ARID ZONE JOURNAL OF ENGINEERING, TECHNOLOGY & ENVIRONMENT
AZOJETE December 2019. Vol. 15(4):929-938
Published by the Faculty of Engineering, University of Maiduguri, Maiduguri, Nigeria.
**Print ISSN: 1596-2490, Electronic ISSN: 2545-5818**
www.azojete.com.ng

ORIGINAL RESEARCH ARTICLE

# SYMMETRIC AND ASYMMETRIC BASED ENCRYPTION MODEL FOR MOBILE COMMERCE

**O. C. Abikoye, A. H. Dokoro* and A. Abdullahi**

*(Department of Computer Science, University of Ilorin, Ilorin, Nigeria)*

**ARTICLE INFORMATION**

Submitted 22 November, 2018
Revised 01 May, 2019
Accepted 10 May, 2019

**Keywords:**
Cryptography
encryption
symmetric and asymmetric
AES and RSA model
Security
mobile commerce.

**ABSTRACT**

*Secure information exchange in a mobile commerce environment has become a difficult task due to the involvement of sensitive financial information and the tremendous development in information technology in recent years. This poses a great threat while conducting transaction in a mobile commerce environment. Cryptography has been employed to eliminate this using symmetric and asymmetric cryptography. However, in symmetric cryptography, secret key distribution can create a performance bottleneck, while asymmetric ciphers consume significant computational resources. This paper proposed symmetric and asymmetric based encryption model so as to achieve robust security and faster processing speed, by employing Advanced Encryption Standard (AES) as symmetric algorithm and Rivest-Shamir-Adleman (RSA) as asymmetric algorithm. In this model, RSA was used to encrypt AES secret key in order to secure the exchange of the key, while the rest of the sensitive data was encrypted using AES. The proposed model was implemented using Java programming language. Performance evaluation of the proposed model was carried out in terms of encryption/decryption time and the results show that the proposed model takes a little longer time than the RSA algorithm. This is as a result of the AES key encryption being introduced into the model. It is therefore recommended that the model be implemented in mobile commerce applications as an added layer of security in order to strengthen the applications against numerous security threats due to the robust security and faster processing speed provided by the proposed model.*



** Corresponding author's email address: harunadokoro@gmail.com*

## 1.0 Introduction

Information security has become a serious issue due to the tremendous development in information technology (Nath, et al, 2015). Nowadays, it is a real challenge to exchange confidential information (such as credit/debit card details, account information) between two end points without facing the threat of the information being intercepted while on transit (Nath et al, 2015). To achieve high degree of confidentiality, sensitive information needs to be encoded into a format that can only be decoded by the authorized parties so that it would be rendered meaningless to the would-be interceptor (Nath et al., 2015). In order for the

authorized parties to read the encrypted or cipher text, they must have access to a secret key or password with which only the message or information can be decrypted. Two forms of encryption algorithms exist; symmetric and asymmetric. Symmetric uses a single key for both encryption and decryption of data while asymmetric uses key pair, public and private key for encryption and decryption respectively (Choudhary and Som, 2016).

According to Kalaiselvi and Anand (2016), combination of symmetric and asymmetric key cryptographic algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) is one of the possible proactive solutions for securing sensitive information.

### 1.1 Review of the AES Algorithm

Advance Encryption Standard (AES) being symmetric cryptographic algorithm developed by Vincent Rijmen and Joan Daeman was established as the specification for encrypting electronic data by the United States (US) National Institute of Standards and Technology (NIST) in the year 2001. AES is a block cipher with a block size of 128 bit and allows for three different key lengths; 128 bits, 192 bits and 256 bits. The key length determines the number of encryption rounds to be performed Ritambhara et al. (2017). Table1 below summarizes the relationship between the key lengths and the encryption rounds of the AES algorithm.

