Problema 1

(1) Ambos usuarios obtienen sus certificados de CA:

A → $K_{P_A} = (e_A, N_A)$

$N_A = p_A \cdot q_A = 3 \cdot 11 = 33$

$\phi(N_A) = (p_A - 1) \cdot (q_A - 1) = 2 \cdot 10 = 20$

$mcd(d_A, \phi(N_A)) = mcd(7, 20) = 1$ ok!

$e_A \cdot d_A = k \cdot \phi(N_A) + 1 \rightarrow$ **$e_A \cdot 7 = k \cdot 20 + 1$** → ¡Condición que siempre se ha de cumplir!

$e_A = \frac{20k+1}{7} = 2k + \frac{6k+1}{7}$

e_A entero → k es un entero ⇒ k = 1

$K_{P_A} = (e_A, N_A) = (3, 33)$

$e_A = 3$

e_A : 00000011
N_A : 00100001
} $K_{P_A} = e_A \| N_A$ = 00000011 || 00100001

Certificado firmo (A) = $ID_A \| K_{P_A}$ = 00001111 || 00000011 || 00100001

M_A = 00001111 00000011 00100001
m_0 m_1 m_2 m_3

Esto A envía a CA.

$h_0 = DCD(m_0) = 100001$

$h_1 = DCD(h_0 \oplus m_1) = DCD(\ldots) = 101000$

$h_2 = DCD(h_1 \oplus m_2) = DCD(100100) = 010010$

$h_3 = DCD(h_2 \oplus m_3) = DCD(\ldots) = 111001$

$H_A(M) = 00111001_2$ → $H_A(M) = 57_d$ → La FDA requiere, CA la firma con su d_{CA}!!

$N_{CA} = p_{CA} \cdot q_{CA} = 119$

$FD_A = (H_A(M))^{d_{CA}} \bmod N_{CA} = 57^5 \bmod 119 = 92_d \equiv 01011100_b$

Firma digital de CA.

Esto es lo que CA devuelve a A: su certificado. A lo puede enviar a cualquiera para comunicarle su K_{PA} y que le pueda autenticar!

Certificado_firmado(A) = certificado_claro(A) || Firma Digital =

K_{PA}

= ID_A (0000 1111) || e_A (0000 0011) || N_A (0010 0001) || 0101 1100

M_A | $FD_A = D_{SCA}(H(M_A))$

B →

Certificado_claro = ID_B || KP_B = 1111 0000 || 0000 0011 || 0011 0111

$N_B = p_B \cdot q_B = 55 \equiv 11\,0111$

M_B = 1111 0000 | 0000 0011 | 0011 0111

m_0 m_1 m_2 m_3

$h_0 = DCD(m_0) = 011110$

$h_1 = DCD(h_0 \oplus m_1) = DCD(011110) = 001111$

$h_2 = DCD(h_1 \oplus m_2) = DCD(000011) = 100001$

$h_3 = DCD(h_2 \oplus m_3) = DCD(010110) = 001011$

$K_{PB} = (3, 55)$

$H_B(M) = 0000\,1011 \equiv 11_d$

$FD_B = (H_B(M))^{d_{CA}} \bmod N_{CA} = 11^5 \bmod 119 = 44 \equiv 0010\,1100$

Certificado_firmado(B) = certificado_claro(B) || FD_B =

K_{PB}

= ID_B (1111 0000) || e_B (0000 0011) || N_B (0011 0111) || 0010 1100

M_B | $FD_B = D_{SCA}(H(M_B))$

② A y B intercambian sus certificados en claro. Desean intercambiarse las claves públicas, autenticando la clave pública que el otro le ha enviado.

A → • Le llega el certificado_firmado(B) => lee en claro $K_{PB} = (e_B, N_B) = (3, 55)$

• lee $FD_B = 44_d$

• Como conoce la K_{PCA}, podrá averiguar $H(M_B)$.

