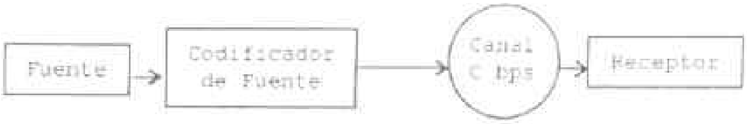
J. Mata

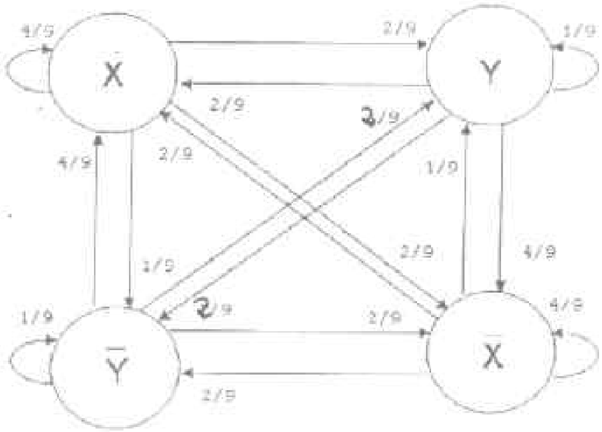
Ejercicio 1. En un sistema simple de clave pública RSA se emplea una entidad de certificación (EC) para obtener las claves públicas de las entidades que intervienen en él. Este sistema utiliza en todas las claves públicas el mismo valor $e = 11$ por lo que las claves se reducen a un único valor n. Se ha averiguado que en este sistema todas las claves públicas disponen de un mismo factor primo y que la función resumen empleada es una reducción modular en un cuerpo conmutativo. Sabiendo que la clave pública de la EC es $Kp_{EC} = 9263$ y que un certificado de una entidad A tiene por valor $Kp_A|F(R[Kp_A])= 5959|5811$.

a) halle la clave secreta (Ks_{EC}) de la EC
b) calcule el resumen de una clave que incluya el factor primo 127
c) halle la clave pública de valor mínimo en este sistema que tenga la misma firma que la clave anterior. Razone la validez de la función resumen empleada.

Ejercicio 2. Una fuente binaria con memoria 1 envía de forma periódica símbolos a un codificador de fuente cada Tf.

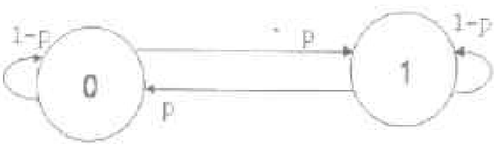


El codificador aplica una extensión de fuente concatenando dichos símbolos de dos en dos de forma que trabaja con un alfabeto $\{X, \overline{X}, Y, \overline{Y}\}$. El comportamiento de la fuente extendida puede ser modelado mediante la cadena de Markov:



a) Para el régimen estacionario, calcule la probabilidad de que la fuente extendida genere cada uno de los símbolos. (Tenga en cuenta las simetrías de la cadena de Markov para el cálculo)
b) Determine la Entropía ($H(F_e)$) de la fuente extendida en bits
c) Suponiendo que la codificación de la fuente extendida obtiene una longitud media de 1.88 dígitos binarios por símbolo, halle el valor mínimo de Tf para un canal de 64Kbps.

Teniendo en cuenta que la fuente binaria se puede modelar con la cadena de Markov:



d) identifique el valor de p a partir del modelo de fuente extendida y la asociación entre los valores del alfabeto de la fuente extendida y los pares de símbolos binarios.
e) Para un valor de $p=1/3$, halle la relación entre entropías de la fuente extendida y la fuente binaria. Discuta los valores obtenidos respecto al caso sin memoria.

