RC - PEC 1

2017

MTU

Cabecera 20b
Longitud 1684 b
MTU 536

1º Tamaño Paquete

MTU - Cab = 536 - 20 = 516 b.

516 | 8
64 → Desplazamiento
4

516 - 4 = 512 b útiles
Tamaño PKTs

2º Nº Paquetes L / Tamaño PKT

1684 | 512
148 3 28 => 4 pkt's de 512 (3) y 148 (1)

3º Tabla

Long	ID	Índice	Desplazamiento
512 + 20	777	1	0
512 + 20	777	1	64
512 + 20	777	1	128
148 + 20	777	0	192

Índice: Siempre 1 y último 0
Empieza en 0 y se suman el desplazamiento que hemos calculado.

Longitud 4000 b.
MTU 1500 b.

Tamaño = 1500 - 20 = 1480 b.

1480 | 8
68 185 desplazamiento
40
0

4000 | 1480
1040 2 7
3 pkt

Long	ID	Índice	Desplazamiento
1480+20	777	1	0
1480+20	77	1	185
1040+20	777	0	370

L = 2400 b
C = 20 b
MTU = 700 b

Tamaño = 700 - 20 = 680 b.

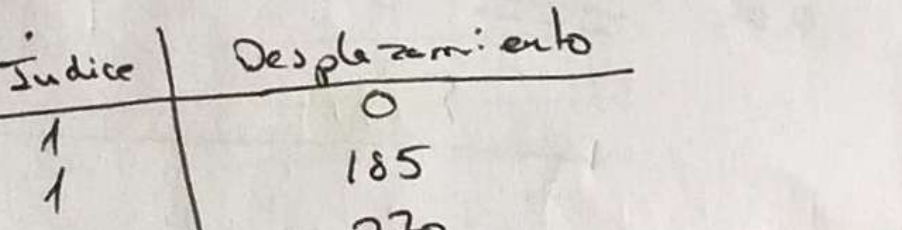
680 | 8
0 85 desplazamiento.

2400 | 680
-360 3 5
4 pkts

long	ID	Índice	Despl.
680 + 20	7	1	0
680 + 20	7	1	85
680 + 20	7	1	170
360 + 20	7	0	255

NAT

IP 212.128.48.32 (WAN)
192.168.1.0/24 (LAN)



b) 173.194.34.215 / 5001
173.194.34.215 / 5002
173.194.34.215 / 5003

192.168.1.2 : 3343
192.168.1.3 : 3344
192.168.1.4 : 3345

$x^3+1 = x^3+x^2+x+1$
$1\ 0\ 0\ 1$

CRC

Hacemos una XOR y despreciamos el de la izquierda.

XOR	
00	0
01	1
10	1
11	0

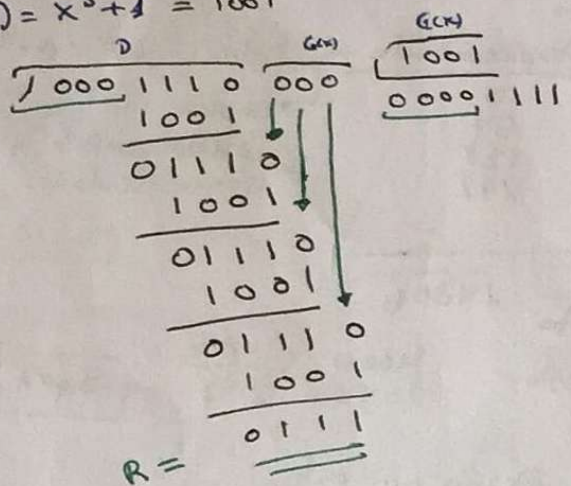
$G(x) = x^3+1 \Rightarrow 1001$ Dividimos entre 1001.

Añadimos 000 al D (numerador) y dividimos.

