International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206520

RSA Encryption and Decryption System

Neha Bansal, Sukhdeep Singh

Department of Computer Science Engineering, Institute of Technology, Bhaddal, Ropar, Punjab, India

Article Info
Volume 6, Issue 5
Page Number: 109-113
Publication Issue :
September-October-2020

Article History
Accepted : 20 Sep 2020
Published : 28 Sep 2020

ABSTRACT

For communication in the wireless networking, transmission of data over network sometimes is not safe. In such case security of network is one of the essential aspect in computer networking. Cryptography is antechnique of transforming an plaindata into encrypted one, and then retransform that encrypted data back to its plain (original) form. In this we authenticate the sender to whom you want to send that data file. There are two different techniques of cryptography, symmetric key cryptography (called public-key cryptography) algorithms and asymmetric key cryptography (called public-key cryptography) algorithms. There are also various algorithms for encrypted data using either public or private key or both. This paper describes RSA algorithm which first convert our data into other form and then encrypt it using RSA public key encryption at sender side & at receiver side, first it authenticate the receiver then decrypt the data/ file and convert into original form.

Keywords : Encryption, Symmetric Key Cryptography, Asymmetric Key Cryptography, RSA Encryption& Decryption, Key Distribution, RSA

I. INTRODUCTION

Due to greed, power, publicity or desire to access forbidden information, an unauthorized person may try to access our person information while we send our data over internet in wireless environment. Every day, many users generate data and send it over internet in many areas. So, communication over internet is important part in today life.When we set up network there should be high data securitydue to the growing threat of hackers trying to infect as many computers possible. So to avoid misuse of data, there is need of protecting the data/ file in such era. Network security involves the authentication of receiver and decrypts the data to right person. So cryptography algorithms are used for encrypting data and make it unreadable to understand and the only way to make it understand we can use key to decrypt data. There are various techniques for this purpose. We can use Hash function for this purpose can be used in which we use hash key for encrypting data and send it over internet. Same hash key is used to decrypt data over receiver. Other method, symmetric encryption key in which same key is used for decrypting the data. Sender first encrypts the data into cipher text using key and Receiver use the same key for decrypting the data. In the Asymmetric Key Encryption, different key are use at receiver end and also at sender end. The cryptography not only ensure the confidentiality but also ensure data-integrity, non-repudiated and authentication.

II. METHODS AND MATERIAL

Why Encryption?

With increase in demand of sending data over internet in wireless network, may be stolen by unauthorized person. Hackers always try to steal and reveal someone's personal information. The reason behind hacking is not to learn something but to take revenge by blackmailing to reveal their personal information to the world or sometimes it may be their greed. To avoid such things encryption techniques are used. The goal of encryption techniques are as:

1) **Authentication**: while sending message over internet wirelessly, Sender and receiver' identity should be verified.
2) **Data Confidentiality**: It ensures that unauthorized person is not able to gain access on the data. Only authorize persons are able to gain access on data.
3) **Integrity**: There is no change in the content of message while sending over wireless network. The correct message is received to receiver. There is no modification or amendment of data.
4) **Non- repudiated**: It ensures that sender is actually sending the data. He can't deny that he is not sending message.

Symmetric Key Cryptography

In this data is converted into other form which is not understood by anyone who does not how to decrypt it. In this cryptography same private key is used by both receiver and sender. Various algorithm are use in this like AES, DES, IDEA, which are block cipher. AES (Advance Encryption Standard) are like blocked cipher in which data is encrypted in block of electronic data with its secret key. During encryption it will be in the main memory.

Asymmetric Key Cryptography

As compared to symmetric key, in Asymmetric key cryptography we use two different key.one for encrypting the data at sender side and other at receiver side for decrypting the data. Sender send us public key for encryption of data and while encrypting the data it generate cipher text and also generate the private key. When sender sends the data at other end, it sends cipher key as well as private key for decryption of data. This cryptography technique resolves two problems of symmetric algorithms. One of the problem is key distribution i.e. two different users use same key which is distributed over network which compromises the security of data. Second one is digital signatures which ensure all the user that data is send by particular individual. So there is lack of authentication of receiver.Various algorithm are used for this purpose like RSA ,Diffie Hellman, XTR etc. XTR based on difficulties of solving discrete logarithm related problems in the finite field which make it more complex. In Diffie Hellman, it allows the two nodes to exchange data over an insecure medium it is also based on discrete algorithm problems. On the other hand if we consider RSA algorithm this algorithm is used both for encrypting the data as well as for digital signature. The key size for this RSA algorithm must be greater that 1024 bits to get reasonable security of exchange data over internet in wireless medium. In further section we how RSA algorithm works.

