II. Public Key Cryptography Algorithms

- Uses pair of keys :
  - → Public Key for encryption (KU)
  - → Private Key for decryption (RU)

- RSA (Rivest - Shamir - Adleman)

→ **Key Generation**

1) Select two large prime numbers p and q
2) Compute $n = p \times q$
3) Compute Euler's function $\phi(n) = (p-1)(q-1)$
4) Choose a public exponent e such that
   $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
5) Compute the private key d such that
   $d \times e \equiv 1 \mod \phi(n)$
   $d \times e = 1 + K \times \phi(n)$
6) KU: $\{e, n\}$, KR: $\{d, n\}$

Notes :

- d should be : integer , $< \phi(n)$
- K is just an integer (e.g., 1, 2, 3, 4, ...) that helps us solve d
- We try different options of K to find a valid solution
- e and d should not be the same

→ **Encryption**: $C = M^e \mod n$

→ **Decryption** : $M = C^d \mod n$

Note :

- M is converted to a nb. based on the alphabetical order

6) Public Key: (e.n) , Private Key: (d.n)

. RSA Encryption and Decryption

→ Encryption (Sender Side)

$C = M^e \bmod n$

M: Message (as a nb)
C: Encryption message

→ Decryption (Receiver Side)

$M = C^d \bmod n$

Only the receiver (who had d) can decrypt it

. Examples

I)

1) $p = 17$, $q = 11$

2) $n = p \times q = 17 \times 11 = 187$

3) $\phi(n) = (p-1)(q-1) = (16 \times 10) = 160$

4) e? $\gcd(\phi(n), e) = 1$ "should be prime" $1 < e < \phi(n)$

$\Rightarrow 1 < e < 160$

options: $e = 3$, $e = 7$, $e = 11$

5) $d.e = 1 \bmod (160)$; $d < 160$

$e.d = 1 + K.\phi n$

$3 \times d = 1 + K.160$ } $K = 1$

$3d = 161$

$d = 53.66$ (not integer) $\Rightarrow e = 3$ ✗

Try $e = 7$

$7 \times d = 161$

$d = 23$ ✓ Then $e = 7$

6) Public Key: $KU\{e, n\} = \{7, 187\}$

Private Key $KR\{d, n\} = \{23, 187\}$

II) 1) $p = 3 \quad q = 11$

2) $n = p \times q = 33$

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

4) e ?

gcd $(\phi(n), e) = 1$

gcd $(20, e) = 1$ } e can be 3, 7, 11 ....

$1 < e < 20$

5) $d.e = 1 \bmod (\phi(n))$

$d.e = 1 \bmod (20) \Rightarrow d < 20$

$e.d = 1 + K.\phi(n)$

- Let $K = 1$ and $e = 3$

$3.d = 1 + 20$

$3.d = 21$

$d = 7$

6) Private Key : $KR = \{d, n\} = \{7, 20\}$

Public Key : $KU = \{e, n\} = \{3, 20\}$

III) 1) $p = 5$, $q = 7$, $M = L$ (12 in alphabelical order)

2) $n = q \times p = 7 \times 5 = 35$

3) $\phi(n) = (p-1)(q-1) = 4 \times 6 = 24$

4) $e = ?$

gcd $(24, e) = 1$ } e can be 5, 7, 11 ..

$1 < e < 24$

5) $e.d = 1 \bmod (24) \Rightarrow d < 24$

$e.d = 1 + K\phi(n)$

↳ let $K = 1$ and $e = 5$

$5.d = 25$

$d = 5$ and $e = 5$ (e and d are the same : not logical)

↳ let $K = 6$, $e = 5$

$5.d = 1 + 6(24)$

$5.d = 145$

$d = 29$ ✓

=> Public Key : $KU = \{5, 35\}$ → For encryption

Private Key : $KR = \{29, 35\}$ → For decryption

. Encryption :

$C = L^e \bmod n$

$C = 12^5 \bmod 35$

248832	35
248815	7109
17	

=> $C = 17$

. Decryption : $M = C^d \bmod n = 17^{29} \bmod 35$