International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Secure Data Communication using Cryptography

Ch.Sri Lakshmi, Y.Roshini, M.Sukanya, M.Hema sai sree, S.Jyothika

Abstract*: Any type of digital information is called as data. In today's world, precarious data are growing and used in communication over internet. Hence, data security is most important factor for the internet users. The best solution is to use some cryptography algorithms which encrypts data in some cipher and transmit it over the internet and again decrypted to genuine data. Cryptography is eternal. The field of cryptography manages the technique for passing on information safely. The objective is to permit the expected recipients to get the message appropriately while interfere with snoopers from understanding the message. Key arrangement layout allows communicating parties to establish a mutual cipher key. The situation of present day of data security framework incorporates secrecy, legitimacy, trustworthiness, non-repudiation. This paper introduces a improved system for securing text-data communication benefiting the use of RSA algorithm. It is the public-key cryptosystem and is mainly used for secure data transmission[1].

Keywords* : cryptography, RSA algorithm, cipher text, public key, private key.

I. INTRODUCTION

The methodology of concealing the gist of messages is called Cryptography. The word cryptography is from the Greek word "Kryptos", means hidden, and other word "graphikos" which means writing. Cryptography is the shielding strategy of information from the unapproved party by changing over into the non-readable structure. The principle motivation behind cryptography is keeping up the security of the information from outsider. In other words we can say that Cryptography as the study of makingthe transmitted information safe. It gives information encryption to verify correspondence .To transmit, encryption has to be applied and decryption procedure is applied to get the encoded data.

A message is called plain text and can take any form of, executable programs, characters, pictures, numerical data,or any other kind of information [4]. The process of masking a message so as to conceal its substance can be defined as Encryption. Encrypted message is called as cipher text. Decryption is the process of converting cipher text back into original text.

The cryptography was classified into two types:

- public key cryptography
- private key cryptography[5].

A. Public key Cryptography

Public key cryptography is asymmetric scheme that uses both of the keys for encryption. Public key used for encryption of data while private key (secret key) is used for decryption. By keeping private key as secret, we have to share our public key. Any person can encrypt information with our public key, which can be read by ourselves only. It is mathematically impossible to decode the private key from the public key. If anyone knows the public key can encrypt, but cannot decrypt the information. The person who has the corresponding private key can decrypt the information. The most advantage of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Rivest Shamir Adleman, Digital Signature Algorithm. In public-key cryptography, the key size is proportional to security of the cipher text.

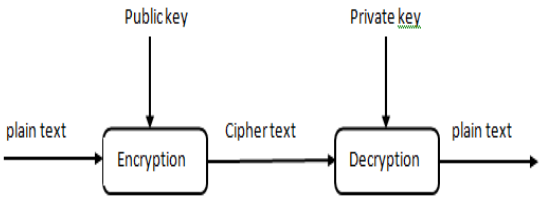

Fig. 1. Public key cryptography

B. Private key cryptography

Private key Cryptography is also called as Secret key cryptography. In this method, only a single key is used for encryption and decryption.

Revised Manuscript Received on April 11, 2020.
* Correspondence Author
Ch.Sri Lakshmi *, Assistant Professor in ECE, PVPSIT, Kanuru, Vijayawada, India. Email: chandana.463@gmail.com
Y.Roshini, ECE student, PVPSIT, Kanuru, Vijayawada, India. Email: yelchuriroshini438@gmail.com
M.Sukanya, ECE student, PVPSIT, Kanuru, Vijayawada, India. Email: sukanya.medidhi@gmail.com
M.Hema sai sree, ECE student, PVPSIT, Kanuru, Vijayawada, India. Email: miriyalahemasaisree@gmail.com
S.Jyothika, ECE student, PVPSIT, Kanuru, Vijayawada, India. Email: jyothikasomana1999@gmail.com

That means, the key for both encrypting and decrypting the file has to be known to all recipients. Else, message could not be decrypted by conventional means. The user who wants to send the message uses one key to encrypt and transmits the encrypted data to recipient. The receiver uses the same key to decrypt the message and recover the original text. Because a single key is used for both encryption and decryption, this is also called symmetric encryption. From this type of cryptography, it is clear that the key must be known to both sender and the receiver. The difficulty arises with the distribution of the key. The Data Encryption Standard is a conventional cryptosystem that isused by the United States government. Other examples are Advanced Encryption Standard (AES), blowfish, Rivest ciphers, etc.