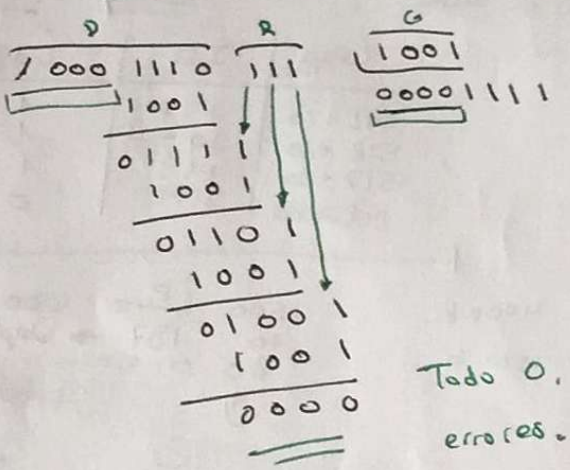
Cambiamos el Resto por los 000 de antes y volvemos a dividir. todo 0 - OK algún 1 - fallo

$D = 1000\ 111\ 0$

$G(x) = x^3+1 = 1001$



COMPROBACIÓN



Todo 0, sin errores.

ALOHA

$P(1-P)^{n-1}$ → Probabilidad de que un nodo transmita.

$Np(1-p)^{n-1}$ → Probabilidad de que algún nodo transmita.

$t_{trans} = \frac{L}{R}$

$V_{trans} = \frac{R}{L}$

A, B, C y D ≠

L fija

R ancho banda

a) A tenga éxito

b) Algún nodo tenga éxito

c) PA 20% PC 30% PD = [illegible] L=1500b R=100Mb/s Vmedia transmisión?

a) $P \neq \Rightarrow P(A) = P(A)\cdot(1-P_B)\cdot(1-P_C)\cdot(1-P_d)$

$P = \Rightarrow P(A) = P(A)\,(1-P(A))^3$

b) $P \neq \Rightarrow P(x) = P_A(1-P_A)^3 + P_B(1-P_B)^3 + P_C(1-P_C)^3 + P_D(1-P_D)^3$

$P = \Rightarrow P(x) = 4P(1-P)^3$

A, B y C ≠

a) A tenga éxito b) Algun nodo c) PA 20% PB/C 30% L 1500b R 100Mb/s

a) $P \neq \Rightarrow P(A) = P_A\cdot(1-P_B)\cdot(1-P_C)$

$P = \Rightarrow P(A) = P_A(1-P_A)^2$

b) $P \neq \Rightarrow P(x) = P(A)(1-P_A)^2 + P_B(1-P_B)^2 + P_C(1-P_C)^2$

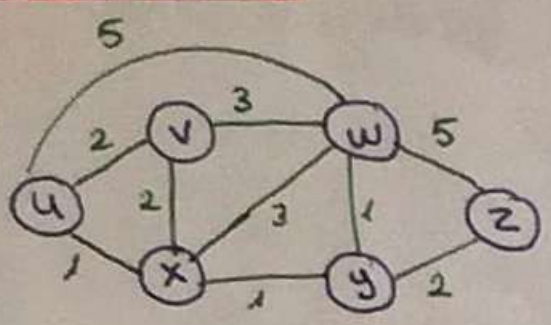
$P = \Rightarrow P(x) = 3P(1-P)^2$

c) $V_{PA} = P_A\cdot R = 20\,M/s$

$V_{PA\,y\,C} = P_B\cdot R = 30\,M/s$

$V_{Px} = \frac{\sum V_{Px}}{N} = \frac{80}{3} = 26\frac{2}{3}\,M/s$

Dijsktra

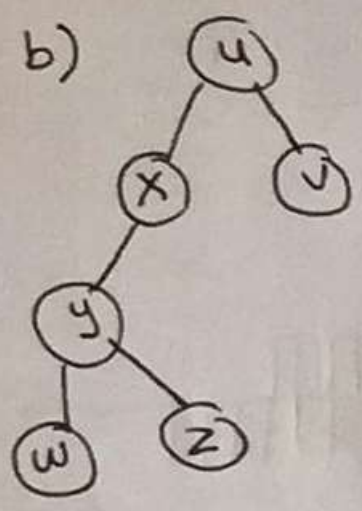


a)

	v	w	x	y	z
u	2,u	5,u	1,u	∞	∞
u x	2,u	4,x		2,x	∞
u x y	2,u	3,y			4,y
u x y v		3,y			4,y
u x y v w					4,y
u x y v w z					