Problema 1

$k_{PCA} = 0$ $\quad e_{CA} \cdot d_{CA} = k \cdot \phi_{CA}(N) + 1 = 96 \cdot k + 1$

$\phi_{CA}(N) = (p_A - 1)\cdot(q_{CA} - 1) = 6 \cdot 16 = 96$

$mcd(d, \phi(N)) = mcd(5, 2^5 \cdot 3) = 1$. OK!

$e = \frac{96k+1}{5} =$

$= 19k + \frac{k+1}{5}$

$k = 4 \rightarrow e_{CA} = 77$

$H(M_B) = 44^{e_{CA}} \bmod N_{CA} = 44^{77} \bmod 119 = 11$

$77 = 1001101$ (64 8 4 1) ;; $44^{77} = \left(\left(\left(\left((44^2)^2\right)^2 \cdot 44\right)^2 \cdot 44\right)^2 \cdot 44\right)^2 \cdot 44$

$44^2 = 1936$	mod 119 →	32
$32^2 = 1024$		72
$72^2 = 5184$		67
$67 \cdot 44 = 2948$		92
$92^2 = 8464$		15
$15 \cdot 44 = 660$		65
$65^2 = 4225$		60
$60^2 = 3600$		30
$30 \cdot 44 = 1320$		11 = $H_B(M)$

OK! Coinciden!

• Una vez averiguado $H_B(M)$, calcula de nuevo $H_B(M)$ a partir del M se lo ha llegado. Si coinciden, autentificado el contenido y el origen del certificado.

B → Del mismo modo que A:

• lee $k_{PA} = (e_A, N_A) = (3, 33)$ del certificado de A.

• lee $FD_A = 92$

• A partir de FD_A y k_{PA}, averigua $H(M_A)$:

$H(M_A) = 92^{77} \bmod 119 = (*) = 57$

• Recalcula $H(M_A)$ a partir del M_A que lee del certificado.

• Si coinciden, autentica la k_{PA}.

(*) $92^{77} \bmod 119 = \left(\left(\left(\left((92^2)^2\right)^2 \cdot 92\right)^2 \cdot 92\right)^2\right)^2 \cdot 92 \bmod 119 = 57$

		mod 119	
92^2	= 8464		15
15^2			106
106^2	= 11236		50
$50 \cdot 92$	= 4600		78
78^2	= 6084		15
$15 \cdot 92$	= 1380		91
91^2	= 5041		43
43^2	= 1849		64
$64 \cdot 92$	= 5888		57 = $H_1(M)$ OK! Coinciden!

(3) A y B se intercambian la clave de sesión, $K_S = 5$:

- A empieza a enviar un mensaje, por lo se cuenta cuál la K_S a B, usando clave pública RSA:

$K_{sesión} = 5 \equiv 101 = M$

$C = M^{e_B} \bmod N_B = 5^3 \bmod 55 = 125 \bmod 55 = 15$

- B recibe el criptograma $C = 15$ y lo descifra con su $K_{secreta}$:

$M = C^{d_B} \bmod N_B = 15^{27} \bmod 55 \overset{(*)'}{=} [5 = K_{sesión}]$

$e_B \cdot d_B = k \cdot \varphi_B(N) + 1 \quad ;; \quad \varphi_B(N) = (p_B - 1)\cdot(q_B - 1) = 4 \cdot 10 = 40$

$3 \cdot d_B = k \cdot 40 + 1 \quad ;; \quad d_B = \frac{40k+1}{3} = 13k + \frac{k+1}{3}$

$k = 2 \rightarrow d_B = 27$

(*)' $27 \equiv 11011_b \rightarrow C^{27} = \left(\left(\left(C^2 \cdot C\right)^2\right)^2 \cdot C\right)^2 \cdot C$

