SECURING DATA USING HYBRID CRYPTOSYSTEM

KOUNG HSU WAI

M.C.Tech **JUNE 2022**

SECURING DATA USING HYBRID CRYPTOSYSTEM

By

KOUNG HSU WAI

B.C.Tech(Hons:)

A dissertation submitted in partial fulfillment of the requirements for the degree of

Master of Computer Technology

(M.C.Tech).

University of Computer Studies, Yangon

JUNE 2022

ACKNOWLEDGEMENTS

To complete this thesis, many things are needed like my hard work and the supporting of many people who gave a lot of idea to me to complete this thesis.

Firstly, I would like to express my appreciation and thanks to **Dr.Mie Mie Khin**, Rector of the University of Computer Studies, Yangon, for her kind permission to submit this dissertation.

I am remarkably and especially thankful to my Pro-Rector, **Dr.Yuzana**, the University of Computer Studies, Pyay.

I would like to thank course coordinators, **Dr. Amy Tun**, Professor, Faculty of Computer Systems and Technologies, University of Computer Studies, Yangon for her superior suggestions and administrative supports during my academic study.

I also would like to express my gratitude and appreciation to **Daw Mya Hnin Mon**, Associate Professor, Department of English, University of Computer studies, Yangon, for her advice, editing and suggestion from the language point of view.

I am thankful to my thesis supervisor, **Dr. Myat Thu Zar**, for her close supervision, proper guidance, valuable suggestions, guidance, advice and encouragement during the course of this work.

I also like to acknowledge my thanks to **all my teachers** who taught me throughout the master's degree course and **my friends** for their corporation and wish to express my gratitude to **my beloved parents** for their invaluable support and encouragement to fulfill my wish. If not for the above mentioned people, my master degree's would never have been completed in such a successfully manner. I once again extend my sincere thanks to all of them.

STATEMENT ORIGINALITY

This is to certify to the best of my knowledge, the content of this thesis is my own work. I certify that intellectual content of this thesis is the product of my own work and that all the assistance received in preparing this thesis and sources have been acknowledged.

Signed

ABSTRACT

Data security plays an important role in every organization. Therefore, many organizations need to protect their information or data when data in transmission. This system intends to implement the combination of the Advanced Encryption Standard (AES) and Rivest-Shamir-leman (RSA) algorithm in order to more secure than single algorithm. Pyay Education College to (PEC)'s Student marks file is sent from Pyay Education College to Naypyidaw office for examination result. Student's data are stored in excel files format and placed in the computer. In this system, AES algorithm uses to encrypt the student's mark file, RSA algorithm uses to encrypt the AES's key. Hash based Message Authentication Code (HMAC) is applied to generate the hash value and to authenticate transferred information between the two sides (that share a secret key). Advantages of RSA algorithm and AES algorithm are combined in this system. The proposed system is implemented using PHP programming language. The experimental results show that hybrid AES-RSA cryptography system has been performed along with data integrity.

TABLE OF CONENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Cryptography is the ability to send information between participants in a way that prevents others from reading it. Cryptography is used to achieve all the security goals as the plaintext is not available to anyone until he/she knows the key. It allows people to communicate or transfer data electronically without worries of deceit and deception (confidentially).There are three different types of encryption algorithms; symmetric and asymmetric encryption techniques [3]. These algorithms and techniques are applied to cryptographic key generation, digital signature, authentication, verification and confidentiality for data transmission and prevention.

Four main objectives of modern cryptography concerns are as follows:

1. Confidentiality
2. Integrity
3. Non-repudiation
4. Authentication

General process of cryptography is shown in Figure 1.1. Original data (plaintext) is encrypted with some algorithm and then the resulted ciphertext cannot be read. After applying decryption process, the final readable format data will be reobtained.

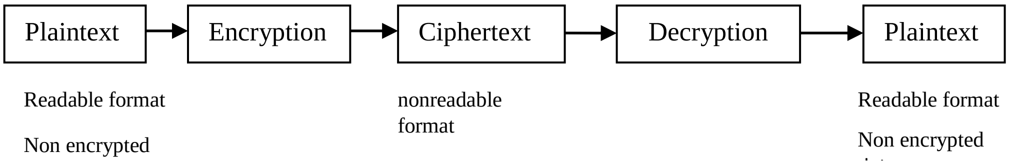


Figure 1.1 Process of cryptography

1.1 Types of Cryptography

There are two types of cryptography such as:

- Single key or symmetric-key encryption algorithm and
- Public key or asymmetric key encryption algorithm

1.1.1 Single Key or Symmetric Key Encryption Algorithm

Symmetric key algorithms define a fixed length of bits is also called a block cipher that share a secret key in order to apply for both encryption and decryption. It is shown in figure 1.2. Advanced Encryption Standard (AES) is the example of symmetric key cryptography to protect information [4]. It uses different key lengths such as 128-bit, 192-bit and 256-bit to protect brute force attack and other attack.

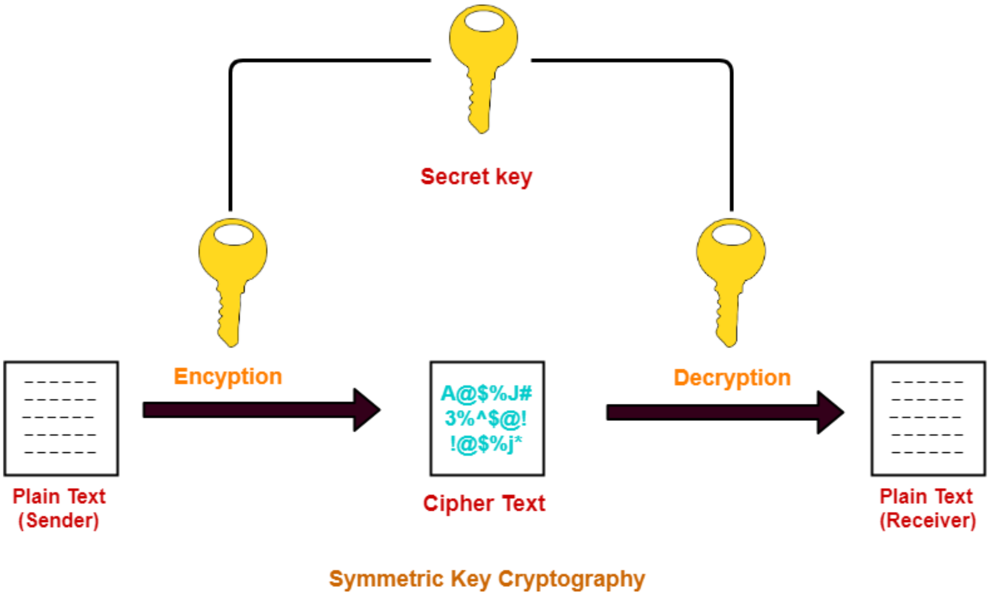


Figure 1.2 Symmetric cryptography

1.1.2 Asymmetric Cryptography

Asymmetric key cryptography is also called (public key cryptography) use a key pair of public key and private key. Public key is used for encrypting data and private key is used for decrypting that data. This process is displayed in Figure 1.3. Popular example of asymmetric cryptography is the RSA (Rivest-Shamir-Adleman) algorithm [5]. Other public key cryptographic algorithms are:

- Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin
- Digital Signature Algorithm (DSA) adopted as a Federal Information Processing Standard for digital signatures by NIST in FIPS 186-4
- Diffie-Hellman key exchange

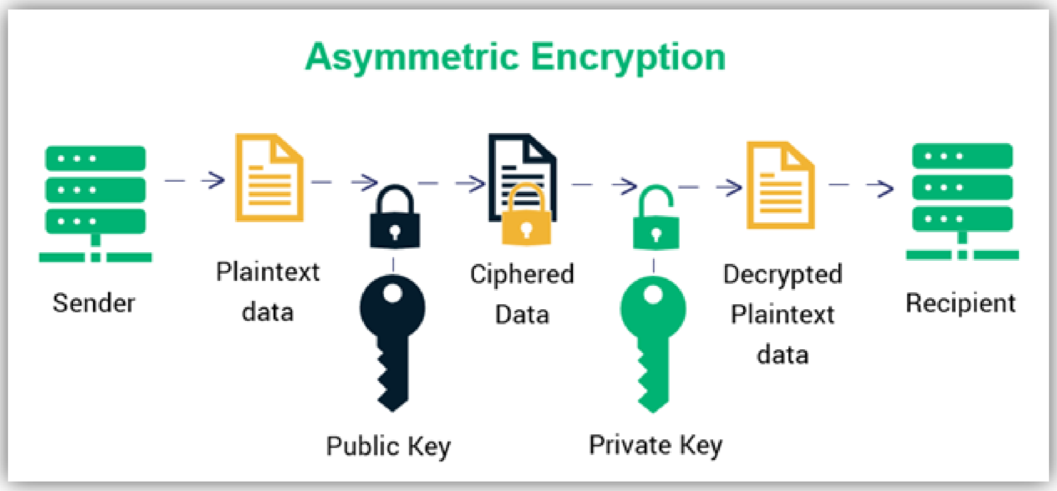


Figure 1.3 Asymmetric cryptography

1.2 Objectives of the Thesis

The major objectives of the proposed system are as follows:

- To study the basic concepts of cryptography.
- To understand the AES algorithm of symmetric cryptography.
- To understand the RSA algorithm of asymmetric cryptography.
- To take the advantages of Hybrid Cryptosystem.
- To support the effective encryption techniques for handling sensitive data.
- To provide the security of students' exam marks in PEC (Pyay Education College).

1.3 Motivation of the Thesis

- To protect the PEC' student's exam marks between the head of PEC and the director of the Ministry of Education.
- To maintain the PEC' student's exam marks before the results have announced on the board for getting to attend the B.Ed.

1.4 Organization of the Thesis

This thesis composed of five chapters. The organization structure of the proposed system is as follows:

Firstly, chapter 1 expresses the introduction of cryptography and its nature, type of cryptography and objectives. It provides the motivations of the thesis.

The literature reviews and some existing methods are surveyed and briefly reviewed in Chapter 2. After that describes the purposes, concepts, principles and types of cryptography and then differences of public-key and private key cryptosystem.

Chapter 3 explains the detail process of hybrid encryption system and the proposed system architecture.

Chapter 4 shows the implementation of proposed system and compare the processing time between AES, RSA and hybrid encryption algorithm of PEC's student file with various file size.

Chapter 5 concludes the system with limitations, benefits and further extension of this thesis.

CHAPTER 2

THEORY BACKGROUND

2.1 Introduction

Cryptography is very interested and can be applied to wide range of application. Kahn's The Codebreakers is the perfect non-technical account of the cryptography subject. From Last 4000 years ago to twentieth century in Egypt, this book played an important role in words wars. The primary goal for cryptography is to apply at military, government organization and other information security objectives. Therefore cryptography was operated as a device to prevent national secrets and plans [10].

To prevent digital information and data in order to support security services in the growth of computers and communications system. It lead to improve for private sector requirement in the 1960s. In the early 1970s, start Feistel at IBM for encrypting uncatalogued information and come to a head with the assumption as a U.S. Federal information Processing Standard. Data Encryption Standard, (DES) is the most popular cryptographic mechanism. Various financial organizations and institution around the world, requires secure electronic commerce and then DES supported for this purpose.

In 1976, Diffie and Hellman released new methodology in cryptography and it is the most evidence development in the history of cryptography. They initiated the concept of public key cryptography and key exchange method that applied intractability of the discrete logarithm problem solving and it provided more security. Although the user has no knowledge of a public key encryption scheme at the time, the design and objective was comprehensible and it improved very large interest and undertaking the cryptographic community.

Rivest, Shamir and Adleman found the first practical public key encryption and signature scheme in 1978 and also known as RSA. The RSA algorithm is based on another difficult mathematical problem and composed of factoring large integers such as large prime number. Due to the difficult mathematical problem to cryptography of this algorithm, this application attract to find more efficient to factor. RSA system is more secure than other system but it has another shortcoming facts.

Therefore, EIGamal discovered another class of powerful and practical public key schemes in discrete algorithm problem is also based on these schemes.

Digital signature is the most significant contributions in public key cryptography. This was acquired by the first International standard for digital signatures (ISO/IEC 9796) in 1991. Digital signature is based on the RSA public key scheme. The U.S Government approved the Digital Signature Standard in 1994, which implemented based on the EIGamal public key scheme. Set up the various standard and infrastructure in cryptography. Inventing security products are being required for many organization.

2.2 The Purpose of Cryptography

In circa 1900 B.C., cryptography applied with first documented is written by secret code and do not understandable other people and only the writer know the meaning of document. Some researchers think that the technology of cryptography would be disappeared in recent year for some application ranging with applications ranging from diplomatic missives to war-time battle plans. As increasing the development of communication in computer society, cryptography play an important in that new forms. When data and information passed through the untrusted medium such as internet or any other network communication, cryptography is required for this trusted communication [10].

2.3 Terminology of Cryptography

The main goal of cryptography is to support information security services in various application [6]. The basic components of cryptosystem are as follows:

- Plaintext
  - Plaintext is the data or information to be prevented during0transmission between sender and receiver'
- Encryption Algorithm
  - Encryption algorithm is the cryptographic algorithm that can create ciphertext for any type of data or information in plaintext and encryption key.
  - In these algorithms, plaintext and encryption key are used as input and output is the ciphertext.

- Ciphertext
    - Ciphertext is the unreadable format of the plaintext that are created by applying the some encryption algorithm with certain key.
- Decryption Algorithm
    - Decryption algorithm is used to convert the ciphertext to plaintext by using decryption key.
    - Therefore ciphertext and decryption key are given as input in decryption algorithm and then produce a plaintext.
- Encryption Key
    - Encryption key is normally a value and sender need to know define this value to make encryption process.
- Decryption Key
    - Receiver need to know the decryption key in order to extract the ciphertext.
    - Normally, decryption key and encryption key is the same for some algorithm. But not always the same in many other algorithms.

2.4 Concepts of Using Cryptography

The origin of cryptography is derived from the Greek kryptos (hidden) and the last thousands of years, cryptography used in the computer communication. Therefore cryptography start used in Egypt and well documented back over 4000 years ago. Julius Caesar was invented his own cryptography and called a name as Caeser's cipher. Alphabet letters are rotated to the right by three in Caesar's Cipher. For example, A moves to D and T moves to W. The standards of the Caeser Cipher is very simple in today but it distribute Julius just fine in his day. People want to keep secret information and the objective of cryptography is to secret information or convert to unreadable form, because this unreadable format is not easily understandable for unintended user or people in communication. Cryptographic technique consists of two types such as encryption and steganography.

- **Encryption**, which include an algorithm and this algorithm composed of a procedure which applied to convert from a plain text to cipher text. This form is not turn to original plaintext if anyone does not the decryption key.

- **Steganography**, which is a means of covering the existence of the data, not just it's disturb. Steganography is usually made by concealing it within other, safe data.

Cryptography can give various services such as

- Confidentiality
- Integrity
- Authentication
- Non-repudiation.
- Access control

2.4.1 Confidentiality

Confidentiality means that only authorized person can access an organization's private data and can decrypt the encrypted message. Most security algorithms are secure. Therefore, attacker cannot read the original message if he/she does not have the related "key". When using the symmetric key algorithm, the user needs to keep the secret key and when using the asymmetric key algorithm, the user needs to secret private key. The message of confidentiality will be lose when a secret key or private key is compromised.

2.4.2 Integrity

Integrity is another important feature of cryptography. Data integrity means accuracy, trusted data and consistency of information. The most powerful method to protect data integrity is hash algorithm. Compare the hash value of receive message with the hash value of original message. If the hash value is matched, the receive message is trusted and if not, the receive message is not guaranteed to trust. In symmetric algorithm, validation method is used to validate all the outputs are equivalent to the inputs. This validation method is referred to as digital signature.

2.4.3 Authentication

Authentication is required when the receiver to verify the sender. But the receiver cannot always verify the sender. This verification depends on the type of encryption. In symmetric cryptography, the receiver cannot verify the sender. However, in cases of asymmetric cryptography, the receiver can verify the sender. In asymmetric cryptography, message may be encrypted and decrypted with the secret key. By creating the private key in asymmetric cryptography, user can authenticate the sender because assuming that the key is stored in private. Because each person kept their private key and message is encrypted with public key. Therefore, the person who possess the private can decrypt the message. Moreover, message can sign with their private key that is validated with their public key.

2.4.4 Non Repudiation

Asymmetric cryptography assume that the private key is secure. A particular message has been sent to make sure that an author cannot deny that they signed or encrypted. The individual person should be access the message with their own private key. The message can sign with only the person private key. Non-repudiation make guarantee that person cannot deny the validity of message. Therefore, non-repudiation is applied to information security as a legal concept which support the integrity and authenticity of that message.

