Ejercicio 1 **(50%)**

Sea una fuente binaria equiprobable F_1={-1, 1}. Sea una fuente (F) cuya salida es la suma del símbolo actual y el símbolo anterior de F_1, es decir, el símbolo de F en el instante i vale: $F(i) = F_1(i) + F_1(i-1)$

a) Calcule la eficiencia de una codificación de Huffman de la fuente F, suponiendo que F no tiene memoria. **(1 punto)**

b) Determine un modelo markoviano de F y calcule la eficiencia de una codificación de Huffman de F (suponiendo memoria 1) **(2 puntos)**

c) Decodifique la secuencia 2332712 generada por una codificación LZW de una secuencia de símbolos de F (el diccionario inicial contiene -2, 0 y 2 en las posiciones 1, 2 y 3 respectivamente). **(1 punto)**

d) Suponiendo que $F_1(-1) = -1$, obtenga el valor de la secuencia de símbolos de F_1 que generaron la secuencia decodificada en el apartado anterior. **(1 punto)**

Ejercicio 2 (50%)

En un sistema simple de clave pública RSA se emplea una entidad de certificación (EC) para verificar las claves públicas de las entidades que intervienen en él. Estas entidades quedan identificadas por un valor numérico de 8 bits que se asigna arbitrariamente. El sistema utiliza de forma universal el mismo valor e = 39 en todas las claves públicas, incluida la EC, por lo que las claves públicas se reducen a un único valor n expresado con 12 bits.

Se ha averiguado que en este sistema todas las claves públicas disponen de un mismo factor primo p y que la función resumen empleada es una reducción modular en un cuerpo conmutativo Z_m.

Sabiendo que la clave pública de la EC es Kp_{EC} = 3403 y que un certificado de una entidad A, cuyo identificador es Id_A, tiene por valor en decimal:

$$Id_A \mid Kp_A \mid F_{KsEC}(R\,[Id_A|Kp_A]) = 0 \mid 2407 \mid 383$$

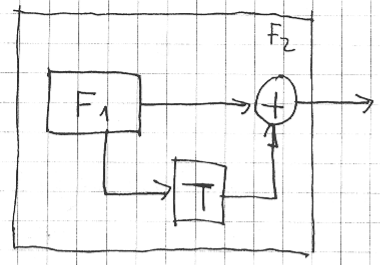
a) calcule el factor primo p **(1 punto)**

b) halle la clave secreta (Ks_{EC}) de la EC mediante el algoritmo extendido de Euclides **(2 puntos)**

c) determine el valor del resumen $R[Id_A|Kp_A]$ **(1 punto)**

d) obtenga el valor de m **(1 punto)**

PROBLEMA 1



$F(i) = F_1(i) + F_1(i-1)$

a]

	$F_1(i)$	$F_1(i-1)$	F
equiprob	-1	-1	-2
	-1	+1	0
	+1	-1	0
	+1	+1	2

SIMBOLOS DE F $\left\{ \underset{\frac{1}{4}}{-2}, \underset{\frac{1}{2}}{0}, \underset{\frac{1}{4}}{2} \right\}$

$p = 1/4 \quad p = 1/2 \quad p = 1/4$

$$H(F) = \frac{1}{2}\log_2 2 + 2 \cdot \frac{1}{4}\log_2 4 = 1'5 \text{ bits}$$

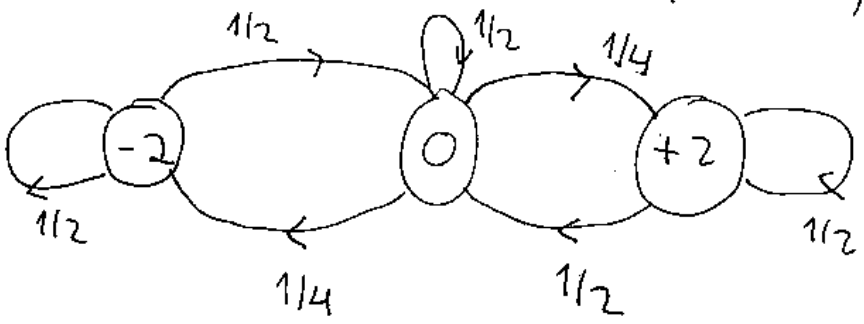
HUFFMAN

0	→	0
-2	→	10
+2	→	11

$\bar{l} = 1'5$

$$E = \frac{H(F)}{\bar{l}} = 1$$

b] MODELO MARKOVIANO (observando tabla apartado a)



$H(F) = P(-2)\, H(F|-2) + P(0)\, H(F/0) + P(2)\, H F(2)$

$H(F/-2) = H(F|2) = H(1/2) = 1$

$H(F/0) = H(1/2, 1/4, 1/4) = 1'5$

$\boxed{H(F) = \frac{1}{4} \cdot 1 + \frac{1}{2}\, 1'5 + \frac{1}{4} \cdot 1 = 1'25}$

$\bar{l}$ igual que en apartado anterior, pues Huffman no considera memoria de fuente

$\bar{l} = 1'5$

$$\boxed{E = \frac{H(F)}{\bar{l}} = \frac{1'25}{1'50} = 0'833}$$

DNI

PROB 1 (cont)

c) (2) (3) (3) (2) (7) (1) (2)

ENTRADA	DICC	SALIDA
(2)	—	0
(3)	(4) 0 2	+2
(3)	(5) 2 2	+2
(2)	(6) 2 0	0
(7)	(7) 0 0	0 0
(1)	(8) 0 0 -2	-2
(2)	(9) -2 0	0

(1)	-2
(2)	0
(3)	+2

SALIDA: 0 2 2 0 0 0 -2 0

d)

n:	-1	0	1	2	3	4	5	6	7
F:		0	2	2	0	0	0	-2	0
F_1	-1	+1	+1	+1	-1	+1	-1	-1	+1

$F_1(n) = F(n) - F_1(n-1)$

$F_1(n)$: +1 +1 +1 -1 +1 -1 -1 +1

Ejercicio 2

a) $k_{P_{EC}} = p \cdot q_{EC} = 3403 = 83.41$

$k_{P_A} = p \cdot q_A = 2407 = 83.29$

Para hallar p aplicamos el algoritmo de Euclides

3403	2407		2407	996		996	415		415	166	
996	1		415	2		166	2		83	2	
996	415		415	166		166	83	← m.c.d			
166	2		83	2		0					

b) $k_{S_{EC}} = (d, n) = (d, 3403)$

$n = 3403 = 83.41$

$\Phi(n) = 3280$

$d \cdot e = 1 + k \Phi(n)$

$k_1 e + k_2 \cdot \Phi(n) = 1$

Aplicando Euclides extendido se obtiene: $\boxed{d = 2439}$

Verificación: $e \cdot d \bmod \Phi(n) = 95121 \bmod 3280 = 1$

c) $R[Id_A ; k_{P_A}] = F^{-1}_{k_{SEC}}(383)$

$R[Id_A ; k_{P_A}] = 383^{e_{EC}} \bmod n_{EC} = 383^{39} \bmod 3403$

$= (((383^2)^2)^2 \cdot 383)^2 \cdot 383 \bmod 3403 = 3$

d) $R[Id_A ; k_{P_A}] = Id_A ; k_{P_A} \bmod m = 3$

$2407 \bmod m = 3 \iff 2407 = 3 + km \Rightarrow k \cdot m = 2404$

$K \cdot m = 2404 = 2^2 \cdot 601$

$m > 3$ y m primo $\Rightarrow m = 601 \Rightarrow \not\equiv_{601}$