CONTROL DE TRANSMISIÓN DE DATOS. 20 de Mayo de 2004

Notas Importantes:

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Los problemas se entregan por separado, ponga su nombre y apellidos en cada hoja, enumerándolas.
3. Un error conceptual grave, puede anular todo el problema.

Problema 1 (25%)

Sea un canal con la matriz de probabilidades de transición siguiente:

$$p[D/F] = \begin{bmatrix} \frac{1-p}{2} & \frac{1-p}{2} & \frac{p}{2} & \frac{p}{2} \\ \frac{p}{2} & \frac{p}{2} & \frac{1-p}{2} & \frac{1-p}{2} \end{bmatrix}$$

a) Se pide dibujar un diagrama de transiciones del canal.

b) Calcular su capacidad de canal.

c) Comparar dicha capacidad con la de un canal BSC (Canal Binario Simétrico).

Problema 2 (25%)

La trayectoria de un coche se puede modelar como la de una pieza que se mueve a través de una retícula cuadriculada con pasos elementales, en direcciones verticales u horizontales, dando un único paso cada vez. Así, se puede representar su movimiento como una sucesión de símbolos del conjunto {N, S, E, y W} que representan los sucesivos pasos en las direcciones (para indicar norte, sur, este y oeste, respectivamente).

El comportamiento de este coche tiene memoria: El 50% de las ocasiones repite el movimiento anterior, y en el resto de los casos da un giro de 90° a derecha (con probabilidad 30%) o a izquierda (con probabilidad 20%) respecto del paso anterior.

Se pide:

a) Modelar el proceso que describe el movimiento.

b) Calcular la probabilidad de cada uno de los símbolos.

c) Calcular la tasa de entropía de esta fuente de información.

d) Diseñar un codificador *Huffman* de esta fuente.

Problema 3 (50%)

Sea un sistema de clave pública RSA. Considere dos usuarios A y B y una entidad CA que expende certificados para autenticar el origen de los mensajes. Los usuarios del sistema utilizan criptografía asimétrica RSA para intercambiar una clave de sesión. La clave de sesión se utiliza para codificar mensajes mediante cifrado en flujo síncrono. Las secuencias binarias se consideran con más peso a la izquierda (MPI).

El algoritmo de cifrado en flujo trabaja sobre bloques de 4 bits, donde el mensaje de entrada se coloca como estado inicial de un LFSR con polinomio primitivo de conexiones $C(D)=D^4+D+1$. El criptograma se obtiene como el estado del LFSR al cabo del número de iteraciones que indique la clave de sesión.

Parámetros RSA de los usuarios y de la entidad certificadora, e identificadores de cada usuario:

Usuario A	$p_A=3$, $q_A=11$, $d_A=7$	$ID_A=0011$
Usuario B	$p_B=7$, $q_B=11$, $e_B=17$	$ID_B=0010$
Entidad certificadora CA	p_{CA}, q_{CA}, $e_{CA}=7$	

La función resumen o *Hash* H(M) de un mensaje M, se obtiene aplicando la operación OR-exclusiva ($\oplus$), bit a bit, sobre los sucesivos bloques del mensaje M de entrada. El funcionamiento es el siguiente:

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden a la izquierda del mensaje tantos ceros como sea necesario para que la longitud sea múltiplo de 4.
- Se divide el mensaje resultante desde la izquierda en m bloques b_j, de $n=4$ bits cada uno, siendo $1 \leq j \leq m$.
- b_{ij} es el bit i-ésimo del bloque j-ésimo; $1 \leq i \leq n$
- $H(M)=C$. La función *Hash* de M es un bloque resultante $C=C_1C_2C_3\ldots C_n$ de $n=4$ bits, donde:
- El bit i-ésimo del bloque C es: $C_i=b_{i1}\oplus b_{i2}\oplus b_{i3}\oplus\ldots\ldots\oplus b_{im}$.

