Tomás Higuera Viso e359327

Ejercicio 1

(2)

K = 0xA → 1010

Encadenamiento ECB

Nia . 359327 → 1010 1111 0111 0011 1111

I II III (con padding)

00000101 01111011 10011111

Cifrado:

I: 00000101
k: 00001010
XOR 00001111

III: 10011111
000 01010
XOR 10010101

II: 01111011
k: 00001010
XOR 01110001

Mensaje cifrado: 00001111 01110001 10010101

Primeros 5 bits de padding → Sin padding: 0xF1A5

---

(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
k 01111011
XOR 11100100
k 00001010
11101110

Cifrado: 00000011 01111011 11101110

Sin padding: 0x37BEE