Ejercicio 1

Se determina el factor primo común.

$$Kp_{EC} = 9263 = p \cdot q \qquad m.c.d\,(Kp_{EC}, Kp_A) = p$$
$$Kp_A = 5959 = p \cdot q'$$

Algoritmo de Euclides

$$9263 \,\underline{|\,5959}\quad 3304 \;\; 1 \qquad 5959 \,\underline{|\,3304}\quad 2655 \;\; 1 \qquad 3304 \,\underline{|\,2655}\quad 649 \;\; 1$$

$$2655 \,\underline{|\,649}\quad 59 \rightarrow m.c.d \qquad 649 \,\underline{|\,59}\quad 0) \;\; 11$$

Luego $p = 59 \Rightarrow \begin{cases} Kp_{EC} = 9263 = 59 \cdot 157 \\ Kp_A = 5959 = 59 \cdot 101 \end{cases}$

a) Derivamos la K_{SEC}

$$e \cdot d = 1 + k\, \Phi(Kp_{EC})$$

$$\Phi(Kp_{EC}) = 58 \cdot 156 = 9048$$

$$11 d = 1 + k\; 9048$$
$$k_1\, 9048 + k_2\, 11 = 1$$

Algoritmo Euclides

$$9048 \,\underline{|\,11}\quad 6 \;\; 822 \qquad 11 \,\underline{|\,6}\quad 5 \;\; 1 \qquad 6 \,\underline{|\,5}\quad 1) \;\; 1$$

Algoritmo de Euclides Extendido:

$$9048 \cdot 1 + 11 \cdot 0 = 9048$$
$$9048 \cdot 0 + 11 \cdot 1 = 11 \qquad (-822)$$
$$9048 \cdot 1 + 11\,(-822) = 6 \qquad (-1)$$
$$9048\,(-1) + 11\,(1 + 822) = 5 \qquad (-1)$$
$$9048\,(1+1) + 11\,(-822-823) = 1$$
$$9048 \cdot 2 + 11\,(-1645) = 1$$

$$k_2 = -1645 \Rightarrow d = k_2 \bmod 9048 = 7403$$
$$K_{SEC} = (d, n) = (7403, 9263)$$

b) Operación modular realizada. ②

$$r = K_{SA} \bmod m$$

Firma obtenida

$$f = E_{K_{SEC}}(r) = 5811 \Rightarrow r = D_{K_{PEC}}(f)$$

$$r = 5811^{e} \bmod n = 5811^{11} \bmod 9263 = 7$$

Se debe verificar: $5959 \bmod m = 7$

siendo m primo al trabajar en un cuerpo conmutativo

De forma equivalente: $5959 = 7 + km$

$$5952 = k \cdot m$$

Hallamos los factores primos de 5952 e identificamos

$$5952 = 2^6 \cdot 3 \cdot 31 = k \cdot m \Rightarrow \begin{cases} m = 31 \\ k = 2^6 \cdot 3 \end{cases}$$

$m = 31$ porque debe ser primo y $m > 7$.

Por lo tanto, la operación resumen es:

$$r = K_p \bmod 31$$

Para una clave $K_p = 127 \cdot 59 = 7493$

el resumen será:

$$r = 7493 \bmod 31 = 22$$

③

c) La k_p mínima que verifica:

$$r = k_p \bmod 31 = 22$$

Se obtiene probando factores primos q pequeño

Con $q = 3$ tenemos:

$$k_p = 59 \cdot 3 = 177 \quad y \quad r = k_p \bmod 31 = 22$$

Otra manera: $(59 \cdot q) \bmod 31 = 22 \Rightarrow 59q + 31k =$

$59 \cdot 10 - 31 \cdot 19 = 1$ Euclides Extendido

$59 \cdot 220 - 31 \cdot 418 = 22$ Multiplicando por 22

$59 \cdot 31 - 31 \cdot 59 = 0$ Ecuación trivial.

Combinación

$$59 \cdot (220 - k_1 31) - 31 (418 - k_1 \cdot 59) = 22$$

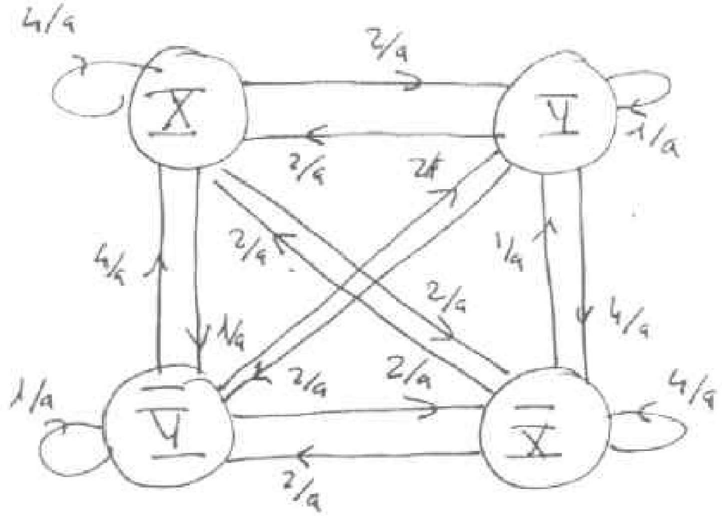
Se busca el valor primo más pequeño de:

$$220 - k_1 31 = q \Rightarrow q = 3 \text{ con } k_1 = 7$$

Ejercicio 2

a)

