CONTROL DE TRANSMISIÓN DE DATOS. 11 de diciembre de 2008

Problema 1. CODIFICACIÓN DE FUENTE (50%)

Sea dos fuentes ternarias equiprobables e independientes F_1={1, 2, 3} F_2={1, 2, 3} Sea una fuente (F) cuya salida vale: $F(i) = F_1(i) \cdot F_2(i) \bmod 7$. Sea un canal C cuyo alfabeto de entrada y salida está compuesto por los símbolos {A, B, C}, y su modelo estadístico corresponde a la figura 1.

a) Calcule la entropía de la fuente F.

b) Realice una codificación de Huffman ternaria de la fuente F para su transmisión sobre el canal C. Calcule la longitud media de codificación.

c) Calcule la capacidad de canal en función de p. NOTA: Por comodidad, llame $H(p) = -p \cdot \log_2 p - (1-p) \cdot \log_2 (1-p)$

d) Calcule los valores máximo y mínimo de la capacidad de canal. Dibuje una gráfica de la capacidad de canal en función de p.

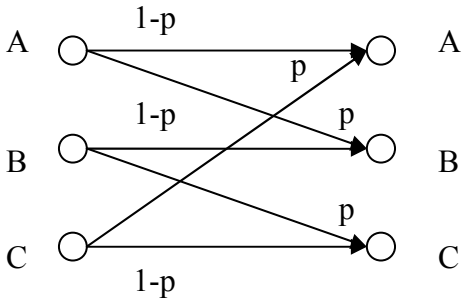


Figura 1

Problema 2. CRITOGRAFÍA (50%)

Sea un sistema RSA con los siguientes datos:

	Clave de **A**lice	Clave de **B**ob
Primo p	47	37
Primo q	83	19
Clave pública e	13	13

Se pide:

a) Usando el algoritmo de exponenciación rápida cifre el mensaje "A" que Bob desea enviar de forma confidencial a Alice. Calcule el valor del criptograma C en hexadecimal. Use codificación ASCII: A_{ASCII} = 0100 0001

b) Cifre el mensaje $M=23_H$ (codificación hexadecimal) mediante un cifrado de Vernam utilizando como clave k la decodificación por Alice del criptograma generado en el apartado anterior.

c) Calcule la firma de Bob sobre el mensaje "B". Suponga que H(M)=00000111. (B_{ASCII} = 0100 0010).

d) Calcule $X = 2156^{3774} \bmod 3901$

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Cognoms JORDI FORNÉ Nom

Centre

Assignatura / especialitat

DNI Núm. matrícula Curs Grup Data

PROBLEMA 1

a]

F_1	F_2	F
1	1	1
1	2	2
1	3	3
2	1	2
2	2	4
2	3	6
3	1	3
3	2	6
3	3	2

$F = \{1, 2, 3, 4, 6\}$

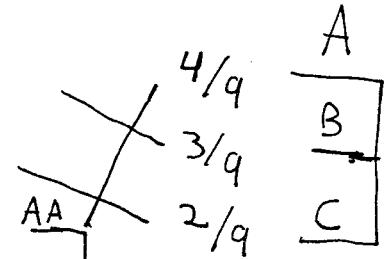
$P(S_i) = 1/9 \quad 3/9 \quad 2/9 \quad 1/9 \quad 2/9$

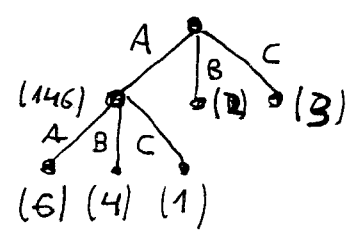
$$H(F) = \sum_i p_i \log_2 \frac{1}{p_i} = 2 \cdot \frac{1}{9} \log_2 9 + 2 \cdot \frac{2}{9} \log_2 \frac{9}{2} + \frac{3}{9} \log_2 3$$

$$= 2'197 \text{ bits}$$

b]

