CONTROL DE TRANSMISIÓN DE DATOS. 2 de diciembre 2005

GRUPO 40

DURACIÓN: 100 MINUTOS

Jordi Forné

Notas Importantes:

Un error conceptual grave, puede anular todo el problema.

Problema 1 (50%)

Sean $F_1=\{1, 2, 3, 4\}$ y $F_2=\{2, 4, 6, 8\}$ dos fuentes equiprobables independientes. Sea una fuente (F) cuya salida es el mínimo común múltiplo de la salida de las fuentes anteriores $F = \text{mcm}(F_1, F_2)$.

a) Calcule la entropía de la fuente H(F). **(1 punto)**

b) Calcule la información mutua $I(F, F_1)$ **(1 punto)**

c) Calcule la longitud media de una codificación de Huffman de la fuente F. **(1 punto)**

d) Suponga que le proponen adivinar F, y como ayuda le dejan escoger entre conocer F_1 o conocer F_2. ¿Qué opción preferiría? Justifique la respuesta y calcule la probabilidad de adivinar F con la opción que ha escogido anteriormente. **(2 puntos)**

Problema 2 (50%)

Tenemos dos usuarios, **A:** $p_A = 563$, $q_A = 991$, $e_A = 31$ y **B:** $p_B = 401$, $q_B = 677$, ($d_B =$ 105.497).

Usarán RSA para intercambiarse una clave de sesión del DES. Para ello el usuario A genera una clave 0x 10BD FA8C 9022 DE83 que envía a B. El cifrado se hace en cuatro bloques de 16 bits.

NOTA: Deberá usar obligatoriamente el algoritmo extendido de Euclides para el cálculo de inversos y el algoritmo de exponenciación rápida para el cálculo de la cifra.

a) ¿Qué tamaño máximo de bloque de clave K_i en bits podrían intercambiarse A y B? **(1,5 puntos).**

b) Exprese en valores (sin calcularla) la ecuación del primer bloque de clave K_1 que A envía a B. **(1,5 puntos)**

c) Calcule el valor del primer bloque (K_1) de clave cifrada que A envía a B. **(2 puntos)**

Datos de interés:

Operaciones en mod 271.477:

$4.285^2 = 172.266$	$172.266^2 = 152.409$	$152.409^2 = 116.730$
$116.730^2 = 190.793$	$190.793^2 = 160.873$	$160.873^2 = 219.719$
$219.719^2 = 227.005$	$227.005^2 = 48.839$	$48.839^2 = 50.999$
$50.999^2 = 148.341$	$148.341^2 = 212.569$	$212.569^2 = 133.450$
$133.450^2 = 11.300$	$11.300^2 = 95.810$	$95.810^2 = 104.299$

$(104.299)*(148.341)*(160.873)*(116.730) = 160.873$

Otros datos de interés: 33.833 = 1000010000101001; 10BD = 1000010111101 = 4.285

$2^{15} = 32.768$; $2^{16} = 65.536$; $2^{17} = 131.072$; $2^{18} = 262.144$; $2^{19} = 524.288$; $2^{20} = 1.048.576$

$P(2) = 1/8$

$P(4) = 1/4$ a) $\boxed{H(F) = 2'453}$ (1)

$P(6) = 1/4$ b) $\boxed{I(F, F_1) = 0'703}$ (1)

$P(8) = 3/16$ $\boxed{c)\ \bar{l} = 2'5}$ (1)

$P(12) = 1/8$ d) $\boxed{H(F|F_2) = 0'98325 < H(F|F_1) = 1'75}$
Escogería F_2 (1)

$P(24) = 1/16$ $\boxed{P(\text{adivinar}) = \frac{11}{16} = 0'6875}$ (1)

