Ejercicio 1. Dos fuentes de información, S1 y S2, emiten símbolos de un alfabeto {A,B,C,D,E,F,G,H,I} con una probabilidad:

$$P(A)=1/3;\ P(B)=P(C)=P(D)=P(E)=P(F)=1/9;\ P(G)=P(H)=P(I)=1/27.$$

Ambas fuentes emplean respectivamente un canal de comunicaciones ternario para transmitir la información. Para maximizar la explotación del ancho de banda del canal se emplea en cada caso un codificador de fuente cuyos códigos emplean los símbolos del alfabeto **{-1,0,1}**.

a) Determine si existe un código instantáneo donde la codificación de todos los símbolos de fuente de lugar a palabras código de longitud 2
b) Halle cuál es la longitud media mínima de las palabras código para una fuente
c) Calcule mediante el algoritmo de Huffman las palabras código para cada uno de los símbolos de fuente. ¿ Cuál es la eficiencia del código resultante ?
d) Razone cuál sería una cota superior de la entropía conjunta de las fuentes S1 y S2 en bits.

Se observa en la generación de símbolos de las fuentes que existe una dependencia entre las fuentes S1 y S2. Esta dependencia se manifiesta de la siguiente manera:

i) Cuando S1 emite A entonces S2 sólo emite A
ii) Cuando S1 emite B, C o D entonces S2 sólo emite B, C o D
iii) Cuando S1 emite E, F, G, H o I entonces S2 sólo emite E, F, G, H o I

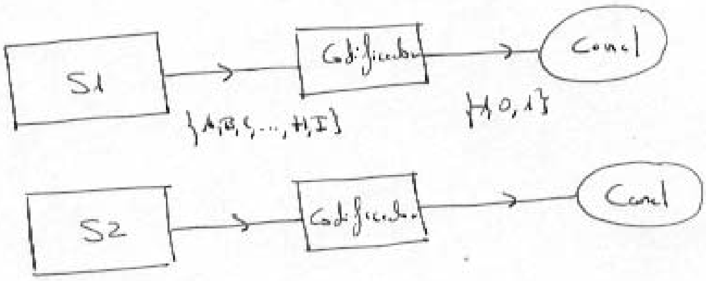
e) Teniendo en cuenta la dependencia entre las fuentes, calcule la entropía de la fuente S2 en bits para los casos en que la fuente S1 toma el valor: S1=A y S1=C.

Dos fuentes de información S1 y S2

$P(A) = 1/3$

$P(B) = P(C) = P(D) = P(E) = P(F) = 1/9$

$P(G) = P(H) = P(I) = 1/27$



a) Para que un código sea instantáneo debe cumplir la desigualdad de Kraft

$$\sum_{k=1}^{n} D^{-l_k} \leq 1$$

En nuestro caso:

$n = 9$ número de símbolos de fuente

$D = 3$ número de símbolos que emplean los códigos

$l_k = 2 \quad \forall k$ longitud de todos los códigos.

$$\sum_{k=1}^{9} 3^{-2} = \sum_{k=1}^{9} \frac{1}{9} = 1 \leq 1 \quad \text{(cumple)}$$

b) $\bar{L}_{min} = H$

Puesto que el código es ternario debemos utilizar base 3

$$\bar{L}_{min} = \sum_{k=1}^{9} p_k \cdot \log_3 \frac{1}{p_k} = -\sum_{k=1}^{9} p_k \log_3 p_k$$

$$= \frac{1}{3} \log_3 3 + 5 \cdot \frac{1}{9} \log_3 3^2 + 3 \cdot \frac{1}{27} \log_3 3^3$$

$$= \frac{1}{3} + \frac{10}{9} + \frac{1}{3} = 1'77$$

$$\boxed{\bar{L}_{min} = 1'77}$$

c) Calcular la codificación por Huffman

$$\begin{array}{l} A \to 1/3 \\ B \to 1/9 \\ C \to 1/9 \\ D \to 1/9 \\ \left.\begin{array}{l} E \to 1/9 \\ F \to 1/9 \\ \left.\begin{array}{l} G \to 1/27 \\ H \to 1/27 \\ I \to 1/27 \end{array}\right\} J \to 1/9 \end{array}\right\} K \to 1/3 \end{array}$$

$$\begin{array}{l} A \to 1/3 \\ K \to 1/3 \\ \left.\begin{array}{l} B \to 1/9 \\ C \to 1/9 \\ D \to 1/9 \end{array}\right\} L \to 1/3 \end{array}$$

Resultando:

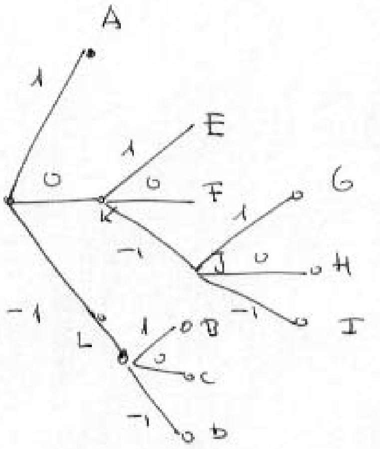


Tabla de codificación:

