25 Mayo 2006 . Control Aguilar

(1) $P(Y_1\backslash X_1) = 3/4 \Rightarrow P(Y_2\backslash X_1) = 1 - 3/4 = 1/4$

$P(Y_2\backslash X_2) = 1/2 \Rightarrow P(Y_1\backslash X_2) = 1 - 1/2 = 1/2$

$H(Y) = H(Y\backslash X_1)\cdot P(X_1) + H(Y\backslash X_2)\cdot P(X_2)$

$H(Y\backslash X_1) = P(Y_1\backslash X_1)\cdot \log_2 \frac{1}{P(Y_1\backslash X_1)} + P(Y_2\backslash X_1)\cdot \log_2 \frac{1}{P(Y_2\backslash X_1)} =$

$= \frac{3}{4}\cdot \log_2 \frac{4}{3} + \frac{1}{4} \log_2 4 = 0'3113 + 0'5 = 0'8113$ bits/símbolo

$H(Y\backslash X_2) = P(Y_1\backslash X_2)\cdot \log_2 \frac{1}{P(Y_1\backslash X_2)} + P(Y_2\backslash X_2)\cdot \log_2 \frac{1}{P(Y_2\backslash X_2)} =$

$= \frac{1}{2}\cdot \log_2 2 \cdot 2 = 1$ bit/símbolo

$P(x_1) + P(x_2) = 1$;; $\frac{1}{2}\cdot P(x_2) + P(x_2) = 1$;; $\frac{3}{2}\cdot P(x_2) = 1$;; $P(x_2) = \frac{2}{3}$

$P(x_1) = 1/3$

$$\boxed{H(Y) = 0'8113\cdot \frac{1}{3} + 1\cdot \frac{2}{3} = 0'9371 \ \frac{\text{bits}}{\text{símbolo}}}$$

(2)

$0'04 \Rightarrow A$

$\frac{0'04 - 0}{1/4} = 0'16 \Rightarrow A$

$\frac{0'16 - 0}{1/4} = 0'64 \Rightarrow B$ //

[Secuencia AAB]

(3) Sabemos que $\begin{cases} a^{\phi(n)-1} \bmod n = a^{-1} \bmod n, \text{ cuando} \\ \text{mcd}(a, n) = 1 \end{cases}$

1021 primo   91537 = 383 · 239, dos primos

Entonces,

$a \cdot a^{-1} = 1 + \underset{\text{entero}}{k} \cdot n$ ⇒ OK, mcd(1021, 91537) = 1.

¿$1021 \cdot 74682 = 1 + k \cdot 91537$? ⇒ K = 833, un entero! OK!

(4) Sabemos que para $n = \prod_i (p_i)^{\alpha_i} \Rightarrow \phi(n) = \prod_i (p_i)^{\alpha_i - 1} \cdot (p_i - 1)$

$7875 = 5^3 \cdot 3^2 \cdot 7$

$$\boxed{\phi(7875) = (5^2 \cdot 4) \cdot (3^1 \cdot 2) \cdot (7^0 \cdot 6) = 3600}$$

(5)

F_1	F_2	$F = mcm(F_1, F_2)$
1	1	1
1	2	2
1	3	3
1	4	4
2	1	2
2	2	2
2	3	6
2	4	4
3	1	3
3	2	6
3	3	3
3	4	12
4	1	4
4	2	4
4	3	12
4	4	4

→ todos los factores al máximo exponente

$\equiv$

F	p(F)
1	1/16
2	3/16
3	3/16
4	5/16
6	2/16
12	2/16

$$H(F) = \frac{1}{16} \cdot \log_2 16 + 2 \cdot \frac{3}{16} \cdot \log_2 \frac{16}{3} + \frac{5}{16} \cdot \log_2 \frac{16}{5} + 2 \cdot \frac{2}{16} \cdot \log_2 8 =$$

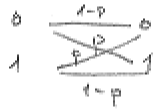
$$= \frac{4}{16} + \frac{6}{16} \cdot 2'4150 + \frac{5}{16} \cdot 1'678 + \frac{1}{4} \cdot 3 = \boxed{2'43 \ \frac{\text{bits}}{\text{símbolo}}}$$

(6)

$p(0) = 0'4$
$p(1) = 0'6$

— [BSC] —

$p = 0'1$



$p(0) = 0'4\,(1-p) + 0'6 \cdot p = 0'4 \cdot 0'9 + 0'6 \cdot 0'1 = 0'42$

$p(1) = 0'4 \cdot p + 0'6 \cdot (1-p) = 0'4 \cdot 0'1 + 0'6 \cdot 0'9 = 0'58$

$$\boxed{H(S) = 0'42 \cdot \log_2 \frac{1}{0'42} + 0'58 \cdot \log_2 \frac{1}{0'58} = 0'9814 \text{ bits/símbolo}}$$