La autoridad certificadora CA sigue el siguiente esquema para expender los certificados: Un usuario i entrega a la CA el certificado en claro correspondiente a la concatenación (||) de su identificador ID_i y de su clave pública K_{Pi}. La CA firma digitalmente dicho certificado en claro y añade la firma detrás: *Certificado firmado = certificado en claro || firma digital.*

a) Genere las claves pública y privada de los usuarios A y B.

b) Sabiendo que la CA utiliza $\phi(N_{CA})=480$, averigüe la clave privada de CA, d_{CA}.

c) Averigüe p_{CA}, q_{CA}.

d) Independientemente del apartado anterior, suponga $p_{CA}=17$, $q_{CA}=31$. Obtenga el certificado en claro que A envía a CA, expréselo en hexadecimal. Obtenga el certificado firmado que la entidad CA genera al usuario A, expréselo en hexadecimal.

e) B desea comunicar a A una clave de sesión para cifrar la información que le trasmitirá posteriormente: $K_{SESIÓN}=44$. Enumere los pasos del protocolo a seguir para lograr dicho intercambio, de forma que el usuario B autentique al usuario A.

f) Codifique la clave de sesión que B envía a A.

g) B envía el mensaje $M_{BA}=10011011$ a A. Cifre dicho mensaje con el algoritmo de cifrado en flujo para codificar mensajes descrito en el enunciado.

Nota: Lista de los números primos menores que 100: 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

UPC ETSETB

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. 1

Nombre total de fulls 4

Qualificació

Cognoms: Control Resuelto de Transmisión de Datos

Nom

Centre: Prof.: Mónica Aguilar

Assignatura / especialitat

DNI | Núm. matrícula | Curs | Grup: 50 | Data: 20/05/04

Problema 1

(1) $\boxed{\text{Fuente}}$ — $\boxed{\text{Canal}}$ — $\boxed{\text{Destino}}$

F — D

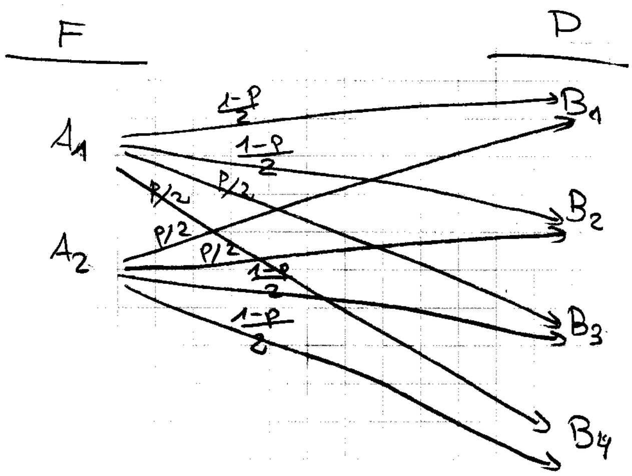
m símbolo A_i, $p(A_i)$ — n símbolo B_j, $p(B_j)$

0'3 a) $m = 2$, $F = \{A_1, A_2\}$, $i = \{1, 2\}$

$n = 4$, $D = \{B_1, B_2, B_3, B_4\}$, $j = \{1, 2, 3, 4\}$

$$p(D \backslash F) = \begin{array}{c} A_1 \\ A_2 \\ \\ \end{array} \begin{array}{c} \left[\begin{array}{cccc} \frac{1-p}{2} & \frac{1-p}{2} & \frac{p}{2} & \frac{p}{2} \\ \frac{p}{2} & \frac{p}{2} & \frac{1-p}{2} & \frac{1-p}{2} \end{array}\right] \\ \begin{array}{cccc} B_1 & B_2 & B_3 & B_4 \end{array} \end{array}$$

Canal simétrico.



1'7p b) $$C\left[\frac{\text{bits}}{\text{símb}}\right] = \max_{\{p(A_i)\}} I(F, D) = \max_{\{p(A_i)\}} \left[H(D) - H(D \backslash F) \right]$$

$$H(D\backslash F) = \sum_i p(A_i) \cdot H(D \backslash A_i) = H(D\backslash A_1) = H(D \backslash A_2) =$$

$\sum_i p(A_i) = 1$, simetría $\forall$ fila.