Table 1: Relationship Between Key lengths and Encryption Rounds of AES

| AES Version | Key Length (Bits) | Encryption Rounds |
|---|---|---|
| AES-128 | 128 | 10 |
| AES-192 | 192 | 12 |
| AES-256 | 256 | 14 |

The AES algorithm consists of four invertible transformations; SubBytes, ShiftRows MixColumns, and AddRoundKey as seen from Figure 1. These transformations are performed in all the encryption rounds, except the final round where the MixColumns transformation is omitted in order to make the encryption and decryption scheme symmetric.

The SubBytes transformation replaces each byte of the state by a byte indexed by row (first 4-bits of the state byte) and column (second 4-bits of the state byte) of a 16x16 substitution table (S-Box) with special mathematical properties. The ShiftRows move the rows of the state by shifting the bytes in each row by a certain offset so as to ensure that columns are not encrypted independently. The Mix Column is a matrix operation composed of multiplication and addition of the entries, treated as coefficients of polynomial of order x7. During the Add round key operation, 16-byte sub-key derived from the main key using Rijndael's Key Schedule is added to the 16-byte state by combining each byte of the round key with the corresponding byte in the state using bitwise exclusive or (XOR) operation Ritambhara et al (2017).

*Corresponding author's e-mail address: harunadokoro@gmail.com*

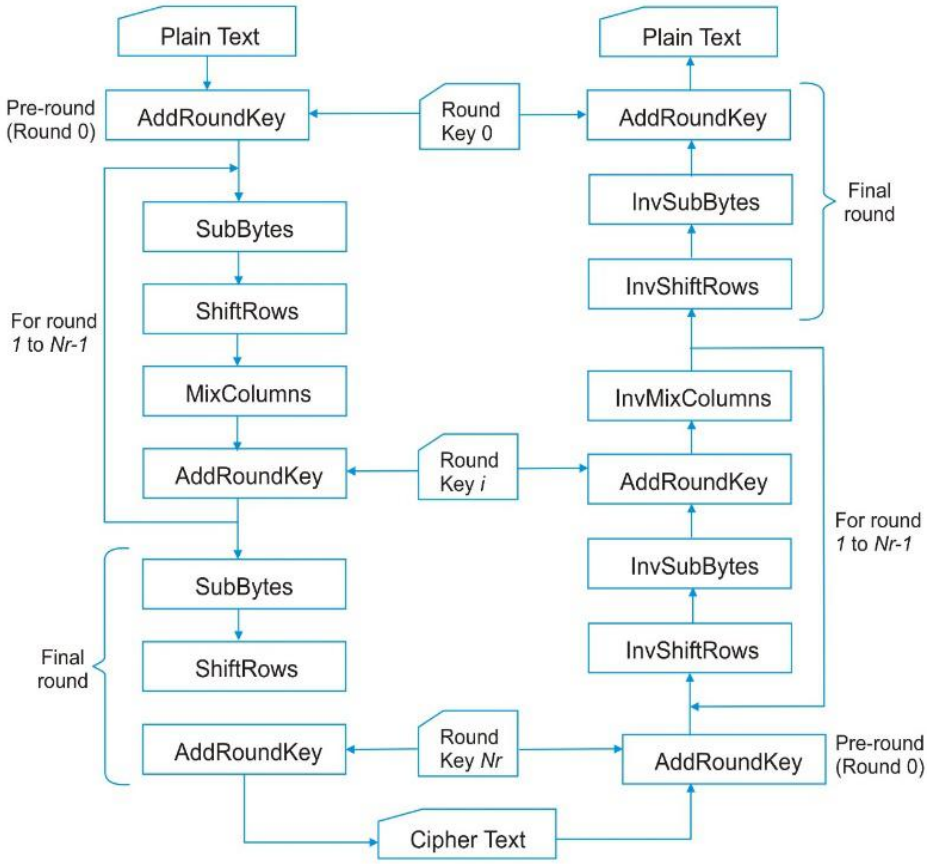


Figure 1: Description of AES Algorithm (Source: Ritambhara et al, 2017)

