International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Secure System to Store Crime Data

Sai Venkatesh Aravapalli[1]

[1]Computer Science and Engineering & Vellore Institute of Technology

---

Abstract – Main aim of this work is to secure the data. In order to keep the data secured I proposed a solution Hybrid Cryptography. When Sender tries to send the crime data to receiver, the data will be encrypted through symmetric encryption using symmetric key. Generally, recipient will get symmetric key which he uses to decrypt the data. But we use hybrid cryptography to enhance security even more by encrypting the symmetric key through the asymmetric encryption and both encrypted symmetric key and encrypted crime data is transmitted to recipient. Recipient who has private key decrypts the encrypted symmetric key and further decrypts encrypted crime data using decrypted symmetric key and thus secured crime data reaches recipient safely.

***Key Words*:** Data Storage, Security, Confidentiality, Integrity, Hybrid Encryption.

1.INTRODUCTION

In Police departments and other government organizations, data of criminals such as their background, record, and information related to their prison details and officers who handled them is stored in cloud which is highly confidential. But for the purpose of department, that data is transferred from one department to another. In this process that data can hacked by supporters of the criminals and can be corrupted. In order to keep this data secured we propose a solution Hybrid Cryptography.

2. METHODOLOGY

First, encryption of message is done using symmetric encryption (DES Algorithm) and the symmetric key used to encrypt the message is also encrypted using asymmetric encryption (RSA Algorithm) by receiving public key from receiver who wants to access the file. Now both encrypted message and encrypted symmetric key are sent to receiver. Receiver decrypts the encrypted symmetric key using RSA algorithm by allowing his private key to decrypt it. With obtained symmetric key, receiver further decrypts the encrypted message and he gets access to the message.

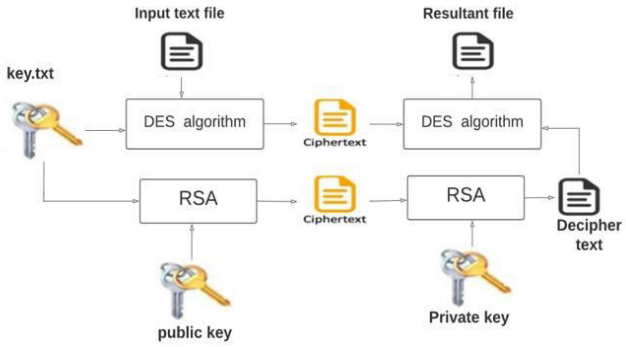

Figure 1: Overview of the proposed model.

2. 1 DES Algorithm:

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm.

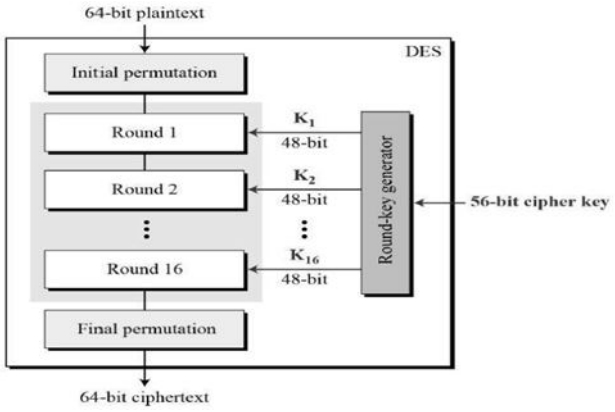

Figure 2: *Working of DES algorithm*

2. 2 RSA Algorithm:

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption.
The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

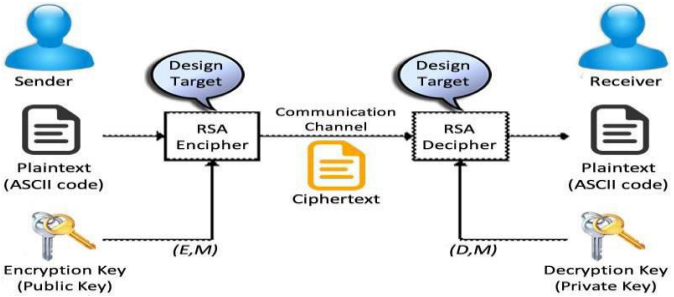

Figure 3: *Working of RSA algorithm*

3. RESULTS AND DISCUSSION

Thus, using Hybrid cryptography, we can double the security level and enhance the protection of information. Because encryption and decryption using one algorithm doesn't provide security level provided by encryption and decryption using combination of symmetric and asymmetric algorithms. The proposed hybrid protocol tries to trap the intruder by splitting the plain text and then applies two different techniques. First, it takes the advantages of the combination of both Symmetric and Asymmetric cryptographic techniques using both DES and RSA algorithms. Second, combination of two algorithms is used since it is more robust and cannot be easily attacked. The attractiveness of the proposed protocol, compared to other existing security protocols, is that it appears to offer better security for a shorter encryption and decryption time, and smallest cipher text size. There by, reducing processing overhead and achieving lower memory consumption that is appropriate for all applications.

