Ejercicio 1. Una fuente binaria simétrica F emite ráfagas de longitud L, con L>0, según una distribución geométrica de parámetro p:

$$\text{Prob}\,[L=k] = p^{k-1}\,(1-p) \text{ con } k=1,2,\ldots \text{ y } 0<p<1$$

a) Proponga un modelo markoviano de la fuente F, con memoria 1, y evalúe su entropía H(F) para un valor p genérico. Particularice el resultado para p=1/2.

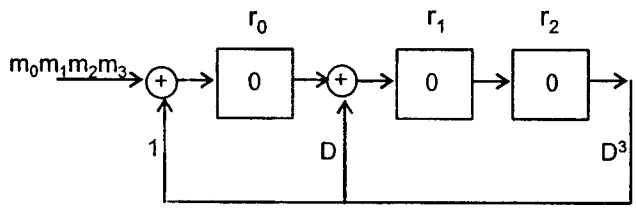
b) Aplicando una codificación de fuente por ráfagas resulta una fuente F' cuyos símbolos representan la longitud de las ráfagas de F, {1, 2, 3, ...}.

b.1) Determine la entropía H(F') para p=1/2.
b.2) Suponiendo que en la práctica la fuente no genera ráfagas de longitud mayor a 7 y despreciando la probabilidad de estos casos, realice una codificación binaria de Huffman de F' para el caso p=1/2.
b.3) A partir de los resultados obtenidos en los apartados anteriores, discuta las ventajas e inconvenientes de la codificación por ráfagas para el caso p=1/2.

c) Utilizando el algoritmo LZW con un diccionario de 8 posiciones (3 bits), indique cuál será la codificación binaria de la secuencia generada por la fuente a ráfagas:

00011100110011

Ejercicio 2. Un sistema de votación desde terminales móviles emplea el algoritmo RSA para proporcionar el servicio de verificabilidad a la aplicación. En este sistema cada terminal móvil dispone de una clave pública secreta K_s que se emplea para firmar la concatenación del mensaje m y el resumen r. La concatenación es un valor v de 7 bits que se obtiene con la unión de los 4 bits del mensaje y los 3 bits del resumen, de mayor a menor peso ($v = 0x\ m_3\ m_2\ m_1\ m_0\ r_2\ r_1\ r_0$). Para determinar el valor del resumen r se emplea un LFSR con estado inicial nulo y polinomio de conexiones $1+D+D^3$, el cual se alimenta con los bits del mensaje, empezando con el de mayor peso. Una vez se ha operado en el LFSR con todos los bits del mensaje, el resumen se deriva directamente del polinomio de estado del LFSR como se muestra en la figura.



Teniendo en cuenta que en un terminal:

i) $K_s = (d,n) = (7, 221)$

ii) $m = 14\ (0x1110)$

Nota: $\sum_{k=1}^{\infty} kp^k = \frac{p}{(1-p)^2}$

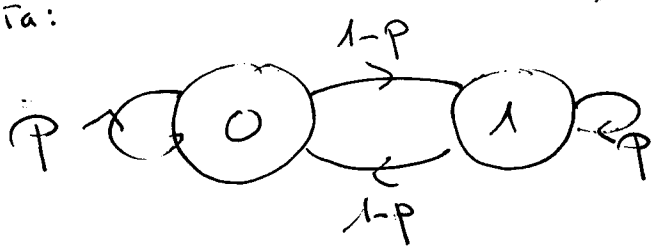
a) Calcule la clave pública $K_P = (e, n)$ asociada al terminal.
b) Halle el valor del resumen en binario.
c) Especifique el valor concatenado v en decimal. Determine el resultado de la firma de v.
d) Indique cuántos bits son necesarios para enviar cualquier posible valor de la firma de v. Razone la respuesta.
e) A partir de la expresión polinómica para el cálculo iterativo del estado de un LFSR y con un polinomio M(D) de grado n-1 como alimentación externa, obtenga la relación del polinomio de estado en la iteración n ($P^n(D)$) con su valor inicial ($P^0(D)$) y con el polinomio M(D).
f) Particularice la expresión anterior para el caso en que el estado inicial del LFSR es nulo y el valor de M(D) es $D^7+D^6+D^5+D^4+D^2+1$.

