Aguilar

CONTROL DE TRANSMISIÓN DE DATOS. 20 de Mayo de 2005

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 (50%)

Considere 3 canales discretos con los siguientes diagramas de transiciones:

a) Obtenga la matriz de probabilidades de transición P(D\F), para cada canal. **(0.5p)**

b) Calcule la capacidad de canal, para cada canal. Exprésela en función de p para los canales 2 y 3. **(4p)** = 1+1+2

c) Calcule las 3 capacidades de canal anteriores para $p=1/2$. ¿Con qué canal se puede transmitir más información por cada uso que se haga de él? **(0.5p)**

Nota: Para mayor claridad de la solución, llame $H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{(1-p)}$

Problema 2 (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 se realiza mediante un LFSR con polinomio de conexiones $C(D)=D^4+D^3+D^2+D+1$. La $K_{SESIÓN}$ es el estado inicial del LFSR (p.ej. para $K_{sesión}=36$, $P^0(D)=100100 \equiv 1+D^3$). La secuencia pseudoaleatoria generada se utiliza para cifrar el mensaje. Considere que el primer bit de salida del LFSR es el bit de mayor peso MPI (más peso a la izquierda) de la secuencia pseudoaleatoria generada.

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

Usuario A	$p_A=17$, $q_A=31$, $e_A=7$	$ID_A=0001$
Usuario B	$p_B=3$, $q_B=11$, $d_B=7$	$ID_B=0010$
Entidad certificadora CA	$p_{CA}=7$, $q_{CA}=11$, $e_{CA}=17$, $d_{CA}=53$	

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: $C_i=b_{i1}\oplus b_{i2}\oplus b_{i3}\oplus\ldots\oplus b_{im}$.

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. **(0.75p)**

b) Obtenga el certificado en claro que A envía a CA, expréselo en hexadecimal. Obtenga el certificado firmado que la entidad CA devuelve al usuario A, expréselo en hexadecimal. **(0.75p)**

c) Obtenga el certificado en claro que B envía a CA, expréselo en hexadecimal. Obtenga el certificado firmado que la entidad CA devuelve al usuario B, expréselo en hexadecimal. **(0.75p)**

d) A desea comunicar a B su clave de sesión para cifrar la información que le trasmitirá posteriormente: $K_{SESIÓN\_AB}$=6. B desea comunicar a A su clave de sesión para cifrar la información que le trasmitirá posteriormente: $K_{SESIÓN\_BA}$=4. Enumere los pasos del protocolo a seguir para lograr dicho intercambio, de forma que ambos usuarios se autentiquen mutuamente. **(0.75p)**

e) Codifique la clave de sesión $K_{SESIÓN\_AB}$ que A envía a B. **(0.25p)**

f) Codifique la clave de sesión $K_{SESIÓN\_BA}$ que B envía a A. **(0.25p)**

g) A envía el mensaje M_{AB}=1101001011001010l a B. Cifre dicho mensaje con el algoritmo de cifrado en flujo para codificar mensajes descrito en el enunciado. **(0.75p)**

h) B envía el mensaje M_{BA}=1010 a A. Cifre dicho mensaje con el algoritmo de cifrado en flujo para codificar mensajes descrito en el enunciado. **(0.75p)**

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.

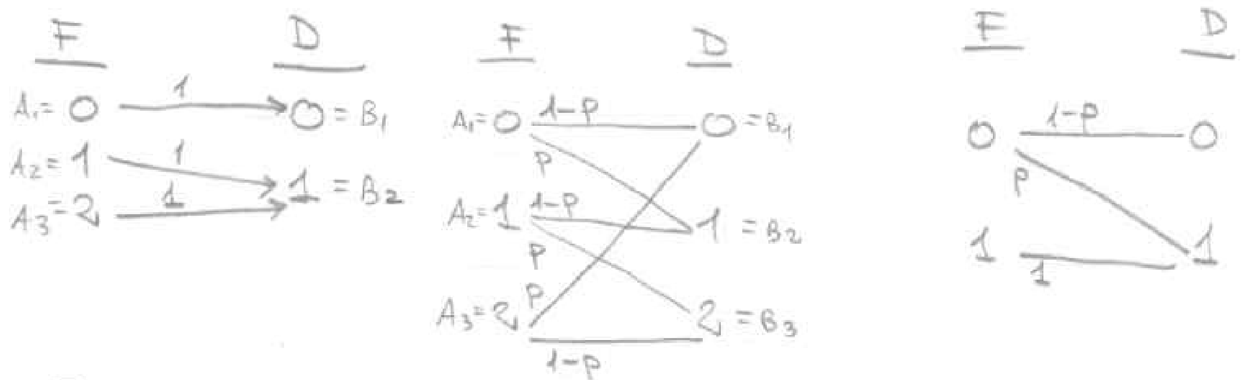
Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. 1 — Nombre total de fulls 3 — Qualificació

