Hoja 1

5.

$y = ax + b$ en $\mathbb{Z}_m$

Para que sea un criptosistema: $\forall k_1 \exists k_2 : D_{k_2}(E_{k_1}(x)) = x$

$x = (y-b)a^{-1} \Rightarrow a$ tiene que tener inverso en $\mathbb{Z}_m$.

Por tanto, y según el algoritmo de Euclides $\boxed{mcd(a,m) = 1}$

8.

a) $a = 63 \quad b = 28$ $\quad mcd(63, 28) = 7$

$63 = 28 \cdot 2 + 7$

$28 = 7 \cdot 4 + 0$

$\boxed{7 = 63 + (-2) \cdot 28}$

$\boxed{u = 1 \quad v = -2}$

b) $a = 56 \quad b = 27$ $\quad mcd(56, 27) = 1$

$56 = 27 \cdot 2 + 2$

$27 = 2 \cdot 13 + 1$

$2 = 1 \cdot 2 + 0$

$1 = 27 + (-13) \cdot 2$

$1 = 27 + (-13)[56 + (-2)27]$

$\boxed{1 = 27 - 27 + (-13)56}$

$\boxed{u = -13 \quad v = 27}$

c) $a = 721 \quad b = 488$ $\quad \boxed{mcd(721, 488) = 1}$

$721 = 488 \cdot 1 + 233$

$488 = 233 \cdot 2 + 22$

$233 = 22 \cdot 10 + 13$

$22 = 13 \cdot 1 + 9$

$13 = 9 \cdot 1 + 4$

$9 = 4 \cdot 2 + 1$

$4 = 1 \cdot 4 + 0$

$1 = 9 + (-2) \cdot 4$

$1 = 9 + (-2)[13 + (-1)9] = 3 \cdot 9 + (-2)13$

$1 = (-2)13 + 3[22 + (-1)13] = 3 \cdot 22 + (-5)13$

$1 = 3 \cdot 22 + (-5)[233 + (-10)22] = -5 \cdot 233 + 53 \cdot 22$

$1 = -5 \cdot 233 + 53[488 + (-2) \cdot 233] = 53 \cdot 488 + (-111) \cdot 233$

$1 = 53 \cdot 488 + (-111)[721 + (-1) \cdot 488] = -111 \cdot 721 + 164 \cdot 488$

$\boxed{u = -111 \quad v = 164}$

10

a) $3x \equiv 4 \bmod 7$ $\quad \gcd(7,3) = 1 \Rightarrow 1 = 7 - 2 \cdot 3 \Rightarrow 4 = 4 \cdot 7 - 8 \cdot 3$

$\boxed{x \equiv -8 \bmod 7 \equiv 6 \bmod 7}$ $\quad 7 = 3 \cdot 2 + 1$ $\quad$ ~~$1 = 3 \cdot 7 + 12 \cdot 3$~~

b) $3x \equiv 4 \bmod 12$ no se puede

c) $ax \equiv 12 \bmod 21$ $\quad \gcd(21, a) = 3$

$\boxed{x \equiv -8 \bmod 21 \equiv 13 \bmod 21}$ $\quad 21 = a \cdot 2 + 3$ $\quad 3 = 21 - 2 \cdot a$

$a = 3 \cdot 3 + 0$ $\quad \downarrow$

$12 = 4 \cdot 21 - 8 \cdot a$

d) $27x \equiv 25 \bmod 256$ $\quad \gcd(256, 27) = 1$ $\quad 1 = 27 - 2 \cdot 13$

$\boxed{x \equiv 475 \bmod 256 \equiv 219 \bmod 256}$ $\quad 256 = 27 \cdot a + 13$ $\quad 1 = 27 - 2(256 - a \cdot 27)$

$27 = 13 \cdot 2 + 1$ $\quad 1 = -2 \cdot 256 + 19 \cdot 27$

$\downarrow$

$25 = -50 \cdot 256 + 475 \cdot 27$

11

$3 \equiv 41 \rightarrow 1203$ $\quad \mathbb{Z}_6$

$$\begin{cases} a3 + b = 1 \\ a2 + b = 2 \end{cases}$$

$\boxed{a = -1 \bmod 6 = 5 \bmod 6}$

$\boxed{b = -8 \bmod 6 = 4 \bmod 6}$

12.

1 3 23 → 0 1 2 1 en $n=2$

$$1\ 3\ 2\ 3 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0\ 1\ 2\ 1$$

$$\left| \begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix} \right| = 6 \bmod 4 = 2$$

↓

NO ✗

$a+3c=0$ $\quad 2a+3c=2$ $\quad$ a=2 $\quad$ c=-2=2

$b+3d=1$ $\quad 2b+3d=1$ $\quad$ b=0

$3d=1 \bmod 4 \Rightarrow$ d=-1=3

$1 = 4 + (-1)\cdot 3$

no forma un criptosistema en $\mathbb{Z}_4$

13.

$\mathbb{Z}_{26}$ $\quad \left| \begin{pmatrix} 11 & 7 \\ 3 & 7 \end{pmatrix} \right| = 1$ $\quad$ 1 y 26 coprimos

$$\begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix} \rightarrow \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

17.

- Criptología
  - criptomonedas
  - criptografía
    - por bloques
    - flujo

por bloques → clave pública

flujo → clave privada

20

a) $\text{mcd}(7469, 2464) = 77$

$7469 = 2464 \cdot 3 + 77$

$2464 = 77 \cdot 32 + 0$

b) $\text{mcd}(2689, 4001) = 1$

$4001 = 2689 \cdot 1 + 1312$

$2689 = 1312 \cdot 2 + 65$

$1312 = 65 \cdot 20 + 12$

$65 = 12 \cdot 5 + 5$

$12 = 5 \cdot 2 + 2$

$5 = 2 \cdot 2 + 1$

21

$31 = 7 \cdot 4 + 3$

$7 = 3 \cdot 2 + 1$

$1 = 7 + (-2)3 = 7 + (-2)[31 - 4 \cdot 7]$

$= \boxed{-2 \cdot 31 + 9 \cdot 7}$

22.

$a = 7$

$a^{-1} = 4$

$\exists a^{-1}?$

$27 = 7 \cdot 3 + 6$

$7 = 6 \cdot 1 + 1$

$1 = 7 - 1 \cdot 6 = 7 - 1[27 - 3 \cdot 7]$

$1 = -1 \cdot 27 + 4 \cdot 7$

$27 = a \cdot 3$

$a = 9$

$a^{-1} = \text{NOPE}$

23.

$e_1(x) = a_1 \cdot x + b_1$ $\quad e(x) = e_1(e_2(x))$

$e_2(x) = a_2 \cdot x + b_2$

$$e(x) = a_1[a_2 \cdot x + b_2] + b_1 = \underbrace{a_1 a_2}_{a} x + \underbrace{a_1 b_2 + b_1}_{b}$$

I+I => Pares de a_1 y a_2 en $\mathbb{Z}_m$ cuyo producto sea coprimo con m y a la vez no sean cero.

24.

$\phi(a) = a - 1$ si a primo.

$\phi(b) = b^{m-1} \cdot (b-1)$ si b factorizable

$\phi(a \cdot b) = \phi(a)\,\phi(b)$ para ambos cop

$\left[\phi(p\,q) = \phi(p)\,q(q) \pm (p-1)(q-1) = p^0(p-1) + q^0(q-1)\right)$

31

$d_{12} = 165$

$a_{23} = 70$

$d_{3n} = 40$

$d_{452} \quad 10$

$165 = 3 \cdot 5 \cdot 11$

$70 = 2 \cdot 5 \cdot 7$

$40 = 2^3 \cdot 5$

$10 = 5 \cdot 2$

$mcd = 5$

Hoja 2.

