CONTROL DE TRANSMISIÓN DE DATOS. **20 de mayo de 2005**

GRUPO 50

DURACIÓN: 100 MINUTOS

J. Forné

Notas Importantes:

Un error conceptual grave, puede anular todo el problema.

Problema 1 (50%)

Sea una fuente (F) generada por la suma módulo 3 de la salida de 3 fuentes binarias equiprobables (F_1, F_2 y F_3).

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

b) Calcule y $H(F_1/F)$ y $H(F/F_1)$. **(1 punto)**

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

d) Calcule el tiempo mínimo para poder transmitir 500.000 símbolos de fuente por un canal con W = 30 KHz y S/N = 15 a la entrada del receptor (en escala lineal). **(1 punto)**

e) Realice una codificación de Huffman de la fuente extendida de orden 2 (F^2). Calcule la longitud media del código. **(1 punto)**

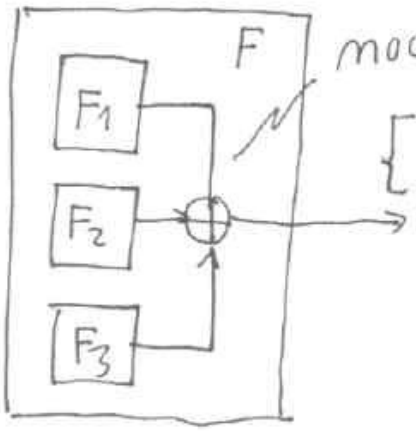
Problema 2 (50%)

a) Sea un sistema RSA con los siguientes parámetros para un usuario A (p=47, q=59, d=157). Para la codificación de los mensajes de texto, sustituimos cada letra por un número de 2 dígitos según la siguiente codificación: espacio=00, A=01, B=02, ..., Z=26 y codificamos 2 letras por bloque. Codifique el mensaje M="IT" para transmitirlo confidencialmente al usuario A. **(2 puntos)**

b) Realice un cifrado de Vigènere del mensaje M="HOLA" con la clave obtenida al descifrar el criptograma generado en el apartado anterior con la clave privada de A. **(1 punto)**

c) El conocimiento de la función de Euler $\phi(n)$ permite factorizar n en un sistema RSA. Factorice $n = p \cdot q = 2782799$ sabiendo que $\phi(n) = 2779440$. AYUDA: Obtenga $p+q$ como una cierta función de n y $\phi(n)$. Utilice la identidad $(p-q)^2 = (p+q)^2 - 4p \cdot q$. **(2 puntos)**

PROBLEMA 1



$\{0,1,2\}$ F_i fuente binaria equiprob.

$P(0) = p(1) = 1/2$

F_1	F_2	F_3	F
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
1	0	0	1
1	0	1	2
1	1	0	2
1	1	1	0

$P(0) = \frac{1}{4}$

$P(1) = P(2) = \frac{3}{8}$

F no tiene memoria

a) $\boxed{H(F)} = \frac{1}{4}\log_2 4 + 2\cdot\frac{3}{8}\log_2\left(\frac{8}{3}\right) =$

$= \frac{1}{4}\,2 + \frac{3}{4}\,\frac{1}{\log 2}\cdot\log\left(\frac{8}{3}\right) = \frac{1}{2} + 1'061 = \boxed{1'561 \text{ bits}}$

b) $\boxed{H(F_1|F)} = P(F=0)\cdot H(F_1/F=0) + P(F=1)\cdot H(F_1|F=1) +$

$+ P(F=2)\cdot H(F_1|2)$

$= \frac{1}{4}\cdot 1 + \frac{3}{8}\cdot 2\cdot 0'9183 = \boxed{0'9387 \text{ bits}}$

$F=0 \quad H(F_1|0) = H(1/2) = 1$ bit

$F=1 \quad H(F_1|1) = H(1/3) = \frac{1}{3}\log_2 3 + \frac{2}{3}\log_2 \frac{3}{2} = 0'918$

$F=2 \quad H(F_1|2) = H(1/3) = 0'9183$

$$H(F|F_1) = P(F\neq 0)\, H(F|0) + P(F_1=1)\, H(F|1) = 1'5$$

$$H(F|0) = \frac{1}{4}\log_2 4 + \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1'5$$

$F_1=0 \quad F=0 \ (P=1/4) \quad F=1 \ P(1/2) \quad F=2 \ P(1/4)$

$H(F|1) = 1'5$

c) $I(F, F_1) = I(F_1|F) = H(F_1) - H(F_1|F) =$

$= 1 - 0'9387 = 0'0613 = H(F) - H(F|F_1)$

d) $V_t \leq C = W \log_2 \left(1 + \frac{S}{N}\right) = 30\cdot 10^3 \log_2 16 = 1'2\cdot 10^4$