RSA Encryption & Decryption

RSA algorithm is public key encryption cryptography in which it generates two keys i.e. public key and private key. Public key is published to all other users hence all users know about this key while private key is kept with user or authenticate receiver only.RSA

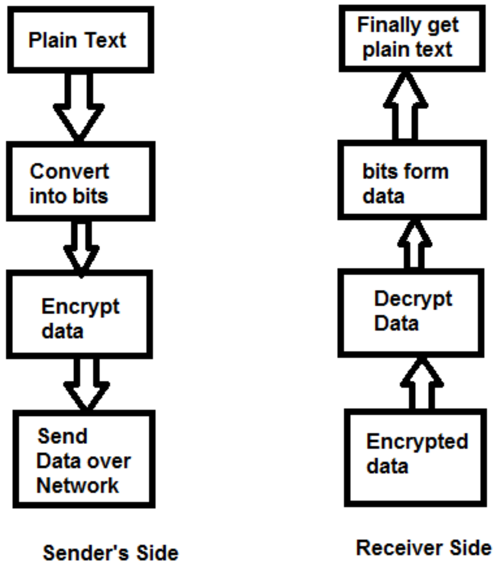
2048 encryption technique crypt the data of length up to 245 bytes. The most important advantage of using this key is that it is almost support on all hardware. Also it take less time to generate the key thus less CPU usage and as result less battery drainage. RSA Algorithm is generally based on idea that it generate two prime number which must be kept secret only for authenticate receiver. If any unauthorized person know about these prime numbers, that person can decode the message.

III. RESULTS AND DISCUSSION

Key Distribution:

Suppose that user (1) wants to send message to user(2) using RSA encryption, then user(1) uses the public key for encrypting the message. User(1) does not use his public key. For encrypting the message, user(1) use the public key of the user(2) i.e. user(1) must have knowledge of user(2)'s public key. For this, user(2) distribute his public key to the entire user. The sender (user1) who wants to send message to user(2), his public key which is already distributed over network. Thus using user(2)'s public key ,user(1) encrypt his message and send to user(2). Now at receiver end, if any unauthenticated user tries to decrypt this message, he is not able to encrypt that message because only public key is distributed over network. For decrypted the message, user need private key. Hence if any unauthorized person tries to do so, it indicates that you are not authorized user. This level of security is used in this method of key distribution. As private key is not distributed over network, data is safely decrypted by authenticate user only. At receiver end, receiver has to use his private key for decrypt the message. If private key is lost then it is not possible to decrypt message.

How RSA algorithm actually works:



The idea behind the RSA algorithm is that it is difficult to compute the prime factors for decrypting message. On the basis of prime factors generate by the client' private key, it generate the public key which is send over wireless network to all. Here in this case, private key is only at client end and which lead to secure transformation.

1) First of all, on receiver system, private key is generated by receiver. For this , he select any two prime Numbers. Receiver also choose RSA public key and generate his private key. Now at receiver end private key is generated.
2) If any sender wants to send message to receiver, first of all he has to obtain his public key which receiver has used or sending message. This key is distributed by the receiver over the network.
3) Sender who sends the message use receiver' public key and decrypt the message. In this case, he is not encryption of text message, first of all plain text message is converted into bits form i.e. 0010000100010111001001 then sender encrypt the message using public key for encryption. After encryption, send the crypted file over network with authenticate receiver.

4) At receiver end if any unknown person tries to access the data, due to encryption, he is not able to encrypt the message because he does not know about the private key. Private key is not distributed over network. So not possible for unauthorized user to decrypt the message.
5) When authorized receiver tries to see the actual message from encrypted one then he has to use his private key for encryption. First it verify the user then show him the encrypted message. Using private key when he tries to decrypt the message, first message is convert into bits form as security is done at physical layer. From that bits form, original data is extracted. Thus receiver is able to read the message.

Key Selection:

The security of this encryption technique relies on the fact of calculating the prime numbers. As computation decrease, less effective the algorithm works. To make the algorithm more effective computation power must be high. The encryption of data/ message is completely depending on the Key size which is used for encrypting the message. Higher the key size, it increases the exponential terms which lead to decrease in computation power lead to less effective algorithm. RSA keys are1024 or 2048 or 4096-bits long. The National Institute of Standards and Technology (NIST) has published some standards and guidance for which cryptography technique is used for protecting for sensitive and unclassified information. Using RSA-1024 key size, security is less as it is no longer fully secured against all the attacks or also it is says that 1024 bits RSA may be cracked by hackers in the near future. They predict that the key with longer size may affect the performance i.e. it take long time to process data but too small size key may or may not provide adequate security. They predict that 1024-bits is good till 2010 while 2048-bits is good till 2030 after that 3072-bits is needed. This is completely up to their prediction. So in this paper RSA-2048 is used for encrypting the message.

