Nigerian Journal of Mathematics and Applications
Volume **24**, (2015), 252 – 260
©*Nig. J. Math. Appl.* *http : //www.njmaman.com*

On a Hybrid Cryptography System for Data Using Advanced Encryption Scheme (AES) and Ron Rivest Shamir Adleman (RSA) Algorithms

A. O. Babatunde* and M. O. Mohammed

Abstract

Nowadays, the use of information technology has taken over so many sectors. The survivals of many organizations are based on the information that is received or sent out. Due to the dependency on an unsecure communication network, some information that is confidential to the organization is revealed to an unauthorized user and this has necessitated the need for data security.

This research work therefore made use of two algorithms for data cryptography to produce a more secure hybrid system. To achieve this aim, Advanced Encryption Scheme algorithm is used to encrypt a message and the secret key of Advanced Encryption is in turn encrypted using Ron Rivest Adi Shamir Leonard Adleman algorithm.

This does not only produce a more secure method of data encryption, but also help to solve the problem of key sharing.

The result shows that the hybrid Cryptographic system is able to prevent data from unauthorised user.

Received November 02, 2015. * Corresponding author.

2010 *Mathematics Subject Classification.* 68P25 & 14G50.

Key words and phrases. Cryptography, Cipher, Data Communication, Public & Private key.

Department of Computer Science, University of Ilorin, Ilorin, Nigeria.

Department of Computer Science, Federal Polytechnic, Offa, Kwara State, Nigeria.

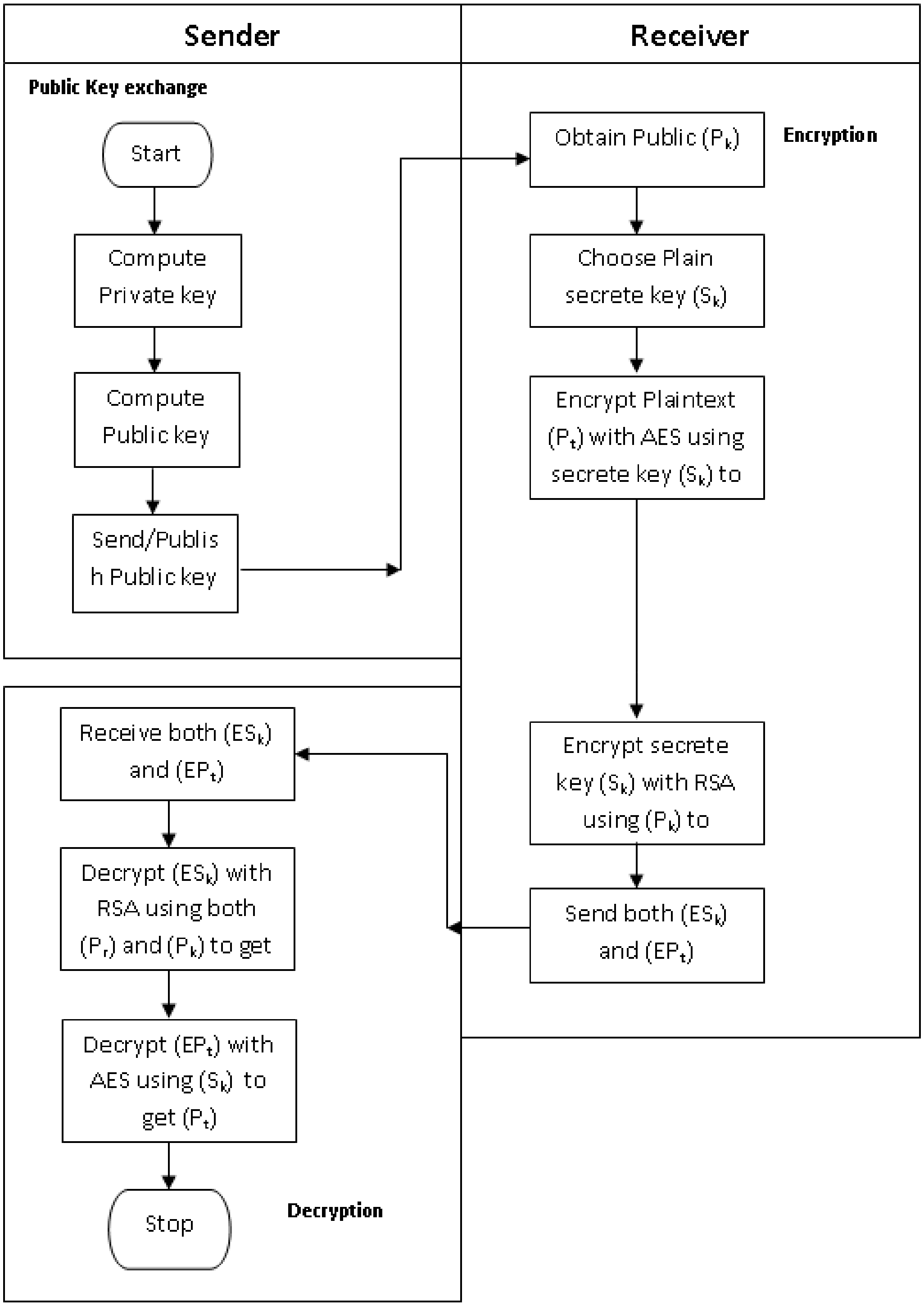
e-mail addresses: babatunde.ao@unilorin.edu.ng & mohammedmistura04@gmail.com