1.

x, y, z. $A_x = A_y = A_z = \{0, 1\}$

$P_x = \{p, 1-p\}$ $P_y = \{q, 1-q\}$ x e y indep

$z = x + y \mod 2$.

a) $z=0$ $x=1$ $y=1\}$ $p \cdot q$

~~$x=0$ $y=0\}$~~ $(p-1)(q-1) = pq - p - q + 1$ } $2pq - p - q + 1$

$z=1$ $x=1$ $y=0\}$ $pq - p$

$x=0$ $y=1\}$ $pq - q$ } $2pq - p - q = 1 - P_z(0)$

$\left[P_z = \{2pq - p - q + 1,\ 2pq - p - q\}\right]$

b) $P_z = \{l, 1-l\}$ $y_0 + p = l \Rightarrow y_0 = l - p$

$P_x = \{p, 1-p\}$ $y_1 + 1 - p = 1 - l \Rightarrow y_1 = p - l$

$P_x = \{y_0, y_1\} = \{l-p, p-l\}$

2.

a) $Z = x + y \quad z \in \{2, 12\}$

11	12	13	14	15	16
21	22	23	24	25	26
31	32	33	34	35	36
41	42	43	44	45	46
51	52	53	54	55	56
61	62	63	64	65	66

$P_z(2) = 1/36$

$P_z(3) = 2/36$

$P_z(4) = 3/36$

$P_z(5) = 4/36$

$P_z(6) = 5/36$

$P_z(7) = 6/36$

$P_z(8) = 5/36$

$P_z(9) = 4/36$

$P_z(10) = 3/36$

$P_z(11) = 2/36$

$P_z(12) = 1/36$

b) $Z = |x - y| \quad z \in \{0, 5\}$

$P_z(0) = 6/36$

$P_z(1) = 10/36$

$P_z(2) = 8/36$

$P_z(3) = 6/36$

$P_z(4) = 4/36$

$P_z(5) = 2/36$

3.

$P = \{0,1\}$

$K = \{00, 01, 10, 11\}$

$C = \{00, 01, 10, 11\}$

k	P=0	P=1
00	00	01
01	10	11
10	01	00
11	11	10

$P_K(x) \Rightarrow P_K(0) = P_K(1) = 0,5 \qquad P_K(k_i) = 0,25$

¿ $P_C(x) = P_C(x|y)$?

$P_C(y)$

$P_C(00) = (0,25 \cdot 0,5) 2 = 0,25$

$P_C(01) = (0,25 \cdot 0,5) 2 = 0,25$

$P_C(10) = (0,25 \cdot 0,5) 2 = 0,25$

$P_C(11) = (0,25 \cdot 0,5) \cdot 2 = 0,25$

$P(y|x)$

$P_C(00|0) = 0,25 \quad P_C(10|0) = 0,25$

$P_C(00|1) = 0,25 \quad P_C(10|1) = 0,25$

$P_C(01|0) = 0,25 \quad P_C(11|0) = 0,25$

$P_C(01|1) = 0,25 \quad P_C(11|0) = 0,25$

$P(x|y) = \frac{P(x)}{P(y)} \cdot P(y|x)$

$P(0|00) = 0,5 = P(0)$

$P(1|00) = 0,5 = P(1)$

$P(0|01) = 0,5 = P(0)$

$P(1|01) = 0,5 = P(1)$

$P(0|10) = 0,5 = P(0)$

$P(1|10) = 0,5 = P(1)$

$P(0|11) = 0,5 = P(0)$

$P(1|11) = 0,5 = P(1)$

SÍ

¿ Dot. unicidad?

$|C| \neq |P|$

$$\ell_0 = \frac{\log_2(|K|)}{\log_2|C| + (1-P_L)\log_2|P|} = \frac{\log_2(2^2)}{\log_2(2^2) \to 0} = 1$$

$$P_L = 1 - \frac{H_L}{\log_2|P|} = 1 - \frac{1}{\log_2 2} = 0$$

$$H_L = \sum_{i=1}^{2} P(x_i) \log_2\left(\frac{1}{P(x_i)}\right) = 2 \cdot \left[0,5 \cdot \log_2 \frac{1}{0,5}\right] = 1$$

4.

$P = \{a, b\}$ $K = \{k_1, k_2, k_3\}$ $C = \{1, 2, 3\}$

k	a	b
k_1	1	2
k_2	1	3
k_3	3	2

$P(K = k_1) = P(K = k_2) = 1/4$ $P(K = k_3) = 1/2$

$P(P = a) = 1/3$ $P(P = b) = 2/3$

¿ $P(x|y)$?

a) $P_2(y)$

$P_2(1) = P_K(k_1) P_P(a) + P_K(k_2) P_P(a) = 1/3 \left[\frac{1}{2}\right] = \boxed{1/6}$

$P_2(2) = P_K(k_1) P_P(b) + P_K(k_3) \cdot P_P(b) = 2/3 \, [3/4] = 6/12 = \boxed{1/2}$

$P_2(3) = P_K(k_2) P_P(a) + P_K(k_2) P_P(b) = 1/3 \cdot 1/2 + 2/3 \cdot 1/4 = \boxed{1/3}$

$P_2(y|x)$

$P_2(1|a) = 1/2$

$P_2(1|b) = 0$

$P_2(2|a) = 0$

$P_2(2|b) = 3/4$

$P_2(3|a) = 1/2$

$P_2(3|b) = 1/4$

$P_P(x|y)$

$P_P(a|1) \; P_P(a|1) = 1/2 \cdot \frac{1/3}{1/6} = 1$

$P_P(b|1) \; P_P(a|2) = 1/2 \cdot \frac{1/3}{1/2} = 0$

$P_P(a|2) \; P_P(a|3) = 1/2 \cdot \frac{1/3}{1/3} = 1/2$

$P_P(b|2) \; P_P(b|1) =$

$P_2(a|a) \; P_P(b|2) =$

$P_P(b|3) =$

$P_P(b|1) = 0 \cdot \frac{2/3}{1/6} = 0$

$P_P(b|2) = 3/4 \cdot \frac{1/3}{1/2} = 1$

$P_P(b|3) = 1/4 \cdot \frac{2/3}{1/3} = \frac{1}{2}$

5.

1	2	3
3	1	2
2	3	1

$e_i(1) = L_{i1}$

No hay repes en filas ni columnas $\Rightarrow \left[\forall x \in P, \forall y \in C \quad \exists! k \in K : e_k(x) = y\right]$

Sí. Tiene seg perfecta

10.

