Ejercicio 1. Un sistema de apuestas desde un teléfono móvil permite realizar operaciones a un usuario si éste dispone de créditos. Para facilitar el conocimiento al usuario del número de créditos disponible o saldo se desarrolla una aplicación para el teléfono móvil. Esta aplicación interacciona con un servidor dedicado a la función de consulta de saldos por parte de los usuarios.

Para garantizar la seguridad al usuario, la aplicación del móvil dispone de la clave pública (K_P) del servidor y la transferencia del saldo se realiza a través de clave simétrica con un cifrador en flujo.

El móvil emplea la clave pública RSA del servidor para enviarle la clave de sesión o simétrica (k) del cifrador en flujo. El cifrador en flujo utilizado se basa en un LFSR únicamente. La clave simétrica k se corresponde directamente con el polinomio de estado P(D) y el polinomio de conexiones C(D) del LFSR.

$$P(D)=b_2D^2+b_1D+b_0$$

$$C(D)=c_3D^3+c_2D^2+c_1D+c_0$$

El valor binario de k se obtiene de la codificación de los valores de los coeficientes de ambos polinomios de forma que en binario:

$$k=(b_2\, b_1\, b_0\, a_3\, a_2\, a_1\, a_0) \quad \text{en base 2}$$

El cifrado en flujo se realiza enviando los dígitos del saldo con cuatro bits siempre de **menor a mayor peso** tanto para los dígitos como para su codificación binaria.
Sabiendo que el móvil transmite el criptograma $C_{asim}=3$ al servidor y recibe del servidor el criptograma $C_{sim}=55$, determine para $K_P=(e,n)=(187,319)$ ¿ cuál es el valor decimal del saldo disponible del usuario ?

Nota: $n=319=29\cdot 11$

Ejercicio 2. Se desea realizar la compresión de un fichero cuyo contenido es:

"A B D B D A D C A C C A D C B B"

Suponiendo que se ha fijado a priori para cada símbolo de la fuente la siguiente asociación binaria de dos bits:

{ A='00', B='01', C='10', D='11'}

a) Indique cuál es la mínima longitud en bits del resultado de la compresión del fichero.
b) Exprese en hexadecimal el resultado de la compresión de fichero cuando:
    1) se emplea el algoritmo LZ-77 con una memoria de almacenamiento de 8 posiciones (3 bits de direccionamiento).
    2) se emplea el algoritmo LZ-78 con un diccionario de 64 posiciones (6 bits de direccionamiento).
    3) se emplea el algoritmo LZW con un diccionario de 256 posiciones (8 bits de direccionamiento).

Ejercicio 1

$$K_P = (e, d) = (187, 319) = (187, 29 \cdot 11)$$

$$C_{Asim} = 3$$

$$C_{Sim} = 55$$

Para obtener el valor de k debemos descifrar C_{Asim}. Conocida la factorización de $n = 29 \cdot 11$ podemos hallar la clave privada del servidor K_S.

$$\Phi(n) = \Phi(319) = (p-1) \cdot (q-1) = 28 \cdot 10 = 280$$

$$e \cdot d = 1 \mod \Phi(n)$$

Aplicando el algoritmo de Euclides extendido:

$$d \cdot e = 1 + K \cdot \Phi(n) \qquad K \in \mathbb{Z}$$

$$\begin{array}{r|l} 280 & 187 \\ \hline 093 & 1 \end{array}$$

(1) $280 \cdot 1 + 187 \cdot 0 = 280$

(2) $280 \cdot 0 + 187 \cdot 1 = 187$

$280 - 187 \cdot 1 = 93 \Rightarrow (1) - 1 \cdot (2) \Rightarrow (3)$

$$\begin{array}{r|l} 187 & 93 \\ \hline 01 & 2 \end{array}$$

(3) $280 \cdot 1 - 187 \cdot 1 = 93$

$187 - 93 \cdot 2 = 1 \Rightarrow (2) - 2(3) \Rightarrow (4)$

$$(280)(-2) + (187)(3) = 1$$

Por tanto:

$$\underset{d}{3} \cdot \underset{e}{187} = 1 + \underset{K}{2} \cdot \underset{\Phi(n)}{280}$$

Obtenemos $K_S = (d, n) = (3, 319)$

Desciframos $C_{A_{sim}} = 3$

$$m = C_{A_{sim}}^{d} \bmod n = 3^3 \bmod 319 = 27$$

El mensaje m se corresponde con la clave simétrica

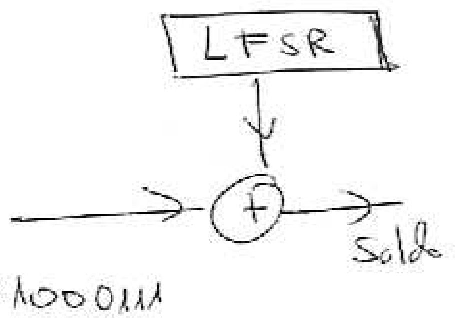
$$k = 27 = 1B\,h = 00011011 = (b_2 b_1 b_0 c_3 c_2 c_1 c$$

