RSA Algorithm

- RSA (Rivest - Shamir - Adleman) used to encrypt & decrypt
- Asymmetric cryptographic Algorithm.

Encryption

$$C = P^e \bmod n$$

Decryption

$$P = C^d \bmod n$$

Public key = $\{e, n\}$

Private key = $\{d, n\}$

Key Generation

1) Consider two large Prime number q, P.
2) Calculate $n = P \times q$
3) $\phi(n) = (P-1)(q-1)$
4) Choose a small number e
   with GCD $(\phi(n), e) = 1$ and $1 < e < \phi(n)$
5) Find d such that $d \times e \bmod \phi(n) = 1$

Example

1) Two Prime number $P = 3, q = 5$

2) $n = P \times q$
   $= 3 \times 5$
   $\boxed{n = 15}$

3) $\phi(n) = (P-1)(q-1)$
   $= (3-1)(5-1)$
   $= 2 \times 4$
   $\phi(n) = 8$

4) Assume e such that $\gcd(\phi(n), e) = 1$ and $1 < e < \phi(n)$

   $\boxed{e = 3}$

   $\gcd(2,8) = 2$
   $\gcd(3,8) = 1$
   $\gcd(5,8) = 1$
   $\gcd(7,8) = 1$

5) find d

$$d \times e \bmod \phi(n) = 1$$

$d \times 3 \bmod 8 = 1$

Consider $d = 1$

$1 \times 3 \bmod 8 \neq 1$

consider $d = 2$,

$2 \times 3 \bmod 8 = 1$

$6 \bmod 8 \neq 1$

consider $d = 3$

$3 \times 3 \bmod 8 = 1$

$9 \bmod 8 = 1$

$d = 3$

Public key $= \{e, n\} = \{3, 15\}$

Private key $= \{d, n\} = \{3, 15\}$

Encryption

$$C = P^e \bmod n$$

Consider Plain Text $P = 8$

$$C = P^e \bmod n$$

$$= 8^3 \bmod 15$$

$$= 512 \bmod 15$$

$$\begin{array}{r} 34 \\ 15 \overline{)\,512} \\ \underline{510} \\ 2 \end{array}$$

$C = 2$

Decryption

$$P = C^d \bmod n$$

$$= 2^3 \bmod 15$$

$$= 8 \bmod 15$$

$P = 8$