1. Introduction

Today, life is highly driven by Information Technology (IT). The use of IT is also playing a vital role in decision-making in all commercial and non-commercial organizations (Anwar Pasha & Riyazuddin, 2011). All activities are now centered on data, its security and storage. In the present scenario, organizations survival is at stake if its data is misused or not secured . The need to protect the organization information is therefore one of the major problems facing the organization in this world of rapid technological development. The question of data security therefore has been the topic many researchers have been trying to solve. A fundamental problem in cryptography is also how to communicate data over an insecure channel, which might be controlled by an adversary (Michel, 2001). Security is therefor a vital tool needed in every organization both public and private. The important of this concept has caught the heart of many researchers and different algorithms have been developed to solve the problem of security, however, this algorithm individually are not able to secure transfermission of data. This research therefore solved the limitation of this algorithms by hybridizing these algorithms. This hybridized system complements the weakness of each other to produce a more secure algorithm. This research therefore developed a two level data security system that will combine the strength of the two type of cryptography system to form a hybrid system that will be more secure.

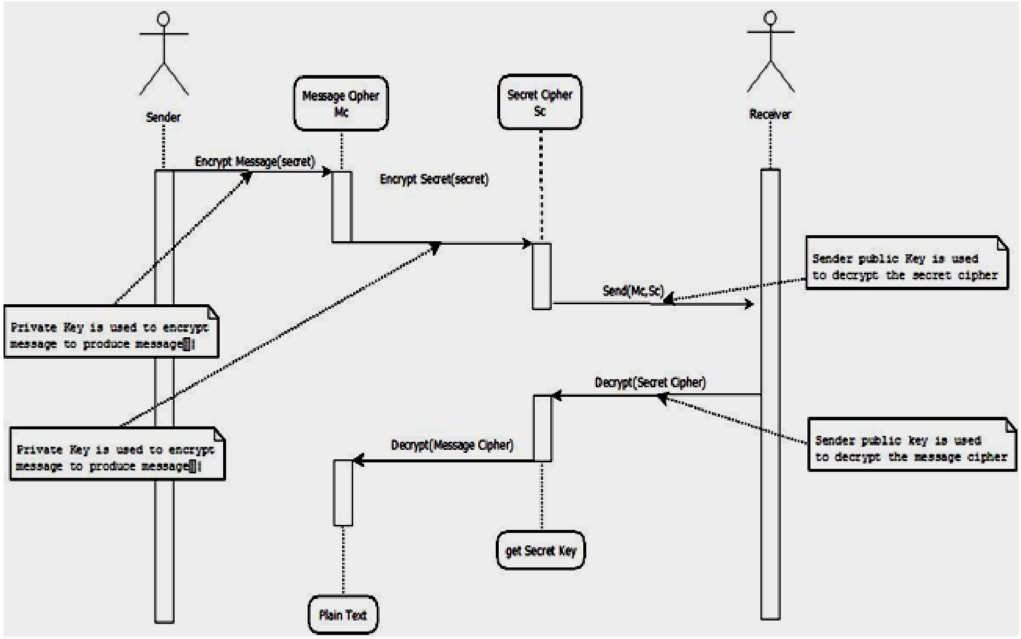
2. Material and Methods

In order to carry out the hybrid cryptography, An Advanced Encryption Scheme (AES) algorithm is used in combination with Ron Rivest Adi Shamir Leonard Adleman algorithm. The plain message is first encrypted using AES and the secret key of the AES algorithm will in turn be encrypted using the sender private key of RSA algorithm. The encrypted message and the encrypted key are then transmitted to the receiver. At the receiving end, the receiver first decrypts the message using the sender public key of RSA algorithm. The result of the decrypted key is then used as the key with which the cipher is decrypted before the text can be read. In modeling the system, the Unified Modeling Language (UML) sequence diagram and class diagram are used. The flowchart is also used to describe the flow of the program as shown in figure 1.