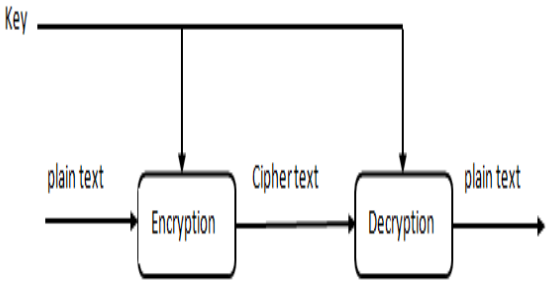

Fig. 2. Private key cryptography

II. DESIGN AND IMPLEMENTATION

The proposed design employs encryption and decryption using RSA algorithm. This method is used for those who seek the ultimate in private communication.

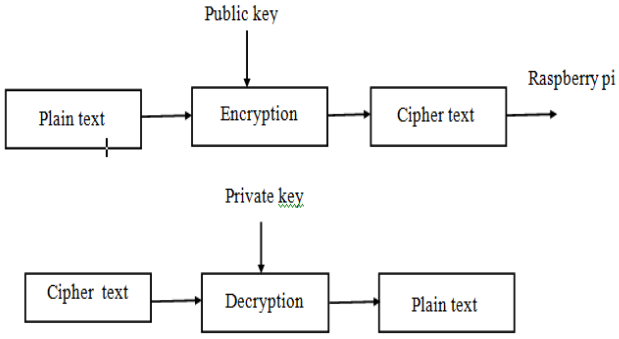

Fig. 3. Block diagram of proposed model

A. RSA Algorithm

This algorithm is based on Chinese Remainder Theorem (factoring two large prime numbers). It undergoes three steps: Key Generation, Encryption and Decryption [6].

1. Key Generation:

- Consider two random primes, *p* and *q*, of same size and the product n = p*q is the numberwhich has required number of bits.
- Compute phi(φ) = (p-1)*(q-1).
- Select an integer *e*which satisfies 1 < e < phi, and gcd(e, phi) = 1.
- Calculate the secret exponent *d*which satisfies, 1 < d < phi and also ed ≡ 1 (mod phi).
- The public key is given by (n, e) and the private key is represented by (n, d). We need to keep all the values phi, q, p and das secret.

2. Encryption:

- The sender has to know the public key(n,e) of respective receiver to whom we need to send data.
- Let us denote the message or plain text as 'm', which is a positive integer.
- Now the sender determines the cipher text using $c = m^e \bmod n$.
- Then he transmits the cipher text, cto recipient.

3. Decryption:

- Recipient uses his own private key (n, d) to find $m = c^d \bmod n$.
- Extracts plaintext from the message representative m.

B. Sending and Receiving

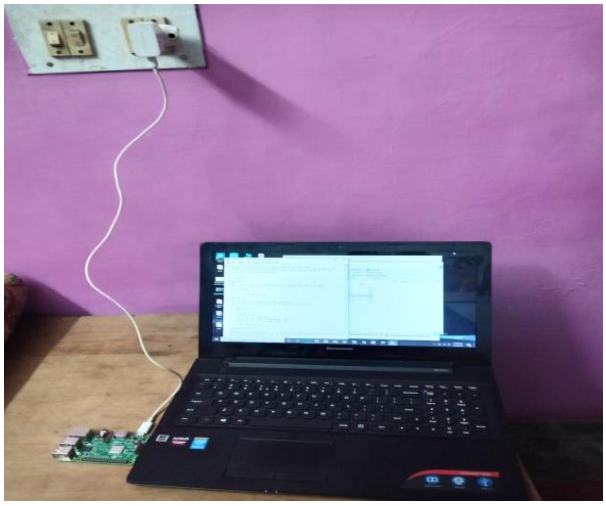

Fig. 4. Experimental Setup

1) The receiver will generate the set of keys and the public key can be shared to everyone.
2) The sender then encrypts the data with use of receiver's public key and transmitted to receiver.
3) The receiver then decrypts the cipher text using his private key. The original message can be retrieved only with the help of private key.

The proposed system uses Python software to encrypt the text message and the cipher text is transmitted to Raspberry Pi, in which the decryption mechanism is done.

Hiding of data is uni-directional. i.e. message encoded by the sender can only be decrypted using private key by the recipient[7]. This technique is independent of size of message. The proposed model encrypts large messages and is robust against attacks, since the factorization of large numbers is highly complex and less possible.

III. SIMULATION RESULTS

We performed simulation(encryption) in Python 3.8 version, under Windows 10 with dual Core processor, 4GB RAM and decryption process is done using Python of same version, under Raspberry Pi with 1GB RAM.

