ISSN No:-2456-2165

A Comparative Analysis of Cryptographic Algorithms: AES & RSA and Hybrid Algorithm for Encryption and Decryption

Sa'idu Sani
M.Tech (CSE) Student 4th Semester
Dept. of Computer Science and Eng.
AP Goyal University, Shimla, India

Prashansa Taneja
Assistant Professor
Dept. of Computer Science and Eng.
AP Goyal University, Shimla, India

Shreya Kalta
Assistant Professor
Dept. of Computer Sc. & Eng.
AP Goyal University, Shimla, India

Abstract:- Cryptography was provided to secure communication between two parties known as sender and receiver in the appearance of unassigned user known as attackers with the process called encryption. The process of changing the plaint text uses an algorithm and a key to convert a plaintext into another format. The used procedure transforms the same plaintext into the same cipher text if the same process followed. The objective of this research is to propose an improved cryptographic algorithm that would combined the two different algorithms to encrypt and decrypt file using more than one key. It will also analyze the confidentiality, integrity and authenticity provided by cryptography on a network by examining some selected algorithm such as data encryption standard (DES), blowfish encryption algorithm, RSA encryption algorithm and advance encryption standard (AES) algorithms as they are among the most useful algorithms today. The research examines cryptographic algorithms using secondary data obtained from related journals and conference papers. The study result shows that the proposed system improved the maximum accuracy required due to the increases in the security level as it uses more than one key for encryption and decryption.

Keywords:- *Encryption, Decryption, Security, Plaintext, Ciphertext, Algorithm, Secret Key,Cryptographic Algorithm.*

I. INTRODUCTION

Due to the emergence of the phone network, online documents have attracted the interest of people, due to the modification and also transferring from one point to another, therefore they become common. Still there exist more security accident for data in the electronic devices, which include defending on software in file protection, scarcity in data protection, and unwantedattacking of data that has change the format. The more the important part of information is seen by the unwanted user, it will lead to the serious security threat to people, organization and nation security. The research paper concerned mainly on the analysis of AES as one of the symmetric algorithm and the, RSA algorithm as one the asymmetric algorithm. Many scholars have regarded the research as a very important topic. Some scientist consider the uses of RSA for file encryption, and observed that only small files can be encrypted with RSA [1] . beside that the technique makes RSA use strong key management advantage, but the problem of securing large files were not achieved because of the limited speed in RSA technique is not appropriate[2]. "cipher text misappropriation" of the AES technique to promote the file encryption to resolve inappropriate combining data to be processed, although the level of security in AES technique did not consider, the that may be attacked based on some criteria[3]. But the AES and the RSA techniques were been widely applied in the field of cryptosystem, still there may be some inconsistency in the security level of protection and protection efficiency. The research is,considering make full advantage of the AES encryption speed, high security, and strong key management properties of RSA, propose a combination of AES and RSA encryption algorithms, and apply it to file encryption[4]. The experiment, java programming language (Eclipses IDE) was used to implement the algorithm; the proposed algorithm consider the advantages ofverifying the performance of encrypted files. The figure below illustrates the encryption and decryption process.

