PROBLEMA 1

1) Si $P_0 = P_{0/0} = P_{0/1} = P_{0/2}$

$P_1 = P_{1/0} = P_{1/1} = P_{1/2}$

$P_2 = P_{2/0} = P_{2/1} = P_{2/2}$, la fuente no tendría memoria.

Por inspección: $P_{2/0} = 0 \neq P_{2/1} = 0.6 \Rightarrow$ F. CON MEMORIA

2) En E0: $0.7 P_0 = 0.2 P_2$, $P_2 = 7/2 P_0 = 21/62$

En E1: $P_2 = 0.6 P_1$, $P_1 = 35/6 P_0 = 35/62$.

$\rightarrow P_0 = \frac{1}{(1 + 7/2 + 35/6)} = 3/31$

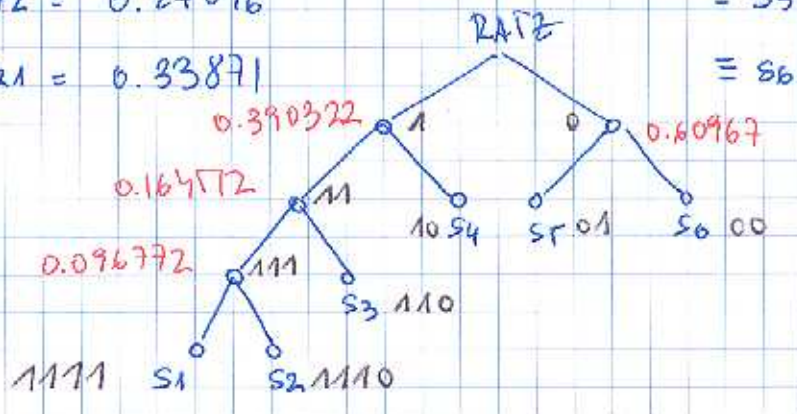
$H(X) = H(0.7) P_0 + H(0.6) P_1 + H(0.2) P_2$

$H(p) = -(p \log p + (1-p) \log(1-p))$, entropía binaria.

$= 0.87793$ [bits/símbolo]

3)

			Codificación
$P_{00} = P_{0/0} \cdot P_0 = 0.3 P_0 = 0.029032$		$\equiv S_1$	1111
$P_{02} = 0.06774$		$\equiv S_2$	1110
$P_{10} = 0.06774$		$\equiv S_3$	110
$P_{11} = 0.22581$		$\equiv S_4$	10
$P_{12} = 0.27096$		$\equiv S_5$	01
$P_{21} = 0.33871$		$\equiv S_6$	00



$\bar{L}_2 = 2\,(0.60967 + 0.2281) + 3 \cdot 0.06774 + 4 \cdot 0.096772$

$= 2.261268$ [bits / "supersímbolo"]

$\rightarrow \bar{L} = \bar{L}_2 / 2 = 1.130634$ [bits / símbolo]

$\rightarrow E = H(S) / \bar{L} = \underline{\underline{0.7765}}$

4) $S = \dots\; 2\,1\,1\,1$

↑ instante i (último 1); instante i-1 (penúltimo 1)

$\rightarrow S_4 = 11$ y $S_5 = 12$. (notación apartado 3)).

$\rightarrow$

S	P(S)	F(S)	$F(S) - 1/2\,P(S)$	$l(S) = \lceil \log_2 \frac{1}{P(S)} \rceil + 1$
11	0.22581	0.22581	0.112905	4
12	0.27096	0.49677	0.36129	3

$0.112905 \rightarrow 0.000111001\ldots \Rightarrow 0001$

$0.36129 \rightarrow 0.010111\ldots \Rightarrow \underline{\underline{010}}$.

5)

```
 7 6 5 4 3 2 1
 0 0 0 0 1[1 2]: 1 2 0 1 1 2 1 | 2 1 1 2 1 1 2 1 1 2 1 1 1
 0[1 1 2 1 2]0 : 1 1 2 1 2 1 1 | 2 1 1 2 1 1 2 1 1 1
 0 1 1 2[1 2 1 : 1 2 1]1 2 1 1 | 2 1 1 1 1
 1 2 1 1[2 1 1]: 2 1 1 1
```

$\Rightarrow (2,2,0)\,(6,5,1)\,(3,6,1)\,(3,3,1)$. Se necesitan 3 bits para los índices y 3 para las longitudes. Para los símbolos se necesitan 2 bits.

$\rightarrow$ **010 010 00 110 101 01 011 110 01 011 011 01**

6) $H(Y) = H(P(Y=0))$, entropía binaria

$P(Y=0) = P(X=0) \cdot P(Z_1=0) + P(X=1) \cdot P(Z_1=1)$

↑ MOEP.

$H(Z_1) = 0.8 = H(p) \Rightarrow$ por tanto se tiene $p \simeq 0.243$

, como $P(Z_1=0) > P(Z_1=1) = 0.243$

$\Rightarrow P(Y=0) = 0.40748$

$\Rightarrow H(Y) = H(0.40748) = \underline{0.97316}$ [bits/símbolo]

$H(Y^n) = n H(Y) = 0.97316 \cdot n$ [bits/símbolo]

↑ fuentes sin memoria.

7) $H(Y/X) = H(Z_1) = 0.8$ [bits/símbolo]

$H(Y^n/X^n) = n H(Z_1) = 0.8n$ [bits/símbolo]

PROBLEMA 2

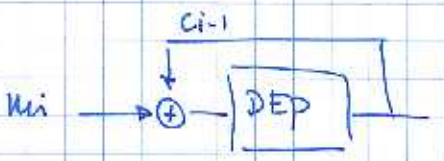
1) $IP^{-1} = [2\ 6\ 4\ 8\ 1\ 5\ 3\ 7]$

↑ LSB.