Con cada paso se va actualizando la tabla

b)



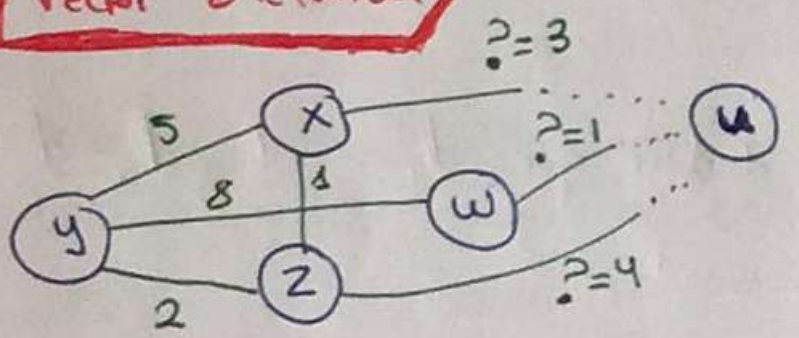
c)

destino	enlace
v	u,v
w	u,x
x	u,x
y	u,x
z	u,x

→ 1º Nodo y el siguiente para llegar al destino.

x e v llega directamente, pero el resto pasan por x.

Vector Distancia



	y	x	z	w	u
y	—	5 3	2 2	8 7	∞ 6
x	3	—	1	4	3
z	2	1	—	5	4
w	7	4	5	—	1
u	6	3	4	1	—

Ethernet

$t_{prop} = \frac{d}{v}$ (max tiempo retardo entre 2 nodos)

$t_{trans} = \frac{L}{R}$ (tiempo trasmitir una trama máximo)

$\eta = \frac{1}{1 + 2e\,\frac{t_{prop}}{t_{trans}}}$ (Puede variar la formula)

t_{prop} tiende a 0 / ∞ } η tiende a 1.

t_{trans} tiende a ∞

$\frac{2}{3}\ \frac{5}{4} = \frac{2 \cdot 4}{3 \cdot 5} = \frac{8}{15}$

a) Longitud trama Lo

$\eta = \frac{1}{1 + 2e\,\frac{t_{prop}}{\frac{L}{R}}}$

Cuanto mas grande es L > es η

b) $R = 100\ M/s \rightarrow 100 \cdot 10^6\ b/s$

$V = 2 \cdot 10^8\ m/s \rightarrow 2 \cdot 10^8\ m/s$

$L = 15000\ By \rightarrow 15000 \cdot 8 = 120000\ b.$

$\eta \leq 0'7$?

$0'7 \leq \frac{1}{1 + 2e\,\frac{\frac{d}{V}}{\frac{L}{R}}}$;

$0'7 \leq \frac{1}{1 + 2e\,\frac{\frac{d}{2 \cdot 10^8}}{\frac{120000}{100 \cdot 10^6}}}$; $0'7 \leq \frac{1}{1 + 2e\,\frac{100 \cdot 10^6 \cdot d}{2 \cdot 10^8 \cdot 12000}}$; $0'7 \leq \frac{1}{1 + \frac{543656365'7 \cdot d}{2'4 \cdot 10^{12}}}$; $0'7 \leq \frac{1}{\frac{2'4 \cdot 10^{12}}{2'4 \cdot 10^{12}} + \frac{\ldots \cdot d}{2'4 \cdot 10^{12}}}$