**Review of the RSA Algorithm**

Rivest-Shamir-Adleman (RSA) is the most commonly used asymmetric key cryptographic algorithm that was developed by three scientists; Ron Rivest, Adi Shamir, and Leonard Adleman in the year 1997 (Christof & Jan, 2010). RSA can be used for ensuring both confidentiality (encryption) and authentication (digital signatures) of a message (Christof & Jan, 2010). In this study, RSA was used to eliminate the difficulty of symmetric key distribution of the AES algorithm. The RSA implementation process is described as follows:

Two random secret primes p, q are selected such that the modulo $n = p * q$.

Phi of n ($\phi(n)$) is then calculated using the relation $\phi(n) = (p-1) * (q-1)$.

An integer e is randomly selected such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

According to congruence equation, $ed \bmod \phi(n) \equiv 1$, the decryption key d is then obtained such that the key pairs (e, n) is used for encryption, and (d, n) is used for decryption.

To encrypt a message m, the sender uses the public key (e, n), such that, cipher text $c = m^e \pmod n$.

To decrypt the cipher text c, the receiver uses the private key (d, n) such that, $m = c^d \pmod n$.

Note that, p, q, d, and $\phi(n)$ must remain secret to the owner of the key pairs. The encryption or public key (e, n), as the name suggest should be made available to anyone that wants to communicate with the recipient.

*Corresponding author's e-mail address: harunadokoro@gmail.com*

The security of the RSA algorithm lies on the factorisation of a big prime number, at least 1024 bits which prove to be a problem till today because it requires very long processing time and huge computational power. This is referred to as the factorisation problem.

To achieve a reasonable level of security, at least 1024-bits key lengths is recommended.

**Mobile Commerce**

Mobile e-commerce (M-Commerce) is a term used to describes online sales transactions that use wireless electronic hand-held devices such as, smart phones and tablets (Lu and Lei, 2017). These wireless devices interact with computer networks that have the ability to conduct online merchandise purchases. It is referred to as next-generation e-Commerce (Rouse, 2017).

The industries affected by M-Commerce include:

**Financial services such as mobile banking.**

Brokerage services in which stock trading can be conducted using handheld device.

Telecommunications, in which service such as bill payment and account reviews can all be conducted using handheld device

Service/retail, as consumers are given the ability to place and pay for orders on-the-fly

It has been noted that, M-Commerce has incomparable superiorities when compared to traditional e-commerce. However, it has brought forward higher request for a robust security (Jianping, 2011).

**Related Work**

Kumar, et al (2017) proposed the hybridization of symmetric and asymmetric encryption techniques to ensure confidentiality, integrity, and authentication of digital medical images. The researchers employed the use of RSA and AES cryptographic algorithms to guarantee authentication and confidentiality of the image. Encryption keys are generated using RSA algorithm. Once the keys are generated, AES algorithm is used to encrypt the image using the key generated. while Least Significant Bit (LSB) method is used to embed the encrypted image into the cover image.

Baihaqi and Briliyant (2017) worked on an e-learning system that implements both encryption and digital signature as security services to prevent data theft and modification. The design uses RSA 2048-bit for digital signature in order to verify the authenticity of information sent, while AES 128-bit encryption was proposed to ensure data confidentiality. RSA was not used to eliminate the difficulty of AES key distribution, it was only used to authenticate users of the system.

Sadikin and Wisnu (2016) presents an implementation of RSA-1048 and AES-256 with digital signature for securing health record application. The system is used in two schemes; verification and protection schemes. RSA-1048 and SHA-256 are used for digital signatures for the purpose of verifying the authenticity of users of the system. While the electronic health record is then protected using the AES-256 cryptographic algorithm.

