Control. Mata.

(1)

Transmisión de Datos. Control de Primavera de 2008.

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

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

La fuente F es caracterizable por un modelo markoviano de dos estados donde la probabilidad de transición entre los estados es siempre igual a 1-p.

a) Evalúe la entropía H(F) de la fuente para un valor p genérico.

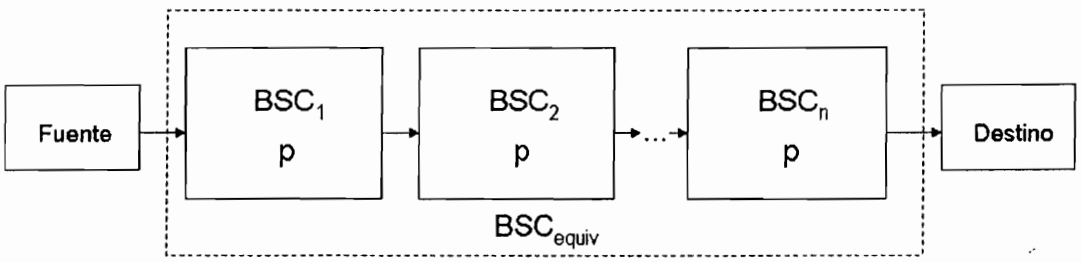
b) Aplicando una codificación de fuente por ráfagas resulta una fuente F' cuyos símbolos representan la longitud de las ráfagas de F, {1, 2, 3, ...}. Determine la entropía H(F') para un valor p genérico.

c) Sabiendo que en la práctica la fuente F no genera ráfagas de longitud mayor a 7, se realiza una codificación de las longitudes utilizando el algoritmo LZ-78 con un diccionario de 32 posiciones (5 bits) y con una codificación del valor de la longitud de 3 bits. Indique cuál será la codificación en hexadecimal resultante para la secuencia de longitudes:

1 2 4 2 4 1 4 3 1 3 3 1 4 3 2 2

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

Ejercicio 2. Se desea analizar el comportamiento de n canales binarios simétricos, con probabilidad de error p, conectados en serie como se muestra en la figura:



Responda a las siguiente cuestiones:

a) Para el caso de dos canales BSC en cascada (n=2), determine la matriz estocástica de probabilidades del canal BSC equivalente.

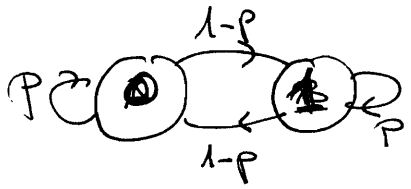
b) Determine la probabilidad de error del BSC equivalente, p_{equiv}, cuando n=2. Halle la capacidad del canal BSC equivalente para este caso n=2.

c) Para el caso el caso general donde $p<<1/n$ obtenga un valor aproximado de p_{equiv} que dependa sólo de n y p. Para este caso especifique una expresión simple de la capacidad del canal BSC equivalente.

Primavera 2008

Ejercicio 1

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



a) Por simetría $P(F=0) = P(F=1) = 1/2$

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

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

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

Finalmente

$$H(F) = P(F=0) \cdot H\left(F_n / F_{n-1}=0\right) + P(F=1)\, H\left(F_n / F_{n-1}=1\right)$$

$$\boxed{H(F) = H(p)}$$

b) Alfabeto de $F' = \{1,2,3,4,\ldots\}$

$$\text{Prob}[F'=k] = \text{Prob}[L=k] = p^{k-1}(1-p)$$

$p_1 = \text{Prob}[F'=1] = 1-p$

$p_2 = \text{Prob}[F'=2] = (1-p)p$

$\vdots$

$p_k = \text{Prob}[F'=k] = (1-p)p^{k-1}$

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

$$H(F') = \sum_{k=1}^{\infty} p_k \log_2 \frac{1}{p_k} = \sum_{k=1}^{\infty} \left[(1-p) p^{k-1} \log_2 \frac{1}{(1-p) p^{k-1}} \right]$$

$$H(F') = -(1-p) \cdot \sum_{k=1}^{\infty} p^{k-1} \left[\log_2 (1-p) + \log_2 p^{k-1} \right] =$$

$$= -(1-p) \left[\sum_{k=1}^{\infty} \log_2 (1-p) \cdot p^{k-1} + \sum_{k=1}^{\infty} (k-1) p^{k-1} \log_2 p \right]$$

$$= -(1-p) \log_2 (1-p) \sum_{k=1}^{\infty} p^{k-1} - (1-p) \log_2 p \sum_{k=1}^{\infty} (k-1) p^{k-1}$$

