An Improved Cryptographic Scheme Using AES & RSA Algorithms for Maximum Security in File Encryption and Decryption

Sa'idu Sani

Department of Computer Studies
Hassan Usman Katsina Polytechnic
Katsina

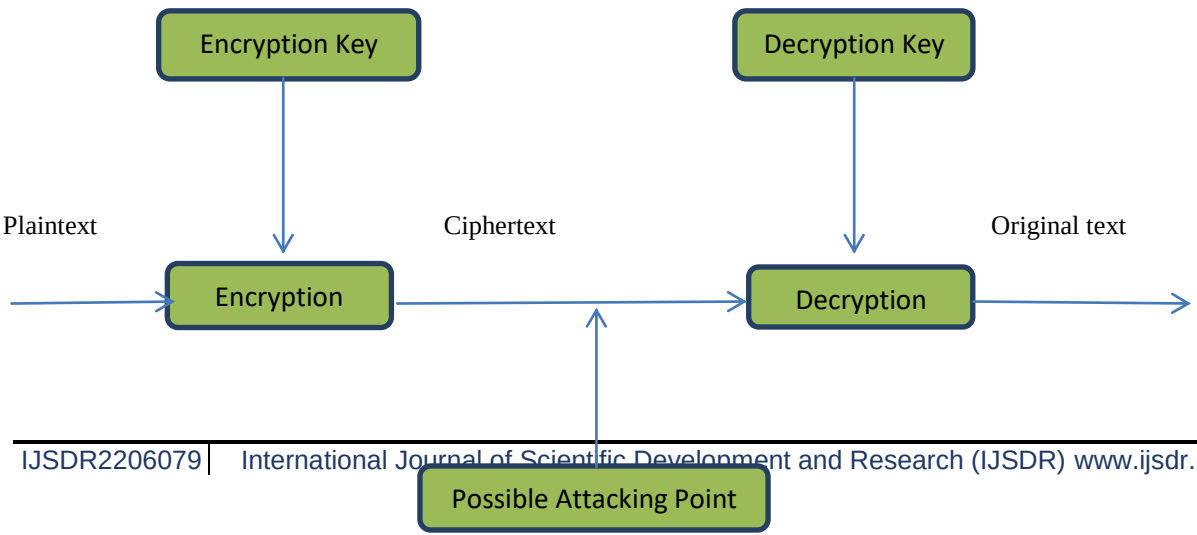
Abstract:

Cryptography was provided to secure communication between two parties known as sender and receiver in the presence of malicious third-parties known as attackers using the process called encryption. Encryption uses an algorithm and a key to transform an input into an encrypted output. The given algorithm transforms the same plaintext into the same cipher text if the same key is used. The objective of this research is to propose an improved cryptographic algorithm that would combined the two different algorithms and 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 speed of encryption and decryption and increases the security level as it uses more than one key.

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

1. Introduction

Due to the emergence of the mobile network, online documents have gradually entered people's lives, due to their easy modification and transferring from one point to another, therefore they are widely used. There are still exist many security risks for data in the computer, which include relying on software in file encryption, insufficient data encryption, and brute force attacking of encrypted data. Once the important part of the data is leaked, it will pose a serious security threat to individuals, businesses and even national security. The research paper focuses mainly on the typical representative of AES algorithm in symmetric encryption algorithm and the RSA algorithm in asymmetric encryption algorithm. Many scholars have regarded the research as a very important topic. Some scientist demonstrated the application of RSA algorithm in file encryption, and proposed that small files can be encrypted using RSA algorithm[1] . Although the technique makes full use of the key management advantages of RSA, but the encryption of very large files has not been solved due to the low speed in RSA algorithm is not efficient[2]. "cipher text misappropriation" in the AES algorithm to optimize the file encryption and resolve the problem of grouping data of the data to be processed, but the security of the AES algorithm did not consider, which may still be attacked under certain conditions[3]. Although the AES and the RSA algorithm have been widely used in the field of cryptosystem, also there are still some problems in terms of encryption security and encryption efficiency. In this research paper, considering the existing RSA and AES algorithms used in file encryption alone in the application of some problems, make full use of the AES encryption speed, high security RSA and strong key management characteristics of RSA, put forward a combination of AES encryption algorithm and RSA encryption algorithm, and apply it to file encryption[4]. In the experiment, java programming language was used to implement the algorithm; the hybrid algorithm has the advantages of verifying the performance of encrypted files. The figure below illustrates the encryption and decryption process.



