Ejemplo: RSA

① Llaves:

$\Sigma = (0: \sqcup, 1: A, 2: B, \ldots, 26: Z)$

Monogramas $\longrightarrow$ máx. 26

Elegimos p y q, tal que $n = p \cdot q > 26$:

$$p = 5 \quad y \quad q = 7$$

Calculamos: $\phi(35) = (5-1) \cdot (7-1) = 24$

Elegimos un e, tal que:

1) $e < \phi(n)$

2) $mcd(e, \phi(n)) = 1$

Por ejemplo, $e = 11 \longrightarrow (11, 35)$

public key

Calculamos d, tal que:

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

$$11d \equiv 1 \pmod{24}$$

$$\therefore d \equiv 11 \pmod{24} \longrightarrow (11, 35)$$

private key

ó:

③ Encriptación: Bob

Mensaje $M = \text{HIDE}$

08 09 04 05

$$C_i = m_i^e \pmod{n}$$

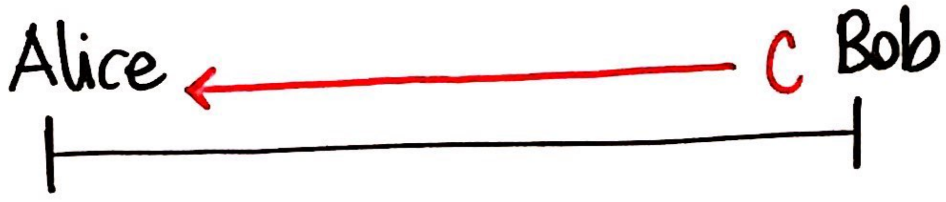
$$H: 08^{11} \pmod{35} \equiv_{35} 22$$

$$I: 09^{11} \pmod{35} \equiv_{35} 04$$

$$D: 04^{11} \pmod{35} \equiv_{35} 09$$

$$E: 05^{11} \pmod{35} \equiv_{35} 10$$

Cipher: $C = 2204 \quad 0910$



④ Desencriptar: Alice

Cipher: $C = 2204 \quad 0910$

$$m_i = c_i^{d} \pmod{n}$$

$$22: \quad 22^{11} \pmod{35} \equiv_{35} 08 \rightarrow H$$

$$04: \quad 04^{11} \pmod{35} \equiv_{35} 09 \rightarrow I$$

$$09: \quad 09^{11} \pmod{35} \equiv_{35} 04 \rightarrow D$$

$$10: \quad 10^{11} \pmod{35} \equiv_{35} 05 \rightarrow E$$

① Bigramas $\longrightarrow$ máx. 2626

$$p = 53 \quad y \quad q = 89$$

Calculo $\phi(4717) = (53-1)\cdot(89-1)$

$$= 4576$$

Elijo e, tal que:

1) $e < 4576$

2) $\text{mcd}(e, 4576) = 1$

$e = 3041 \longrightarrow (3041, 4717)$

public key

Calculo d:

$$3041\, d \equiv 1 \pmod{4576}$$

$d = 2209 \longrightarrow (2209, 4717)$

private key

③ $M = \underbrace{PI}\underbrace{ZZ}\underbrace{AS}$

$PI: 1609^{3041} \pmod{4717} \equiv 0993$

$ZZ: 2626^{3041} \pmod{4717} \equiv 0064$

$AS: 0119^{3041} \pmod{4717} \equiv 0738$

Cipher: $C = 099300640738$

④ Cipher: $C = \underbrace{0993}\underbrace{0064}\underbrace{0738}$

$0993: 993^{2209} \pmod{4717} \equiv 1609 \rightarrow PI$

$0064: 64^{2209} \pmod{4717} \equiv 2626 \rightarrow ZZ$

$0738: 738^{2209} \pmod{4717} \equiv 0119 \rightarrow AS$