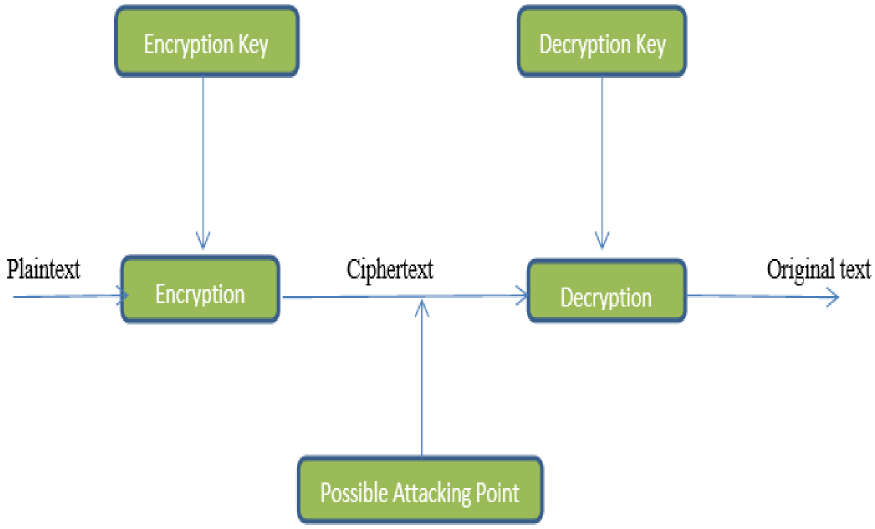


Fig 1: Encryption and Decryption Process

II. RELATED LITERATURE

Thapar, S.S. and H. Sarangal. In their article "*A study of data threats and the role of cryptography algorithms*", At The 9th Annual Conference on Information Technology, Electronics, and Mobile Communication, Many feature combine to throw network security to the top issues in the organization and face IT professional daily. The number one driver of worry about network security nowadays is the decentralization of company operations and the rise of computer networks' correspondence. As far as security concern, many organization networks are accidently waiting to occur, such accident will occur is impossible to predict but security breaches will occur. When organization network security chooses is 100% involve cryptography technology[5]**.**

According to Thakur, J. and N. Kumar, in their study "DES, AES, and Blowfish: Simulation- Based Performance Analysis of Symmetric Key Cryptography Algorithms*"*. The main categories of cryptography depending on the kind of security applied to encrypt and decrypt the data[6]. These two groups include asymmetric and symmetric encryption algorithms.

In the article "Comparative analysis of cryptographic algorithms" by Hercigonja, Z. Asymmetric cryptography includes RSA, that is asymmetric key cryptographic techniques. Keys in asymmetry are achieved by multiplying two huge prime numbers together. Messages encryptedin a reasonable amount of time, the public key can be decrypted with the private key. To produce public and private keys, modulus and exponent procedures are used[7]. The RSA cryptosystem's security is built on factoring huge numbers and calculating the eth root modulus of a compositen, then finding a value m such that C=me(mod n), where (n,e) is the public key and C is the cypher text.

B.E.H.H. Hamouda, Different cryptography methods are compared. In response to the increasingpossibility of assaults against DES, the National Institute of Standards and Technology (NIST) issued a request for proposals for an official successor that meets 21st-century security requirements.

S. Koko and A. Babiker We compare the measured encryption speed to several methods includedin Sun's JDK as standard, and then provide a summary of the algorithms' other characteristics[8].AES is one of the encryption methods that is taken into consideration here (with 128 and 256-bit keys)

S. Sharma and Y. Gupta, "Study on Cryptography and Techniques," *Int. J. Sci. Res. Comput. Sci.Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 1, no. 2, pp. 2456–3307, 201, RSA stands for Rivest Shamir and Adleman name of three inventors. RSA is one of the first practical public- key cryptosystems and is widely used for secure data transmission[9]. The encryption key is public unlike the decryption key, which is kept secret in such a cryptosystem. The factoring problem, which is the practical difficulty of factoring the product of two large prime integers, is premised on this imbalance in RSA. RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly announced the approach in 1977.. [10].

III. METHODOLOGY

Research is the process to collect knowledge about the given topic. Research can be described as the process of investigation. In conducting research one came make his paper more meaningful and reliable.

Using a good research procedure or research methods for a particular research, the possibility of incorrectness may be less. The chart below describes step by step used in research. Topic was firstly chosen and data was collected related to the topic from past research work. Then analysis was done on the research problems given by other authors. After the analyzing the problems of the previous research thenmodified hybrid algorithm was proposed and find out the solution.

Java programming language (Eclipses IDE) was used for the implementation of the proposed algorithm. The algorithm below was followed for conducting this research.