$P = \{0,1\}$ $P_P(0) = 1/3$ $P_P(1) = 2/3$

$K = \{00, 01, 10, 11\}$ $P_K(00) = P_K(01) = P_K(10) = 1/5$ $P_K(11) = 2/5$

K \ P	P=0	P=1
00	00	01
01	10	11
10	01	00
11	11	10

al explicar teorema y $P_D(x|y) = P(x)$

01 $P_C(y)$

$P_C(00) = \frac{1}{3} \cdot 1/5 + 2/3 \cdot 1/5 = 1/5$

$P_C(01) = 1/3 \cdot 1/5 + 2/3 \cdot 1/5 = 1/5$

$P_C(10) = 1/3 \cdot 1/5 + 2/3 \cdot 2/5 = 1/3$

$P_C(11) = 1/3 \cdot 2/5 + 2/3 \cdot 1/5 = 4/15$

$P_C(y|x)$

$P_C(00|0) = 1/5$

$P_C(00|1) = 1/5$

$P_C(01|0) = 1/5$

$P_C(01|1) = 1/5$

$P_C(10|0) = 1/5$

$P_C(10|1) = 2/5$

$P_C(11|0) = 2/3$

$P_C(11|1) = 1/5$

$P_D(x|y)$

$P(0|00) = 1/3 \cdot \frac{1/3}{1/5} = 1/3 = P(0)$

$P(1|00) = 1/5 \cdot \frac{2/3}{1/5} = 2/3 = P(1)$

$P(0|01) = 1/5 \cdot \frac{1/3}{1/5} = 1/3 = P(0)$

$P(1|01) = 1/5 \cdot \frac{2/3}{1/5} = 2/3 = P(1)$

$P(0|10) = 1/5 \cdot \frac{1/3}{1/3} = 1/3 = P(0)$

$P(1|10) = 1/5 \cdot \frac{2/3}{2/3} = 2/5 = P(1)$

$P(0|11) = 1/5 \cdot \frac{1/3}{4/5} = 1/12 \neq P(0)$

$P(1|11) = 1/5 \cdot \frac{2/3}{4/5} = 2/12 \neq P(1)$

c) ~~$n_0 = \log_2 2$~~ $H_X = \sum_{i=1}^{n} P_X(x_i) \log_2\left(\frac{1}{P_X(x_i)}\right) = 2/3 \cdot \log_2 3 + 2/3 \cdot \log_2(3/2) = 0{,}91829$

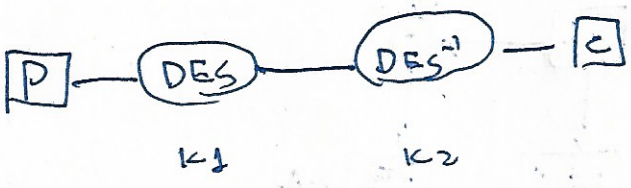
$$R_L = 1 - \frac{H_L}{\log_2 D} = 1 - \frac{0{,}91829}{\log_2(2)} = 0{,}08170$$

$$n_0 = \frac{\log_2 K}{\log_2(2) + (1-R_L)\log_2 P} = \frac{2}{2 + 0{,}91829} = \boxed{0.68533}$$

Hoja 3

(3) Menor tiempo de ejecución, ya que permite preprocesar el DES aplicado al contador. Por tanto, solo requiere el xor con el bloque.

(6)



cifras no p posibles con todas las k1 posibles

cifras no < ~~posibles~~ con todas las k2 posibles

Checkeas coincidencias y pruebas.

(7)

$[L_1' = R_0' = R_{n+1} = L_n = R_{n-1}]$

$[R_1' = L_{n+1} \oplus F(R_0', k_n) = R_n \oplus F(R_{n-1}, k_n) =$

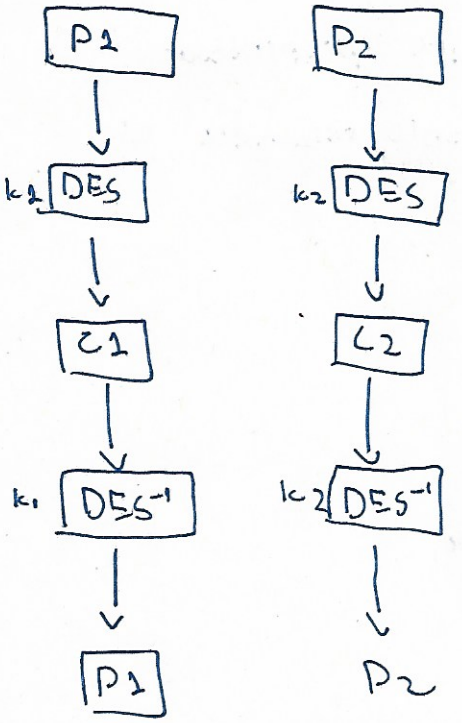
$= L_{n-1} \oplus F(R_{n-1}, k_n) \oplus F(R_{n-1}, k_n) = L_{n-1}]$

(8)

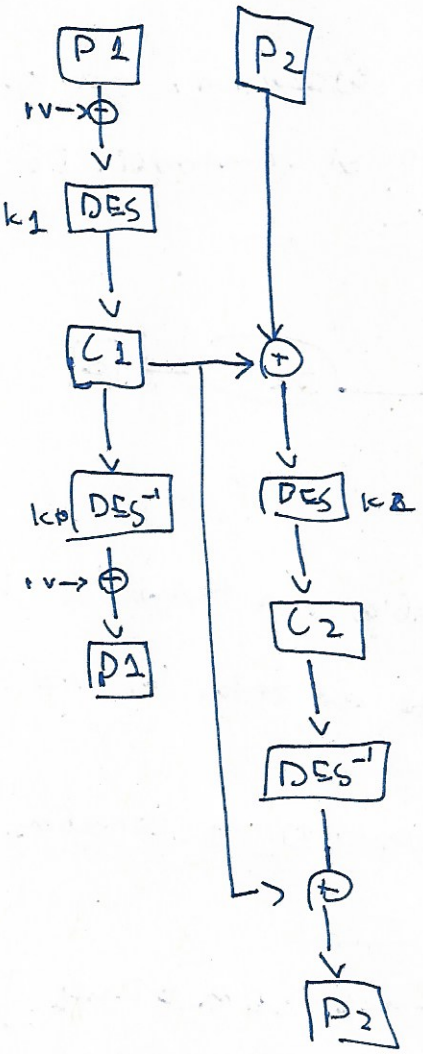
(NO) La $\exists$ de claves semidébiles no permiten cumplir que $[\forall x \in P, y \in C, \exists! k \in K : E_k(x) = y]$. Esto forma parte del teorema de seguridad perfecta.