$$= \cancel{2} \cdot \frac{1-p}{\cancel{2}} \cdot \log_2 \frac{2}{1-p} + \cancel{2} \cdot \frac{p}{\cancel{2}} \cdot \log_2 \frac{2}{p} =$$

$$= \sum_j p(B_j \backslash A_1) \cdot \log_2 \frac{1}{p(B_j \backslash A_1)}$$

$$H(D) = \sum_j p(B_j)\cdot \log_2 \frac{1}{p(B_j)} \le \log_2 n \quad , \text{ con } = \text{ para } p(B_j) = \frac{1}{n} .$$

$$p(B_j) = \sum_i p(B_j \backslash A_i)\cdot p(A_i) \underset{\text{si } p(A_i) = \frac{1}{m}}{=} \frac{1}{m}\cdot \sum_i p(B_j\backslash A_i) = \quad (= \forall i)$$

$$= \frac{1}{m}\cdot (\underbrace{\text{Suma de Columnas cte.}}_{\frac{1}{2}}) = \frac{1}{2m} = \frac{1}{n} \text{, son equiprobables}$$

$$\Longrightarrow \boxed{\underset{\left[\frac{bits}{simb}\right]}{C} = \log_2 n - \sum_j p(B_j\backslash A_1)\cdot \log_2 \frac{1}{p(B_j\backslash A_1)}} =$$

$$= \log_2 4 - \left[(1-p)\cdot \log_2 \frac{2}{1-p} + p\cdot \log_2 \frac{2}{p}\right] =$$

$$= 2 - \left[(1-p)\cdot\{\underbrace{\log_2 2}_{1} - \log_2(1-p)\} + p\cdot\{\underbrace{\log_2 2}_{1} - \log_2 p\}\right] =$$

$$= 2 - \left[(1-p)\cdot[1 - \log_2(1-p)] + p\cdot[1-\log_2 p]\right] =$$

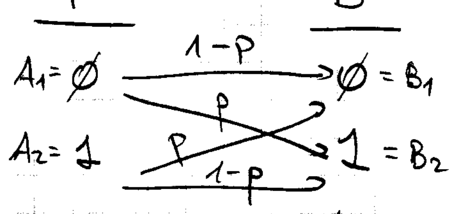
$$= 2 - \left[(\cancel{1-p}) - (1-p)\cdot\log_2(1-p) + \cancel{p} - p\cdot \log_2 p\right] =$$

$$= 2 - \left[1 - \left(p\cdot\log_2 p + (1-p)\cdot\log_2(1-p)\right)\right] =$$

$$= 1 + \left(p\cdot \log_2 p + (1-p)\cdot \log_2(1-p)\right)$$

0'5p

c) BSC $\Longrightarrow$



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

También se trata de un canal simétrico, $m=2$, $n=2$:

$$C_{BSC} = \underbrace{\log_2 2}_{1} - \left[(1-p)\cdot \log_2 \frac{1}{1-p} + p\cdot\log_2 \frac{1}{p}\right] =$$

$$= 1 + \left(p\cdot \log_2 p + (1-p)\cdot \log_2(1-p)\right) = C_{\text{apartado b)}}$$

Son iguales.

Cognoms: Control Trans. Datos.
Nom:
Centre:
Assignatura / especialitat:
DNI: | Núm. matrícula: | Curs: | Grup: 50 | Data: 20/05/04

(2)

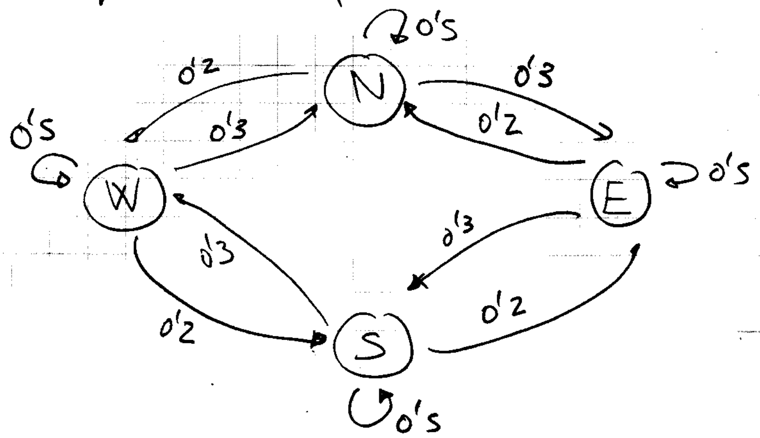
N, S, E, W

ahora / antes

antes \ ahora	N	S	E	W
N	0'5	—	0'3	0'2
S	—	0'5	0'2	0'3
E	0'2	0'3	0'5	—
W	0'3	0'2	—	0'5

0'6 a)

Se puede modelar con una cadena de Markov, memoria 1, cuyo diagrama de probabilidades de transición de estados es:



0'6 b)

$$P(N) = \overset{0'5}{P(N\backslash N)}\cdot P(N) + \cancel{P(N\backslash S)\cdot P(S)} + \overset{0'2}{P(N\backslash E)}\cdot P(E) + \overset{0'3}{P(N\backslash W)}\cdot P(W)$$

$$P(S) = \cancel{P(S\backslash N)\cdot P(N)} + \overset{0'5}{P(S\backslash S)}\cdot P(S) + \overset{0'3}{P(S\backslash E)}\cdot P(E) + \overset{0'2}{P(S\backslash W)}\cdot P(W)$$

$$P(E) = \overset{0'3}{P(E\backslash N)}\, P(N) + \overset{0'2}{P(E\backslash S)}\cdot P(S) + \overset{0'5}{P(E\backslash E)}\cdot P(E) + \cancel{P(E\backslash W)\cdot P(W)}$$

$$P(W) = \overset{0'2}{P(W\backslash N)}\cdot P(N) + \overset{0'3}{P(W\backslash S)}\cdot P(S) + \cancel{P(W\backslash E)\cdot P(E)} + \overset{0'5}{P(W\backslash W)}\cdot P(W)$$

$0'5\cdot P(N) = 0'2\cdot P(E) + 0'3\cdot P(W)$ $\qquad$ $P(N) = 0'4\cdot P(E) + 0'6\cdot P(W)$

$0'5\cdot P(S) = 0'3\cdot P(E) + 0'2\cdot P(W)$ $\quad\Rightarrow\quad$ $P(S) = 0'6\cdot P(E) + 0'4\cdot P(W)$

$0'5\cdot P(E) = 0'3 P(N) + 0'2\cdot P(S)$ $\qquad$ $P(E) = 0'6\cdot P(N) + 0'4\cdot P(S)$

$0'5\cdot P(W) = 0'2\cdot P(N) + 0'3\cdot P(S)$ $\qquad$ $P(W) = 0'4\cdot P(N) + 0'6\cdot P(S)$

$P(N) + P(S) = P(E) + P(W)$

$P(N) + P(S) + P(E) + P(W) = 1 \Rightarrow 2\,P(N) + 2\,P(S) = 1$

$\boxed{P(N) + P(S) = \frac{1}{2}}$ $\boxed{P(E) + P(W) = \frac{1}{2}}$

$$P(N) = 0'4\,(\overbrace{0'6\cdot P(N) + 0'4\,P(S)}^{P(E)}) + 0'6\cdot(\overbrace{0'4\cdot P(N) + 0'6\cdot P(S)}^{P(W)}) =$$

$$= 0'24\cdot P(N) + 0'16\cdot P(S) + 0'24\,P(N) + 0'36\cdot P(S) =$$

$$= 0'48\cdot P(N) + 0'52\cdot P(S)$$

$$0'52\cdot P(N) = 0'52\cdot P(S) \Rightarrow \boxed{P(N) = P(S)} \Rightarrow \boxed{P(N) = P(S) = \frac{1}{4}}$$

$$P(E) = 0'6\cdot(\overbrace{0'4\cdot P(E) + 0'6\cdot P(W)}^{P(N)}) + 0'4\cdot(\overbrace{0'6\cdot P(E) + 0'4\cdot P(W)}^{P(S)}) =$$

$$= 0'24\cdot P(E) + 0'36\cdot P(W) + 0'24\cdot P(E) + 0'16\cdot P(W)$$

$$\boxed{P(E) = P(W)} \Rightarrow \boxed{P(E) = P(W) = \frac{1}{4}}$$

0'9

c) $H(F) = H(F\backslash N)\cdot P(N) + H(F\backslash S)\cdot P(S) + H(F\backslash E)\cdot P(E) + H(F\backslash W)\cdot P(W)$