$$= -(1-p) \log_2 (1-p) \sum_{k=1}^{\infty} p^{k-1} - (1-p) \log_2 p \left(\sum_{k=1}^{\infty} k p^{k-1} - \sum_{k=1}^{\infty} p^{k-1} \right)$$

$$= \sum_{k=1}^{\infty} p^{k-1} \cdot \left[-(1-p) \log_2 (1-p) + (1-p) \log_2 p \right] - (1-p) \log_2 p \sum_{k=1}^{\infty} k p^{k-1}$$

$$= \sum_{k=1}^{\infty} p^{k-1} \cdot \left((1-p) \log_2 \frac{p}{1-p} \right) - (1-p) \log_2 p \sum_{k=1}^{\infty} k p^{k-1}$$

$$= \frac{1}{1-p} \left((1-p) \log_2 \frac{p}{1-p} \right) - (1-p) \log_2 p \, \frac{1}{p} \sum_{k=1}^{\infty} k p^{k}$$

$$= \log_2 \frac{p}{1-p} - \frac{1-p}{p} \log_2 p \, \frac{p}{(1-p)^2}$$

$$= \log_2 \left(\frac{p}{1-p} \right) - \frac{1}{1-p} \log_2 p$$

$$= \log_2 p - \log_2 (1-p) - \frac{1}{1-p} \log_2 p$$

$$= -\frac{p}{1-p} \log_2 p - \log_2 (1-p)$$

$$H(F') = \log_2\left(\frac{P}{1-P}\right) - \frac{1}{1-P}\log_2 P = \frac{P}{1-P}\log_2\frac{1}{P} + \log_2\frac{1}{1-P}$$

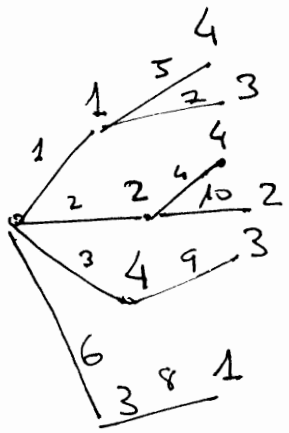
c) $F' = \{1, 2, 3, \ldots, 6, 7\}$

LZ-78 (posición, nuevo carácter)

(posición: 5 bits; nuevo carácter: 3 bits)

1 2 4 2 4 1 4 3 1 3 3 1 4 3 2 2

(0,1) (0,2) (0,4) (2,4) (1,4) (0,3) (1,3) (6,1) (3,3) (7,2)



Posición	Carácter
1	1
2	2
3	4
4	24
5	14
6	3
7	13
8	31
9	43
10	22

Codificación

00000.0 001 → 01
00000.0 010 → 02
00000.0 100 → 04
00001.0 100 → 14
00000.1 100 → 0C
00000.0 011 → 03
00000.1 011 → 0B
00001.0 001 → 31
00001.1 011 → 1B
00001.0 010 → 12

Transmisión de Datos. Control de Primavera de 2008.

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

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

La fuente F es caracterizable por un modelo markoviano de dos estados donde la probabilidad de transición entre los estados es siempre igual a 1-p.

a) Evalúe la entropía H(F) de la fuente para un valor p genérico.

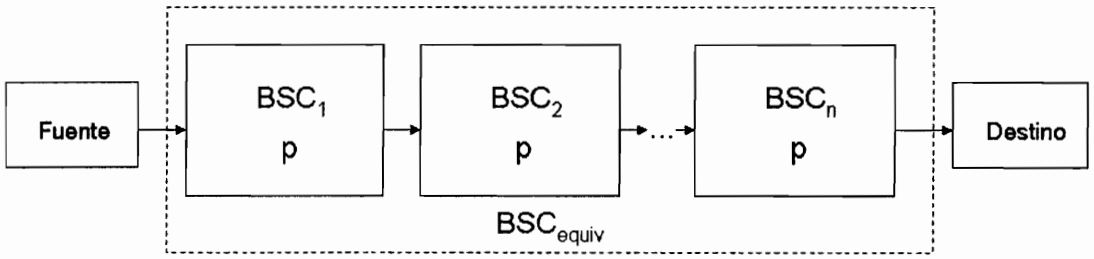
b) Aplicando una codificación de fuente por ráfagas resulta una fuente F' cuyos símbolos representan la longitud de las ráfagas de F, {1, 2, 3, ...}. Determine la entropía H(F') para un valor p genérico.