Cognoms: AGUILAR — Nom: MÓNICA
Centre: Grupo 30
Assignatura / especialitat: TRANSMISSIÓ DE DADES
DNI: — Núm. matrícula: — Curs: — Grup: — Data: 20/05/05

PROBLEMA 1

Canal 1 — Canal 2 — Canal 3



ⓐ

Canal 1

$$P(D\backslash F) = \begin{array}{c|cc} & B_1 & B_2 \\ \hline A_1 & 1 & 0 \\ A_2 & 0 & 1 \\ A_3 & 0 & 1 \end{array}$$

Canal simétrico respecto de la entrada.

Canal 2

$$P(D\backslash F) = \begin{array}{c|ccc} & B_1 & B_2 & B_3 \\ \hline A_1 & 1-p & p & 0 \\ A_2 & 0 & 1-p & p \\ A_3 & p & 0 & 1-p \end{array}$$

Canal simétrico

Canal 3

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

ⓑ

a partir de las $p(D\backslash F)$

$$I(F;D) = H(F) - H(F\backslash D) = H(D) - H(D\backslash F) \quad [\text{bits/símbolo}]$$

Información Mutua

$$C = \max_{p\{A_i\}} I(F;D) = \max_{p\{A_i\}} [H(D) - H(D\backslash F)] \quad [\text{bits/símbolo}]$$

Capacidad de Canal

Canal 1

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

$$H(D\backslash A_1) = H(D\backslash A_2) = H(D\backslash A_3) = 1 \cdot \log_2 1 = \emptyset$$

Canal Determinista, pues $H(D\backslash F) = \emptyset$.

$$H(D) = \sum_j p(B_j) \cdot \log_2 \frac{1}{p(B_j)}$$

$$P(B=0) = P(B=0 \backslash A=0)\cdot P(A=0) + \cancel{P(B=0 \backslash A=1)}\cdot P(A=1) + \cancel{P(B=0 \backslash A=2)}\cdot P(A=2)$$

$$\underset{1}{} \qquad \phi \qquad \phi$$

$$= P(A=0)$$

$$P(B=1) = \cancel{P(B=1 \backslash A=0)}\cdot P(A=0) + \underset{1}{P(B=1 \backslash A=1)}\cdot P(A=1) + \underset{1}{P(B=1 \backslash A=2)}\cdot P(A=2) =$$

$$= P(A=1) + P(A=2)$$

$$\left[C = \max_{p\{A_i\}} \left[H(D) - \underset{\phi}{\cancel{H(D \backslash F)}} \right] = \boxed{\max_{p\{A_i\}} H(D)} \right.$$

→ Para hacer máxima la Información mutua $I(F;D)$, debe ser máxima la $H(D)$ ⇒ Eso será cuando la distribución de probabilidades de D $p\{B_j\}$ sea uniforme:

$$p(B=0) = p(B=1)$$

$$\begin{cases} p(B=0) = p(B=1) = p(A=0) = p(A=1) + p(A=2) \\ p(B=0) + p(B=1) = 1 \end{cases} \Rightarrow \left[\begin{array}{l} p(B=0) = p(B=1) = p(A=0) = 1/2 \\ p(A=1) + p(A=2) = 1/2 \end{array} \right]$$

Será para una F tal que $p\{A_i\}$ sean así.

