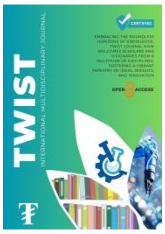
DOI https://doi.org/10.5281/zenodo.10049652#184

BY NC SA

TWIST, 2024, Vol. 19, Issue 2, pp. 508-512

TWIST

Journal homepage: www.twistjournal.net



Secure Transmission of Information through Hybrid Cryptographical Techniques

Pawan Kumar*
Department of Computer Science, Babasaheb Bhimrao Ambedkar University,
Lucknow, U.P. 226025, India
[**Corresponding author*]

Vipin Saxena
Department of Computer Science, Babasaheb Bhimrao Ambedkar University,
Lucknow, U.P. 226025, India

Abstract
The cloud computing is gaining popularity among the users as the cloud servers are arranged through the dynamic topological structures. The main aim of every user is to transmit secure information from one device to another device. From the literature, it is observed that there is very less information available on the hybrid cryptographical techniques. The present work is an attempt in this direction and based upon the hybrid cryptographical techniques which can be applied for secure transfer of information especially confidential information from one device to another device. The newly proposed algorithms have been tested through a case study and computed results are depicted in the form of tables and graphs.

Keywords
Cloud Computing, Topology, Information, Hybrid Cryptography, Security

INTRODUCTION

Day by day, the network is growing in the distributed manner and daily interactions across the network are tremendously increasing. The privacy of individual is at the risk due to involvement of digital currency which is to be transferred by the users over the network from one device to another device. Since the evolution of network, users are facing the challenges related to the security of information although the researchers have investigated the various cryptographical techniques from time to time. The primary goal of security is to keep information hidden from the public and cyber attackers. This necessity gave rise to a variety of cryptographic primitives, such as hash functions, digital signatures, and symmetric and asymmetric cryptography. A key that is exchanged by the sender and the recipient in symmetric encryption is kept hidden from the unwanted party. As a symmetric cipher that uses a fixed 128-bit block and a shared secret key to encrypt and decode any communication. Three separate key lengths can be used with Advance Encryption Standard (AES), and term as AES-128, AES-192, and AES-256, sequentially 128,192, 256, to denote the key's length in bits. In Asymmetric cryptography, encrypts and decrypts messages using a pair of keys. The first of these two keys is referred to as the public key because it is shared with everyone, while the other is referred to as the private key because it is kept private.

Every message is typically encrypted using a public key, which can only be decoded with the associated secret key. Rivest, Shamir, Adleman (RSA) algorithm has three parts, key generation, encryption and decryption. It was created in 1977 by Ron Rivest, Adi Shamir, and Len Adlemen as a public key encryption technique. XOR logic gate gives output 1 (high) when number of inputs 1 (high) will odd. A output 0 (low) is produced if either both inputs are 0 (low) or both are 1 (high). XOR logic gate work like one time pad.