(1)



Se observa que: $P(X) = P(\overline{X})$

$P(Y) = P(\overline{Y})$

Se debe cumplir $P(X) + P(\overline{X}) + P(Y) + P(\overline{Y}) = 1$

Por lo tanto, falta una ecuación que se derive de la CM: por ejemplo: para el estado X se verifica en R.P.

$$P(X) \cdot \left[\frac{2}{9} + \frac{2}{9} + \frac{1}{9} \right] = P(Y) \cdot \frac{2}{9} + P(\overline{Y}) \frac{4}{9} + P(\overline{X}) \cdot \frac{2}{9}$$

Simplificando:

$$5 P(X) = 2 P(Y) + 4 P(\overline{Y}) + 2 P(\overline{X})$$

$$\begin{cases} P(X) = P(\overline{X}) \\ P(Y) = P(\overline{Y}) \\ P(X) + P(Y) = \frac{1}{2} \\ P(X) = 2 P(Y) \end{cases}$$

$$\boxed{\begin{aligned} P(Y) &= 1/6 \\ P(X) &= 1/3 \\ P(\overline{Y}) &= 1/6 \\ P(\overline{X}) &= 1/3 \end{aligned}}$$

b) $H(F_e) = P(\overline{X}) \cdot H(F_e/X) + P(\overline{X}) \cdot H(F_e/\overline{X}) +$
$P(Y) \cdot H(F_e/Y) + P(\overline{Y}) \cdot H(F_e/\overline{Y})$

$$H(F_e/X) = p_{x/x} \log_2 \frac{1}{p_{x/x}} + p_{\bar{x}/x} \log_2 \frac{1}{p_{\bar{x}/x}} + p_{y/x} \log_2 \frac{1}{p_{y/x}} + p_{\bar{y}/x} \log_2 \frac{1}{p_i}$$

$$H(F_e/X) = \frac{4}{9} \log_2 \frac{9}{4} + \frac{2}{9} \log_2 \frac{9}{2} + \frac{2}{9} \log_2 \frac{9}{2} + \frac{1}{9} \log_2 9$$

$$H(F_e/X) = \frac{4}{9} \log_2 \frac{9}{4} + \frac{4}{9} \log_2 \frac{9}{2} + \frac{1}{9} \log_2 9$$

$$H(F_e/X) = \frac{4}{9}(\log_2 9 - 2) + \frac{4}{9}(\log_2 9 - 1) + \frac{1}{9} \log_2 9$$

$$H(F_e/X) = \log_2 9 - \frac{12}{9} = 2 \log_2 3 - \frac{4}{3} = 1'83 \ \text{bits}/_{\text{simb } F^2}$$

Dado que todos los estados tienen el mismo conjunto de probabilidades de transición,

$$H(F_e/X) = H(F_e/\overline{X}) = H(F_e/Y) = H(F_e/\overline{Y})$$

por lo que: $\underline{H(F_e)} = H(F_e/X) = \underline{2 \log_2 3 - \frac{4}{3} = 1'83 \ \text{bits}/_{\text{simb}}}$

c) $L_{F^2} = 1'88 \ \text{dig bin}/_{\text{sim } F^2}$

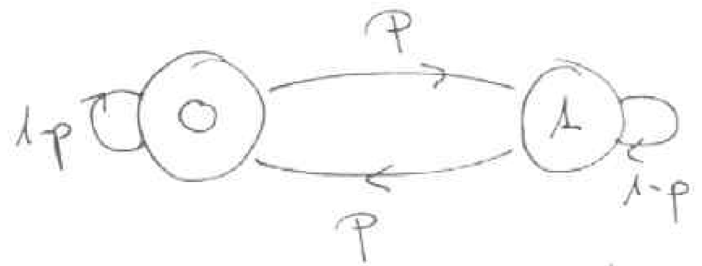
La velocidad máxima de la fuente extendida será:

$$V_{F^2} = \frac{C}{L_{F^2}} = \frac{64000}{1'88} = 34042'55 \ \text{sim } F^2/_{sg.}$$

