RSA (Rivest–Shamir–Adleman)

RSA was proposed by Rivest, Shamir & Adleman of MIT in 1977. It is a widely used public-key scheme. The algorithm uses number theory and modular arithmetic along with large integers. It is very a very secure approach due to cost of factoring large numbers.

RSA Encryption/ Decryption

- For encrypting a message M the sender:
  - obtains public key of recipient PU={e,n}
  - computes: $C = M^e \bmod n$, where $0 \le M < n$
- To decrypt the ciphertext C the owner:
  - uses their private key PR={d,n}
  - computes: $M = C^d \bmod n$
- It should be noted that the message M must be smaller than the modulus n

RSA Key Set up

Each user generates a public/private key pair by

- selecting two large primes at random: p, q
- computing their system modulus n = p . q
  - note, $ø(n)=(p-1)(q-1)$
- selecting at random the encryption key e
  - where $1<e<ø(n)$, $\gcd(e, ø(n))=1$
- solving the following equation to find decryption key d
  - $e \cdot d=1 \bmod ø(n)$ and $0 \le d \le n$
  - By Euler's theorem, $e \cdot d = 1 + k \cdot ø(n)$ for some k

The public encryption key is PU={e,n} which is published and the private decryption key is PR={d,n} which is kept secret.

RSA Example

- **Key Setup**
  - At first, p and q are selected; p=17 & q=11
  - Then, n is calculated. $n = p \times q = 17 \times 11 = 187$
  - ø(n) is calculate. $ø(n)=(p-1) \times (q-1) = 16 \times 10 = 160$
  - e is selected so that gcd(e,160) = 1; e=7
  - d is determined. $d \times e = 1 \bmod 160$ & $0 \le d \le 187$. d=23 as, $23 \times 7 = 161 = 10 \times 160 + 1$
  - Public key PU= {7,187} is published.
  - Private key PR= {23,187} is kept secret.
- **Encryption/Decryption**

  Sample RSA encryption/decryption is:
  - Given message M = 88 (nb. 88<187)
  - Encryption: $C = 88^7 \bmod 187 = 11$
    - Exploiting the properties of modular arithmetic, following can be done: $88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$
  - Decryption: $M = 11^{23} \bmod 187 = 88$

RSA Example with text

p = 73, q = 151
n = 11023
ø(n) = 10800
e = 11
d = 5891

Text = How are you?

H=	33	a=	00	y=	24
o=	14	r=	17	o=	14
w=	22	e=	04	u=	20
_	62	_	62	?=	66

$M_1 = 3314$	$M_2 = 2262$	$M_3 = 0017$
$M_4 = 0462$	$M_5 = 2414$	$M_6 = 2066$

$C_1 = 3314^{11} \bmod 11023 = 10260$
$C_2 = 2262^{11} \bmod 11023 = 9489$
$C_3 = 17^{11} \bmod 11023 = 1782$
$C_4 = 462^{11} \bmod 11023 = 727$
$C_5 = 2414^{11} \bmod 11023 = 10032$
$C_6 = 2006^{11} \bmod 11023 = 2253$

$M_1 = 10260^{5891} \bmod 11023 = 3314$
$M_2 = 9489^{5891} \bmod 11023 = 2262$
$M_3 = 1782^{5891} \bmod 11023 = 0017$
$M_4 = 727^{5891} \bmod 11023 = 0462$
$M_5 = 10032^{5891} \bmod 11023 = 2414$
$M_6 = 2253^{5891} \bmod 11023 = 2006$