Bloque 3

Ejercicio 1

d? privadas

e = 5 n = 391

Corleone → Forrado

RSA sobre DIM5

Clave pública: 7 Módulo: 403

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

DIM5 → 10 11 01 00 → 180

128 64 32 16 8 4 2 1

6 mod 4

31 mod 4

8 mod 4

DIM5

8 bits

2 2 2 2 → nº "a" mod 4

↑ nº líneas mod 4

↑ longitud línea más larga mod 4

↑ 1er num mod 4

Sí ha sido firmado por Corleone

79 → $79^5 \bmod(391) = 180$

hash de DIM5 con RSA

DIM5

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

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

No es fuerte a colisiones pues habrá muchos mensajes con esas características.

Examen CITIT 21

Ejercicio 2

a)

```
hash = SHA3(X)                ← Creamos el hash del fichero
(Kpub, Kpriv) = GenKey()      ← Generamos la clave con la que firmar
C = E(hash, Kpriv)            ← Firma generada
```

b)

```
hash = SHA3(X)                ← Calculamos el hash
M = D(C, Kpub)                ← Obtenemos de la firma el hash
if(hash == M){                ← Si los hash son iguales se ha firmado correctamente.
    V = "firma valida"
} else  V = "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

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

$50^7 \bmod 65 = 15$

Mensaje original

Autenticidad siempre que las claves sean realmente de A.

Integridad del mensaje con claves correctas sino

Certificado

- Datos identificativos
- Clave pública

→ hash → encripta con clave privada → Firma

- Firma de alguien reconocido que da confiado