Sender
Receiver
Public Key exchange
Start
Compute Private key
Compute Public key
Send/Publis h Public key
Obtain Public (P_k)
Encryption
Choose Plain secrete key (S_k)
Encrypt Plaintext (P_t) with AES using secrete key (S_k) to
Encrypt secrete key (S_k) with RSA using (P_k) to
Send both (ES_k) and (EP_t)
Receive both (ES_k) and (EP_t)
Decrypt (ES_k) with RSA using both (P_r) and (P_k) to get
Decrypt (EP_t) with AES using (S_k) to get (P_t)
Stop
Decryption

Flowchart

A Sequence diagram is an interaction diagram that shows how processes operate with one another as well as their orderliness. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with case realizations in the Logical View of the system development. Sequence diagrams are sometimes called event diagrams or event scenarios. The sequence diagram of the system is shown in figure 2.

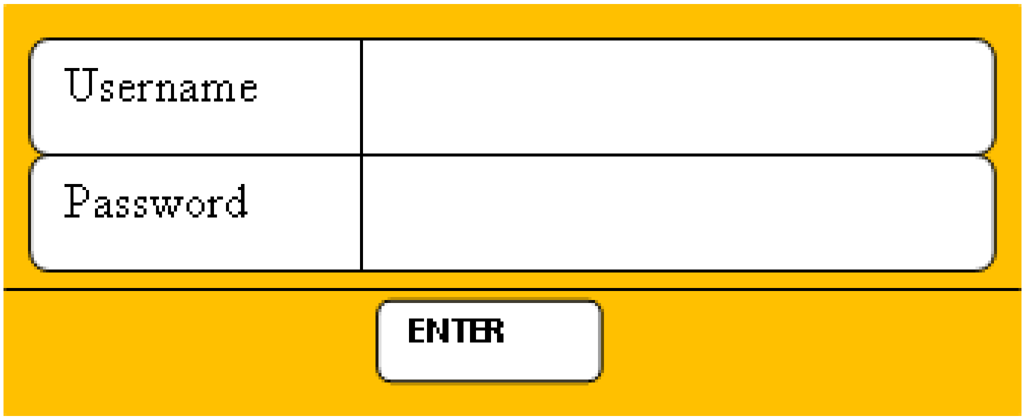

Sender
Message Cipher Mc
Secret Cipher Sc
Receiver
Encrypt Message(secret)
Encrypt Secret(secret)
Sender public Key is used to decrypt the secret cipher
Send(Mc,Sc)
Private Key is used to encrypt message to produce message
Decrypt(Secret Cipher)
Private Key is used to encrypt message to produce message
Decrypt(Message Cipher)
Sender public key is used to decrypt the message cipher
get Secret Key
Plain Text