$0'7 \leq \frac{1}{\frac{2'4 \cdot 10^{12} + 543656365'7 \cdot d}{2'4 \cdot 10^{12}}}$; $0'7 \leq \frac{2'4 \cdot 10^{12}}{2'4 \cdot 10^{12} + 543656365'7 \cdot d}$; $\frac{\frac{2'4 \cdot 10^{12}}{0'7} - 2'4 \cdot 10^{12}}{543656365'7} \leq d$;

$\frac{1'02 \cdot 10^{12}}{543656365'7} \leq d$; $1891'9_m \leq d$

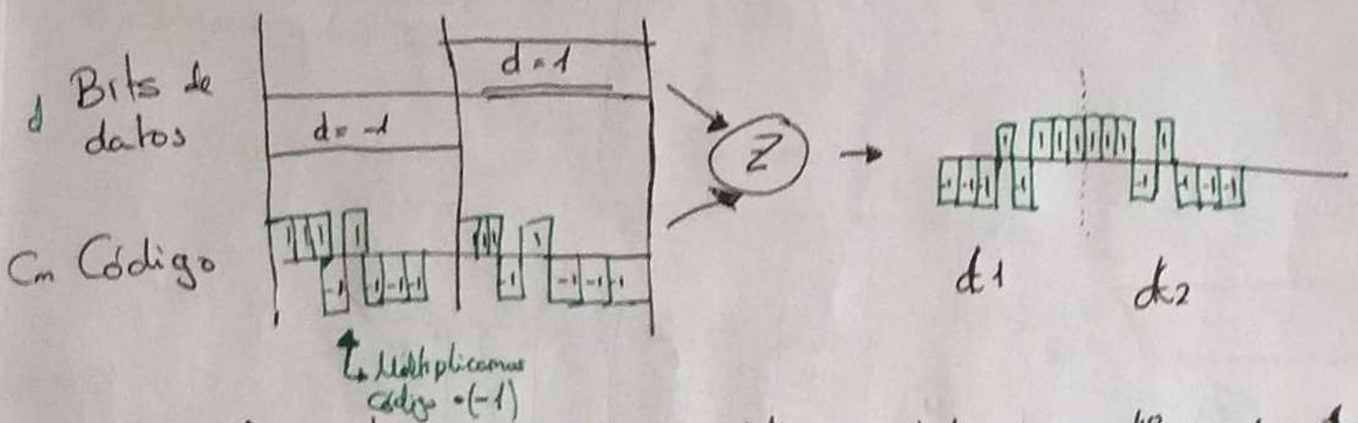
→ lo de la calle

CDMA

Se van retrasmitiendo bit's, y cada uno con un código CDMA. Existen varios ejemplos. Al final nos sale Z. Que es el resultado de multiplicar d (bit) · C_m