(4) A cifra el mensaje "aparta por flecha" con cifrado de César y clave 5: $C' = (M + 5) \bmod 26$

a b c d e | f g h i j k l | m n o p | q r s t | u v w x | y z

f g h i j | k l m n o p q | r s t u | v w x y | z a b c | d e

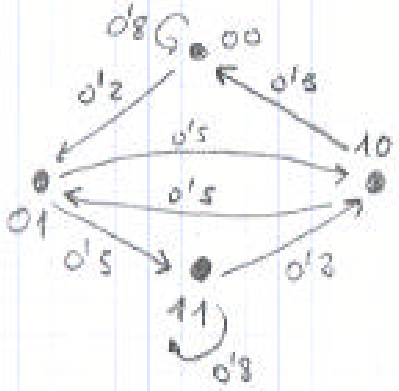
"fuzjxyf ulw kqjhmf"

(5) B lo descifra con la $K_{sesión} = 5 \Rightarrow M = (C - 5) \bmod 26$ y le devuelve:

"fuzjxyf kqjhmf tp" (6) A lo descifra con $K_{ses.} = 5$.

Problema 2

a)



$P(0\backslash 00) = P(1\backslash 11) = 0'8$

$P(1\backslash 00) = P(0\backslash 11) = 0'2$

$P(0\backslash 01) = P(0\backslash 10) = P(1\backslash 01) = P(1\backslash 10) = 0'5$

Nota: Le ayudarán pensar que los nuevos símbolos que emite la fuente, se colocan por la derecha:

Estado inicial = 10 → 0 → Nuevo estado 00; → 1 → 01

$$\left.\begin{aligned} P(00) &= P(00)\cdot P(0\backslash 00) + P(10)\cdot P(0\backslash 10) \\ P(01) &= P(00)\cdot P(1\backslash 00) + P(10)\cdot P(1\backslash 10) \\ P(10) &= P(01)\cdot P(0\backslash 01) + P(11)\cdot P(0\backslash 11) \\ P(11) &= P(11)\cdot P(1\backslash 11) + P(01)\cdot P(1\backslash 01) \end{aligned}\right\} + \quad 1$$

(0.9, 0.5, 0.2, 0.5, 0.8, 0.5)

$P(00) - P(11) = 0'6 \cdot P(00)$

$0'4 \cdot P(00) = P(01)$

$P(11) - P(10) = 0'6 \cdot P(11)$

$0'4 \cdot P(11) = P(10)$

$P(00) + 0'4 \cdot P(00) + 0'4 \cdot P(11) + P(11) = 1$

$1'4 \cdot P(00) + 1'4 \cdot P(11) = 1$

$2 \cdot 1'4 \cdot P(00) = 1$

$P(00) = P(11) = \frac{5}{14}$ 0'3572

$P(00) = 0'8 \cdot P(00) + 0'4 \cdot 0'5 \cdot P(11)$

$P(00) = P(11)$

$P(01) = P(10) = \frac{2}{14}$ 0'1428

Problema 2

b) $H(F) = H(F\backslash 01)\cdot P(01) + H(F\backslash 10)\cdot P(10) + H(F\backslash 00)\cdot P(00) + H(F\backslash 11)\cdot P(11)$

$H(F\backslash 01) = \underset{0'5}{P(0\backslash 01)}\cdot \log_2 \frac{1}{P(0\backslash 01)} + \underset{0'5}{P(1\backslash 01)}\cdot \log_2 \frac{1}{P(1\backslash 01)} = 2\cdot 0'5 \cdot \underbrace{\log_2 \frac{1}{0'5}}_{1} = 1$

$H(F\backslash 10) = \underset{0'5}{P(0\backslash 10)}\cdot \log_2 \frac{1}{P(0\backslash 10)} + \underset{0'5}{P(1\backslash 10)}\cdot \log_2 \frac{1}{P(1\backslash 10)} = 1$

$H(F\backslash 00) = \underset{0'8}{P(0\backslash 00)}\cdot \log_2 \frac{1}{P(0\backslash 00)} + \underset{0'2}{P(1\backslash 00)}\cdot \log_2 \frac{1}{P(1\backslash 00)} = 0'7219$

