Ron Rivest, Adi Shamir and Len Aldeman have developed this algorithm (Rivest-Shamir-Aldeman) in 1978. It is a public-key encryption algorithm. It is a block-cipher which converts plain text into cipher text at sender side and vice versa at receiver side.

The algorithm works as Follows

1. Select two prime numbers a and b where $a \neq b$.
2. Calculate $n = a * b$
3. Calculate $\phi(n) = (a - 1) * (b - 1)$.
4. Select e such that, e is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
5. Calculate of such that $d = e^{-1} \bmod \phi(n)$ or $ed \bmod \phi(n) = 1$.
6. Public key = {e,n}, private key = {d,n}.
7. Find out ciphertext using the formula,

   $C = P^e \bmod n$ where, $P < n$ and

   C = Ciphertext, P = Plaintext, e = Encryption key and n = Block size.
8. $P = C^d \bmod n$. Plaintext P can be obtain using the given formula.

   Where, d = decryption key.

Both sender and receiver know the value of n. In addition, the sender must know encryption key 'e' and receiver must know decryption key 'd'.

Example

1. Select two prime numbers a = 13, b = 11.
2. $n = a*b = 13 * 11 = 143$.
3. $\phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.
4. Select e = 13, gcd (13, 120) = 1.
5. Finding d :

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

   $13 * d \bmod 120 = 1$

   Do the following procedure till you are not getting a integer numbers

$$d = \frac{(\phi(n) * i) + 1}{e}$$

$$d = \frac{(120 + 1)}{13} = \frac{121}{13} = 9.30 \ (i = 1)$$

where, i = 1 to 9

$$d = \frac{240 + 1}{13} = \frac{241}{13} = 18.53 \ (i = 2)$$

$$d = \frac{360 + 1}{13} = \frac{361}{13} = 27.76 \ (i = 3)$$

$$d = \frac{480+1}{13} = \frac{481}{13} = 37$$

Hence d = 37

6. Hence public key = {13, 143} and Private key = {37, 143}
7. Encryption :

Consider any integer as a plaintext (P)

Such that P < n

Example : 13 $\because (13 < 143)$

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

$C = 13^{13} \bmod 143$

Here to find out $13^{13} \bmod 143$, use the following procedure

$13 \bmod 143 = 13$

$13^2 \bmod 143 = 169 \bmod 143 = 26$

$13^4 \bmod 143 = 26^2 \bmod 143 = 104$

$13^8 \bmod 143 = 104^2 \bmod 143 = 91$

$\therefore \quad C = [(13^8 \bmod 143) * (13^4 \bmod 143) * (13 \bmod 143)] \bmod 143$

$= [91 * 104 * 13] \bmod 143 = 52$

8. Decryption :

$P = C^d \bmod n = 52^{37} \bmod 143$

Again use above mentioned procedure to find out $52^{37} \bmod 143$. As

$52 \bmod 143 = 52$

$52^2 \bmod 143 = 130$

$52^4 \bmod 143 = (130)^2 \bmod 143 = 26$

$52^8 \bmod 143 = (26)^2 \bmod 143 = 104$

$52^{16} \bmod 143 = (104)^2 \bmod 143 = 91$

$52^{32} \bmod 143 = (91)^2 \bmod 143 = 130$

Hence, $P = 52^{37} \bmod 143 = [(52^{32} \bmod 143) * (52^4 \bmod 143) * (52 \bmod 143)] \bmod 143$

$= [130 * 26 * 52] \bmod 143 = 13$

2.12.1 Solved Examples on RSA Algorithm

Ex. 2.12.1 : What is RSA ? Prime number a = 3, b = 11, e = 3, m = 00111011 (m-message) then calculate private key d and cipher text C.

Soln. :

Use RSA Algorithm [Refer Section 2.12]

Step 1 : Prime numbers $a = 3, \quad b = 11$

Step 2 : $n = a * b = 33$

Step 3 : $\phi(n) = (a - 1) * (b - 1)$

$= (3 - 1) * (11 - 1)$

$= 2 * 10$

$= 20$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ (n)) = 1

$\gcd(e, 20) = 1$

$\gcd(3, 20) = 1$

$e = 3$ is given.

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

$ed \bmod \phi(n) = 1$

$3 * d \bmod 20 = 1$

$$d = \frac{(\phi(n) * i) + 1}{e}$$

Find d such that it is divisible by e.

Where $i = 1$ to 100

$$d = \frac{(20 \times i) + 1}{3}$$

$$= \frac{(20 \times i) + 1}{3} = \frac{21}{3} = 7 \qquad \text{Where } i = 1$$

$d = 7$

Step 6 : Public key = {e, n} = {3, 33}

Private Key = {d, n} = {7, 33}

Step 7 : Calculate cipher text message for given plain text message.