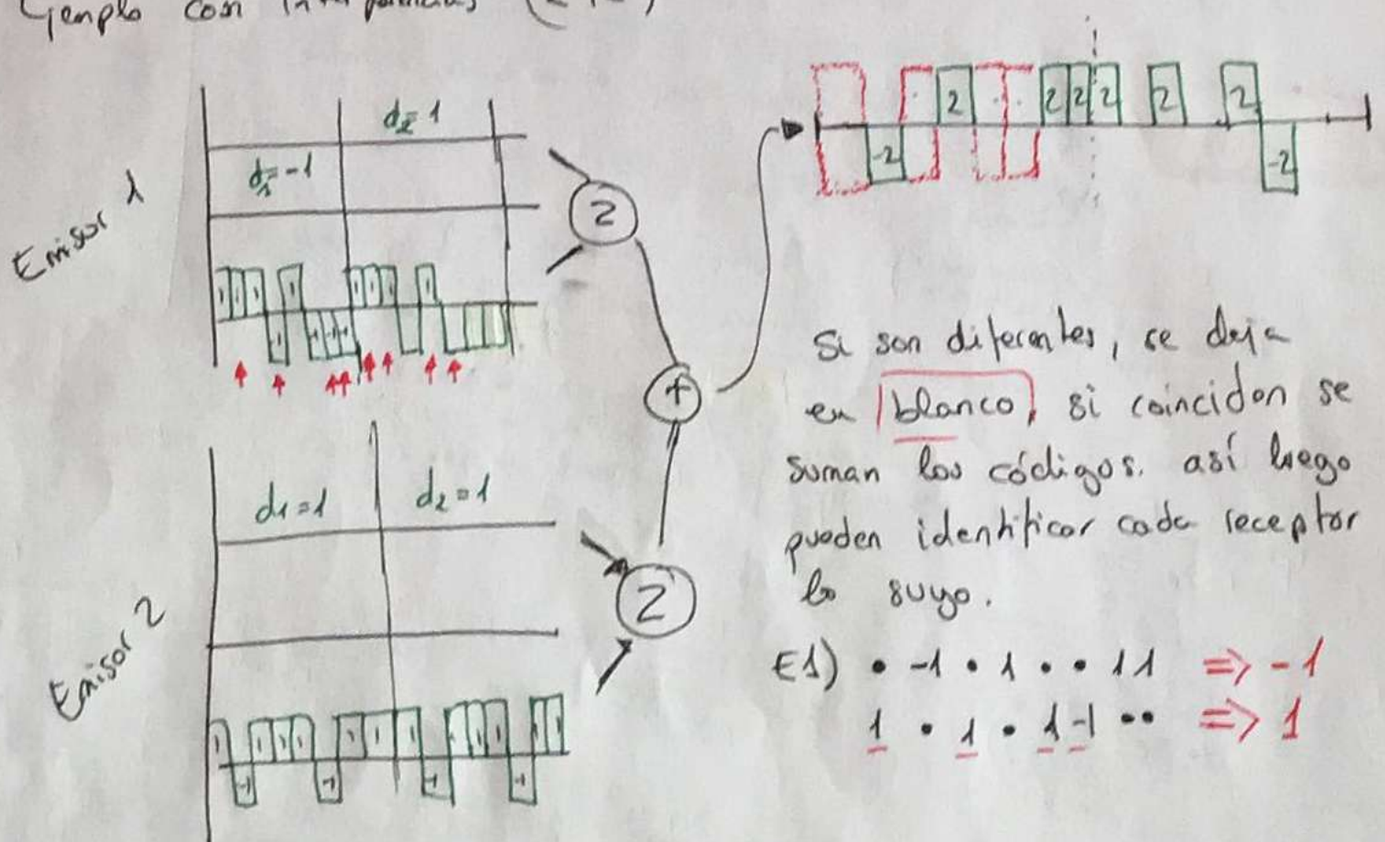
$$Z = d \cdot c$$

Ejemplo sin interferencias



El receptor compara con el código y dedisce que $d_1^0 = -1$ y $d_2 = 1$

Ejemplo con interferencias (2PC)



Si son diferentes, se deja en blanco, si coinciden se suman los códigos. así luego pueden identificar cada receptor lo suyo.

E1) · -1 · 1 · · 1 1 ⇒ -1

1 · 1 · 1 -1 · · ⇒ 1

	⊕
00	0
01	1
10	1
11	0

CBC

P6) Bloque 3 bits

0	000	→ 110	6
1	001	→ 111	7
2	010	→ 101	5
3	011	→ 100	4
4	100	→ 011	3
5	101	→ 010	2
6	110	→ 000	0
7	111	→ 001	1

Tabla 8.1

$m = 100\ 100\ 100$

a) $C = 011\ 011\ 011$ (SIN CBC)

c) CBC con IV = 111 (Semilla) [111 100 100 100]

Initialization Vector

$c(i) = ks(m(i) \oplus c(i-1))$

$c(1) = 100 \oplus 111 \rightarrow 011 \rightarrow 100$ (4)

$c(2) = 100 \oplus 100 \rightarrow 000 \rightarrow 110$ (6)

$c(3) = 100 \oplus 110 \rightarrow 010 \rightarrow 101$ (5)