2.4.5 Access Control

The additional feature of cryptography system is the access control mechanisms. Key signature based access control can be provided in some system.X.509 certificate is a digital certificate that use these similar manner. The design of this mechanism is that the user has a certificate who can be authenticated and identified. Once the authentication has occurred, software access controls can be provided to the user [4].

2.5 Principles of Cryptography

Weak or strong of cryptosystem can be defined by the use of different key length in the system. U.S government use the cryptosystem to prevent the eavesdropping on illegal or antigovernment activities. The design of DES owned by the National Security Agency (NSA) could be applied for cracking purposes, processing under the premise that no other supercomputers of their sort are in the public hands or control.

By producing ciphertext as random to statistical tests, cryptography come to strong system. Their finding procedure reach to zero because keys are generated using robust random number generators for uniqueness. Therefore, attackers try to steal the key from the store rather than trying to estimate a key’s value. So, extra precautions time must be required and message or file can be protected from these thefts.

Perfect secure cryptosystem does not exist in anywhere but a cryptosystem can indicate the resistant to attacks. People have trust in currency therefore cryptosystems are used as currency people. If the attacker want to break vulnerability of cryptosystem, then the system try to growth the security strength of system. If the cryptosystem is once violated or if the system vulnerability is not recovered, anyone will not use these system. Although weak system cannot resists all attacks, the strongest system ensure the data security and can be tested for data integrity.

The strongest of cryptosystem is mainly depend on the use of secret key and key length size rather than keeping of a cryptosystem is described in the size and the secrecy of the keys that are used rather than keeping secret this algorithm itself. Cryptanalysis try to break the ciphertext and try to break the work or goal of the cryptosystem, therefore they survey the structure of the new released system. Any cryptosystem that hasn’t been subjected to brutal attacks should be considered suspect. National system declared AES is replaced to DES in order to create confidence in their cryptosystem [4].

2.6 Data Encryption Standard (DES)

Data encryption standard (DES) is the symmetric key algorithm. It is a block cipher. In DES algorithm, 56-bit cipher key is shared for both sender side and receiver side. 64-bit plaintext is used for encryption in DES and then create 64-bit ciphertext. The overview process is shown in Figure 2.1.

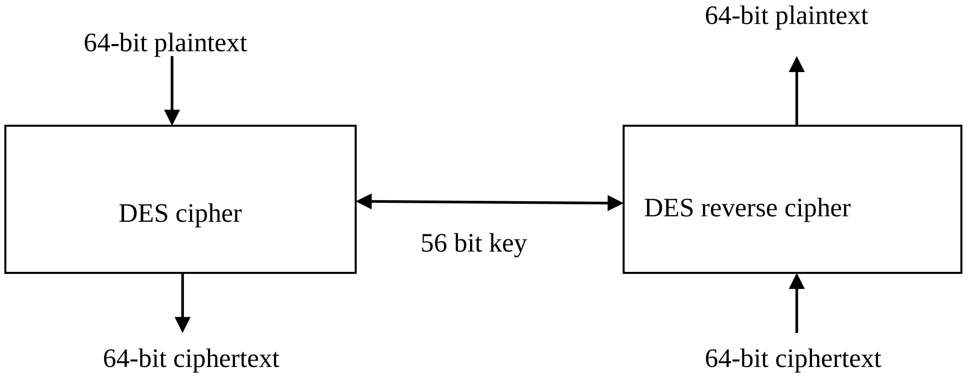


Figure 2.1 Data Encryption Standard

2.7 Types of Cryptographic Function

Cryptographic functions consist of three main types: secret key function (Symmetric), public key function (Asymmetric) and hash function. Secret key cryptography contain the use of one key for encryption and decryption. Public key cryptography using two keys, one key for encryption and other key for decryption. Zero key is used in hash function. Algorithm without need to have secret is the imagery but need to try.

2.7.1 Secret Key Cryptography

Secret key cryptography can be defined as being either stream ciphers or block ciphers. Stream ciphers process a single bit of plaintext at a time and key is constantly changing due to the implementation of some feedback mechanism. In block cipher, data are encrypted one block at each time using the same key on each block. Block cipher process one block of plaintext at a time. Block ciphers can handle various modes and the most popular and important modes are as follow [13]:

1. Electronic Codebook (ECB) mode
2. Cipher Block Chaining (CBC) mode
3. Cipher Feedback (CFB) mode
4. Output Feedback (OFB) mode

The main difference between stream cipher and block cipher are as follow:

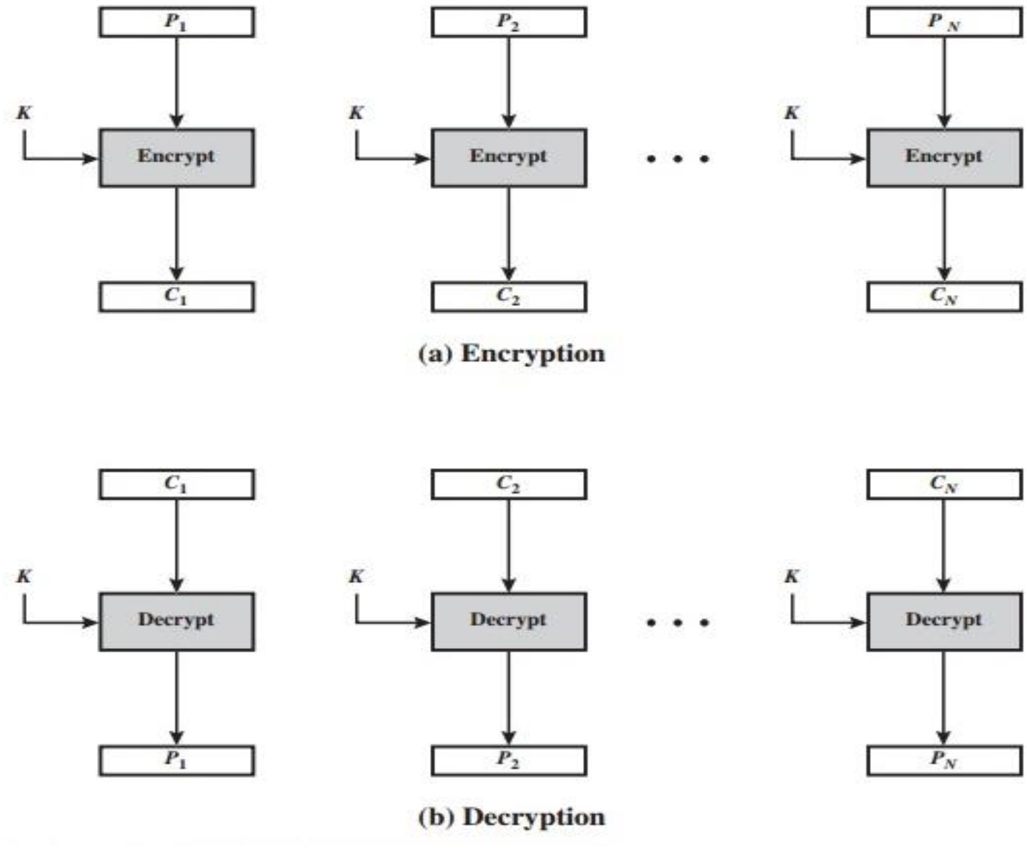
Table 2.1 Difference between Stream cipher and Block cipher

	Block Cipher	**Stream Cipher**
1	At a time, one block of plaintext is used to convert from plaintext to ciphertext in block cipher at a time.	At a time, one byte of plaintext is used to convert from plaintext into ciphertext in stream cipher.
2	At least 64 bits or more is used in block cipher	Sstream cipher uses only 8 bits in operation.
3	The structure and process of block cipher is understandable and complexity is simple.	But stream cipher is more difficult.
4	Block cipher uses not only confusion but also diffusion.	While stream cipher uses only confusion.
5	Decryption from encrypted text is hard in block cipher.	Converting from encrypted text to original form is easy in stream cipher.

6	Two type of modes ECB (Electronic Code Book) and CBC (Cipher Block Chaining) are applied in block cipher.	CFB (Cipher Feedback) and OFB (Output Feedback) modes are applied in stream cipher.

2.7.1.1 Electronic Codebook (ECB) Mode

ECB is the simplest mode. In electronic codebook (ECB) mode, the same key is used to encrypt the each block of plaintext and processed one block at a time [13]. A key is given and this is known as codebook. This codebook is defined as a unique ciphertext for every b-bit block of plaintext. Therefore, for displaying corresponding ciphertext with every possible b-bit pattern, a huge amount of codebook is imagined. The encryption process of ECB is shown in Figure 2.2 (a) and decryption process of ECB is displayed in Figure 2.2 (b).



(a) Encryption

(b) Decryption

Figure 2.2 Electronic Codebook (ECB) mode

If the encryption key consists of a short amount of data, the ECB method is the best mode. Therefore, ECB is the best mode when the people want to transmit a DES key securely. In other word, if the encrypted message contains long length, ECB mode is not suitable and unsecure for transmission. Applying the same b-bit block of plaintext is the most attractive characteristic of ECB. When this characteristic is appeared in the message, the system produces the same ciphertext.

2.7.1.2 Cipher Block Chaining (CBC) mode

Cipher block chanining (CBC) mode is designed to overcome the security weakness of ECB mode [13]. In CBC mode, the same plaintext block is repeated and then produced different ciphertext blocks. Therefore, CBC mode support this requirement and it is shown in figure 2.3. Figure 2.3 (a) illustrates the encryption process of CBC mode and figure2.3 (b) shows the decryption process of CBC mode. In CBC mode encryption process, the input of the encryption algorithm and current plaintext are XOR and the same key is applied for each block in the ciphertext. In effect, the procedure of plaintext blocks are placed together to be more secure. Therefore, plaintext block and the input of encryption function for each plaintext have not relation. Therefore, b bits repeating patterns are not showed.

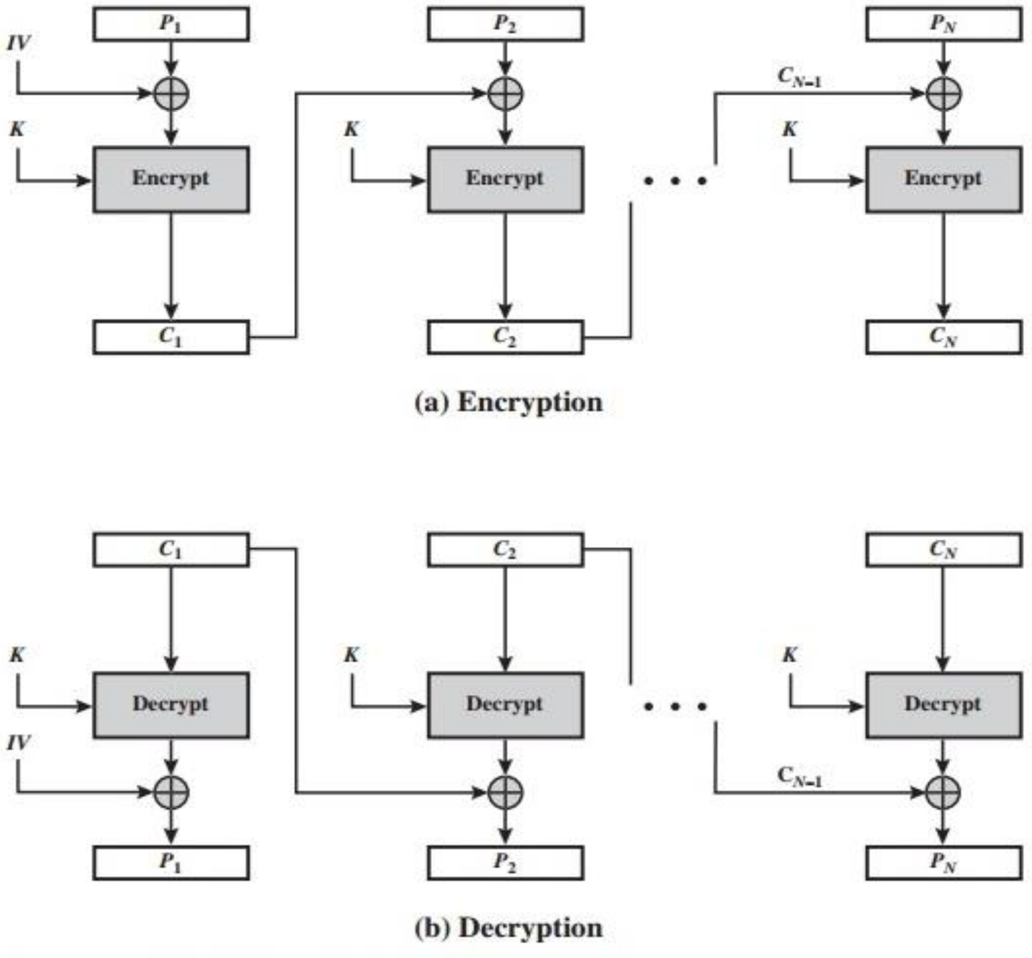


Figure 2.3 Cipher Block Chaining (CBC) mode

Each cipher block is passed through the step of decryption algorithm for decryption process. And then previous ciphertext and result is XORed to obtain the plaintext block. The steps for this process are as follow:

$$C_j = E(K[C_{j-1} \oplus P_j])$$

Then

$$D(K_i, C_j) = D(K, E(K_i(C \oplus P_j]))$$

$$D(K_i, C_j) = C_{j-1} \oplus P_j$$

$$C_{j-1} \oplus D(K_i, C_j) = C_{j-1} \oplus C_{j-1} P_j = P_j$$

First block of plaintext is XORed with aninitialization vector (IV) in order to produce the ciphertext first block at the encryption. At the decryption side, the output of the decryption algorithm and the IV is XORed to reobtain the first block of plaintext. The IV and cipher block have the equal size and the IV means data block. Although the contents of IV cannot be estimated by a third party, both the receiver and sender must be known definitely.

In case of unauthorized changes in IV should be defined for more secure. This could be done by transferring the IV using ECB encryption. IV protection is required because an opponent use a different value of IV to make fool to the receiver. To make a different value of IV, an opponent changed the selected bits in the first block of plaintext. This process can consider as follow:

$$C_1 = E(K, [IV \oplus P_1])$$

$$P_1 = IV \oplus D(K, C_1)$$

2.7.1.3 Cipher Feedback (CFB) Mode

The DES scheme is block cipher technique that utilizes b-bit block. However, by applying the cipher feedback (CFB) mode or output feedback mode to the DES scheme, which can invert from block cipher technique to stream cipher technique [13]. A stream cipher creates the integral number of blocks by removing the need to pad a message. This operation can be done in real time. Therefore, when a character stream is being transmitted, character oriented stream cipher supports to transmit and encrypt immediately for each character contain in the stream. The one characteristic of a stream cipher is that the length of plaintext and ciphertext is equal. For example, if the sender transmits 8-bit characters, each character should be encrypted to produce a cipher text output of 8 bits. Transmission capacity is misused when the output ciphertext produces more than 8 bits. Figure 2.4 displays the process of the CFB scheme.