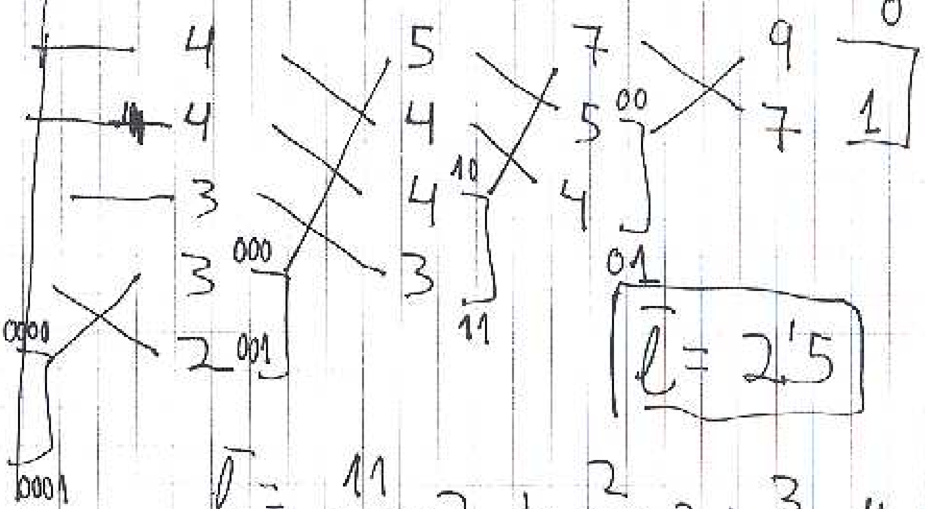
b) $\boxed{I(F, F_1)} = H(F) - H(F/F_1) = 2'453 - 1'75 = 0'70$

$H(F|F_1)$ $F_1 = \begin{cases} 1 & H(F|1) = 2 \\ 2 & H(F|2) = 2 \\ 3 & H(F|3) = \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 + \frac{1}{4}\cdot 2 = 1'5 \\ 4 & H(F|3) = 1'5 \end{cases}$

$H(F|F1) = \frac{1}{2}\cdot 2 + \frac{1}{2}\cdot 1'5 = 1'75$ ~~= 0'703~~

c)

	S_k	$p(s_k)$	$p/16$
(01)	4	4/16	4
(10)	6	4/16	4
(11)	8	3/16	3
(001)	2	2/16	3
(0000)	12	2/16	2
(0001)	24	1/16	



$\boxed{\bar{l} = 2'5}$

$\bar{l} = \frac{11}{16}\cdot 2 + \frac{2}{16}\cdot 3 + \frac{3}{16}\cdot 4 = \frac{40}{16} =$

d) $H(F|F_1) = 1'75$

$H(F|F_2) = 0'98325$

$$F_2 = \begin{cases} 2 & H(F|2) = 1'5 \\ 4 & H(F|4) = \frac{3}{4}\log_2\left(\frac{4}{3}\right) + \frac{1}{4}\cdot 2 = 0'811 \\ 6 & H(F|6) = 0'811 \\ 8 & H(F|8) = 0'811 \end{cases}$$

	ESCOJO		P (ADIVINAR)
$F_2 = 2$	$\longrightarrow$	$F = 2$	$1/2$
$F_2 = 4$	$\longrightarrow$	$F = 4$	$3/4$
$F_2 = 6$	$\longrightarrow$	$F = 6$	$3/4$
$F_2 = 8$	$\longrightarrow$	$F = 8$	$3/4$

$$\boxed{P(\text{ADIVINAR})} = \frac{1}{4}\cdot\frac{2}{4} + \frac{3}{4}\cdot\frac{3}{4} = \boxed{\frac{11}{16}} = \boxed{0'6875}$$

PROBLEMA 2 CONTROL

Tenemos dos usuarios, **A**: $p_A = 563$, $q_A = 991$, $e_A = 31$ y **B**: $p_B = 401$, $q_B = 677$, ($d_B =$ 105.497).

Usarán RSA para intercambiarse una clave de sesión del DES. Para ello el usuario A genera una clave 0x 10BD FA8C 9022 DE83 que envía a B. La cifra se hace en cuatro bloques de 16 bits.

NOTA: Deberá usar <u>obligatoriamente</u> el algoritmo extendido de Euclides para el cálculo de inversos y el algoritmo de exponenciación rápida para el cálculo de la cifra.

a) Exprese en valores (sin calcularla) la ecuación del primer bloque de clave K_1 que A envía a B.

a) Calcule el valor del primer bloque (K_1) de clave cifrada que A envía a B.

b) ¿Qué tamaño máximo de bloque de clave K_i en bits podrían intercambiarse A y B?