$C = 111\ 100\ 110\ 101$

$m(i) = ks^{-1}(c(i)) \oplus c(i-1)$

$m(1) = 100 \oplus 111 = 100$ (011)

$m(2) = 110 \oplus 100 = 100$ (000)

$m(3) = 101 \oplus 110 = 100$ (010)

Ejemplo Kroose)

$m = 010\ 010\ 001$ IV = 001

$c(1) = 010 \oplus 001 = 011 \rightarrow 100$

$c(2) = 010 \oplus 100 = 110 \rightarrow 000$

$c(3) = 001 \oplus 000 = 001 \rightarrow 111$

$C = 100\ 000\ 111$ IV = 001

$m(1) = 100 \oplus 001 \Rightarrow 010$ (011)

$m(2) = 000 \oplus 100 \Rightarrow 010$ (110)

$m(3) = 111 \oplus 000 \Rightarrow 001$ (001)

P3 Examen) Tabla

	9	28	26	26	16	25	12	29	15	3	14	17	25
m =	17	27	20	20	24	12	25	6	13	11	2	9	12

IV

$c(0) = 10001$ (17)

$m(1) = ks^{-1}(c(1)) \oplus c(0) = ks^{-1}(11011)$ (27) $\oplus$ (10001) = 11100 $\oplus$ 10001 = 01101 ⇒ 13 M

$m(1) = 11010$ (26) $\oplus$ 11011 (27) = 00001 ⇒ 1 A

$m(2) = 11010$ (26) $\oplus$ 10100 (20) = 01110 ⇒ 14 N

$m(3) = 11010$ (26) $\oplus$ 10100 (20) = 00100 ⇒ 4 D

$m(4) = 10000$ (16) $\oplus$ 10100 (20) = 00001 ⇒ 1 A

$m(5) = 11001 \oplus 11000 = 00000 \Rightarrow 0$ -

$m(6) = 01100 \oplus 01100 = 00100 \Rightarrow 4$ D

$m(7) = 11101 \oplus 11001 = 01001 \Rightarrow 9$ I

$m(8) = 01111 \oplus 00110 = 01110 \Rightarrow 14$ N

$m(9) = 00011 \oplus 01101 = 01110 \Rightarrow 5$ E

$m(10) = 01110 \oplus 01011 = 00101 \Rightarrow 19$ R

$m(11) = 10001 \oplus 00010 = 10010 \Rightarrow 16$ O

$m(12) = 11001 \oplus 01001 = 10000 \Rightarrow 16$

Sol.	13	1	14	4	1	0	4	9	14	5	19	16
	M	A	N	D	A	-	D	I	N	E	R	O

RSA

$n = p \cdot q$ $\quad n=667$

$z = (p-1)(q-1)$

$d = \frac{z+1}{e}$ $\Longrightarrow$ Buscamos que sea un número entero. Si no, vamos probando múltiplos de z. $20 \to 40 \to 60 \to 80$

$d = e^{-1} \bmod z$

e = nº < n y coprimo z

667 \| 23 → p
29 \| 29 → q
1 \|

K+ {n, e} C. Pública
K- {p, q, d} C. Privada

Cifrar	$c = m^e \bmod (n)$
Descifrar	$m = c^d \bmod (n)$
firma	$F = (H(m))^d \bmod (n)$
Resumen	$H(m) = F^e \bmod (n)$