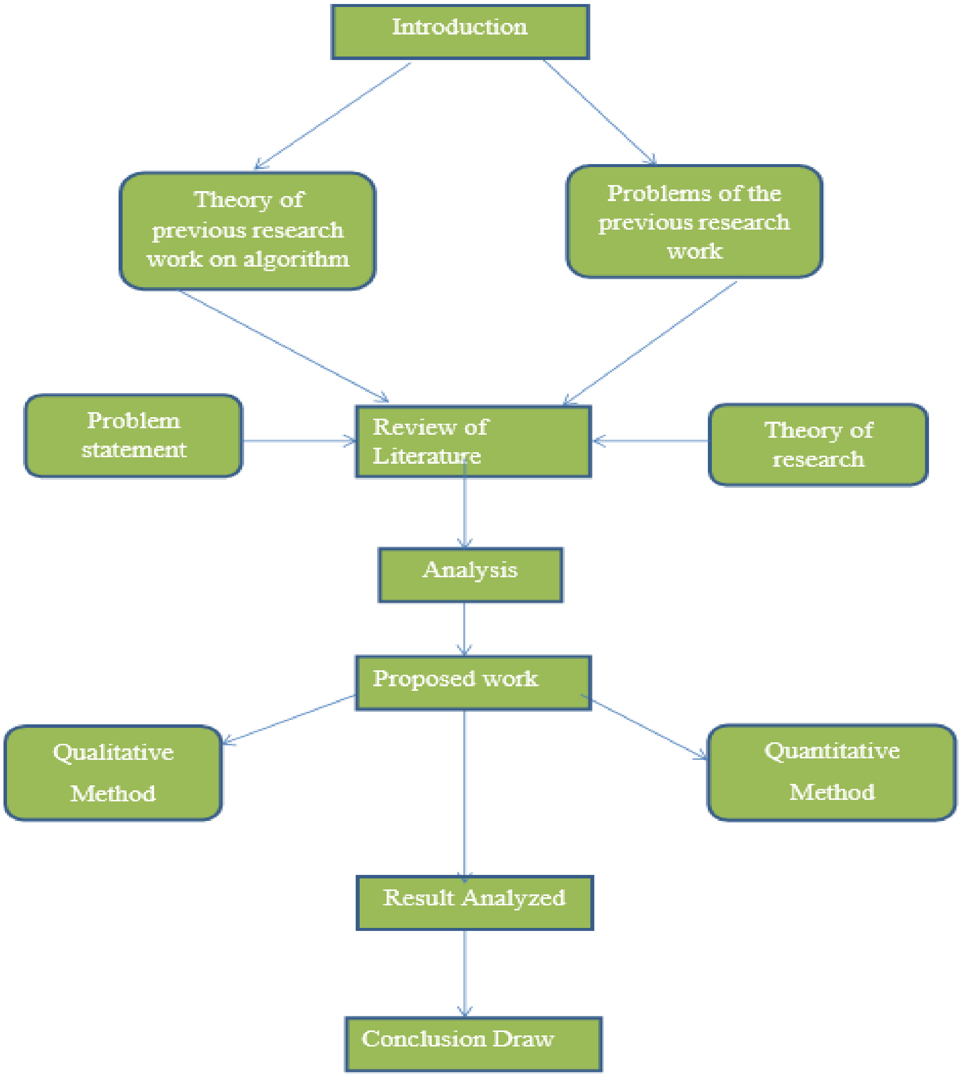


Fig 2: Flowchart of Proposed Methodology

The key research methodologies employed for the research endeavor are qualitative and quantitative research methodologies. Following the use of both approaches result will be highlighted in detail and conclusion of my research described.

AES: - NIST announced the Advanced Encryption Standard algorithm in 2001. AES is one ofthe symmetric cypher algorithms which were created in order to take the role of DES. Following this, AES's security process and security strength are on par with 3DES, with much enhanced accuracy. The Rijndael that was proposed for AES established an encryption that the block and the key lengths are set to 128,192, or 256 bits, respectively. The AES specification makes use of the same algorithm. three key size options as DES specification However, the block size is limited to 128 bits.. In the AES structure “A” stand for add round as illustrated in the figure below.