Entonces, $H(D) = 2 \cdot \frac{1}{2} \log_2 2 = 1$ bit/símbolo

$$\left[C = 1 \text{ bit/símbolo} \right]$$

<u>Canal 2</u>

$$H(D \backslash F) = \sum_i p(A_i)\cdot H(D \backslash A_i) \underset{(*)}{=} H(p) \cdot \sum_i p(A_i) = H(p)$$

$$H(D \backslash A_1) = H(D \backslash A_2) = H(D \backslash A_3) = p \cdot \log_2 \frac{1}{p} + (1-p)\cdot \log_2 \frac{1}{(1-p)} = H(p)$$

$$H(D) = \sum_j p(B_j)\cdot \log_2 \frac{1}{p(B_j)}$$

$$\left. \begin{array}{l} p(B=0) = p(A=0)\cdot(1-p) + p(A=2)\cdot p \\ p(B=1) = p(A=0)\cdot p + p(A=1)\cdot(1-p) \\ p(B=2) = p(A=2)\cdot(1-p) + p(A=1)\cdot p \end{array} \right\} (*)$$

Cognoms
Nom Problema 1
Centre T. D.
Assignatura / especialitat
DNI | Núm. matrícula | Curs Grupo 30 | Grup | Data 20/05/05

$$C = \max I(F;D) = \max_{p\{A_i\}} [H(D) - H(D\backslash F)] = \max_{p\{A_i\}} H(D) - \underbrace{H(p)}_{\text{cte, indep. de } p\{A_i\}}$$

→ Para obtener C, he de hacer H(D) máxima ⟹ Eso será para $p\{B_j\} = 1/3 \quad \forall j$.

¿$\exists F, p\{A_i\} \mid p\{B_j\} = 1/3$?

Sí, para $p\{A_i\} = \frac{1}{3}, \forall i \overset{(*)}{\Longrightarrow} p\{B_j\} = \frac{1}{3}, \forall j$

Entonces, $H(D) = 3 \cdot \frac{1}{3} \log_2 3 = \log_2 3 = 1'5849$ bits/símbolo

$$\boxed{C = 1'5849 - H(p) \quad [\text{bits/símbolo}]}$$

Canal 3

$* \; H(D\backslash F) = \sum_i p(A_i) \cdot H(D\backslash A_i) = p(A=0) \cdot H(D\backslash A=0) + p(A=1) \cdot H(D\backslash A=1)$

$$H(D\backslash A=0) = \sum_j p(B_j\backslash A=0) \cdot \log_2 \frac{1}{p(B_j\backslash A=0)} = (1-p) \cdot \log_2 \frac{1}{1-p} + p \cdot \log_2 \frac{1}{p} = H(p)$$

$$H(D\backslash A=1) = \sum_j p(B_j\backslash A=1) \cdot \log_2 \frac{1}{p(B_j\backslash A=1)} = \emptyset + 1 \cdot \log_2 1 = \emptyset$$

$$\boxed{H(D\backslash F) = p(A=0) \cdot H(p) + p(A=1) \cdot \emptyset = p(A=0) \cdot H(p)}$$ → No es cte! depende de $\left\}\begin{matrix} p(A=0) \\ F \end{matrix}\right.$

$$* \; H(D) = \sum_j p(B_j) \cdot \log_2 \frac{1}{p(B_j)} = (1-p) \cdot p(A=0) \cdot \log_2 \frac{1}{(1-p) \cdot p(A=0)} +$$

$p(B=0) = (1-p) \cdot p(A=0)$

$p(B=1) = p \cdot p(A=0) + p(A=1)$

$$+ \left(p \cdot p(A=0) + p(A=1)\right) \cdot \log_2 \frac{1}{p \cdot p(A=0) + p(A=1)}$$

$$\left[C_1 = \max_{p\{A_i\}} \left[H(D) - H(D|F) \right] \right] = \max_{p\{A_i\}} \Bigg[(1-p)\cdot z \cdot \log_2 \frac{1}{(1-p)\cdot z} +$$

$\boxed{\text{llamo } z = p(A=0)} \longrightarrow p(A=1) = 1 - p(A=0) = 1 - z$

$$+ \left(p\cdot z + (1-z)\right)\cdot \log_2 \frac{1}{p z + (1-z)} - z\cdot H(p) \Bigg] \Rightarrow F(z)$$

¿Para qué $p\{A_i\}$ / z la $I(F;D)$ se hace máxima?

