A Comparative Analysis of AES and RSA Algorithms

Shaili Singhal[1]
M.Tech. Student
Shobhit University, Meerut
shailisinghal1907@gmail.com

Dr. Niraj Singhal[2]
Associate Professor
Shobhit University, Meerut
sonia_niraj@yahoo.com

ABSTRACT

Cryptography is an art or science of transforming an intelligible message into unintelligible one, and then retransforming that message back to its original form. Cryptography can also be used to authenticate the sender and receiver of the message to each other. There are two techniques of cryptography, symmetric key cryptography (called secret-key cryptography) algorithms and asymmetric key cryptography (called public-key cryptography) algorithms. AES is private key based algorithm and RSA is public key based algorithm. Both the algorithms are very efficient. This paper presents performance of both the algorithms as well as their comparison.

Keywords: Cryptography, AES, RSA, Key.

1. INTRODUCTION

Nowadays, network security is an important aspect in networking applications. Every day, millions of users generate and exchange useful information in many areas, such as legal, medical, engineering, banking and other fields via internetwork. The information which is to be transferred must be secure against the unauthorized users. Cryptography (as shown in Figure 1) is used to transform an intelligible or original message into one that is unintelligible or encoded, and then retransforming that message back to its original form.

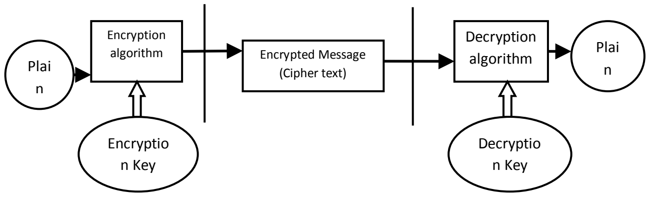

Figure 1. Process of Encryption and Decryption

Cryptography can also be used to authenticate the sender and receiver of the message to each other. There are two methods of cryptography symmetric key cryptography (also called secret-key cryptography algorithms) and asymmetric key cryptography (also called public key cryptography algorithms). Cryptography has many commercial uses and applications such as protecting confidential company information, to allowing someone to order a product on the Internet without the fear of their credit card number being intercepted and used against them anymore. Moreover, there are various issues in the security of cryptographic system. For eg. Remote Biometric Authentication systems faces various security issues over the network, but to solve the privacy issues secret keys are randomly and dynamically generated without human intervention, and each transaction has different secret keys and this can be done by novel chaos-based cryptosystem in which chaotic cryptographic schemes are used for encrypting the biometric templates and modulated by the chaotic spread spectrum modulation technique that makes it more difficult to decipher under attacks [6].

2. RELATED WORK

The original message is known as plain text and the encoded message is called as Cipher text. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. This process is done at the sender side which needs a plain text that is to be encoded, a secret key and, an encryption algorithm for transforming the message. While decryption is the process of generating the original message from the encoded one. This is done at receiver side which needs an encoded form of message, a secret key and, a decryption algorithm for generating the plain text. The keys which are used to encrypt and decrypt the messages are categorized into two forms, Symmetric key (secret key), also called as secret-key cryptography and Asymmetric key (public key) also called as asymmetric-key cryptography. In reference [1], a new symmetric key cryptography method used which is based on randomization method for generating the keys for encrypting as well as decrypting any file such as binary files, text or any other files. This method could be appropriate in sensor network where security of data is important.

2.1 AES Algorithm

Advanced Encryption Standard (AES) algorithm is based on a design principle known as substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware [2]. It is based on private- key cryptography algorithm in which same keys are used for encryption and decryption. The steps of AES algorithm through which a plain text is converted into the cipher text are as follows [3]:-

(a) It takes 128-bit long plain text data block as input and keys length may be 128, 192 or 256- bits long and generate output of 128- bit block.

(b) The 128-bit plain text undergoes an initial round in which each byte of the state is combined with the round key using bitwise XOR.

(c) After performing the initial round, plain text undergoes 10 rounds if the key length of size 128-bit, 12 rounds if key length of size 192-bit or 14 rounds if key length of size 256-bit. There are following steps for each round: -

(i) Sub-Bytes transformation- it is a non-linear substitution is performed where each byte is replaced with another according to a lookup table.