10

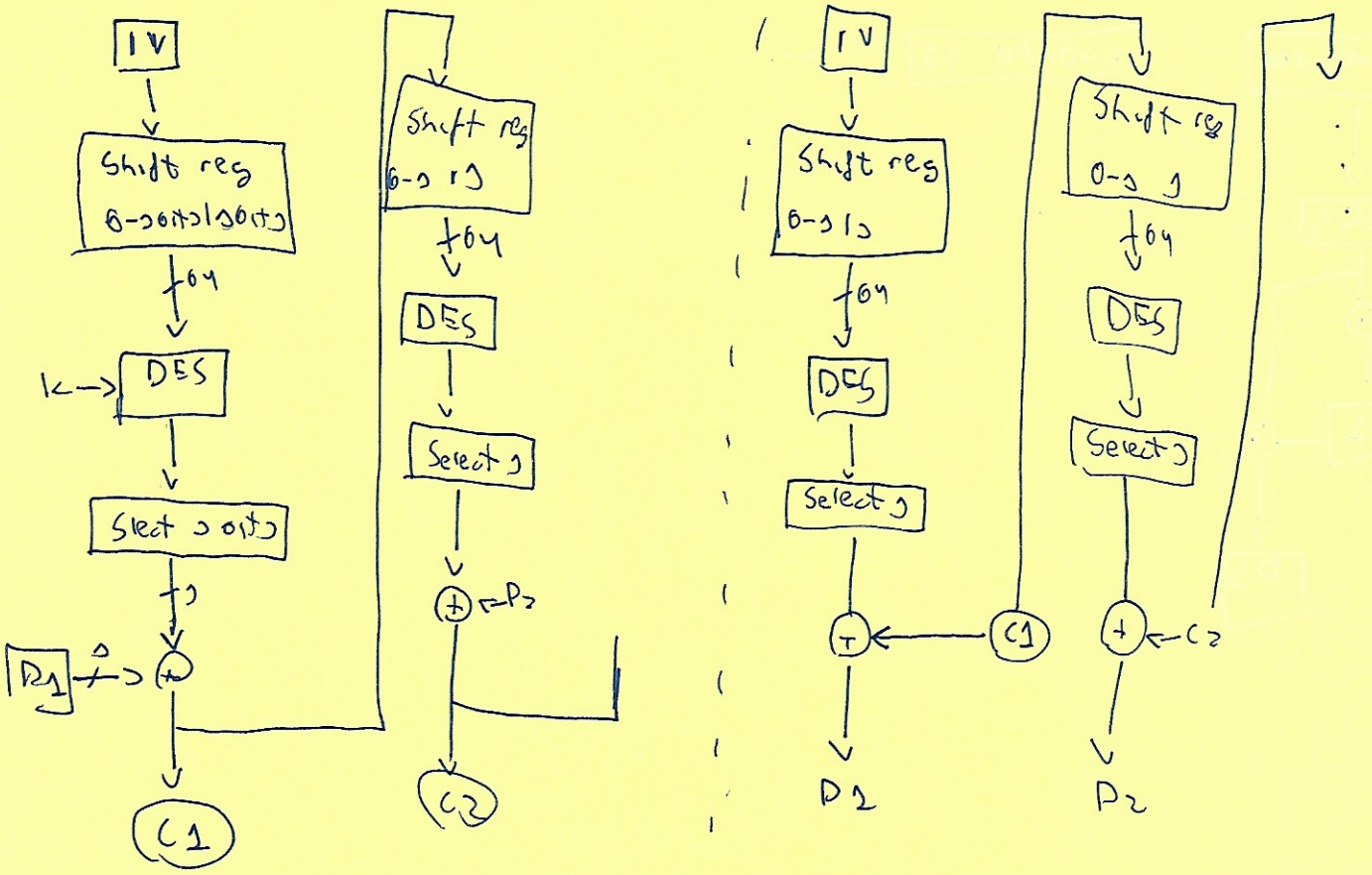
ECB


P1
k1
DES
C1
k1
DES⁻¹
P1
P2
k2
DES
C2
k2
DES⁻¹
P2

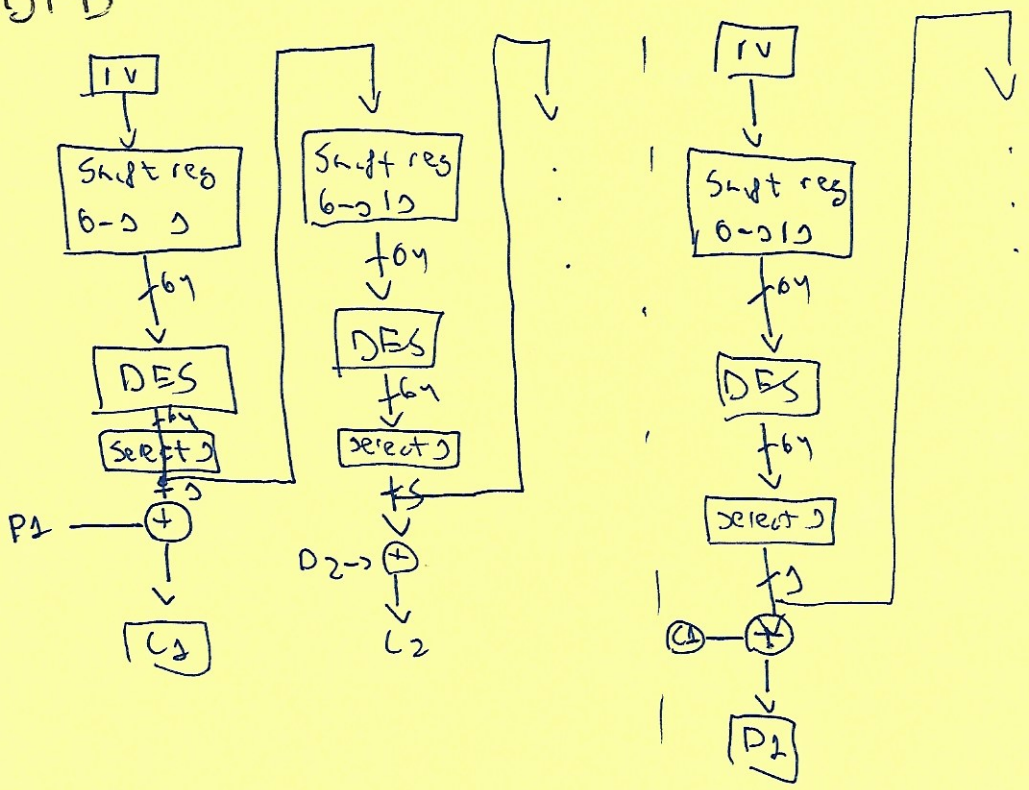
CBC


P1
+V
k1
DES
C1
k1
DES⁻¹
+V
P1
P2
+
DES
k2
C2
DES⁻¹
+
P2

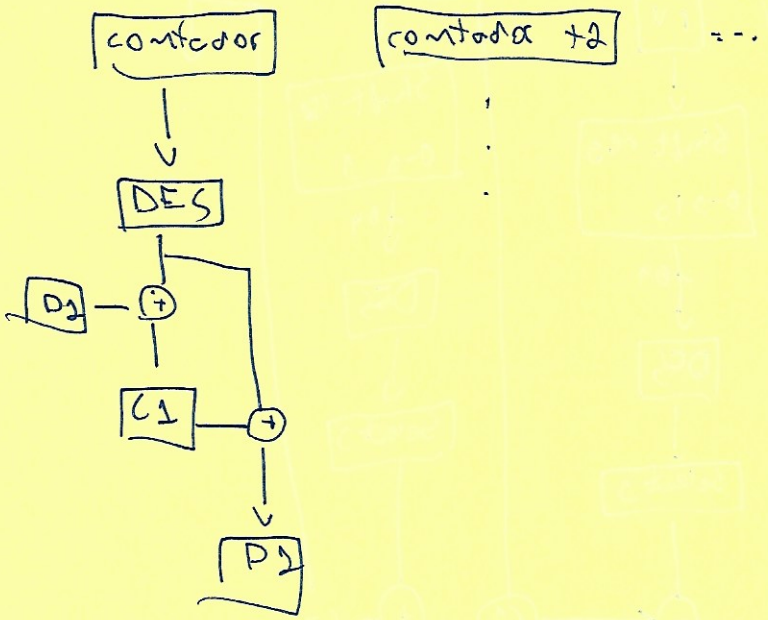
CFB


IV
Shift reg
DES
Select
P1
P2
C1
C2
D1
D2

OFB


IV
Shift reg
DES
Select
P1
P2
C1
C2
D1
D2

C+R



1 1

a) Al cifrar

-> $DES^{-1}_{k}(E_k(k)) = x$

Entonces

$DES^{-1}_{k2}(E_{k2}(E_{k1}(PT))) = E_{k1}(PT)$

$DES^{-1}_{k1}(E_{k1}(PT)) = PT$

} ↓ orden inverso de cifrado

b) $S_1(111111) = 13$

↳ fila: 11
↳ col: 1111

$S_2(00\,0000) = 14$

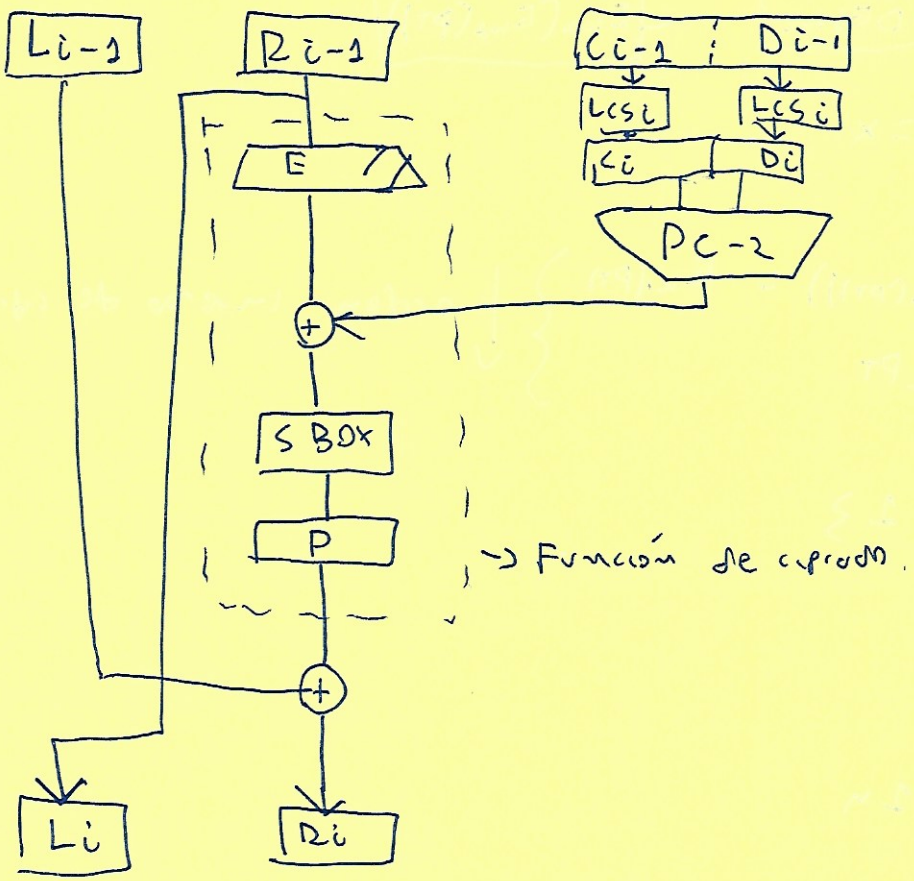
↳ fila: 00
↳ col: 0000

$S_3(100001) = 15$

↳ fila: 11
↳ col: 0000

12.

a) La forma más sencilla es viendo el esquema de una ronda de cifrado



→ Función de cifrado.

→ Partiendo que Pt (Li-1 y Ri-1) están mezclados y la clave también.

→ Sabemos que la sustitución de la SBox es igual y, por tanto, el resultado del cifrado ($\bar{A} \oplus \bar{B} = A \oplus B$)

→ Li-1 SÍ que está mezclado

→ Ri-1 igual, pero en la función se invierte con el ⊕.

→ $Li = \overline{Ri-1}$ y $Ri = \overline{Li-1} \oplus$ cifrado

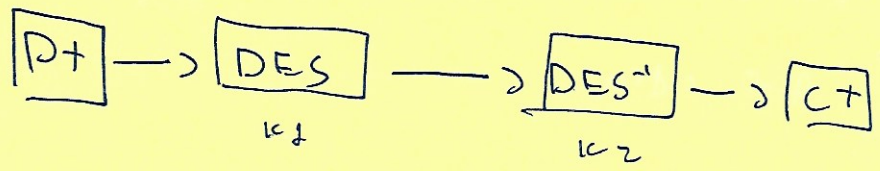
Si no están invertidos

$Li = Ri-1$ y $Ri = Li-1 \oplus$ Cifrado

$E_{\bar{K}}(\bar{P_T}) = E_K(P_T)$

$E_K(P_T) \oplus E_{\bar{K}}(\bar{P_T}) = 0$

6)



consiste en aplicar DES al texto plano y al cifrado. Una vez lo hemos hecho con todas las claves posibles buscamos coincidencias para obtener las claves.

-> $2 \cdot 2^{56}$ veces DES

-> $2^{56} \cdot 2^{56}$ comparaciones, aunque es descifrable.

13.

a) - No linealidad $f(x \oplus \Delta x) \neq f(x) \oplus f(\Delta x)$

- Un cambio en un bit de entrada produce cambio en la salida con prob 1/2

- El cambio en la salida entre 2 bits es indep. cuando uno de la entrada es invertido.

b) nuevo: $S[i,j] = c_2$

1º: Invertir el valor en GF(28)

2º: $(S[i,j]^{-1}) \cdot \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$

invertir: $\bar{a}_{ij} = Y_{ij} \oplus d \quad Y = \begin{pmatrix} 0 & 0 & 1 & 0 & \cdots \\ \cdots & & & & \end{pmatrix}$