Liang, Ye, et al (2016) proposed a hybrid cryptographic consisting of improved RSA and AES. User's files are encrypted using AES algorithm, while RSA algorithm encrypts the AES secret key. The encrypted file is uploaded to the cloud storage system. When users need to retrieve their

*Corresponding author's e-mail address: harunadokoro@gmail.com*

file, they will need to first download the encrypted file from the cloud storage system, use the RSA algorithm to decrypt the AES secret key in order to obtain the plaintext key of the AES algorithm. The AES algorithm is then used to decrypt the ciphertext data to get the original file.

Mahalle and Shahade (2014) presented a hybrid (RSA-1024 and AES-128) algorithm for securing data in cloud environment. When a user tries to upload a file, four different keys wil be generated; RSA public key-n, RSA public key-e, RSA private key-d, and AES secret key. RSA private key-d, and AES secret key are known only to the user. The file is then encrypted using both RSA and AES algorithms with RSA-public key-e and AES secret key before it is stored into the database corresponding to the user's account. Later when the user wants to access the stored file, the user has to specify the filename to download, and then provide the AES secret key and RSA private key-d which will be used to decrpyt the downloaded encrypted file. This approach is proved to be time consuming due to the double encryption involved. This is not ideal for most systems.

Khanezaei and Mohd (2014) introduced a framework based on RSA and AES encryption algorithms that can be used for cloud computing. The researchers argued that, to secure cloud storage services, combination of encryption algorithms such as RSA and AES is one of the possible solutions. The framework consists of three entities: Sender, Receiver, and Cloud Storage Service (CSS). To send a file, the sender request from the cloud system its public key and the cloud system will respond by sending the public key together with the generated file id. The sender then encrypts the file using RSA with the public key and sends it to the cloud server. To receive a file, the receiver sends a request for a particular file to the cloud system and the cloud system encrypt the file using AES algorithm and sends it to the receiver. The receiver again sends his public key to the cloud system, the cloud system then encrypts the secret key (the key used to encrypt the requested file) and sends it to the receiver. The receiver then uses his own private key to decrypts the encrypted secret key received, and later uses this decrypted secret key to decrypt the file. Nevertheless, the double encryption and decryption processes for each files can cause system overhead.

## The Proposed Model

The proposed model combines AES and RSA algorithms to ensure secure secret key establishment as well as confidentiality in exchanging sensitive data. The model is divided into two phases. Phase one deals with the secret key establishment, while phase two deals with the secure exchange of information.

### 3.1 Phase One

Phase one of the model deals with the symmetric or secret key establishment, that is, ensuring the secure exchange of the generated AES secret key between the sender and the receiver. Secure key establishment can be achieved through the following operations:

The sender (client) generates AES secret key whose length is either 128, 192, or 256 bits.

The receiver (server) generates RSA key pairs; public and private keys.

The sender requests the receiver's public key.

The receiver then sends his/her public key to the sender.

The sender encrypts the AES secret key using the receiver's public key and sends it to the receiver.

*Corresponding author's e-mail address: harunadokoro@gmail.com*

Lastly, the receiver decrypts the encrypted AES secret key using his/her private key to obtain the plain AES secret key.

The secret key is now established between the sender and the receiver, data can now be encrypted with the secret key and exchanged between the two end points using the AES algorithm.

**Phase Two**

The second phase of the model, also known as the secure message exchange phase, involves the use of the AES algorithm to carry out the rest of the communication between the communicating points after the secret key has been established. For encryption, the plain message and the plain AES secret key (whose ciphered version was sent to the recipient in phase one) serves as input to the AES algorithm. The output from the AES algorithm, which is the cipher message is then sent to the recipient. Upon the receipt of the cipher message, the recipient uses the decrypted version of the AES secret key received in phase one to decrypt the message using the AES algorithm. The communication continues until all the data is sent. The operations are summarized as follows:

Sender uses the AES secret key to encrypts the plain message using AES algorithm.

The encrypted message (cipher message) is then sent to the receiver.

The receiver uses the decrypted version of the AES secret key received in phase one to decrypt the cipher message using AES algorithm.