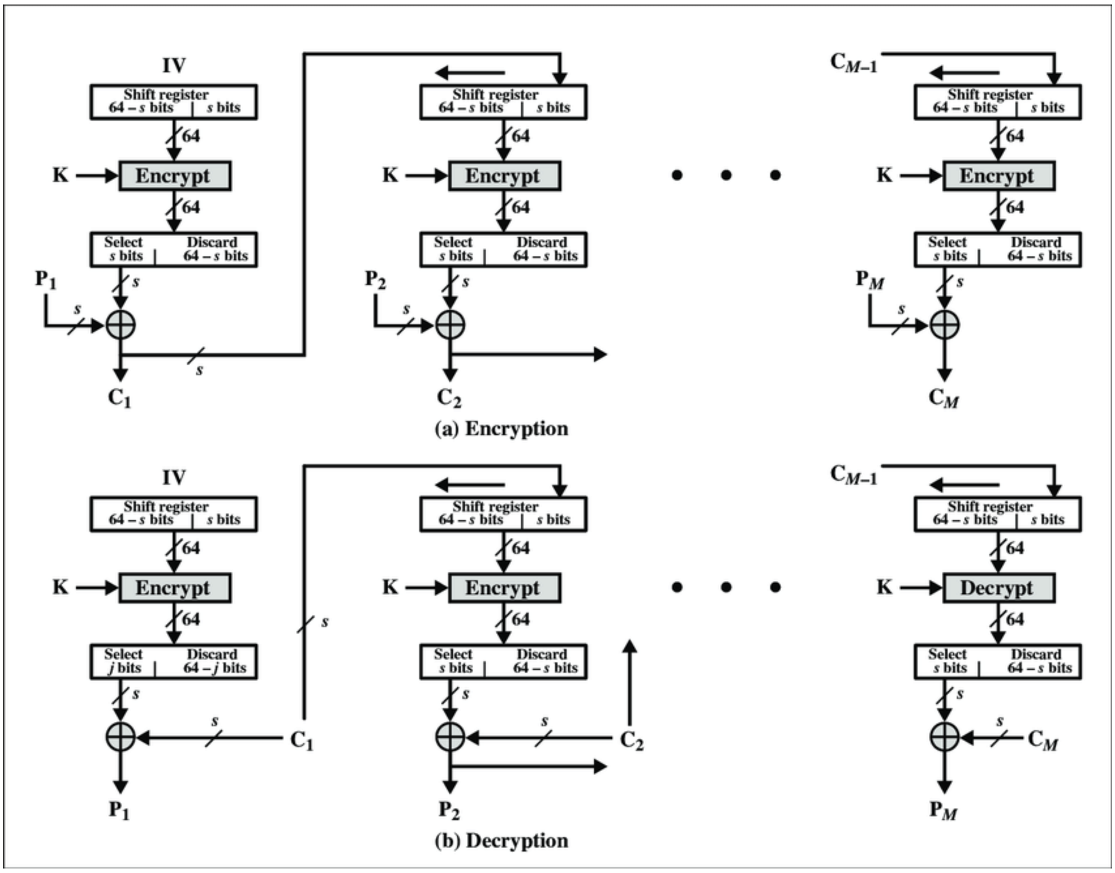


Figure 2.4 Cipher Feedback (CFB) Mode

Cipher feedback (CFB) mode is shown in figure and s bit unit is transmitted, the common value of s is 8. CFB is similar CBC, so that the ciphertext unit of any plaintext become a function of all the preceding plaintext. Unlike CBC mode, in CFB mode, b bits of the plaintext unit separated into segment and defined as s bit. The processes of encryption are as follow:

- b-bit shift register is the input function for encryption. This mean that it is the primary set to initialization vector (IV).
- P_1 is the first segment of plaintext, which is XORed with the leftmost s-bit of the encryption function. The output result is the first unit of ciphertext C_1. After getting the ciphertext C_1, it transfers to the receiver.

- In addition, s bit of shift register are shifted to the left and the position of ciphertext C_1 is the rightmost s bit of the register. After encrypting all plaintext unit, this process is complete.

For decryption,

- To reobtain the plaintext, the output of the encryption function and ciphertext is XORed for the decryption process.

Note that it is the encryption function (X) be defined as the most significant s bits of X. Then that is used, not the decryption function. This is easily explained. Let S s(X) be defined as the most significant s bits of X. Then

$$C_1 = P_1 \oplus S_s[E(K, IV)]$$

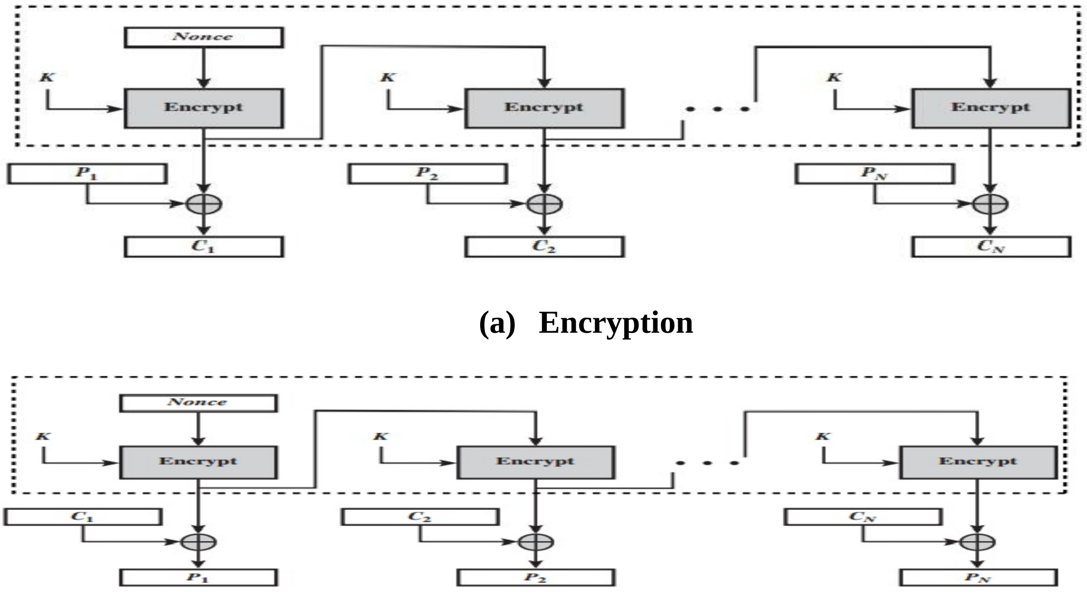
Therefore,

$$P_1 = C_1 \oplus S_s\ [E(K, IV)]$$

The equal reasoning holds for subsequent steps in the process.

2.7.1.4 Output Feedback (OFB) mode

The structure of output feedback (OFB) is similar to cipher feedback **(**CFB) mode. This is shown in Figure 2.5. While in CFB the ciphertext is fed back to the shift register, encrypted result is fed back to the shift register in OFB [13]. It can be seen easily in figure.



(a) Encryption

(b) Decryption

Figure 2.5 Output feedback (OFB) Mode

2.7.2 Symmetric Key Cryptography

Symmetric key cryptography can be used by relating the cryptographic keys for encryption and decryption in cryptography. This process shown in Figure 2.6. In symmetrical key cryptography, the encryption key and decryption have relation, so the key for both process may be identical or in other word, the transformation of key sharing is very simple. Sharing the secret key between two or more parties should be used private information link in order to secure.

Symmetric key algorithm can be divided into stream ciphers and block ciphers. Stream cipher encrypts the bits of the message one at a time and block cipher take a number of bit (block) and encrypt them as a single unit. Unlike the key used with public key algorithms, symmetric key are frequently changed. For this reason, they are referred to here as session keys. Compared to public key algorithms, symmetric algorithms are very fast and that are preferred when encrypting large amount of data.

In symmetric algorithms, block of 64 bits have been commonly used, the Advanced Encryption Standard (AES) algorithm approved by NIST (National Institute of Standard and Technology) in December-2001 use 128 bit block. Some examples of popular and well respected symmetric algorithm include Twofish, Serpent, Blowfish, DES, Triple DES, AES (Advanced Encryption Standard), RC-5, IDEA, RC4,CASTS.

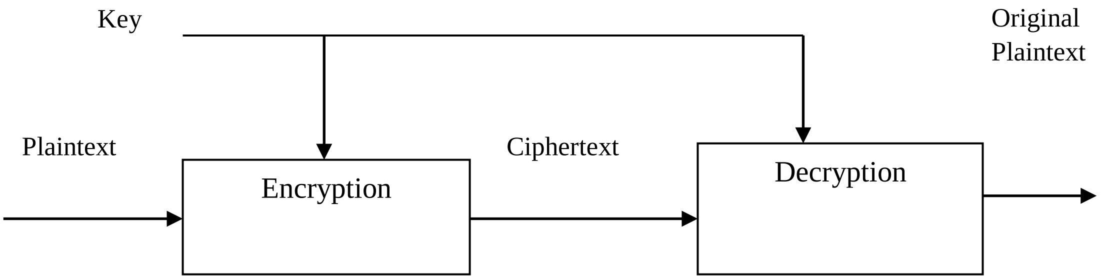


Figure 2.6 Symmetric Key Cryptosystem

2.7.3 Asymmetric Key Cryptography

Last thousands of year, public key encryption is very popular encryption technology in cryptographic system. Public key algorithm does not based on substitution and permutation. It is mainly based on mathematical function. But the most important point for public key cryptosystem is the asymmetric. It contains the use of two separate keys while the conventional symmetric key is used only key. The outcome of using two keys has the confidentiality key distribution and authentication.

Public key is used for encryption process in asymmetric key cryptosystem and a different but related key called private key is used for decryption process. Although public key have accessed by all participants, private keys must be secret by each participants therefore need never be distributed. The system pick up the public key and execute encryption operation. And then, only the receiver can decrypt the message by using his or her private key.

The system communication and transmission is secure until the private key is maintained secretly. The complement key may be produced to replace with its old private key. Because the system has the permission to change its private key. These system do by "trapdoor" mathematical problem. Although the computation of these problems are not complicated, do not easy to convert such as long division is more harder than multiplication. The process of asymmetric cipher is shown in Figure 2.7.

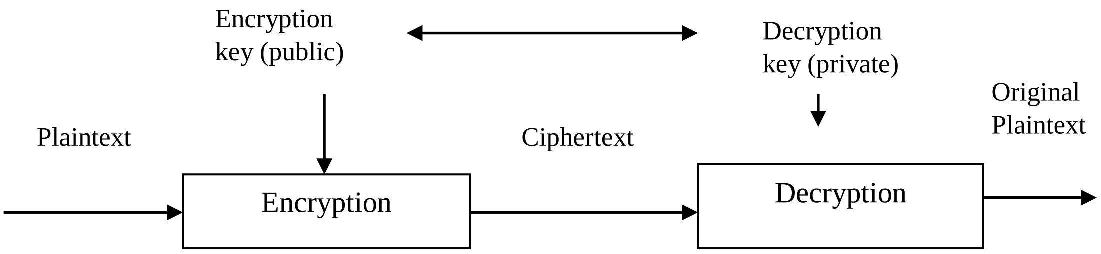


Figure 2.7 Asymmetric Key Cryptosystem

2.7.4 Hash Functions

Although the symmetric or asymmetric algorithm requires the key for encryption and decryption, hash function does not require any key. Message digests or one way encryption also called the hash function. Hash function is applied to the plaintext and the result is the fixed length block. Therefore the attacker or intruder cannot estimate either the contents of the plaintext or cannot retrieve the length of the plaintext. Therefore, hash algorithm is used as the digital signature and this can provided the validity of message or file, which has not been altered by an intruder or masquerader. In addition, by applying hash algorithm to the encryption and decryption system, the proposed system can also provide the integrity of a file or message. The most popular hash algorithm are listed as below:

- *Message Digest 5 (MD5)*: MD5 is the most commonly used hashing algorithm and produces the output of 128-bit from an arbitrary length message.
- *SHA-1*: SHA-0 is the first version of secure hash algorithm and SHA-1 is is the second version. SHA-1 creates 160-bit outputs. MD5 checksum algorithm contain the weakness and SHA-1 hash algorithm is used to substitute at the place of MD5.
- SHA-1 hash algorithm is become popular and it was actually implemented as a FIPS 140 compliant hashing algorithm.
- *SHA-2*: SHA-2 is the third version of hashing algorithm and it contain subtype of hash algorithm such as SHA-224, SHA-256, SHA-384, and SHA-512. Each algorithm is represented by the length of its output. SHA-2 algorithms are more secure than SHA-1 algorithms, but SHA-2 has not gained widespread use.

The new hash algorithm is invented and it is names as *Keyed hash* algorithm. This algorithm is more secure when apply to application. Using the secret key in Keyed hashes algorithm and this algorithm is similar with regular hashes except. The .NET Framework support two keyed hashing algorithms:

- **HMACSHA1. The design of HMACSHA1 is** based on SHA-1 hash algorithm and the output is the hash-based message authentication code. The combination of secret key with the original message and create a hash value by using SHA-1 in HMACSHA1. HMACSHA1 algorithm also produces a 160-bit hash, this length is similar to SHA-1.
- **MACTripleDES.** Messages or files are encrypted with TripleDES also known as MACTripleDES. In this hash algorithm, the bits of ciphertext is discarded until remain the final 64 bits.

2.8 Related Works

A. Guru, A. Ambhaikar explained about AES and RSA- based Hybrid Algorithm for message encryption & Decryption [1]. This paper described not only the advantages of AES algorithm is faster speed in encryption and decryption with short length of key but also utilizes the stability and key management of RSA algorithm. Therefore these advantages are combined in encryption and decryption of the system.

This paper applied these advantages AES and RSA hybrid encryption algorithm to the implementation of file encryption and suggest their advantages and drawbacks.

B.Rana, S. Wankhade analyzed Hybrid Cryptographic Algorithm for Enhancing Security of text at International Conference on emanations in Modern Technology and Engineering, 2017 [2]. The hybrid model used a combination of three symmetric algorithms AES, DES and IDEA. This paper presented the comparison of different parameter of result analysis for different .The proposed algorithm used three different keys of different length for encryption and decryption process.

Salini Dev P V, A.P. Jose, J.Joseph, show that hybrid encryption algorithm for data transmission over public network [7]. This paper compared the combination results of 3DES and RSA algorithms with the combination of ABE and AES algorithms. In addition, this paper proposed an effective method for safe transmission of message via internet. This paper compared the facts of DES, 3DES and AES. This paper presented the effective method to resolve the problem of safe transmission in Internet.

E.S.I.Harba analyzed the combination of AES, RSA and HMAC algorithm for secure data encryption [4]. This system proposed well known designed of file encryption for transferring secure file. This system expand authorization to protect passwords and other credentials from being stolen. This paper presented to combine the benefits of three encryption techniques such as symmetric algorithm, AES, asymmetric algorithm, RSA and HMAC hash algorithm. AES is used to encrypt the data file, RSA is used to encrypt the AES key and hash function is used to create the hash value to protect a secure transmitting between server and client or client to client. HMAC hash value is difficult to attack by common attacked methods.

G.V.S Pavan Mallik and Y. Saranya Bala presented methods which upgrades the security of data especially sent through emails by hybrid encryption [5]. The proposed solution is an implementation of Hybrid Encryption that uses RSA and AES cryptographic algorithms. This model encrypts the data in email and can only be decrypted by authorized users.

S. Kuswaha, P.B. Choudhary designed to combine the benefits of AES and RSA cryptographic algorithms [8]. The primary goal for all types of data transmission over the network is to have great security due to the large amount of data in transmitted increase day by day. This is reached by using security control in the system. As the role of data issue security is increasingly important, to protect the transferring information between sender and receiver over the network become difficult task.

CHAPTER 3

HYBRID AES-RSA ENCRYPTION

3.1 Public Key Cryptosystem

Two keys are applied in public key cryptosystem, one key is used for encryption and another key for decryption but these two are related for this system. The main attractive features of public key cryptosystem are defined as follow:

- The person who have the knowledge of cryptography and the encryption key, it is computationally impractical to define the decryption key for the decryption process.

In addition, RSA public key cryptosystem also reveal the following features:

- Either of the two related keys can be used for encryption, with the other used for decryption.

A public key encryption scheme consists of six components:

- **Plaintext**: plaintext is the primary input of the system with the form of readable message format.
- **Encryption algorithm**: encryption algorithm is the mathematical computation on the plaintext by using transformations.
- **Public key and private key**: public key and private key pair is used in public key cryptosystem. Public key is used for encryption process and private key is used for decryption. The exact transformation is carry out by the encryption algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** ciphertext is the output of the system with the form of unreadable message format. The ciphertext format is depend on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm**: Decryption algorithm receive the ciphertext from the sender and the matching key and produces the original plaintext. The main important steps are the following:
    - Each participant create a key pair to be applied for the message encryption and decryption process.

- And then one of these two keys is placed in a public register or other available file by each participants. This key is referred to as public key. Other associate key is the private key and is kept secret. As figure 3.1a demonstrates each participant keep a collection of public keys from other participants.
- For example, if Bob want to transfer a confidential data or message to Alice, Bob use the Alice's public key to encrypt the data.
- At the receiver side, Alice accept the message from the Bob, Alice decrypt the message using her private key. Other participant cannot decrypt the message because Alice use her own private key.

For public key cryptosystem, public keys can be accessed by all participants. Private keys are created by each participant and therefore this key need to be distributed. Private key plays an important role for controlling the system and therefore transmission between sender and receiver become secure. The system can alter its private at any time and the associate public key is shared to its old public key.