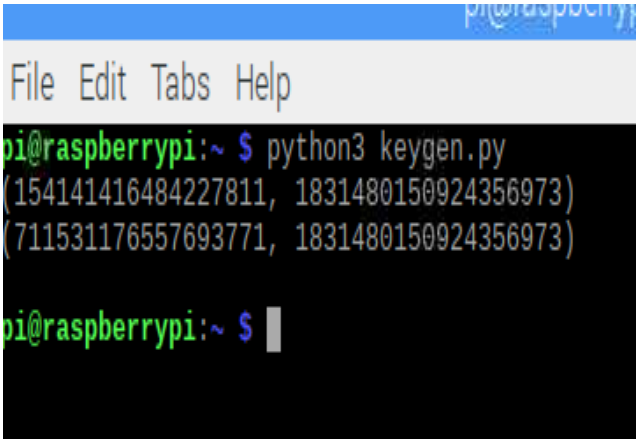

Fig. 5. Key Generation

```
========== RESTART: E:\rsa final\rsa_enc.py ==========
Enter public key:
154141416484227811
1831480150924356973
(154141416484227811, 1831480150924356973)
Please write your message:
> commnication

Original message:

commnication

Encrypted message:
799002253990431486_6043604695348_1716996312013867614_1716996312013867614_1263794
631370300541_519738699038684 57_799002253990431486_1039348897395690472_1082450111
216296761_519738699038684 57_6043604695348_1263794631370300541

>>>
```

Fig. 6. Encryption of message

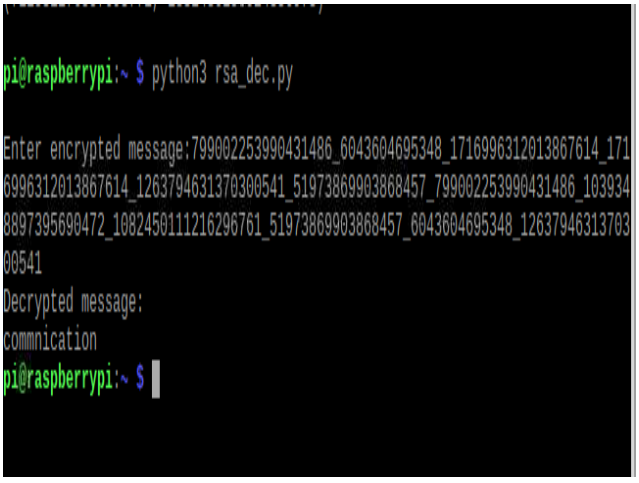

Fig. 7. Decryption of cipher text

IV. CONCLUSION

Since ancient times, man has found a desire in the ability to communicate covertly. In current computer systems, cryptography provides a strong, close basis for keeping data classified and for validating data indignity. This paper presented the security to information using a powerful cryptographic technique. This mechanism makes it impossible for intruders to stole the information when transmitted in an insecure channel. In other words, we can say that this design increases security in a simple way.

V. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

1. Moe Moe Myint, Aye Aye Cho , Soe Moe Myint, "A Study of RSA Algorithm in Cryptography", IJTSRD, 2019.
2. Jaya Jeswani, JoansMichael, Akash Singh, Joseph Selvanayagam, "Secure File Storage On Cloud Using Cryptography", IRJET, 2018.
3. Pooja Bhadauriya, Foram Suthar, Sumit Chaudhary, "A Novel Technique for Secure Communication in cryptography" IJAR, in Computer and Communication Engineering, 2017.
4. Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques", IJECS, 2017.
5. https://www.garykessler.net/library/crypto.html
6. B.Sarala, N.Pavani, "Secure Data Communication using Cryptography and Steganography Standards", IJEERT, 2015.
7. Arun Kumar Yadav, Gangadhar Tiwari , Madhusudhan Mishra, "Secret Communication using Public key Steganography", ICAIRE, 2014.
8. https://www.geeksforgeeks.org/python-programming-language/
9. Supriya, Gurpreet Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", IJCA, 2013.

AUTHORS PROFILE

Chandana Sri Lakshmi received the M.Tech, Degree in Electronics and Communication Engineering in the Specialization of Embedded Systems (ES) from the Jawaharlal Nehru Technological University (JNTUK), Kakinada. She is currently working as an Assistant Professor in the Department of Electronics and Communication at P.V.P. Siddhartha Institute of Technology, Vijayawada, India.

Yelchuri Roshini is pursuing Bachelor of Technology in the department of ECE at Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, India. She is a member of IETE Student forum and a Certified LabVIEW Associate Developer in National Instruments.

Medidhi Sukanya is pursuing Bachelor of Technology in the department of ECE at Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, India. She is a member of IETE Student forum.

Miriyala Hema sai sree is pursuing Bachelor of Technology in the department of ECE at Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, India. She is a member of IETE Student forum.

Somana Jyothika is pursuing Bachelor of Technology in the department of ECE at Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, India. She is a member of IETE Student forum.