$a_{ij} = (\bar{a}_{ij})^{-1}$

$d = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

c) Porque DES utiliza el cifrado de Feistel que descifra "igual" que cifra.

21.

$r_0 = x^3 + x + 1$

$r_1 = x^2$

$r_2 = x + 1$

$r_3 = 1$

1 0 1 1 | r00
1 0 0 | 10
0 0 1 1

$x + 1 = x^3 + x + 1 - x^2 (x)$
r0 r1

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

1 0 0 | 11
1 1 | 11
1 0
1 1
1
(1)

~~$1 = x^2 - (x+1)$~~

$1 = r_1 - (x+1)[r_0 - x \cdot r_1] =$

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

$[x^2]^{-1} = x^2 + x + 1$

22.

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

$r_1 = x^7 + 1$

$r_2 = x^4 + x^3 + 1$

$r_3 = x^2 + x$

$r_4 = 1$

1 0 0 0 1 1 0 1 1 | 10000001
1 0 0 0 0 0 0 1 | 10
0 0 0 0 1 1 0 0 1

$x^4 + x^3 + 1 = r_0 - x\, r_1$

1 0 0 0 0 0 0 1 | 11001
1 1 0 0 1 | 1111
0 1 0 0 1 0
1 1 0 0 1
2 0 1 2 0
1 1 0 0 1
1 2 1 2 1 2
1 1 0 0 1
r0

$\hookrightarrow x^2 + x = r_1 - (x^3 + x^2 + x + 1)(r$

23.

$(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) =$

$= x^{13} + x^7 + x^6 + x^4 + x^5 + x^4 + x^3 + x^3 + x^2 + x^8 + x^2 + x + x + 1 =$

$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$

1 0 1 0 1 1 0 1 1 1 1 | 0 0 1 | 1 0 0 0 1 1 0 1 1

1 0 0 0 1 1 0 1 1 | 2 0 1 0 0 0

0 0 1 0 0 0 0 0 1 1

1 0 0 0 1 1 0 1 1

0 0 0 0 1 1 0 0 0 0 0 1

$x^7 + x^6 + 1$

25.

'23' . '81'

↳ 0000 0011

'81' . '01' = '81'

'81' . '02' = L('81') ⊕ '1B' = '19'

'81' . '04' = L('19') = '32'

'81' . '08' = L('32') = '64'

'81' . '10' = L('64') = '08'

'81' . '20' = L('08') ⊕ '1B' = '1A'

'81' . '01' ⊕ '81' . '02' ⊕ '81' . '20' = '33'

33.

$02x^3 + 01x^2 + 01x + 02$ por las columnas

$$\begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} 02 & 01 & 01 & 02 \\ 02 & 02 & 01 & 01 \\ 01 & 02 & 02 & 01 \\ 01 & 01 & 02 & 02 \end{pmatrix}$$

↳ $a_{00} \cdot 02x^3 + a_{10} \cdot 01x^2 + a_{20} \cdot 01x^1 + a_{30} \cdot 02$

34.

ShiftRow es un desplazamiento y SubBytes es obtener el valor de la SBox. Da igual que hagamos primero, ya que el final es igual.

SubBytes => Cada casilla es sustituida

ShiftRows => desplazamiento

Da igual reemplazar y desplazar que desplazar y reemplazar.

