UNIT 4: Network Security (Page-5)

13.8.1. The RSA Algorithm

As a matter of fact, RSA is the most widely used public key algorithm. It is named after its creators – Rivest, Shamir and Adleman. The principle of RSA is simple. It is based upon a fact that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back. The algorithm is as follows :

(i) Take two very large prime numbers A and B of equal lengths and obtain their product (N).

Therefore, $N = A \times B$ ... (13.1)

(ii) Subtract 1 from A as well as B and take the product T.

Therefore, $T = (A - 1)(B - 1)$

(iii) Choose the public key (E) which is a randomly chosen number such that it has no common factors with T.

(iv) Obtain the private key (D) as under :

$$D = E^{-1} \bmod T \quad \ldots (13.2)$$

(v) The rule for encryption of a block of plaintext M into ciphertext (C) is as under :

$$C = M^E \bmod N \quad \ldots (13.3)$$

This means that the plaintext M is raised to the power of E (public key) and then divided by N. The mod term in equation (13.3) indicates that the remainder of this division is sent as the ciphertext C as shown in figure 13.11.

(vi) The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule.

$$M = C^D \bmod N \quad \ldots (13.4)$$

The encryption and decryption process using the RSA algorithm is illustrated diagrammatically in figure 13.11.

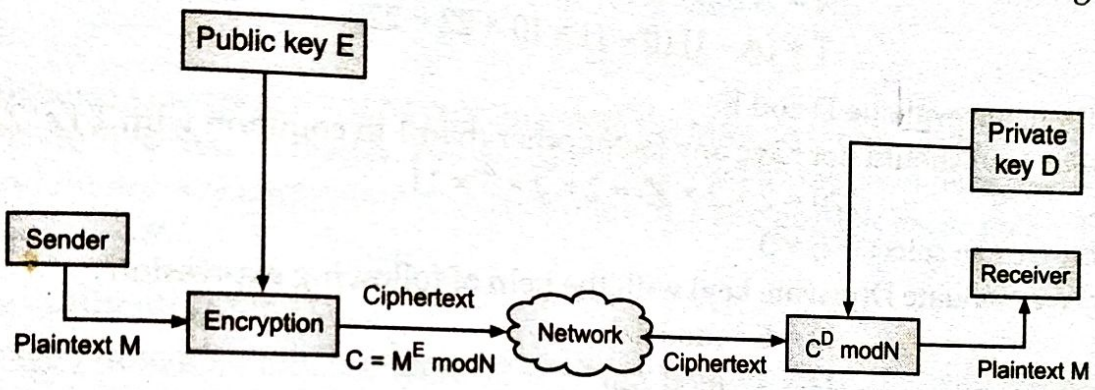

Fig. 13.11 Encryption and decryption in RSA

Security of RSA

The security of RSA is decided by the ability of the hacker computer to factorize numbers. RSA provides a very good security since it uses very large prime numbers *A* and *B* their product is so large that an attempt to break the code using even the fastest computer shall require a few years. However, as the computers improve all the time, the time required to break the code will also reduce and one has to use larger keys. However, then the time needed for encryption and decryption will also increase. A key size of 768 bits is recommended for the personal use, 1024 bits for the corporate use and 2048 bits for extremely valuable keys. The user's key must be changed regularly in order to enhance security.

EXAMPLE 13.1. If $N = 119$, public key E = 5, and private key D = 77, then demonstrate how to send the character *F* using RSA.

Solution : The character *F* is the sixth character in alphabets. Hence, we can represent it by 6.

Therefore, as per RSA, the encryption is given by,

$$C = M^E \bmod N$$
$$= 6^5 \bmod 119$$

Now, the process of getting C is as under :

$$6^5 = 7776$$

Therefore, $C = 7776 \div 119$

Because the quotient of this division is 65 and remainder is 41, we take C = 41.

This number is sent to the receiver as ciphertext.

The receiver uses the decryption algorithm to get the plaintext M back as under :

$$M = C^D \bmod N$$

$$M = 41^{77} \bmod 119$$

$M = 6$ (which is the original number). Ans.

EXAMPLE 13.2. Select suitable values of *A*, *B*, *N*, *D* and *E* and demonstrate the encryption and decryption procedures used in RSA algorithm.

Solution :

(i) First, let us select *A* and *B*.

Let the two prime numbers *A* and *B* be as under :

$$A = 11, \quad B = 23$$

(ii) Then, we evaluate N and T.

$$N = A \times B = 11 \times 23 = 253$$

$$T = (A - 1)(B - 1) = 10 \times 22 = 220.$$

(iii) Then, we evaluate D and E.

E(public key) should not have any factor other than 1 in common with T i.e. 220.

Thus, $220 = 2 \times 2 \times 55 = 2 \times 2 \times 5 \times 11$

Hence, we can select $E = 3$

Now, we evaluate D(private key) with the help of following expression :

$$D = E^{-1} \bmod T$$

Therefore, $D = 3^{-1} \bmod 220$

Now, D can be calculated as under :

Next, we find the (multiple of 220 + 1) which is divisible by 3. Then, we divide that number by 3 and select the quotient of this division as *D*.

Therefore, $(220 \times 1) + 1 = 221$ not divisible by 3

$(220 \times 2) + 1 = 441$ it is divisible by 3.

Therefore, $\frac{441}{3} = 147$

or $D = 147$

(iv) Now, let us carryout encryption.

Let the letter I is to be sent.

Therefore, Plaintext $M = 9$, as *F* is the ninth alphabet.

Hence, Ciphertext $C = M^E \bmod N$

or $C = 9^3 \bmod 221$

Hence, $C = 729 \bmod 221$

or $C = \frac{729}{221}$

$Q = 3$ remainder $= 66$

Therefore, Ciphertext $C = 66$

This number is sent to the receiver.

(v) Finally, let us carryout decryption.

Plaintext $M = C^D \bmod N = 66^{147} \bmod 221 = 9$.

Thus, the original number is obtained.