Plain text message given in binary 00111011 which can be written as 59

Binary to decimal conversion

00111011 ⇒ 59 (P = 59)

$$C = P^e \bmod n \text{ where } p < n$$

$$= 59^3 \bmod 33 - [59^2 \bmod 33] * [59 \bmod 33] \bmod 33$$

$$= 3481 \bmod 33 * [59 \bmod 33] \bmod 33$$

$$C = [16 * 26] \bmod 33$$

$$C = 20$$

Step 8 : Calculate plain text message.

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

$$= 20^7 \bmod 33$$

$$P = [20^4 \bmod 33] * [20^3 \bmod 33] \bmod 33$$

$$= [20^2 \bmod 33] * [20^2 \bmod 33] * [20^2 \bmod 33] * [20^1 \bmod 33] \bmod 33$$

$$= [400 \bmod 33] * [400 \bmod 33] * [400 \bmod 33] * [20 \bmod 33] \bmod 33$$

$$= [4] * [4] * [4] * [20] \bmod 33$$

$$= 1280 \bmod 33$$

$$P = 26$$

Ex. 2.12.2 : Calculate cipher text using RSA algorithm given data as follows : Prime numbers p, q as 7, 17 respectively and plain text message is to be send is 10.

Soln. :

By using RSA Algorithm : [Refer Section 2.12]

Step 1 : Prime numbers are 7 and 17 a = 7, b = 17

Step 2 : n = a * b = 7 * 17 = 119.

Step 3 : $\phi(n) = (a - 1) * (b - 1) = (7 - 1) * (17 - 1) = 6 * 16 = 96$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ(n)) = 1

If we select e = 3 then it is not relatively prime $\phi(n) = 96$ because

$$3 = 1 * 3$$

$$96 = 2 * 2 * 2 * 2 * 2 * 3$$

gcd must be 1.

We select e as 5 (gcd must be 1)

$$5 = 1 * 5$$

gcd (5, 96) = 1

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

$$ed \bmod \phi(n) = 1$$

$$5 * d \bmod 96 = 1$$

Using RSA algorithm

$$d = \left(\frac{(\phi(n) * i) + 1}{5}\right)$$

where i = 1 to 9 = $\frac{(96 * 1) + 1}{5} = 19.4$

d must be completely divisible by 'e'.

$$= \frac{(96 * 2) + 1}{5} = 38.6 = \frac{(96 * 3) + 1}{5}$$

$$= 57.8 = \frac{(96 * 4) + 1}{5} = 77$$

$$d = 77$$

Step 6 : Public key = $\{e, n\} = \{5, 119\}$

Private key = $\{d, n\} = \{77, 119\}$

Step 7 : Calculate cipher text message for given plain text message m = 10.

Plain text denoted as p = 10 (m denoted as p)

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

$$= 10^5 \bmod 119$$

It can be represented as

$$10^5 \bmod 119 = [10^3 \bmod 119] * [10^2 \bmod 119] \bmod 119$$

$$= [1000 \bmod 119] * [100 \bmod 119] \bmod 119$$

$$= 100000 \bmod 119$$

$$C = 40$$

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 40 to the receiver then receiver can calculate plain text p.

$$P = C^d \bmod n = 40^{77} \bmod 119$$

Now represent $40^{77} \bmod 119$ as mention above it will results p as 10.

Because decryption process always yields original message / plain text

$\therefore P = 40^{77} \bmod 119 = 10$

$P = 10$

Ex. 2.12.3 : Calculate cipher text using RSA algorithm given data is as follows : Prime numbers P, Q as 13, 17 and the plain text to be send is 12. Assume public key e as 19.

Soln. :

Using RSA Algorithm [Refer Section 2.12]

Step 1 : P and Q denoted as a and b in our algorithm

$a = 13, \quad b = 17$

Step 2 : $n = a * b = 13 * 17 = 221.$

Step 3 : $\phi(n) = (a - 1) * (b - 1)$

$= (13 - 1) * (17 - 1)$

$= 12 * 16$

$= 192$

Step 4 : Select e such that it is relatively prime to ϕ (n) e is given as 19.

