International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Encryption Data Measurement and Data Security of Hybrid AES and RSA Algorithm

Khet Khet Khaing Oo[1], Yan Naung Soe[2]

[1]Faculty of Computer System and Technology,
[2]Faculty of Information Technology Support and Maintenance,
[1,2]University of Computer Studies, Myitkyina, Myanmar

ABSTRACT

Transferring the secure data becomes vital for the important data of every day's life. The system is a secure data transferring, combining the two techniques, Advance Encryption Standard (AES) and RSA. The data file is encrypted by using AES with the randomly generated key. This key is also encrypted by RSA using the receiver's public key. The encrypted data file and encrypted key file are combined to form an output file to send to the receiver. The file at the receiver's side is separated into two files, the encrypted data file and encrypted key file. The encrypted key file is decrypted by RSA method using the receiver's private key. The AES key is acquired, the encrypted data file is then decrypted by AES method using the acquired AES key. The system includes file transferring process based on the Java socket technology.

Key Words: *AES (Advanced Encryption Standard) and RSA (Rivest, Shamir and Adleman) algorithms*

How to cite this paper: Khet Khet Khaing Oo | Yan Naung Soe "Encryption Data Measurement and Data Security of Hybrid AES and RSA Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.834-838, URL: https://www.ijtsrd.com/papers/ijtsrd29243.pdf

IJTSRD29243

1. INTRODUCTION:

To introduce cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Regardless of who is involved, to one degree or another, all parties to a transaction must have confidence that certain objectives associated with information security have been met.

Conceptually, the way information is recorded has not changed dramatically over time. Whereas information was typically stored and transmitted on paper, much of it now resides on magnetic media and is transmitted via telecommunications systems, some wireless. What has changed dramatically is the ability to copy and alter information. Someone can produce thousands of identical copies of a piece of information stored electronically and each is indistinguishable from the original. With information on paper, this is much more difficult. What is needed then for a society where information is mostly stored and transmitted in electronic form is a means to ensure information security which is independent of the physical medium recording or conveying it. The objectives of information security rely solely on digital information itself [3].

To gain more secure data transferring, the developments of the encryption methods have been established. Since there are two types of encryption method, one uses the public key encryption and the other use the private key encryption. The public key encryption methods use a pair of two key. One of them is used at the encryption step. This is known as the public key. This key is public for everybody who would like to send data. The other one is used at the decryption step. This is known as the private key. The pair of two keys method is known as asymmetric type of encryption. One of the most popular encryption methods of this type is RSA. The other type of encryption method uses the same key for the encryption steps and decryption steps. This method is type of symmetric type of encryption. One of the most popular encryption methods of this type is Advanced Encryption Standard (AES).

The system is a type of a crypto system. It is a file encryption system. The system will accept a file from the user and performs the necessary encryptions. In this step of encryption, there will be actually two encryption methods but in a combined manner for the system's security affairs. To get the better security for system, the system is considered to use both encryptions as a hybrid system.

The system is composed of two main portions. They are the crypto techniques and the communication technique. The system can also send and receive the data files. The system uses the socket technology supported by JAVA.

2. RELATED WORKS

T. Mrokel expressed that encryption can be traced back for thousands of years. Since people first started to use encryption methods, the techniques that we know and use today have come a long way. The purpose of this paper is to construct a timeline of important encryption events that have occurred throughout the ages, and to discuss current and future encryption methods. Each event in the timeline is further researched and presented in more detail. Added attention is given to quantum encryption, the latest addition to encryption techniques. In this paper, different encryption techniques are evaluated, especially from a business perspective, and compared according to a set of criteria [5].

Syed S. Rizvi presents the implementation of a secure application for an academic institution that offers numerous services to both students and the faculty. The primary focus of this paper is to provide a technical implementation of a new architecture for encrypting the database. The scope of this paper mainly includes but is not limited to symmetric and public-key cryptography, authentication, key management, and digital signatures. The final results of this paper demonstrate that what security features one should implement in order to achieve a highly secured application. This paper presents the implementation of a stand alone system that can be implemented on any legacy systems, and still operates effectively. In other words, it is self sufficient in terms of the data that it stores [4].

