Hoja 3 ejercicio 29

ByteSub: $b = x \cdot \tilde{a} + C$ $\quad Y = x^{-1}$ $\quad C = x^6 + x^5 + x + 1$ $\quad D = x^2 + 1$

InvByteSub: $a = Y \cdot b + D$

$Yb + D = Y(x \cdot \tilde{a} + C) + D = \underbrace{Y \cdot x}_{1} \tilde{a} + \overbrace{YC + D}^{0} = \tilde{a}$

$YC = x^2 + 1 = D$ $\quad \tilde{a}^{-1} = a$

Hoja 3 ejercicio 31

ByteSub

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} \oplus \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \end{pmatrix}$$

$b_0 = a_0 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus C_0$
$b_1 = a_1 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_0 \oplus C_1$
$b_2 = a_2 \oplus a_6 \oplus a_7 \oplus a_0 \oplus a_1 \oplus C_2$
$b_3 = a_3 \oplus a_7 \oplus a_0 \oplus a_1 \oplus a_2 \oplus C_3$
$b_4 = a_4 \oplus a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus C_4$
$b_5 = a_5 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus C_5$
$b_6 = a_6 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus C_6$
$b_7 = a_7 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus C_7$

$$b_i = a_i \oplus a_{i+4} \oplus a_{i+5} \oplus a_{i+6} \oplus a_{i+7} \oplus C_i \quad \text{mod } 8$$

InvByteSub

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = \begin{pmatrix} 0&0&1&0&0&1&0&1 \\ 1&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1 \\ 1&0&1&0&0&1&0&0 \\ 0&1&0&1&0&0&1&0 \\ 0&0&1&0&1&0&0&1 \\ 1&0&0&1&0&1&0&0 \\ 0&1&0&0&1&0&1&0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \oplus \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \\ d_6 \\ d_7 \end{pmatrix}$$

$a_0 = b_2 \oplus b_5 \oplus b_7 \oplus d_0$
$a_1 = b_3 \oplus b_6 \oplus b_0 \oplus d_1$
$a_2 = b_4 \oplus b_7 \oplus b_1 \oplus d_2$
$a_3 = b_5 \oplus b_0 \oplus b_2 \oplus d_3$
$a_4 = b_6 \oplus b_1 \oplus b_3 \oplus d_4$
$a_5 = b_7 \oplus b_2 \oplus b_4 \oplus d_5$
$a_6 = b_0 \oplus b_3 \oplus b_5 \oplus d_6$
$a_7 = b_1 \oplus b_4 \oplus b_6 \oplus d_7$

$$a_i = b_{(i+2) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus d_i$$

Hoja 3 ejercicio 33

Producto de matrices estudiado en teoría

$C(x) = A(x) \cdot B(x)$

$D(x) = C(x) \bmod M(x) = A(x) \cdot B(x) \bmod M(x)$

$d_0 = (a_0 \cdot b_0) \oplus (a_3 \cdot b_1) \oplus (a_2 \cdot b_2) \oplus (a_1 \cdot b_3)$

$d_1 = (a_1 \cdot b_0) \oplus (a_0 \cdot b_1) \oplus (a_3 \cdot b_2) \oplus (a_2 \cdot b_3)$

$d_2 = (a_2 \cdot b_0) \oplus (a_1 \cdot b_1) \oplus (a_0 \cdot b_2) \oplus (a_3 \cdot b_3)$

$d_3 = (a_3 \cdot b_0) \oplus (a_2 \cdot b_2) \oplus (a_1 \cdot b_2) \oplus (a_0 \cdot b_3)$

MixColumn

La función MixColumn multiplica cada columna del state por el polinomio $03x^3 + 01x^2 + 01x + 02$, por lo que se realizarán cuatro operaciones iguales como la siguiente:

$(03x^3 + 01x^2 + 01x + 02) \cdot (C_3x^3 + C_2x^2 + C_1x + C_0) = c' = c'_6x^6 + c'_5x^5 + c'_4x^4 + c'_3x^3 + \dots$

$c'_6 = '03' \cdot C_3$

$c'_5 = '03' \cdot C_2 \oplus '01' \cdot C_3$

$c'_4 = '03' \cdot C_1 \oplus '01' \cdot C_2 \oplus '01' \cdot C_3$

$c'_3 = '03' C_0 \oplus '01' C_1 \oplus '01' C_2 \oplus '02' C_3$

$c'_2 = '01' C_0 \oplus '01' C_1 \oplus '02' C_2$

$c'_1 = '01' C_0 \oplus '02' C_1$

$c'_0 = '02' C_0$

Para hacer el módulo x^4+1, observamos que $x^i = x^{i \bmod 4} \bmod x^4+1$, por lo que