$I \geq H(F)\cdot 500.000$

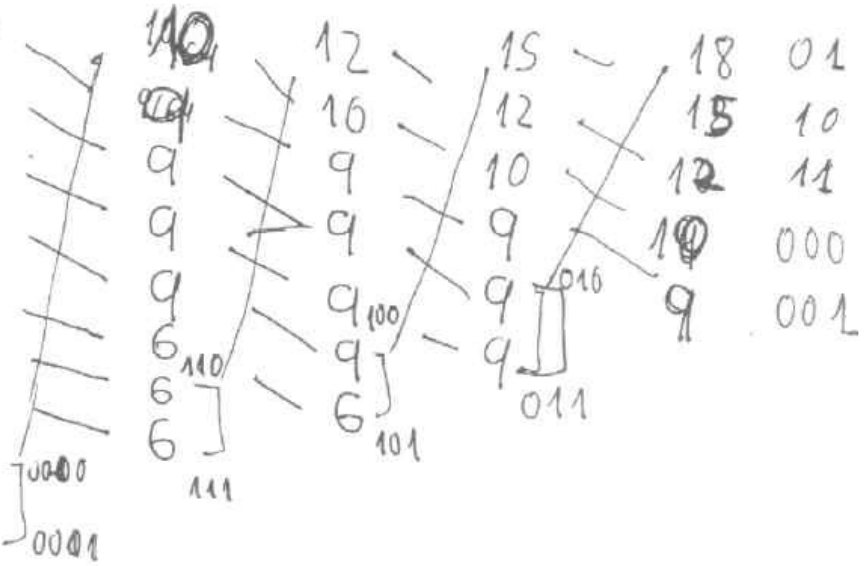
$$\frac{I}{t_{min}} \leq C \Rightarrow t_{min} = \frac{500.000 \cdot 1'561}{1'2\cdot 10^4}$$

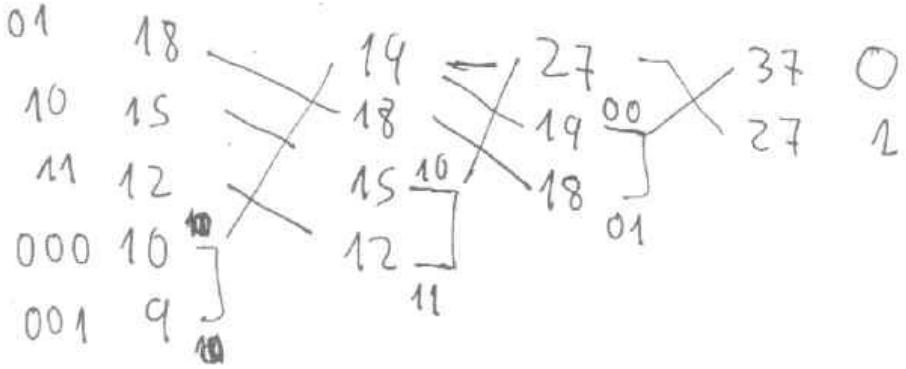
$$t_{min} \simeq 6'505 \text{ s}$$

PROB 1

e) F^2_{si} P_i

(0011) – 22 – 9/64
(0010) – 21 – 9/64
(0111) – 12 – 9/64
(0100) – 11 – 9/64
(1012) – 10 – 6/64
(1110) – 01 – 6/64
(1111) – 20 – 6/64
(00020) – 02 – 6/64
(00012) – 00 – 4/64





$$\bar{l} = 4 \cdot \frac{10}{64} + 3 \cdot \frac{54}{64} = \frac{202}{64} = 3'1562S \text{ bits/símbolo}$$

PROB 2

a) e=17; C=948

b) C = ΦHUU

c) p=1879; q=1481

PROB 2

RSA

a) $p = 47$; $q = 59$

$n = p \cdot q = 47 \cdot 59 = 2773$

$d = 157$ $\quad \phi(2773) = 46 \cdot 58 = 2668$

$\boxed{e = 17}$

blank = 00

A = 01, B = 02, ..., I = 09; T = 20

$m = 0920$ $\quad M = 920$

$\boxed{C = M^{17} = 948}$

FACT

c) $N = 1879 \cdot 1481 = 2.782.799$

$\phi(N) = 1878 \cdot 1480 = 2\,779\,440$

→ Factorize N

$p + q = n - \phi(n) + 1 = 3360$

$p - q = \sqrt{(p+q)^2 - 4pq} = \sqrt{(3360)^2 - 4 \cdot 2.782799}$

$= \sqrt{11289600} = 398$

$2p = (p+q) + (p-q) = 3758 \Rightarrow \boxed{p = 1879}$

$\boxed{q = 1481}$

b) HOLA
ITIT

8 15 12 1
9 20 9 20
17 35 21 21 mod 27

0 1 2 3 4 5 10 15 20 25
_ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C = Q H U U