3. BACKGROUND THEORY

3.1. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, enhanced from AES originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.

The Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. Rijndael (pronounced [rɛinda:l]) is a portmanteau of the names of the two inventors.

AES is based on a design principle known as a Substitution permutation network. It is fast in for implementation with software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key [2][1].

3.2. RSA Encryption Method

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by encoding the message as a number M in a predetermined set. That number is then raised to a first predetermined power (associated with the intended receiver) and finally computed.

The remainder or residue, C, is... computed when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver) [2].

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation: RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Encryption: The sender of the message uses the public key of the receiver and encrypts the message by mathematical calculations defined for RSA encryption.

Decryption: After the receiver received the encrypted message (cipher-message), the receiver decrypt the encrypted message using the private key of the receiver by mathematical calculations defined for RSA decryption [6].

4. OVERVIEW OF THE SYSTEM

The system is an implementation for secure data transfer for local area network as a portable program structure. The symmetric key encryption uses the same key for encryption and decryption. For the asymmetric key encryption, a key is applied for encryption and the other key is applied for decryption.

The system comes in contact with the two encryption method. The data file being transferred is being encrypted by the symmetric key encryption. The key for the former encryption is also encrypted by the asymmetric key encryption method. The former encryption applied for the system is Advanced Encryption Standard (AES). And the later encryption is the RSA encryption system. The two encrypted files are combined to form a file. The result file is sent from the send to the receiver. At the receiver side, there will be an accepted file. This file has to be separated by the system running at the receiver's side. Then the two files will be gained. One file is the encrypted AES key file and the other file is a encrypted data file.

The encrypted AES key is first decrypted by means of the RSA decryption using the receiver's private key. The applied AES key is gained. The system will use this key to decrypt the encrypted data file by means of AES decryption method.

The system is aimed to develop the secure data transfer for any types of data file such as audio file, movie file, DBMS file. The system also aimed to be in portable program structure. The system just only needs the JAVA run time environment, no other web features are not necessary for the system to be executed.

The overview of the system is divided into sender side and the receiver side. The figure 1 shows the overview of the system for the sender's side. The figure 2 shows the overview of the system for the receiver's side.

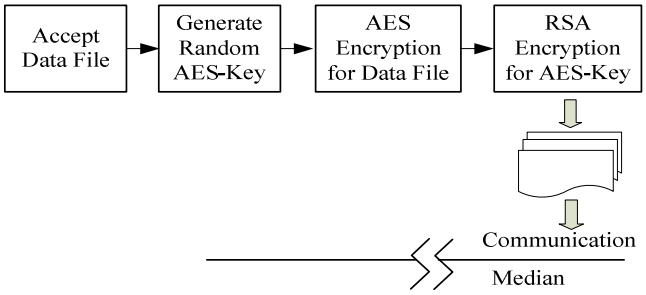

Figure1. Overview of the system for the sender's side

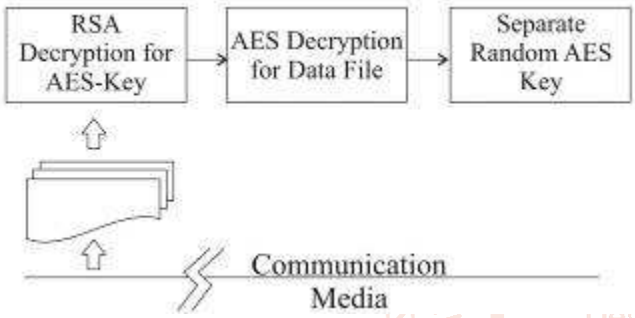

Figure2. Overview of the system for the receiver's side

At the two end points of the communication median, there will be two instances of system at each end point. The two instances of the system will be running at both end points.

The system accepts the file to be transmitted on the communication media, performs the random generation of AES key, perform the encryption with AES, encryption of the AES key with RSA and sending the encrypted files to the send. These activities are of the sender's side of the system.

The system accepts the file from the communication-media, performs the RSA decryption technique to encrypted file of AES-Key, performs the AES encryption to the encrypted data file sent from the sender. These activities are of the receiver's side of the system.