Figure 2 depicts the proposed model which combines symmetric (AES) and asymmetric (RSA) encryption algorithms.

*Corresponding author's e-mail address: harunadokoro@gmail.com*

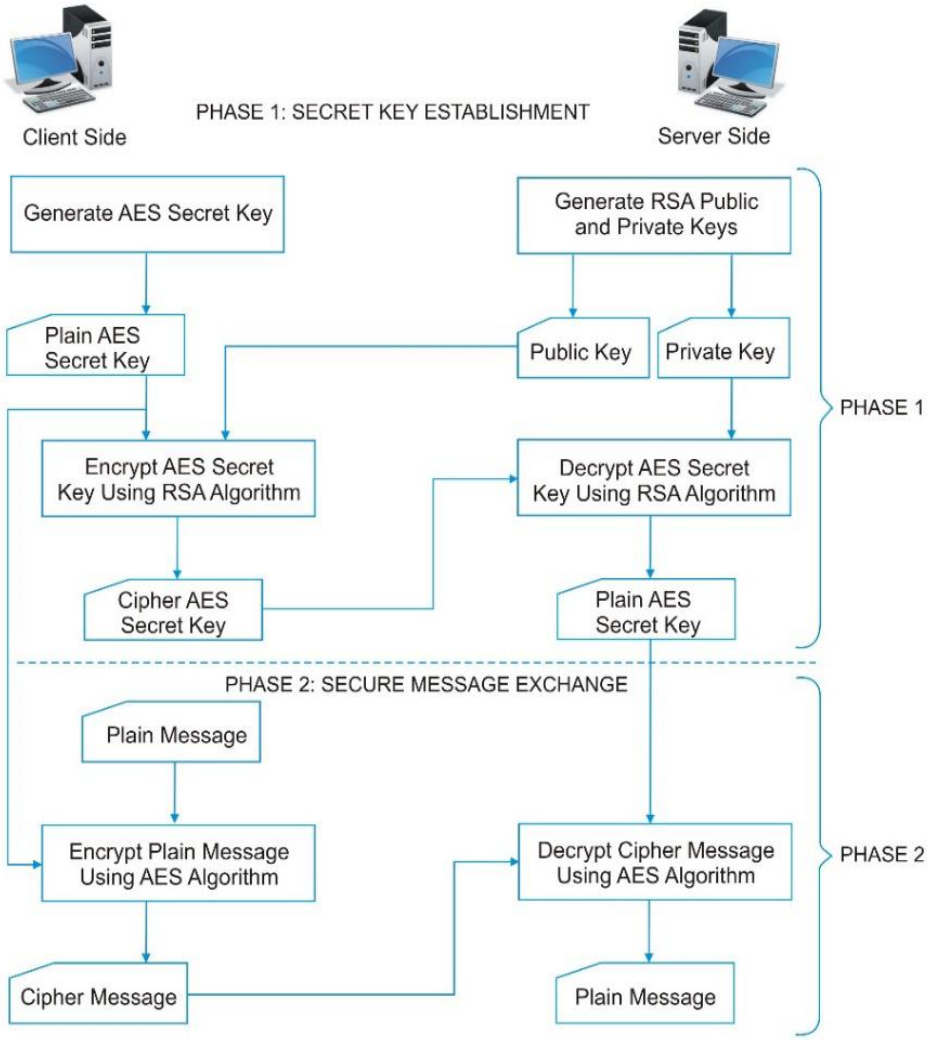


Figure 2: Model for Combined AES and RSA

### 3.3 System Implementation

The proposed model was implemented in Java. Java was chosen because of its platform independent feature; this means that a single program can runs on different platforms. NetBeans 8.2 was used as the Integrated Development Environment (IDE) to implement the system.