$H(F\backslash N) = H(F\backslash S) = H(F\backslash E) = H(F\backslash W)$

$$H(F\backslash N) = p(N\backslash N)\cdot \log_2 \frac{1}{p(N\backslash N)} + \cancel{p(S\backslash N)\cdot \log_2 \frac{1}{p(S\backslash N)}} + p(E\backslash N)\cdot \log_2 \frac{1}{p(E\backslash N)} +$$

$$+ p(W\backslash N)\cdot \log_2 \frac{1}{p(W\backslash N)} = 0'5\cdot\log_2 \frac{1}{0'5} + 0'3\cdot\log_2 \frac{1}{0'3} + 0'2\cdot\log_2 \frac{1}{0'2}$$

$$= 0'5 + 0'5211 + 0'4644 = 1'4855 \left[\text{bits}/\text{símbolo}\right]$$

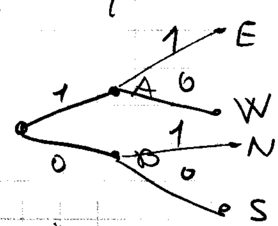
$$H(F) = H(F\backslash N) = 1'4855 \left[\text{bits}/\text{símbolo}\right]$$

0'4

d) El Código Huffman no contempla que la fuente tenga MEMORIA:

N	1/4		
S	1/4		
E	1/4	}	A 1/2
W	1/4	}	

A	1/2		
N	1/4	}	B 1/2
S	1/4	}	



N	01
S	00
E	11
W	10

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. 3

Nombre total de fulls 4

Qualificació

Cognoms

Nom

Centre

Assignatura / especialitat: Control Trans. de Datos

DNI | Núm. matrícula | Curs | Grup: 50 | Data: 20/05/04

3

0'6

a) A. $N_A = p_A \cdot q_A = 3 \cdot 11 = 33$;; $\Phi(N_A) = (p_A - 1)\cdot(q_A - 1) = 2 \cdot 10 = 20 = 5 \cdot 4$

$e_A \cdot d_A = 1 + K \cdot \Phi(N_A)$;; $e_A = \dfrac{1 + K \cdot 20}{7} = \dfrac{1 + K\cdot(7 \cdot 2 + 6)}{7} = 2K + \dfrac{6K+1}{7}$

$20 \,\underline{|7}$, $6 \quad 2$

$K = 1 \Rightarrow e_A = 2 + 1 = 3$

$\text{mcd}(d, \Phi(N)) = 1$, $d = 7$, $\Phi(N) = 5 \cdot 4$

$$\boxed{\begin{aligned} K_{PA} &= (e_A, N_A) = (3, 33) \\ K_{SA} &= d_A = 7 \end{aligned}}$$

B. $N_B = p_B \cdot q_B = 7 \cdot 11 = 77$;; $\Phi(N_B) = (p_B - 1)\cdot(q_B - 1) = 6 \cdot 10 = 60 = 2^2 \cdot 3 \cdot 5$

$e_B \cdot d_B = 1 + K \cdot \Phi(N_B)$;; $d_B = \dfrac{1 + K \cdot 60}{17} = \dfrac{1 + K\cdot(17 \cdot 3 + 9)}{17} = 3K + \underbrace{\dfrac{9K+1}{17}}_{K_2}$

$60 \,\underline{|17}$, $9 \quad 3$

$K_2 = \dfrac{9K+1}{17}$;; $K = \dfrac{17K_2 - 1}{9} = \dfrac{(9 \cdot 1 + 8)K_2 - 1}{9} = K_2 + \underbrace{\dfrac{8K_2 - 1}{9}}_{63 \to K_2 = 8}$

$17 \,\underline{|9}$, $8 \quad 1$

$K_2 = 8 \to K = 8 + \dfrac{8 \cdot 8 - 1}{9} = 8 + \dfrac{63}{9} = 15$

$d_B = 3 \cdot 15 + \dfrac{9 \cdot 15 + 1}{17} = 45 + 8 = 53$

$\text{mcd}(e, \Phi(N)) = 1$, $e = 17$, $\Phi(N) = 2^2 \cdot 3 \cdot 5$

$$\boxed{\begin{aligned} K_{PB} &= (e_B, N_B) = (17, 77) \\ K_{SB} &= d_B = 53 \end{aligned}}$$

0'6 c) $\Phi(N_{CA}) = 480 = 2^5 \cdot 3 \cdot 5 = 2^4 \cdot 2 \cdot 3 \cdot 5 = 16 \cdot 30 = (p_{CA} - 1)\cdot(q_{CA} - 1)$

con p_{CA} y q_{CA} dos nºs primos. $\Rightarrow \begin{cases} p_{CA} = 17 \\ q_{CA} = 31 \end{cases}$ OK!