→ He de maximizar $F(z)$ y ese valor máximo será C_1:

$$F(z) = (1-p)\cdot z \cdot \log_2 \frac{1}{(1-p)\cdot z} + (zp + 1 - z)\cdot \log_2 \frac{1}{(zp+1-z)} - z\cdot H(p)$$

(ver Nota2)

$$F'(z) = (1-p)\cdot \log_2 \frac{1}{(1-p)z} + \frac{(1-p)^2\cdot z^2}{\ln 2}\cdot\left(\frac{-1\cdot(1-p)}{(1-p)^2 z^2}\right) + (p-1)\cdot \log_2 \frac{1}{zp+1-z} +$$

$$+ \frac{(zp+1-z)^2}{\ln 2}\cdot\left(\frac{-p+1}{(zp+1-z)^2}\right) - H(p) =$$

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

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

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

$$F'(z) = \emptyset \longrightarrow \log_2 \frac{1-(1-p)\cdot z}{(1-p)\cdot z} = \frac{H(p)}{1-p}$$

$$2^{\frac{H(p)}{1-p}} = \frac{1-(1-p)z}{(1-p)\cdot z}$$

(ver Nota1)

$$2^{\frac{H(p)}{1-p}}(1-p)\cdot z = 1 - (1-p)z$$

$$\left(2^{\frac{H(p)}{1-p}} + 1\right)\cdot(1-p)\cdot z = 1 \;;\; \boxed{z_{MAX} = \frac{1}{(1-p)\cdot\left(2^{\frac{H(p)}{1-p}} + 1\right)} = p(A=0)}$$

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. 3 — Nombre total de fulls 3 — Qualificació

Cognoms: T. D. — Nom: Problema 1
Centre:
Assignatura / especialitat:
DNI: — Núm. matrícula: — Curs: Grupo 30 — Grup: — Data: 20/05/05

Ya he encontrado la F con una p de A que maximiza I(F)!

$$\begin{cases} p(A=0) = z_{MAX}(p) \\ p(A=1) = 1 - z_{MAX}(p) \end{cases}$$

$$C(p) = (1-p)\cdot z_{MAX}\cdot \log_2 \frac{1}{(1-p)\cdot z_{MAX}} + \left(p\cdot z_{MAX} + (1-z_{MAX})\right)\cdot$$

$$\cdot \log_2 \frac{1}{p\cdot z_{MAX} + (1-z_{MAX})} - z_{MAX}\cdot H(p) \quad \left[\frac{\text{bits}}{\text{símbolo}}\right]$$

c) $p = 1/2$

canal 1 $\rightarrow$ $\left[C_1' = 1 \text{ bit/símbolo}\right]$

canal 2 $\rightarrow$ $\left[C_2' = 1'5849 - H(p=1/2) = 0'5849 \left[\frac{\text{bits}}{\text{símb}}\right]\right.$

canal 3

$$H(p=\tfrac{1}{2}) = \tfrac{1}{2}(\log_2 2)\cdot 2 = 1$$

$$z_{MAX} = p(A=0) = \frac{1}{\frac{1}{2}\cdot\left(2^{1/1/2}+1\right)} = \frac{2}{5} = 0'4 \;;\; p(A=1) = 0'6$$

$$\begin{cases} p(B=0) = \frac{1}{2}\cdot 0'4 = 0'2 \\ p(B=1) = \frac{1}{2}\cdot 0'4 + 0'6 = 0'8 \end{cases}$$

$$C_3 = \frac{1}{2}\cdot 0'4\cdot \log_2 \frac{2}{0'4} + \underbrace{\left(\tfrac{1}{2}\cdot 0'4 + 0'6\right)}_{0'8}\cdot \log_2 \frac{1}{0'8} - 0'4 =$$

$$= 0'2\cdot\log_2 5 + 0'8\cdot\log_2 1'25 - 0'4 = 0'3219 \;\frac{\text{bits}}{\text{símbolo}}$$

Con el canal 1 puedo transmitir más información.

Nota1: Para ser estrictos, faltaría comprobar que z_{MAX} ofrece un Máximo en $F(z)$:

$$F''(\underset{0'4}{z_{MAX}}) < \emptyset .$$

Otra manera de verlo, es ver si $F(z) < d$ para un $z < z_{MAX}$ y un $z > z_{MAX}$, y que sólo $F(z_{MAX}) = d$. $(z_{max} = 0'4)$

$$F(0'3) = 0'3098 < d = 0'3219$$

$$F(0'5) = 0'3113 < d = 0'3219$$

Nota2:

$$\log_a x = \frac{\ln x}{\ln a} \qquad (\ln x)' = \frac{1}{x}$$

$$(\log_a x)' = \left(\frac{\ln x}{\ln a}\right)' = \frac{1}{\ln a} \cdot \frac{1}{x}$$