(7) $D^L \bmod C(D) = 1$ para $C(D)$ primitivo, L = periodo

$$D^L \cdot P^{(0)}(D) \bmod C(D) = P^{(0)}(D)$$

$P^{(0)}(D) = D+1$, $P^{(0)}(D) = D+1$

$$\left(D^{L+1} + D^L\right) \bmod C(D) = D+1 \iff \left(D^{256} + D^{255}\right) \bmod C(D) = D+1$$

$L = 255 = 2^n - 1$, n = grado de $C(D)$

$$\boxed{n = \log_2 256 = 8}$$

(8) LZW de AABBCBCBABA

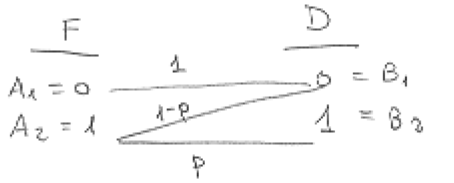
1	A
2	B
3	C
4	AA
5	AB
6	BB
7	BC
8	CB
9	BCB
10	BA
11	ABA

4 5 6 7 8 9 10 11

A A B B C BC B AB A

1 1 2 2 3 7 2 5

1º codifico
2º introduzco nueva palabra en el diccionario

(9) 

$$p(D \backslash F) = \begin{array}{c|cc} & B_1 & B_2 \\ \hline A_1 & 1 & 0 \\ A_2 & 1-p & p \end{array}$$

$$H(D \backslash F) = p(A=0) \cdot \underbrace{H(D \backslash A=0)}_{\emptyset = 1 \cdot \log_2 1} + p(A=1) \cdot \underbrace{H(D \backslash A=1)}_{(1-p) \cdot \log_2 \frac{1}{1-p} + p \cdot \log_2 \frac{1}{p} = H(p)} = p(A=1) \cdot H(p)$$

$$H(D) = \sum_{j=1}^{2} p(B_j) \cdot \log_2 \frac{1}{p(B_j)} = \cdots$$

$$p(D=0) = 1 \cdot p(A=0) + (1-p) \cdot p(A=1) = \overbrace{p(A=0) + p(A=1)}^{1} - p \cdot p(A=1)$$
$$= 1 - p \cdot p(A=1)$$

$$p(D=1) = p \cdot p(A=1)$$

$$\cdots = p \cdot p(A=1) \cdot \log_2 \frac{1}{p \cdot p(A=1)} + \left(1 - p \cdot p(A=1)\right) \cdot \log_2 \frac{1}{1 - p \cdot p(A=1)}$$

$$C = \max_{p\{A_i\}} \left[H(D) - H(D \backslash F) \right] \overset{\to\, p(A=1)=x}{=}$$

$$= \max_{\substack{p\{A_i\} \\ x}} \Big[\underbrace{(p x) \cdot \log_2 \frac{1}{(p \cdot x)} + (1 - p x) \cdot \log_2 \frac{1}{(1 - p \cdot x)} - H(p) \cdot x}_{f(x) \,\to\, f^{ón} \text{ a maximizar}} \Big]$$

$$f'(x) = p \cdot \log_2 \frac{1}{p x} + p x \cdot \frac{1}{\ln 2} \cdot \frac{-p x}{(p x)^2} \cdot p - p \cdot \log_2 \frac{1}{1 - p x} +$$

$$+ (1 - p x) \cdot \frac{1}{\ln 2} \cdot \frac{-(1 - p x)}{(1 - p x)^2} \cdot (-p) - H(p) =$$

$$= p \cdot \log_2 \frac{1}{p x} - \cancel{\frac{p}{\ln 2}} - p \cdot \log_2 \frac{1}{1 - p x} + \cancel{\frac{p}{\ln 2}} - H(p) =$$

$$= p \cdot \left[\log_2 \frac{1}{p x} - \log_2 \frac{1}{1 - p x} \right] - H(p) = p \cdot \log_2 \frac{1 - p x}{p x} - H(p)$$

$$f'(x) = 0 \to \log_2 \frac{1 - p x}{p x} = \frac{H(p)}{p} \;;\; 2^{\frac{H(p)}{p}} = \frac{1 - p x}{p x}$$

$$2^{\frac{H(p)}{p}} \cdot p \cdot x = 1 - p x \;;\; p \cdot \left(2^{\frac{H(p)}{p}} + 1 \right) \cdot x = 1$$

$$\boxed{\begin{array}{l} x_{MAX} = p(A=1) = \dfrac{1}{p \cdot \left(2^{H(p)/p} + 1 \right)} \\[2ex] C = f(x_{MAX}) \quad \left[\text{bits}/\text{símbolo} \right] \end{array}}$$