F	P
B - (2)	3/9
C - (3)	2/9
AA - (6)	2/9
AB - (4)	1/9
AC - (1)	1/9

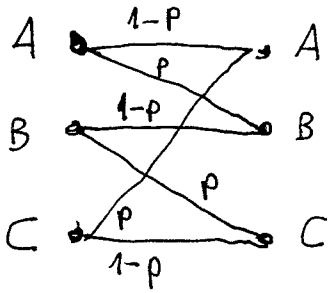




$$\bar{l} = \frac{5}{9} \cdot 1 + \frac{4}{9} \cdot 2 = \frac{13}{9} = 1'\hat{4}$$

dígitos

c]



$$C = \max \{ I(X;Y) \}$$

$$I(Y;X) = H(Y) - H(Y/X)$$

$$H(Y/X) = H(p)$$

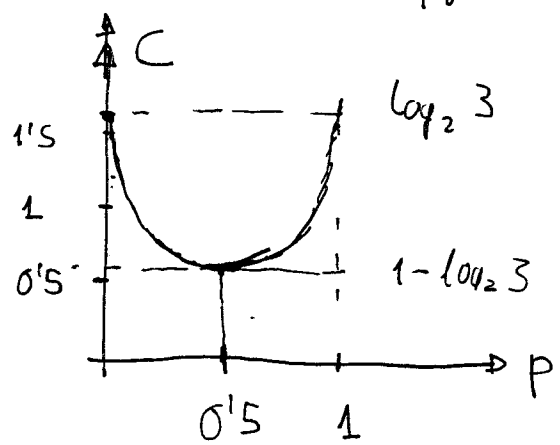
↳ v.a dos salidas, con probabilidades $(p;\ 1-p)$

$$C = \max \{ I(X;Y) \} = \max \{ H(Y) \} - H(p) =$$

$$\boxed{C = \log_2 3 - H(p)}$$

d] $C_{max} = \log_2 3 = 1'58$ bits

$C_{min} = \log_2 3 - 1 = 0'58$ bits



Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. | Full núm.
Nombre total de fulls

Cognoms | Nom
Centre
Assignatura / especialitat
DNI | Núm. matrícula | Curs | Grup | Data

PROBLEMA 2

a) $p_A : \quad e_A = 13 \qquad \boxed{N_A = p_A \cdot q_A = 47 \cdot 83 = 3901}$

$$\boxed{C = M^{e_A} \bmod N_A = 65^{13} \bmod 3901 = 3527}$$

$$\boxed{C = DC7_H}$$

b) $m = 00100011$
$k = 01000001$
$C = 01100010 \qquad \boxed{C = 62_H}$

c) $H(m) = 7$

$$FIRMA = E_{S_A}(H(m)) = (H(m))^{d_B} \bmod N_B$$
$$= 7^{d_B} \bmod N_B$$

CALCULO CLAVE

I) $N_B = p_B q_B = 37 \cdot 19 = 703$

II) $\phi(N_B) = (p_B - 1)(q_B - 1) = 36 \cdot 18 = 648$

III) $d_B = e_B^{-1} \bmod \phi(N_B) = 13^{-1} \bmod 648$

$$13 d_B = k \cdot 648 + 1$$

$$648 = 1 \cdot 648 + 0 \cdot 13$$
$$\times(-49) \quad 13 = 0 \cdot 648 + 1 \cdot 13$$
$$\times(-1) \quad 11 = 1 \cdot 648 + (49) \cdot 13$$
$$\times(-5) \quad 2 = (-1) \cdot 648 + 50 \cdot 13$$
$$1 = 6 \cdot 648 + \underbrace{(-299)}_{d_B} \cdot 13$$

$$\boxed{d_B = -299 \bmod 648 = 349}$$

$$\boxed{FIRMA = 7^{349} \bmod 703 = 330}$$

$$\boxed{FIRMA = 14A_H}$$

d) $X = 2156^{3774} \bmod 3901$

(apartado a):) $N_A = 3901 = 47 \cdot 83$

$\phi(N_A) = 46 \cdot 82 = 3772$

$$\boxed{X = 2156^{3774} \bmod 3901 = 2156^{\phi(3901)+2} \bmod 3901 =}$$

$$= 2156^2 \bmod 3901 = \boxed{2245}$$