c) Sabiendo que en la práctica la fuente F no genera ráfagas de longitud mayor a 7, se realiza una codificación de las longitudes utilizando el algoritmo LZ-78 con un diccionario de 32 posiciones (5 bits) y con una codificación del valor de la longitud de 3 bits. Indique cuál será la codificación en hexadecimal resultante para la secuencia de longitudes:

1 2 4 2 4 1 4 3 1 3 3 1 4 3 2 2

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

Ejercicio 2. Se desea analizar el comportamiento de n canales binarios simétricos, con probabilidad de error p, conectados en serie como se muestra en la figura:



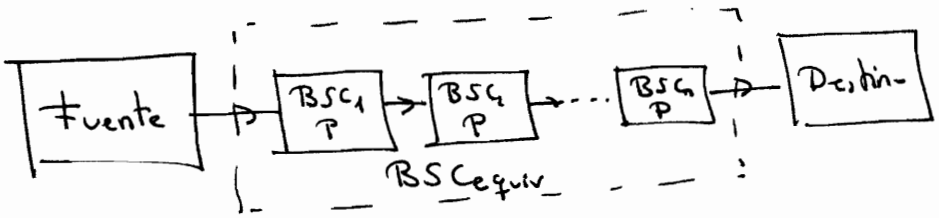
Responda a las siguiente cuestiones:

a) Para el caso de dos canales BSC en cascada (n=2), determine la matriz estocástica de probabilidades del canal BSC equivalente.

b) Determine la probabilidad de error del BSC equivalente, p_{equiv}, cuando n=2. Halle la capacidad del canal BSC equivalente para este caso n=2.

c) Para el caso el caso general donde $p<<1/n$ obtenga un valor aproximado de p_{equiv} que dependa sólo de n y p. Para este caso especifique una expresión simple de la capacidad del canal BSC equivalente.

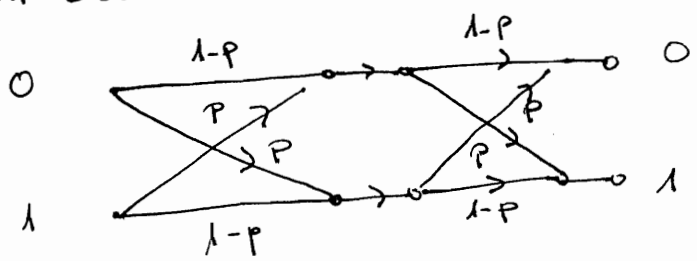
Ejercicio 2



a) $n=2$

$$Q_{BSC_1} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \triangleq Q_{n=1}$$

En cascada:



$$P(S=0/e=0) = (1-p)^2 + p^2$$

$$P(S=1/e=0) = p\cdot(1-p) + (1-p)\cdot p = 2p(1-p)$$

$$P(S=1/e=1) = (1-p)^2 + p^2$$

$$P(S=0/e=1) = p(1-p) + (1-p)\cdot p = 2p(1-p)$$

$$Q_{n=2} = \begin{bmatrix} (1-p)^2+p^2 & 2p(1-p) \\ 2p(1-p) & (1-p)^2+p^2 \end{bmatrix} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

Se observa que: $Q_{n=2} = Q_{n=1}^2$

En general $\boxed{Q_n = Q_{n=1}^n}$

b) $n=2$

$$Q_{equiv} = \begin{bmatrix} 1-p_{equiv} & p_{equiv} \\ p_{equiv} & 1-p_{equiv} \end{bmatrix} = \begin{bmatrix} (1-p)^2+p^2 & 2p(1-p) \\ 2p(1-p) & (1-p)^2+p^2 \end{bmatrix}$$

Identificando $p_{equiv} = 2p(1-p) = 2p - 2p^2$

La capacidad para el BSC es: $C = 1 - H(p)$

Para el BSC$_{equiv}$ será: $C = 1 - H(p_{equiv}) = 1 - H(2p-2p^2)$

c) Si $p << 1/n < 1$ entonces $p^i << p$ con $i = 2, 3, 4, \ldots$

Considerando que se produce un error en recepción cuando hay un número impar de errores en los n canales podemos hallar la expresión general. Así,

$$p_i \triangleq \text{Prob}[\text{ } i \text{ errores en } n \text{ canales }] = \binom{n}{i} p^i (1-p)^{n-i}$$

$$p_{equiv} = p_1 + p_3 + p_5 + \ldots + p_{2k-1} \quad , \quad k = \left\lfloor \frac{n+1}{2} \right\rfloor$$

$$p_{equiv} = \sum_{k=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor} p_{2k-1} = \sum_{k=1}^{\left\lfloor \frac{n+1}{2} \right\rfloor} \binom{n}{2k-1} p^{2k-1} (1-p)^{n-2k+1}$$

