**T.Y. B.Tech EE (2020-21)**

**Trimester: VII Subject: Communication Protocols**

**Name: Class:**

**Roll No.: Batch:**

**Experiment No.: 07**

**Name of the Experiment**: Study of RSA algorithm.

**Performed on:**

**Submitted on:**

**Aim:** To study the RSA encryption algorithm.

**Prerequisite:**

Basic knowledge of data communication.

**Objectives:**

* To understand how data encryption and decryption works.
* To learn logic behind RSA algorithm.

**Theory:**

**What is Data Encryption?**

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses an encryption algorithm to generate ciphertext that can only be read if decrypted.

**The Need for Encryption**

Beyond the obvious benefit of protecting private information from being stolen or compromised, encryption also provides a means of proving that information is authentic and comes from the point of origin it claims to come from. It can be used to verify the origin of a message and confirm that it hasn't been altered during transmission.

**RSA Algorithm** (Rivest-Shamir-Adleman)

RSA is one of the most successful, asymmetric encryption systems today. RSA is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. The idea of RSA is based on the fact that it is difficult to factorize a large integer.

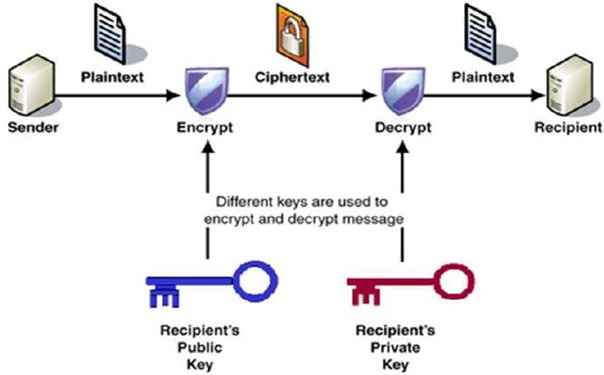
Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. As the name suggests, the private key must be kept secret.

The public key consists of two numbers where one number is multiplication of two large prime numbers and the private key is also derived from the same two prime numbers. Under RSA encryption, once data or a message has been turned into a cipher text with a public key, it can only be decrypted by the private key from the same key pair. Private keys are composed of d and n. We already know n, and the following equation is used to find d:

d =1/e mod λ(n). And public keys are made up of a prime number e, as well as n. The number e can be anything between 1 and the value for λ(n).

RSA encryption can be used by previously unknown parties to securely send data between themselves as shown below:

* First, they each need to set up their own key pairs and share the public key with one another. The two entities need to keep their private keys secret in order for their communications to remain secure.
* Once the sender has the public key of their recipient, they can use it to encrypt the data that they want to keep secure. Once it has been encrypted with a public key, it can only be decrypted by the private key from the same key pair. Even the same public key can’t be used to decrypt the data. This is due to the properties of trapdoor functions.
* When the recipient receives the encrypted message, they use their private key to access the data. If the recipient wants to return communications in a secure way, they can then encrypt their message with the public key of the party they are communicating with. Again, once it has been encrypted with the public key, the only way that the information can be accessed is through the matching private key.



**Key Generation Algorithm:**

1. Generate two large random primes, p and q, of approximately equal size such that their product n=pq is of the required bit length, e.g. 1024 bits.
2. Compute n=pq and ϕ=(p−1)(q−1).
3. Choose a random integer e, 1<e<ϕ, such that gcd(e,ϕ)=1.
4. Compute the secret exponent d, 1<d<ϕ, such that ed≡1modϕ.
5. The public key is (n,e) and the private key (d,p,q). Keep all the values d, p, q and ϕ secret.

**Encryption:**

1. Obtains the recipient's public key (n,e).
2. Represents the plaintext message as an integer m with 0<M<n.
3. Computes the ciphertext C=Me mod N
4. Sends the ciphertext C to the recipient.

**Decryption:**

1. Uses his private key (n,d) to compute M=Cd mod N
2. Extracts the plaintext from the message representative M.

**Conclusion:**

---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Post Lab Questions:**

1. Describe the symmetric and asymmetric key cryptography?
2. Enlist and briefly describe the important features of five most popular algorithms for cryptography.
3. Compare RSA algorithm with any other cryptography algorithms