39.

$(1\,000\,0001) \Rightarrow$ no invertido.

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

$r_1 = x^7 + 1$

$r_2 = x^4 + x^3 + 1$

$r_3 = x^2 + x$

$r_4 = 1$

$100011011 \;|\; 10000001$

$10000000 \;|\; 10$

$\downarrow x$

$10000001 \;|\; 11001$

$11001 \;|\; 1111$

$\downarrow$

$x^3 + x^2 + x + 1$

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

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

$= -x^2 r_1 + (x^5 + x^4 + x^3 + x^2 + 1)(x^4 + x^3 + 1) =$

$= -x^2 r_1 + (x^5 + x^4 + x^3 + x^2 + 1)[r_0 - x\, r_1] =$

$= -(x^6 + x^5 + x^4 + x^3 + x^2 + x)\, r_2 + (x^3 + x^4 + x^3 + x^2 + 1)\, r_0$

$11001 \;|\; 1110$

100

$(1000\,0001)^{-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x = (0111\,1110)$

$$\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} 0 \\ - \\ - \\ - \\ - \\ - \\ - \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ - \\ - \\ - \\ - \\ - \\ - \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ - \\ - \\ - \\ - \\ - \\ - \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ - \\ - \\ 0 \\ 0 \\ - \\ - \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ - \\ - \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = (60)$$

40.

'0a'

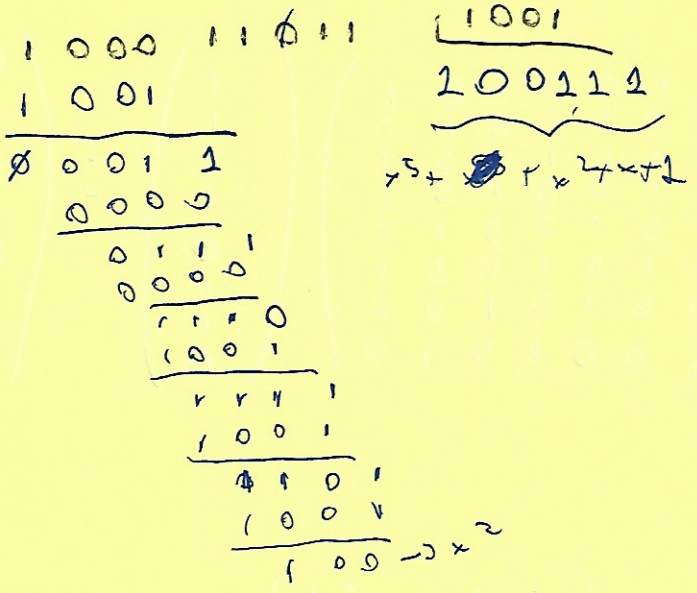
$('0a')^{-1} = ?$

$r_0 = x^7 + x^4 + x^3 + x + 1$

$r_1 = x^3 + 1$

$r_2 = x^2$

$r_3 = 1$



$1 = r_1 - x \cdot r_2 =$

$= r_1 - x\left[r_0 - (x^5 + x^2 + x + 1) \cdot r_1\right] =$

$= -x r_0 + (x^6 + x^3 + x^2 + x + 1)\, r_1$

$M \cdot \begin{pmatrix} 1 \\ - \\ - \\ - \\ - \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ - \\ 0 \\ 0 \\ - \\ - \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ - \\ 0 \\ 0 \\ 0 \\ - \\ - \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ - \\ - \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$= 01$

n2

[6F]

$$\begin{pmatrix} 0&0&1&0&0&1&0&1\\ 1&0&0&1&0&0&1&0\\ 0&1&0&0&1&0&0&1\\ 1&0&1&0&0&1&0&0\\ 0&1&0&1&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&1&0&1&0 \end{pmatrix} \begin{pmatrix} 1\\1\\1\\1\\0\\1\\0\\0 \end{pmatrix} = \begin{pmatrix} 0\\1\\1\\1\\1\\1\\1\\0 \end{pmatrix}$$

$$\begin{pmatrix} 0\\ \vdots \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix} = \begin{pmatrix} 1\\0\\ \vdots \\0 \end{pmatrix} = {}'7\,B'$$

$('7B')^{-1} =$

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

$r_1 = x^6 + x^3 + x^4 + x^3 + x^2 + 1$

$r_2 = x^4 + x^2 + 1$

$r_3 = x + 1$

$r = 1$

$1 = r_2 - (x^2+x)\, r_3 =$

$= r_2 - (x^2+x)\left[r_1 - (x^2+x)\, r_2\right] =$

$= -(x^2+x)\, r_1 + (x^4+x^2)\, r_2 =$

$= -(x^2+x)\, r_1 + (x^4+x^2)\left[r_0 - (x^2+x)\, r_1\right] =$

$= -(x^6+x^4+x^5+x^3+x^2+x)\, r_0 + (x^4+x^2)\, r_0$

Hoja 4.

1. $3^{301} \mod 11$ $\quad \varphi(11)=10$ y 11 primo $\Rightarrow \boxed{3^{10} \mod 11 = 1}$

$3^{300} \cdot 3 \mod 11 \Rightarrow (3^{10})^2 \cdot 3 \mod 11 \Rightarrow 3^4 \mod 11 \Rightarrow$

$\Rightarrow 81 \mod 11 \Rightarrow \boxed{81 \equiv 4 \mod 11} \Rightarrow \boxed{3^{301} \equiv 4 \mod 11}$

2.

$5^{506} \mod 1234$ $\quad 1234 = \boxed{2 \cdot 617}$ $\quad \boxed{\varphi(1234) = 616}$

$5^{616} \mod 1234 \equiv 1 \mod 1234$

3.

7^{-1} en $\mathbb{Z}_{27}$ $\quad \varphi(27) = 3^3 - 3^2 = 18$

$7^{18} \mod 27 = 1 \Rightarrow 7 \cdot 7^{17} \mod 27 = 1$

$7^{-1} \equiv 7^{17} \mod 27$

$7^{10} \cdot 7^7 \mod 27 \Rightarrow 7 \cdot 9 \mod 27$

$\downarrow$

$\boxed{4 \mod 27}$

4

① $x \equiv 2 \bmod 3$

② $x \equiv 2 \bmod 5$

③ $x \equiv 2 \bmod 7$

$M = 5 \cdot 3 \cdot 7$

① $M_1 = 5 \cdot 7 = 35$

$a_1 = 2$

$y_1 = 35^{-1} \bmod 3$

$2^{-1} \bmod 3$

↳ ②

$35 = 3 \cdot 11 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (35 - 11 \cdot 3)$

$= -1 \cdot 35 + 12 \cdot 3$

$c_1 = 35 \cdot 2$

② $M_2 = 3 \cdot 7 = 21$ $\quad c_2 = 21 \cdot 1$

$a_2 = 2$

$y_2 = 21^{-1} \bmod 5 \quad 1^{-1} \bmod 5 = 1$

③ $M_3 = 5 \cdot 3 = 15$ $\quad c_3 = 15 \cdot 1$

$a_3 = 2$

$y_3 = 15^{-1} \bmod 7 = 1^{-1} \bmod 7 = 1$

$x \equiv (35 \cdot 2 \cdot 2) + (21 \cdot 1 \cdot 2) + (15 \cdot 1 \cdot 2) \bmod 105 \equiv 212 \bmod 105 = \boxed{2 \bmod}$

3.