$A \longrightarrow 1$

$B \longrightarrow -1\ \ 1$

$C \longrightarrow -1\ \ 0$

$D \longrightarrow -1\ \ -1$

$E \longrightarrow 0\ \ 1$

$F \longrightarrow 0\ \ 0$

$G \longrightarrow 0\ \ -1\ \ 1$

$H \longrightarrow 0\ \ -1\ \ 0$

$I \longrightarrow 0\ \ -1\ \ -1$

Dado que la longitud del código de cada símbolo coincide con la información que proporciona (en base 3) entonces es inmediato que:

$$L = 1'77 \Rightarrow \qquad E = \frac{H}{L} = 1$$

d) Una cota superior de $H(S1, S2)$ se obtiene cuando ambas fuentes son independientes:

$$H(S1, S2) \leq H(S1) + H(S2) \underset{\text{iguales}}{=} 2H(S_1) = 2H(S_2)$$

Para expresar la información en bits empleamos base 2

$$H(S_1) = \frac{1}{3}\log_2 3 + \frac{5}{9}\log_2 3^2 + \frac{3}{27}\log_2 3^3 = 2'81$$

$$\boxed{H(S_1, S_2) \leq 5'63} \text{ bits}$$

e) Cuando $S_1 = A \Longrightarrow S_2 = A$

$$S_1 = C \begin{cases} \rightarrow S_2 = B \\ \rightarrow S_2 = C \\ \rightarrow S_2 = D \end{cases}$$

Las probabilidades condicionadas serán:

$$P(S_2 = A / S_1 = A) = 1$$

Para el caso $S_1 = C$ hay tres símbolos. Considerando que estos símbolos mantienen la relación de probabilidades de la fuente S2 entonces:

$$P(S_2 = B / S_1 = C) + P(S_2 = C / S_1 = C) + P(S_2 = D / S_1 = C) = 1$$

$$P(S_2 = B / S_1 = C) = \frac{P(S_2 = B)}{P(S_2 = B) + P(S_2 = C) + P(S_2 = D)} = 1/3$$

De la misma manera $P(S_2 = C / S_1 = C) = P(S_2 = D / S_1 = C) = 1/3$

Finalmente:

$$H(S_2 / S_1 = A) = P(S_2 = A / S_1 = A) \log_2 \frac{1}{P(S_2 = A / S_1 = A)} = 0$$

$$H(S_2 / S_1 = C) = \underset{\substack{\uparrow \\ \text{todos} \\ \text{son iguales}}}{3} \cdot P(S_2 = B / S_1 = C) \cdot \log_2 \frac{1}{P(S_2 = B / S_1 = C)}$$

$$= 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1'58 \text{ bits}$$

Se puede comprobar que $H(S_2 / S_1) = 1'23$ bits

$$H(S_1, S_2) = H(S_1) + H(S_2 / S_1) = 5'1 \text{ bits}$$

Ejercicio 2. Para facilitar el desarrollo de nuevos servicios a través de redes celulares una operadora incorpora en sus teléfonos móviles tres claves:

i) S: clave secreta Triple-DES asociada al móvil
ii) K_{Pop}: clave pública RSA de la operadora
iii) K_{Sm}: clave privada RSA asociada al móvil

Para dar soporte a los nuevos servicios la operadora dispone de un servidor que puede acceder a las claves:

i) K_{Sop}: clave secreta RSA de la operadora
ii) K_{Pm}: clave pública RSA de cada móvil

En un teléfono móvil se instala una aplicación que permite acceder al servicio de televoto de un concurso. El servicio emplea un sencillo algoritmo de clave simétrica. La aplicación garantiza la confidencialidad de la votación y la identificación de usuario del servicio a través de un número de identificación *k* que se emplea también como clave simétrica del algoritmo simple de cifrado.

a) Describa el mecanismo empleado por la operadora para la autenticación del teléfono móvil
b) Teniendo en cuenta que las aplicaciones residentes en el teléfono sólo pueden acceder a las claves asimétricas instaladas en el dispositivo por la operadora, proponga un método para transferir de forma confidencial y con firma digital el identificador de usuario *k* desde el móvil al servidor.

Considerando el caso en que los valores empleados son:

K_{Pm}: (e,n)= (35,119) K_{Sm}: (d,n)= (11,119)

K_{Pop}: (e,n)= (17, 1357) K_{Sop}: (d,n)= (1201,1357)

k= 19

c) Determine el valor enviado al servidor de televotación por el teléfono móvil.