Calcular Modulo grande

$51^{11} \bmod 77 = \text{ERROR}$

$[(51^5 \bmod 77)(51^5 \bmod 77)(51 \bmod 77)] \bmod 77$

Calcular Módulo menor

$208 \bmod 255 \Rightarrow 208.$

Calcular Módulo

$3^9 \bmod 33 = 19683 \bmod 33$

1º $19683 / 33 = 596'454545$

2º $596 \cdot 33 = 19668$

3º $19683 - 19668 = 15$

Ejercicio ① Cifrar y descifrar "dog" $d=4$ $o=15$ $g=7$

$p=3$
$q=11$
$e=9$

$n = p \cdot q = 33$

$z = (p-1)(q-1) = 20$

$d = \frac{z+1}{e} = \frac{20+1}{9} = 2'33$ ✗

$d = \frac{80+1}{9} = \frac{81}{9} = 9$ ✓

Cifrar
1º $c(1) = d^9 \bmod 33 = 4^9 \bmod 33 = 25$
2º $c(2) = o^9 \bmod 33 = 15^9 \bmod 33 = 3$
3º $c(3) = g^9 \bmod 33 = 7^9 \bmod 33 = 19$

Descifrar
1 $m(1) = 25^9 \bmod 33 = 4 \sim d$
2 $m(2) = 3^9 \bmod 33 = 15 \sim o$
3 $m(3) = 19^9 \bmod 33 = 7 \sim g$

Ejercicio ② función Resumen y firma $\quad x_0 = 27 \quad x_i = a(x_{i-1} + m_i) + b \bmod (m) \quad n = 521,\ a = 17,\ b = 45$

$m = 5\,4\,8\,2\,7\,8\,3\,1\,9\,2$ tabla: 0=47, 1=49, 2=50, ..., 8=56 y 9=57

Empieza

$n = 667$
$e = 17$

667 \| 23
29 \| 29
1 \|

$p = 23$
$q = 29$

$z = (p-1)(q-1) = 616$

$d = \frac{z+1}{e} = \frac{616+1}{17} = 36'29$ ✗

$d = \frac{(616 \cdot 4)+1}{17} = 145$ ✓

$x_0 = 27$
$x_1 = 17(27 + 50) + 45 \bmod 521 = 312$
$x_2 = 17(312 + 57) + 45 \bmod 521 = 66$
...
$x_{10} = 17(249 + 53) + 45 \bmod 521 = 490$

$H(m) = 490$

$F = (H(m))^d \bmod (n)$
$H(m) = F^e \bmod (n)$

$F = (490)^{145} \bmod 667 = 250$

Comprobación:

$H(m) = (250)^{17} \bmod 667 = 490$

$B+ \begin{cases} n=253 \\ e=13 \end{cases}$ $\quad h_0 = 1$

$A+ \begin{cases} n=323 \\ e=11 \end{cases}$ $\quad A \longrightarrow B$

$c = (144, 136, 26, 126)$

$f = 118$

$c = m^e \bmod n$

$m = c^d \bmod n$

$F = (H(m))^d \bmod n$

$H(m) = F^e \bmod n$

$m(1) = 144^{17} \bmod 253 = 12 - L$

$m(2) = 136^{17} \bmod 253 = 5 - E$

$m(3) = 26^{17} \bmod 253 = 16 - O$

$m(4) = 126^{17} \bmod 253 = 14 - N$

$m(1) = (\underbrace{144^4}_{\to 100} \cdot 144^4 \cdot 144^4 \cdot 144^4 \cdot 144) \bmod 253$

$100^4 \bmod 253 = 232$

$(232 \cdot 144) \bmod 253 = \underline{12}$

$m(2) = (\underbrace{136^4}_{\to 223} \cdot 136^4 \cdot 136^4 \cdot 136^4 \cdot 136) \bmod 253$

$223^4 \bmod 253 = 147$

$(147 \cdot 136) \bmod 253 = 5$

$m(3) = (\underbrace{26^4}_{58} \cdot 26^4 \cdot 26^4 \cdot 26^4 \cdot 26) \bmod 253$

$58^4 \bmod 253 = 59$

$(59 \cdot 26) \bmod 253 = 16$

$m(4) = (\underbrace{126}_{174} \cdot 126 \cdot 126 \cdot 126 \cdot 126) \bmod 253$