2. Related Literature

Thapar, S.S. and H. Sarangal. In their article "*A study of data threats and the role of cryptography algorithms*", At 9th Annual Information Technology, Electronics and Mobile Communication Conference, 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 type of security keys used to encrypt/decrypt the data[6]. Asymmetric and symmetric encryption techniques fall under these two groups.

In the article "Comparative analysis of cryptographic algorithms" by Hercigonja, Z. Asymmetric cryptography includes RSA, which is a public key cryptographic algorithm. The key's asymmetry is achieved by multiplying two huge prime numbers together. Messages encrypted with the public key can be decrypted with the private key in a reasonable amount of time. 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 composite n, then finding a value m such that C=me(mod n), where (n,e) is the public key and C is the cypher text.

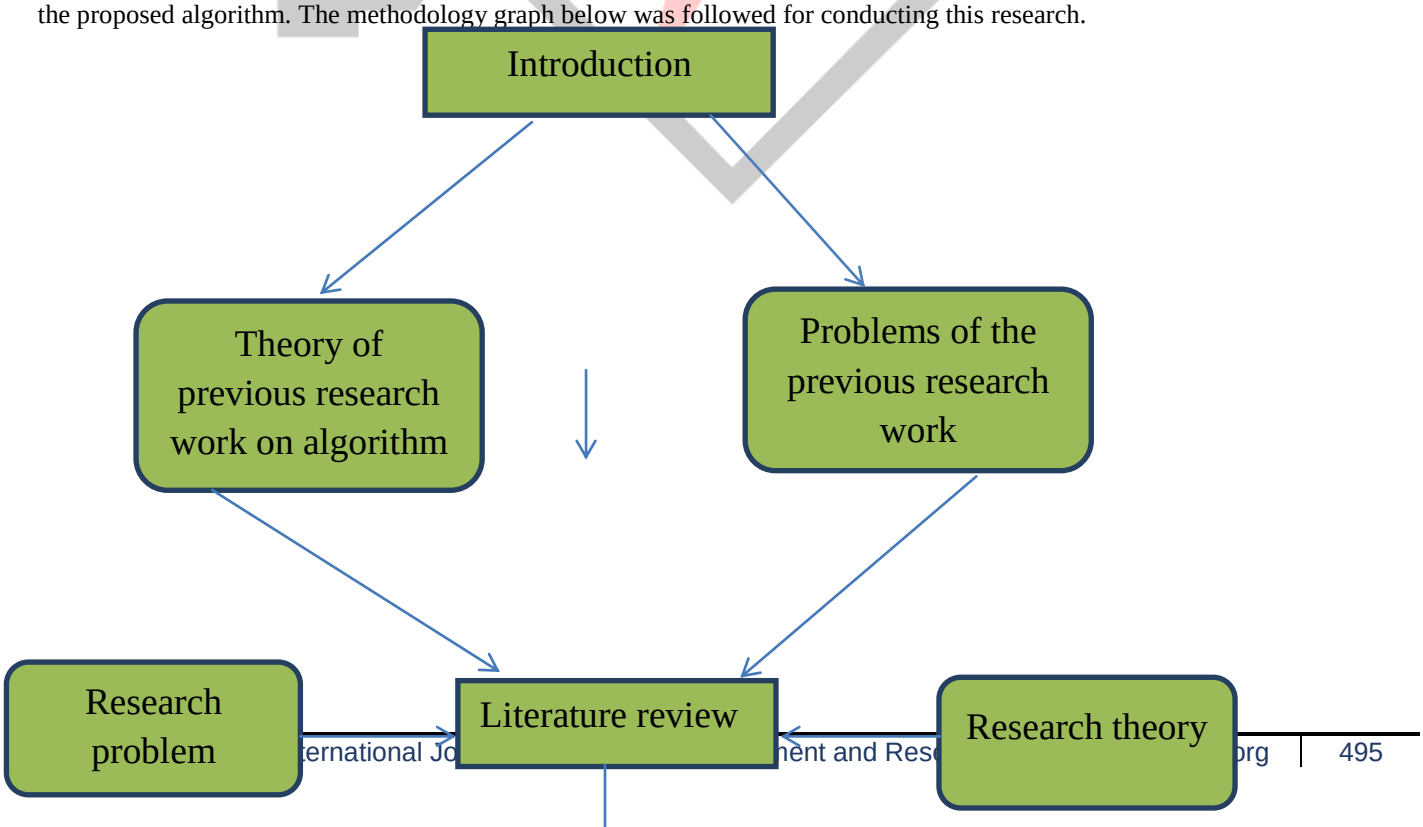
B.E.H.H. Hamouda, Different cryptography methods are compared. In response to the increasing possibility of assaults against DES, the National Institute of Standards and Technology (NIST) issued a request for proposals for an official successor that meets 21st-century security requirements.