RELATED WORK

In the year 2011, Zhou and Tang [1] have discussed encryption/decryption based on RSA algorithm and public key. In the year 2013, Padmavathi and Kumari [2] have implemented three encryption methods DES, AES, and RSA along with a steganographic method Least Significant Bit (LSB) substitution and compared the effectiveness of these methods based on an analysis of their stimulated times during the encryption and decryption processes. In the year 2018, Lee et al. [3] have implemented Heroku as a cloud infrastructure, and then secure Heroku's information with AES cryptography. According to the performance evaluation, data security is achieved by AES cryptography. The data encryption process delay in calculation that demonstrate the bigger data sizes result in longer data delay times. In the year 2019, Patel [4] has discussed performance and evaluation of symmetric algorithm on Blowfish, AES, and Data Encryption Standard (DES). Performance evaluations are based on how much memory and how long it takes for certain algorithms to run. The evaluation shows that DES algorithm better than other algorithm such AES and Blowfish. According to experimental findings, Blowfish is a superior solution to AES and DES in terms of memory. In the year 2020, Muttaqin and Rahmadaoni [5] have tested on all files of various file sizes as well as on the ciphertext produced by the encryption process. Santoso et al. [6] have discussed combination of two algorithm, Twofish and AES. The SHA -256 algorithm key generates for AES and Twofish algorithm which is 256-bit long key. Arman et al.[7] have discussed, quick execution time and low memory in AES-128-bit version. In terms of performance, this is a great improvement over the conventional AES. In the year 2020, Gupta and Kapoor [8] have implement hybrid cryptography to protect data in web applications. In the hybrid algorithm, AES and ECC algorithm replaced by Blowfish and RSA respectively. For original data authentication, used message digest version-5 hash algorithm. Hamza and Kumar [9] have discussed function of symmetric algorithm and asymmetric algorithm in term of number of keys, encryption/decryption speed, complexity of process, security/strength factoring primes and other functions. In the year 2020, Abbas et al. [10] have implemented hybrid cryptography along with use of stenography for cloud data security. The LSB method used to mask the encrypted data within a picture and the SHA hashing method throughout the data validation stage. In the year 2022, Kumar and Saxena [11] have enhanced the security of pattern with combination of fuzzy rule, pseudo random number generator and Elgamal cryptography.

PROPOSED WORK

The proposed work is combination of two cryptography algorithm. All the cryptography algorithm discuss below:

RSA

RSA algorithm one of the most popular algorithms in asymmetric algorithm. RSA algorithm based on prime number factorization. RSA algorithm has three parts, first part is key generation, second part is encryption and third is decryption. RSA algorithm steps defined in below[1]:

Key generation

Step 1. choose two distinct prime number *prime_num1*, *prime_num2* with equal size.
Step 2. *n= (prime_num1 * prime_num2*)
Step 3. ϕ*(n)= (prime_num1 -1) * (prime_num2-1)*
Step 4. Generate encryption key *e* which must be co-prime of ϕ*(n) and* 1 < e < $\emptyset(n)$
Step 5. Calculate $d \cong e^{-1}(mod\emptyset(n))$
Step 6. *pub_Key = (e, n)*
priv_key= (d, n)

Encryption

Step 1. Message for encryption *Mssg*
Step 2. the ciphertext of a message $Cipher\_text = (Mssg)^{e}$ *mod n*

Decryption

Step 1. Cipher Text at receiver end $Cipher\_text$
Step 2. Message *Mssg*=$(Cipher\_text)^{d}$ *mod n*

AES

AES is symmetric type of cryptography algorithm. AES algorithm has three types: AES-128, AES-192 and AES-256. AES-128 represents 128-bit key length and 10 rounds, AES- 192 represents 192 key length and 12 rounds and AES-256 represents 256 key length and 14 rounds.

All rounds contain following functions such that Sub Bytes, Shift Rows, Mix Columns and Add Round Key except last round. In last round contains following function such that Byte Sub, Shift Row and Add Round Key [5], [6].