Nota3: * $d_A = e_A^{-1} \bmod \phi(N_A) = e_A^{\phi(\phi(N_A))-1} \bmod \phi(N_A)$

$$\phi(N_A) = 480 = 2^5 \cdot 3 \cdot 5$$

$$\phi(\phi(N_A)) = (2^4 \cdot \underset{2-1}{1}) \cdot (3^0 \cdot \underset{3-1}{2}) \cdot (5^0 \cdot \underset{5-1}{4}) = 2^4 \cdot 2 \cdot 4 = 128$$

$$d_A = e_A^{127} \bmod 480 = 7^{127} \bmod 480 = \underset{\text{Campesino Ruso}}{\cdots} = 343$$

* $e_B = d_B^{-1} \bmod \phi(N_B) = d_B^{\phi(\phi(N_B))-1} \bmod \phi(N_B)$

$$\phi(N_B) = 20 = 2^2 \cdot 5 \rightarrow \phi(\phi(N_B)) = 2^1 \cdot 1 \cdot 4 = 8$$

$$e_B = d_B^7 \bmod 20 = 7^7 \bmod 20 = \cdots\cdots = 3$$

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Full núm. 1 | Nombre total de fulls 2 | Qualificació

Cognoms: AGUILAR | Nom: MÓNICA
Centre:
Assignatura / especialitat: TRANSMISSIÓ DE DADES
DNI: | Núm. matrícula: | Curs: | Grup: 30 | Data: 20/05/05

PROBLEMA 2

a) $N_A = p_A \cdot q_A = 17 \cdot 31 = 527$

$480 = 7 \cdot 68 + 4$

$\phi(N_A) = (p_A - 1)\cdot(q_A - 1) = 16 \cdot 30 = 480$

$e_A \cdot d_A = 1 + K \cdot \phi(N_A)$;; $7 d_A = 1 + K\, 480$;; $d_A = \dfrac{1+K\cdot 480}{7} = \dfrac{1+K\cdot(7\cdot 68+4)}{7}$

(ver Nota3)

$d_A = 68K + \dfrac{4K+1}{7} \underset{K=5}{=} 340 + 3 = 343$

¿ mcd$(e_A, \phi(N_A)) = 1$?
$e_A = 7$; $480 = 2^5 \cdot 3 \cdot 5$
Sí
$\exists\ d_A = e_A^{-1} \bmod \phi(N_A)$

Clave Pública(A) $= (e_A, N_A) = (7, 527) = K_{P_A}$
Clave Secreta(A) $= d_A = 343 = K_{S_A}$

$N_B = p_B \cdot q_B = 3 \cdot 11 = 33$

$20 = 7 \cdot 2 + 6$

$\phi(N_B) = (p_B - 1)\cdot(q_B - 1) = 2 \cdot 10 = 20$

$e_B \cdot d_B = 1 + K \cdot \phi(N_B)$;; $e_B \cdot 7 = 1 + K \cdot 20$;; $e_B = \dfrac{1+K\cdot 20}{7} = \dfrac{1+K\cdot(7\cdot 2+6)}{7}$

$e_B = 2K + \dfrac{6K+1}{7} \underset{K=1}{=} 2 + 1 = 3$

¿ mcd$(d_B, \phi(N_B)) = 1$.
$d_B = 7$; $20 = 2^2 \cdot 5$
Sí
$\exists\ e_B = d_B^{-1} \bmod \phi(N_B)$

Clave Pública(B) $= (e_B, N_B) = (3, 33) = K_{P_B}$
Clave Secreta(B) $= d_B = 7 = K_{S_B}$

b) $A \longrightarrow CA \Rightarrow ID_A \,\|\, e_A \,\|\, N_A$

$\underbrace{0001}_{ID_A}\,|\,\underbrace{0111}_{e_A}\,|\,\underbrace{0010\,|\,0000\,|\,1111}_{N_A} = M$

$\boxed{1\ 7\ 2\ \emptyset\ F}$ = Certif. en claro $A \to CA$

$H(M) = 1011 \equiv 11$

$FD(M) = H(M)^{d_{CA}} \bmod N_{CA} = 11^{53} \bmod 77 = \ldots$

$N_{CA} = p_{CA} \cdot q_{CA} = 7 \cdot 11 = 77$

$53 \equiv 110101$

$11^{53} = ((((11^2 \cdot 11)^2)^2 \cdot 11)^2)^2 \cdot 11$

$\cdots = 44 \equiv 0010|1100 \equiv 2C$

$11^2 = 121 \xrightarrow{mod\,77} 44$;; $44 \cdot 11 = 484 \longrightarrow 22$;; $22^2 = 484 \longrightarrow 22$

