A Review: RSA and AES Algorithm

Ashutosh Gupta*
Sheetal Kaushik**

Abstract

ARPANET to today's Internet, the amount of data and information increased to several thousand times. The amount of security problems are also increased with this development. In this paper we aim to review the working of two algorithms, RSA and AES to secure our data over the internet and communication channels. One of these algorithms is symmetric which is developed in early days of modern cryptography and other one is asymmetric, which is advance and still trustworthy.

Keywords: Asymmetric, symmetric, RSA, AES, Cryptography, Encryption.

I. Introduction

Cryptography Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver. Cryptography may also refer to the art of cryptanalysis, by which cryptographic codes are broken [1].Information is the most important thing for a company or a nation to be secure after human resource. While most of the information now a days are in Digital form, they are equally in that much unsecured Environment[2].So, techniques like cryptography help in making the environment and the path of information travelling more secure and trustworthy. A good encryption algorithm must provide confidentiality, integrity, non- repudiation, and Authentication [3].

Cryptography can be further divided in two major types: Secret-Key Cryptography and public key cryptography.Secreate key encryption uses same key for encryption and decription.This type of encryption easier and faster but equally less secure. While on the other hand Public key encryption is more secure and most preferable now days. In this encryption key for encryption and decryption both are different but logically and mathematically they are linked [1][4][5].

Ashutosh Gupta*
BCA-II Year
Institute of Information Technology and Management

Sheetal Kaushik**
IT Department
Institute of Information Technology and Management

A. Data Encryption

This is the process of scrambling, stored or transmitted information so that it is meaningless until it is unscrambled by the intended recipient. This is also known as Ciphering of data. With increasing data and technology advancement, the significance of data encryption is also increasing not only for highly diplomatic and military uses but also from life of ordinary men's to the high value money and information transfer of big multinationals[6].

The history of the cryptography can be traced back into hieroglyphs of early Egyptian civilization (c.1900 B.C.).Ciphering is always considered as the essence of diplomatic and military secrecy. There is several other example of cryptography even in the era of Holy Bible which replete with examples of ciphering [7].

Now a day's Encryption standards are increased so high that Several Government even talking about banning of strong encryption over certain level. The reason behind is the time consumption and work involved even in simple day to day federal cases. For example, the United Kingdom could pass a law that bans encryption stronger than 64-bit keys, knowing its intelligence agency has the resources to crack any form of legal encryption in the country [5].

The early cryptography is done with the standard algorithm of 64 bit key known as DES or Data Encryption Algorithm given by FIPS (Federal Information Processing Standard) [3], [8].

DES algorithm is further replaced by Rijndael algorithm and named as Advance encryption algorithm or AES [8], [9].AES has more flexible key strength that may be help in future manipulation for betterment of it.

RSA was named on their inventor names in 1977, Ron Rivest, Adi Shamir and Len Adleman[10].This algorithm is asymmetric and still in use. RSA algorithms have dual benefit as it used for data encryption as well as digital signatures.

II. AES

Now a Days Security is Equally essential as Speed of data communication and Advance Encryption standard has best suited for it as it provide speed as well as increase security with hardware. Because of its dual base which consists of hardware as well as software this System is more advance and secure than basic DES [8].

AES also advance in the sense of its structure as it uses key in bytes instead of bits whereas in DES number of rounds for encryption of data is not fixed, it depends on the size of the plain text it has to encrypt. If size of text is 128 bit it will treated as 16 Bytes and these 16 Bytes then arranged in form of 4x4 matrixes. In AES 10 rounds of encryption is performed for 128 bit key, 12 rounds for 192 bit keys, and 14 rounds for 256 bit keys. Following Algorithm Encrypt the data [11].

Step 1:- Input a plaintext of 128 bits of block cipher which will be negotiated as 16 bytes.

Step 2: - Add Round Key: - each byte is integrated with a block of the round key using bitwise XOR.

Step 3:- Byte Substitution: - the 16 input bytes are substituted by examining S- box. The result will be a 4x4 matrix.

Step 4:- Shift row: - Every row of 4x4 matrices will be shifted to left. Entry which will be left placed on the right side of row.

Step 5:- Mix Columns: - Every column of four bytes will be altered by applying a distinctive mathematical function (Galois Field).

Step 6:- Add Round Key: - The 16 bytes of matrix will be contemplated as 128 bits and will be XORed to 128 bits of the round key.

Step 7:- This 128 bits will be taken as 16 bytes and similar rounds will be performed.

Step 8:- At the 10th round which will be last round a ciphered text will be produced.