$\boxed{p_{CA} = 17 \;;\; q_{CA} = 31}$

$N_{CA} = p_{CA} \cdot q_{CA} = 17 \cdot 31 = 527$

0'7 b) $e_{CA} \cdot d_{CA} = 1 + K \cdot \Phi(N_{CA})$;; $d_{CA} = \dfrac{1 + K \cdot 480}{7} = \dfrac{1 + K\cdot(7 \cdot 68 + 4)}{7} = 68K + \dfrac{4K+1}{7}$

$480 \,\underline{|7}$, $4 \quad 68$

$K = 5 \to \boxed{d_{CA} = 343}$

1'5

d) $p_{CA} = 17$

$q_{CA} = 31$

$ID_A \| e_A \| N_A \longrightarrow CA$

A

$\underbrace{ID_A \| e_A \| N_A}_{M} \| \underbrace{FD(M)}$

$M \longrightarrow H(M) \longrightarrow H(M)^{d_{CA}} \bmod N_{CA}$

$ID_A = \overset{8421}{0011} \equiv 3_H$

$e_A = 3 = 0011 \equiv 3_H$

$N_A = 33 = 00\underset{32}{1}0|000\underset{1}{1} \equiv 21_H$

$\boxed{\text{Certif. Claro} = ID_A \| e_A \| N_A = 0011|0011|0010|0001 = 3321_H}$

$M = 00\underset{4096}{1}1|00\underset{256}{1}1|00\underset{32}{1}0|000\underset{1}{1}$

$b_1 \quad b_2 \quad b_3 \quad b_m = b_4$ $\quad m = 4$ bloques de 4 bits c.u.

$H(M) = C = c_1c_2c_3c_4 \;\overset{?}{=}\; 0001$

$c_1 = b_{11} \oplus b_{12} \oplus b_{13} \oplus b_{14} = 0 \oplus 0 \oplus 0 \oplus 0 = 0$

$c_2 = b_{21} \oplus b_{22} \oplus b_{23} \oplus b_{24} = 0 + 0 + 0 + 0 = 0$

$c_3 = b_{31} \oplus b_{32} \oplus b_{33} \oplus b_{34} = 1 + 1 + 1 + 0 = 1$

$c_4 = b_{41} \oplus b_{42} \oplus b_{43} \oplus b_{44} = 1 + 1 + 0 + 1 = 1$

$\boxed{H(M) = 0011 \equiv 3}$

$\boxed{FD(M)} = (H(M))^{d_{CA}} \bmod N_{CA} = 3^{343} \bmod 527 = 334 \equiv \underset{256}{1}|0100|1110 = \boxed{14E_H}$

$343 \equiv \underset{256}{1}\;\underset{128}{0}\;\underset{64}{1}\;\underset{32}{0}\;\underset{16}{1}\;\underset{8}{0}\;\underset{4}{1}\;\underset{2}{1}\;\underset{1}{1}$

$3^{343} = ((((((3^2)^2 \cdot 3)^2)^2 \cdot 3)^2)^2 \cdot 3)^2 \cdot 3)^2 \cdot 3$

$243^2 = 59049 \bmod 527 = 25$

$25^2 = 625 \bmod 527 = 98$

$98 \cdot 3 = 294$

$294^2 = 86436 \xrightarrow{527} 8$

$64 \cdot 3 = 192$

$192^2 = 36864 \longrightarrow 501$

$501 \cdot 3 = 1503 \longrightarrow 449$

$449^2 = 201601 \longrightarrow 287$

$287 \cdot 3 = 861 \longrightarrow 334$

Certificado firmado $= \overbrace{ID_A \| e_A \| N_A}^{M} \| FD(M) =$

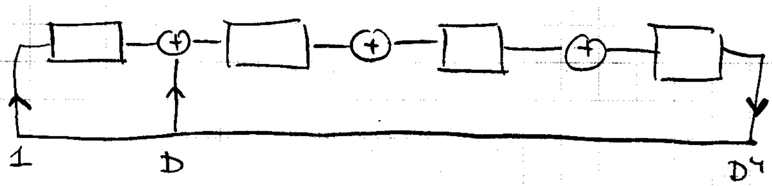
$= 332114E_H$

Cognoms: Control Transmisión de Datos
Nom
Centre
Assignatura / especialitat
DNI | Núm. matrícula | Curs | Grup: 50 | Data: 20/05/04

0'4 e) $K_{sesión} = 44$ $A \xleftarrow{K_{sesión}} B$

- A envía su certificado a B : $\underbrace{ID_A \| e_A \| N_A}_{M} \| FD(M)$
- B lee la $K_{PA} = (e_A, N_A)$
- B extrae $H(M)$ ya que conoce $K_{PCA} = (e_{CA}, N_{CA})$.
- B recalcula $H(M)$ a partir del M que lee. Si coincide con el anterior, autenticado queda A.
- Ahora, B envía a A la $K_{sesión}$ codificada RSA con la K_{PA}.

