ s = -9 \end{matrix}$$

5 * $M = C_{AB}^{s} \cdot C_{BA}^{r} \bmod N = 41^{-9} \cdot 59^{38} \bmod 403 = \left((41)^{-1}\right)^{9} \cdot 59^{38} \bmod 403$

$$41^{-1} \cdot 41 = 1 + K \cdot 403$$

$$41^{-1} = \frac{1 + K \cdot 403}{41} \underset{\substack{403 \mid 41 \\ 34 \mid 9}}{=} \frac{1 + k(41 \cdot 9 + 34)}{41} = 9 \cdot K + \underbrace{\frac{34K + 1}{41}}_{K_1} \underset{k=6}{=} 54 + 5 = 59$$

$$k = \frac{41 \cdot K_1 - 1}{34} \underset{\substack{41 \mid 34 \\ 7 \mid 1}}{=} \frac{(34 \cdot 1 + 7) K_1 - 1}{34} = K_1 + \frac{7K_1 - 1}{34} \underset{K_1 = 5}{=} 6$$

$M = 59^9 \cdot 59^{38} \bmod 403 = 59^{47} \bmod 403 = \cdots = 288$

$47 \equiv 101111 \rightarrow 59^{47} = (((((59^2)^2 \cdot 59)^2 \cdot 59)^2 \cdot 59)^2 \cdot 59$

$\boxed{M = 288}$

Comprobación: $C_{AB} = M^{e_B} \bmod N = 288^{97} \bmod 403 = \cdots = 41$

$97 \equiv 1100001 \rightarrow 288^{97} = (((((288)^2 \cdot 288)^2)^2)^2)^2 \cdot 288$

$C_{BA} = M^{e_A} \bmod N = 288^{23} \bmod 403 = \cdots = 59$

$23 \equiv 10111 \rightarrow 288^{23} = (((((288)^2)^2 \cdot 288)^2 \cdot 288)^2 \cdot 288$

(2)

A

$p_A = 7$
$q_A = 11$
$e_A = 7$
$C_{AB} = 19$ (A lo envía a B)
$M'_{AB} = \#\,\% $

B

$p_B = 3$
$q_B = 11$
$e_B = 3$
$C_{BA} = 53$ (B lo envía a A)

3 * $C'_{AB} = M'_{AB} \oplus K_S$. K_S = Clave de Sesión, cifrado de Vernam (12 bits)

$M'_{AB} = \#\,\% = 0010\,|\,0011\,0010\,0101 = \underbrace{000000000010}_{M_1\ (12\ bits)} \,\|\, \underbrace{001100100101}_{M_2\ (12\ bits)}$

3 * $n_A = p_A \cdot q_A = 77$; $\phi(N_A) = (p_A - 1)\cdot(q_A - 1) = 60 = 5 \cdot 2^2 \cdot 3$; $\phi(60) = 4 \cdot 2 \cdot 2 = 16$

$d_A = e_A^{-1} \bmod \phi(N_A) = e_A^{\phi(\phi(N_A))-1} \bmod \phi(N_A) = 7^{15} \bmod 60 = \boxed{43}$

$n_B = p_B \cdot q_B = 33$; $\phi(N_B) = 2 \cdot 10 = 5 \cdot 3^2 = (p_B - 1)\cdot(q_B - 1) = 20$; $\phi(20) = 4 \cdot 2 = 8$

$d_B = e_B^{-1} \bmod \phi(N_B) = e^{\phi(\phi(N_B))-1} \bmod \phi(N_B) = 3^7 \bmod 20 = \boxed{7}$

3 * $C_{AB} = 19 = (K_{SA})^{e_B} \bmod N_B \rightarrow \boxed{K_{SA} = C_{AB}^{d_B} \bmod N_B = 19^7 \bmod 33 = 13}$

$K_{SA} = 00\,1101$

3 * $C_{BA} = 53 = (K_{SB})^{e_A} \bmod N_A \rightarrow \boxed{K_{SB} = C_{BA}^{d_A} \bmod N_A = 53^{43} \bmod 77 = 25}$

$K_{SB} = 011001$

3 * $M_1 = 000000\,|\,000010 \longrightarrow \oplus \longrightarrow C_1 = 001101\,|\,011011$

$K_S = 001101\,|\,011001$

$M_2 = 001100\,|\,100101 \longrightarrow \oplus \longrightarrow C_2 = 000001\,|\,111100$

A envía dos subcriptogramas, al haber partido M en dos bloques de 12 bits cada uno.

