RSA Algorithm

The algorithm was developed 1977 by **Ron** Rivest, **Adi** Shamir, and **Len** Adleman at MIT and first published in 1978. The RSA scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.

It is a block cipher in which the plaintext and ciphertext are integers between 0 and n 1 for some n.

The algorithm consists of below:

- **Part #1 : Key Generation**

  - Select p, q where: p and q both prime, $p \neq q$
  - Calculate $n = p \, x \, q$
  - Calculate $\varphi\ (n) = (p-1)(q-1)$
  - Select integer e where:$gcd\ ((\varphi\ (n), e) = 1;\ 1 < e < \varphi(n)$
  - Calculate d where: $d \equiv e^{-1}(mod\ \varphi(n))$
  - Public Key $PU = \{e, n\}$
  - Private Key $RP = \{d, p, q\}$

- **Part #2: Encryption:**
  - Plaintext: M<n
  - Ciphertext: $C = M^e \bmod n$
- **Part #3 Decryption:**
  - Ciphertext: C
  - Plaintext $M = C^d \bmod n$

Example:

Suppose p=17, q=11. Using RSA to encrypt the message M=88

Solution:

- n=p*q → 17*11 =**187**
- φ (n) = (p-1)(q-1) = 16*10
  =**160**
- choose e verifies $gcd\ ((\varphi\ (n), e) = 1\ ;\ 1 < e < \varphi(n)$
  then $\boldsymbol{e = 7}$
- choose d verifies $e.d \equiv\ 1\ mod\ \varphi\ (n)$, then $\boldsymbol{d = 23}$
  $7.23\ \equiv\ 1\ mod\ 160$
- PU={7, 187}
- PR={23,17,11}

To encrypt m=88 using the encryption formula

$C\ = M^e\ mod\ n$→ 88^7 mod 187 =11

The decryption:

$M\ = C^d\ mod\ n$

$M\ = 11^{23}\ mod\ 187 = 88$