Aproximando con $p >> p^3 >> p^5 \ldots$

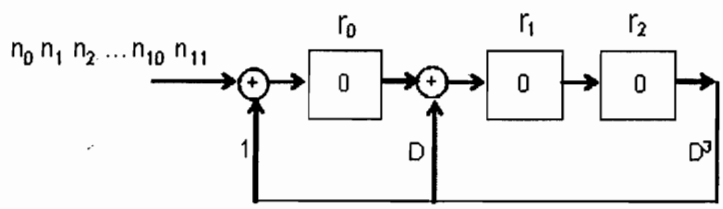
$$p_{equiv} \simeq n p (1-p)^{n-1}$$

Considerando que $1-p \simeq 1$, entonces

$$p_{equiv} \simeq np$$

y $$C = 1 - H(np)$$

Ejercicio 3. Un sistema de votación desde terminales móviles emplea el algoritmo RSA para proporcionar el servicio de confidencialidad a la aplicación que envía mensajes al servidor. Para obtener la clave pública del servidor los terminales acuden a una entidad de certificación, EC, que les proporciona dicha clave firmada. El formato empleado por la EC dispone de 12 bits para el valor de n de la clave pública a certificar y 5 bits concatenados para el valor de la firma del resumen de dicho valor de la clave, así: ($v = 0x\ n_{11}\ n_{10} \ldots n_1\ n_0\ f_4\ ..f_1\ f_0$). 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 (n), el resumen se deriva directamente del polinomio de estado del LFSR como se muestra en la figura.



Teniendo en cuenta que:

i) La clave pública de la EC tiene por valor: $K_P = (e,n) = (17, 33)$.

ii) El valor de v proporcionado por la EC para el servidor de votación es:
$v = 29Bh \mid 1Bh$

iii) El valor e empleado para todas las claves públicas RSA del sistema es común y de valor $e = 13$.

iv) Se supone que un número grande es aquel de valor mayor que 2.

Responda la siguientes cuestiones:

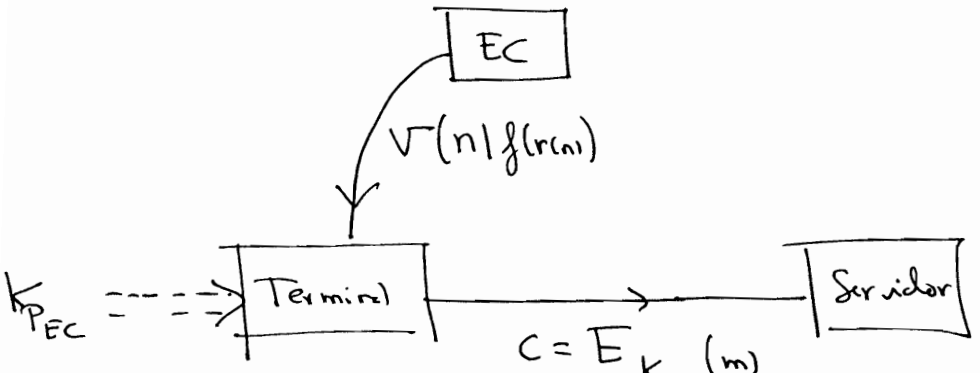
a) Verifique que la clave pública del servidor es válida.

b) El conocimiento de la función de Euler $\phi(n)$ permite factorizar n en un sistema RSA. Para un valor de $\phi(n)=616$, factorice la clave pública del servidor de votación.
Nota: Exprese (p+q) como función de n y $\phi(n)$ y utilice la igualdad $(p-q)^2=(p+q)^2-4pq$.

c) Determine si los p y q hallados son primos fuertes.

d) Calcule la clave privada del servidor de votación.