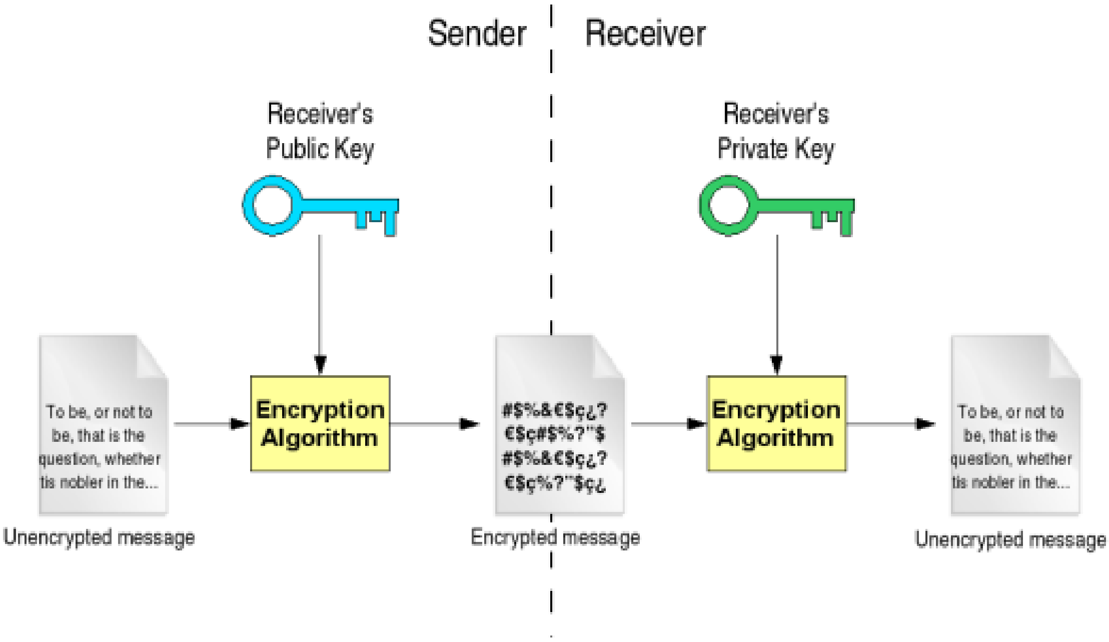


Figure 3.1 Public Key Cryptosystem

The important feature of symmetric and public key encryption algorithms are outline in Figure 3.1. The most different factor between these two systems is the usage of key as a secret key in public key encryption. The two keys used for public key encryption are referred to as the public key and private key. The private key is kept secret but it is referred to as a private key rather than a secret-key to avoid confusion with symmetric encryption [10].

Table 3.1 Conventional and public key encryption

Conventional	Public Key Encryption
Need to work: 1. For encryption and decryption process, the same key is supported for the same algorithm. 2. Key is same for the algorithm, so same key is used by sharing the sender and receiver. **Need for Security** 1. The share key between sender and receiver must be maintained secretly. 2. If the information is stored in unreadable format, the person should not get the original message or at least inappropriate to decipher content of the message. 3. The key cannot be estimated even though the person have the sample of ciphertext and knowledge of the cryptographic algorithm.	**Need to work** 1. Single algorithm is used with the pair of key, one key for encryption and other key for decryption. 2. Each sender and receiver must have one of the matched pair of keys. **Need for Security** 1. Public or private key must be kept secret. 2. It must not be possible or at least impractical to decipher a message if no other information is available. 3. There is no sufficient to estimate the key even though that the person have the knowledge of the algorithm, have one of the key and have the part of ciphertext.

3.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is the popular encryption algorithm in cryptographic system. This is start established by the National Institute of Standard and Technology (NIST) in 2001 [11]. There are two types of cipher in cryptography such as stream cipher and block cipher. In block cipher encryption, plaintext messages or data are divided into fixed size blocks before transforming these messages into ciphertext using a key. AES is the symmetric block cipher algorithm with a block size of 128 bits. Three types of block ciphers are composed in AES such as AES-128, AES-192 and AES-256. This means AES-128 uses 128-bit key length, AES-192 uses 192-bit key length and AES-256 uses256-bit key length for encryption and decryption a block of message. In AES, data is encrypted and decrypted for each block in 128 bits using the key size of 128, 192 and 256 bits, respectively. The number of rounds depends on the key length as follows:

- 10 rounds for 128 bit key
- 12 rounds for 192 bit key
- 14 rounds for 256 bit key

Four main processes are composed in AES encryption such as Substitution byte, shift row, Mix-column and Addround key. These four operation are operated as inverse in decryption process. Data are operated on bytes rather than bits in AES. Therefore 128 bit block size of input data process 128 bits (16 bytes) at a time.

3.2.1 AES Encryption

Four main processes are composed in AES encryption such as Substitution byte, shift row, Mix-column and Addround key. These four operation are operated as inverse in decryption process. This processes are shown in Figure 3.2**.** Data are operated on bytes rather than bits in AES. Therefore 128 bit block size of input data process 128 bits (16 bytes) at a time.

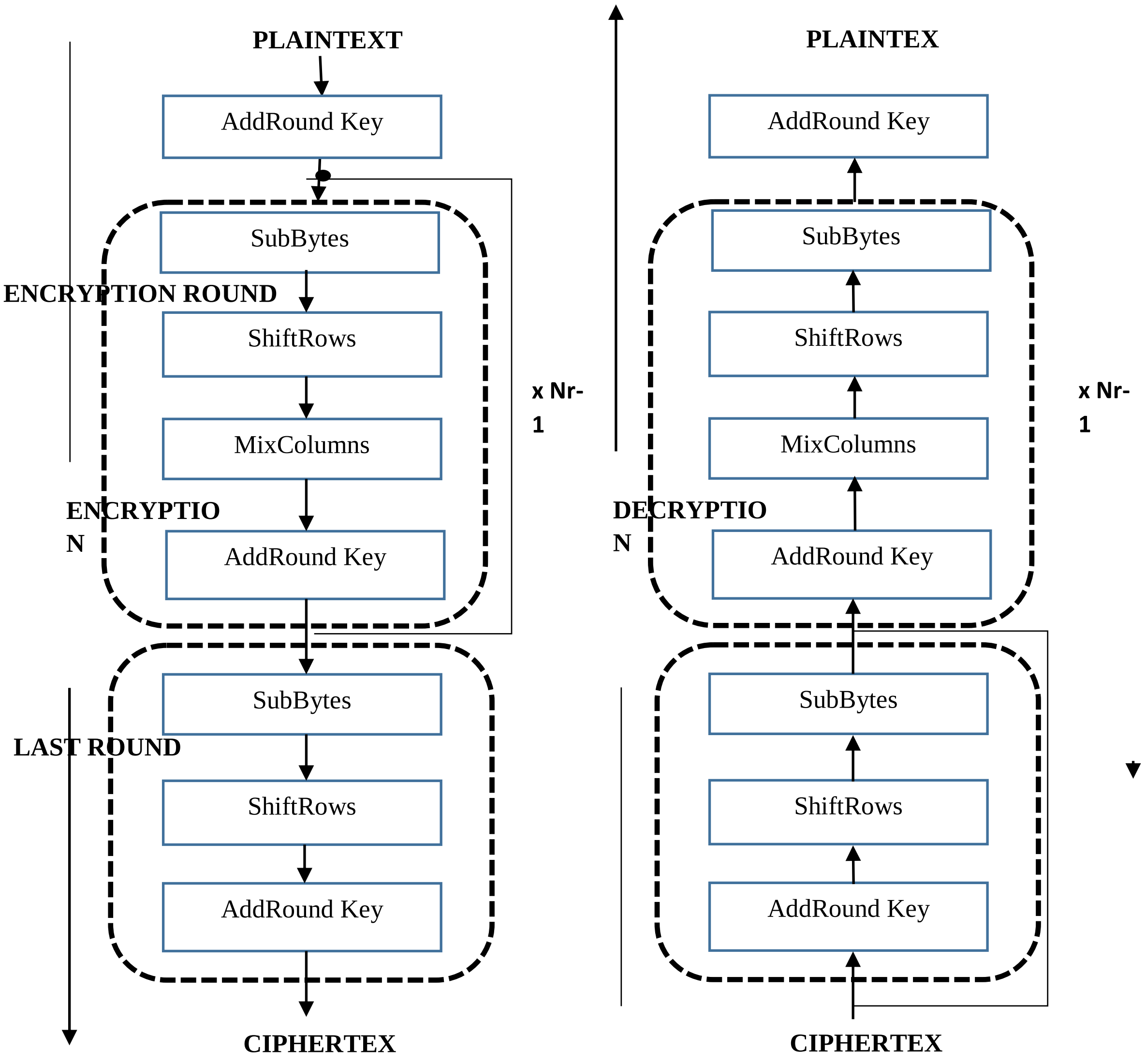


Figure 3.2 Encryption and decryption process in AES

3.2.1.1 SubBytes

SubByte perform the substitution process. Each byte is substituted by another byte and this operation is made using a lookup table also called S-box. This is shown in Table 3.2. In these substitution a byte is never substituted by itself and do not substituted by another the compliment of the current byte. The result consists of 16 byte (4×4) matrix. This process is shown in Figure 3.3.

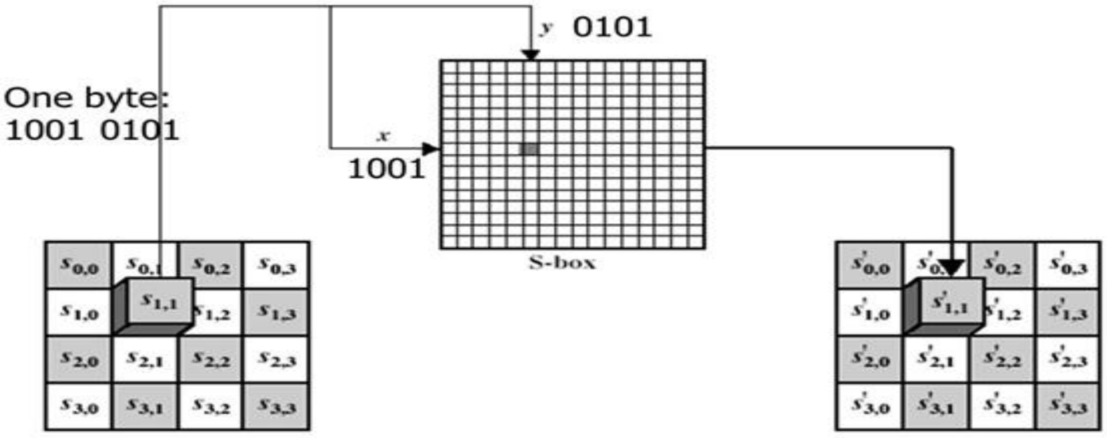

One byte:
1001 0101
y 0101
x
1001
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Figure 3.3 Substitute byte transformation

Table 3.2 SubByte transformation table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

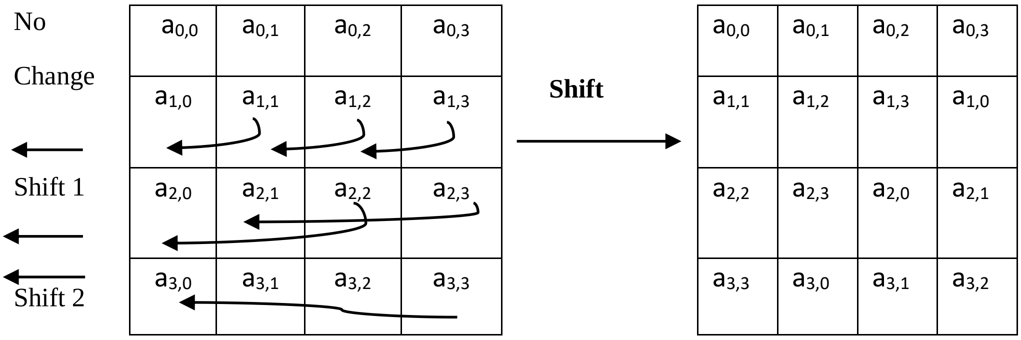
3.2.1.2 ShiftRows

In this step, each row is shifted in particular number of times. In ShiftRows process,

- There is no shifted at the first row. Therefore the value in the first row is not changed.
- Each byte is shifted one to the left at the second row.
- Similarly, each byte of third row is shifted twice to the left.
- Then, each byte of fourth row is shifted thrice to the left.

By this way, ShiftRows step produce output state contain the bytes from each column of the input state. In ShiftRows step, the important notice point is to avoid the columns are encrypted independently because AES will generate into four independent block ciphers for this case. This detail process is shown in Table 3.3.

Table 3.3 ShiftRows in AES



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

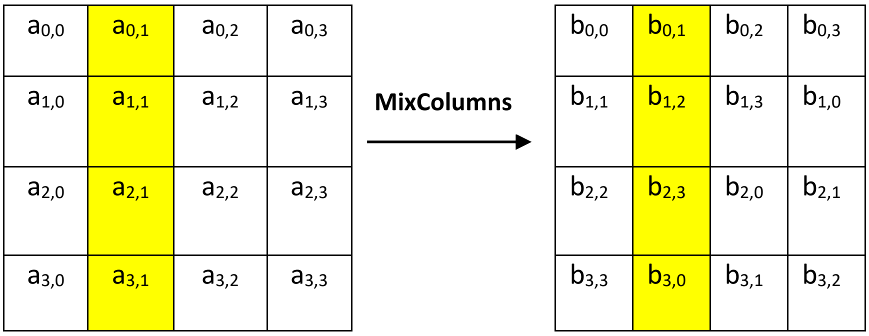
3.2.1.3 MixCloumns

In this step, apply an invertible linear transformation method to combine four bytes of each column of the state. This step performs matrix multiplication. Specific matrix is used to multiply each column of the state and therefore, the output matrix contains the position of each byte in the column is changed.

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad 0 \le j \le 3$$

Matrix multiplication is done by the combination of entries with addition and multiplication. Addition process is done by XOR operation. In the multiplication process each column is multiplied with fixed polynomial c(x). This is shown in Table 3.4

Table 3.4 MixColumns in AES



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	$b_{1,0}$
$b_{2,2}$	$b_{2,3}$	$b_{2,0}$	$b_{2,1}$
$b_{3,3}$	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$

3.2.2 AES Decryption Process

For AES decryption process, addround key stage does not need to perform the inverse. The steps of each round in decryption are as follow:

- Add round key
- Inverse mix column
- ShiftRows
- Inverse Subbyte

3.2.2.1 Add Round Key

The inverse add round key operation is defined to the forward add round key transformation because the XOR operation is its own inverse.

3.2.2.2 Inverse Mix Column

The inverse mix column operation called InvMixColumns is done by the following matrix multiplication:

$$\begin{bmatrix} a_{0,1} & a_{0,2} & a_{0,3} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

3.2.2.3 Inverse Shift Rows

The inverse shift row operation called InvShiftRows performs the circular shifts in the opposite direction for each of the last three rows, with a one byte circular right shift for the second row, and so on.

3.2.2.4 Inverse Subbyte

The inverse substitute byte transformation also called inverse SubByte (InvSubBytes) and this work is done by inverse S-box as shown in Table 3.5.

Table 3.5 Inverse SubByte transformation table

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	ca	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

3.2.3 AES Key Expansion

In the key expansion process of AES, the input key have the length of 4-word (16 bytes) and generate 44 words as linear array (176 bytes). This 4-word round key is enough to supply for the primary stage of key expansion known as Add Round Key stage. It is shown in figure 3.4.

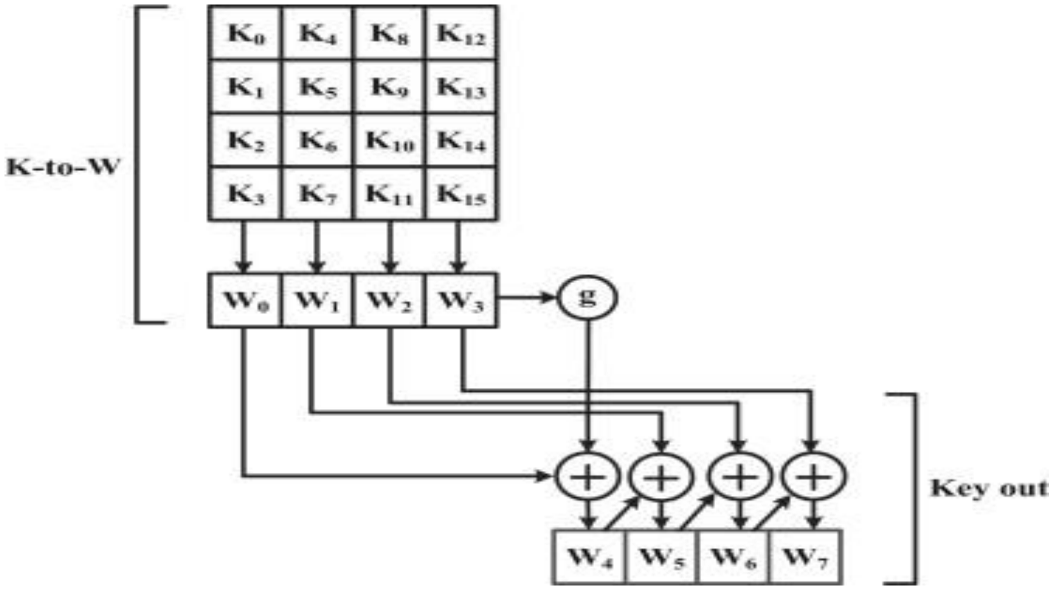

K-to-W
K_0 K_4 K_8 K_{12}
K_1 K_5 K_9 K_{13}
K_2 K_6 K_{10} K_{14}
K_3 K_7 K_{11} K_{15}
W_0 W_1 W_2 W_3
g
Key out
W_4 W_5 W_6 W_7

Figure 3.4 AES key expansion

At the key expansion process, the first four word is replaced with the key. And then next four words is added at the rest of the expanded key at a time. The filled word w[i] depend on the previous word, w[i-1]. Therefore, the position of four word is back, w[i-4]. XOR operation is used for three out of four cases. The more complex function is applied in **w** array and the position of word is multiply by 4. Figure 3.3 demonstrates the creation of the first eight words of the expanded key. In this figure, the symbol **g** means the complex function.