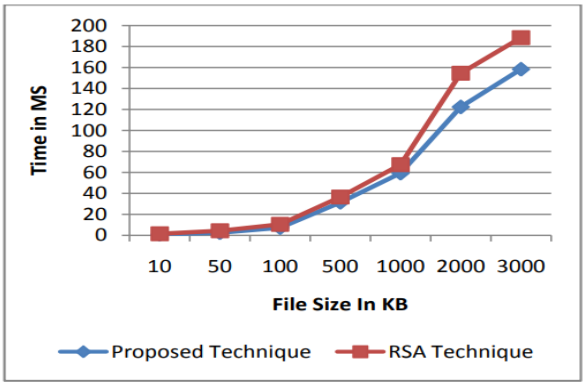

Figure 4: *Encryption time of proposed model and RSA*

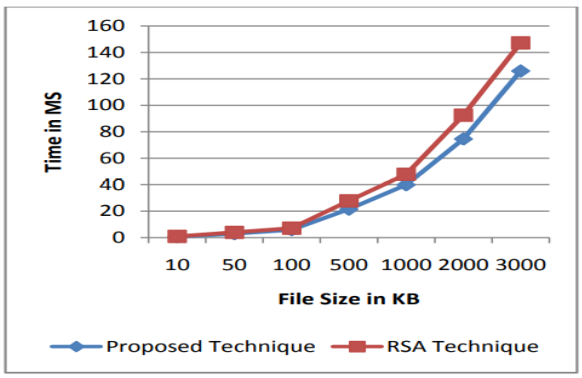

Figure 5: *Decryption time of proposed model and RSA*

S.No.	Parameters	Proposed	RSA
1	Encryption Time	Low	High
2	Decryption Time	Low	High
3	Encryption Memory	Low	High
4	Decryption Memory	Low	High

Table 1: *Results Comparison of proposed model and RSA*

4. CONCLUSION

Finally, using this hybrid cryptography technique which involves the RSA, DES, keys, symmetric encryption and asymmetric encryption we can conclude that:

- It can be used to safe guard data when it is being transferred from one government organization to another.
- It can be to highly encrypt the data by using 2 different algorithms one symmetric and the other asymmetric to ensure its safety.
- It can be used to ensure the data cannot be corrupted during the transfer.
- To make sure the data can be decrypted by the receiver and receive the original message intact.

ACKNOWLEDGEMENT

I would like to thank Dr. Murugan K for helping me to find this interesting topic.

REFERENCES

[1] Maitri, P. V., & Verma, A. (2016, March). Secure file storage in cloud computing using hybrid cryptography algorithm. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1635-1638). IEEE.

[2] Nepal, S., Friedrich, C., Henry, L., & Chen, S. (2011, December). A secure storage service in the hybrid cloud. In 2011 Fourth IEEE International Conference on Utility and Cloud Computing (pp. 334-335). IEEE.

[3] Swarna, C., & Eastaff, M. S. Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm, vol 5, issue 3, 2013, April, aetsdjaras.

[4] Mata, F., Kimwele, M., & Okeyo, G. Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish), 2015, March, Vol 6, issue 3, IJSR.

[5] Subasree, S., & Sakthivel, N. K. (2010). Design of a new security protocol using hybrid cryptography algorithms. IJRRAS, 2(2), 95-103.

[6] V. Kapoor & Rahul Yadav (May, 2016). A Hybrid Cryptography Technique for Improving Network Security, Volume 141 – No.11, IJCA.

[7] Swapnil Chaudhari, Mangesh Pahade, Sahil Bhat, Chetan Jadhav, Tejaswini Sawant (2018). A Research Paper on New Hybrid Cryptography Algorithm, Vol-3, Issue-11, IJIR.

[8] M. Hoobi (2020). Efficient Hybrid Cryptography Algorithm, vol 55, No 3, JSJU.

[9] Gaurav R. Patel, & Prof. Krunal Pancha (2014). Hybrid Encryption Algorithm, volume 2, Issue 2, IJEDR.

[10] S. Gokulraj, P. Ananthi, R. Baby, E. Janani (Mar, 2021). Secure File Storage Using Hybrid Cryptography, SSRN.