5. SYSTEM DESIGN AND IMPLEMENTATION

The system can be divided into following steps. They are divided into sender's steps and receiver's steps. Actually, the system is a multi-threaded program. The main thread of the program is handling two sub-threads. One of the sub-threads is to accept from the user for encryption and sending to the other. The other sub-thread is to check the incoming signal from the other.

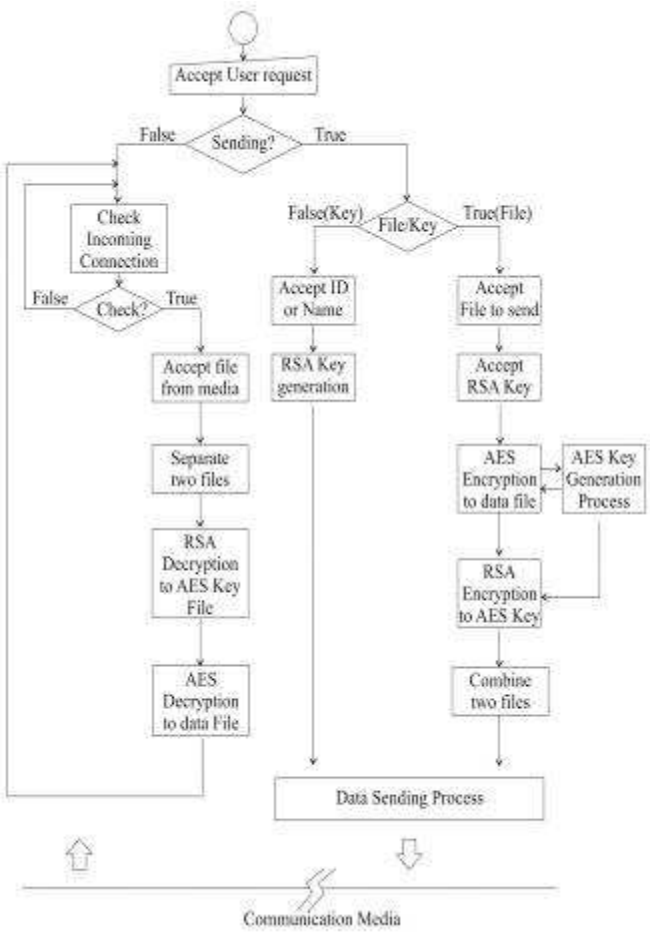

Figure3. System flow diagram of the system

The steps of the system are as follows:

1. Accept data file for encryption and sending to the others
2. Accept the RSA key from the user
3. Generate AES key process
4. Encryption process using AES method to data file
5. Encryption process using RSA method to applied AES key
6. Files Sending Process
7. Files Accepting process
8. Decryption process using RSA method to accepted encrypted AES key
9. Decryption process using AES method to accepted encrypted data file
10. Generate the new RSA key pair
11. Sending the new RSA key

The Figure 3 shows the system flow diagram of the system. The system flow diagram shows the processes of the system and the interactions among the process of the system and interactions between the user and the process of the system.

6. SYSTEM EXECUTION STEPS

On the main graphical user interface, there are three groups of buttons shown to the user. The first group of button is for crypto-activities which are encryption, decryption and generation of new RSA key pair. The second group of button is for communication-activities for sending and receiving data to and fro. The last group of button has only one button which is for terminating the system.

At this step, user has to enter or choose the input file for encryption process at the text field labeled with In File Name.

The user can click to Generate AES key for generation of AES key for this time of encryption. If the user does not generate, the recently generated key will be used at the encryption process.

The user must type or choose the file name of the RSA public key file at the text field labeled with RSA Key(receiver's public).

After the system performs the encryption, and a file will be result. This result filename for the system can be entered at the text field labeled with Out File Name.

To ask the system to perform the encryption process according to the input, the user must click the Encrypt button. At this time, the system will perform the encryption and will generate an output file of encryption process with the name at the text field labeled with Out File Name. This file has to be send to the receiver.

The user must send the encryption-output file to the receiver. The sender must start the send process by clicking the Send button of the main graphical user interface of the system. The user must enter the file name of the sending file at the text field labeled with Send File.