Ejercicio 1.

$$\text{Prob}[L=k] = p^{k-1}(1-p) \qquad k=1,2,\ldots$$

$$0<p<1$$

a) La fuente F genera ráfagas de 0 y 1
Un modelo markoviano con memoria 1 de F
sería:



Por simetría $\text{Prob}(F=0) = \text{Prob}(F=1) = 1/2$

$$H\left(F_n/_{F_{n-1}=0}\right) = P_{0/0}\log_2\frac{1}{P_{0/0}} + P_{1/0}\log_2\frac{1}{P_{1/0}}$$

$$H\left(F_n/_{F_{n-1}=0}\right) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{(1-p)}$$

Por simetría:

$$H\left(F_n/_{F_{n-1}=1}\right) = H\left(F_n/_{F_{n-1}=0}\right)$$

Luego $H(F) = P[F=1]\cdot H\left(F_n/_{F_{n-1}=1}\right) + P[F=0]H\left(F_n/\right.$

$$H(F) = \frac{1}{2}\cdot 2\cdot H\left(F_n/_{F_{n-1}=0}\right) \Rightarrow$$

$$\boxed{H(F) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{(1-p)}}$$

Si: $p=1/2 \Rightarrow H(F) = 1 \text{ bit/símbolo}$

b)

$$F' = \{1, 2, 3, 4, \dots\}$$

$$P_{rob}(F' = k) = P_{rob}[L = k] = p^{k-1}(1-p)$$

b.1) $$H(F') = p_1 \log_2 \frac{1}{p_1} + p_2 \log_2 \frac{1}{p_2} + p_3 \log_2 \frac{1}{p_3} + \dots$$

Si: $p = 1/2$

$$p_1 = P_{rob}[F' = 1] = 1 - p = 1/2$$
$$p_2 = P_{rob}[F' = 2] = p(1-p) = 1/2 \cdot 1/2 = 1/2^2$$
$$p_3 = P_{rob}[F' = 3] = p^2(1-p) = 1/2^3$$
$$p_k = P_{rob}[F' = k] = 1/2^k$$

$$H(F') = \frac{1}{2} \log_2 2 + \frac{1}{2^2} \log_2 2^2 + \frac{1}{2^3} \log_2 2^3 + \dots$$

$$H(F') = \frac{1}{2} + 2 \cdot \frac{1}{2^2} + 3 \cdot \frac{1}{2^3} + \dots$$

$$H(F') = \sum_{i=1}^{\infty} i \left(\frac{1}{2}\right)^i = \frac{1/2}{\left(1 - 1/2\right)^2} = \frac{1/2}{\left(1/2\right)^2} = 2 \text{ bits/simb}$$

b.2) $K = \{1, 2, 3, 4, 5, 6, 7\}$ $\quad P_{rob}[L \geq 8] \simeq 0$

Suponiendo $p = 1/2$

$p_1 = 1/2 = 0'5$

$p_2 = 0'250$

$p_3 = 0'125$

$p_4 = 0'0625$

$p_5 = 0'03125$

$p_6 = 0'015625$

$p_7 = 0'0078125$

$p_6, p_7 \rightarrow A \rightarrow 0'0234375$

$p_5, A \rightarrow B \rightarrow 0'0546$

$p_4, B \rightarrow C \rightarrow 0'11718$

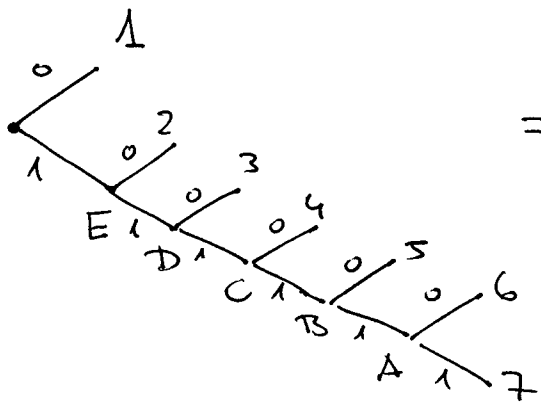
$P_1 = 0'5$

$P_2 = 0'25$

$P_3 = 0'125$

$P_C = 0'11718$

→ D → $0'242$ → E → $0'492$ → fin.



⇒

1 → 0

2 → 10

3 → 110

4 → 1110

5 → 11110

6 → 111110

7 → 111111

b.3)

Obsérvese que si no se hubiera truncado la longitud de las ráfagas, cada valor de longitud requiere un número de dígitos de codificación igual al tamaño de la ráfaga. Por lo tanto, esta codificación no ofrece ninguna ventaja respecto a enviar el valor de cada símbolo de F.

c) LZW

0 00 11 00 11 00 11

↓ ↓ ↓ ↓ ↓ ↓ ↓

0 2 1 4 3 1 6

0 → 0

1 → 1

2 → 00

3 → 01

4 → 11

5 → 110

6 → 0011

7 → 10

Codificación:

000.010.001.100.011.001.110.