$C'_{AB} = \underbrace{001101\,011011}_{C_1} \,\|\, \underbrace{000001\,111100}_{C_2}$

(3) $N = p \cdot q = 387833$

$\phi(N) = (p-1)\cdot(q-1) = pq - (p+q) + 1$

$\phi(N) = 386448$

$p+q = pq - \phi(N) + 1$

$\boxed{p+q = N - \phi(N) + 1}$ 2'5

$(p+q)^2 = p^2 + q^2 + 2pq$

$-\ (p-q)^2 = p^2 + q^2 - 2pq$

$(p+q)^2 - (p-q)^2 = 4pq \rightarrow \boxed{(p+q)^2 = (p-q)^2 + 4\cdot N}$ 2'5

$p+q = 387833 - 386448 + 1 = 1386$

$1386^2 = (p-q)^2 + 4\cdot 387833$

$p-q = 608$

$p+q = 1386$
$p-q = 608$
$\Big\} \boxed{\begin{array}{l} p = 997 \\ q = 389 \end{array}}$ 2'5

(4) a) 2'5

$p(6) = 2\cdot p(1) = 2p$

$p(1) = p(2) = p(3) = p(4) = p(5) = p$

$\Big\} \sum_{i=1}^{6} p(i) = 1 \quad 7p = 1 \quad p = \frac{1}{7}$

$H(\text{dado truncado}) = H(dt) = \frac{2}{7}\log_2\frac{7}{2} + 5\cdot\frac{1}{7}\log_2 7 = 2'5216 \ \frac{\text{bits}}{\text{símbolo}}$

2'5 b) $H(\text{dado normal}) = H(dn) = 6\cdot\frac{1}{6}\log_2\frac{1}{1/6} = \log_2 6 = 2'5849 \ \frac{\text{bits}}{\text{símbolo}}$

($p(i) = \frac{1}{6}$)

2'5 c) Cuando las probabilidades son muy dispersas (unos eventos[1] muy probables y otros eventos poco probables) la entropía de la fuente disminuye.

En el límite, para esta fuente "dado truncado",

$p(6) = 1$, $p(1) = p(2) = p(3) = p(4) = p(5) = 0 \Rightarrow H = 0 \ \frac{\text{bits}}{\text{símb.}}$

No hay incertidumbre, fuente determinista.

(1) "evento" para la fuente "dado" es el resultado obtenido al lanzarlo.

(5) * Denominación de Sucesos:

"Nadal gana" = N_g "Hace sol" = S

"Nadal pierde" = N_p "No hace sol" = nS

Variables aleatorias:

N → resultado partido

t → tiempo que hace

$P(N\backslash t)$	$N=N_g$	$N=N_p$
$t=S$	0'7	0'3
$t=nS$	0'3	0'7

Si $p(N_g\backslash S)=0'7 \Rightarrow P(N_p\backslash S)=0'3$

Si $p(N_g\backslash nS)=0'3 \Rightarrow p(N_p\backslash nS)=0'7$

$$p(N,t) = p(N\backslash t)\cdot p(t)$$

$p(N,t)$	$N=N_g$	$N=N_p$
$t=S$	$0'7\cdot 0'2$	$0'3\cdot 0'2$
$t=nS$	$0'3\cdot 0'8$	$0'7\cdot 0'8$

$p(t=S)=0'2$

$p(t=nS)=0'8$

8 t's a) $H(N)=\sum_{i=1}^{2} P(N_i)\cdot \log_2 \frac{1}{p(N_i)}$ $\quad p(N_j)=\sum_{i=1}^{2} p(N_j,t_i)$

$p(N_g) = 0'7\cdot 0'2 + 0'3\cdot 0'8 = 0'38$

$p(N_p) = 0'3\cdot 0'2 + 0'7\cdot 0'8 = 0'62 = 1-p(N_g)$

$$H(N) = 0'38 \log_2 \frac{1}{0'38} + 0'62 \log_2 \frac{1}{0'62} = 0'9580 \text{ bits/símbolo}$$