The function **g** consists of the following sub functions:

1. Left shift circulation is carry out for one byte of a word and this word is known as Rotword. It is defined as [k0,k1,k2,k3] is transformed into [k1,k2,k3,k0].
2. SubWord carry out a byte substitution on each byte of its input word, using S-Box.
3. The round constant, Rcon [j] is XORed with the output of step 1 and step 2

The value of word is always 0 at three rightmost bytes of the round constant, Rcon [j]. Therefore, XOR operation is performed only on the leftmost byte of the word and the round constant Rcon [j] is XORed with a word. At each round, the round constant is not equal and is defined as Rcon [j] = (RC[j], 0, 0), with RC[1] =1, RC[j]= 2 XOR RC[j-1]. The hexadecimal values of RC[j] are as follows:

J	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

3.2.4 Advantages and Disadvantages of AES Algorithm

Advantages of AES algorithm are listed as below**:**

- AES algorithm have the robust security scheme because this algorithm is evaluated in both software and hardware.
- The most significant factor for robust security of AES is the various key length sizes of this algorithm. AES use three different key length size such as 128 bits, 192 bits and 256 bits.
- AES algorithm is widely used in various transmission protocol for the security reason such as wireless communication, financial transactions, e-business, encrypted data storage etc.
- It is one of the most spread commercial and open source solutions used all over the world.
- Attacker cannot hack the personal information.
- No one can hack your personal information.
- In AES, attacker must try 2^{128} time to break the result for 128-bit length key size. So the system with AES algorithm is assumed as secure because this amount of time is difficult.

Disadvantages of AES Algorithm are listed as below:

- The main drawback of AES algorithm is it uses very simple algebraic structure.
- Another factor is using the same way to encrypt every block.
- Although this algorithm can be implemented in both software and hardware, implement in software is difficult.

- Because the counter mode of AES is complex and therefore the performance and security point of AES must be considered.

3.3 RSA Rivest- Shamir- Adleman (RSA)

RSA encryption algorithm is the type of public key encryption algorithm. This algorithm is the most popular algorithm among other algorithms. RSA used large integer factorization in operation such as public key and private key generation, encryption process and decryption process [3]. RSA algorithm use a key pairs for encryption and decryption, the one key use for encryption process is called public key and another key use for decryption process is called private. The public key is shared among every participants as public and this key can be used to encrypt message and verify the signature. Private key is kept as secret and only the related person know this key value. Private key can be used to decrypt the ciphertext message and signs the data [12]. RSA algorithm consists of three parts:

1. Public key and private key generation
2. Encryption process
3. Decryption process

3.3.1 RSA Public Key and Private Key Generation

Steps of private key and public key generation for RSA algorithm are as follow:

- Two unequal large prime numbers p and q are randomly chosen.
- And then calculate n of p and q, $n= p \times q$
- $Ø(n) = (p-1) (q-1)$ is calculated by Euler function.
- Positive integer **e** is randomly selected between $1 < e < Ø(n)$ and $\gcd (e, Ø(n)) = 1$.
- By applying the formula of $ed =1 \bmod Ø(n)$, and then private key value d is obtained where $0 < d < n$.
- The public key **e** is get by applying the formula of, Public key, PU = {e, N}. PU is public key.
- Private Key, PR = {d, p, q}, the private key is saved, where d is the private key. PR is private key.

3.3.2 RSA Encryption process

Public key is needed to encrypt the file at the sender side.

$$C \quad = P^e \text{ mod n}$$

Where, C is the ciphertext, P is the Plaintext, e is the public key and n is the public key.

3.3.3 RSA Decryption Process

At the receiver side, decryption need the private key related with the public key used for encryption.

$$P = C^d \text{ mod n}$$

Where, P is the Plaintext, C is the ciphertext, d is the private key and n is the public key.

3.3.4 The Security of RSA

There are three types of attack possible in RSA algorithm, these are described as follows:

- **Brute force**: Brute force attack try to break up all possible private key.
- **Mathematical attacks**: various methods are applied, to reveal the product of two prime numbers.
- **Timing attacks**: timing attack usually occur at the running time of the decryption algorithm.

By using a large key space, the cryptosystem can protect the brute-force attack for RSA algorithm. This is commonly use method in other cryptosystem for the security. As the number of bits in e and d is larger, the security of the system is better. However, this approach involves complex calculation both in key generation and in encryption/decryption process. Therefore, as increasing the key length size, the execution time of the system may be slower [10].

3.3.5 Advantages and Disadvantages of RSA Algorithm

Advantages of RSA

- The implementation of RSA algorithm is very easy.
- When transmitting confidential data, RSA algorithm is safe and secure.

- Involving mathematical calculation in RSA, attacker confuse to attack and difficult to break.
- Key sharing between the sender and receiver is simple and easy.

Disadvantages of RSA

- Although some system consider security option but they fail security suspect because to complete encryption, their system required both symmetric and asymmetric encryption. However, RSA support symmetric encryption only.
- The main shortcoming point of RSA algorithm is slow data transfer rate because RSA algorithm contain large number of mathematical calculation.
- In addition, at sometimes RSA algorithm needs third party to verify the reliability.
- When receive the encrypted file or message at the receiver side, the system required high processing for decryption.

3.4 HMAC SHA-256 Algorithm

Accurate and reliable data is very important for organization to make decision on these data. Therefore, user need to measure data integrity and authentication for this system. HMAC SHA-256 algorithm is used to provide data integrity for this proposed system. HMAC is a message authentication code get by processing a cryptographic has function SHA 256 over the data [3]. HMAC SHA-256 algorithm apply both data integrity and authentication due to the both use of key and hash function. The work of HMAC SHA-256 is shown in figure 3.5.

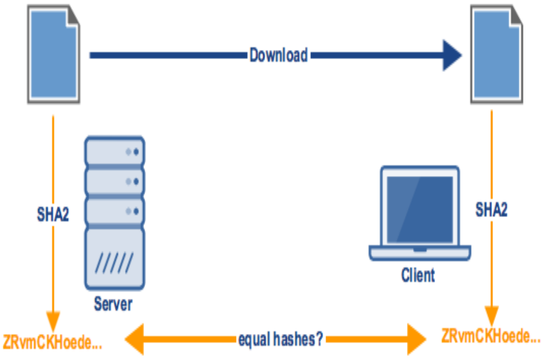


Figure 3.5 HMAC algorithm

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 Overview of the System

Data are very important for organization. Therefore many organization need to protect their information or data when transmission. This system intends to implement the combination of the AES and RSA algorithm in order to more secure than single algorithm. PEC's Student marks file is sent from Pyay Education College to Naypyidaw office for examination result. Student's data are stored in excel files format and place in the computer. This file is encrypted using AES algorithm. And then AES's Key is encrypted by using RSA's public key. SHA-256 algorithm is applied to generate the hash value. Hash value is used for authentication. The encrypted file, key and hash value are sent to the receiver. The receiver decrypts the encrypted key by using the RSA's private key. And then, the receiver also decrypts the encrypted file by using the AES's decryption algorithm. In the receiver side, SHA-256 algorithm is also applied to generate hash key value. And then compare this hash key value with the receive hash key value. If the key value is matched with the sender and receiver, this file is authenticate and if not, assume the receive file is not correct and the decryption process will be exit. The overview of the proposed system is shown in Figure 4.1.

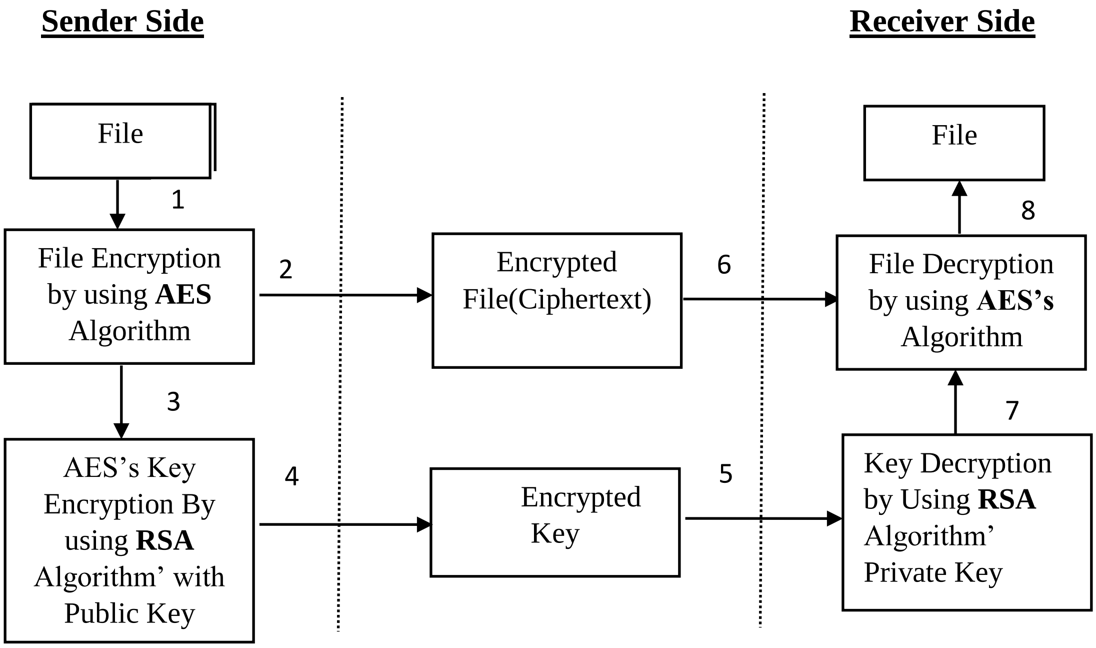

Sender Side
Receiver Side
File
1
File Encryption by using AES Algorithm
2
Encrypted File(Ciphertext)
6
File Decryption by using AES's Algorithm
8
File
3
AES's Key Encryption By using RSA Algorithm' with Public Key
4
Encrypted Key
5
Key Decryption by Using RSA Algorithm' Private Key
7

Figure 4.1 Overview of the proposed system

4.1.1 Data Format

Pyay Education College's student mark files are stored in computer hard disk and recorded as excel format. This files contain student's Roll No., Student Names, Subjects, Total marks, Result, Grade. Storage file sizes are vary depend on the attending student number on each academic year. Sample data record is shown in Table 4.2.

Table 4.2 Sample Record Data

No.	Roll No.	Name	Methodology					Academic							Total	Result	Grade	Remark
			Theory	Psychology	Myanmar	English	Maths	Geology	History	Myanmar	English	Maths	Physis	Biology				
1	D.T.Ed(19/15)-2	Ma Aye Mya Mya	43	40	40	38	41	46	42	41	37	37	39	43	487	PASS	4.5	*
2	D.T.Ed(19/15)-9	Ma Ei Nandar	42	37	41	35	40	45	42	44	42	41	37	41	487	PASS	4.5	*
3	D.T.Ed(19/15)-6	Mg Hein Lin	45	45	35	44	39	38	45	39	39	36	39	38	482	PASS	4.5	*
4	D.T.Ed(19/15)-3	Mg Wai Yan	45	42	43	40	45	33	37	38	34	37	45	42	481	PASS	4.5	*
5	D.T.Ed(19/15)-4	Ma Thin Ei Ei	33	44	42	42	37	34	42	40	42	44	41	40	481	PASS	4.5	*
6	D.T.Ed(19/15)-10	Ma Thandar	41	36	40	43	33	32	39	42	38	40	39	40	463	PASS	4	*
7	D.T.Ed(19/15)-1	Ma Hnin Htet Hlaing	34	31	41	39	42	39	40	41	37	35	33	36	448	PASS	3.5	
8	D.T.Ed(19/15)-8	Ma Wai Hnin	35	30	35	38	41	40	37	38	41	33	40	39	447	PASS	3.5	

4.2 Encryption Process of the Proposed System

In sender side, choose the input student's mark file (plaintext). The sender generates the hash key value by using HMAC SHA-256 algorithm. The key is used to encrypt the Students' file with AES's algorithm. Data in the file are transformed to encrypted value. RSA's public key is utilized to encrypt the AES Key. And then, the sender sends the encrypted file, encrypted key and hash value to the receiver. This process is shown in Figure 4.2.

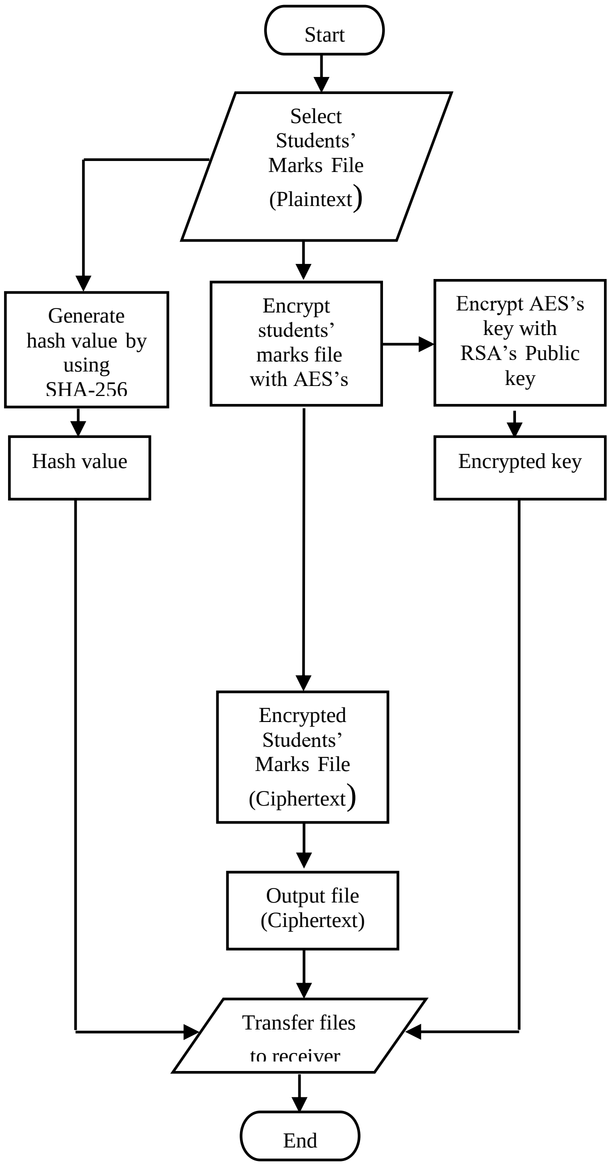
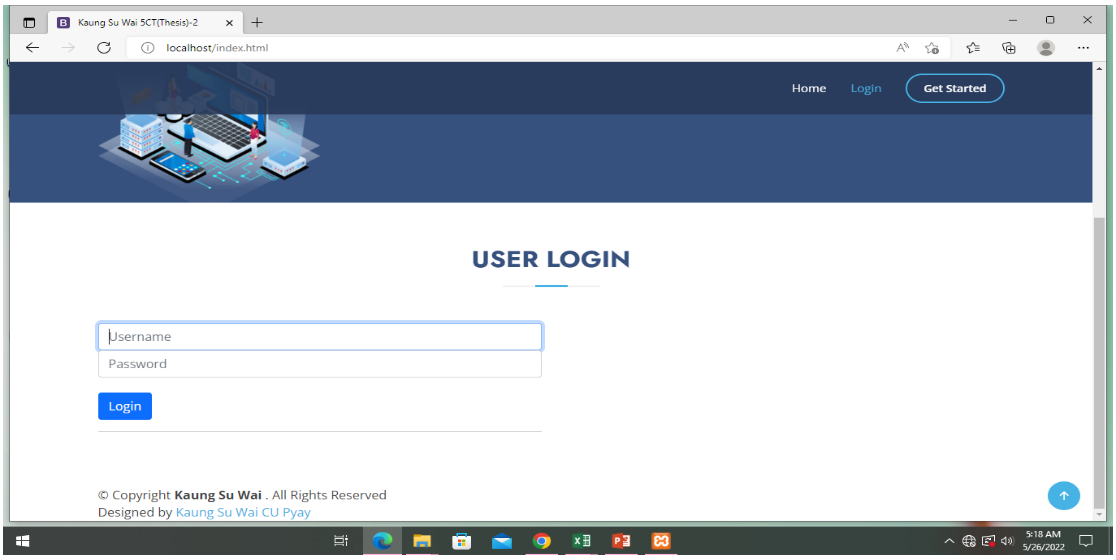

Start
Select Students' Marks File (Plaintext)
Generate hash value by using SHA-256
Encrypt students' marks file with AES's
Encrypt AES's key with RSA's Public key
Hash value
Encrypted key
Encrypted Students' Marks File (Ciphertext)
Output file (Ciphertext)
Transfer files to receiver
End

Figure 4.2 Flow diagram of the sender side

4.2.1 User Interface of Sending Process

The first interface of the proposed system is ‘User Login’ page. User need to type username and password in order to access the system. This is shown in Figure 4.3.

