

**A DOUBLE KEY-BASED PUBLIC-PRIVATE KEY ENCRYPTION-DECRYPTION
PROCESS FOR SECURED MESSAGE TRANSACTION**

BY

**MUHAMMAD RASHIDUZZAMAN
ID: 183-25-717**

This Report Presented in Partial Fulfillment of the Requirements for the Degree
of Master of Science in Computer Science and Engineering

Supervised By

Dr. Md. Ismail Jabiullah

Professor

Department of Computer Science and Engineering
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2019

APPROVAL

This Thesis titled “**A Double Key-based Public-Private Key Encryption-Decryption Process for Secured Message Transaction**”, submitted by Muhammad Rashiduzzaman, ID No: 183-25-717 to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 6th December 2019.

BOARD OF EXAMINERS



Dr. Syed Akhter Hossain
Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Dr. Md. Ismail Jabiullah
Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

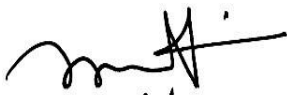
Internal Examiner



Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Mohammad Shorif Uddin
Professor

Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

DECLARATION

I hereby declare that, this thesis has been done by me under the supervision of **Dr. Md. Ismail Jabiullah, Professor, Department of CSE** Daffodil International University. I also declare that neither this thesis nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Dr. Md. Ismail Jabiullah

Professor

Department of Computer Science and Engineering
Daffodil International University

Submitted by:



Muhammad Rashiduzzaman

ID: 183-25-717

Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

First, I express my heartiest thanks and gratefulness to almighty Allah (God) for His divine blessing makes me possible to complete the M.Sc. thesis successfully.

I really grateful and wish my profound my indebtedness to **Dr. Md. Ismail Jabiullah, Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of “*Cryptography and Information Security*” to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this thesis.

I would like to express my heartiest gratitude to **Dr. Syed Akhter Hossain, Professor and Head**, Department of CSE, for his kind help to finish my thesis and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

ABSTRACT

In modern communication age, security of electronic message transaction is the demand of time. It is most essential in various aspects. Currently a large amount of sensitive data is transmitted over the open network or internet or other communication channels on a daily basis. Without strong security, we cannot protect these sensitive information from malicious attacks. Currently, it is main concern to impose additional security services to the communicating message, communication channel and communicating participants. For this, a better approach for electronic message transaction system has been developed using Python programming language. It performs electronic message transactions with all the fundamental security requirements, which are confidentiality, integrity, authentication and non-repudiation for both communicating message and communicating participants. To do this, simple cryptographic encryption and decryption techniques are used to the communicating messages. At first message is encrypts with the private key of sender PR_a and the output is again encrypts with a shared secret key K_1 that generates ciphertext, which is again encrypts with another shared secret key K_2 that generates a code that serves as message authenticator known as MAC, which is concatenates with the ciphertext and again encrypts them with shared secret key K_1 that builds the new ciphertext, which is again encrypts with the receiver's public key PU_b to produce final ciphertext that is to be send to the intendent recipient. In the receiving end, to retrieve the message, receiver at first decrypts the received information with his private key PR_b and again decrypts with the shared secret key K_1 that gives the ciphertext and MAC of the ciphertext, and then only decrypts the MAC to generate a new ciphertext' and compare the new ciphertext' with the received ciphertext that ensures the ciphertext authentication as well as message authentication; if ciphertexts are found same, then decrypts the ciphertext with shared secret key K_1 and again decrypts with the sender public key PU_a and retrieve the message; otherwise discard it. This technique can be applied anywhere of electronic communications in a secure fashion.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
List of Figures	viii
List of Tables	ix
CHAPTER	
CHAPTER 1: INTRODUCTION	1-3
1.1 Introduction	1
1.2 Motivation	1
1.3 Rationale of the Study	2
1.4 Research Questions	3
1.5 Expected Output	3
1.6 Report Layout	
CHAPTER 2: BACKGROUND	4-17
2.1 Introduction	4
2.2 Cryptographic Terms	4
2.3 Secured Message Transaction Model	8
2.4 Security Services	9

2.5 Secret Key Generation	11
2.6 Random Number Generation	11
2.7 Secret Key Cryptography	12
2.8 Conventional Approaches	12
2.8.1 Conventional Message Authentication	13
2.8.2 Conventional Message Confidentiality Checking	15
2.8.3 Conventional Message Authentication and Confidentiality Checking	15
2.8.4 Identified Limitations of the Conventional System	16
2.9 Summary	17
CHAPTER 3: RESEARCH METHODOLOGY	18-26
3.1 Introduction	18
3.2 Process Description of the Proposed System	18
3.3 Encryption-Decryption Process and Diagrams of the Proposed System	18
3.4 Algorithms of the Proposed System	20
3.5 Step-by-Step Flow Diagram of the Proposed System	21
3.6 Summary	26
CHAPTER 4: EXPERIMENTAL RESULTS AND DISSCUSSION	27-32
4.1 Introduction	27
4.2 Experimental Results	27
4.3 Descriptive Analysis	31
4.4 Summary	32

