① Key Generation: (create Public and Private key).

(i) Choose two large Prime numbers: p and q

(ii) Compute:
- $n = p \times q$ → used as Part of both keys.
- $\phi(n) = (p-1)(q-1)$ → used internally

(iii) chose a Public exponent / key "e" such that:
- $1 < e < \phi(n)$
- "e" and $\phi(n)$ are coprime

(iv) Compute the Private exponent / key "d"
- $d \times e \bmod \phi(n) = 1$
- $1 < d < \phi(n)$.

🔓 Public key = (e, n)

🔒 Private key = (d, n).

② Encryption (Sender Uses Receiver's Public key).

If Alice wants to send "Hi" to Bob:
- Alice converts the message to a number m
- Encrypts it using Bob's Public key:

$$\text{cipher} = m^e \bmod n.$$

③ Decryption (Receiver Uses Their Private Key)

- Bob uses his Private key to decrypt.

$$\text{message} = \text{cipher}^{d} \bmod n$$

Example (with Small Numbers).

① $P = 3$, $q = 11$

② $n = 3 \times 11 = 33$

③ $\phi(n) = (P-1)(q-1)$
$= 2 \times 10 = 20$

④ choose $e = 3$ (coprime with 20)

⑤ Find $d = 7$ (because $7 \times 3 = 21 \bmod 2$

Public Key = (3, 33)
Private key = (7, 33)

Message = $m = 4$.
Encryption: cipher = $4^3 \bmod 33 = 31$

Decryption: message = $3^7 \bmod 33 = 4$