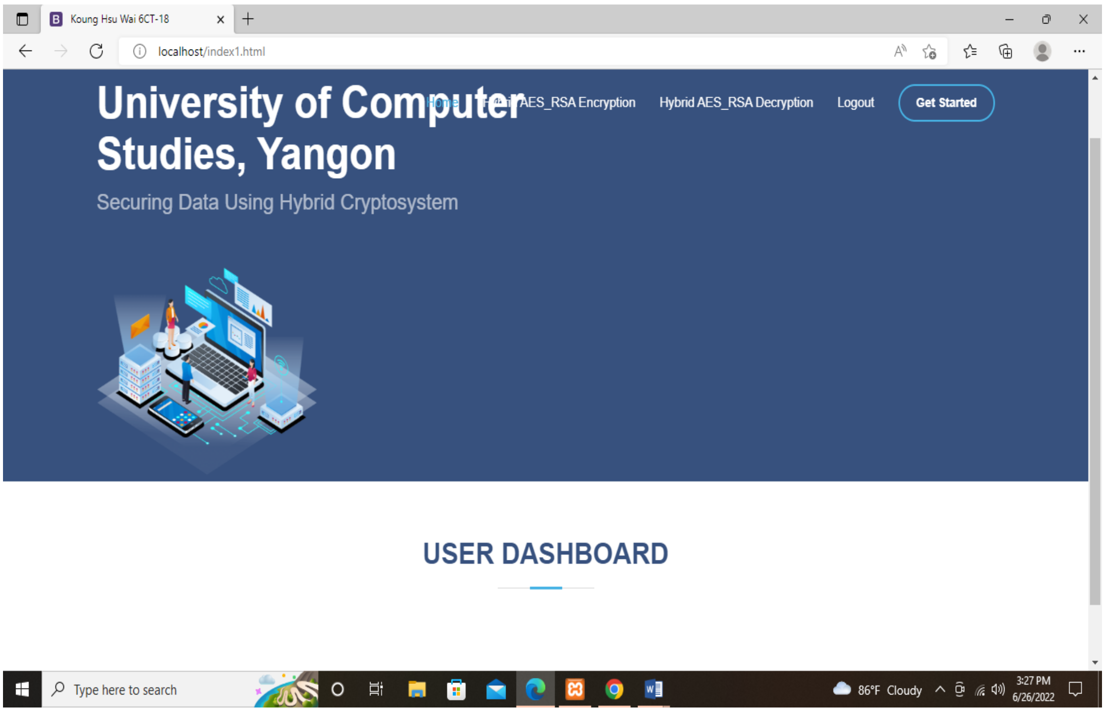


USER LOGIN

© Copyright **Kaung Su Wai** . All Rights Reserved
Designed by Kaung Su Wai CU Pyay

Figure 4.3 User login page

After login into the system with user name and password, ‘User Dashboard’ of my proposed system is showed as in Figure 4.4. In this page user must choose the Hybrid AES_RSA Encryption tab in order to make encryption process.



University of Computer Studies, Yangon

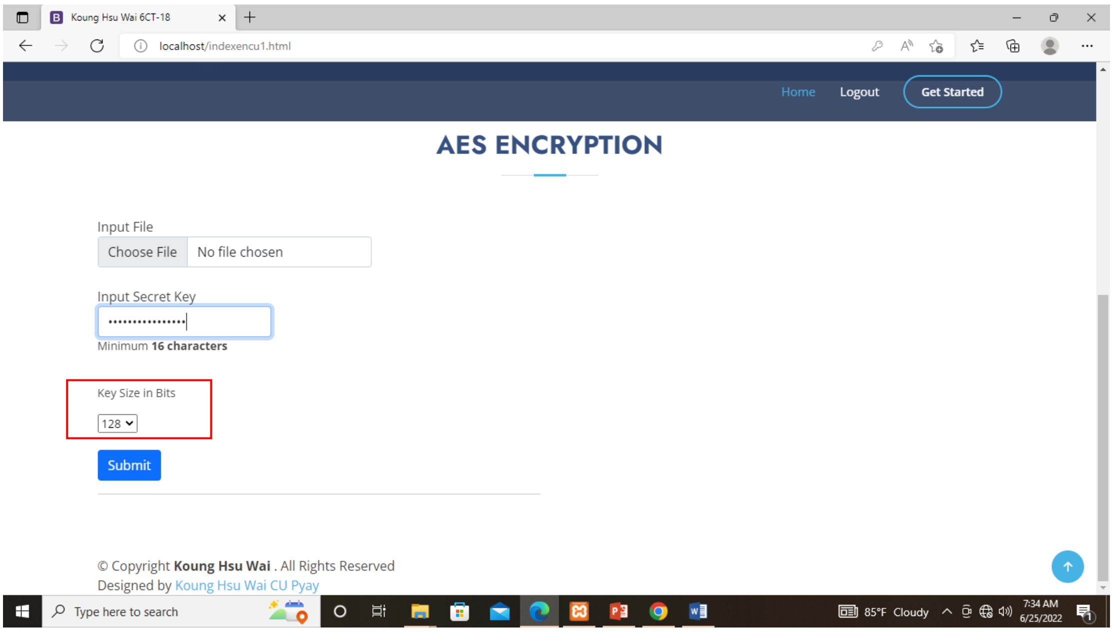
Securing Data Using Hybrid Cryptosystem

USER DASHBOARD

Figure 4.4. User Dashboard

4.2.2 Encryption Process in Sender Side

In the sender side, the user choose the plaintext PEC student's mark file in order to make encryption with AES key. These mark files are stored in computer drive with excel file. This process is shown in Figure 4.5. After selecting the file from computer drive, give the input key to encrypt the file. Input key must contain one lowercase letter, one capital letter, one number and at least minimum 8 character for one password creation. AES algorithm have three types of key length size such as 128 bit, 192 bits and 256 bits. Therefore, user must choose the key length size. It is shown by red rectangular box in figure 4.6. And then click the submit button to do AES encryption.



AES ENCRYPTION

Input File

Choose File No file chosen

Input Secret Key

••••••••••••••••

Minimum **16 characters**

Key Size in Bits

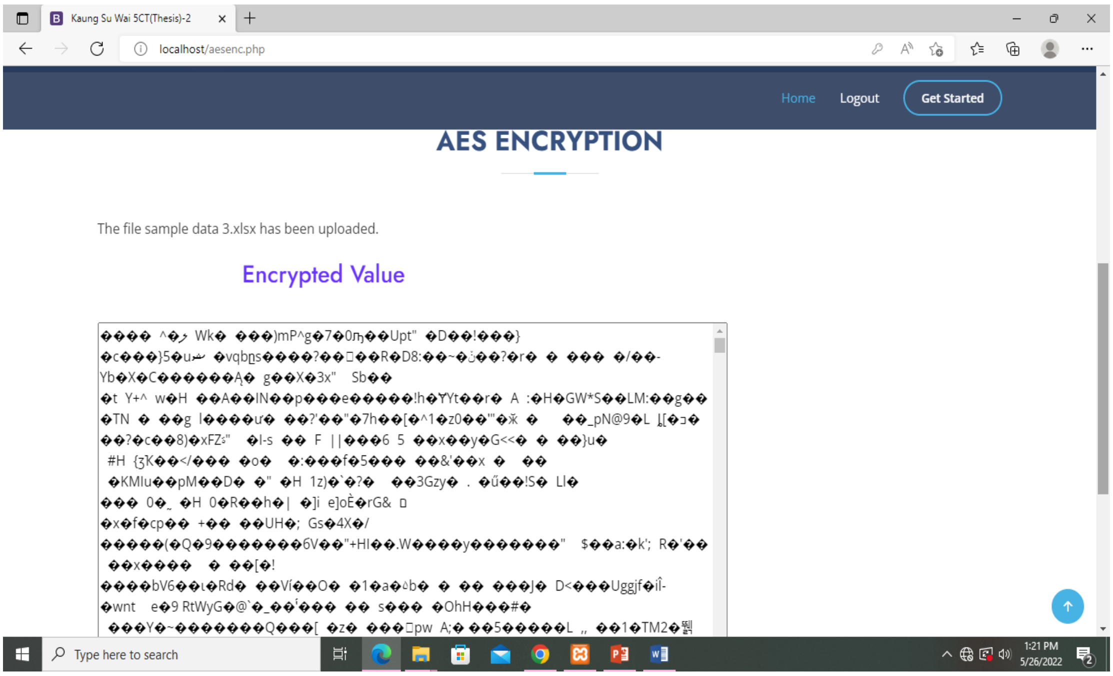
128

© Copyright **Koung Hsu Wai** . All Rights Reserved

Designed by Koung Hsu Wai CU Pyay

Figure 4.5 AES encryption

After encryption, the input plaintext file is changed to encrypted value file. This result is shown in figure 4.6. In this stage, data are not readable format. If the input file is once selected, the message of "The file sample data*.xlsx has been uploaded" will be showed at the top of the page.



AES ENCRYPTION

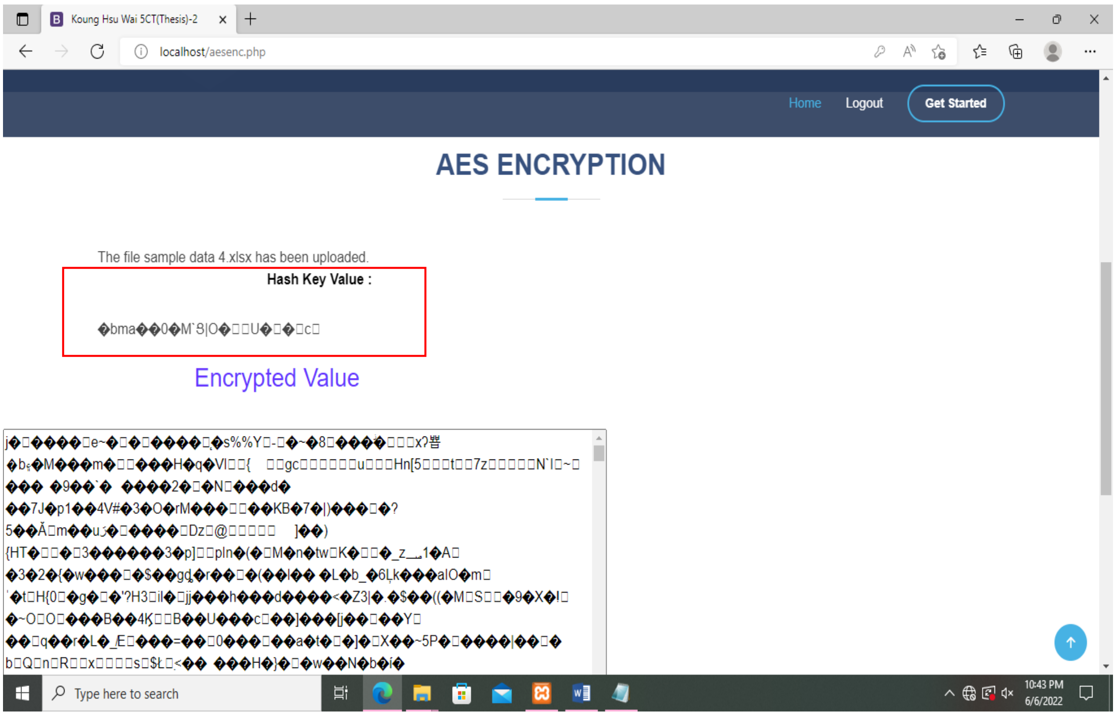
The file sample data 3.xlsx has been uploaded.

Encrypted Value

```
���� ^�ؼ Wk� ���)mP^g�7�0ђ��Upt" �D��!���}
�c���}5�uڛ �vqbฏs����?��□��R�D8:��~�ڎ��?�r� � ��� �/��-
Yb�X�C������Ą� g��X�3x" Sb��
�t Y+^ w�H ��A��IN��p����e������!h�ƔYt��r� A :�H�GW*S��LM:��g��
�TN � ��g l����ư� ��?'��"�7h��[�^1�z0��"'�ӂ �   ��_pN@9�L ʵ[�ב�
��?�c��8)�xFZؤ" �l-s �� F ||���6 5 ��x��y�G<<� � ��}u�
 #H {ʒK��</��� �o� �:���f�5��� ��&'��x � ��
 �KMIu��pM��D� �" �H 1z)�`�?� ��3Gzy� . �ű��!S� Ll�
��� 0�˷ �H 0�R��h�| �]i e]oÈ�rG& ם
�x�f�cp�� +�� ��UH�; Gs�4X�/
�����(�Q�9���������6V��"+Hl��.W�����y��������" $��a:�k'; R�'��
 ��x����  � ��[�!
����bV6��ι�Rd� ��Ví��O� �1�a�ᐞb� � �� ���J� D<���Uggjf�iÎ-
�wnt e�9 RtWyG�@`�_��ʹ��� �� s��� �OhH���#�
 ���Y�~��������Q����[ �z� ���□pw A;� ��5������L „ ��1�TM2�뛢
```

Figure 4.6 Encrypted value

HMAC SHA-256 algorithm is used to generate the hash key value. Hash key value is used to verify data integrity and authenticate the data for this proposed system. This is shown in figure 4.7 with red rectangular box.



AES ENCRYPTION

The file sample data 4.xlsx has been uploaded.