0'8 g)



- A recibe $C_{K_{sesión}}$ y la decodifica con su K_{PA}:

$$K_{sesión} = \left(C_{K_{sesion}}\right)^{d_A} \bmod N_A = \dots = 44.$$

- $M_{BA} = \underbrace{1001}_{M_1} \mid \underbrace{\overset{1\,D\,D^2\,D^3}{1011}}_{M_2}$

$p^{(0)}(D) = 1 + D^3$ $p^{(\delta)}(D) = 1 + D^2 + D^3$

- LFSR $\Rightarrow p^{(n+1)}(D) = D \cdot p^{(n)}(D) \bmod C(D)$
- $C(D)$ es primitivo, $L = 2^m - 1 = 2^4 - 1 = 15$
- $44 = 3 \cdot 15 - 1$
- $p^{(44)}(D) = p^{(-1)}(D) \Rightarrow$ Retroceder un Estado.

$$\begin{array}{l|l} D\cdot p^{(n)}(D) & C(D) \\ \hline p^{(n+1)}(D) & Q(D) \begin{smallmatrix}\to \phi \\ \to 1\end{smallmatrix} \end{array}$$

$$D\cdot p^{(n)}(D) = C(D)\cdot \begin{cases}\phi\\1\end{cases} + p^{(n+1)}(D)$$

$$D\cdot p^{(-1)}(D) = C(D)\cdot \begin{cases}\phi\\1\end{cases} + p^{(\phi)}(D)$$

$$p^{(0)}(D) = 1+D^3 \to D\cdot p^{(-1)}(D) = (D^4+D+1)\cdot\begin{cases}\phi\\1\end{cases} + (1+D^3)$$

$$1 \Rightarrow D\cdot p^{(-1)}(D) = D^4+D+\cancel{1}+\cancel{1}+D^3$$

$$p^{(-1)}(D) = 1+D^2+D^3 \equiv 1011$$

$$\boxed{M_1 = \underset{1\,D\,D^2\,D^3}{1001} \longrightarrow C_1 = 1011}$$

$$p^{(0)}(D) = 1+D^2+D^3 \to D\cdot p^{(-1)}(D) = (D^4+D+1)\cdot\begin{cases}\phi\\1\end{cases} + (1+D^2+D^3)$$

$$1 \Rightarrow D\cdot p^{(-1)}(D) = D^4+D+\cancel{1}+\cancel{1}+D^2+D^3 =$$

$$= D+D^2+D^3+D^4$$

$$p^{(-1)}(D) = 1+D+D^2+D^3$$

$$\boxed{M_2 = \underset{1\,D\,D^2\,D^3}{1011} \longrightarrow C_2 = 1111}$$

$$\boxed{M_{BA} = 1001|1011 \longrightarrow C_{BA} = 1011|1111}$$

0'4

f) $C_{K_{SESION}} = (K_{SESION})^{e_A} \bmod N_A$, ¡para $\phi \leq K_{SESION} \leq N_A - 1$!

En este caso, $44 > 32$! Usemos 5 bits $\Rightarrow \underbrace{\underset{32}{0\,0\,0\,0\,1}}_{K_s^1} : \underbrace{\underset{16\ 8\ 4\ 2\ 1}{0\,1\,1\,0\,0}}_{K_s^2}$

$K_s^1 \to C_s^1 = (K_s^1)^{e_A} \bmod N_A \to 00001$

$K_s^2 \to C_s^2 = (K_s^2)^{e_A} \bmod N_A \to 10110$

$C_s^1 = 1^3 \bmod 33 = 1 \to 00001$

$C_s^2 = 12^3 \bmod 33 = 1738 \bmod 33 = 22 \to 10110$

$$\boxed{C_{K_{SESION}} = 00001\ 10110}$$