<u>Datos del examen:</u>

Operaciones en mod 271.477:

$4.285^2 = 172.266$	$172.266^2 = 152.409$	$152.409^2 = 116.730$
$116.730^2 = 190.793$	$190.793^2 = 160.873$	$160.873^2 = 219.719$
$219.719^2 = 227.005$	$227.005^2 = 48.839$	$48.839^2 = 50.999$
$50.999^2 = 148.341$	$148.341^2 = 212.569$	$212.569^2 = 133.450$
$133.450^2 = 11.300$	$11.300^2 = 95.810$	$95.810^2 = 104.299$

$(104.299)*(148.341)*(160.873)*(116.730) = 160.873$

<u>Otros datos de interés:</u> 33.833 = 1000010000101001; 10BD = 1000010111101 = 4.285

$2^{15} = 32.768$; $2^{16} = 65.536$; $2^{17} = 131.072$; $2^{18} = 262.144$; $2^{19} = 524.288$; $2^{20} =$ 1.048.576

SOLUCIÓN:

a) La ecuación de envio del bloque 1 de la clave K desde A hacia B será: $K_1^{eB} \bmod n_B$

Conocemos el valor de K_1 en hexadecimal = 10BD = 1000010111101 = 4.285

$n_B = p_B*q_B = 401*677 = 271.447$. Nos falta conocer la clave pública de B, $e_B = \text{inv}\,[d_B, \phi(n_B)]$.

Como $\phi(n_B) = (p_B -1)*(q_B -1) = 400*676 = 270.400 \Rightarrow e_B = \text{inv}\,[d_B, \phi(n_B)] = \text{inv}\,(105.497, 270.400)$

Usando el algoritmo extendido de Euclides:

i	y_i	g_i	u_i	v_i	<u>Algoritmo</u>: (apuntes de clase)
0	-	270.400	1	0	x = inv (A, B)
1	-	105.497	0	1	$(g_0, g_1, u_0, u_1, v_0, v_1, i) = (B,A,1,0,0,1,1)$
2	2	59.406	1	-2	Mientras $g_i \neq 0$ hacer
3	1	46.091	-1	3	y_{i+1} = parte entera (g_{i-1}/g_i)
4	1	13.315	2	-5	$g_{i+1} = g_{i-1} - y_{i+1}*g_i$
5	3	6.146	-7	18	$u_{i+1} = u_{i-1} - y_{i+1}*u_i$
6	2	1.023	14	-41	$v_{i+1} = v_{i-1} - y_{i+1}*v_i$
7	6	8	-91	264	$i = i+1$
8	127	7	11.571	–33.569	Hacer $x = v_{i-1}$
9	1	1	-11.662	**<u>33.833</u>**	
[redacted]					
10	7	0			

Clave pública e_B = inv (105.497, 270.400) = 33.833 (aparece en los datos)

La ecuación del primer bloque de clave con valores será: $K_1^{eB} \bmod n_B = 4.285^{33.833}$ mod 271.477.

a) Como dato tenemos 33.833 = 1000010000101001 =

c) $\mathbf{b_{15}}b_{14}b_{13}b_{12}b_{11}\mathbf{b_{10}}b_9b_8b_7b_6\mathbf{b_5}b_4\mathbf{b_3}b_2b_1\mathbf{b_0}$,

j	**0**	1	2	**3**	4	**5**	6	7	8	9	**10**	11	12	13	14	**15**

j

4.285^2 (los valores desde j = 1 hasta j = 15 están en los datos)

Multiplicamos sólo los bits con valor 1 (en negrita) es decir: $b_{15}b_{10}b_5b_3b_0$ mod 271.477.
Según los datos que se entregan en el examen, esta multiplicación será:
K_1 = (104.299)*(148.341)*(160.873)*(116.730)*4.285 = 160.873*4.285 mod 271.477
K_1 = 160.873*4.285 mod 271.477 = 60.702.
[redacted]

c) Como $n_A = p_A*q_A$ = 653*991 = 557.933 y $n_B = p_B*q_B$ = 401*677 = 271.477, viendo los datos entregados en el examen, A puede enviar a B un bloque máximo de 18 bits (2^{18} < 271.477 < 2^{19}), en cambio B puede enviar a A un bloque máximo de 19 bits (2^{19} < 557.933 < 2^{20}). Por lo tanto la clave de B fuerza a que el intercambio de bloques de clave sea como máximo de 18 bits. [redacted]

APARTADO a CONTRA