4.7.1 The RSA Algorithm

The RSA algorithm developed in 1977 by Rivest, Shamir, Adleman (RSA) at MPT. RSA algorithm is public key encryption type algorithm. In this algorithm, one user (party) uses a public key and other user uses a secret (private key) key. In the RSA algorithm each station independently and randomly chooses two large primes p and q number, and multiplies them to produce $n = pq$ which is the modulus used in the arithmetic calculations of the algorithm. The process of RSA algorithm is as follows.

1. Select p and q but both are prime number.
2. Calculate $n = pq$
3. Calculate $z = (p-1)(q-1)$
4. Select integer D which is relatively prime to 2. $gcd\ \phi(n)\ D = 1 \qquad (\phi(n) = z)$
5. Calculate ED = 1 mod $(\phi(n))$

For encryption :

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

where P is plaintext, C is cipertext (encryption)

For Decryption (for calculating plaintext)

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

Let us consider an example. By selecting two prime number p and q, calculate the $n = p \times q$, which is the modulus for encryption and decryption. The $\phi(n)$ which is the number of positive integers less than n and relatively prime to n. Select D which is relatively prime to $\phi(n)$. Finally calculate E. For calculating E, ED (mod n) = 1 condition must satisfy. The private key consists of *(D, n)* and the public key consists of *(E, n)*. Suppose that user A has published its public key and that user B wishes to send the message (P) to user A. Then user B calculate $C = P^E \pmod{n}$ and transmits C. After receiving this ciphertext, user A decrypts that message by calculating $P = C^D \pmod{n}$.

➡ Example 4.1 :

1. Select two prime numbers p = 7 and q = 17
2. Calculate $n = pq = 7 \times 17 = 119$
3. Calculate $z = \phi(n) = (p-1)(q-1)$
   $= (7-1)(17-1)$
   $= (6)(16)$
   $= 96$
4. Select D such that D is relatively prime to $\phi(n)$. The factors of 96 are 2, 2, 2, 2, 2 and 3. We choose D as 5, which is not a factor of 96.
5. Determine E such that $DE\ (mod\ \phi(n)) = 1$

Here D is 5 and $mod\,\phi(n) = 96$. We choose E = 77 so check E = 77 with $DE\,(mod\,\phi(n)) = 1$.

$$5 \times 77\ (mod\ 96) = 1$$
$$385\ (mod\ 96) = 1$$
$$1 = 1$$

[For mod 96, after dividing 385 by 96, remainder is 1 (one). In mod operator only remainder is consider.]

Example 4.2 : *Using public key crypto system with $a = 1$, $b = 2$ .... etc.*

i) If $p = 7$ and $q = 11$ list five legal value for d.

ii) If $p = 13$ and $q = 31$ and $d = 7$ find e.

iii) Using $p = 5$, $q = 11$ and $d = 27$ find e and encrypt "abcdefghij".

Ans. : i) $p = 7$, d = ?, $q = 11$

$$z = \phi(n) = (p-1)(q-1)$$
$$= (7-1)\ (11-1)$$
$$= 6 \times 10$$
$$= 60$$
$$n = pq$$
$$= 7 \times 11$$
$$= 77$$

Select integer 'd' which is relatively prime to z.

$$gcd\,(\phi(n) \cdot d) = 1$$

Factors of 60 is = 2, 2, 3, 5

So the value for d is = 7, 11, 13, 17, 19

ii) $p = 13$, $q = 31$ and $d = 7$, $e = ?$

$$z = \phi(n) = (p-1)\ (q-1)$$
$$= (13-1)\ (31-1)$$
$$= 12 \times 30$$
$$= 360$$
$$n = p\,q$$
$$= 13 \times 31$$
$$= 403$$

Calculate $e\,d = 1\ mod\ (\phi\,(n))$

For calculating e, check the condition

$$e\ d\ (mod\ \phi\,(n)) = 1$$

Here e = 103 for d = 7

Check the value.

$$103 \times 7\ (mod\ 360) = 1$$

$$721 \text{ mod } 360 = 1$$

$$1 = 1$$

$\therefore$ For given $d=7$, value for $e=103$.

iii) $p=5$, $q=11$ and $d=27$, e = ?

$$z = \phi\,(n) = (p-1)\,(q-1)$$

$$= (5-1)\ (11-1)$$

$$= 4 \times 10$$

$$= 40$$

$$n = p \times q = 5 \times 11 = 55$$

$$e\,d = 1\ mod\ \phi\,(n)$$

$$e_{27} = 1\ mod\ (40)$$

$$e = 3$$

Plaintext (P)			Encrypt (C)
Symbolic	**Numeric**	P^3	$P^3 mod\ (55)$
a	1	1	1
b	2	8	8
c	3	27	27
d	4	64	09
e	5	125	15
f	6	216	51
g	7	343	13
h	8	512	17
i	9	729	14
j	10	1000	10