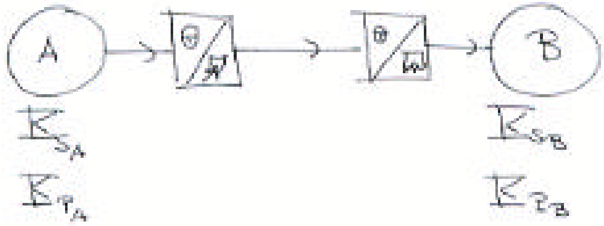
Ejercicio 1 J. Mata ①



5 bits ← → 7 bits

Mensaje	$F[R[i]]$	i
	$F[Fh]$	$76h$

$F(\cdot)$ = firma
$R(\cdot)$ = resumen

a) $K_{P_A} = (e,n) = (17,33)$
$K_{S_A} = (d,n) = (13,33)$

a.1) $F(Fh) = 15^{13} \bmod 33$

$13 = 1101_2$

$15^{13} = 15^{2^3+2^2+0\cdot 2^1+1} = ((15^2\cdot 15)^2\cdot)^2\cdot 15$

$((15^2\cdot 15)^2)^2 15 \bmod 33 = 9$

$F(Fh) = 9 = 1001_2$

a.2) $M = 1001\ 111{,}0110_2$

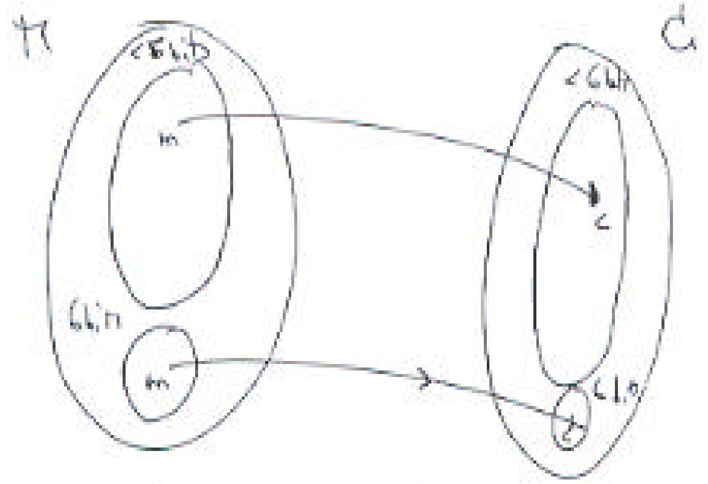
$M = 4F6h$

$M = 1270$

a.3) Si $n = 33$ las firmas podrán tener hasta 6 bits ya que según el RSA

$c = m^e \bmod n < n$

Para que los cifrados ~~requieran~~ de valores de 5 bits o menos bits requieran sólo 5 bits es necesario que los cifrados de valores de 6 bits den lugar a valores de 6 bits. Así



En nuestro caso el único mensaje de 6 bits es $m = 32$. Luego, si se verifica que

$$32 = 32^{e} \bmod n \quad \text{ó} \quad 32 = 32^{d} \bmod n$$

nuestro caso cumple que un cifrado de 5 o menos bits da lugar a un resultado de 5 o menos bits.

En este caso:

$$(32)^{13} \bmod 32 = \left(\left(32^{2} \cdot 32\right)^{2}\right)^{2} \cdot 32 \bmod 33 = 32$$

b) K_{P_B}, K_{S_B} a partir de

$$p = 59,\quad q = 83,\quad e = 11$$

b.1) número primo > 3

$$p' = \frac{p-1}{2} = 29 \qquad q' = \frac{q-1}{2} = 41$$

i) p' y q' son primos grandes $p', q' >> 3$

ii) $p'+1$, $q'+1$ factor primo grande
$p'-1$, $q'-1$ factor primo grande

$$p'+1 = 30 = 2 \cdot 3 \cdot \underline{\underline{5}} \qquad q'+1 = 42 = 2 \cdot 3 \cdot \underline{\underline{7}}$$
$$p'-1 = 28 = 2^2 \cdot \underline{\underline{7}} \qquad q'-1 = 40 = 2^3 \cdot \underline{\underline{5}}$$

Por tanto, p y q son primos fuertes.