$x \equiv 5 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 10 \bmod 7$

$M = 7 \cdot 5 \cdot 3 = 105$

① $M_1 = 7 \cdot 5 = 35$

$y_1 = 35^{-1} \bmod 3 = 2^{-1} \bmod 3 = \boxed{2 \bmod 3}$

$C_1 = 35 \cdot 2$

$a_1 = 2$

② $M_2 = 7 \cdot 3 = 21$

$y_2 = 21^{-1} \bmod 5 = 1^{-1} \bmod 5 = 1 \bmod 5$

$C_2 = 21 \cdot 1$

$a_2 = 3$

③ $M_3 = 3 \cdot 5 = 15$

$y_3 = 15^{-1} \bmod 7 = 1 \bmod 7$

$C_3 = 15 \cdot 1$

$a_3 = 10$

$x = (35 \cdot 2 \cdot 2) + (21 \cdot 1 \cdot 3) + (15 \cdot 1 \cdot 10) \bmod 105 \Rightarrow \boxed{38 \bmod 105}$

6.

$x \equiv 3^n \bmod n6$

$x \equiv 31 \bmod 51$

$x \equiv 10 \bmod 55$

$M = n6 \cdot 31 \cdot 55$

(1) $M_1 = 51 \cdot 55 = 2805$

$y_1 = 2805^{-1} \bmod n6 = n5^{-1} \bmod n6 = n5 \bmod n6$

$C_1 = 2805 \cdot 1$

$a_1 = 3^n$

(2) $M_2 = 55 \cdot n6 = 2530$

$y_2 = 2530^{-1} \bmod 51 = 31^{-1} \bmod 51 = -23 \bmod 51$

$-23 \bmod 51 = 28$

$C_2 = 28 \cdot 2530$

$a_2 = 31$

(3) $M_3 = n6 \cdot 51 = 23n6$

$y_3 = 10^{-1} \cdot 23n6^{-1} \bmod 55 = 36^{-1} \bmod 55$

$C_3 = M_2 \cdot y_3 = 23n6 \cdot 26$

$26 \bmod 55$

$a_3 = 10$

$51 = 31 \cdot 1 + 20$

$31 = 20 \cdot 1 + 11$

$20 = 11 \cdot 1 + 9$

$11 = 9 \cdot 1 + 2$

$9 = 2 \cdot 4 + 1$

$1 = 9 - 4 \cdot 2 = 9 - 4[11 - 1 \cdot 9] =$

$= -4 \cdot 11 + 5 \cdot 9 = -4 \cdot 11 + 5[20 - 1 \cdot 11] =$

$= 5 \cdot 20 - 9 \cdot 11 = 5 \cdot 20 - 9[31 - 1 \cdot 20] =$

$= -9 \cdot 31 + 14 \cdot 20 = -9 \cdot 31 + 14[51 - 1 \cdot 31] =$

$= 14 \cdot 51 - 23 \cdot 31$

$55 = 36 \cdot 1 + 19$

$36 = 19 \cdot 1 + 17$

$19 = 17 \cdot 1 + 2$

$17 = 2 \cdot 8 + 1$

$1 = 17 - 8 \cdot 2 = 17 - 8[19 - 1 \cdot 17] =$

$= -8 \cdot 19 + 9 \cdot 17 = -8 \cdot 19 + 9[36 - 1 \cdot 19] =$

$= 9 \cdot 36 - 17 \cdot 19 = 9 \cdot 36 - 17[55 - 1 \cdot 36] =$

$= 26 \cdot 36 - 17 \cdot 55$

$x = (2805 \cdot 3n) + (2530 \cdot 28 \cdot 31) + (23n6 \cdot 26 \cdot 10)$

$= 2401370 \bmod 129030 =$

$\Rightarrow \boxed{x = 82710 \bmod 129030}$

8.

$n = 35$ $\quad \varphi(n) = 6 \cdot 4 = 24$ $\quad [d = 5^{-1} \bmod 24 = 5]$

$e = 5$

$[10^5 \bmod 35 = 5] \Rightarrow$ descifrado.

9.

$p = 11$ $\quad n = 29 \cdot 11 \quad \varphi(n) = 28 \cdot 10 = 280$

$q = 29$

$e = 3$ $\quad d = 3^{-1} \bmod 280 \qquad 280 = 3 \cdot 93 + 1$

$= -93 \bmod 280$ $\qquad 1 = 280 - 93 \cdot 3$

$= 187 \bmod 280$

$\Rightarrow (d = 187)$

$100^e \bmod n = 100^3 \bmod 319 \Rightarrow (254)$

10.

$p = 17$ $\quad n = 17 \cdot 11 = 187$

$q = 11$ $\quad \varphi(n) = 160$

$e = 7$ $\quad d = 7^{-1} \bmod 160 = 23$

$160 = 22 \cdot 7 + 6$

$7 = 6 \cdot 1 + 1$

$1 = 7 - 1 \cdot 6 = 7 - 1 \cdot [160 - 22 \cdot 7] =$

$= 23 \cdot 7 + (-1) \cdot 160$

$E_K(M) = 88^7 \bmod 187 = 20$

$= 88 \cdot 77 \cdot 77 \cdot 77 \bmod 187 = (11)$

$D_K(11) = 11^{23} \bmod 187 =$

$= 11^3 \cdot (11^2)^{10} \bmod 187 = 11^3 \cdot 55^{10} \bmod 187 =$

$= 22 \cdot 33^5 \bmod 187 = 22 \cdot 33 \bmod 187 =$

$7 = 2^2 + 2^1 + 2^0$

$88^7 \bmod 187 = (88^2)^2 \cdot 88^2 \cdot 88 \bmod 187 = 77^2 \cdot 77 \cdot 88 \bmod 187 =$

$= 132 \cdot 77 \cdot 88 \bmod 187 = (11)$

$23 = 2^4 + 2^2 + 2^1 + 2^0$

$11^{23} \bmod 187 = (11^2)^{\frac{23}{2}} \cdot ((11)^2)^2 \cdot 11^2 \cdot 11 = ((121)^2)^2 \cdot 121^2 \cdot 121 \cdot 11 \bmod 187 =$

$= ((55)^2)^2 \cdot 55 \cdot 121 \cdot 11 \bmod 187 = 33^2 \cdot 55 \cdot 121 \cdot 11 \bmod 187 = 154 \cdot 55 \cdot 121 \cdot 11 \bmod$

$= \boxed{88}$

12

$n = pq$

$\phi = (p-1)(q-1) = pq - p - q + 1 = n - p - \frac{n}{p} + 1 = \phi \Rightarrow$

$\Rightarrow np - p^2 - n + p = \phi\, p \Rightarrow p^2 + (\phi - n - 1)p + n = 0$

$p = \frac{n+2 \pm \sqrt{2n-52356}}{2} = \frac{n+2 \pm 158}{2} = \begin{cases} pq = 306 \\ p+q = n+6 \end{cases}$

13.

$n = 35qq \Rightarrow 5q \cdot 61 \qquad \phi(n) = 3480$

$e = 31$

$d = 31^{-1} \bmod 3480 = \cancel{-13 \bmod 3480 = 3467}$

$\boxed{1451}$

$3480 = 111 \cdot 31 + 19$

$31 = 1q \cdot 1 + 12$

$1q = 12 \cdot 1 + 7$

$12 = 7 \cdot 1 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2 = 5 - 2[7 - 1 \cdot 5] = 0 - 2 \cdot 7 + 3 \cdot 5 =$

$= -2 \cdot 7 + 3[12 - 1 \cdot 7] = 3 \cdot 12 - 5 \cdot 7 = 3 \cdot 12 - 5[1q - 1 \cdot 12]$

$= -5 \cdot 1q + 8 \cdot 12 = -5 \cdot 1q + 8 \cdot [31 - 1 \cdot 1q] =$

$= 8 \cdot 31 - 13 \cdot 1q = 8 \cdot 31 - 13[3480 - 111 \cdot 31] =$

$= 1451 \cdot 31 - 13 \cdot 3480$

14.