$d_0 = C_0 \oplus C_4 = ('02' b_0) \oplus ('01' '03' C_1) \oplus ('01' C_2) \oplus ('01' C_3)$

$d_1 = C_1 \oplus C_5 =$

$d_2 = C_2 \oplus C_6 =$

$d_3 = C_3 =$

c.q.d

Hoja 3 ejercicio 39

$r_0 = x^8+x^4+x^3+x+1$

$r_1 = x^7+1$

$100011011 \;|\; 10000001 \;\; 10$

100000001

11001

$r_0 = r_1(x) + (x^4+x^3+1) \rightarrow (x^4+x^3+1) = r_0 - r_1(x)$

$10000001 \;|\; 11001 \;\; 1111$

10001

10010

11001

10110

11001

11111

11001

110

$r_1 = (x^4+x^3+1)(x^3+x^2+x+1) + (x^2+x)$

$(x^2+x) = r_1 - (x^4+x^3+1)(x^3+x^2+x+1)$

$11001 \;|\; 110 \;\; 100$

110

001

$(x^4+x^3+1) = (x^2+x)(x^3)+1$

$1 = (x^4+x^3+1) - (x^2+x)(x^3)$

$110 \;|\; 1 \;\; 110$

110

001

$(x^2+x) = 1 \cdot (x^2+x) + 0$

$= (x^4+x^3+1)\left[(x^3) \cdot (r_1 - (x^4+x^3+1)(x^3+x^2+x+1))\right] =$

$= (x^4+x^3+1)(x^6+x^5+x^4+x^3) - x^3 r_1 =$

$= (r_0 - r_1(x))(x^6+x^5+x^4+x^3) - x^3 r_1 =$

$= (x^6+x^5+x^4+x^3) r_0 + (x^7+x^6+x^5+x^4+x^3) r_1 \rightarrow 11111000 = 'F8'$

$b_0 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1$

$b_1 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0$

$b_2 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$b_3 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 0$

$b_4 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$b_5 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 = 0$

$b_6 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1$

$b_7 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1$

$11000001 = 'C1'$

Hoja 3 ejercicio 40

$r_0 = x^8 + x^4 + x^3 + x + 1$

$r_1 = x^3 + 1$

$10001011 \;|\; 1001$ → 100111

$r_0 = r_1(x^5 + x^2 + x + 1) + x^2 \rightarrow x^2 = r_0 - r_1(x^5 + x^2 + x \ldots$

1110

1001

1111

1001

0110

1001

100

$1001 \;|\; 100$ → 10

$r_1 = x^2(x) + 1 \rightarrow 1 = r_1 - x^2(x)$

$100 \;|\; 01$ → 100

$x^2 = 1(x^2) + 0$

$01001110 = 4E$

$\rightarrow 1 = r_1 - x^2(x) = r_1 - \left[r_0 - r_1(x^5 + x^2 + x + 1)\right](x) = -x r_0 + (x^6 + x^3 + x^2 + x)\, r_1$

$b_0 = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 0$

$b_1 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1$

$b_2 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 1$

$b_3 = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$

$b_4 = 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1$

$b_5 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0$

$b_6 = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$b_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$1F$

Hoja 3 ejercicio 41

$r_0 = x^8 + x^4 + x^3 + x + 1$

$r_1 = '6F' = 0110\,1111 = x^6 + x^5 + x^3 + x^2 + x + 1$

$r_0 = r_1(x^2+x+1) + (x^4+x^2+x) \quad (x^4+x^2+x) = r_0 - r_1(x^2+x+1)$

$r_1 = (x^4+x^2+x)(x^2+x+1) + (x^3+x^2+1) \quad (x^3+x^2+1) = r_1 - (x^4+x^2+x)(x^2+x+1)$

$(x^4+x^2+x) = (x^3+x^2+1)(x+1) + 1$

$1 = (x^4+x^2+x) - (x^3+x+1)(x+1)$

$(x^3+x^2+1) = 1 \cdot (x^3+x^2+1) + 0$

$1 = (x^4+x^2+x) - (x^3+x+1)(x+1) = (x^4+x^2+x) - (x+1)\left(r_1 - (x^4+x^2+x)(x^2+x+1)\right) =$