b.2)

$$\text{m.c.d}\,(e, \Phi(n)) = 1$$

$$\Phi(n) = (p-1) \cdot (q-1) = 4756 = 2^2 \cdot 29 \cdot 41$$

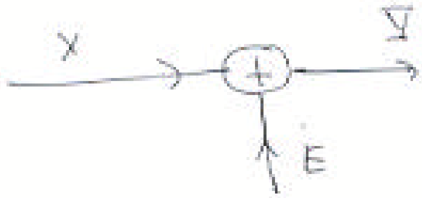
$e = 11$

$$\text{m.c.d}\,(\Phi(n), e) = 1$$

Obsérvese que: $\Phi(n) = 2^2 \cdot p' \cdot q'$

$$\text{m.c.d}\,(e, p') = 1$$
$$\text{m.c.d}\,(e, q') = 1$$

Ejercicio 2



a)

$X \Rightarrow 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0$

$E \Rightarrow 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0$

$Y = X \oplus E \Rightarrow 1\ 0\ 1\ 1\ \underline{1}\ 0\ \underline{0}\ 0$

bits erróneos

b)

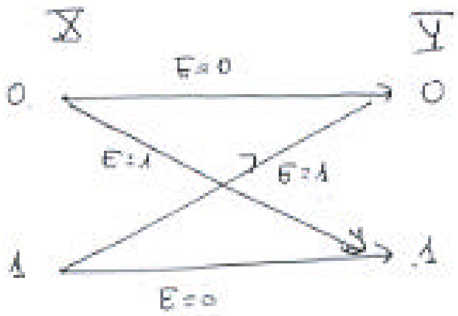
$Pr[X=1] = p \Rightarrow Pr[X=0] = 1-p$

$Pr[E=1] = q \Rightarrow Pr[E=0] = 1-q$

$Pr[Y=1] =$ Prob[(emitir un 1 y ruido 0) $\cup$ (emitir un 0 y ruido 1)]

$Pr[Y=0] =$ Prob[(emitir un 0 y ruido 0) $\cup$ (emitir un 1 y ruido 1)]

Por lo tanto:



$Pr[Y=1] = p\cdot(1-q) + (1-p)\,q$

$Pr[Y=0] = (1-p)(1-q) + p\cdot q$

b.3) $K_{Z_B} = (e, n) = (11, 4897)$

$K_{S_B} = (d, n) = (d, 4897)$

En RSA se debe verificar que

$$e \cdot d = 1 + k\Phi(n) \Rightarrow d = e^{-1} \text{ en } \mathbb{Z}_{\Phi(n)}$$

Utilizando el algoritmo de Euclides extendido

$$k_1 \cdot \Phi(n) + k_2 e = 1 \Rightarrow k_2 = d$$

$$k_1\, 4756 + k_2 \cdot 11 = 1$$

$$\begin{array}{l|l} 4756 & 11 \\ \hline 35 & 432 \\ \ \ 26 & \\ \ \ \ \ 4) & \end{array} \qquad \begin{array}{l|l} 11 & 4 \\ \hline 3 & 2 \end{array} \qquad \begin{array}{l|l} 4 & 3 \\ \hline 1) & 1 \end{array}$$

(1) $1 \cdot 4756 + 0 \cdot 11 = 4756$

(2) $0 \cdot 4756 + 1 \cdot 11 = 11$

$(1) - (2) \cdot 432 \Rightarrow$

(3) $4756 + (-432)\, 11 = 4$

$(2) - (3) \cdot 2 \Rightarrow$

(4) $(-2)\, 4756 + ((-2)(-432) + 1)\, 11 = 3$

$(3) - (4) \Rightarrow$

(5) $(1+2)\, 4756 + (-432 - [(-2) \cdot (-432) + 1]) \cdot 11 = 1$

$\underline{3} \cdot 4756 + \underline{(-1297)}\, 11 = 1 \Rightarrow \underline{d = 3459}$

b4) $C = m^e \bmod n \qquad K_{P_B} = (e,n) = (11, 4897)$

$C = 1270^{11} \bmod 4897$

$1270^{2^3 + 0\cdot 2^2 + 2^1 + 2^0} \bmod 4897 =$

$\left(\left(1270^2\right)^2 \cdot 1270\right)^2 \cdot 1270 \bmod 4897 = 4104 = \underline{\underline{1008h}}$

b5) Para codificar n necesitamos 13 bits

$n = 4897 = 1321h$

Puesto que hay valores de menos de 13 bits que dan lugar a criptogramas de 13 bits debemos asignar 13 bits para el envío del criptograma.