Hash Key Value :

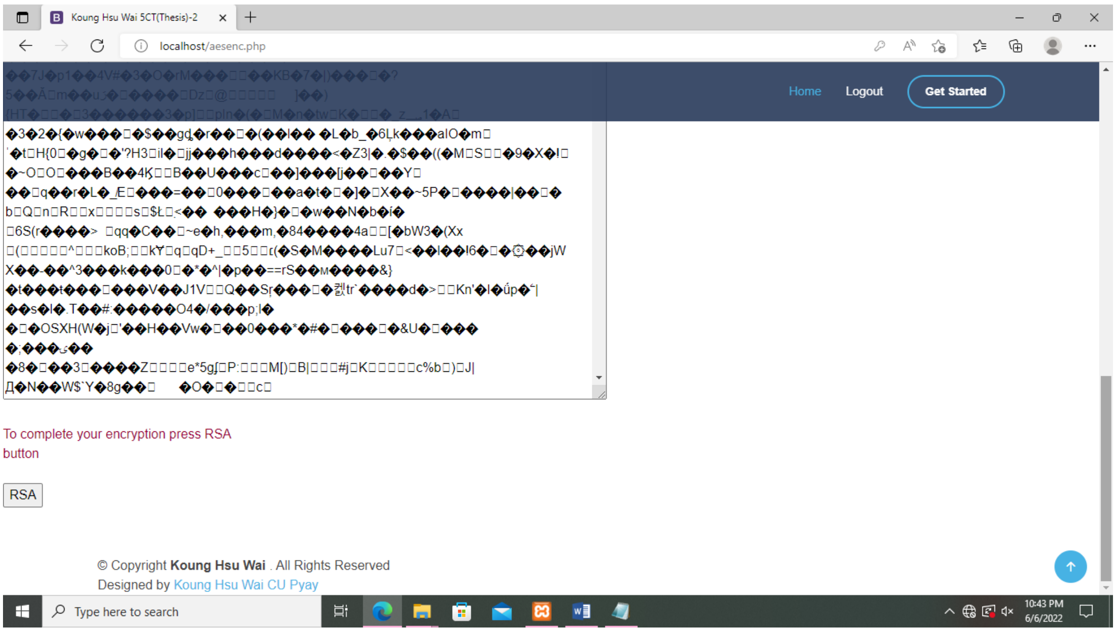
�bma��0�M`8|O�□□U�□�□c□

Encrypted Value

```
j�□����□e~�□�□����□�s%%Y□-□�~�8□����□□□x?볼
�b;�M���m�□□���H�q�Vl□□{   □□gc□□□□□□u□□□Hn[5□□□t□□7z□□□□□N`l□~□
��� �9��`� ����2�□�N□���d�
��7J�p1��4V#�3�O�rM���□□��KB�7�|)���□�?
5��Â□m��u;�□����□Dz□@□□□□□   ]��)
{HT�□□�□3������3�p]□□pln�(�□M�n�tw□K�□□�_z_1�A□
�3�2�{�w���□�$��gd�r��□�(��!�� �L�b_�6Lk���alO�m□
`�t□H{0□�g�□�'?H3□il�□jj���h���d����<�Z3|�.�$��((�M□S□□�9�X�!□
�~O□O□���B��4K□□B��U���c□��]���[j��□��Y□
��□q��r�L�_Ɇ□���=��□0���□��a�t�□�]�□X��~5P�□����|��□�
b□Q□n□R□□x□□□□s□$Ł□<�� ���H�}�□�w��N�b�i�
```

Figure 4.7 Hash key value

In the sender side, after encrypting the PEC student's mark file with AES key, the system go with RSA algorithm to complete the encryption process. So, user click RSA button and display in figure 4.8.



```
��7J�p1��4V#�3�O�rM���□□��KB�7�|)���□�?
5��Â□m��u;�□����□Dz□@□□□□□   ]��)
{HT�□□�□3������3�p]□□pln�(�□M�n�tw□K�□□�_z_1�A□
�3�2�{�w���□�$��gd�r��□�(��!�� �L�b_�6Lk���alO�m□
`�t□H{0□�g�□�'?H3□il�□jj���h���d����<�Z3|�.�$��((�M□S□□�9�X�!□
�~O□O□���B��4K□□B��U���c□��]���[j��□��Y□
��□q��r�L�_Ɇ□���=��□0���□��a�t�□�]�□X��~5P�□����|��□�
b□Q□n□R□□x□□□□s□$Ł□<�� ���H�}�□�w��N�b�i�
□6S(r����> □qq�C��□~e�h,���m,�84����4a□□[�bW3�(Xx
□(□□□□□^□□□koB;□□kY□q□qD+_□□5□□ɩ(�S�M����Lu7□<��l��l6�□�□۞��jW
X��-��^3���k����0□�*�^|�p��==rS��м����&}
�!���t���□���V��J1V□□Q��Sɾ���□�캤tr`����d�>□□Kn'�l�úp�"|
��s�l�.T��#.�����O4�/���p;l�
�□�OSXH(W�j□'��H��Vw�□��0���*�#�□���□�&U�□���
�;���ی��
�8�□��3□����Z□□□□e*5g[□P:□□□M[)□B|□□□#j□K□□□□□c%b□)□J|
Д�N��W$`Y�8g��□    �O�□�□□c□
```

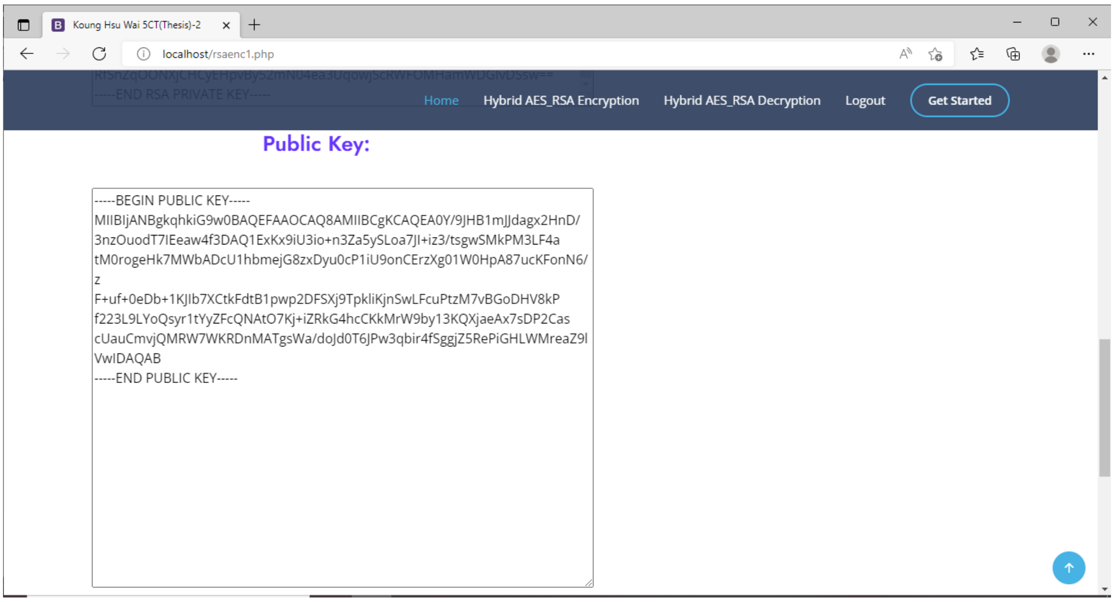
To complete your encryption press RSA button

RSA

© Copyright **Koung Hsu Wai** . All Rights Reserved
Designed by Koung Hsu Wai CU Pyay

Figure 4.8 RSA

In this step, RSA’s public key is applied to encrypt the secret key of AES. Public key of RSA algorithm is displayed in figure 4.9.

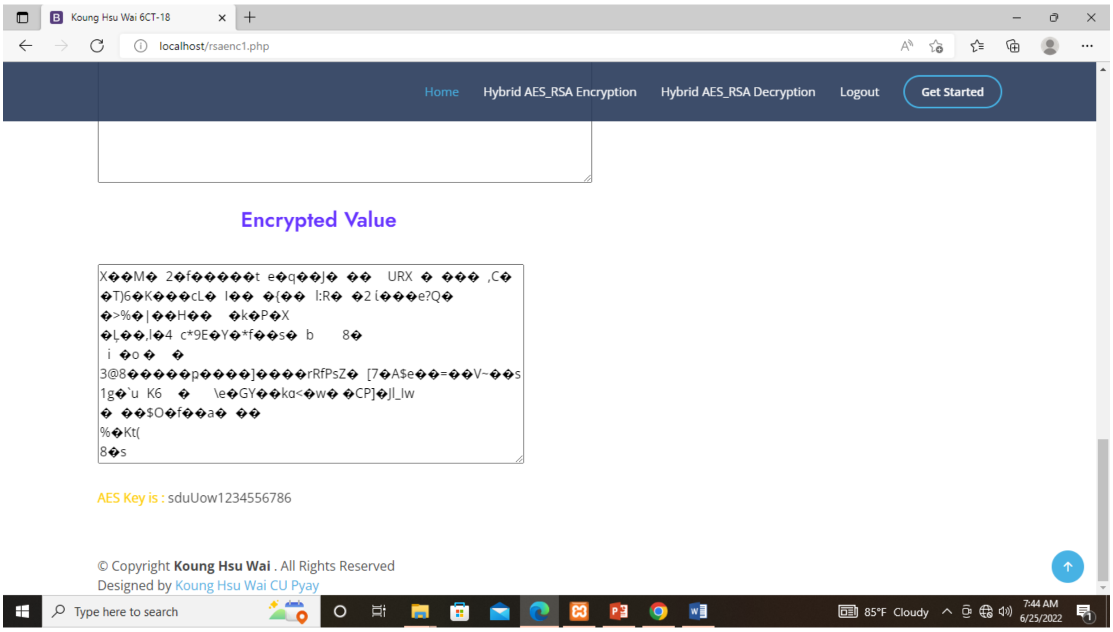

Koung Hsu Wai 5CT(Thesis)-2
localhost/rsaenc1.php
-----END RSA PRIVATE KEY-----
Home
Hybrid AES_RSA Encryption
Hybrid AES_RSA Decryption
Logout
Get Started

Public Key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0Y/9JHB1mJJdagx2HnD/
3nzOuodT7IEeaw4f3DAQ1ExKx9iU3io+n3Za5ySLoa7JI+iz3/tsgwSMkPM3LF4a
tM0rogeHk7MWbADcU1hbmejG8zxDyu0cP1iU9onCErzXg01W0HpA87ucKFonN6/
z
F+uf+0eDb+1KJIb7XCtkFdtB1pwp2DFSXj9TpkliKjnSwLFcuPtzM7vBGoDHV8kP
f223L9LYoQsyr1tYyZFcQNAtO7Kj+iZRkG4hcCKkMrW9by13KQXjaeAx7sDP2Cas
cUauCmvjQMRW7WKRDnMATgsWa/doJd0T6JPw3qbir4fSggjZ5RePiGHLWMreaZ9l
VwIDAQAB
-----END PUBLIC KEY-----
```

Figure 4.9 RSA’s public key

After applying RSA’s public key to the AES’s key, the final encrypted key will be obtained and this is shown in figure 4.10.



Encrypted Value

```
X��M�  2�f������t  e�q��J�  ��    URX  �  ���  ,C�
�T)6�K���cL�  I��  �{��  I:R�  �2 ί����e?Q�
�>%�|��H��    �k�P�X
�Ļ��,l�4  c*9E�Y�*f��s�  b      8�
 i  �o �     �
3@8������p�����]�����rRfPsZ�  [7�A$e��=��V~��s
1g�`u  K6    �      \e�GY��kα<�w� �CP]�Jl_Iw
�  ��$O�f��a�  ��
%�Kt(
8�s
```

AES Key is : sduUow1234556786

© Copyright **Koung Hsu Wai** . All Rights Reserved
Designed by Koung Hsu Wai CU Pyay

Figure 4.10 Final encrypted value

4.3 Decryption Process of the Proposed System

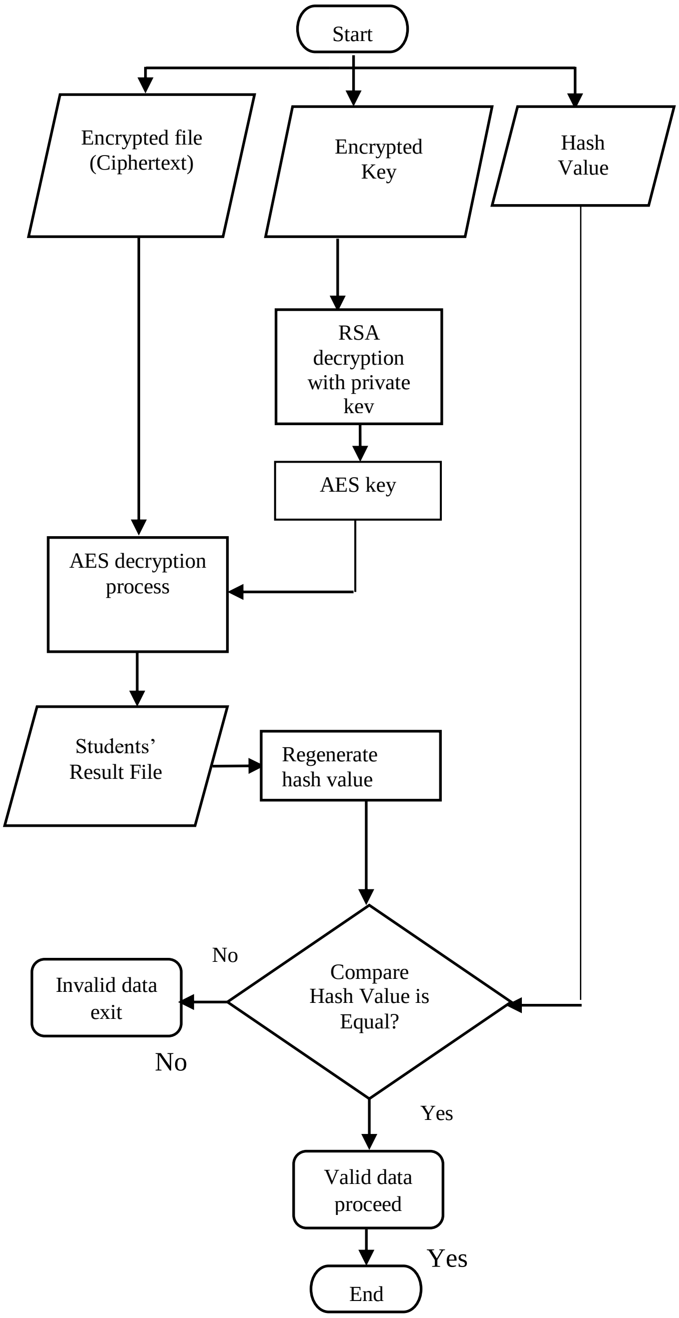
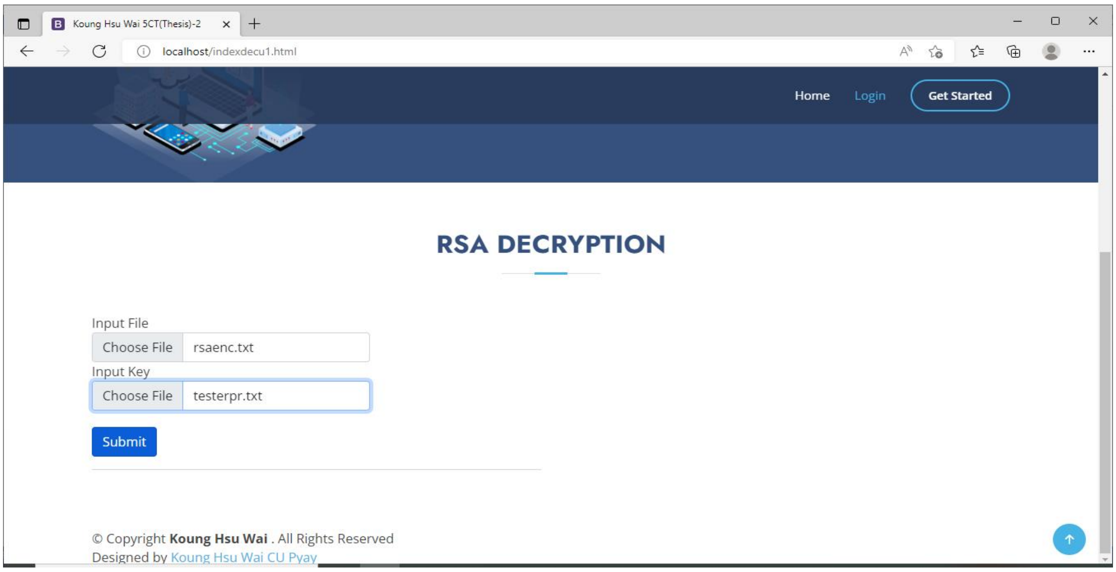


Figure 4.11 Decryption process of receiver side

Encrypted key, encrypted file and hash value are received at the receiver side and then make decryption process to this file. The detail process of the receiver side is shown in Figure 4.11. To make decryption process "Hybrid AES_RSA Decryption" button is selected. And then the place of choose file is appeared and it shown in Figure 4.12. Then, press the "Submit" button in the user interface.



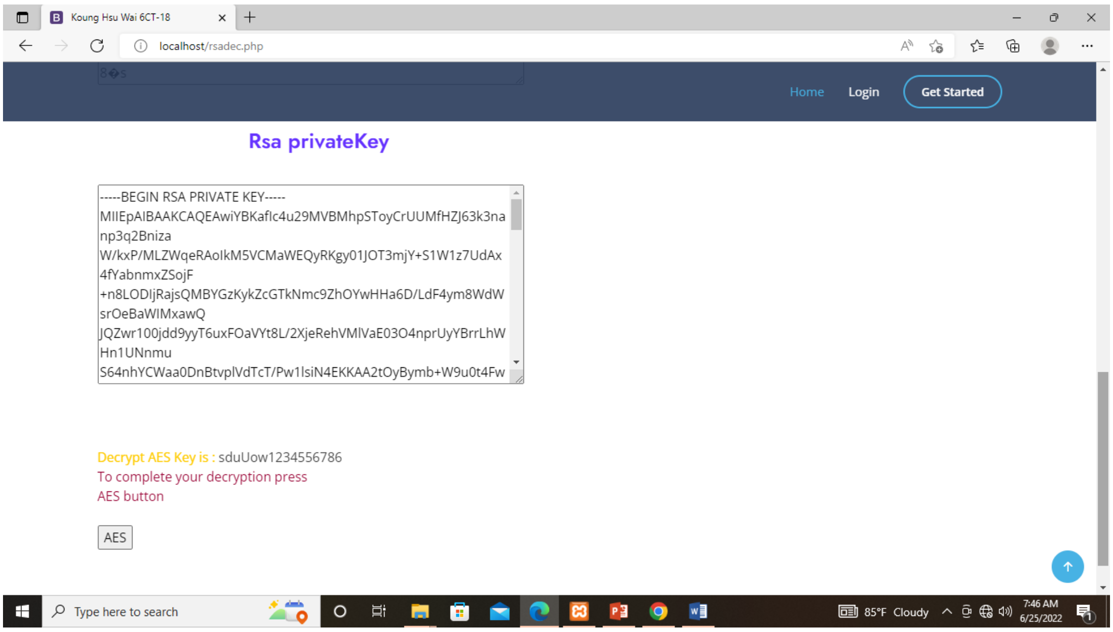
RSA DECRYPTION

Input File
Choose File rsaenc.txt
Input Key
Choose File testerpr.txt

© Copyright **Koung Hsu Wai** . All Rights Reserved
Designed by Koung Hsu Wai CU Pyay

Figure 4.12 RSA decryption

RSA's private is used to decrypt the file and press "AES" button to complete the decryption process. RSA's private key is shown in Figure 4.13.



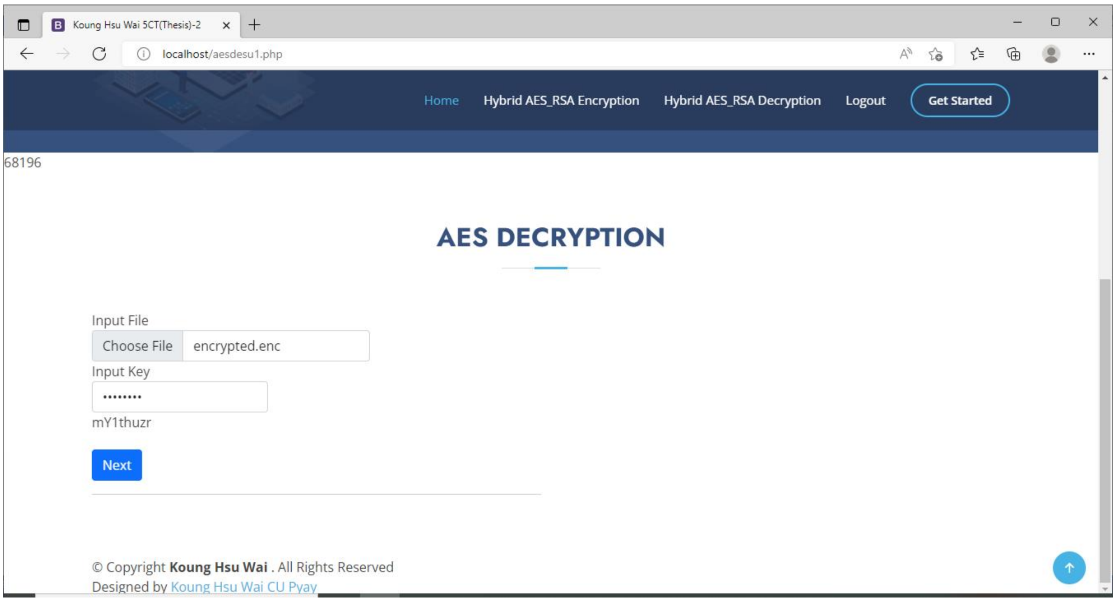
Rsa privateKey

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAwiYBKafIc4u29MVBMhpSToyCrUUMfHZJ63k3na
np3q2Bniza
W/kxP/MLZWqeRAoIkM5VCMaWEQyRKgy01JOT3mjY+S1W1z7UdAx
4fYabnmxZSojF
+n8LODIjRajsQMBYGzKykZcGTkNmc9ZhOYwHHa6D/LdF4ym8WdW
srOeBaWIMxawQ
JQZwr100jdd9yyT6uxFOaVYt8L/2XjeRehVMlVaE03O4nprUyYBrrLhW
Hn1UNnmu
S64nhYCWaa0DnBtvplVdTcT/Pw1lsiN4EKKAA2tOyBymb+W9u0t4Fw
```