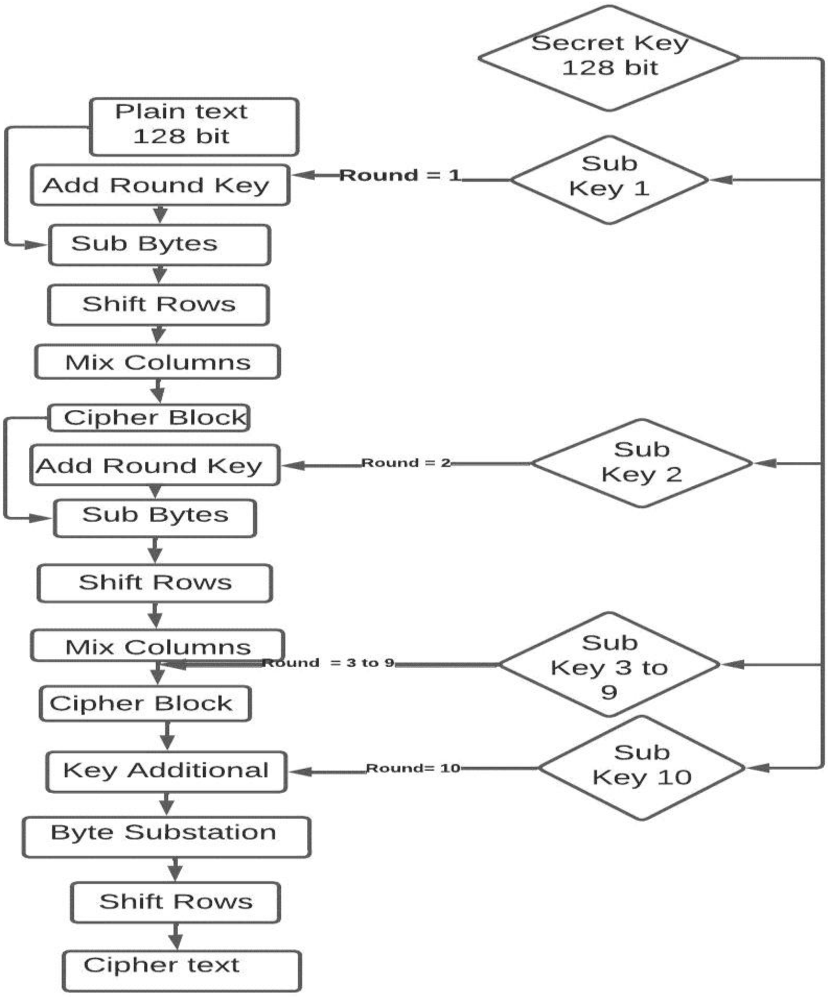


Fig. 1 Flow diagram of AES algorithm

The RSA algorithm is asymmetric algorithm and AES algorithm is symmetric algorithm. The message divided in to two parts. Each part encryption and decryption are done by RSA and AES algorithm.

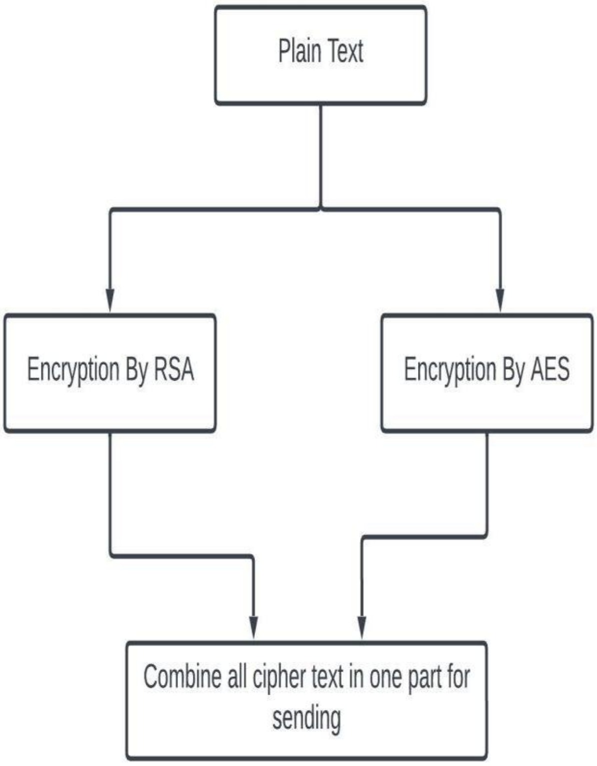


Fig. 2 Encryption by Proposed Algorithm

Fig. 2 shows the plain text divides in two parts, the first part is encrypted by RSA and the second part is encrypted by AES. Then encrypted message sends over communication channel.