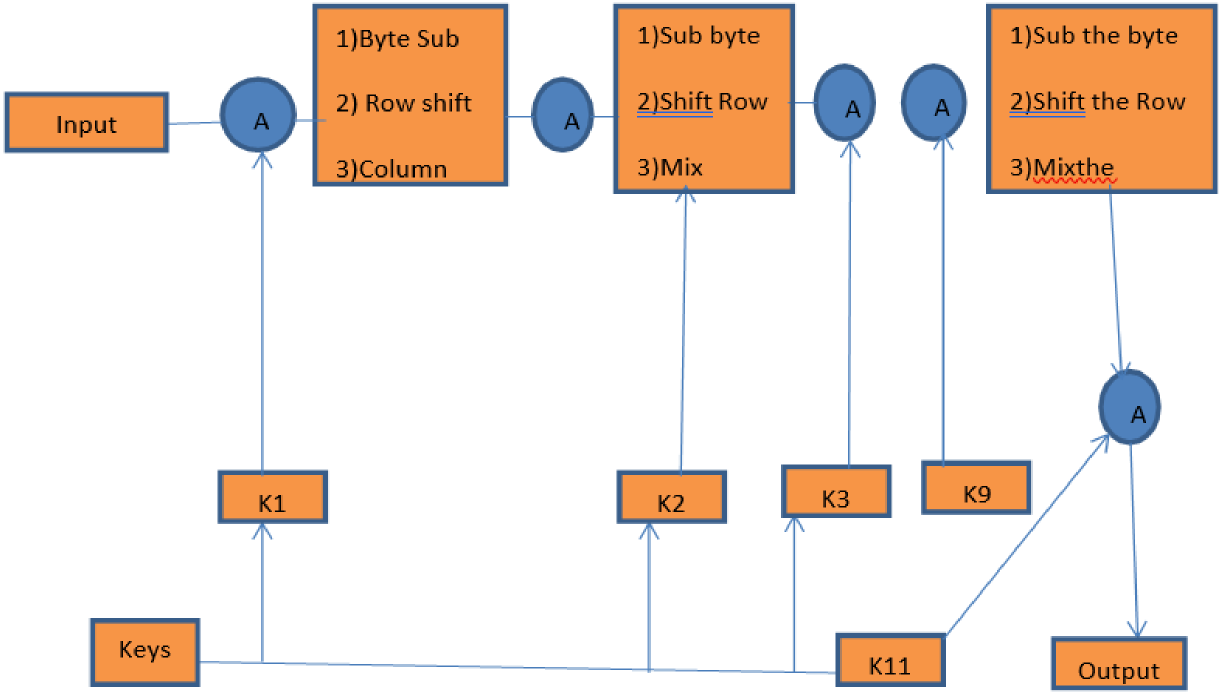


Fig 3: Structure of AES algorithm

Asymmetric encryption algorithm: In this type of algorithm two keys are used that is private and public key. The public key is used to encrypt the data, while to decode it, a private key is used. However, the fundamental drawback of public key encryption is that it relies on mathematical functions. Because asymmetric encryption techniques demand more computational processing capacity than symmetric encryption approaches, they are much slower. When using an asymmetric algorithm we will take a look at RSA algorithm as it is the most commonasymmetric algorithm

RSA: RSA algorithm was developed by Leonard Adleman, Ron Rivest, and Adi Shamir It was first created in 1977. It is widely used in a variety of applications, such as web browsers. It's an asymmetric key security algorithm that's very similar to DES. It's a patented algorithm. The RSAalgorithm employs two distinct keys, one for encryption and the other for decryption. The publicand private keys are the two types of keys.

IV. PROPOSED WORK

The application of many different cryptography techniques can provide a mechanism for the solution to more deficiencies that are happening in a security cryptographic system whichinclude:

1. Key encryption management guarantees that all security objectives are met.
2. To develop a secure communication application that allows users to share information and dataover the Internet.
3. Since people are transferring a lot of data, there should have been a cryptographic technique created that was examined, tested, and reliable.

The proposed algorithm combined the features of symmetric key encryption (AES) and asymmetric key encryption(RSA) to overcome the problem of key management in AES and hightime taken of RSA due to the high key length respectively.

It employs a variety of applications in order to get accurate result. The AES key algorithm is used to encrypt and decode data. AES -Key generated cipher text will be encrypted using RSA key algorithm, which ensures the data integrity, authentication and non-repudiation will besaved.

Proposed hybrid encryption technique follows the following steps:

Encryption:

- Provide AES key
- Provide RSA public key
- Provide RSA private
- Get the data to be encrypted
- Data encrypt using AES key
- Encrypt AES key generated cipher text using RSA public key

Decryption

- Verify signature using RSA public key
- Decrypt AES key generated cipher text using RSA private key
- Decrypt data using AES key
- Get the original data encrypted