Step 5 : Calculate d such that,

$$d = e^{-1} \bmod \phi(n)$$

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

$$d = \frac{(\phi(n) * i) + 1}{e} \quad \text{where } i = 1 \text{ to } 9$$

$$= \frac{(192 * 1) + 1}{19} = 10.1 = \frac{(192 * 2) + 1}{19} 20.2$$

$$= \frac{(192 * 3) + 1}{19} = 30.3$$

$$= \frac{(192 * 4) + 1}{19} = 40.4 = \frac{(192 * 5) + 1}{19} = 50.5$$

$$= \frac{(192 * 6) + 1}{19} = 60.6 = \frac{(192 * 7) + 1}{19}$$

$$= 70.7 = \frac{(192 * 8) + 1}{19} = 80.8$$

$$= \frac{(192 * 9) + 1}{19} = 91$$

$d = 91$

Step 6 :

Public key = {e, n} = {19, 221}

Private key = {d, n} = {91, 221}

Step 7 : Calculate cipher text c for given plain text message 12.

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

$$= 12^{10} \bmod 221 = [12^{10} \bmod 221] * [12^5 \bmod 221] * [12^4 \bmod 221]$$

$$= [12^5 \bmod 221] * [12^5 \bmod 221] * [12^5 \bmod 221] * [12^4 \bmod 221] \bmod 221$$

$$= [207] * [207] * [207] * [183] \bmod 221$$

$$C = 181$$

Step 8 : Send c = 181 to receiver as if required for decryption to obtain original plain text p.

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

$$= 181^{91} \bmod 221$$

This yields value of original plain text message i.e. 12

$$P = 12$$

Ex. 2.12.4 : In public key cryptosystem given N = 187 and encryption key (E) as = 17. Find out corresponding private key (D).

Soln. :

RSA Algorithm [Refer Section 2.12]

Step 1 : Select two large random prime numbers a and b. if we select a = 17 and b = 11 which results n = 187.

$n = a * b = 17 * 11 = 187.$

Step 2 : Calculate $\phi(n) = (a - 1)\ (b - 1)$

$$= (17 - 1)\ (11 - 1) = 16 * 10 = 160$$

Step 3 : Select e such that it is relatively prime to ϕ (n) and less than ϕ (n). But it is given in problem statement that e = 17.

Step 4 : Calculate d such that,

$$d = e^{-1} \bmod \phi(n)$$

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

$$d = \frac{(\phi(n) * i) + 1}{e} \quad \text{where } i = 1 \text{ to } 20$$

$$= \frac{(160 * 1) + 1}{17} = 9.4 = \frac{(160 * 2) + 1}{17}$$

$$= 18.8 = \frac{(160 * 3) + 1}{17} = 28.2$$

$$= \frac{(160 * 4) + 1}{17} = 37.70 = \frac{(160 * 5) + 1}{17}$$

$$d = 47.11 = \frac{(160 * 6) + 1}{17} = 56.52$$

$$= \frac{(160 * 7) + 1}{17} = 65.94 = \frac{(160 * 8) + 1}{17}$$

$$= 75.35 = \frac{(160 * 9) + 1}{17} = 84.76$$

$$= \frac{(160 * 12) + 1}{17} = 113$$

d = 113

Ex. 2.12.5 : Using the RSA algorithm encrypt the following :

(i) p = 3 , q = 11, e = 7, M = 12

(ii) p = 7 , q = 11, e = 17, M = 25

(iii) Find the corresponding ds for (i) and (ii) and decrypt the ciphertexts.

Soln. :

Use RSA Algorithm [Refer Section 2.12]

(i) Consider p as *a* and q as *b* as per our notations for prime numbers.

Step 1 : Prime numbers a = 3, b = 11

Step 2 : n = a * b = 33

Step 3 : $\phi(n) = (a - 1) * (b - 1)$

$= (3 - 1) * (11 - 1) = 2 * 10 = 20$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ (n)) = 1

gcd (e, 20) = 1

gcd (7, 20) = 1

e = 7 is given.

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

$ed \bmod \phi(n) = 1$

$7 * d \bmod 20 = 1$

$$d = \frac{(\phi(n) * i) + 1}{e} \quad \text{Where } i = 1 \text{ to } 100$$

Find d such that it is divisible by e.

Consider i = 1 you can continue till d will get integer value, Q(n) = 20 and e = 7

$d = ((20 * 1) + 1)/7 = 21/7 = 3$

d = 3

Step 6 : Public key = {e, n} = {7, 33}

Private key = {d, n} = {3, 33}

Step 7 : Calculate cipher text message for given plain text message.

Plain text message given is M = 12 we consider M as i.e. P = 12

$C = p^e \bmod n$ where $p < n = 12^7 \bmod 33$

$C = 12$

Step 8 : Calculate plain text message.

$P = c^d \bmod n = 12^3 \bmod 33$

$P = 12$

$P = 12$

When we convert plain text message into cipher text the corresponding cipher text yields the same plain text.