### 3.4 Encryption Window

Using the encryption window, client first generates the RSA keys by providing the RSA key length (in bit) and click on Generate RSA Keys button. The AES version is then selected and the AES secret key is entered in the space provided. The AES secret key entered is then encrypted using RSA algorithm, utilizing the generated RSA public key pair to obtain the ciphered AES secret key. The user then entered the plain text in the space provided and click on the Encrypt button to encrypt the plain text using the AES algorithm. Figure 3 shows the implemented encryption window of the proposed model.

*Corresponding author's e-mail address: harunadokoro@gmail.com*

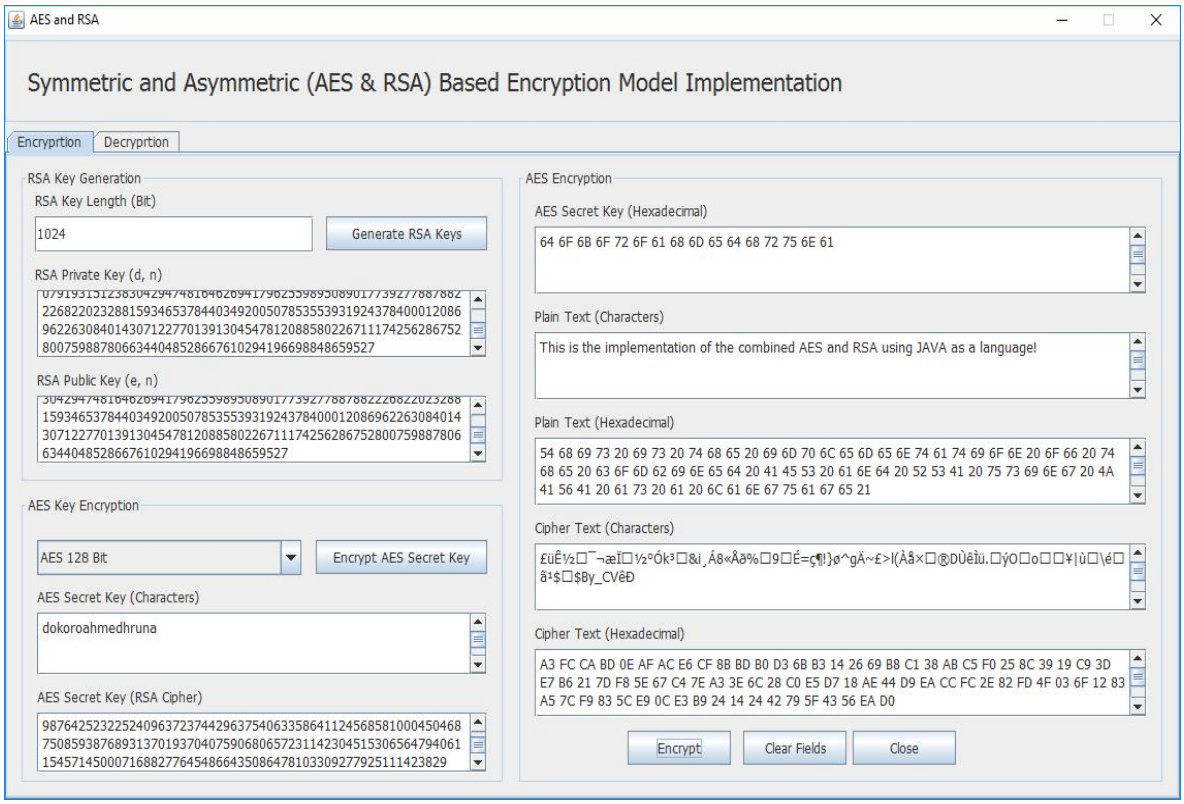


Figure 3: Encryption Window of the Proposed Model

### 3.5 Decryption Window

To decrypt a given cipher text, the user has to first get the RSA encrypted AES secret key by clicking on the Get AES Secret Key (Cipher) button. The encrypted AES secret key is then decrypted using RSA algorithm to reveal the plain AES secret key, by utilizing the private key component of the previously generated RSA keys. Lastly, the cipher text is decrypted using the AES algorithm with the decrypted AES secret key. Figure 4 shows the implemented decryption window of the proposed model.