At the time of sending, the system at the receiver's side must start the Accept File graphical user interface by clicking the Accept button on the main graphical user interface of the system.

After file transfer has been done, the system at the receiver side must start the decryption process by clicking the Decrypt button on the main graphical user interface of the system.

User must enter the accepted sent file from the sender. This file name must be entered or chosen at the text field labeled with In File Name. Then the user must enter or choose the file name of the RSA private key file at the text field labeled with RSA key (receiver's private). The user must enter out file name at the text field labeled without file name.

7. EXPERIMENTAL RESULT

The following table, table 1, shows the run time taken by the system along with the time taken by the other encryption system.

The following figure, figure 4, shows the cluster column chart for the table1. The time taken by the system is less than the RSA encryption method and is greater than the AES encryption method.

Table1. Run time taken by the systems

File Name	AES	RSA	Proposed System AES+RSA
db1.mdb 560Kb	1200 ms	2650 ms	1355 ms
image.jpg 3255Kb	7000 ms	12355ms	8047 ms

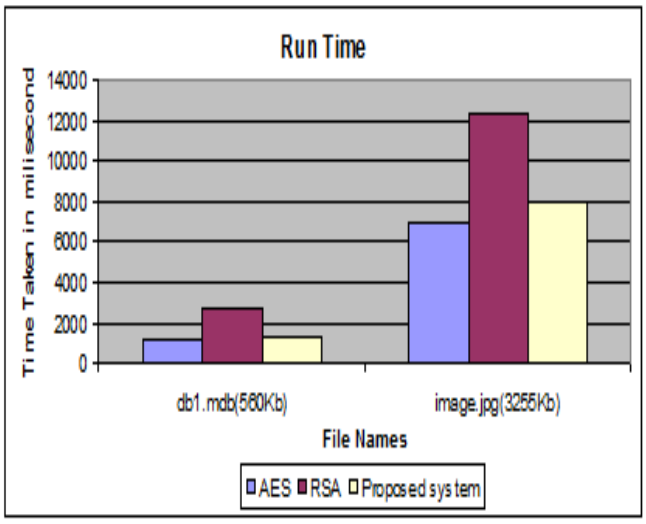

Figure4. Run time analysis of the systems

The system generates random AES Key and performs the encryption for the accepted data file. Then the applied AES key is encrypted with the RSA encryption method. The encrypted AES key and the encrypted data file are combined and sent through the communication media. At the receiver's side, the combined file is accepted. This file is split into two files, one is the encrypted AES key file and the other is the encrypted data file. The receiver uses the RSA key of its own and the AES key is decrypted with RSA method. The gained AES key is applied for the decryption with AES method for the data file.

The system is aimed to gain more security by using the random AES key. This process can make the hacking person with more difficulties. The system can also allow the users (sender and receiver) to change the RSA key pair periodically. For this process, the system can gain more security than other hybrid systems.

8. CONCLUSION

The system is a secure data transfer system using the combined method of the two encryption algorithms. The two algorithms used for the system are the Advance Encryption Standard (AES) and RSA. The system can perform the encryption and decryption of any data file. It is aimed to be applied in portable program format.

The advantages of the system are as follows:

1. The system is a more secure system than the system using only one method of encryption, such as DES, AES and RSA.
2. The system uses Random key generation for AES key and lets the user to change its keys of RSA periodically.

3. Although the system uses two encryption techniques as a hybrid system, the system takes lesser time than using only RSA method.

REFERENCES

[1] A. Menezes, P. V. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[2] E. Schaefer, Santa Clara University, "An introduction to cryptography and cryptanalysis".

[3] S. Goldwasser, M. Bellare, "Lecture Notes on Cryptography", MIT Computer Science and Artificial Intelligence Laboratory, 2008.

[4] S. S. Rizvi, International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010, "Combining Private And Public Key Encryption Techniques For Providing Extreme Secure Environment For An Academic Institution Application".

[5] T. Mrokel, Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, South Africa, "Encryption Techniques: A Timeline Approach".

[6] http://www.umich.edu/~umich/fm-34-40-2.