$H(F\backslash 11) = P(0\backslash 11)\cdot \log_2 \frac{1}{P(0\backslash 11)} + P(1\backslash 11)\cdot \log_2 \frac{1}{P(1\backslash 11)} = 0'7219$

$$\boxed{H(F_1) = 2\cdot 1\cdot \frac{2}{14} + 2\cdot 0'7219\cdot \frac{5}{14} = 0'80137 \text{ bit/símbolo}}$$

c) $P(0) = P(0\backslash 01)\cdot P(01) + P(0\backslash 10)\cdot P(10) + P(0\backslash 00)\cdot P(00) + P(0\backslash 11)\cdot P(11) =$

$= 0'5\cdot \frac{2}{14} + 0'5\cdot \frac{2}{14} + 0'8\cdot \frac{5}{14} + 0'2\cdot \frac{5}{14} = \frac{2}{14} + \frac{5}{14} = 0'5$

$P(1) = P(1\backslash 01)\cdot P(01) + P(1\backslash 10)\cdot P(10) + P(1\backslash 00)\cdot P(00) + P(1\backslash 11)\cdot P(11) =$

$= 0'5\cdot \frac{2}{14} + 0'5\cdot \frac{2}{14} + 0'2\cdot \frac{5}{14} + 0'8\cdot \frac{5}{14} = 0'5$

$P(0) + P(1) = 1$ Aumenta, por haber más incertidumbre, más información.

$$\boxed{H(F_2) = 0'5\cdot \log_2 \frac{1}{1/2} + 0'5\cdot \log_2 \frac{1}{1/2} = 1 \text{ bit/símbolo}}$$

Problema 2

d) $F_2 \to \begin{matrix} \emptyset \\ 1 \end{matrix}$ $\quad \bar{L} = 1 \text{ bit/símbolo}$

$$\boxed{E = \frac{H}{\bar{L}} = 1}$$

e) $H(F_1, F_2) \leq H(F_1) + H(F_2)$ con igualdad si F_1 y F_2 son independientes, como es el caso.

$$\boxed{H(F_1, F_2) = H(F_1) + H(F_2) = 1'80137 \text{ bit/símbolo}}$$

$H(F_1, F_2) = H(F_1) + H(F_2 \setminus F_1) = H(F_1) + H(F_2)$

$\Big\Vert$

$H(F_2) + H(F_1 \setminus F_2)$

$\Big\Vert$

$H(F_2) + H(F_1)$

si F_1 y F_2 son independientes.

$H(F_2 \setminus F_1) = H(F_2)$ si F_1 y F_2 son independientes.

$$\boxed{H(F_1 \setminus F_2) = H(F_1) = 0'80137 \frac{\text{bit}}{\text{símbolo}}}$$

$$\boxed{H(F_2 \setminus F_1) = H(F_2) = 1 \text{ bit/símbolo}}$$

Problema 2

a) 10|10|11|01|00|100|111|010|1000 = mensaje usuario (son 23 bits)

→ 23 bits

Diccionario

posición	entrada al diccionario
0001 (1)	1
0010	0
0011	10 → se añade al final (1)
0100	11
0101	01
0110	00
0111 (10)	100
1000	111
1001	010
1010	1000 → y se añade (10)
1011	
1100	
1101	
1110	
1111	

Codificación:

- 00001 → ya que aún no habíamos aparecido.
- 00000
- 00010 (1)
- 00011
- 00101
- 00100
- 00110
- 01001
- 01010
- 01110 (10)

→ Ocupa 50 bits !!

tasa "compresión" → $\frac{50}{23} \times 100 =$

$= 217'3913\ \%$

$100\% - 217'3913 = -117'39\%$

No comprime.

- El mensaje de usuario es demasiado corto, y no comprime.
- Comprimirá para mensajes más largos, si había más palabras largas repetidas.