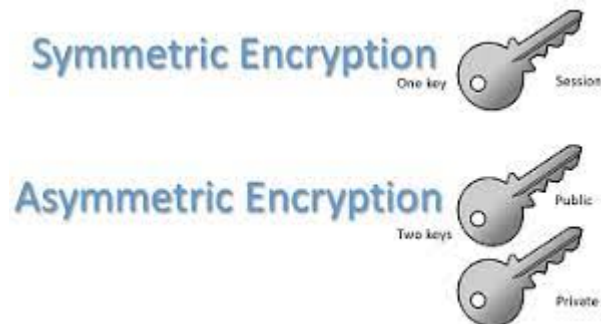


6.4. Criptografía asimétrica o de clave pública

En la criptografía asimétrica tenemos, en lugar de única clave compartida por el emisor y el receptor, 2 claves por cada persona.



¿Qué claves se necesitan?

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.

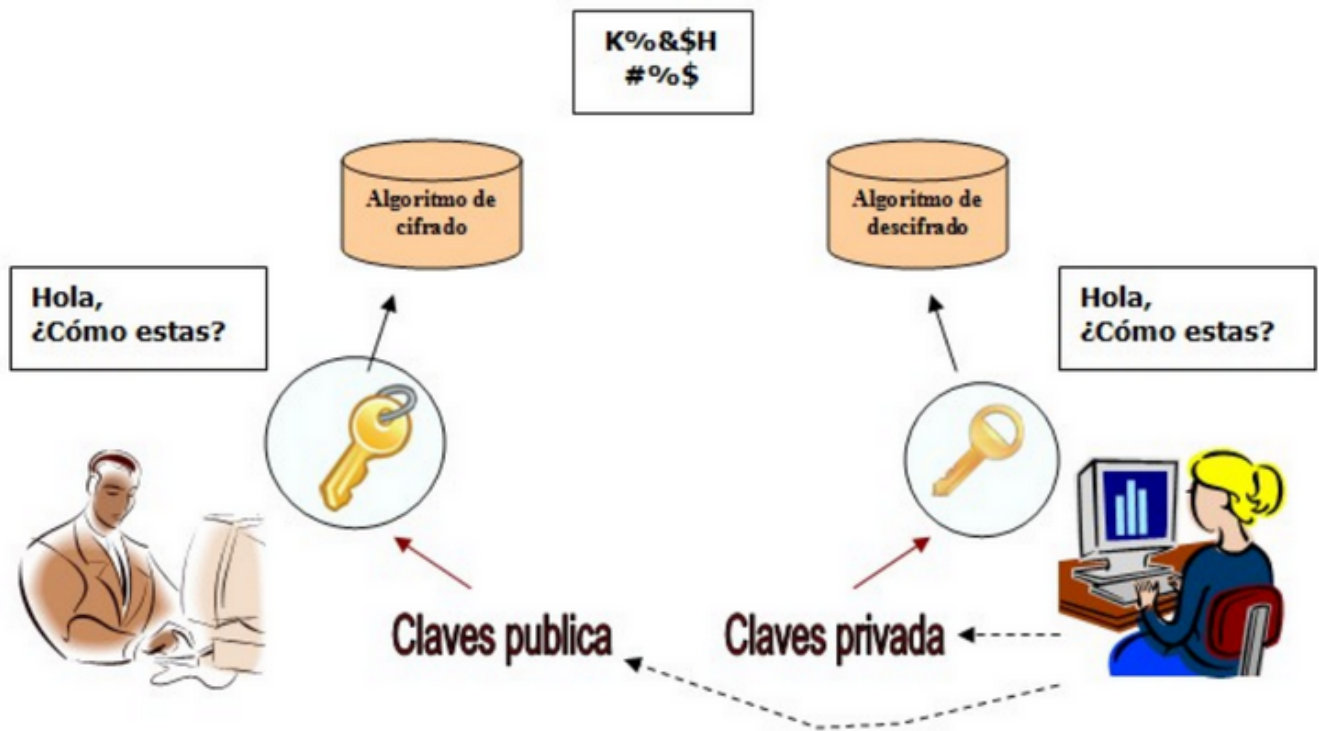


¿Qué relación tienen estas 2 claves?