*Corresponding author's e-mail address: harunadokoro@gmail.com*

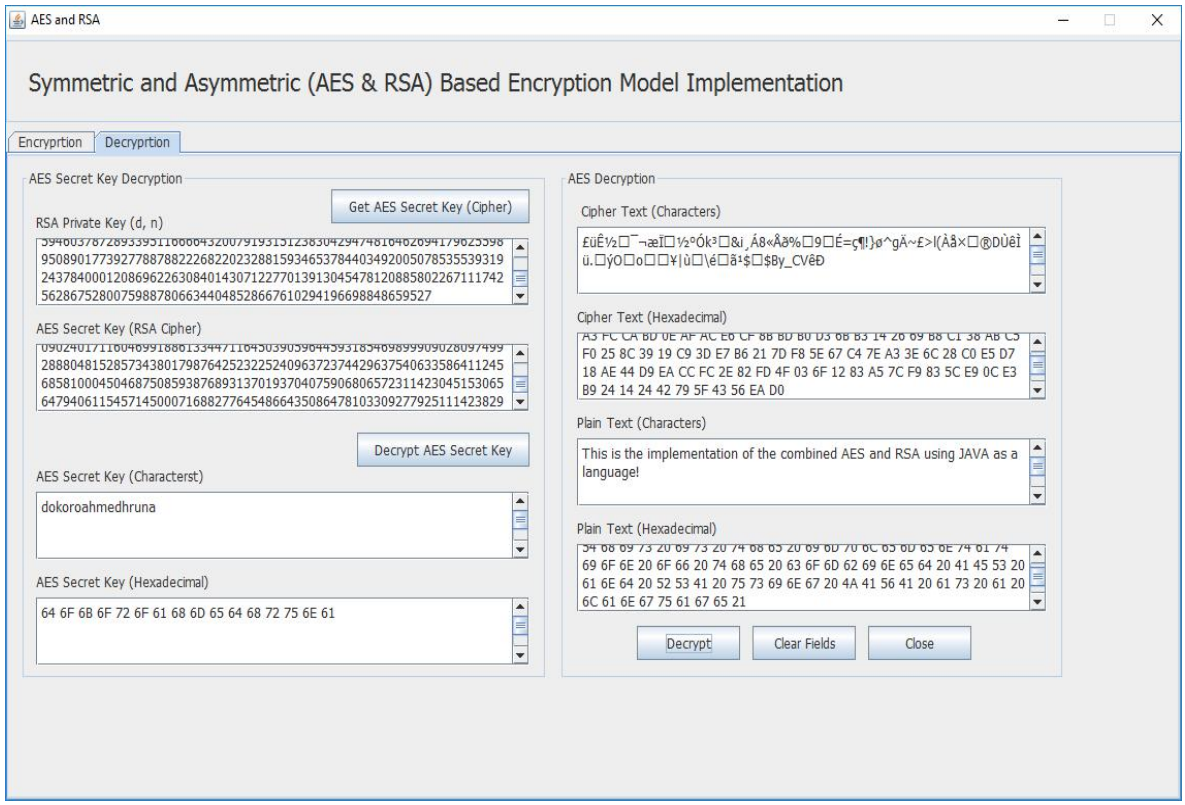


Figure 4: Decryption Window of the Proposed Model

## 4. Results and Discussion

The proposed model was evaluated against the AES and RSA algorithms in terms of encryption and decryption time. The results are obtained by encrypting 1024 bytes of data using the three algorithms; AES, RSA, and the proposed model. The results are presented in Table 2.