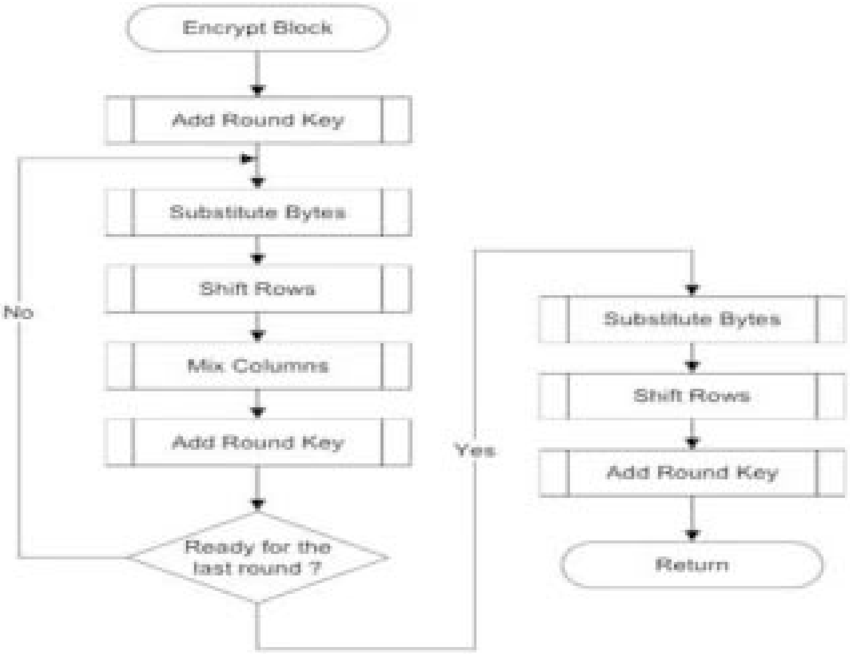

Fig.1 Flow Chart of AES Encryption.

III. RSA

RSA is a public key algorithm, means it uses two different keys one of which must be kept private know as private key and other is public key which is not essentially needed to be secret. Public Key from these two keys is usually used for encryption and private key is used for decryption [14].The RSA Encryption method is Explained Below:

Equations

Step 1: Select Two Large Prime number (Such that Number does not exceed printable ASCII Character).

Select Two Large Prime number p and q

Step 2: Generate the RSA modulus (The answer of multiplication will be considered the Key Length)

$$n=p*q\text{(Public Key)}$$

Step 3: Generate Random Key using Euler function.

$$e= (p-1) *(q-1)$$

Step 4: Form the public key

(n, e) form RSA public Key

Step 5: Generate the private key (Number d is the inverse of e modulo (p - 1) (q – 1).This means that d is the number less than (p - 1) (q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1) (q - 1))

$$ed = 1 \bmod (p\ H\ 1)(q\ H\ 1)$$

RSA security system depends on two different functions.RSA is one of the most secure Cryptography algorithm, whose difficulty is actually based on practical factoring of very large prime numbers [15][16].

IV. Comparison

In the below table the comparison is done between RSA and AES on the base of the keysize,block size, speed , key used in encryption and decryption, type of algorithm, round of encryption and decryption.[17]

FACTOR	AES	RSA
DEVELOPED	2000	1978
KEY SIZE	128,192,256 bits	>1024 bits
BLOCK SIZE	128 Bits	Minimum 512 bits
ENCRYPTION AND DECRYPTION	SAME	DIFFERENT
ALGORITHM	SYMMETRIC	ASYMMETRIC
SPEED	FASTER	SLOWER
ROUNDS	10/12/14	1

V. Conclusion

Encryption of Data plays very vital role in today's time. Our research work served the famous AES and RSA algorithm. Based on research work used in this survey, we can conclude that RSA takes more time for encryption compared to AES. We also concluded that the RSA is more secured than AES, because of its longer key size and different keys for encryption and decryption.

Our future work will be focused on the study of other algorithm including Hyper Image Encryption Algorithm. Our focus will also be on the path of transferring the private key of Asymmetric Encryption.

References

1. www.britannica.com/topic/cryptography.
2. ENISA's Opinion Paper on Encryption December 2016.
3. https://www.tutorialspoint.com/cryptography/data_encryption_standard. htm.
4. https://www.tutorialspoint.com/cryptography/cryptosystems.htm.

5. http://www2.itif.org/2016-unlocking-encryption.pdf.

6. http://www.infoplease.com/encyclopedia/science/data-encryption.html.

7. http://www.infoplease.com/encyclopedia/society/cryptography.html.

8. http://www.ijarcce.com/upload/2016/march-16/IJARCCE%20227.pdf0.

9. https://www.britannica.com/topic/AES#ref1095337.

10. http://www.di-mgt.com.au/rsa_alg.html.

11. https://www.irjet.net/archives/V3/i10/IRJET-V3I10126.pdf.

12. ahttps://en + b =.wikipedia c. .org/wiki/Advanced(1) (1) _Encryption_Standard.

13. https://www.tutorialspoint.com/cryptography/advanced_encryption_stan dard.html.

14. A Novel Approach to Enhance the Security Dimension of RSA Algorithm Using Bijective Function.

15. http://paper.ijcsns.org/07_book/201608/20160809.pdf.

16. Research and Implementation of RSA Algorithm for Encryption and Decryption.

17. https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf