**CONTROL DE TRANSMISIÓN DE DATOS.** **3 de diciembre 2006**
**GRUPO 40**

## Notas Importantes:

Un error conceptual grave, puede anular todo el problema.

### Problema 1 (50%)

Sea un canal discreto con de N símbolos (tanto a la entrada como a la salida, $N \geq 2$). $x_i \in \{0,..,N-1\}$ $y_i \in \{0,..,N-1\}$, que puede modelarse estadísticamente mediante $\Pr\{x_i = y_i\} = 1-p$ y $\Pr\{x_i = y_{(i+1) \bmod N}\} = p$. Sea una fuente sin memoria compuesta por 6 símbolos $F = \{A, B, C, D, E, F\}$ con probabilidades $\{0.3, 0.2, 0.2, 0.1, 0.1, 0.1\}$ respectivamente.

a) Calcule la información mutua entre la entrada y la salida del canal $I(X;Y)$, así como la capacidad de canal (C), en función de N y p. Particularice para N=4 y p=0.5 **(2 puntos)**

b) Realice una codificación de Huffman de la fuente F para el canal anterior (con N=4). Calcule la eficiencia de codificación **(1 punto)**

c) Calcule la entropía a la salida del canal (para N=4, p=0.5 y fuente F). **(1 punto)**

d) Realice una codificación aritmética de la secuencia BACCDE emitida por F **(1 punto)**

### Problema 2 (50%)

Sea $C(D) = D^7 + D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$ el polinomio de conexiones de un cifrador en flujo síncrono y $S(D) = D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$ el estado inicial. Tenemos dos usuarios RSA, **A**: $p_A = 67$, $q_A = 89$, $e_A = 31$ y **B**: $p_B = 73$, $q_B = 97$, $e_B = 31$.

e) Decodifique el criptograma C=7, enviado confidencialmente por A a B (usando RSA). Obtenga M. **(2 puntos)**

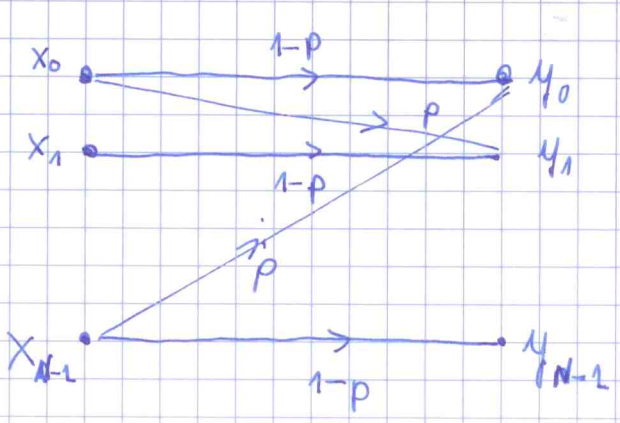
f) Calcule el estado del LFSR al cabo de número de iteraciones que indica M. **(1 punto)**

g) Vamos a cifrar en flujo el mensaje S (ASCII = 01010011) usando para ello un generador compuesto por dos LFSR con polinomios primitivos, cuyas salidas se unen en una puerta suma módulo 2 XOR para entregar la secuencia cifrante o clave S. Los polinomios asociados son: LFSR1 = $D^5 + D^2 + 1$; LFSR2 = $D^6 + D + 1$. Las semillas son todos 1s. Encontrar los primeros 8 bits de la secuencia cifrante y luego cifrar el mensaje. **(1 punto)**

h) Indicar el tamaño del mensaje máximo en bytes que se recomendaría cifrar con la clave $S_i$ completa generada en este caso y comentar porqué. **(1 punto)**

# PROBLEMA 1

a)




$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X)$$

$$H(Y) = -\sum_{i=0}^{N-1} p(y_i) \log_2 p(y_i)$$

$$H(Y/X) = H(p) \sum_{n=0}^{N-1} p(x_i) = H(p) \quad \text{(VER TEORÍA)}$$

$$\boxed{I(X;Y) = -\sum_{i=0}^{N-1} p(y_i) \log_2 p(y_i) - H(p)}$$

$$H(p) \triangleq -p \log_2 p - (1-p) \log_2 (1-p$$

$$C = \max_{p(a_i)} I(X;Y) = \log_2 N - H(p)$$

MAXIMIZAR $\sum_{i=0}^{N-1} p(y_i) \log_2 p(y_i)$ $\Rightarrow$ CUANDO SÍMBOLOS EQUIPROBABLES