IV.CONCLUSION

A public key encryption technique is generally used for this security in the network. During the lifetime of cryptographic information, the information is either “in transit” (e.g., is inthe process of distributed nature information is available to theauthorized communications users for use) or is “at rest” (e.g., theInformation is stored in storage). In either case, there is need of protecting the key material. However, which protection mechanism is used may vary with time. With increase in development technique various ways of hacking are developed.Although there are several methods of protecting our data, these methods are not provide same security for different data. So it is completely upto which type is data is selected for sending, then protection mechanism is used. In addition, the mechanisms used donot guarantee for protection of data. The implementation and the associated keymanagement need to provide adequate security to prevent any attack from beingsuccessful.

V. FUTURE SCOPE

In today’s world, protection of data is most critical. Encryption is the most reliable way to secure data in wireless data transmission. The sensitive dataof National security agencies and major financial institutions have protected using various mechanisms of cryptography and encryption. The use of such techniques is growing rapidly. It is spread in a much wider set of industry sectors. With increase in the range of applications and platforms cryptography and encryption have become one of the latest technologies in the IT security industry – the challenge is that we are able to handle such difficulties to secure our data. Also we have to increase CPU performance via selecting suitable key size for variety of data and also send data in parallel form i.e. multiple data is send to multiple receiver simultaneously. Only selected user is able to receive data that is already added in the sender's list. The encryption and decryption of data is only for enhancing the security for secure data transmission over internet. It also provide assurance that an unauthorized person is not able to access this data. The future work is to provide to encrypt or decrypt other types of files (except text file), including audio, & video. Also there is need to develop such algorithm which take the advantage of both symmetric and asymmetric key cryptography which makes the encryption process more easier and faster.

VI. REFERENCES

[1]. Xin Zhou and XiaofeiTang,"Research and implementation of RSA algorithm for encryption and decryption,"Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang,2011,pp. 1118-1121,doi:10.1109/IFOST.2011.6021216

[2]. Abdelhalim, mohamed b & El-Mahallawy, Mohamed &Ayyad, Mohammad. (2013). In RFID SystemDesign and Implementation of an Encryption Algorithm is available. International Journal of RFID Security and Cryptography.2)51-57.10.20533/ijrfidsc.2046.3715.2013.0007.

[3]. Osho, Oluwafemi&Zubair, Yunus&Ojeniyi, Joseph &Osho, Lauretta. (2014). A Simple Encryption and Decryption System.

[4]. Aminudin, Nur&Maseleno, Andino&Shanmugam, Hemalatha& Kumar, K &Fauzi, &Irviani, Rita &Muslihudin, Muhamad. (2018). Nur Algorithm on Data Encryption and Decryption.International Journal of Engineering and Technology.7. 10.14419/ijet.v7i2.26.14363.

[5]. Agrawal, Ekta& Pal, Parashu. (2017). It is a Secure and Fast Approach for Encryption and Decryption of Message Communication. International Journal of Engineering Science and Computing. 7. 5.

[6]. Panford, Joseph &Yeng, Prosper &Hayfron-Acquah, James &Twum, Frimpong. (2016). An Efficient Symmetric Cipher Algorithm for Data Encryption. International Resaerch Journal of Engineering and Technology. 3. 1713 - 1732.

[7]. Nisha, Shireen&Farik, Mohammed. (2017). RSA Public Key Cryptography Algorithm – A Review.International Journal of Scientific & Technology Research. 6. 187-191.

[8]. F. Yan,C. Lin, and Y. Jian-Wen in 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation,"Computer Network Security and Technology Research,". Nanchang, 2015, pp. 293-296, doi: 10.1109/ICMTMA.2015.77.

[9]. Abdullah, Ako. (2017). For Encrypt and Decrypt Data Advanced Encryption Standard (AES).

[10]. Ukwuoma, Henry &Hammawa, Mohammed. (2015). Optimised Key Generation for RSA Encryption. IISTE. 6. 2222-2871.

Cite this article as :

Neha Bansal, Sukhdeep Singh, "RSA Encryption and Decryption System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 5, pp. 109-113, September-October 2020. Available at doi : https://doi.org/10.32628/CSEIT206520
Journal URL : http://ijsrcseit.com/CSEIT206520