(ii) Shift-Rows transformation- a transposition step where each row of the state is shifted cyclically a certain number of steps.

(iii) Mix Column transformation- it is a mixing operation which operates on the column of the state, combining four bytes in each column.

(iv) Add Round key-

At last, resultant matrix will undergo a final round where sub byte, shift rows transformation are performed and round key is added into the resultant matrix. The complete process is shown in Figure 2.

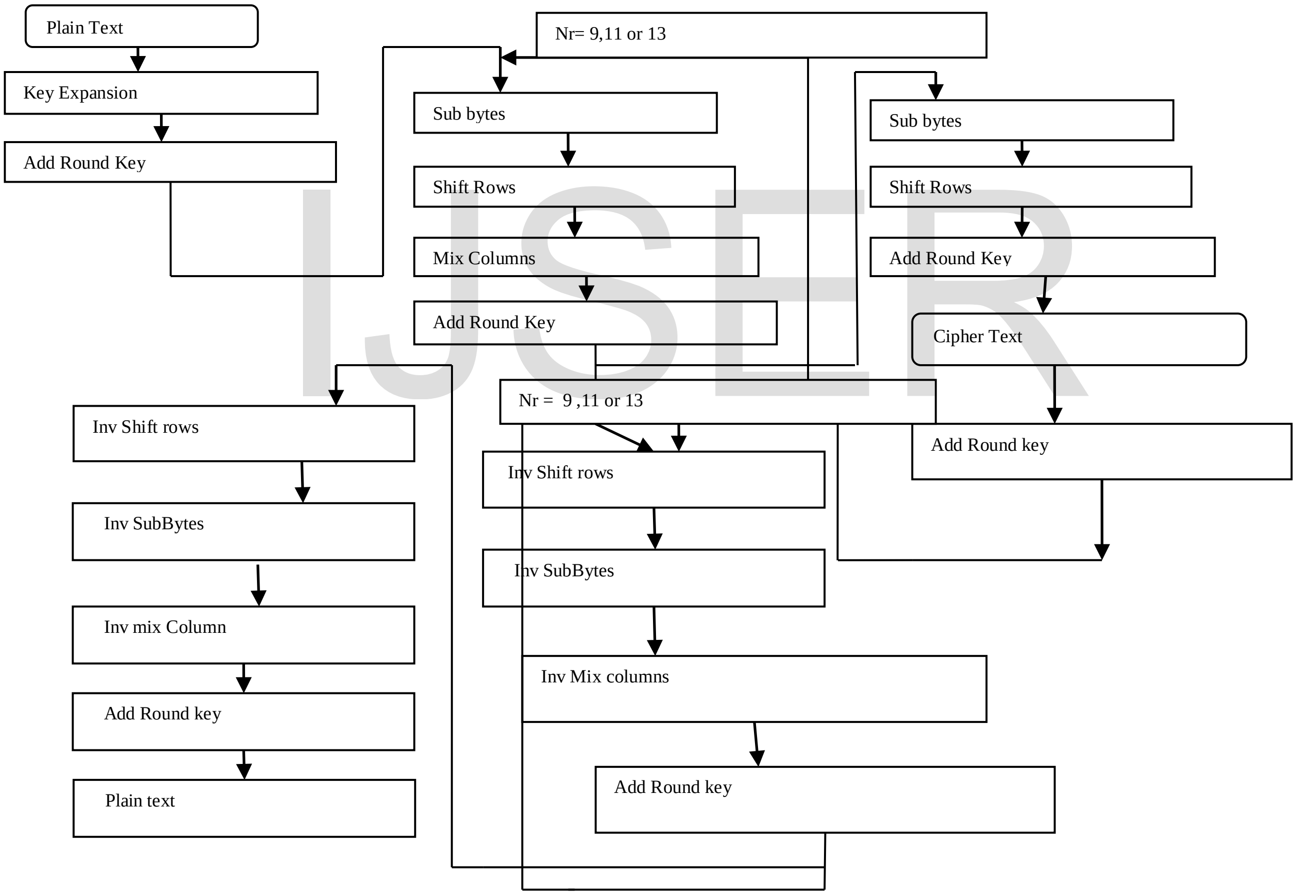

Figure 2. Process of AES algorithm

2.2 RSA Algorithm

RSA algorithm is based on public - key cryptography algorithm which is developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is used by modern computers to encrypt and decrypt the messages. It is asymmetric- key cryptographic algorithm which is used for digital signature. The principle of RSA algorithm is “it is easy to multiply prime numbers but hard to factor them”. Hence it uses large prime numbers to generate public key and private key respectively, as it usually takes long time. In reference [5], it is possible to build a fast implementation of RSA using smart cards with crypto-coprocessor.

The steps of RSA algorithm are as follows: -

a) Choose two large prime numbers P and Q (say) such that P is not equal to Q.
b) Calculate N, by multiplying P and Q; N=P*Q.
c) Now calculate S by formula S= (P-1) *(Q-1).
d) Select a public key e such that e is not the factor of S.
e) Next is to select the private key d such that (d*e) mod S =1.
f) To calculate cipher text (C): C= M^e mod N.
g) To calculate plain text (M): M= C^d mod N.

The cipher text is sent to receiver and at receiver side decryption is performed to get plain text.

3. COMPARATIVE ANALYSIS

From the above analysis one can see that RSA solves the problem of key agreement and key exchange generated in private-key cryptography algorithms but still there is lack of confidentiality.
So, for enhancing the security, a comparative analysis along with various parameters for both the symmetric key encryption and asymmetric key encryption is presented. Hence RSA and AES differ from each other in respect of certain features, as shown in Table 1.

Table 1. Comparison between RSA and AES algorithms