$22^2 = 484 \longrightarrow 22$;; $22 \cdot 11 = 242 \longrightarrow 11$;; $11^2 = 121 \longrightarrow 44$

$44^2 = 1936 \longrightarrow 11$;; $11 \cdot 11 = 121 \xrightarrow{mod\,77} \boxed{44}$

[$\underset{CA \to A}{\text{Certif. Firmado}} = 172\emptyset F|2C$]

c) $B \to CA$ $ID_B \| e_B \| N_B$ $\Rightarrow$ $\underset{ID_B}{0010} \| \underset{e_B}{0011} | \underset{N_B}{0010|0001} = M$

[$\underset{B \to CA}{\text{Certif. Claro}} = 2321$]

$H(M) = 0010 \equiv 2$;; $FD(M) = H(M)^{d_{CA}} \bmod N_{CA} = 2^{53} \bmod 77$

$2^{53} = ((((2^2 \cdot 2)^2)^2 \cdot 2)^2)^2 \cdot 2$

$\to 64$ $64^2 = 4096 \xrightarrow{mod\,77} 15$;; $15 \cdot 2 = 30 \longrightarrow 30$

$30^2 = 900 \xrightarrow{77} 53$;; $53^2 = 2809 \longrightarrow 37$;; $37 \cdot 2 = 74 \longrightarrow \boxed{74}$

64 32 16 | 8 4 2 1

$FD(M) = 74 \equiv 0100|1010 \equiv 4A$

[$\underset{CA \to B}{\text{Certif. Firmado}} = 2321|4A$]

d) 1.- A y B se intercambian sus certificados (firmados por CA previamente) por canal (inseguro).

2.- A lee $K_{PB} \to \underbrace{ID_B \| \underbrace{e_B \| N_B}_{K_{PB}}}_{M} \| FD(M)$

3.- A recalcula $M \to H(M)$
A obtiene $H(M) = FD(M)^{e_{CA}} \bmod N_{CA}$ } Si coinciden, K_{PB} auténtico

4. B lee $K_{PA} \to \underbrace{ID_A \| \underbrace{e_A \| N_A}_{K_{PA}}}_{M'} \| FD(M')$

5.- B recalcula $M' \to H(M')$
B obtiene $H(M') = FD(M')^{e_{CA}} \bmod N_{CA}$ } • Si coinciden, K_{PA} auténtica.

Problema 2

Cognoms
Nom
Centre
Assignatura / especialitat: Transmissió de Dades
DNI
Núm. matrícula
Curs
Grup: 30
Data: 20/05/05

6.- Una vez A y B se han autenticado mutuamente, se intercambian las Ksesión de ambos sentidos de la comunicación:

$A \xrightarrow[K_{sesión\_AB}]{} B$ Codificado RSA con K_{PB}:

$C_{KS\_AB} = (K_{S\_AB})^{e_B} \bmod N_B$

$B \xrightarrow[K_{sesión\_BA}]{} A$ Codificado RSA con K_{PA}:

$C_{KSBA} = (K_{S\_BA})^{e_A} \bmod N_A$

c) $A \xrightarrow[K_{S\_AB}]{} B$ $C_{KS\_AB} = (K_{S\_AB})^{e_B} \bmod N_B = 6^3 \bmod 33 =$

$= 216 \bmod 33 = 18$

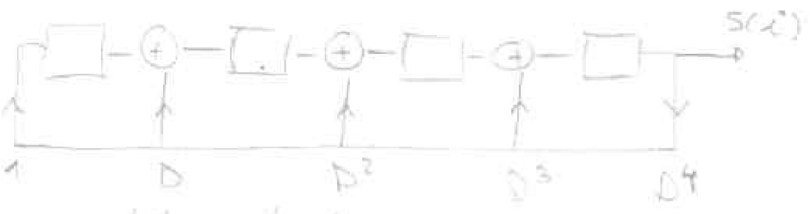
b) $B \xrightarrow[K_{S\_BA}]{} A$ $C_{KS\_BA} = (K_{S\_BA})^{e_A} \bmod N_A = 4^7 \bmod 527 =$