Aunque f no lineal, la red de Fistel modificada no parece fácilmente invertible. Se deberían aumentar las rondas para asegurar que todo $k(m)$ no se pueda encontrar m. Otro mecanismo sería aumentar el nº de bits de la clave y así aumentar la complejidad. Con todo ello, y trabajando en modo CBC (para tener efecto AVALANCHA), parece viable que la clave no sea sencilla.

2) $[4\ 3\ 2\ 1]$ ↑ LSB → | EXPANSIÓN + PERMUTACIÓN | → $[1\ 4\ 3\ 2\ 3\ 2\ 1\ 4]$

3)



$m_0 = 87 \rightarrow C_0 = 16$. (dato)

$m_1 = A1$.

El byte a codificar es

16: 0 0 0 1 0 1 1 0

A1: 1 0 1 0 0 0 0 1

1 0 1 1 0 1 1 1

↑ LSB.

IP: 1 1 0 1 | 1 1 1 0 ↑ LSB

L_0 R_0

Expansión + permutación: $1\ 1\ 1\ 0\ 1\ 0\ 1\ 1 = L_0'$

$0\ 1\ 1\ 1\ 1\ 1\ 0\ 1 = R_0'$

$\oplus$ $K_{DEP,0}$: $0\ 0\ 0\ 0\ 1\ 1\ 0\ 1 = L_0''$

111 00110 = E6hex. $1\ 0\ 0\ 1\ 1\ 0\ 1\ 1 = R_0''$

→ fila 0 columna 0 → 2 | fila 3 columna 2 → 2

→ fila 3 columna 0 → 2 | fila 3 columna 1 → 2

$\Rightarrow$ $L_0''' = 1010$

$R_0''' = 1010 = L_1$

$R_1 = L_0''' \oplus R_0''' = 0000$

$L_1 \| R_1 = 1010\ 0000$ (8 7 6 5 4 3 2 1) $\rightarrow IP^{-1} \rightarrow M(M) = 01010000$ (2 6 4 8 1 5 3 7)

$= \underline{50 \text{ hexa}}$

4) $M_2 \cdot M \bmod 43 = 1$; $M = A187 = 41351$

43 es primo $\Rightarrow$ T$^{\text{e}}$ Fermat : $41351^{42} \equiv_{43} 1$.

$\Rightarrow 41351^{41} \bmod 43 \Leftrightarrow M_2$ (inversa de M mod 43).

$41351 \bmod 43 = 28 \mapsto 28^{41} \bmod 43$?

$(28^6 \bmod 43) = 11$; $11^6 \bmod 43 = 4 \left(\equiv_{13} 28^{36}\right)$

↳ para calculadoras convencionales

$28^5 \bmod 43 = 5$

$\Rightarrow 4 \cdot 5 \equiv_{43} 28^{41} \Rightarrow \underline{M_2 = 20}$.

5) $e \cdot d \bmod \varphi(M) = 1$

$\varphi(M) = 10920$

$\Rightarrow e \cdot 6493 \bmod 10920 = 1$.

$\rightarrow$ Alg. extendido de Euclides:

		q	x	y	
10920	6493	1	-22	37	$\rightarrow e = 37$
6493	4427	1	15	-22	
4427	2066	2	-7	15	
2066	295	7	1	-7	
295	1	295	0	1	

$\uparrow$ mcd(10920, 6493)

Titulació

Assignatura

Cognoms — Nom

$c = 20^{37} \bmod 11147$

$20^6 \bmod 11147 = 5073 \equiv_{11147} 20^6$

$5073^2 \bmod 11147 = 8053 \equiv_{11147} 20^{12}$

$8053^2 \bmod 11147 = 8710 \equiv_{11147} 20^{24}$

$8053 \cdot 8710 \cdot 20 \bmod 11147 = \underline{4944} \equiv_{11147} 20^{37}$.

$M = c^d \bmod 11147 = \cdots = 20^{k\varphi(n)+1} \bmod 11147$

$= 20\,(\underbrace{20^{k\varphi(n)} \bmod 11147}_{\text{debe ser } 1}) \bmod 11147$

⇒ 20 y 11147 son coprimos, se puede asegurar que es 1. En otro caso $20^2, \ldots$

		557	2	1	6	
11147		20	7	6	[1]	0

↳ son co-primos

6) Simon recupera la inversa de 20 mod 43

⇒ $20^{41} \bmod 43$; $20^6 \bmod 43 = 4$

$4^6 \bmod 43 = 11 = 20^{36}$

$20^{41} \bmod 43 = 11 \cdot 20^5 \bmod 43 = 28$.

↳ 28 es diferente a 41351! ⇒ enviar otra inversa de M, congruente por tanto con 20, y que guarde la relación que tienen 28 y 41351:

$41351 = 28 + 43 \cdot \underline{961}$

$41343 = 20 + 43 \cdot 961$

(obviamente $41351 \cdot 41343 \bmod 43 = 1$).

7) lo más habitual es:

1. $K_{D_{SIMON}}(M) \parallel K_{S_{ALDOUS}}(H(M))$
2. Simon rompe M y calcula $H(M)_2$
3. Simon comprueba que $H_2(M) = H(M)$.

Al romper $H(M)$ se consigue la autenticidad de origen.
Al comparar con $H_2(M)$ " " " " contenido.