S. No.	Features	AES	RSA
1	Type of cryptography	Symmetric	Asymmetric
2	Key used	Single (same) key is used for Encryption And Decryption	Different(two) keys used for encryption and decryption
3	Throughput	Very high	Low
4	Confidentiality	High	Low

4. CONCLUSION

In this research paper comparison between AES and RSA algorithms have been studied and summarized. Main differences between both the techniques are also mentioned. As AES is private key based algorithm that suffers from key distribution and key agreement problems however these problem is overcome in RSA algorithm but encryption and decryption takes more time in RSA algorithm. So both the algorithms have their own merits and demerits.

References

[1] A. Nath, S. Ghosh and M. A. Mallik, “Symmetric key Cryptography using Random Key Generator”, Proceedings of International conference on Security and Management, , Las Vegas ,USA, Vol. 2, pp.239-244, 12-15 July, 2010.

[2] “Advanced Encryption Standard”, http://en.wikipedia.org/wiki/Advanced_Encryption_ Standard”. (accessed on November 8, 2015).

[3] W. Stallings, “Cryptography and Network Security”, Prentice Hall, Edition 1995.

[4] AL. Jeeva, V. Palanisamy and K. Kanagaram, “Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms”, Proceedings of International Journal of Engineering Research and Applications, Vol. 2, pp.3033-3037, May-Jun 2012.

[5] C. Lu, A. L. M. Santos, and F. R. Pimentel, “Implementation of fast RSA key generation on Smart Cards”, Proceedings of the 2002 ACM Symposium on Applied computing, pp.214-220, ACM Press, 2002.

[6] Muhammad Khurram Khanand and Jiashu Zhang, “Implementing Templates Security in Remote Biometric Authentication Systems”, Proceedings of IEEE Conference on CIS’06, China, Vol. 2, pp. 1396-1400, 2006.

[7] T. Matsumoto and K. Kato, “Speeding up Secret Computations with Insecure Auxiliary device”, Proceedings of the 8th Annual International Crypto Conference on Advances in Cryptology, London, Springer Verlag, pp. 497-506, 1988.

[8] T. Collins, D. Hopkins and M. Sabin, “Public Key Cryptographic Apparatus and Method” US Patent #5,848,159, Jan. 1997.

[9] D. Boneh and H. Shacham, “Fast Variants of RSA”, RSA Laboratories Cryptobytes, 5(l), pp. 1-8, 2002.

.