Sequence Diagram of the system

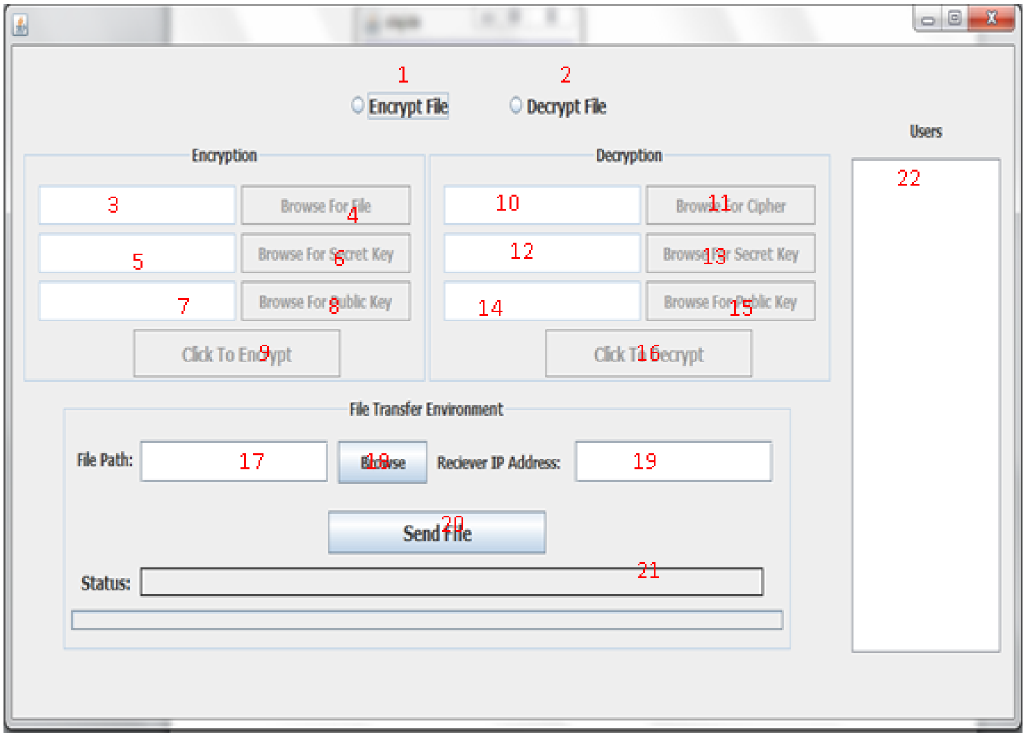
3. Result and Discussion

Form/Interface Design

This application is made up of the following forms that help the users to make judicious use of the application. They are easy to use from which a user can exploit with little or no supervision as illustrated in figures 3 and 4.



Login Interface



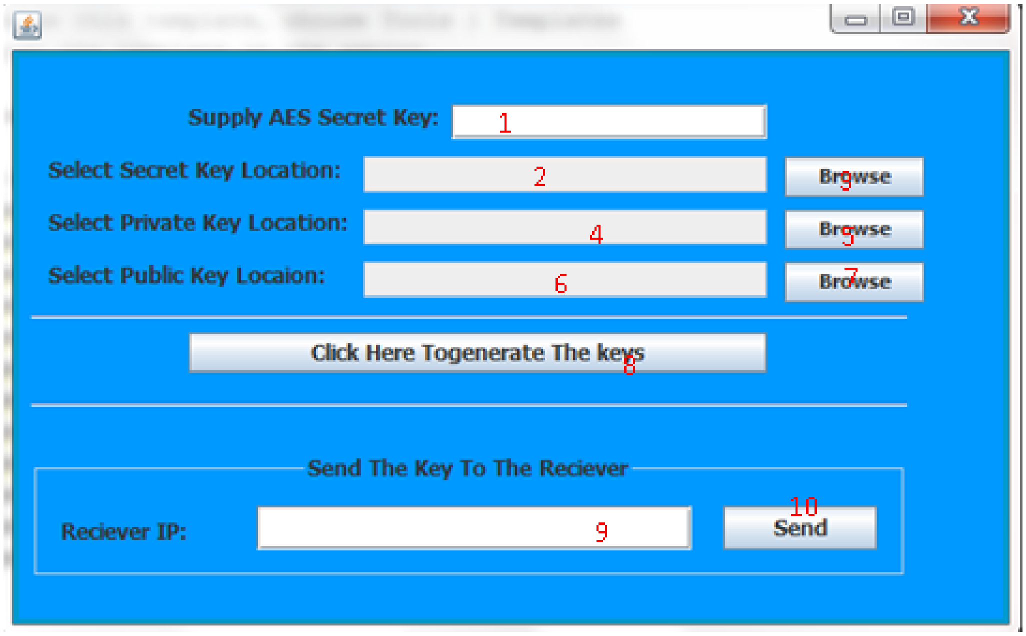
Encryption, decryption and file transfer interface

(1) This is option selected when file needs to be encrypted to enable the panel for encryption

(2) This is option selected when file needs to be decrypted to enable the panel for decryption

(3) It displays the path of the selected file to be encrypted.

(4) It allows the file chooser dialog to be display to enable the user to select to file to be encrypted.
(5) It displays the path of the encrypted secret key.
(6) It allows the file chooser dialog to be display to enable the user to select encrypted secret key.
(7) It displays the path of the public key.
(8) It allows the file chooser dialog to be display to enable the user to select encrypted secret key.
(9) It performs the encryption operation
(10) It displays the path of the selected file to be decrypted.
(11) It allows the file chooser dialog to be display to enable the user to select to file to be decrypted.
(12) It displays the path of the encrypted secret key.
(13) It allows the file chooser dialog to be display to enable the user to select encrypted secret key.
(14) It displays the path of the private key.
(15) It allows the file chooser dialog to be display to enable the user to select decrypted secret key.
(16) It performs the decryption operation
(17) Path to the file to be sent.
(18) Shows file chooser dialog.
(19) Receiver IP address
(20) Send file to the receiver


Supply AES Secret Key:
1
Select Secret Key Location:
2
Browse
3
Select Private Key Location:
4
Browse
5
Select Public Key Locaion:
6
Browse
7
Click Here Togenerate The keys
8
Send The Key To The Reciever
Reciever IP:
9
10
Send

Key Generation Interface

This field accepted the key to be used for AES secret key

(1) Displays the path to where encrypted secret file will be saved
(2) Allows users to select location
(3) Displays the path to where private key file will be saved
(4) Allows users to select location
(5) Displays the path to where public key file will be saved
(6) Allows users to select location
(7) Click to perform key generation

4. Performance Evaluation

In order to evaluate this system, Ron Rivest Adi Shamir Leonard Adleman (RSA) algorithm run side by side with Advanced Encryption System (AES) algorithm and the following parameters are used to evaluate the system.

