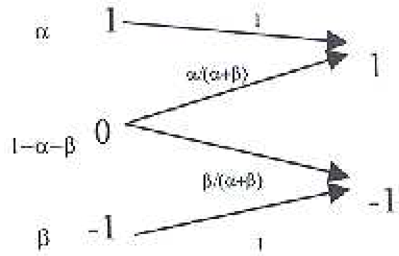
Jordi Mota

Ejercicio 1. Un sistema de transmisión de datos está compuesto por un regenerador de señal. El regenerador tiene por entradas (X) símbolos que pertenecen al alfabeto { 1, 0, -1 }. Las probabilidades de recepción los símbolos son:

$$P[X=1]=\alpha,\ P[X=0]=1-\alpha-\beta,\ P[X=-1]=\beta \text{ para } \mathbf{0<\alpha+\beta<=1.}$$

El regenerador restituye los valores de los borrones (X=0) en valores de salida Y=1 o Y=-1 con la misma proporción con la que se generan y mantiene el mismo valor (Y=X) cuando las entradas son X=1 o X=-1. Así, el sistema de transmisión de datos regeneradors se puede caracterizar a través de la matriz estocástica de probabilidades:

$$Q=\begin{bmatrix} 1 & 0 \\ \alpha/(\alpha+\beta) & \beta/(\alpha+\beta) \\ 0 & 1 \end{bmatrix}$$



a) Determine H(Y)

b) Calcule H(Y/X)

c) Halle I(X;Y)

d) Calcule la capacidad del sistema regenerador en bits por símbolo para los casos:
   i) $\alpha=\beta$
   ii) $\alpha=2\beta$

Ejercicio 2. Dos entidades A y B comparten un secreto utilizando el mecanismo propuesto por Diffie-Hellman utilizando una base a=17 y realizando las operaciones en Z_{31}. Los números aleatorios generados por las entidades A y B son respectivamente x=3 e y=11.

a) Calcule el valor del secreto compartido

Sabiendo que las entidades A y B disponen de una clave pública RSA para comprobación de firma digital y que sus valores son: Kp_A=(187,319) y Kp_B=(1201,1357)

b) Halle las claves secretas de ambas entidades

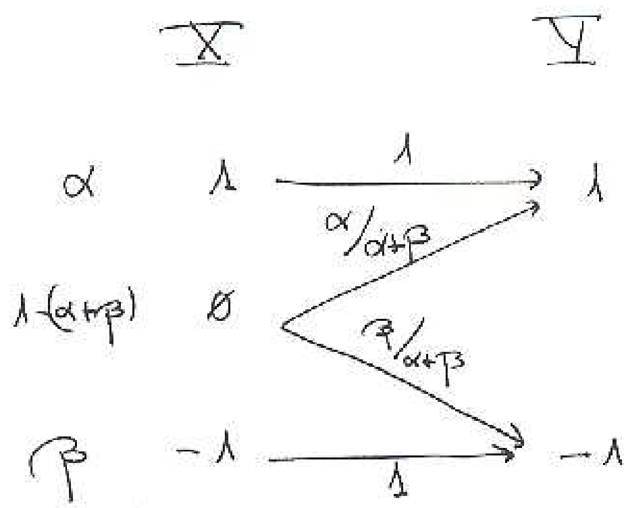
Considerando que los mensajes intercambiados entre las entidades para compartir el secreto se firman por el emisor (no se emplea ninguna función resumen),

c) Especifique el valor de los mensajes intercambiados cuando están firmados.

Nota: 319= 29 x 11 ; 1357= 23 x 59

Ejercicio 3. Un decodificador aritmético opera con un diccionario cuyo alfabeto es { A, B, C, D, E }. Las probabilidades de cada uno de los símbolos son: P(A)=P(B)=P(C)=1/4 y P(D)=P(E)=1/8. Halle el valor del mensaje decodificado de 5 caracteres cuando se recibe el valor decimal 0'55.

Ejercicio 1



$$Q = \begin{bmatrix} 1 & 0 \\ \frac{\alpha}{\alpha+\beta} & \frac{\beta}{\alpha+\beta} \\ 0 & 1 \end{bmatrix}$$

$$0 < \alpha+\beta \leq 1$$

a) Determinar $H(Y)$

$$P(Y=1) = \alpha + [1-(\alpha+\beta)] \cdot \frac{\alpha}{\alpha+\beta} = \alpha + \frac{\alpha}{\alpha+\beta} - \alpha$$

$$P(Y=1) = \frac{\alpha}{\alpha+\beta}$$

$$P(Y=-1) = 1 - P[Y=1] = \frac{\beta}{\alpha+\beta}$$

$$H(Y) = \frac{\alpha}{\alpha+\beta} \log_2 \frac{\alpha+\beta}{\alpha} + \frac{\beta}{\alpha+\beta} \log_2 \frac{\alpha+\beta}{\beta} \triangleq H\left(\frac{\alpha}{\alpha+\beta}\right)$$

b) Hallar $H(Y/X)$

$$P(Y=1/X=1) = 1 \qquad P(Y=-1/X=1) = 0$$

$$P(Y=1/X=0) = \frac{\alpha}{\alpha+\beta} \qquad P(Y=-1/X=0) = \frac{\beta}{\alpha+\beta}$$

$$P(Y=1/X=-1) = 0 \qquad P(Y=-1/X=-1) = 1$$

$$H\left(\frac{Y}{X}\right) = P(X=1)\cdot \cancel{H\left(\frac{Y}{X=1}\right)}^{0} + P(X=-1)\cdot \cancel{H\left(\frac{Y}{X=-1}\right)}^{0}$$

$$+ P(X=0)\cdot H\left(\frac{Y}{X=0}\right) = \left[1-(\alpha+\beta)\right] H\left(\frac{\alpha}{\alpha+\beta}\right)$$

$$H\left(\frac{Y}{X}\right) = \left[1-(\alpha+\beta)\right]\cdot\left(\frac{\alpha}{\alpha+\beta}\log_2\frac{(\alpha+\beta)}{\alpha} + \frac{\beta}{\alpha+\beta}\log_2\frac{(\alpha+\beta)}{\beta}\right)$$

c) $I(X;Y) = H(Y) - H\left(\frac{Y}{X}\right) = H\left(\frac{\alpha}{\alpha+\beta}\right) - \left[1-(\alpha+\beta)\right]H\left(\right.$

$$I(X;Y) = (\alpha+\beta)\, H\left(\frac{\alpha}{\alpha+\beta}\right) =$$

$$= (\alpha+\beta)\cdot\left[\frac{\alpha}{\alpha+\beta}\log_2\frac{\alpha+\beta}{\alpha} + \frac{\beta}{\alpha+\beta}\log_2\frac{\alpha+\beta}{\beta}\right]$$

d) Para $\alpha=\beta$

$$I(X;Y) = 2\alpha\cdot\left[\frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2\right] = 2\alpha$$

$$C = \max_{\alpha} I(X;Y) \qquad \text{con} \qquad 0<\alpha\leq 1/2$$

$$C = I(X;Y)\Big|_{\alpha=1/2} = 1 \text{ bit/símbolo}$$

En este caso el repetidor nunca recibe borrados.

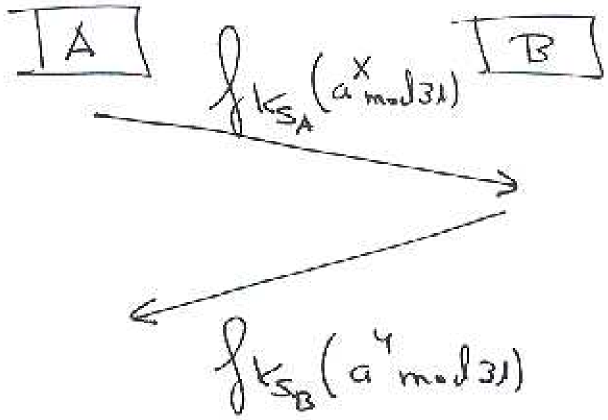
Para $\alpha = 2\beta$, no se generan borrados si $1-\alpha-\beta=0$, por lo que $1-3\beta=0 \Rightarrow \beta = 1/3$ y $\alpha = 2/3$

$$I(X;Y)\Big|_{\alpha=2\beta} = \beta\left[3\log_2 3 - 2\right] \Rightarrow C = \frac{1}{3}\left[3\log_2 3-2\right] = 0'91 \text{ bi}$$

Ejercicio 2

$a = 17$ operaciones en $\mathbb{Z}_{31}$

$x = 3 \quad y = 11$



a) Secreto compartido $a^{xy} \bmod 31 = 17^{33} \bmod 31 = 15$

$K_{P_A} = (187, 319) \qquad K_{P_B} = (1201, 1357)$

b) $K_{S_A} = (d, 319)$

$\Phi(319) = 28 \cdot 10 = 280$

$e \cdot d + k\,\Phi(n) = 1 \Rightarrow d = 3$

$K_{S_B} = (d', 1357)$

$\Phi(1357) = 22 \cdot 58 = 1276$

$e' d' + k' \Phi(n') = 1 \Rightarrow d' = 17$

c)

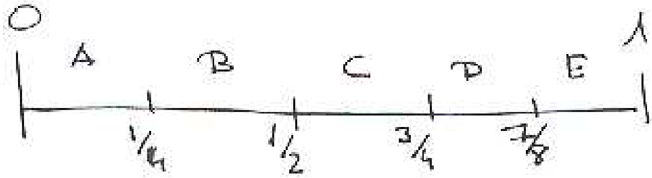
$$a^x \bmod p = 17^3 \bmod 31 = 15$$

$$f_{K_{S_A}}(15) = 15^d \bmod n = 15^3 \bmod 319 = 185$$

$$a^y \bmod p = 17^{11} \bmod 31 = 22$$

$$f_{K_{S_B}}(22) = 22^{d'} \bmod n' = 22^{17} \bmod 1357 = 344$$

Ejercicio 3



$$I_A = [0, 0'25)$$
$$I_B = [0'25, 0'5)$$
$$I_C = [0'5, 0'75)$$
$$I_D = [0'75, 0'875)$$
$$I_E = [0'875, 1)$$

Valor recibido

$$x_0 = 0'55$$

Longitud 5

Iteración

$$x_{n+1} = \frac{x_n - i_j}{\Delta_j} \quad \text{con } x_n \in I_j$$

$$x_0 \in I_C \Rightarrow C$$

$$x_1 = \frac{x_0 - i_C}{\Delta_C} = \frac{0'55 - 0'5}{0'25} = \frac{0'05}{0'25} = 0'2 \in I_A \Rightarrow A$$

$$x_2 = \frac{0'2 - 0}{0'25} = 0'8 \in I_D \Rightarrow D$$

$$x_3 = \frac{0'8 - 0'75}{0'125} = \frac{0'05}{0'125} = 0'4 \in I_B \Rightarrow B$$

$$x_4 = \frac{0'4 - 0'25}{0'25} = \frac{0'15}{0'25} = 0'6 \in I_C \Rightarrow C$$

Decodificación CADBC