$= (x^3+x^2+x+x^2+x+1)(x^4+x^2+x) - (x+1)r_1 = (x^3+1)\left(r_0 + r_1(x^2+x+1)\right) - (x+1)r_1 =$

$= (x^3+1)r_0 + (x^5+x^4+x^3+x^2)r_1 \rightarrow 0011\,1100 = '3C'$

$b_0 = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1$

$b_1 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 1$

$b_2 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0$

$b_3 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$b_4 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$

$b_5 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0$

$b_6 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0$

$b_7 = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 = 1$

$1001\,0011 = '93'$

Hoja 4 ejercicio 3

¿7^{-1} en $\mathbb{Z}_{27}$? $\varphi(27) = 3 \cdot 3 \cdot 3$ $\varphi(27) = 2 \cdot 2 \cdot 2 = 8$

$7^{8-1} \bmod 27 = 7^{7} \bmod 27 = 16 = 7^{-1}$

Hoja 4 ejercicio 4

$x = 2 \bmod 3$
$x = 3 \bmod 5$
$x = 10 \bmod 7$
$\Big\}$ $\text{mcd}(3,5,7) = 1$

$M = 3 \cdot 5 \cdot 7 = 105$
$M_1 = 5 \cdot 7 = 35$
$y_1 = 35^{-1} \bmod 3 = 2$
$M_2 = 3 \cdot 7 = 21$
$M_3 = 3 \cdot 5 = 15$
$y_2 = 21^{-1} \bmod 5 = 1$
$y_3 = 15^{-1} \bmod 7 = 1$
$C_1 = M_1 y_1 = 35$ $C_2 = M_2 y_2 = 21$ $C_3 = M_3 y_3 = 15$

$\sum_{i=1}^{3} a_i c_i \bmod M = 2 \cdot 35 + 3 \cdot 21 + 10 \cdot 15 \bmod 105 = 283 \bmod 105 = 73 \bmod 105$

Hoja 4 ejercicio 9

$p = 11$ $q = 29$ $e = 3$ $n = p \cdot q = 319$ $\varphi(n) = (p-1)(q-1) = 280$

$d = e^{-1} \bmod \varphi(n) = 3^{-1} \bmod 280 = 187$

$C = 100^{e} \bmod n = 100^{3} \bmod 319 = 1000000 \bmod 319 = 254$

~~$P = 254^{187} \bmod 319 =$~~

Hoja 4 ejercicio 11

Teoría de la hoja 102 de los apuntes.

$n = 4386607$ $\varphi(n) = 4382136$

$$p = \frac{n+1-\varphi(n) \pm \sqrt{(\varphi(n)-n-1)^2 - 4n}}{2} = \frac{4386608 - 4382136 \pm \sqrt{(4382136 - 4386606)^2 - 4 \cdot 4386607}}{2}$$

$$p = \frac{4472 \pm \sqrt{24534472}}{2} = \frac{4472 \pm 1562}{2} \begin{cases} \rightarrow p = 3016 \\ \rightarrow q = 1456 \end{cases}$$

Hoja 4 ejercicio 14

$p = 17$ $q = 19$ $n = 17 \cdot 19 = 323$ $\varphi(n) = (p-1)(q-1) = 288$

Los dos casos se encuentran en el rango $1 < e < \varphi(n)$

$\text{mcd}(288, 33) = 3 \rightarrow$ NO ES CORRECTO

$\text{mcd}(288, 35) = 1 \rightarrow$ SI ES CORRECTO

$d = e^{-1} \bmod \varphi(n) = 35^{-1} \bmod 288 = 107$

Pública (323, 35)

Privada (323, 107)

Hoja 4 ejercicio 24

$p = 561 \quad 560 = 2^4 \cdot 35 \begin{cases} k=4 \\ m=35 \end{cases} \quad a=7$

$x = a^m \bmod p = 7^{35} \bmod 561 = 241 \neq 1 \neq 560$

for $i=1$ to 3

$x = 241^2 \bmod 561 = 298 \neq 1 \neq 560$

$i=2$

$x = 298^2 \bmod 561 = 166 \neq 1 \neq 560$

$i=3$

$x = 166^2 \bmod 561 = 67 \neq 1 \neq 560$

Compuesto

Hoja 4 ejercicio 28

$n=187 \quad p=17 \quad q=11 \quad \varphi(n) = (p-1)(q-1) = 160 \quad e=7$

$d = e^{-1} \bmod \varphi(n) = 7^{-1} \bmod 160 = 23$

$C = 88^7 \bmod 187 = [88^3 \bmod 187)(88^2 \bmod 187)] \bmod 187 = 22 \cdot 77 \bmod 187 = 11$