(1) Speed of execution
(2) Input data length
(3) Key sharing
(4) Security.

The table below shows the efficiency of each algorithm after they have been subjected to each of the above parameters.

Properties	**AES Algorithm**	**RSA Algorithm**	**Hybridized Algorithm**
Speed	Faster on Large input than RSA algorithm	Very slow on large data input	Slower than AES but faster than RSA
Input length	Can work perfectly with large input data	It cannot work if the input is too large	Can work perfectly with large input data
Security	Not as secure as RSA	Very secure	Very Secure
Key Sharing	Both parties involve in the process must agree on the key to be used for encryption	The party do not need to meet before message can be encrypted or decrypted	The party do not need to meet before message can be encrypted or decrypted

Table 1.0: Performance Evaluation of the Algorithms

5. Conclusion

This research has employed the advantages of the two types of Algorithms to produce a hybrid system which is more secure and efficient compare to individual symmetric or Asymmetric cryptographic . and the hybrid cryptographic method of data security as used in this work has proved to be highly productive, efficient, and more secure.

This software can therefore be used to curb the security problem in the sectors like communication, education, government, finance, manufacturing and so many other organizations where communication of data do exist.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

References

[1] Abikoye O. C., Adewole K. S. and Oladipupo A. J., *Efficient Data Hiding System using Cryptography and Steganography*, International Journal of Applied Information Systems (IJAIS), (2012), 11-16.

[2] Anwar Pasha D. A. and Riyazuddin Q., *Transparent Data Encryption- Solution for Security of Database Contents*, International Journal of Advanced Computer Science and Applications, (2011).

[3] Asakpa S. O., *Basis of Computing*, Ilorin: Olad Publisher and Printing Enterprises. (2010).

[4] Cohen F., *Chap2-1.html.*, (1995). Retrieved January 18, 2015, from all.net: http://www.all.net/curr/ip/chap2-1.html.

[5] Conghuan Y., Zenggang X., Yaoming D., Guangwei W., Jiping L. and Kaibing Z., *Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks*, Journal of Visual Languages and Computing, (2014).

[6] Dorothy E. R., *Cryptography and Data Security*, USA: Addison-Wesley Publishing Company, Inc., (1982).

[7] Hoffstein J., Pipher J. and Silverman J. H., *An introduction to Mathematical Cryptography*, New York: Springer Science+Business Media, (2000).

[8] KRISHNA A. V., *Performance evaluation of new encryption algorithm with emphasis on probabilistic encryption and timestamp in network security*, Andhra Pradesh, INDIA.: Department of Computer Science and Engineering, Acharya Nagarjuna University, (2009).

[9] Majdi A.-q. and Lin Yi H., *Simple Encryption/Decryption Application*, International Journal of Computer Science and Security, (2007), 33-40.

[10] Mansour M. A. and Fouad M. A., *N-TEA: New Text Encryption Algorithm-Secure Data Exchange*, International Journal of Software Engineering and Its Applications, (2014), 199-206.

[11] Menezes A., Van Oorschot P. and Vanstone S., *Handbook of Applied Cryptography*, CRC Press, Inc., (1997).

[12] Michel F. A., *Design and analysis of secure encyption scheme*, San Diego: University of California, San Diego, (2001).

[13] Obaida M. A., *A New Approach For Complex Encrypting And Decrypting Data*, International Journal of Computer Networks Communication, (2013), 96-103.

[14] Olatunji Y. O., *Design and implementation of chat application with asymmetric cryptograohic system*, Ilorin: Computer Science, University of Ilorin, (2014).

[15] SANTOSH K. Y., *Some Problems in Symmetric and Asymmetric Cryptography*, AGRA: DEPARTMENT OF MATHEMATICS, DR. B. R. AMBEDKAR UNIVERSITY, (2010).

[16] Tony M. D., *A Brief History of Cryptography*, The International Student Journal, 1. wikipedia. (n.d.). Cryptography, (2009). Retrieved January 16, 2015, from en.m.wikipedia: http://www.en.m.wikipedia.org/cryptography.

[17] Williams S., *Cryptography and network security principle and practice*, Pearson Education Inc.: New York, (2011).