Decrypt AES Key is : sduUow1234556786
To complete your decryption press
AES button

Figure 4.13 RSA's private key

At the portion of AES's decryption, receiver choose the encrypted file and AES's key to decrypt the message. And then press "Next" button to continue the process and it shown in Figure 4.14.


Koung Hsu Wai 5CT(Thesis)-2
localhost/aesdesu1.php
Home
Hybrid AES_RSA Encryption
Hybrid AES_RSA Decryption
Logout
Get Started
Choose File
Next

68196

AES DECRYPTION

Input File

encrypted.enc

Input Key

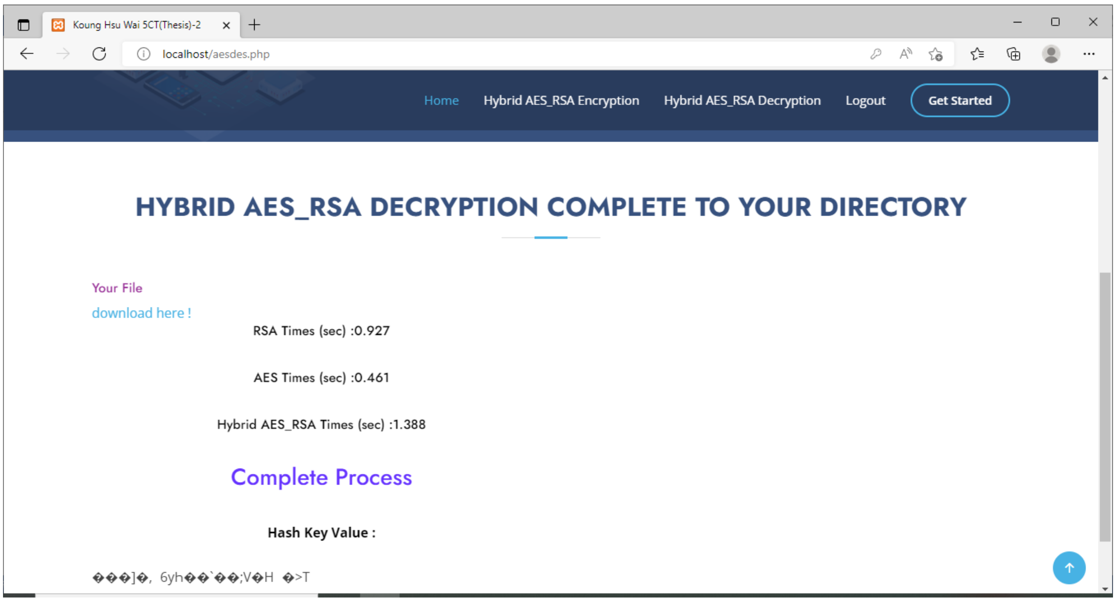
••••••••

mY1thuzr

© Copyright **Koung Hsu Wai** . All Rights Reserved
Designed by Koung Hsu Wai CU Pyay

Figure 4.14 AES Decryption

Finally, the decryption process of hybrid AES_RSA crypto system for PEC student's exam file is completed and the result file is obtained. This file can be download at this place and execution is also shown in GUI. This is displayed in Figure 4.15.


Koung Hsu Wai 5CT(Thesis)-2
localhost/aesdes.php
Home
Hybrid AES_RSA Encryption
Hybrid AES_RSA Decryption
Logout
Get Started

HYBRID AES_RSA DECRYPTION COMPLETE TO YOUR DIRECTORY

Your File

download here !

RSA Times (sec) :0.927

AES Times (sec) :0.461

Hybrid AES_RSA Times (sec) :1.388

Complete Process

Hash Key Value :

���]�, 6yh��`��;V�H �>T

Figure 4.15 Complete process

4.4 Experimental Result

In this proposed system, compare the AES, RSA and hybrid AES_RSA decryption time is made for the experimental analysis. Various length of key size such as 128 bit, 192 bit and 256 bit are applied in AES encryption. The experimental result for 128 bit is shown in figure 4.16, figure 4.17 and figure 4.18 respectively. There are five sample data files are experimented for this proposed system. Based on the results, the RSA algorithm, the AES algorithm and the hybrid algorithm are compared and the variations in decryption time are evaluated.

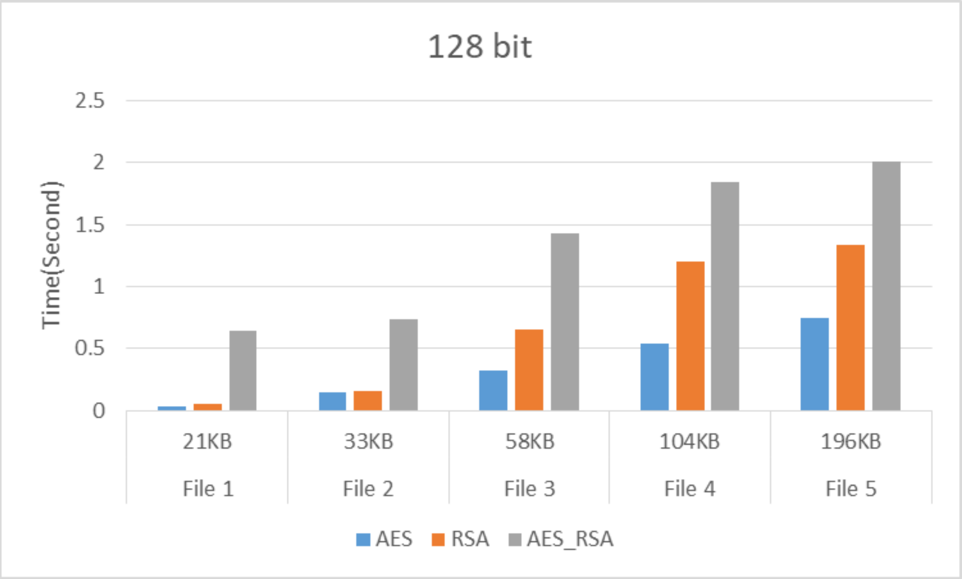


Figure 4.16 Experimental result for 128 bit

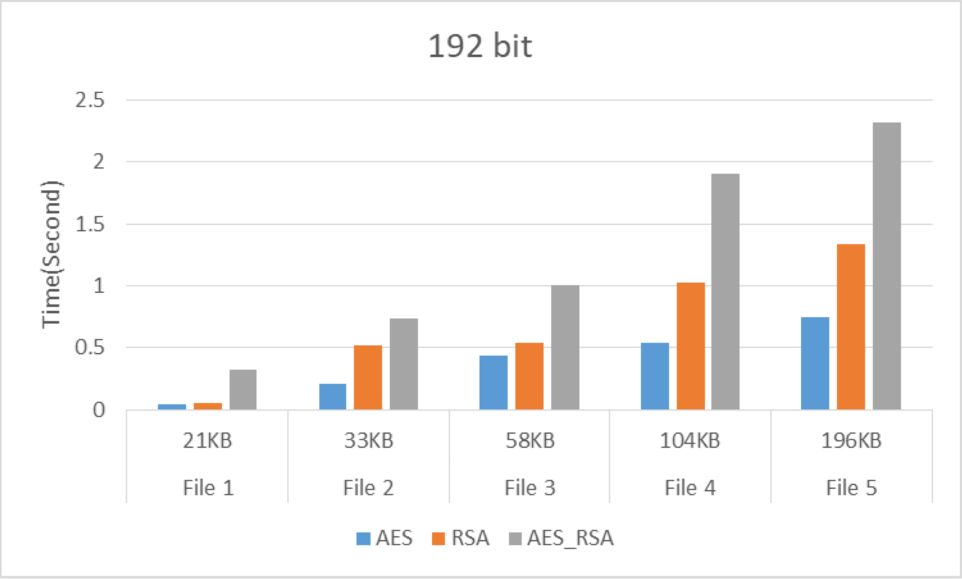


Figure 4.17 Experimental result for 192 bit

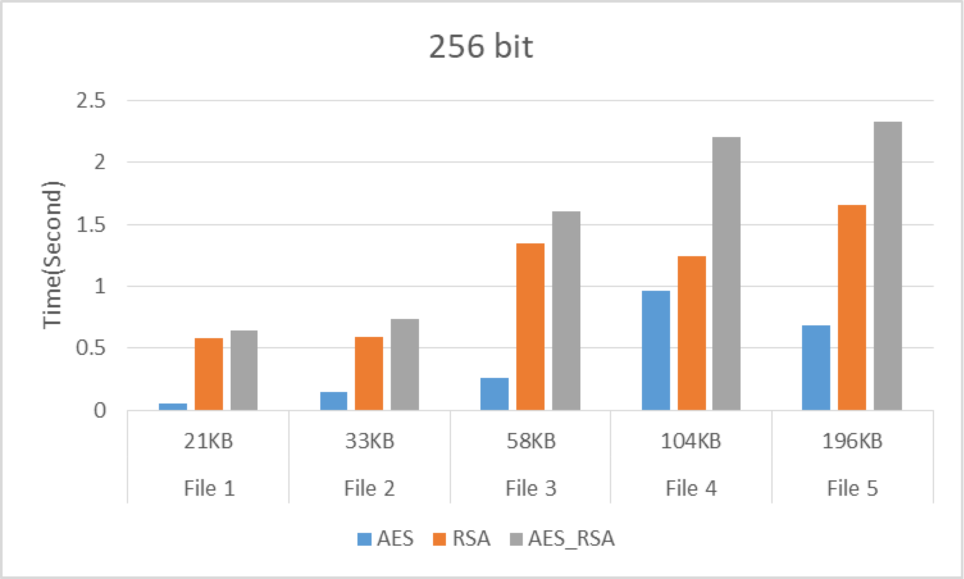


Figure 4.18 Experimental result for 256 bit

Therefore, it can be easily understood that time requirement for encryption of Hybrid AES-RSA is greater than that of the time requirement of individual AES and RSA. The time which we get during the experimental result may vary for same input because it depends upon the processor and memory available during the execution of the program.

CHAPTER 5

CONCLUSION AND FURTHER EXTENSION

In this proposed system, there are three types of encryption have been cooperated in order to utilize the advantages of each one to build a high security system. Cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during transmission. The purpose of creating this hybrid algorithm is to provide better security. The hybrid algorithm provides more security than individual algorithm for the plaintext. By using this hybrid cryptosystem authenticity can be achieved.

5.1 Advantages and Limitations of the System

This system provides safe mechanism for data transmission over the network. This mechanism provides dual protection by taking the advantages of the algorithms used, so the data transmission in the network will be more secured. The proposed system can be applied to other educational organization not only to University infrastructure but also Basic Education High School (BEHS). This system can be applied to any organization that require critical information security. In this analysis, however, there are still some shortcomings, such as the inability to avoid replay attacks in the file encryption process, and data tampering and forgery when the double key is cracked, which will be more refined in future testing.

5.2 Further Extension

After completion of current system, there are many features that can be added to the system to increase the system’s recovery and reliability. Another idea for further work is to implement the secure offline implementation data transmission system for more efficiency. In the future work, adding security is required for this system to prevent many attack.

REFERENCES

[1] Abhishek Guru and Asha Ambhaikar, “AES and RSA based Hybrid Encryption Algorithm for Message Encryption and Decryption”, IT in Industry, March,2021.

[2] B.Rana, S. Wankhade, “Hybrid Cryptographic Algorithm for Enhancing Security of Text”, International Conference on Emanations in Modern Technology and Engineering, 2017.

[3] Cryptography and Network Security (Principles and Practice) Third Edition.

[4] E. S. Ibrahim Harba, “Secure Data Encryption Through a Combination of AES, RSA and HMAC”, Engineering, Technology & Applied Science Research, 2017.

[5] G.V.S Pavan Mallik1, Y Saranya Bala2, “ Securing Email using Hybrid Encryption System”, International Research Journal of Engineering and Technology (IRJET), July 2020.

[6] P. Prajapati, N. Patel, R. Macwan, N. Kachhiya, P. Shah, “Comparative Analysis of DES, AES, RSA Encryption Algorithms”, International Journal of Engineering and Management Research, Vol. 4, No. 1, pp. 292-294, 2014.

[7] Salini Dev P V, A.P. Jose, J.Joseph, “Hybrid Encryption Algorithm for Data Transmission over public network”, IJARIIE-ISSN(O)-2395-4396, 2017

[8] S. Kuswaha, P.B. Choudhary, “Data Transmission using AES-RSA Based Hybrid Security Algorithms”, International Journal on Recent and Innovation Trends in Computing and Communication, Apirl, 2015.

[9] T.Monoth and N. Francis, “An Analysis of Hybrid Cryptographic Approaches for Information Security”, International Journal of Applied Engineering Research, 2018

[10] https://www.techtarget.com/searchsecurity/definition/cryptography.

[11] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[12] https://www.techtarget.com/searchsecurity/definition/RSA

[13] https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

PUBLICATION

[1] K.H.Wai and M.T.Zar, “Securing Critical Data Using Hybrid Cryptosystem”, Local Conference on Parallel and Soft Computing, June 2022.