$P = 11^{23} \bmod 187 = [(11^9 \bmod 187)(11^9 \bmod 187)(11^5 \bmod 187)] \bmod 187 =$

$= 176 \cdot 176 \cdot 44 \bmod 187 = 88$

Hoja 4 ejercicio 29

$n=77 \quad e=7 \quad d=43$

a) ¿p y q? $n-1 = e \cdot d - 1 = 300 = 2^2 \cdot 75 \begin{cases} k=2 \\ m=75 \end{cases}$

$a=3, \quad mcd(3,77) = 1$

$x = 3^{75} \bmod 77 = 34 \neq 1 \neq 76$

for $i=1$ to 1

$y = 34$

$x = 34^2 \bmod 77 = 1 \rightarrow$ "p ó $q = mcd(34+1, 77) = 7$" $\begin{cases} p=7 \\ q=11 \end{cases}$

b) Algoritmo de Las Vegas hoja 104 apuntes

c) Conocimiento del exponente de descifrado hoja 102 apuntes

d) $\varphi(n) = (p-1)(q-1) = 60$

$mcd(60, 7) = 1 \quad y \quad 1 \leq e \leq \varphi(n)$

$d = e^{-1} \bmod \varphi(n) = 7^{-1} \bmod 60 = 43$

Hoja 4 ejercicio 30

a) $p=221$, $a_1=5$, $a_2=21$

$p-1 = 220 = 2^2 \cdot 55$ → $k=2$, $m=55$

a_1:

$x = 5^{55} \bmod 221 = 112 \neq 1 \neq 220$

for $i=1$ to 1:

$x = 112^2 \bmod 221 = 168 \neq 1 \neq 220$

COMPUESTO (no se cumple ninguna propiedad)

a_2:

$x = 21^{55} \bmod 221 = 200 \neq 1 \neq 220$

for $i=1$ to 1:

$x = 200^2 \bmod 221 = 220$ → POSIBLE PRIMO

Si $(\exists i \leq k) \mid a^{2^i m} = p-1 \bmod p$

Hoja 4 ejercicio 31

$n=35$ $e=5$ $d=5$

$e \cdot d - 1 = 24 = 2^3 \cdot 3$ → $k=3$, $m=3$, $a=5$

$\gcd(35,5) = 5 \neq 1$

$p \circ q = \text{mcd} = 5$ → $p=5$, $q=7$

$x = 5^3 \bmod 35 = 20 \neq 1 \neq 34$

for $i=1$ to 2:

$y = 20$

$x = 20^2 \bmod 35 = 15 \neq 1 \neq 34$

$i=2$

$y = 15$

$x = 15^2 \bmod 35 = 15 \neq 1 \neq 34$

"$p \circ q = \text{mcd}(15+1, 35) = 1$" → $p=1$ (¿?), $q=35$ → (¿?) COMPUESTO

pasos si $\gcd(35,5) \neq 1$

Hoja 4 ejercicio 32

Claves de cifrado: $(3, 46)_{B_1}$, $(3, 51)_{B_2}$, $(3, 55)_{B_3}$ $\quad \gcd(46, 51, 55) = 1$

Mensajes cifrados: 34 31 10 Se puede aplicar teorema del resto chino

$x = 34 \bmod 46$

$x = 31 \bmod 51$

$x = 10 \bmod 55$

~~$M = 34 \cdot 31 \cdot 10 = 10540$~~ $M = 46 \cdot 51 \cdot 55 = 129030$

$M_1 = \frac{51 \cdot 55}{2805} = 2805$ $\quad M_2 = \frac{46 \cdot 55}{2530} = 2530$ $\quad M_3 = \frac{46 \cdot 51}{2346} = 2346$

$y_1 = 2805^{-1} \bmod 46 = 45$ $\quad y_2 = 2530^{-1} \bmod 51 = 28$ $\quad y_3 = 2346^{-1} \bmod 55 = 26$

$C_1 = M_1 y_1 = 126225$ $\quad C_2 = 70840$ $\quad C_3 = 60996$

$x = \sum_{i=1}^{3} C_i \bmod M = 126225 \cdot 34 + 70840 \cdot 31 + 60996 \cdot 10 \bmod 129030 = 10000 = M$