The structure of the proposed algorithm is shown below

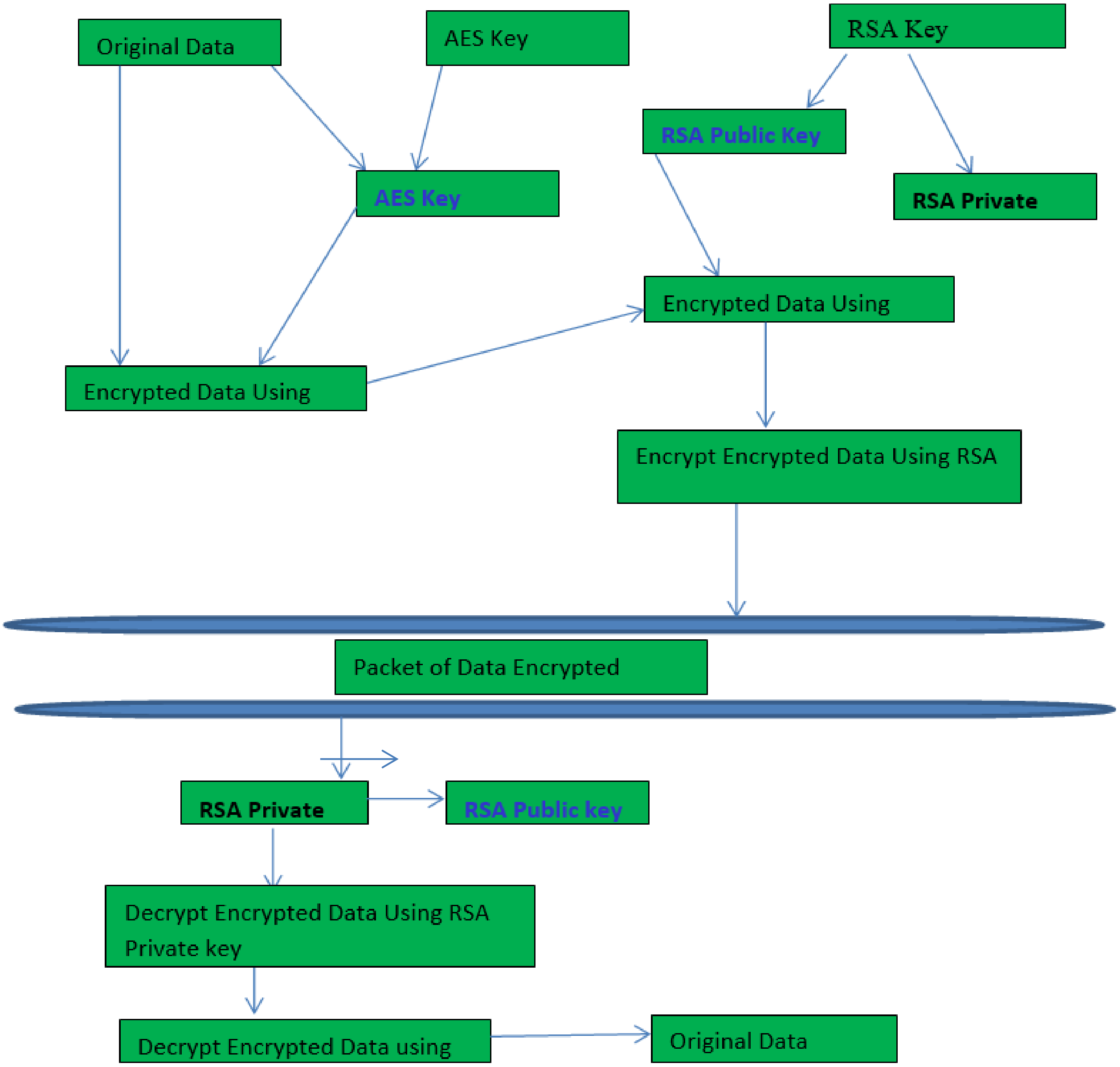


Fig 4: *Proposed algorithm structure*

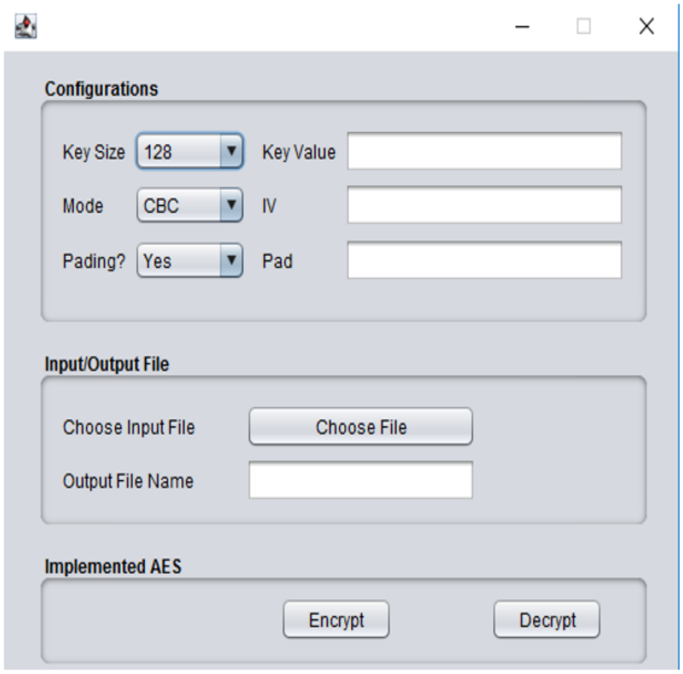
The above figure illustrated in detail on how the proposed algorithm encrypt and decrypt fileusing different steps to ensure maximum security of file.