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:	M
Ciphertext:	C
	$M = C^d \bmod n$

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

Generación de claves

Generate RSA Key Online

Select RSA Key Size

515 bit

Generate RSA Key Pair

Public Key

```
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB  
AJeB  
eevbAeSD/69xV5wTn5Qq4u97ypCdIB6X6r9nA  
qyqs9Q+7CEj+gaH6eq0UoP955XW6JcY5BuxEF  
04vFt8okBECawEAAQ==
```

Private Key

```
MIIBUwIBADANBgkqhkiG9w0BAQEFAASCAT0wg  
gE5AgEAAkEAKF569sB5IP/r3FXnBOflCri73vKkJ3  
UHpfqv2cCrKqzID7sISP6Bofp6rRSg  
/3nldbolxjkG7EQXTi8W3yiQEQIDAQABAKB  
/xK5MzWEmXHjQotH3XlqvqfjTQqkXJpLjSW7yZ3  
rVI7lJmjIUOWzFCEllizhuFga1uD5vSOYbKSaVSA  
cN3Y5IAiEAzKj2HOXAY8zeiqJRQdqrfoDByT6H8K  
HydwKT8bYclw8CIQCzKYeB4C7NC9JCElyClaZX  
czhW/Q4wM/ZVfoG5nt9m3wlgVizgs72  
/G3lQXbXIYC9riGhLcTiwLXRaCCGJkGZVlz0CIG  
cHot2VRIS0T52fYYPW+2me4O9lZxthRm+z6HY  
OXvqRAiBUGnsn  
//Gr5tASLz2mUulzjJWKZVlvcNBr0ok  
/ymG9wA==
```

Enciptar con clave privada

RSA Encryption

Enter Plain Text to Encrypt

Hola soy dani

Enter Public/Private key

MIIBUwIBADANBgkqhkiG9w0BAQEFAASCAT0wg
gE5AgEAAkEAKF569sB5IP/r3FXnBOlCn73vKkJ3
UHpfqv2cCrKqzID7sISP6Bofp6rRSg
/3nldbolxjkG7EQXTi8W3yiQEIDAQABAKB
/xK5MzWEmXHjQotH3XlGvqfjTQqkXJpLjSW7yZ3r
VI7lJmj1UOWzFCEllizhuFgaluD5vSOYbKSaVSAc
N3Y5IAiEAzkj2HOXAY8zeiqJRQdqrOdByT6H8KH
ydwKT8bYclw8CIQCzKYeB4C7NC9JCElyClaZXc
zhW/Q4wm/ZVfoG5nt9m3wlgVizgs72
/G3lQxbXIYC9riGhLcTiwlXRaCCGJkGZVlz0CIGc
Hot2VRIS0T52fYYPW+2me4O9lZxthRm+z6HYOX
vqRAiBUGnsn
//Gr5tASLz2mUulzJWkZV1vcNBr0ok
/ymG9wA==

RSA Key Type: ☐ Public key ☒ Private Key

Select Cipher Type

RSA/ECB/PKCS1Padding

Encrypt

Encrypted Output (Base64):

GjTn3LqUny3c586dtues18FIIEEC23MtZPWe8Vg8
2c3SPycj+CWLBMvkGyZvukhxj9ksiz+HHRogXVp
7c2liwg==

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

GjTn3LqUny3c586dtues18FIIEEC23MtZPWe8Vg
82c3SPycj+CWLBMvkGyZvukhxj9ksiz+HHRogXV
p7c2liwg==

Enter Public/Private key

MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBABJB
eevbAeSD/69xV5wTn5Qq4u97ypCd1B6X6r9nA
qyqs9Q+7CEj+gaH6eq0UoP955XW6JcY5BuxEF
04vFt8okBECawEAAQ==

RSA Key Type: ☒ Public key ☐ Private Key

Select Cipher Type

RSA/ECB/PKCS1Padding

Decrypt

Decrypted Output:

Hola soy dani

Webs para practicar

- <https://cryptii.com/pipes/caesar-cipher>
- <https://cifronline.com/>
- <https://www.devglan.com/online-tools/rsa-encryption-decryption>