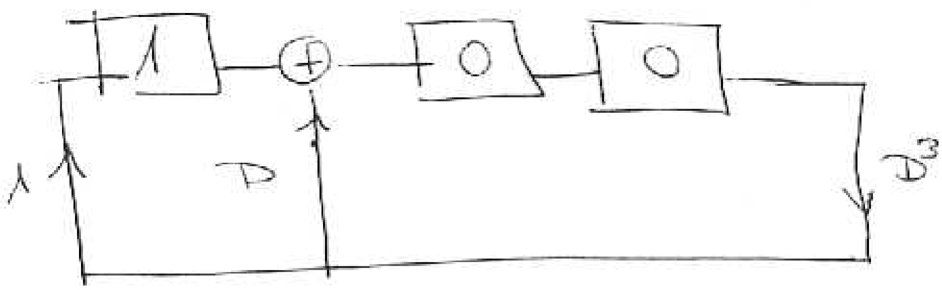
Por lo tanto

$$P(D) = 0 \cdot D^2 + 0 \cdot D + 1$$
$$C(D) = D^3 + 0D^2 + D + 1$$

El valor del saldo disponible lo hallaremos descifrando el criptograma C_{sim} que llega al móvil

$$C_{sim} = 55 = 0011\,0111$$





$P(D)$	Salida	C_{sim}		m_i = salida $\oplus$ C_{sim}	
1 0 0	0	1	1	1	1
0 1 0	0	0	1	0	1
0 0 1	1	1	1	0	0
1 1 0	0	0	0	0	0
0 1 1	1	1	1	0	0
1 1 1	1	0	1	1	0
1 0 1	1	1	0	0	1
1 0 0	0	0	0	0	0

Salida = 0010 . 0001 = $\underline{\underline{21}}$

Ejercicio 2

A B D B D A D C A C C A D C B B

a) Hay 16 símbolos de fuente en el fichero.

Si suponemos que son equiprobables necesitaríamos

16×2 bits $= 32$ bits

En el fichero aparecen los símbolos con probabilidad $1/4$ por lo que son equiprobables. Luego de igual manera, con la estadística del fichero, necesitaríamos al menos 32 bits

b)

1) LZ-77.

A B D B D A D C A C C A D C B B

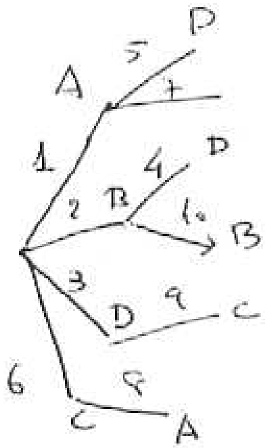
(0,0)A (0,0)B (0,0)D (2,2)A (2,1)C (3,1)C (3,2)D (3,1)B (0,0)B

	Pos Long Car	
(0,0) A →	000 000 00 →	00h
(0,0) B →	000 000 01 →	01h
(0,0) D →	000 000 11 →	03h
(2,2) A →	010 010 00 →	48h
(2,1) C →	010 001 10 →	46h
(3,1) C →	011 001 10 →	66h
(3,2) D →	011 010 11 →	6Bh
(3,1) B →	011 001 01 →	65h
(0,0) B →	000 000 01 →	01h

2) LZ-78

A B D $\underbrace{\text{B D}}$ $\underbrace{\text{A D}}$ $\underbrace{\text{C}}$ $\underbrace{\text{A C}}$ $\underbrace{\text{C A}}$ $\underbrace{\text{D C}}$ $\underbrace{\text{B B}}$

(0,A) (0,B) (0,D) (2,D) (1,D) (0,C) (1,C) (6,A) (3,C) (2,B)



Posición	Carácter
000001	A
000010	B
000011	D
000100	BD
000101	AD
000110	C
000111	AC
8	CA
9	DC
10	BB

(0,A) → 0000,00 00 → 00h

(0,B) → 0000,00 01 → 01h

(0,D) → 0000,00 11 → 03h

(2,D) → 0000,10 11 → 0Bh

(1,D) → 0000,01 11 → 07h

(0,C) → 0000,00 10 → 02h

(1,C) → 0000,01 10 → 06h

(6,A) → 0001,10 00 → 18h

(3,C) → 0000,11 10 → 0Eh

(2,B) → 0000,10 01 → 09h

3) LZW

$$\underset{0}{A}\ \underset{1}{B}\ \underset{3}{D}\ \underbrace{B\ D}_{5}\ \underbrace{A}_{0}\ \underbrace{D}_{3}\ \underbrace{C}_{2}\ \underbrace{A}_{0}\ \underbrace{C}_{2}\ \underbrace{CA}_{10}\ \underbrace{DC}_{9}\ \underbrace{B}_{1}\ \underbrace{B}_{1}$$

0 → A
1 → B
2 → C
3 → D
4 → AB
5 → BD
6 → DB
7 → BDA
8 → AD
9 → DC
10 → CA
11 → AC
12 → CC
13 → CAD
14 → DCB
15 → BB

0 → 00h
1 → 01h
3 → 03h
5 → 05h
0 → 00h
3 → 03h
2 → 02h
0 → 00h
2 → 02h
10 → 0Ah
9 → 09h
1 → 01h
1 → 01h