7's

8's b) $H(N\backslash t) = H(N\backslash S)\cdot p(S) + H(N\backslash nS)\cdot p(nS) = 0'8813 \frac{\text{bits}}{\text{símbolo}}$

($p(S)=0'2$, $p(nS)=0'8$)

$0'2 \log_2 \frac{1}{0'7} + 0'3\cdot \log_2 \frac{1}{0'3} = 0'8813$

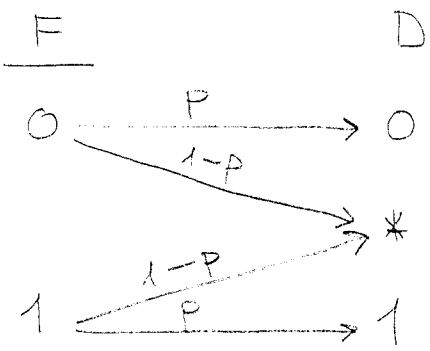
8 c) $I(N;t) = H(N) - H(N\backslash t) = 0'07675 \text{ bits/símbolo}$

(fórmula = 3)

Binary Erasure Channel (BEC)

⑥

5 a)



$$p(D|F) = \begin{array}{c} \\ 0 \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & * & 1 \end{array} \\ \begin{pmatrix} p & 1-p & 0 \\ 0 & 1-p & p \end{pmatrix} \end{array}$$

b) $C = \max_{F} \left[H(D) - H(D|F) \right]$

4 * $H(D|F) = H(D|0)\cdot p(0) + H(D|1)\cdot p(1) = p\cdot \log_2 \frac{1}{p} + (1-p)\cdot \log_2 \frac{1}{1-p} = H(p)$

$H(D|0) = p\log_2 \frac{1}{p} + (1-p)\cdot \log_2 \frac{1}{1-p} + 0$; $p(0)+p(1)=1$

4 * $H(D) = \sum_{i} p(D_i)\cdot \log_2 \frac{1}{p(D_i)} = px \log_2 \frac{1}{px} + (1-p)\log_2 \frac{1}{1-p} + p(1-x)\log_2 \frac{1}{p(1-x)}$

$p(F=0) = x$

$p(D=0) = p\cdot p(F=0) = p\cdot x$

$p(D=*) = p(F=0)\cdot(1-p) + p(F=1)\cdot(1-p) = 1-p$

$p(D=1) = p\cdot p(F=1) = p\cdot(1-x)$

$p(F=0)+p(F=1)=1$

4 * $C(x) = \max_{x} \left[px \log_2 \frac{1}{px} + p(1-x)\log_2 \frac{1}{p(1-x)} \right] + (1-p)\log_2 \frac{1}{1-p} - H(p)$

4 * $C'(x) = p\log_2 \frac{1}{px} + (px)^2 \cdot \frac{-1}{(px)^2}\cdot p\cdot \frac{1}{\ln 2} + (-p)\cdot \log_2 \frac{1}{p(1-x)} + p^2(1-x)^2 \cdot \frac{-1}{p^2(1-x)^2}\cdot(-p)\cdot \frac{1}{\ln 2} =$

$= p\log_2 \frac{1}{px} - \frac{p}{\ln 2} - p\log_2 \frac{1}{p(1-x)} + \frac{p}{\ln 2} = 0$

$p\cdot\left(\log_2 \frac{1}{px} - \log_2 \frac{1}{p(1-x)} \right) = 0$;; $p\cdot \log_2 \frac{p(1-x)}{px} = 0$

$\frac{p(1-x)}{px} = 1 \Rightarrow 1-x = x \Rightarrow 2x = 1 \Rightarrow \boxed{x = \frac{1}{2} = p(F=0)}$

1 * $\boxed{C = C\left(x=\frac{1}{2}\right)} = \frac{p}{2}\left(\log_2 \frac{2}{p}\right)\cdot 2 + (1-p)\cdot \log_2 \frac{1}{1-p} - H(p) =$

$= p\left(\log_2 2 - \log_2 p\right) + (1-p)\cdot \log_2 \frac{1}{1-p} - H(p) =$

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

$-p\cdot\log_2 p = p\cdot \log_2 p^{-1}$

$= p + p\cdot \log_2 \frac{1}{p} + (1-p)\cdot \log_2 \frac{1}{1-p} - H(p) = \boxed{p}$ bits/simbolo