$174^4 \bmod 253 = 2$

$(225 \cdot 126) \bmod 253 = 14$

Clave Privada Begoña

253	11	$p = 11$
23	23	$q = 23$
1		

$Z = (p-1)(q-1) = 220$

$d = \frac{Z+1}{e} = \frac{220+1}{13} = 17$

$h_0 = 1 \to 00001$

$h_1 = 01100 \overset{12}{\oplus} 00001 \overset{1}{=}$

$01101 \overset{13}{\Rightarrow}$ Tabla

$h_2 = 00101 \oplus$

$h_3 = 10000 \oplus$

$h_4 = 01110 \oplus$

$h_4 = H(m)$ **16**

$F = 118$ (La firma alicia)

$H(m) = 118^{11} \bmod 323$

$(\underbrace{118^5}_{169} \cdot 118^5 \cdot 118) \bmod 323$

$(137 \cdot 118) \bmod 323$

$= \boxed{16}$

P3) $x_{i+1} = x_i^2 \bmod (n)$ **CIFRADO FLUJO** Clave Pública

$a \to g^a$, $b \to g^b$, $(g^a)^b$, $(g^b)^a$

$n = 437$

$Z_{257} = \{0, 1, 2 \ldots 256\}$

$g = 3 \bmod 257$

$a = 108$

$b = 46 \in Z_{257}$

a) Valor clave X_0 Diffie-Hellman?

Alicia calcula $A = 3^{a} \bmod 257$

Begoña calcula $B = 46 \bmod 257$ (y envía a Alicia)

Alicia calcula $(g^b)^a = g^{ba}$ X_0

$X_0 = 46^{108} \bmod 257 = 249 \bmod 257$

b) $B \to A$ $\{0, 1, 1, 1, 1, 1, 1, 0\}$ Mensaje?

↑ menos signif.

$m(i) = C(i) \oplus K(i)$

$X_0 = 46^{108} \bmod 257 = 249 \bmod 257$

$X_1 = 249^2 \bmod 437 = 384$

$X_2 = 384^2 \bmod 437 = 187$

$X_3 = 187^2 \bmod 437 = 9$

$X_4 = 9^2 \bmod 437 = 81$

$X_5 = 81^2 \bmod 437 = 6$

$X_6 = 6^2 \bmod 437 = 36$

$X_7 = 36^2 \bmod 437 = 422$

$X_8 = 422^2 \bmod 437 = 235$

PAR = 0 IMPAR = 1

$LSB(X_i) = K(i) = 0 1 1 1 0 0 0 1$

$\oplus$
0 1 1 1 1 1 1 0
0 1 1 1 0 0 0 1

$m(i) = 0 0 0 0 1 1 1 1$

RSA

P4) $B \{n = 323, e = 67\}$
$A \{n = 187, e = 103\}$

a) K- de Begoña
b) Enviar LEON a Alicia
c) Firmar (resumen)
d) Verificar Firma

a) $Z = (p-1)(q-1)$
$n = p \cdot q$

323 | 17 → p
19 | 19 → q
1 |

$Z = (17-1)(19-1) = 288$

$d = \frac{288+1}{67} = 43$ Multiplicamos hasta que vamos buscando x(n)...

b) LEON → (12, 5, 16, 14)

Envío a Alicia con datos de Alicia

$C(1) = 12^{103} \bmod 187 = 97$

$C(2) = 5^{103} \bmod 187 = 110$

$C(3) = 16^{103} \bmod 187 = 44$

$C(4) = 14^{103} \bmod 187 = 118$

c) función Hash 8 bits

L 1100
E 0101
O 1110
N 10000

00 101111

SC = 00101111

$47 = H(m)$

$F = (H(m))^d \bmod n$

$47^{43} \bmod 323 = 15$

$SC + L + E + O + N = 0 \bmod 2^8 - 1$

$255 - 47 = 208$

$208^{43} \bmod 323 = 233$

d) $H(m) = F^e \bmod n$

$H(m) = 15^{67} \bmod 323 = 221$

???

$H(m) = 233^{67} \bmod 323 = 231$???