S. Koko and A. Babiker We compare the measured encryption speed to several methods included in 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 in such a cryptosystem, as opposed to the decryption key, which is kept private. This asymmetry is predicated in RSA on the factoring problem, which is the practical difficulty of factoring the product of two large prime integers. Ron Rivest, Adi Shamir, and Leonard Adleman, who initially publicly revealed the method in 1977, are known as RSA. [10].

3. Methodology

Research is the process to collect knowledge about the given topic. Research is the process of investigation. In the research one came make his project more meaningful and effective.Using a good research methodology or research methods for a particular project then the probability of error and bugs may be less.The below diagram describes the step by step used in this research. Firstly topic was chosen and information was collected about the topic from previous research work. After that analysis was done on the research problems given by other authors. After the analyzing the problems of the previous research then modified hybrid algorithm was proposed and find out the solution.Java programming language (Eclipses IDE) was used for the implementation of the proposed algorithm. The methodology graph below was followed for conducting this research.



Qualitative and quantitative research methodology is major research methodology used for the Research work. After using both methodologies result will be highlighted in detail and conclusion of my research described

4. Proposed Work

The application of many different cryptography techniques can provide a solution for various weaknesses that are being faced in a security cryptographic system including:

1. Key encryption management ensures all the security goals are considered.
2. To achieve secure communication application allowing users to exchange information/data via Internet.
3. There should have implemented cryptographic algorithm checked, tested and reliable since people exchanging a lot of data.

To ensure the data security, it uses the applications of different activities. Data encryption and decryption are made using the AES key algorithm. AES-Key generated cipher text will be encrypted using RSA key algorithm, which ensures the data integrity, authentication and non-repudiation will be saved.

Proposed hybrid encryption technique follows the following steps:

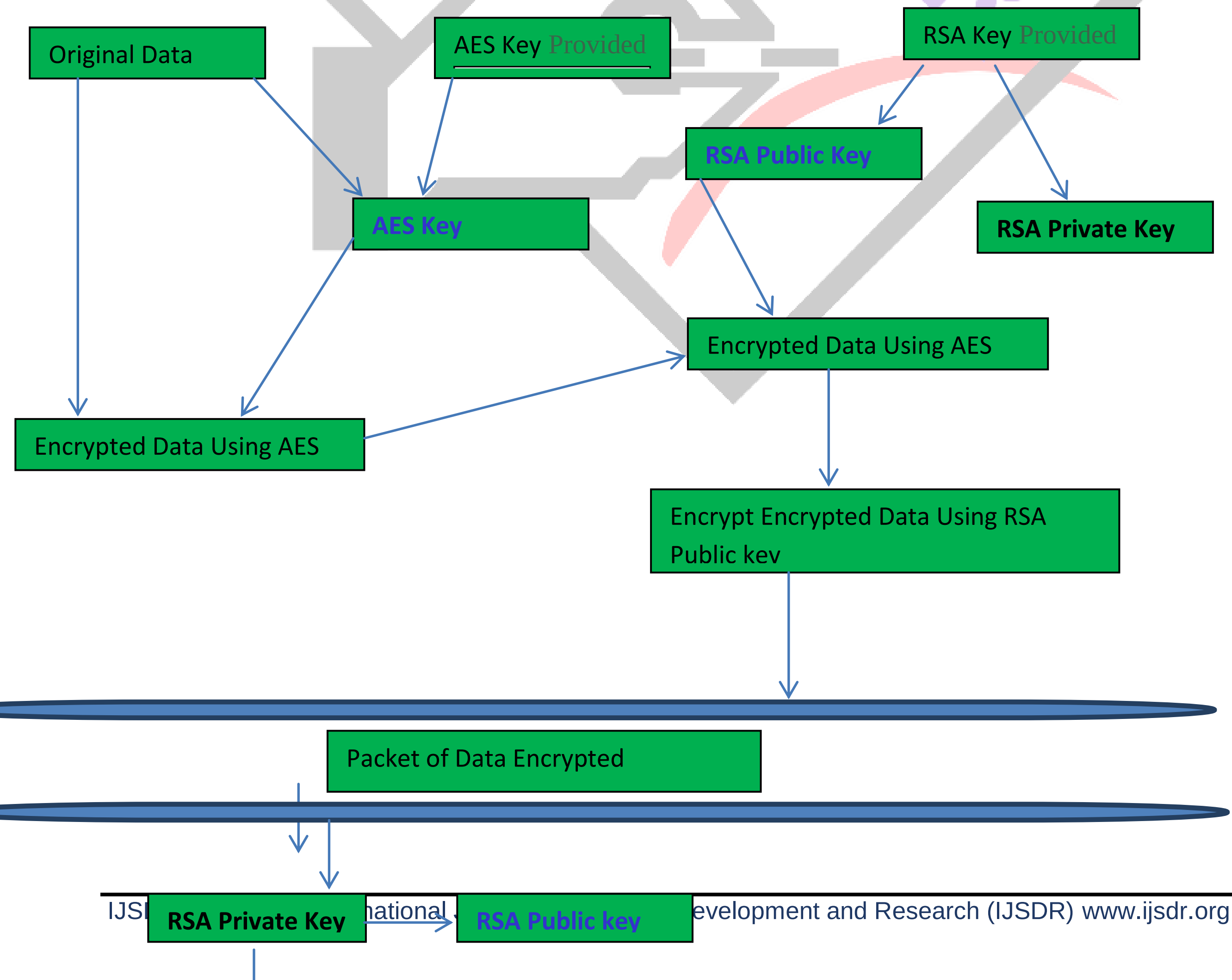
Encryption:

- Provide AES key
- Provide RSA public key
- . Provide RSA private
- Get the data to be encrypted
- Encrypt data 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:



5. Result Analysis

The analysis section of this research uses Java Programming Language (ECLIPE IDE) to realize and compile algorithm under the support of Windows 10 operating system. All files type can be encrypted weather text file, image 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**.** The table below shows the result of files encrypted using AES, RSA and proposed algorithm with different size and format.

Table 5.1: Result of encryption for AES, RSA and proposed algorithm

S/NO.	File Size/mb	AES Encryption Time/s	RSA Encryption Time/s	Proposed Algorithm Encryption Time/s
1	1.5	0.22	19.5	4.0
2	2.16	0.29	28.2	6.0
3	2.63	0.37	30.5	7.0
4	3.06	0.45	40.5	8.0
5	3.79	0.55	45.7	10.0

