Tomás Higuera Viso 2359327

EJERCICIO 1

②

K: 0xA → 1010

Encadenamiento ECB

Nia. 359327 → 1010111101110011111

$\overset{I}{00000101}\,\overset{II}{01111011}\,\overset{III}{10011111}$ (Con padding)

Cifrado:

I: 00000101
k: 00001010
XOR 00001111

III: 10011111
00001010
XOR 10010101

II: 01111011
k: 00001010
XOR 01110001

Mensaje cifrado: $\boxed{000011110111000110010101}$

Primeros 5 bits de padding → Sin padding: $\boxed{0xF7195}$

③

K = 0xA → 1010

Encadenamiento CBC

IV = 0xC → 1100

Cifrado:

I: 00000101
IV: 00001100
XOR 00001001
K 00001010
XOR 00000011

II 01111011
00001010
XOR 01110001
K 00001010
01111011

III 10011111
↓ 01111011
XOR 11100100
K 00001010
11101110

Cifrado: $\boxed{000000110111101111101110}$

$\boxed{\text{Sin padding: 0x37BEE}}$

Tomás Higuera Viso e359327

EJERCICIO 2

② Primero hash del mensaje. Alicia se comunica con Bernardo

$m = 359327$

$H(m) = (2m+7) \bmod 11 = 718661 \bmod 11 = \underline{9}$

Firmamos hash con clave privada.

$K_{priv_A} = [47, 77]$

$c = 9^{77} \bmod 47$ → $9^2 \bmod 47 = 34$; $77 = 38 \cdot 2 + 1$ → $(38 \cdot (9^2 \bmod 47) \cdot 9 \bmod 47) \bmod 47 = \boxed{19}$

③ $m = 359327$

cifrar mensaje

$K_{pub_B} = \{5, 65\}$

clave simetrica: 7

→ Primero ciframos con la clave simetrica

~~[illegible] número~~

1010111101110011111

K = 111

↳ Añadimos 2 bits al principio

001010111101110011111 → Ciframos con clave simétrica

↳ $\boxed{110101000010001100000 \to 1737824}$

~~110101000010001100000 → El mensaje obtenido lo ciframos con la clave pública de Bernardo~~

~~1737824~~

~~1737824~~

~~↳ Ciframos número a número: $1^5 \bmod 65 = 1$, $7^5 \bmod 65 = 37$, $9^5 \bmod 65 =$~~

Ciframos clave simetrica

$c = 7^5 \bmod 65 = \boxed{37}$

Mensaje: 1737824 3719

(3)

Ciframos el mensaje con la clave simetrica:

$$\begin{array}{cccccc} 3 & 5 & 9 & 3 & 2 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \end{array}$$ con 7

$\boxed{4\ 8\ 5\ 4\ 7\ 3}$ + Firma $\begin{array}{cc} 1 & 9 \\ \downarrow & \downarrow \\ 1 & 5 \end{array}$

→ $\boxed{\text{Mensaje final : 4854731537}}$

Clave simétrica cifrada: $k=7$

$c = 7^5 \bmod 65 = \boxed{37}$

Tomás Higuera Viso e359327

EJERCICIO 3

(2) $c = 359327$

(3) $K_{PUB} = \{e=29, n=91\}$

$\boxed{\begin{matrix} n=91 \\ e=29 \end{matrix}}$ → $n = p \cdot q$

$\boxed{n = 7 \cdot 13 = 91}$ → $\boxed{\begin{matrix} p = 7 \\ q = 13 \end{matrix}}$

(4) $Z = (7-1) \cdot (13-1) = \boxed{72}$

(5) $e \cdot d \bmod Z = 1$

$29 \cdot d = 1 \bmod(\phi(n))$

$$d = \frac{72k+1}{29} = \frac{72 \cdot 2 + 1}{29} = \boxed{5}$$

k tiene que ser entero al igual que d.

(6) $c = 359327$

$K_{PRIV} = \{91, 5\}$

$m_0 = 3^5 \bmod 91 = 61$

$m_1 = 5^5 \bmod 91 = 31$

$m_2 = 9^5 \bmod 91 = 81$

$m_3 = 3^5 \bmod 91 = 61$

$m_4 = 2^5 \bmod 91 = 32$

$m_5 = 7^5 \bmod 91 = 63$

→ $\boxed{m = 61-31-81-61-32-63}$

Escaneado con CamScanner