The effectiveness of the proposed algorithm would be measured base on time. Accuracy can only be determine if ensure that the particular file size encrypted can be decrypted successfully without missing any part of it. When the above condition was achieved then the algorithm provided high accuracy required due to security level and less time taken.

V. RESULT ANALYSIS

The analysis section of this research uses Java Programming Language (ECLIPSE IDE) to realize and compile algorithm using Windows 10 operating system. All type of file can be encrypted weather text file, image file, video file etc with different size.

The proposed algorithm requires AES and RSA Keys to encrypt and decrypt any size of file. The system requires the user to import the file that is needed to be encrypted and decrypted from any location in the computer. After importing the file the user will set the encrypted file name with .enc extension in the space provided as shown in the figure below.



Configurations

Key Size 128 ▾ Key Value

Mode CBC ▾ IV

Pading? Yes ▾ Pad

Input/Output File

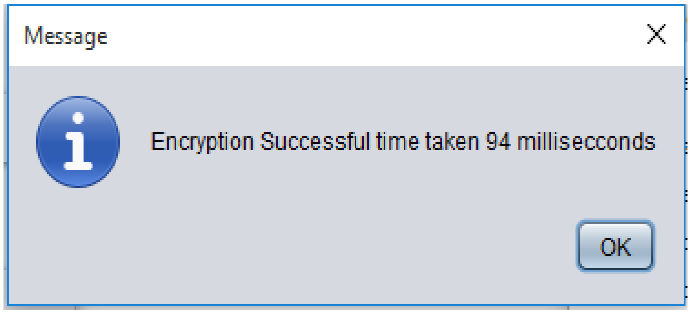
Choose Input File [Choose File]

Output File Name

Implemented AES

[Encrypt] [Decrypt]

Fig 5: layout and some component added

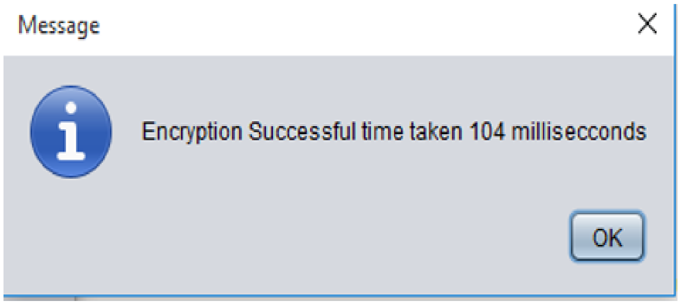


Message

Encryption Successful time taken 94 millisecconds

[OK]

Fig 6: 25kb file Encryption function called and was successful

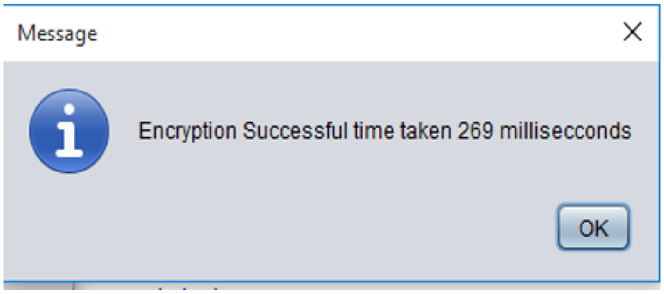


Message

Encryption Successful time taken 104 millisecconds

[OK]

Fig 7: 50kb file Encryption function called and was successful



Message

Encryption Successful time taken 269 millisecconds

[OK]

Fig 8: 1mb file Encryption function called and was successful

When the file selected for encryption was successfully encrypted using the provided keys and save in the project folder, it will be decrypted using the below code when the need for decryptionarisen. For the file to be decrypted the keys must be used and the file should be selected from theproject folder since it was automatically saved there.