(ii) p = 7 , q = 11, e = 17, M = 25

By using RSA Algorithm : [Refer Section 2.12]

Step 1 : Prime numbers are 7 and 11 as per our notations a = 7, b = 11

Step 2 : n = a * b = 7 * 11 = 77.

Step 3 : $\phi(n) = (a-1) * (b-1) = (7-1) * (11-1) = 6 * 10 = 60$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ(n)) = 1

e is given as 17

gcd (17,60)= 1 (gcd must be 1)

Step 5 : Calculate d such that

$d = e^{-1} \bmod \phi(n)$

$ed \bmod \phi(n) = 1$

$17 * d \bmod = 1$

Using RSA algorithm

$$d = \frac{(\phi(n) * i) + 1}{e} \text{ where } i = 1 \text{ to } 100 = ((60*1)+1)/17) = 3.58$$

d must be completely divisible by 'e'.

= After putting value of i = 15 into above formula we got value of d

= ((60*15)+1)/ 17) = 53

d = 53

Step 6 : Public key = {e, n} = {17, 77}

Private key = {d, n} = {53, 77}

Step 7 : Calculate cipher text message for given plain text message M = 25.

Plain text denoted as P = 25 (m denoted as p)

$$C = P^e \bmod n = 25^{17} \bmod 77$$

It can be represented as

$$C = 9$$

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 9 to the receiver then receiver can calculate plain text p.

$$P = C^d \bmod n = 9^{53} \bmod 77$$

$$P = 25$$

Decryption process always yields original plain text message

$$\mathbf{P = 25}$$

(iii) Find the corresponding ds for (i) and (ii) and decrypt the ciphertexts

Decryption key for question (i) is d =3 and for question (ii) is d = 53 which will decrypt the message successfully.

Ex. 2.12.6 : In an RSA system the public key (e, n) of user A is defined as (7, 119). Calculate $\phi(n)$and private key d. What is the cipher text when you encrypt message m =10, using the public key?

Soln. :

By using RSA Algorithm : [Refer Section 2.12]

In the problem statement Public key (e, n) = (7,119) is given, means we don't need to select e and n. if we select following prime numbers which results n = 119 as shown below.

Step 1 : Prime numbers are 7 and 17 a = 7, b = 17

Step 2 : n = a * b = 7 * 17 = 119.

Step 3 : $\phi(n) = (a - 1) * (b - 1)$

$= (7 - 1) * (17 - 1) = 6 * 16 = 96$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. gcd(e, ϕ(n)) = 1

e = 7 as per problem statement.

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

$$ed \bmod \phi(n) = 1$$

$$7 * d \bmod 96 = 1$$

Using RSA algorithm

$$d = ((\phi(n) * i) + 1)/7 \quad \text{where } i = 1 \text{ to } 100$$

$$= (96*1 + 1)/7 = 13.85$$

d must be completely divisible by 'e'.

$= ((96*2) + 1)/7 = 21.57$

$= ((96*3) + 1)/7 = 48.28$

$= ((96*4) + 1)/7 = 55$

$d = 55$

Step 6 : Public key $= \{e, n\} = \{7, 119\}$

Private key $= \{d, n\} = \{55, 119\}$

Step 7 : Calculate cipher text message for given plain text message m = 10.

Plain text denoted as p = 10 (m denoted as p)

$C = P^e \bmod n = 10^7 \bmod 119$

$= 10000000 \bmod 119$

$C = 73$

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 73 to the receiver then receiver can calculate plain text p.

$P = C^d \bmod n$

$= 73^{55} \bmod 119$

Now represent $73^{55} \bmod 119$ as mention above it will results p as 10.

Because decryption process always yields original message / plain text

$\therefore \quad P = 73^{55} \bmod 119 = 10$

$P = 10$

Ex. 2.12.7 : Perform encryption using the RSA algorithm

p = 3, q = 11(two random numbers).

e(encryption key) = 7

M(plaintext message) = 5

Soln. :

Using RSA algorithm

p = 3, q = 11, e = 7 and M = 5

Step 1 : Prime number p = 3, q = 11

Step 2 : $n = p * q = 3 \times 11 = 33$

Step 3 : $\phi(n) = (p-1)*(q-1) = (3-1)*(11-1) = 2*10$

$\phi(n) = 20$

Step 4 : Select e such that it is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$

gcd (e, 20) = 1

gcd (7, 20) = 1

e = 7 is given.