La velocidad máxima de la fuente será:

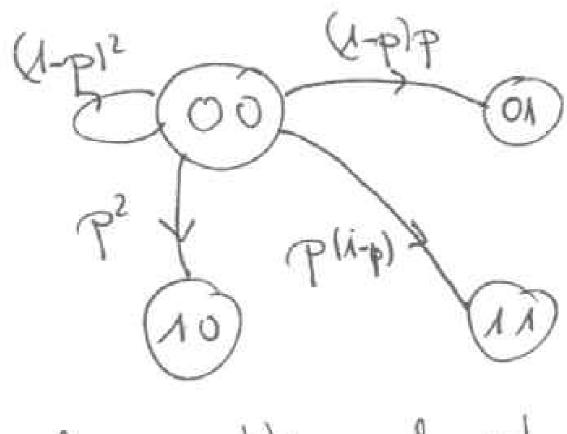
$$V_F = 2 \cdot V_{F^2} = 68085'10 \ \text{sim } F/_{sg.}$$

$$T_F = \frac{1}{V_F} = 1'468 \cdot 10^{-5} = 14'6 \mu s$$ tiempo mínimo entre símbolos



d) El alfabeto extendido será $\{00, 01, 10, 11\}$

En el estado $\emptyset\emptyset$ de la fuente extendida, el último símbolo enviado por la fuente es $\emptyset$ y, por tanto, la fuente elemental está en el estado $\emptyset$. Para que ésta fuente vuelva a enviar otra vez $\emptyset\emptyset$, la fuente elemental se deberá mantener consecutivamente en el mismo estado y esto ocurre con probabilidad $(1-p)^2$. En la fuente extendida esto se refleja con la transición al estado $\emptyset\emptyset$ donde se encontraba, la cual tiene valor $4/9$, para X y $\bar{\mathrm{X}}$, y $1/9$ para Y e $\bar{\mathrm{Y}}$. Completando las transiciones del estado $\emptyset\emptyset$ de la misma forma se obtiene:



Identificando se obtienen dos soluciones posibles:

i) $\mathrm{X}=\emptyset\emptyset$, $\bar{\mathrm{X}}=11$, $\mathrm{Y}=10$, $\bar{\mathrm{Y}}=01 \Rightarrow p=1/3$ $\quad \begin{cases} p(1-p)=2/9 \\ p^2=1/9 \end{cases}$

ii) $\mathrm{X}=01$, $\bar{\mathrm{X}}=10$, $\mathrm{Y}=\emptyset\emptyset$, $\bar{\mathrm{Y}}=11 \Rightarrow p=2/3$ $\quad \begin{cases} p(1-p)=2/9 \\ p^2=4/9 \end{cases}$

e) $p = 1/3$

$$H(F) = P(0) \cdot H(F/_0) + P(1) \cdot H(F/_1)$$

$P(0) = P(1) = 1/2$ por simetría

$$H(F/_0) = H(p) = \frac{1}{3}\log_2 3 + \frac{2}{3}\log_2 \frac{3}{2}$$

$$H(F/_0) = \frac{1}{3}\log_2 3 + \frac{2}{3}\log_2 3 - \frac{2}{3}\log_2 2$$

$$H(F/_0) = \log_2 3 - \frac{2}{3}$$

La probabilidades de transición son las mismas para el estado 1, por lo que:

$$H(F) = H(F/_0) = \log_2 3 - \frac{2}{3} = 0'9183 \text{ bits/sim}$$

La relación será:

$$\frac{H(F_e)}{H(F)} = \frac{2\log_2 3 - \frac{4}{3}}{\log_2 3 - \frac{2}{3}} = 2 \quad \left(\begin{array}{c}\text{concatenación} \\ \text{de 2 símbolos}\end{array}\right)$$

Si F no tuviera memoria, la fuente extendida sería la agrupación de símbolos independientes de F, por lo que la entropía crece linealmente con el número de símbolos concatenados. Así,

$$H(F_e) = 2H(F)$$

Por lo tanto, se mantiene la misma relación como cabría esperar, puesto que la fuente extendida no