

## Criptografía asimétrica o de clave pública

Cada usuario del sistema criptográfico ha de poseer una pareja de claves, formada por:

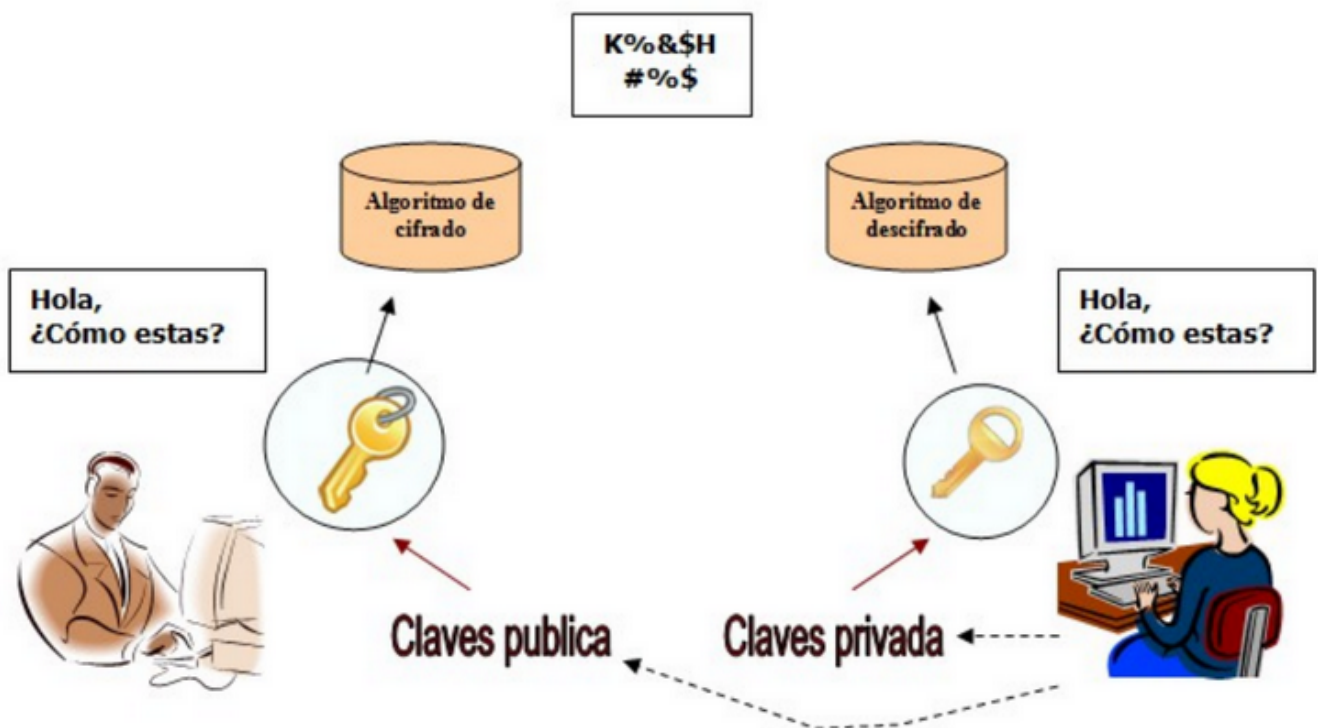
- Una **Clave privada**, que será custodiada por su propietario y no se dará a conocer a ningún otro.
- Una **Clave pública**, que será conocida por todos los usuarios.



Esta pareja de claves es **complementaria**: lo que cifra una solo lo puede descifrar la otra y viceversa.

Como es lógico pensar, estas claves se generan a la vez y se encuentran relacionadas matemáticamente entre sí mediante funciones de un solo sentido.

Resulta prácticamente imposible descubrir la clave privada a partir de la pública



## Algoritmo RSA

# RSA Algorithm

## Key Generation

|                                  |   |
|----------------------------------|---|
| Select $p, q$                    | $p$ and $q$ both prime; $p \neq q$      |
| Calculate $n = p \times q$       |   |
| Calculate $\phi(n) = (p-1)(q-1)$ |   |
| Select integer $e$               | $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$ |
| Calculate $d$                    | $de \bmod \phi(n) = 1$                  |
| Public key                       | $KU = \{e, n\}$                         |
| Private key                      | $KR = \{d, n\}$                         |

## Encryption

|             |                   |
|-------------|-------------------|
| Plaintext:  | $M < n$           |
| Ciphertext: | $C = M^e \bmod n$ |

## Decryption

|             |                   |
|-------------|-------------------|
| Plaintext:  | $C$               |
| Ciphertext: | $M = C^d \bmod n$ |

Práctica: <https://www.devglan.com/online-tools/rsa-encryption-decryption>