para $N=4$, $p=2$ $\Rightarrow$ $\boxed{C = \log_2 N - H(p) = 1 \text{ bit}}$

b]

| | | | | | |
|---|---|---|---|---|---|
| A | (1) | 0'3 | | 0'3 | 0 |
| B | (2) | 0'2 | | 0'3 | 1 |
| C | (3) | 0'2 | | 0'2 | 2 |
| D | (00) | 0'1 | 00 | 0'2 | 3 |
| E | (01) | 0'1 | 01 | | |
| F | (02) | 0'1 | 02 | | |
| (dummy) | | 0 | | | |

$\bar{l} = 0'3 \cdot 2 + 0'7 \cdot 1 = 1'3$ dígitos cuaternarios

$H(F) = \sum_{i=1}^{6} -p(s_i) \log_4 p(s_i) = 1'223$ dígitos cuaternarios

($\log_4$ en dígitos cuaternarios)

($0'2446$ bits, con $\log_2$)

$$\boxed{E = \frac{H(F)}{\bar{l}} = \frac{1'223}{1'3} = 0'94}$$

todo en mismas unidades

c] ENTROPÍA A LA SALIDA DEL CANAL

$$H(Y) = \sum_{i=0}^{N-1} p(y_i) \log_2 \frac{1}{p(y_i)} = -\sum_{i=1}^{3} p(y_i) \log_2 p(y_i)$$ (N=4)

$p = 0'5$

$p(y_0) = (1-p)\, p(x_0) + p\, p(x_3) = 3/13$

$p(y_1) = (1-p)\, p(x_1) + p\, p(x_0) = 4/13$

$p(y_2) = (1-p)\, p(x_2) + p \cdot p(x_1) = 7/26$

$p(y_3) = (1-p)\, p(x_3) + p \cdot p(x_2) = 5/26$

Prob de símbolos a ENTRADA DE CANAL

Sabemos prob símbolos de fuente. Suponga mos que la fuente emite los símbolos según su prob

| p=0'3 | | | p=0'2 | | p=0'2 | | p=0'1 | p=0'1 | p=0'2 |
|---|---|---|---|---|---|---|---|---|---|
| A | A | A | B | B | C | C | D | E | F |
| CODIF: 1 | 1 | 1 | 2 | 2 | 3 | 3 | 00 | 01 | 02 |