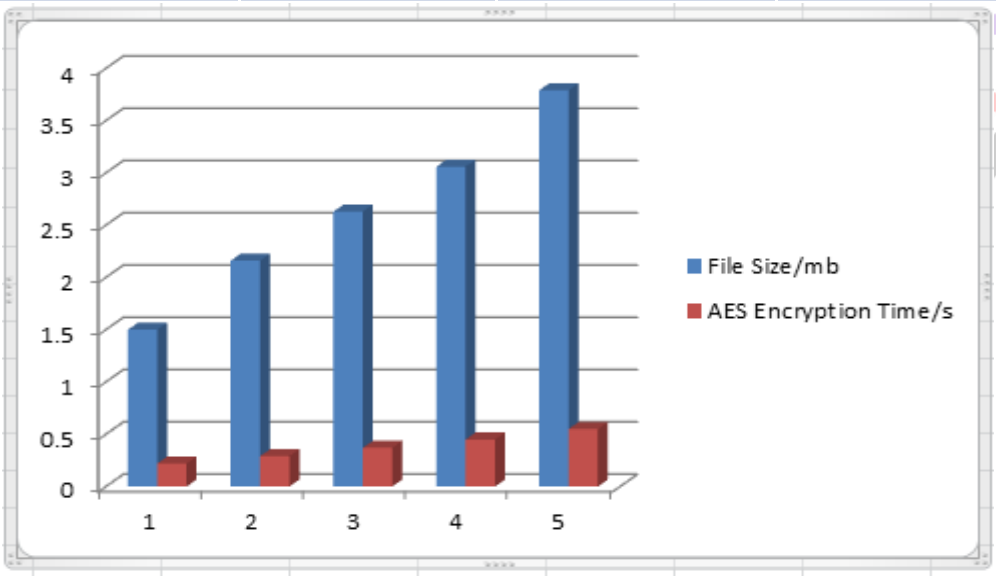


Figure 5.1: EAS encryption time/s

The above figure shows that the AES encryption time increase with the increase of file size significantly

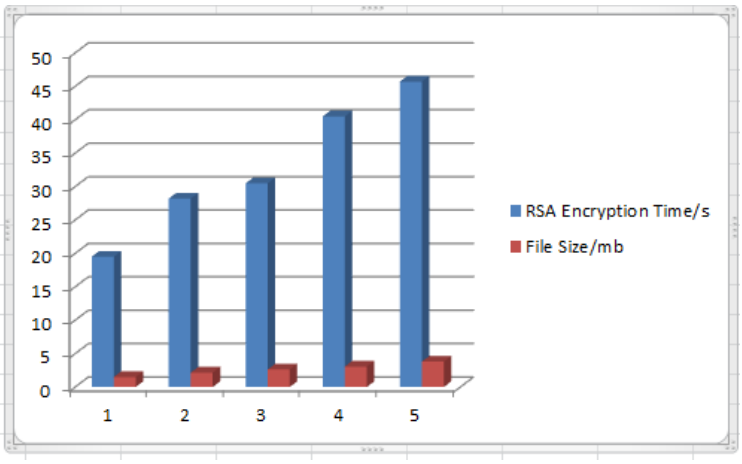


Figure 5.2: RSA encryption time/s

In RSA the encryption time is much higher than that of AES but, it also increase with the increase of file size.

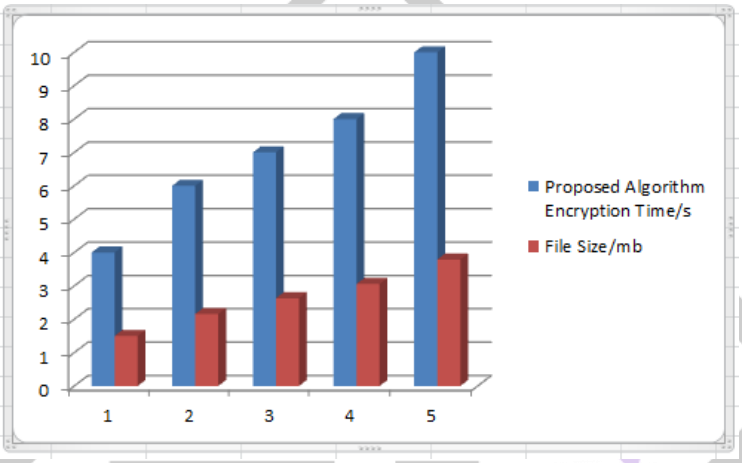


Figure 5.3 Proposed algorithm encryption time/s

The proposed algorithm encryption time is little bit higher that of AES algorithm but the security strength have been increase due to the double key uses and lower than that of RSA algorithm

Table 5.2: Decryption result of AES, RSA and proposed algorithm

S/NO.	File Size/mb	AES Decryption Time/s	RSA Decryption Time/s	Proposed Algorithm Decryption Time/s
1	1.5	0.27	40.1	4.0
2	2.16	0.29	53.0	6.0
3	2.63	0.38	55.7	8.0
4	3.06	0.46	67.7	9.0
5	3.79	0.57	79.6	11.0

Figure 5.4: AES decryption time/s

The above figure illustrate the decryption time of ESA using different file size. The result shows that there is an increase of decryption time with the increase of file size.