The table below shows the result of files encrypted using AES, RSA and proposed algorithm with different size and format; the result analysis was based on the time parameter to determine the speed of the proposed algorithm

Table 1: Encryption time of AES, RSA and Proposed algorithm

S/NO.	File Size/mb	AES Encryption Time/ms	RSA Encryption Time/ms	Proposed Algorithm Encryption Time/ms
1	25kb	550	560[11]	94
2	50kb	600	800[11]	104
3	1mb	610	1400[11]	269

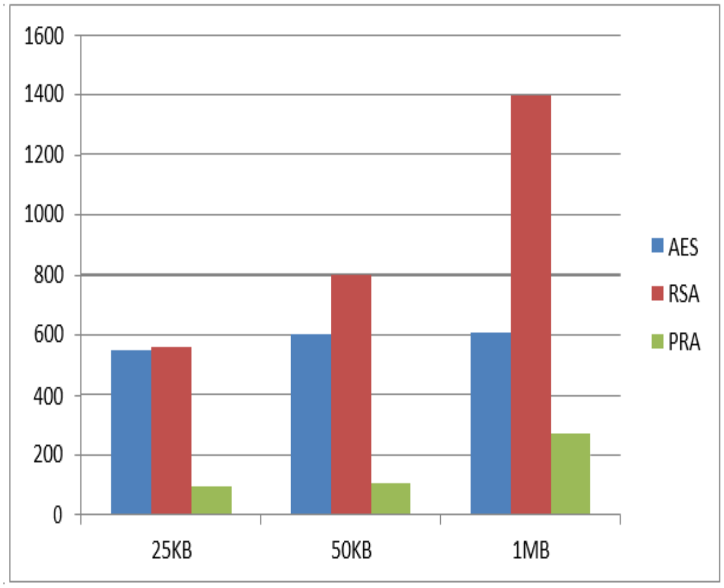
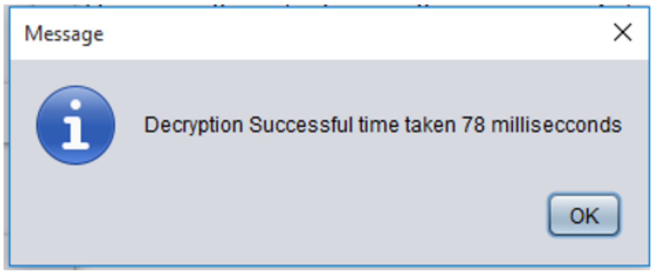


Fig 9: encryption time for AES, RSA and proposed algorithm

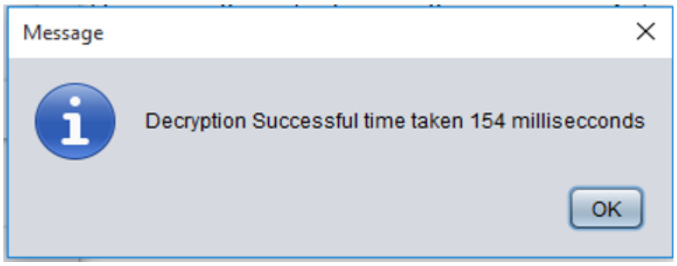
Table 2: Decryption time of AES, RSA and Proposed algorithm

S/NO.	File Size/mb	AES Decryption Time/ms	RSA Decryption Time/ms	Proposed Algorithm Decryption Time/ms
1	25kb	370	320	78
2	50kb	600	580	154
3	1mb	600	850	267


Message

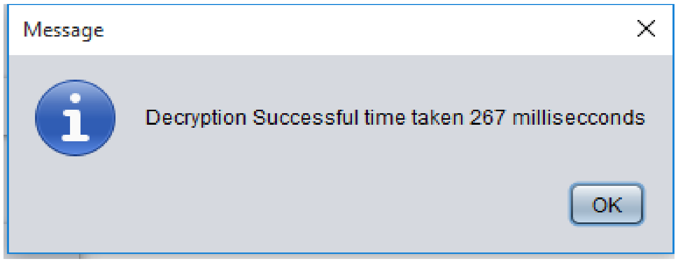
Decryption Successful time taken 78 millisecconds

Fig 10: 25kb decryption time/ms


Message

Decryption Successful time taken 154 millisecconds

Fig 11: 50kb decryption time/ms


Message

Decryption Successful time taken 267 millisecconds

Fig 12: 1mb decryption time/ms

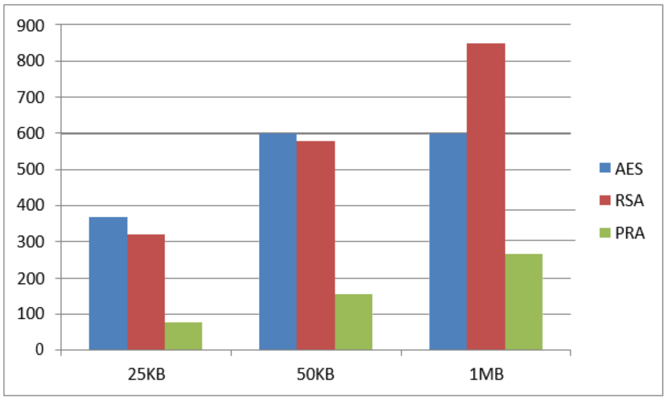


Fig 13: Decryption time for AES, RSA and proposed algorithm

Note:

AES stand for AES Encryption time/msRSA stand for RSA encryption time/ms
PRA stand for Proposed algorithm encryption time/ms

In this research Symmetric and Asymmetric encryption algorithms have been analyzed. According to the study each algorithm has its own benefits to different needs. Shortly, Asymmetric Encryption provides better security but cannot be able handle large file. AES, on the other hand, is fast and feasible to use but it has key management problem.

Symmetric Encryption provides better speed than that of public key encryption. Strength of each algorithm depends upon key management, key size, type of cryptography, number of keys etc.

The result of the analysis in encryption of RSA algorithm shows that it has higher security level but only handle small file size and a lot of time and power, the AES algorithm can handle large size of file but have key management problem, and therefore it is less secured.

When considering the security level of the proposed encryption algorithm, it is very secured due to the double key used for encryption and decryption and it can handle large volume of data in a very limited time and less power consumption Compared to that of RSA algorithm, therefor possibility to maximum accuracy is higher in the proposed algorithm compared to that of AES and that of RSA algorithms.

VI. CONCLUSION AND FUTURE WORK

The technique of file encryption and decryption using only RSA algorithm is somewhat involvedsome difficulties since RSA encryption has a very low limit of data due the high power consumption during encryption and decryption. To over the above problems and enable us to encrypt larger quantities of data, we need to use one of the symmetric type of algorithm such as AES for encryption and asymmetric type of algorithm such as RSA for encrypting the AES encrypted file. The new algorithm that combined the features of two algorithms has solved the problem of key movement in a symmetric encryption algorithm and the problem of high power consumption of asymmetric encryption algorithm.

The research is able to encrypt and decrypt the particular size of file successfully and obtain the time elapse for encryption and decryption. There may still have some deficiencies in the study, such as the When the double key is cracked, data tampering and forgery become possible, which will be the subject of future research.

REFERENCES

[1]. S. A. Ahmad, "Computing : A Review," *2019 15th Int. Conf. Electron. Comput. Comput.*, no. Icecco, pp. 1–6, 2019.

[2]. A. Muhammad Abdullah and A. Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt," no. June, 2017, [Online]. Available: https://www.researchgate.net/publication/317615794.

[3]. D. N. Sengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security,"*Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 5, pp. 4146–4152, 2015, doi: 10.15680/ijircce.2015.0305106.

[4]. E. Mutabaruka, M. Ndego, and M. W. Kimwele, "Enhancing Data Security By Using Hybrid Encryption Technique (Advanced Encryption Standard And Rivest Shamir Adleman)," vol. 2, no. 5, pp. 1–18, 2015.

[5]. S. S. Thapar and H. Sarangal, "A Study of Data Threats and the Role of Cryptography Algorithms," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, pp. 819–824, 2019, doi: 10.1109/IEMCON.2018.8614943.

[6]. S. Sharma and Y. Gupta, "Study on Cryptography and Techniques," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 1, no. 2, pp. 2456–3307, 2017,[Online]. Available: www.ijsrcseit.com.

[7]. A. E. Taki and E. Deen, "Design and Implementation of Hybrid Encryption Algorithm," *Int. J. Sci. Eng. Res.*, vol. 4, no. 12, pp. 669–673, 2013.

[8]. S. Omer, A. Faroog, M. Koko, A. Babiker, and N. Mustafa, "Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication," *IOSR J. Comput. Eng. Ver. III*, vol. 17, no. 1, pp. 2278–661, doi: 10.9790/0661-17136269.

[9]. R. Banerjee, A. K. Chattopadhyay, A. Nag, and K. Bose, "A nobel cryptosystem for group data sharing in cloud storage," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 728–731, 2019, doi: 10.1109/CCWC.2019.8666561.

[10]. J. Toldinas, V. Stuikys, R. Damasevicius, G. Ziberkas, and M. Banionis, "Energy efficiency comparison with cipher strength of AES and Rijndael cryptographic algorithmsin mobile devices," *Elektron. ir Elektrotechnika*, vol. 2, no. 2, pp. 11–14, 2011, doi: 10.5755/j01.eee.108.2.134.

[11]. Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *ProcediaComputer Science*, *78*, 617-624.