$p = 17$

$q = 19$

$n = 17 \cdot 19$ $\quad \phi(n) = 16 \cdot 18 = 288$

e ~~=~~ 33 válido? $\Rightarrow$ ¿inversa en $\mathbb{Z}_{\phi(n)}$?

$33^{-1} \bmod 288$

$288 = 33 \cdot 8 + 24$

$33 = 24 \cdot 1 + 9$

$24 = 9 \cdot 2 + 6$

$9 = 6 \cdot 1 + 3 \Rightarrow$ (ND) $\quad$ e = 33 no sirve

$35^{-1} \bmod 288 = (107) \Rightarrow$ (d)

$288 = 35 \cdot 8 + 8$

$35 = 8 \cdot 4 + 3$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 2$

$1 = 3 - 1 \cdot 2 = 3 - 1 [8 - 2 \cdot 3] = -1 \cdot 8 + 3 \cdot 3 =$

$= -1 \cdot 8 + 3 \cdot [35 - 4 \cdot 8] = 3 \cdot 35 - 13 \cdot 8 =$

$= 3 \cdot 35 - 13 [288 - 8 \cdot 35] = 13 \cdot 288 + (107) \cdot 35$

17, 18 y 19 y 20

1 -> Pequeño teorema de fermat (18)

siendo p primo.

1) x e $y \in \mathbb{Z}_p^*$ $x = y$ $ax \neq ay$ si $a \in \mathbb{Z}_p^*$ (multiplicar por a^{-1} para demostrar)

2) $\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} ai$ (por ①).

$$\prod_{i=1}^{p-1} i = a^{p-1} \prod_{i=1}^{p-1} i \Rightarrow \boxed{a^{p-1} \equiv 1 \bmod p \text{ con } p \text{ primo}}$$

2 -> Euler generalizado (19)

Generalización de P.T Fermat.

(∀ D)

$$\prod_{\text{para } i=1}^{\phi(p)} i = \prod_{\text{SGPI } i=1}^{\phi(p)} ai \Rightarrow \boxed{a^{\phi(p)} \equiv 1 \bmod p}$$ igual que el anterior.

3 -> RSA e inyectividad

P y q primos $\Rightarrow n = p \cdot q$

$\phi(n) = (p-1)(q-1)$

~~e primo~~ (17)

$$\begin{cases} 1 < e < n \\ \text{mcd}(e, n) = 1 \end{cases}$$

$\{ d$ t.q $ed \equiv 1 \bmod \phi(n)$

↳ Expect. ed. $\{a^{ed} \equiv a \bmod n\}$ $ed \equiv 1 \bmod \varphi(n)$

+ Caso 1 $a \in \mathbb{Z}_n^*$

$ed \equiv 1 \bmod \varphi(n) \Rightarrow ed = 1 + k\varphi(n)$

Euler

$a^{ed} = a^{1+k\varphi(n)} = a\, a^{k\varphi(n)}$ $(a^{\varphi(n)} \equiv 1 \bmod n) \Rightarrow$

$\Rightarrow a\,1^k \Rightarrow \boxed{a^{ed} \equiv a \bmod n}$

+ Caso 2 $a \notin \mathbb{Z}_n^*$

$\gcd(a,n) \neq 1 \Rightarrow \gcd(a,n) = \{p, q, n\}$

↳ caso trivial

↳ supongo $p \mid n$

$\gcd(a,q) = 1 \Rightarrow \gcd(a^i, q) = 1 \Rightarrow \gcd(a^{p-1}, q) = 1 \Rightarrow$ ($i = p-1$, P.T Fermat)

$a^{(p-1)(q-1)} \equiv 1 \bmod q$

↳ $a^{ed-a} = 1 + kq$

$a^{ed} = a \cdot a^{k\varphi(n)} \equiv a \bmod q$

$a^{ed} - a = k_1 \cdot q$

como $p \mid a$

$a^{ed} - a = k_2 \cdot p$

$a^{ed} - a = k_3 \cdot \underbrace{pq}_{n}$

$a^{ed} - a \equiv 1 \bmod n \Rightarrow \boxed{a^{ed} \equiv a \bmod n}$

24.

1. $k=4 \quad m=35$

2. $7^{35} \bmod 561 = 241$

   $241 \neq 1 \bmod 561$

   $241 \neq -1 \bmod 561$

   seguimos

3. $i=1$

   $241^2 \bmod 561 = 298$

   $298 \neq -1$

   $298 = 1$

   $i = 2$

   $298^2 \bmod 561 = 166$

   $\vdots$

   $i = 3$

   $166^2 \bmod 561 = 67$

Compuesto

25.

$$p = \frac{1}{1 + \frac{4^m}{m!}}$$

29.

6| Algoritmo de los restos

1 -> $ed - 2 = 2^k \cdot m$

2 -> random $2 \leq a \leq n-1$

3 -> $x = a^m \bmod n$

L-1 o 2 primos

4 -> for i = 1 to k-1

$x = x^2$

if $(x \bmod n == 1) \Rightarrow mcd(x+1, n)$

$(x \bmod n == -1) \Rightarrow$ primos

5 -> $mcd(x+1, n)$

a| $ed - 1 = 300 = 2^2 \cdot 75$

random = 3

$3^{75} \bmod 77 = 31$

i = 1

$y = 31$

$= 31^2 \bmod 77 = 1 \Rightarrow$ primos

$[p = mcd(31-1, 77) = 7] \Rightarrow \boxed{q = 11}$

c) Los 2 propiedades de los primos

d) $\phi(n) = 10 \cdot 6 = 60$

$e^{-1} \bmod 60 = d$

$60 = 7 \cdot 8 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$1 = 4 - 1 \cdot 3 = 4 \cdot -1 [7 - 1 \cdot 4] = -1 \cdot 7 + 2 \cdot 4 =$

$= -1 \cdot 7 + 2 [60 - 8 \cdot 7] = -17 \cdot 7 + 2 \cdot 60 \Rightarrow \boxed{e^{-1} \bmod 60 = -17 = 43}$

30.

a) $p = 221 \Rightarrow 220 = 2^2 \cdot 55$

$k=2 ; m=55$

$a = 5$

$\rightarrow 5^{55} \bmod 221 = 183 \cdot 25 \cdot 5 \bmod 221 = 112$

$5 \bmod 221 = 5$

$5^2 \bmod 221 = 25$

$5^4 \bmod 221 = 183$ (25^2)

$5^8 \bmod 221 = 118$ (183^2)

$5^{16} \bmod 221 = 1$ (118^2)

$5^{32} \bmod 221 = 1$

$112 \neq 1$

$112 \neq -1$

(continuamos)

$\rightarrow i = 1$ a 1

$112^2 \bmod 221 = 168$

$168 \neq -1$

$168 \neq 1$

S. DD

$\rightarrow$ COMPUESTO $\Rightarrow$ NO cumple las propiedades.

a = 21

-> $21^{55} \bmod 221 = 122 \bmod 221 = 220$

$$\begin{bmatrix} 21^1 \bmod 221 = 21 & 21^8 \bmod 221 = 1 \\ 21^2 \bmod 221 = 1 & 21^{16} \bmod 221 = 1 \\ 21^4 \bmod 221 = 1 & 21^{32} \bmod 221 = 1 \end{bmatrix}$$

$220 \neq 1$
$220 \neq -1$ } Contradicción

-> for i = 1 to 1

$[220^2 \bmod 221 = 1]$

$21 \neq 1$ -> COMPUESTO

└> Para cumplir la propiedad debería ser -1 o el anterior haber sido 1