$$p(x_i) = \frac{\#\text{ casos favorables}}{\#\text{ casos posibles}} =$$

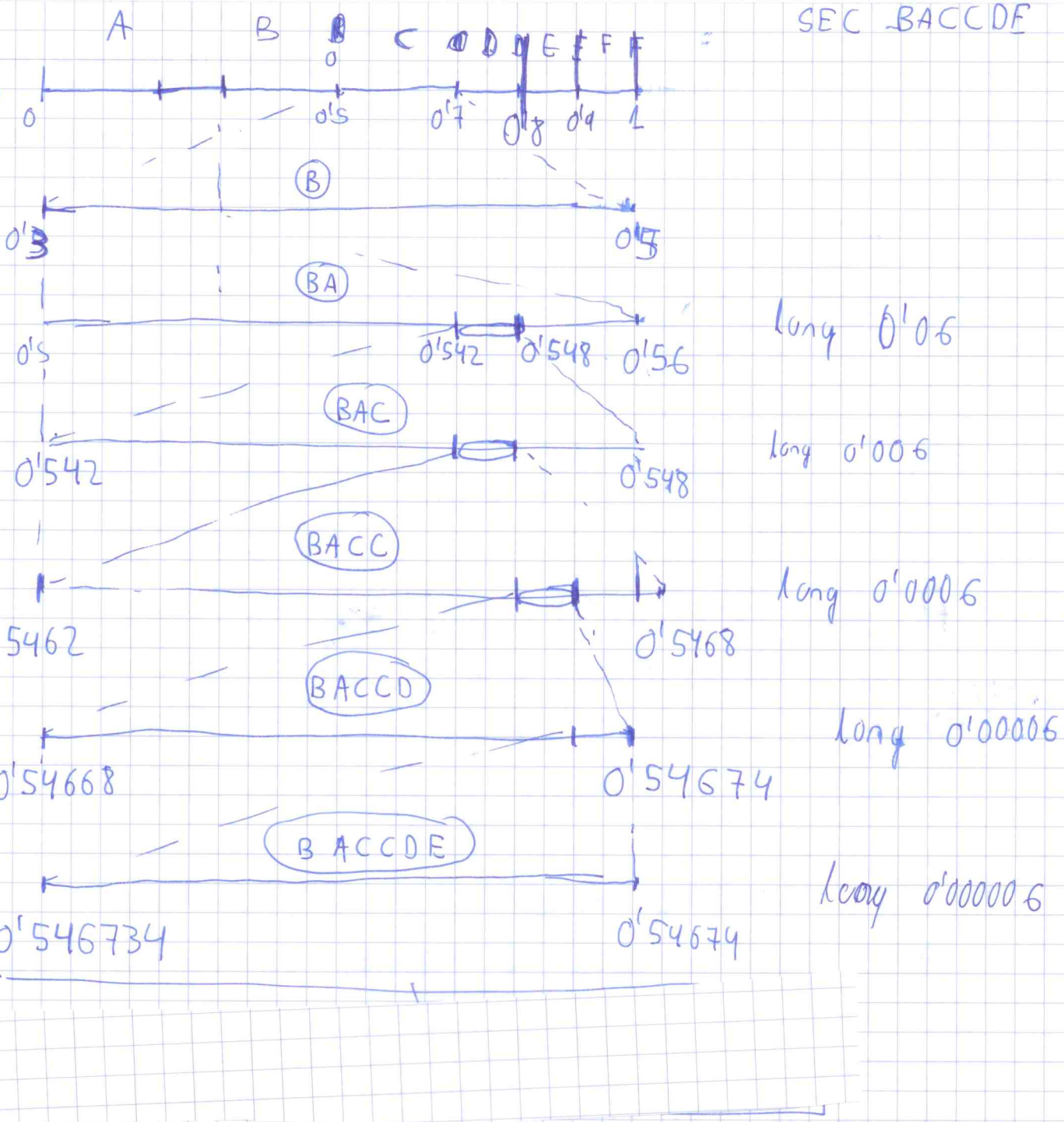
$p(x_0) = 4/13 \quad p(x_1) = 4/13 \quad p(x_2) = 3/13 \quad p(x_3) = 2/13$

$$H(X) = \frac{1}{26}\left(6 \log_2\left(\frac{13}{3}\right) + 8 \log_2\left(\frac{13}{4}\right) + 7 \log_2\left(\frac{26}{7}\right) + 5 \log_2\left(\frac{26}{5}\right)\right)$$

$$= 1'978 \text{ bits}$$

SEC BACCDE

d)




long / intervalo: $0'000006 = 6 \cdot 10^{-6}$

INTERVALO $[0'337872, 0'337896)$

| | S | P |
|---|---|---|
| A | 1 | p(0'3) |
| B | 2 | 0'2 |
| C | 3 | 0'2 |
| D | 0 0 | 0'2 |
| E | 0 1 | 0'1 |
| F | 0 2 | 0'2 |