Ejercicio 2

$K_S = (7, 221)$ $\quad n = 13 \cdot 17 = p \cdot q = 221$

$m = 14$ $\quad e = ?$

$d = 7$

a) $K_P = (e, n)$

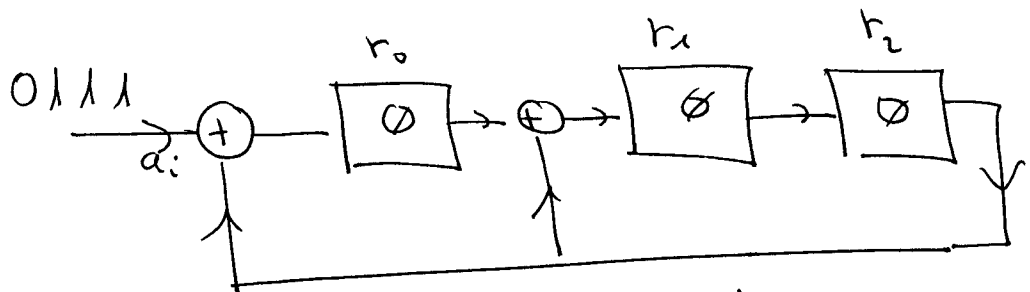
$$d \cdot e \equiv 1 \mod \Phi(n)$$

$$\Phi(n) = (p-1)(q-1) = 192$$

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

Se obtiene que $e = 55$ y $k = 2$ verifican la ecuación $\Rightarrow$ $K_P = (55, 221)$

b) Cálculo del resumen:



i	a_i	r_0	r_1	r_2	$P^{(i)}(D)$
0		0	0	0	0
1	1	1	0	0	1
1	1	1	1	0	D+1
2	1	1	1	1	D^2+D+1
3	1	1	1	1	D^2+D
4	0	1	0	1	

$$r = 0x101$$

c) $V = 0x\ 1110.101 = 117$

$$f = V^d \bmod n = 117^7 \bmod 221 = 195$$

d) Como f se reduce modularmente por n se necesitan tantos bits como sea necesario para codificar el valor $n-1$. En este caso $n-1 = 220$ que requiere 8 bits. En este caso:

$f = 195 = C3h = 0x \underbrace{1100.0011}_{8\ bits}$

e) Suponiendo $M(D) = m_{n-1}D^{n-1} + m_{n-2}D^{n-2} + \dots + m_0$

Expresión polinómica para el cálculo iterativo del LFSR:

$$P^{(i)}(D) = D \cdot P^{(i-1)}(D) \bmod C(D)$$

En nuestro caso cada iteración i da como resultado:

$$P^{1}(D) = D\,P^{0)}(D) \bmod C(D) + m_{n-1}$$
$$= (D P^{0}(D) + m_{n-1}) \bmod C(D)$$

$$P^{2}(D) = D P^{1)}(D) \bmod C(D) + m_{n-2}$$
$$= (D \cdot (D P^{0}(D) + m_{n-1}) + m_{n-2}) \bmod C(D)$$
$$= (D^2 P^{(0)}(D) + m_{n-1} D + m_{n-2}) \bmod C(D)$$

$$P^{n)}(D) = (D^n P^{0)}(D) + m_{n-1} D^{n-1} + m_{n-2} D^{n-2} + \dots + m_0) \bmod C(D)$$

Agrupando

$$P^{(b)}(D) = \left(D^n P^{(0)}(D) + H(D)\right) \bmod C(D)$$

f) $P^{(0)}(D) = \emptyset$

$$H(D) = D^7 + D^6 + D^5 + D^4 + D^2 + 1$$

$$P^{(8)}(D) = H(D) \bmod C(D)$$

$D^7+D^6+D^5+D^4+D^2+1$ | D^3+D+1

$D^7+\ \ +D^5+D^4$ | D^4+D^3+D+1

$D^6\ \ \ +D^2+1$

$D^6+D^4+D^3$

$D^4+D^3+D^2+1$

$D^4\ \ \ +D^2+D$

$D^3\ \ \ +D+1$

0

$H(D)$ es multiplo de $C(D)$