Table 2: Performance Evaluation of AES, RSA and the Proposed Model

| Algorithm | Key Length (Bit) | Encryption Time (ms) | Decryption Time (ms) |
|---|---|---|---|
| AES | 256 | 0.613186 | 0.626901 |
| RSA | 2048 | 1.533471 | 1.594019 |
| Proposed Model | 2048 | 1.856794 | 1.906412 |

From table 2, it can be seen that the encryption and decryption time for the proposed model is less than that of AES and RSA combined, even though the model is a combination of AES and RSA. Moreover, the model eliminates the major problem of symmetric key algorithms by ensuring secure secret key establishment. The

## 5. Conclusion

A model which combines symmetric and asymmetric cryptographic algorithms using AES and RSA was presented. The model was represented as two phase processes, with phase one deals with secret key establishment, while phase two deals with secure information exchange. The proposed model which suggest secure way of AES secret key establishment was implemented in java. Performance evaluation was carried out in terms of encryption/decryption time. The

*Corresponding author's e-mail address: harunadokoro@gmail.com*

evaluation results show that the encryption/decryption time for the proposed model is less than that of the AES and RSA combined but it is a little longer than that of the RSA algorithm, this is as a result of AES key encryption being introduced. Moreover, the model can be implemented as an added layer of security in order to ensure confidentiality while exchanging sensitive financial and personal information in a mobile commerce environment.

**References**

Baihaqi, A. and Briliyant, OC. 2017. Implementation of RSA 2048-bit and AES 128-bit for Secure E-Learning Web-based Application. Lambok, Indonesia, IEEE.

Choudhary, R. and Som, S. 2016. Encryption Technique Using Dynamic Table and Block Division Process on Binary Field. Noida, India, IEEE, pp. 353-358.

Christof, P. and Jan, P. 2010. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Germany: Springer-Verlag Berlin Heidelberg.

Jianping, W. 2011. The Analysis and Optimization on M-Commerce Secure Payment Model. Qingdao, China, IEEE, pp. 41-44.

Kalaiselvi, K. and Anand, K. 2016. Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box. Bangalore, India, IEEE, pp. 1-6.

Khanezaei, N. and Mohd, ZH. 2014. A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services. Kuala Lumpur, Malaysia, IEEE, pp. 58-62.

Kumar, SBJ., Nair, A. and Raj, RVK. 2017. Hybridization of RSA and AES Algorithms for Authentication and Confidentiality of Medical Images. Chennai, India, IEEE, pp. 1057-1060.

Liang, C., Ye, N., Malekian, R. and Wang, R. 2016. The Hybrid Encryption Algorithm of Lightweight Data in Cloud Storage. Bangi, Malaysia, IEEE, pp. 160-166.

Lu, T. and Lei, X. 2007. Study on Security Framework in E-Commerce. Shanghai, China, Iinstitute of Electrical and Electronic Engineers (IEEE), pp. 3541-3544.

Mahalle, VS. and Shahade, AK. 2014. Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm. Amravati, India, IEEE, pp. 146-149.

Nath, A., Madhumita, S., Supriya, M. and Kanij, FA. 2015. Bit Level Encryption Algorithm – Implementation of Bit-wise operations and randomized Bit-wise Columnar Transposition method. Jabalpur, India, IEEE, pp. 1057-1063.

Ritambhara, Gupta, A. and Jaiswal, M. 2017. An Enhanced AES Algorithm Using Cascading Method on 400 Bits Key Size Used in Enhancing the Safety of Next Generation Internet of Things (IoT). Greater Noida, India, IEEE, pp. 422-427.

Rouse, M. 2017. M-Commerce (Mobile Commerce). [Online]
Available at: http://searchmobilecomputing.techtarget.com/definition/m-commerce

Sadikin, MA. and Wisnu, RWM. 2016. Implementation of RSA 2048-bit and AES-256-bit with Digital Signature for Secure Electronic Health Recprd Application. Lombok, Indonesia, IEEE, pp. 387-392.

*Corresponding author's e-mail address: harunadokoro@gmail.com*