Suponiendo NO MEMORIA

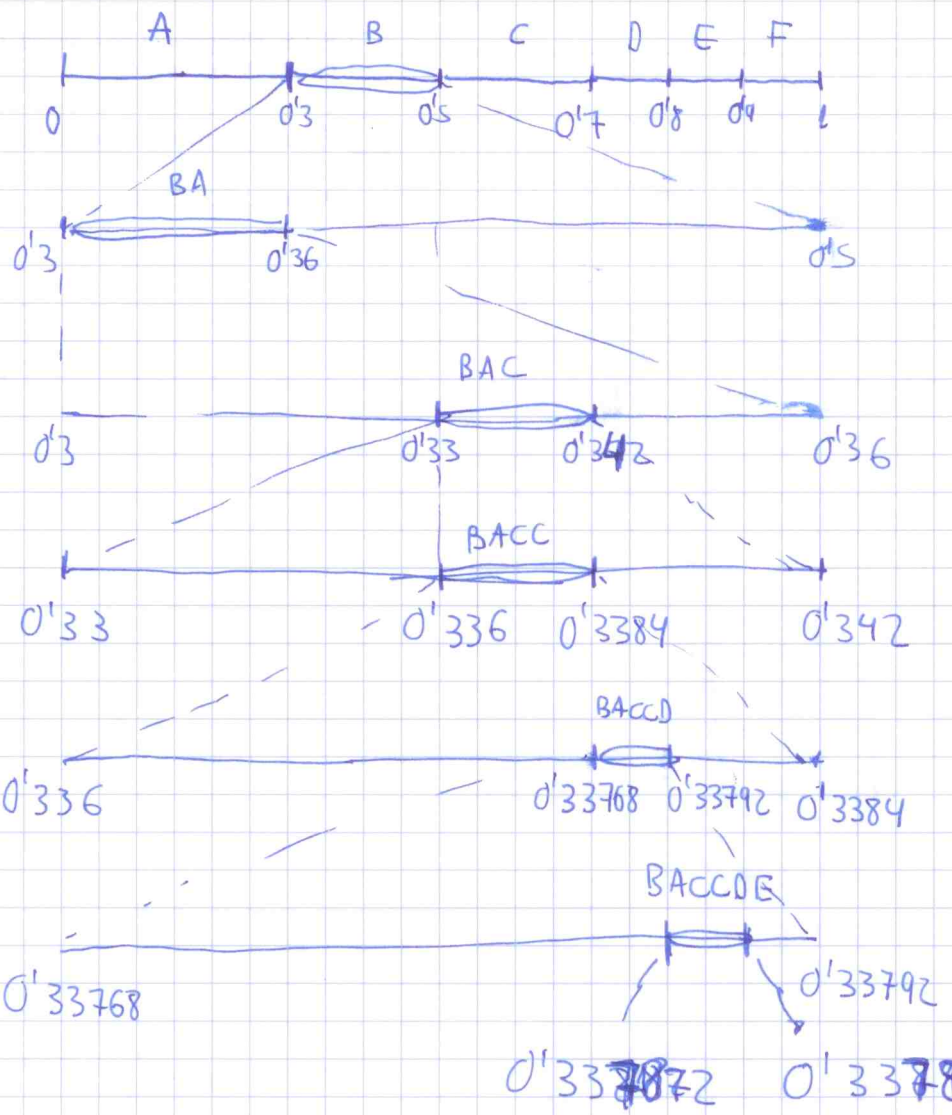
p(3) = 0'2

A A A B B C C D E F

1 1 1 2 2 3 3 0 0 0 1 0 2

p(0) = 4/13 p(2) = 3/13

p(1) = 4/13 p(3) 2/13




BACCDE

Long = 0'06

Long = 0'012

Long = 0'0024

Long = 0'00024

Long = 0'000024

[0'337872, 0'337896)

PROBLEMA 2

e) $A \to B \qquad C = E_{P_B}(m)$

B: $M = D_{S_B}(C) = C^{d_B} \bmod N_B$

$N_B = p_B \cdot q_B = 73 \cdot 97 = 7081$

$\phi(N_B) = (p_B - 1)(q_B - 1) = 6912$

$e_B d_B = k\,\phi(N_B) + 1 \Rightarrow \boxed{d_B = 223}$

$6912 = 1 \cdot 6912 + 0 \cdot 31$
$31 = 0 \cdot 6912 + 1 \cdot 31$ (×(-222))
$30 = 1 \cdot 6912 + (-222) \cdot 31$
$1 = (-1)\,6912 + 223 \cdot 31$

$\boxed{M = C^{d_B} \bmod N_B = 6892} = 6892$

f) Dado $S(D)$ y $C(D)$ $\quad L = m + 1 = 7 + 1 = 8$

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

$S^{6892}(D) = D^{6892} S(D) \bmod C(D) = D^4 \cdot D^{861 \cdot 8} S(D) \bmod C(D)$ (L=8 ✓)

$= D^4 (D^7 + D^6 + D^5 + D^4 + D^3 + D^2 + D + 1) \bmod C(D)$

$\boxed{S(D) = D^3}$ V

d) $L_1 = 31$ (período $LFSR_1$)

$L_2 = 63$ (período $LFSR_2$)

$$mcm(L_1, L_2) = 31 \cdot 63 = 1953$$

$$\#\,max\,(bytes) = \frac{1953}{8} = 244 \text{ bytes}$$

LUEGO, LA SECUENCIA $S_i$ SE REPITE

f)

| LFSR1 $(D^5+D^2+1)$ | | | | | LFSR2 $(D^6+D+1)$ | | | | | | $S_i$ | $R_{ii}$ | $C_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |

$$C_i = 01001000$$