$= 16384 \bmod 527 = 47$

a) $A \longrightarrow B$

$M_{AB} = 11\,01\,00\,10\,1100\,1\,0\,101$

1ª bit salida LFSR (MPI) $s(i)$ $\rightarrow \oplus$

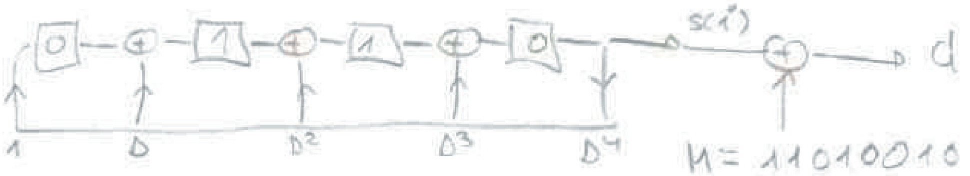


Es un polinomio completo, grado 4 → No es primitivo.

El período como máximo es $m+1 = 5$, pero depende de $p^{(0)}(D)$.

$p^{(0)}(D) \equiv K_{S\_AB} = 6$ → clave secreta de cifrado se utiliza A y de descifrado se utiliza B.

→ Necesito 17 bits de s(i).



$M = 11010010110010101$

$p^{(0)}(D) \equiv 6 \equiv \underset{1\ D\ D^2\ D^3}{0110} \equiv D + D^2$

Bit salida $s(i)$
0
1
0
1
0
0
1
0
1
0
0
⋮

$\left.\right\} L = 5$

$p^{(0)}(D) = 011\underline{\underline{0}} = D + D^2$

$p^{(1)}(D) = 001\underline{\underline{1}} = D^2 + D^3$

$p^{(2)}(D) = (D^4 + D^3) \bmod (D^4 + D^3 + D^2 + D + 1) = D^2 + D + 1 \equiv 111\underline{\underline{0}}$

$p^{(3)}(D) = D^3 + D^2 + D \equiv 011\underline{\underline{1}}$

$p^{(4)}(D) = (D^4 + D^3 + D^2) \bmod (D^4 + D^3 + D^2 + D + 1) = D + 1 \equiv 110\underline{\underline{0}}$

$p^{(5)}(D) = D^2 + D = p^{(0)}(D) \Longrightarrow L = 5 \equiv 011\underline{\underline{0}}$

Por lo tanto,

$$
\begin{array}{rl}
M_{AB} = & 11010 \mid 01011 \mid 00101 \mid 01 \\
\oplus & 01010 \mid 01010 \mid 01010 \mid 01 = s(i) \\
\hline
\end{array}
$$

$$\left[\ d = 10000 \mid 00001 \mid 01111 \mid 00\ \right]$$

h) $B \longrightarrow A$

$M_{BA} = 1010$

$p^{(0)}(D) \equiv K_{S_{B-A}} = 4 \equiv \underset{1\ D\ D^2\ D^3}{0100} \equiv D$

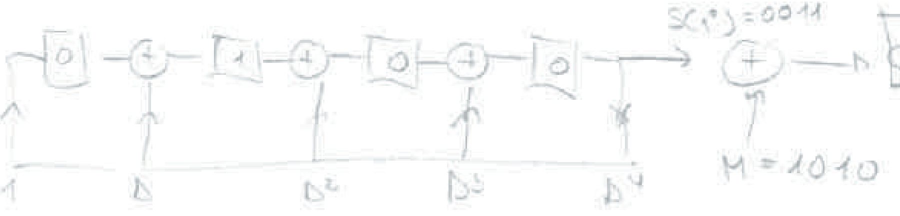
$p^{(0)}(D) = 010\underline{\underline{0}} = D$

$p^{(1)}(D) = 001\underline{\underline{0}} = D^2$

$p^{(2)}(D) = 000\underline{\underline{1}} = D^3$

$$
\begin{array}{l|l}
D^4 & D^4 + D^3 + D^2 + D + 1 \\
\hline
D^4 + D^3 + D^2 + D + 1 & 1 \\
\hline
D^3 + D^2 + D + 1 &
\end{array}
$$

$p^{(3)}(D) = D^4 \bmod (D^4 + D^3 + D^2 + D + 1) = D^3 + D^2 + D + 1 \equiv 111\underline{\underline{1}}$



$\left[\ d = 1001\ \right]$

$$
\begin{array}{rl}
 & 1\ 0\ 1\ 0 = M \\
\oplus & 0\ 0\ 1\ 1 = s(i) \\
\hline
 & 1\ 0\ 0\ 1 = d
\end{array}
$$