→ RSA algorithm

① p & q — Prime numbers

② $n = p \times q$

③ $\varphi(n) = \phi(n) = (p-1)(q-1)$
totient

④ Select e (public key)

check this
(i) $1 < e < \varphi(n)$
(ii) $\gcd(e, \varphi(n)) = 1$

⑤ $d = e^{-1} \bmod \phi(n)$

private key

public key

$P_u\,(e, n)$

$P_r\,(d, n)$

private key

⑥ Encryption: public key is used.

plaintext → m

ciphertext → C

Scanned with CamScanner

Ciphertext $C = M^{e_B} \bmod n$ — e - public key

M ↑ msg

n ↑

* For encryption Receiver ← public key and

* For decryption Receiver → private key and

Decryption

↳ private key (Receiver)

Ciphertext → plaintext

$$\boxed{M = C^{d_B} \bmod n}$$

d → private key

Eg: Problem for RSA

Consider

* $p = 17$, * $q = 11$
* $M = 88$

① $n = p \times q$

$= 17 \times 11$

$= 187$

② $\phi(n) = (p-1) \times (q-1)$

$= 160$

③ choose 'e' → public key selection (e, n)

$gcd(e, 160) = 1$

(or)

$gcd(160, e) = 1$

$n =$

$1 < 7 < 160$

$\boxed{d = e^{-1} \bmod 160}$ → private key creation (d, n)

$d = 7^{-1} \bmod 160$

$d \times 7 = 1 \bmod 160$

$\downarrow$

?

i.e

$\boxed{d \times 7 = 1}$

$\downarrow$

$1 \% 160 = 1$

But.

$161 \% 160 = \underline{1}$

Trick for calculating d

$160 \div 7 = 22.85$

$= \underline{\underline{23}}$

$7 \times 23 = 161.$

$7 \times 23 = 1 \bmod 160$

$\boxed{d = 23}$

$M = 88$

$e = 7$

$d = 23$

If it is not getting actual value you can divide multiples of 160 with 7.

ie. $320 \% 7$, $480 \% 7$

<u>Encryption</u> $M \rightarrow C$

$$C = M^{e_B} \bmod n$$

$$= 88^7 \bmod 187$$

How to calculate $88^7 \bmod 187$?

$\rightarrow 88^1 = 88 \bmod 187$

$= 88.$

$88^2 = 88^2 \bmod 187$

$= 7744 \bmod 187$

$= 77$

$88^4 = 77^2 \bmod 187$

$= 132$

$= 88^7 \bmod 187 = (88)(88^2)(88)^4 \bmod 187$

$= (88)(77)(132) \bmod 187$

$= 894432 \bmod 187$

$\boxed{C = 11}$

(i) $88 \times 88 = 7744$

$7744 \div 187 = 41$

(ii) 187×41

$7667.$

(iii) $7744 - 7667$

77

Decryption: $C \rightarrow M$

$$M = C^{d_B} \bmod n$$

$$= 11^{23} \bmod n$$

$$11^1 = 11 \bmod 187$$

$$= 11$$

$$11^2 = 121 \bmod 187$$

$$= 121$$

$$11^4 = 14641 \bmod 187$$

$$= 55$$

$$11^8 = 55^2 \bmod 18$$

$$= 3025 \bmod 187$$

$$= 33$$

$$11^{16} = 33^2 \bmod 187.$$

$$= 154.$$

$$11^{23} = 11^1 \times 11^2 \times 11^4 \times 11^{16}$$

$$(11) \times (121) \times (55) \times 154$$

Decryption : $C \rightarrow M$

$$M = C^{d_B} \bmod n$$

$$= 11^{23} \bmod n$$

$11^1 = 11 \bmod 187$

$= 11$

$11^2 = 121 \bmod 187$

$= 121$

$11^4 = 14641 \bmod 187$

$= 55$

$11^8 = 55^2 \bmod 18$

$= 3025 \bmod 187$

$= 33$

$11^{16} = 33^2 \bmod 187.$

$= 154.$

$11^{23} = 11^1 \times 11^2 \times 11^4 \times 11^{16}$

$(11) \times (121) \times (55) \times 154$

$M = 11^{23} \bmod 187$

$= (11) \times (121) \times (55) \times (154) \bmod 187$

$= 11273570 \bmod 187$

$\boxed{M = 88}$