(10) a) Certificado firmado de A = $1B7740_h$ =

$$= \underbrace{\underbrace{\underbrace{0001}_{1}}_{ID_A} \; \underbrace{\underbrace{\overset{8\,4\,2\,1}{1011}}_{B}}_{e_A} \; \underbrace{\underbrace{0111}_{7} \; \underbrace{0111}_{7}}_{N_A = p_A \cdot q_A = 119}}_{M_A} \; \underbrace{\underbrace{\overset{2^6}{0100}}_{4} \; \underbrace{0000}_{0}}_{FD(M_A) = 64}$$

• B recalcula $H(M_A) \rightarrow$

$m_0 = 0001$
$m_1 = 1011$
$m_2 = 0111$
$m_3 = 0111$

$h_0 = DCI(m_0) = 0010$

$h_1 = DCI(h_0 + m_1) =$
$= DCI(1001) = 0011$

$h_2 = DCI(0011 + 0111) =$
$= DCI(0100) = 1000$

$h_3 = H(M_A) = DCI(1000 + 0111) =$
$= DCI(1111) = 1111$

$H(M_A) = 1111 \equiv 15$ //

• B obtiene $H(M_A)$ a partir de la $FD(M_A)$:

$$H(M_A) = (FD(M_A))^{e_{CA}} \cdot \bmod N_{CA} = 64^{37} \bmod 77$$

$37 = \underset{32}{1}00\underset{4}{1}0\underset{1}{1}$ $\quad 64^{37} = ((((64^2)^2)^2 \cdot 64)^2)^2 \cdot 64$

$64^2 = 4096 \xrightarrow{mod 77} 15$
$15^2 = 225 \xrightarrow{mod 77} 71$
$71^2 = 5041 \xrightarrow{mod 77} 36$

$36 \cdot 64 = 2304 \xrightarrow{mod 77} 71$
$71^2 = 5041 \xrightarrow{mod 77} 36$
$36^2 = 1296 \xrightarrow{mod 77} 64$
$64 \cdot 64 = 4096 \xrightarrow{mod 77} \boxed{15 = H(M_A)}$

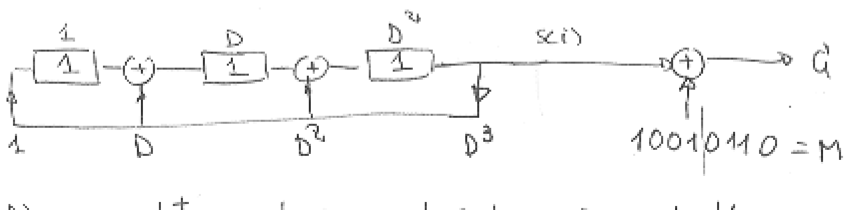
$\Rightarrow$ Como coinciden, B ha autenticado a A.

b) No ha lugar.

c) $K_{sesión} = 7$ que B debe codificar con la K_{PA} para enviarla a A de forma segura:

$$C_{BA} = (K_{sesión})^{e_A} \bmod N_A = 7^{11} \bmod 119 = \dots = 14$$

d) $B \longrightarrow A$ La info se cifra codificando con el
$M = 10010110$ cifrador en flujo LFSR enunciado.



$C(D)$ completo grado $3 \rightarrow L \leq L_{max} = m + 1 = 4$

Para los $p^{(0)}(D) = 1, D, D^2, 1+D+D^2 \Rightarrow L = L_{max} = 4$
(y puede ser para otros $p^{(0)}(D)$, en gnral.)

En este caso, $p^{(0)}(D) = K_{search} = 111 \equiv 1+D+D^2$

$p^{(0)}(D)$:

1	D	D^2
1	1	1
1	0	0
0	1	0
0	0	1
1	1	1
⋮		

$L=4$

se genera la secuencia:

$s(i) = \underbrace{1001}_{L=4}\ 1001\ 1001 \ldots$

$s(i)$: $1001\ 1001 \rightarrow \oplus \rightarrow \boxed{C' = 0000\,1111}$

$1001|0110 = M$