Tomás Higuera Viso e359327

EJERCICIO 2

Alicia se comunica con Bernardo

② Primero hash del mensaje.

$m = 359327$

$H(m) = (7m+7) \bmod 11 = 7 \cdot 18 \cdot 661 \bmod 11 = \underline{9}$

Firmamos hash con clave privada.

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

$c = 9^{77} \bmod 47$

$9^2 \bmod 47 = 34$

$77 = 38 \cdot 2 + 1$

$(38 \cdot (9^2 \bmod 47) \cdot 9 \bmod 47) \bmod 47 = \boxed{19}$

③ $m = 359327$

cifrar mensaje

$K_{pub} = [5, 65]$

clave simetrica ?

Primero ciframos la clave simetrica

1010111011001111 11

$K = 111$

Añadimos 2 bits al principio

00101011101100111111 → ciframos con clave simétrica

11010100001000110000 → 1737824

Ciframos clave simetrica

$c = 7^5 \bmod 65 = 47$

Mensaje: 1737824 3719