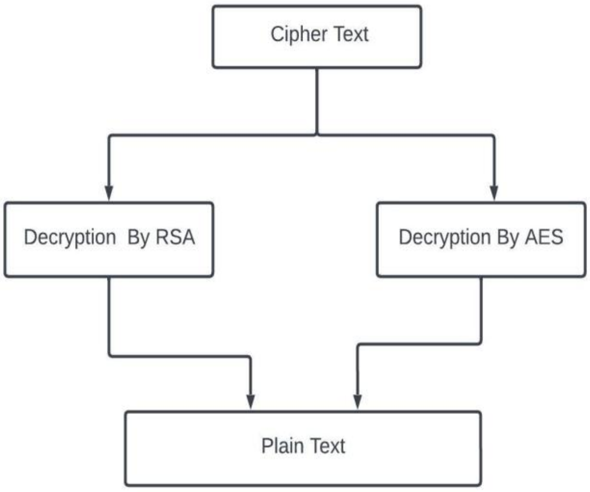


Fig. 3 Decryption by Proposed Algorithm

At the receiver side, the first part is decrypted by RSA and second part is decrypted by AES. All output combines together then find the original message.

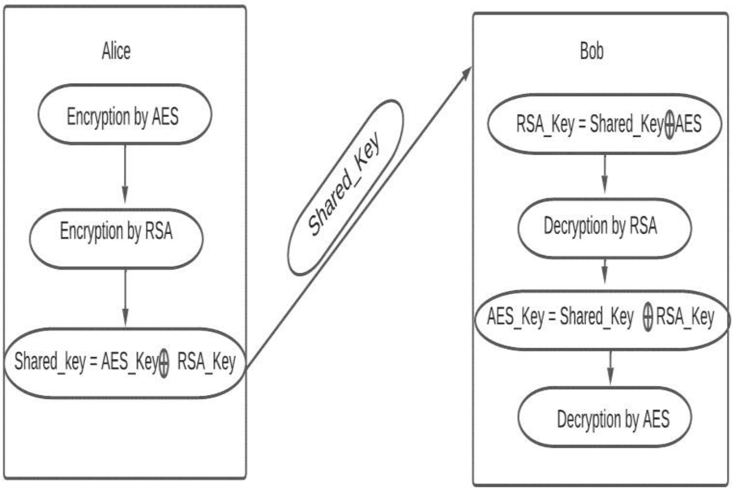
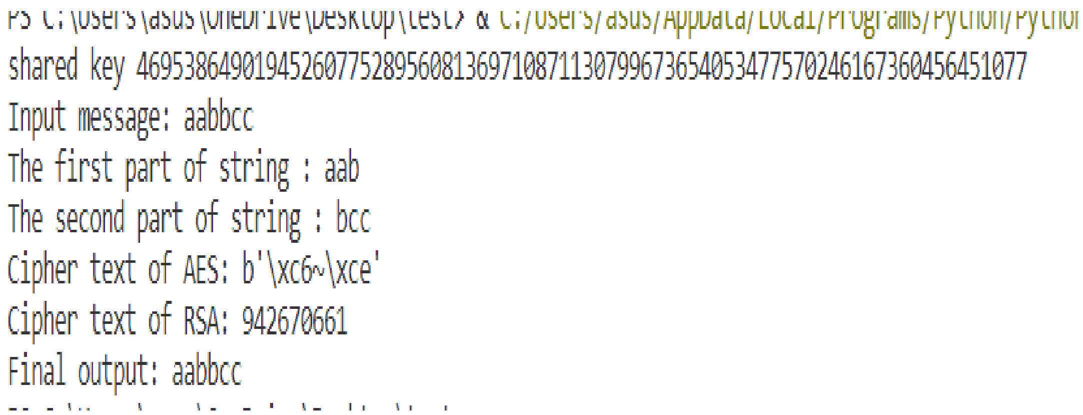


Fig. 4 Share with the help of XOR logic gate

In the above diagram, share public key of RSA and private key of AES help of XOR logic gate. Other side, again perform XOR operation between public key of RSA and *Shared_key* then found AES private key *AES_Key*.