12 bits

M → | 1001 1110 0110 |

C → | 1 0000 0000 1000 |

13 bits

c) $p = 3/4$

$q = 1/8$

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

$$H(X) = p \cdot \frac{\log_{10} 1/p}{\log_{10} 2} + (1-p) \frac{\log_{10}(1/1-p)}{\log_{10} 2}$$

$$H(X) = 0'311 + 0'5 = \underline{\underline{0'811}}$$

$$H(E) = q \log_2 \frac{1}{q} + (1-q) \log_2 \frac{1}{(1-q)}$$

$$H(E) = q \frac{\log_{10} 1/q}{\log_{10} 2} + (1-q) \frac{\log_{10} \frac{1}{1-q}}{\log_{10} 2} =$$

$$H(E) = 0'375 + 0'168 = \underline{\underline{0'543}}$$

d) $Pr[Y=1] \triangleq \alpha = p(1-q) + (1-p)q = 0'6875$

$Pr[Y=0] \triangleq 1-\alpha = (1-p)(1-q) + p \cdot q = 0'3125$

$$H(Y) = \alpha \log_2 1/\alpha + (1-\alpha) \log_2 \frac{1}{(1-\alpha)} = \underline{\underline{0'896}}$$

Obsérvese que: $H(Y) > H(X) > H(E)$

e) $H(Y/X)$ es la cantidad de información que aporta Y cuando se conoce X.

Para determinar $H(Y/X)$ hallamos las probabilidades necesarias:

$$H(Y/X) = \sum_j \sum_i p(x_j)\, p(y_i/x_j) \log_2 \frac{1}{p(y_i/x_j)}$$

$$P_r[Y=1/X=0] = P_r[E=1] = q$$
$$P_r[Y=0/X=1] = P_r[E=1] = q$$
$$P_r[Y=1/X=1] = P_r[E=0] = 1-q$$
$$P_r[Y=0/X=0] = P_r[E=0] = 1-q$$

$$H(Y/X) = P_r(X=0) \cdot \Big[P_r(Y=0/X=0) \cdot \log_2 \frac{1}{P_r[Y=0/X=0]} + P_r(Y=1/X=0) \log_2 \frac{1}{P_r(Y=1/X=0)} \Big]$$
$$+ P_r[X=1] \cdot \Big[P_r[Y=0/X=1] \log_2 \frac{1}{P_r[Y=0/X=1]} + P_r(Y=1/X=1) \log_2 \frac{1}{P(Y=1/X=1)} \Big]$$

$$H(Y/X) = p \cdot \Big[(1-q) \log_2 \frac{1}{(1-q)} + q \cdot \log_2 \frac{1}{q} \Big] + (1-p) \Big[q \cdot \log_2 \frac{1}{q} + (1-q) \log_2 \frac{1}{1-q} \Big]$$

$$H(Y/X) = p \cdot H(E) + 1-p\ H(E)$$

$$\underline{H(Y/X) = H(E)}$$ como conocíamos a priori

④

f)

$$H(X,Y) = H(X) + H(Y/X)$$

$$H(X,Y) = H(X) + H(E) -$$

$$H(X,Y) = 0'811 + 0'543 = 1'354$$

Obsérvese que:

$$H(X,Y) = 1'354 < H(X) + H(Y) = 1'707$$

dado que X e Y no son independientes

g) Dado que:

$$H(X,Y) = H(X) + H(Y/X) = H(Y) + H(X/Y)$$

entonces:

$$H(X/Y) = H(X,Y) - H(Y)$$

Luego

$$H(X/Y) = H(X,Y) - H(Y) = 1'354 - 0'896$$

$$H(X/Y) = 0'458 < H(E) = 0'543$$

h)

$$I(X;Y) = H(Y) - H(Y/X) = H(X) - H(X/Y)$$

$$I(X;Y) = H(Y) - H(Y/X) = H(Y) - H(E)$$

$$I(X;Y) = 0'896 - 0'543 = 0'353$$

Información compartida por X e Y