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

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

$7 * d \bmod 20 = 1$

$$d = \frac{(\phi(n) * i) + 1}{e}$$

Find d such that is divisible by e.

where, i = 1 to 100

$$d = \frac{(20 \times i) + 1}{7} \quad \text{where } i = 1;$$

$$= \frac{20+1}{7} = \frac{21}{7} = 3$$

d = 3

Step 6 : Public key = {e, n} = {7, 33}

Private key = {d, n} = {3, 33}

Step 7 : Calculate cipher text message for given plain text message plain text M = 5.

$C = M^e \bmod n$ where $M < n$

$= 5^7 \bmod 33 = (5^5 \bmod 33) * (5^2 * \bmod 33) * \bmod 33$

$= (5^3 \bmod 33) * (5^2 * \bmod 33) * (5^2 * \bmod 33) * \bmod 33$

$= (125 \bmod 33) * (25 \bmod 33) * (25 \bmod 33) * \bmod 33$

$= (26 * 25 * 25) * \bmod 33 = 16250 * \bmod 33 = 14$

c = 14

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 14 to the receiver then receiver can calculate plain text p.

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

$$14^3 \bmod 33$$

– Now represent $14^3 \bmod 33$ as mention above it will results p as 5.

Because decryption process always yields original message / plain text

$$\therefore \quad P = 14^3 \bmod 33 = 5$$

Ex. 2.12.8 : The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and Calculate the ciphertext if the given plaintext is 7.

Soln. :

Using RSA algorithm

Given : $a = 11,\ b = 3,\ e = 3$ and plain text $P = 7$

Step 1 : Prime number $a = 11, b = 3$

Step 2 : $n = a * b = 11 * 3 = 33$

Step 3 : $\phi(n) = (a-1) * (b-1) = (11-1) * (3-1) = 10 * 2 = 20$

Step 4 : Select e such that it is relatively prime to $\phi(n)$ i.e. $\gcd(e, \phi(n)) = 1$

$$\gcd(e, 20) = 1$$

$$\gcd(3, 20) = 1$$

$$e = 3 \text{ is given.}$$

Step 5 : Calculate d such that

$$d = e^{-1} \bmod \phi(n)$$

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

$$3 * d \bmod 20 = 1$$

$$d = \frac{(\phi(n) * i) + 1}{e}$$

Find d such that it is divisible by e

where $i = 1$ to 100

$$d = \frac{(20 * i) + 1}{3} \quad \text{where } i = 1;$$

$$d = \frac{(20 \times i) + 1}{3} = \frac{21}{3} = 7$$

$$d = 7$$

Step 6 : Public key = {e, n} = {3, 33}

Private key = {d, n} = {7, 33}

Step 7 : Calculate cipher text message for given plain text message.

Plain text message = 7

$$c = P^e \bmod n \text{ where } P < n$$

$$= 7^3 \bmod 33 = [7^2 \bmod 33] * [7 \bmod 33] * \bmod 33$$

$$= [49 \bmod 33] * [7 \bmod 33] * \bmod 33$$

$$= [16 * 7] \bmod 33$$

$$c = 13$$

so, cipher text = 3

Step 8 : Now calculate plain text P required at the time of decryption. Once sender sends 13 to the receiver then receiver can calculate plain text p.

$$P = C^d \bmod n = 13^7 \bmod 33$$

Now represent $14^3 \bmod 33$ as mention above it will results p as 7.

Because decryption process always yields original message / plain text

$$\therefore \quad \mathbf{P = 13^7 \bmod 33 = 7}$$

2.12.2 The Security of RSA

Q. 2.12.3 Which cryptanalytic attack can occur on RSA algorithm? (Refer section 2.12.2) **(4 Marks)**

Q. 2.12.4 List the possible approaches to attacking it. (Refer section 2.12.2) **(4 Marks)**

Q. 2.12.5 Elaborate various kinds of attacks on RSA algorithm. (Refer section 2.12.2) **(6 Marks)**

There are four possible attacks on RSA as follows,

1. **Brute force Attack :** Hacker tries all possible private keys.
2. **Mathematical Attacks :** Hackers attacks on n i.e. tries to factorize the product of two prime numbers.
3. **Timing Attacks :** It totally depends on running time of decryption algorithm.
4. **Chosen Cipher text Attack :** Hacker tries to attack on the properties of RSA algorithm.

2.13 The Knapsack Algorithm

- Public-Key cryptography was invented in by Martin Hellman, Whitfield Diffie and Ralph Merkle in the 1970s.
- Public-key cryptography needs two keys. One key is used for to encrypt a message or code and this is "public" key so anyone can access or use it. The second key used for to decrypt or decode the message. This decryption code is kept private or secret so only the person who knows the key can decode the message. It is also possible for the person with the private key to encrypt a code or massage with the private key, then anyone having the public key can decrypt the message, although this seems to be of little use if you are trying to keep something secret!