Ejercicio 3



$V = 29Bh \,;\, 1Bh$

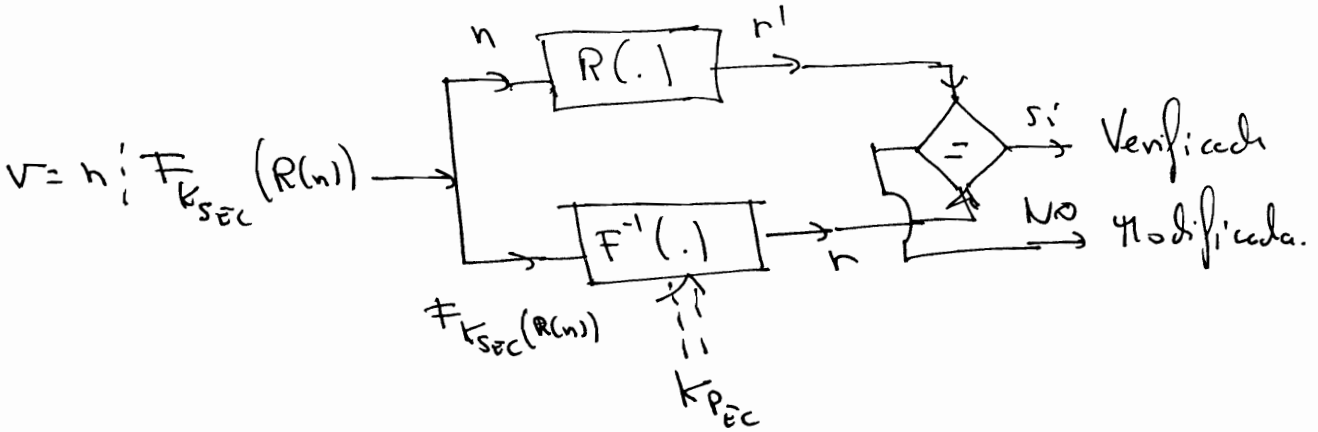
$n = 29Bh = 667$

$F_{K_{SEC}}(R(n)) = 27$

$K_{P_{EC}} = (e, n) = (17, 33)$

$K_{P_{Serv}} = (e, n) = (13, 667)$

a) Verificación de una clave pública



r' se obtiene de operar el LFSR. Como n tiene 12 bits, expresamos n en forma polinomial:

$$N(D) = n_{11} D^{11} + n_{10} D^{10} + \dots + n_1 D + n_0$$

Operamos el LFSR un número de veces $k = \text{grado}(N(D)) + 1$ y obtenemos el estado al cabo de k iteraciones:

$$P^{(k)}(D) = \left(D^k P^{(0)}(D) + N(D)\right) \bmod C(D).$$

Dado que $P^{(0)}(D) = \emptyset$ y $k = 12$, tenemos que:

$$P^{(12)}(D) = N(D) \bmod C(D)$$

Realizando la operación:

$h = 29Bh = 0010.1001.1011_{L2} \Leftrightarrow N(D) = D^9 + D^7 + D^4 + D^3 + D + 1$

$D^9 + D^7 + D^4 + D^3 + D + 1 \mod D^3 + D + 1 = D + 1 = R'(D)$

$R'(D) = D + 1 \Leftrightarrow r' = 11_{L2} = 3$

Por otro lado,

$$r = \mathcal{F}^{-1}_{K_{P_{EC}}}\left[\mathcal{F}_{K_{S_{EC}}}(R(m))\right] = \mathcal{F}^{-1}_{K_{P_{EC}}}[27] = 27^{e_{EC}} \mod n_{EC}$$

$$r = 27^{17} \mod 33 = 3$$

Por lo tanto, $r = r' \Rightarrow h$ es válida. y queda verificada.

b) $n = 667 = p \cdot q$

$\varphi(n) = 616 = (p-1)(q-1) = p \cdot q - p - q + 1 = n - (p+q) + 1$

$(p+q) = n - \varphi(n) + 1 = 667 - 616 + 1 = 52$

$(p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4n = 52^2 - 4 \cdot 667 = 36$

$$\begin{cases} p+q = 52 \\ p-q = 6 \end{cases} \Rightarrow \begin{cases} p = 29 \\ q = 23 \end{cases}$$

c) Para que p y q sean primos fuertes, deben cumplir que:

Siendo $p' \triangleq \frac{p-1}{2}$; $q' \triangleq \frac{q-1}{2}$

i) p' y q' primos grandes, o
m.c.d (p', q') pequeño y p' y q' factor primo gran

$p' = \frac{29-1}{2} = 14 = 2 \cdot 7$ no es primo

$q' = \frac{23-1}{2} = 11 = 11 \cdot 1$ Sí es primo.

m.c.d $(p', q') = 1$ y p' y q' tienen un factor primo grande.

ii) $q'-1 = 10 = 2 \cdot 5$ tiene un factor primo grande

$p'-1 = 13 = 13 \cdot 1$ " " " " "

iii) $q'+1 = 12 = 2^2 \cdot 3$ " " " " "

$p'+1 = 15 = 3 \cdot 5$ " " " " "

Por lo tanto p y q son primos fuertes.

d) $K_{p_{serv}} = (e, n) = (13, 667)$

$\varphi(n) = 616$

Aplicando el algoritmo de Euclides Extendido.

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

$d = 237$

$k = -5$

$K_{S_{serv}} = (237, 667)$