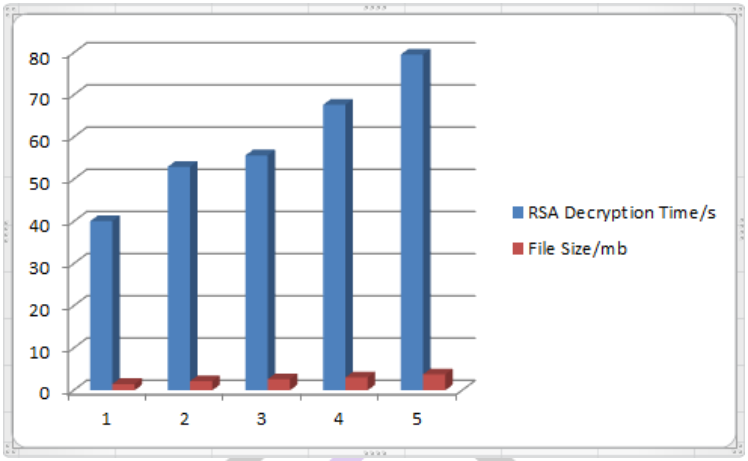


Figure 5.5: RSA decryption time/s

As in the encryption time, RSA has the higher decryption time compare to AES and proposed algorithm and the time also increase with the increase of file size.

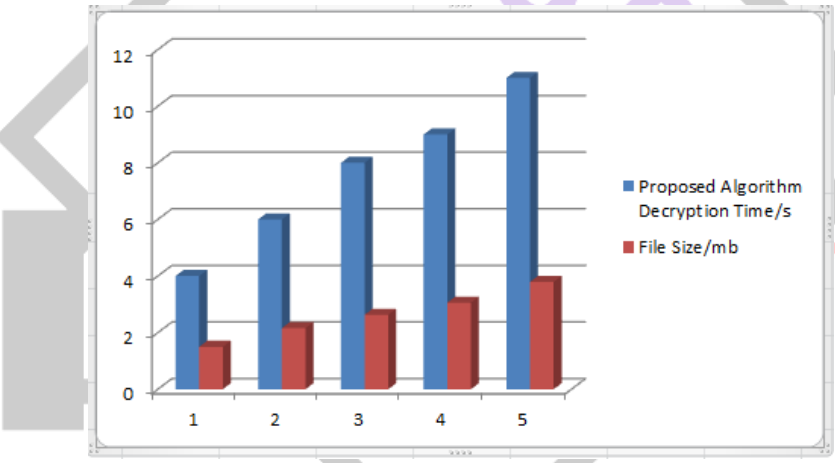


Figure 5.6: Proposed algorithm decryption time/s

The result of the analysis in encryption time of RSA algorithm and that of AES algorithm increases with the increase of file size. But RSA algorithm increases greatly, almost linear growth, AES algorithm has small increase and proposed algorithm also increase small with the increase of file size. When considering the decryption time of the proposed encryption algorithm, it is stable near a certain value, close to that of AES algorithm. Compared with the RSA algorithm and the increase of decryption efficiency have a significant effect under large files

6. Conclusion and Feature work

The technique of file encryption and decryption using only RSA algorithm is somewhat involved some difficulties since RSA encryption has a very low limit and very slow on the data that can be encrypted. 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 will solve the problem of key movement in a symmetric encryption algorithm and the problem of slowness of asymmetric encryption algorithm.

The research is able to encrypt and decrypt the particular size of file successfully. There may still have some deficiencies in the study, such as the data tampering and forgery when the double key is cracked, which will be another further study in future

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 algorithms in mobile devices," *Elektron. ir Elektrotechnika*, vol. 2, no. 2, pp. 11–14, 2011, doi: 10.5755/j01.eee.108.2.134.