RESULT AND DISCUSSION

In the figure 4, shows that input message divides in two parts, the first part is encrypted by RSA and the second part is encrypted by AES. The shared key is defined by XOR operation between RSA's public key and AES's private key. At the sender side, sender perform XOR operation between public key of RSA and shared key then find the private key of AES. The information is encrypted by public key of RSA and private key of AES.



```
PS C:\Users\asus\OneDrive\Desktop\test> & C:/Users/asus/AppData/Local/Programs/Python/Pythor
shared key 4695386490194526077528956081369710871130799673654053477570246167360456451077
Input message: aabbcc
The first part of string : aab
The second part of string : bcc
Cipher text of AES: b'\xc6~\xce'
Cipher text of RSA: 942670661
Final output: aabbcc
```

Fig. 5 Output of Proposed Work

At the receiver side, the cipher text is decrypted by RSA and AES cryptographical algorithm. At last, the receiver combine output of RSA and AES cryptographical algorithm.

CONCLUSION

The proposed work presents, the security methodology for protecting data exchanged between two linked devices that are interacting via internet. By the implementation of hybrid cryptographic algorithm, use of AES, RSA and XOR logic operation, that will secure, reliable and transparent. Proposed work will be benefitted all kinds of the organization which are using a digital transformation of data over internet.

REFERENCES

1. Zhou, X. and Tang, X. (2011, August), Research and Implementation of RSA Algorithm for Encryption and Decryption, In *Proceedings of 2011 6th International Forum on Strategic Technology*, Vol. 2, pp. 1118-1121, IEEE. DOI: 10.1109/IFOST.2011.6021216
2. Padmavathi, B. and Kumari, S. R. (2013), A Survey on Performance Analysis of DES, AES and RSA Algorithm Along with LSB Substitution, *International Journal of Science and Research, India*, *2*, 2319-7064. http://www.ijsr.net/archive/v2i4/IJSRON120134.pdf
3. Lee, B. H., Dewi, E. K. and Wajdi, M. F. (2018, April), Data Security in Cloud Computing Using AES Under HEROKU Cloud, In *2018 27th Wireless and Optical Communication Conference (WOCC)*, pp. 1-5, IEEE, DOI: 10.1109/WOCC.2018.8372705
4. Patel, K. (2019), Performance Analysis of AES, DES and Blowfish Cryptographic Algorithms on Small and Large Data Files, *International Journal of Information Technology*, Vol. 11, pp. 813-819. https://doi.org/10.1007/s41870-018-0271-4
5. Muttaqin, K. and Rahmadoni, J. (2020), Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based, *Journal of Applied Engineering and Technological Science (JAETS)*, Vol. 1,No. 2, pp. 113-123. https://journal.yrpipku.com/index.php/jaets/article/view/78
6. Santoso, K. I., Muin, M. A. and Mahmudi, M. A. (2020, April), Implementation of AES Cryptography and Twofish Hybrid Algorithms for Cloud, In *Journal of Physics: Conference Series*, Vol. 1517, No. 1, pp. 012099, IOP Publishing. doi:10.1088/1742-6596/1517/1/012099
7. Arman, S., Rehnuma, T. and Rahman, M. (2020), Design and Implementation of a Modified AES Cryptography with Fast Key Generation Technique. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* pp. 191-195, DOI: 10.1109/WIECON-ECE52138.2020.9397992
8. Gupta, N. and Kapoor, V. (2020), Hybrid Cryptographic Technique to Secure Data in Web Application, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 23, No.1, pp. 125-135, https://doi.org/10.1080/09720529.2020.1721872
9. Hamza, A. and Kumar, B., "A Review Paper on DES, AES, RSA Encryption Standards," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, Moradabad, India, 2020, pp. 333-338, doi: 10.1109/SMART50582.2020.9336800.
10. Abbas, M. S., Mahdi, S. S. and Hussien, S. A. (2020), Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography, In *2020 International Conference on Computer Science and Software Engineering (CSASE)* (pp. 123-127), IEEE, doi: 10.1109/CSASE48920.2020.9142072
11. Kumar, P. and Saxena, V. (2022), Fuzzy Rule Based Enhancement of Pattern Lock Security System, *NeuroQuantology*, Vol. 20, No. 16, pp. 1651-1661, DOI: 10.48047/NQ.2022.20.16.NQ880164