El algoritmo simple de cifrado que emplea la aplicación de televoto del teléfono móvil es del tipo polialfabético. El alfabeto empleado se compone de los dígitos {0,1,2,...,14,15} de forma que se puede codificar cada símbolo con cuatro bits. La clave empleada está compuesta de dos números que se derivan de los digitos de *k* (en este caso {1,9}). El usuario enviará dos dígitos para identificar el valor de su votación.

d) Suponiendo que el usuario del móvil desee votar el elemento **05**, halle el valor binario del criptograma resultante de cifrado polialfabético.

Para robustecer la seguridad del servicio de televoto se decide aplicar el modo CFB al cifrado polialfabético. El CFB se diseña para que opere con mensajes de sólo dos bits y se inicializa con el valor obtenido de la suma de los dígitos de *k* en módulo 16.

e) Obtenga el valor binario del criptograma para el cifrado polialfabético operando en el modo CFB descrito.

a) Autenticación de dispositivo $\Rightarrow$ Desafío

Se emplea la clave secreta S asociada al móvil que es del tipo Triple-DES.

La operadora envía un mensaje en claro m y el móvil lo devuelve cifrado con la clave simétrica S.

La operadora recibe el mensaje m cifrado por el móvil y comprueba que es el dispositivo. ~~y~~

La comprobación se realiza descifrando el mensaje y ~~con~~ verificando que es igual que el original.

móvil — Operadora

$$\text{móvil} \xleftarrow{m} \text{Operadora}$$

$$E_S(m) \longrightarrow D_S[E_S(m)] \stackrel{?}{=} m$$

b) Móvil — Operadora

Móvil:

$$k$$

$$\downarrow$$

$$D_{KS_m}(k)$$

$$\downarrow$$

$$C = E_{KP_{op}}[D_{KS_m}(k)] \xrightarrow{\;C\;} D_{KS_{op}}[C]$$

Operadora:

$$D_{KS_{op}}[C]$$

$$\uparrow$$

$$E_{KP_m}[D_{KS_{op}}[C]]$$

$$\uparrow$$

$$k = E_{KP_m}\Big[D_{KS_{op}}\big[\overbrace{E_{KP_{op}}[D_{KS_m}(k)]}^{C}\big]\Big]$$

c) $K_{P_m} = (35, 119)$; $K_{S_m} = (11, 119)$

$K_{P_{op}} = (17, 1357)$; $K_{S_{op}} = (1201, 1357)$

$k = 19$

$$C = E_{K_{P_{op}}}\left[D_{K_{S_m}}(k)\right]$$

$$D_{K_{S_m}}(m) = m^d \bmod n = 19^{11} \bmod 119 = \left((19^2)^2 \cdot 19\right)^2 \cdot 19 \bmod 119$$

$$D_{K_{S_m}}(m)\Big|_{m=19} = 59$$

$$E_{K_{P_{op}}}(m) = m^e \bmod n = 59^{17} \bmod 1357 =$$

$$= \left(\left(\left((59)^2\right)^2\right)^2\right)^2 \cdot 59 \bmod 1357 = 236$$

$$C = E_{K_{P_{op}}}\left[D_{K_{S_m}}(19)\right] = 236$$

d) Cifrado polialfabético $K = \{ k_0 = 1, k_1 = 9 \}$

$d = 2$, $n = 16$

$$E_K(m_i) = \left(m_i + k_{(i \bmod d)}\right) \bmod n$$

$m_0 = 0$ $m_1 = 5$

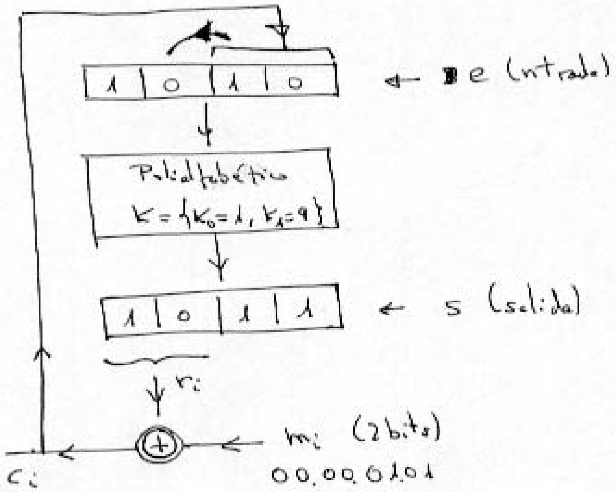
$E_K(0) = \left(0 + k_{0 \bmod 2}\right) \bmod 16 = (0+1) \bmod 16 = 1$

$E_K(5) = \left(5 + k_{1 \bmod 2}\right) \bmod 16 = (5+9) \bmod 16 = 14$

Criptograma enviado = 00011110

e) Suma de dígitos de k en módulo 16 =>

$$(1 + 9) \bmod 16 = 10 = 1010_2 \text{ (binario)}$$



e decimal	e	s	r_i	m_i	c_i	nueva e
10	1010	1011	10	00	10	1010
10	1010	0011	00	00	00	1000
8	1000	1001	10	01	11	0011
3	0011	1100	11	01	10	1110

Criptograma enviado = 1000 1110