

Bloque 3

Ejercicio 1

$d?$ públicas

$$e = 5 \quad n = 391$$

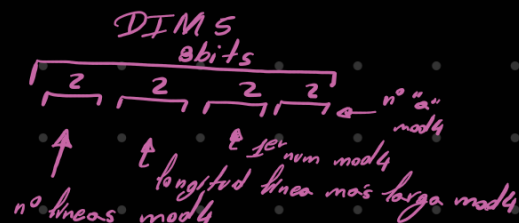
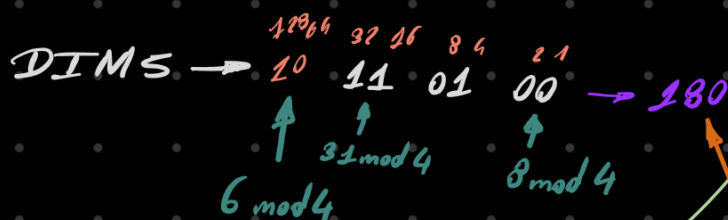
Corleone \rightarrow Forrado

Clave pública: 7

Módulo: 403

} RSA sobre DIM5

$$h(M)^d \bmod (391) = \text{Firma: } 79$$



Si ha sido firmado por Corleone

79

$$79^5 \bmod (391) = 180$$

hash de DIM5 con RSA

DIM5

Resistencia débil a colisiones $M \rightarrow M' \quad h(M) = h(M')$

Resistencia fuerte a colisiones $M \neq M' \rightarrow h(M) = h(M')$

No es fuerte a colisiones por haber muchos mensajes con esas características.

Examen CITIT21

Ejercicio 2

a)

$$\text{hash} = \text{SHA3}(X)$$

← Creamos el hash del fichero

$$(K_{\text{pub}}, K_{\text{priv}}) = \text{GenKey}()$$

← Generamos la clave con la que firmar

$$C = E(\text{hash}, K_{\text{priv}})$$

← Firma generada

b)

$$\text{hash} = \text{SHA3}(X)$$

← Calculamos el hash

$$M = D(C, K_{\text{pub}})$$

← Obtenemos de la firma el hash

$$\text{if}(\text{hash} == M)\{$$

← Si los hash son iguales se ha firmado correctamente.

$$V = \text{"firma valida"}$$

$$\}\text{ else } V = \text{"firma no valida"}$$

Output: V

Examen IWSIM22

Ejercicio 2

$$M^7 \bmod 65 = 50$$

$$50^{13} \bmod 77 = 29$$

$$29^{37} \bmod 77 = 50$$

Mensaje firmado

Autenticidad
siempre que las
claves sean realmente
de A.

Integridad
del mensaje con
claves correctas sino

si lo hubiese firmado
otra, no sería legible al intentar usar la clave A.

$$50^7 \bmod 65 = 15$$

Mensaje original

Certificado

- Datos identificativos
- Clave pública

→ hash → encripta
con clave
privada

- Firma de alguien reconocido que da confianza

← firma