CHAPTER 5: SUMMARY AND CONCLUSION	33-34
5.1 Summary of the Study	33
5.2 Conclusions	33
5.3 Recommendations	34
5.4 Implication for Further Study	34
REFERENCES	35-36

LIST OF FIGURES

FIGURES	PAGE NO
Figure 2.1: A Cryptographic System	6
Figure 2.2: A Public Key Cryptography	7
Figure 2.3: A Private Key Cryptography	8
Figure 2.4: Simplified Model of Conventional Encryption	9
Figure 2.5: Secret Key Cryptography	12
Figure 2.6: Secured Message Transmission with Message Authentication	14
Figure 2.7: Message Authentication and Confidentiality; Authentication Tied to Ciphertext	16
Figure 3.1: Encryption Process of the Proposed System	19
Figure 3.2: Decryption Process of the Proposed System	19
Figure 3.3: Encryption of Intelligible Message with Sender's Private Key	21
Figure 3.4.: Encryption of Encrypted Message with Shared Secret Key K_1	22
Figure 3.5: Generation of MAC	22
Figure 3.6: Concatenation of Ciphertext and MAC	22
Figure 3.7: Encryption of Concatenated Ciphertext and MAC	23
Figure 3.8: Final Ciphertext	23
Figure 3.9: Decryption of Received Information with Receiver's Private Key	24
Figure 3.10: Retrieval of Concatenated Cipherext and MAC	24
Figure 3.11: Generation of new Ciphertext and Compression with Received Ciphertext	25
Figure 3.12: Decryption of Ciphertext with Shared Secret Key K_1	25
Figure 3.13: Retrieval of Message with Sender's Public Key PU_a	25
Figure 4.1: RSA Public-Private Key Generation for Sender	27
Figure 4.2: Encryption Process in the Sender End	28
Figure 4.3: RSA Public-Private Key Pair Generation for Receiver	29
Figure 4.4: Decryption Process in the Receiving End	30

LIST OF TABLES

TABLES	PAGE NO
Table 4.1: Comparative Security Services between two Conventional Systems and Proposed System	31

CHAPTER 1

Introduction

1.1 Introduction

Security of the message transaction over the open network is the vital issue in the electronic communication age. Messages are communicating over the open network environment is now in vulnerable situation. To perform secured message transactions over the unprotected World Wide Web network, there are many mechanisms are available. Currently, it is main concern to impose additional security services to the communicating message, communication channel and communicating participants. The message transmission through the open internet, which is extremely insecure. To perform electronic message transaction, the sender transfers the message to the recipient through a communication channel. The legitimate recipient might not get the genuine information that is sent by the original sender because of unsecured channel [1]. The attacker may modify the original information by malicious activity [1] [3]. For secured electronic message transaction, cryptographic techniques are used; which provide feature of encryption to transform the intelligible message into an unintelligible form that is sent to the intended recipient through the insecure communication channel. In the receiving end, the received unintelligible information turning it back into intelligible message by the related cryptographic techniques and keys.

Our main concern in this thesis is to impose additional security services to ensure electronic message transaction through the insecure channel in a secure fashion.

1.2 Motivation

In modern communication age, security of electronic message transaction is the demand of time. It is most essential in various aspects. Currently a large amount of sensitive data is transmitted over the open network or internet or other communication channels on a daily basis [17]. Without strong security, we cannot protect these sensitive information from malicious attacks. Secured electronic message transaction is mandatory part of E-commerce. Opportunities of the customer, merchant, bank, credit card or debit card cannot be properly served without strong security services.

Cryptographic techniques are used to ensure the security of electronic message transactions; which provides the feature of encryption, that transform the intelligible message into an unintelligible form with cryptographic keys, that is sent to the intended recipient through the insecure communication channel such as open network or internet.

Messages are communicating over the open network environment is now in vulnerable situation. To perform secured message transactions over the unprotected World Wide Web network, there are many mechanisms are available. Currently, it is main concern to impose additional security services to the communicating message, communication channel and communicating participants. In this thesis, our prime concern is to develop an electronic transaction system that ensure the secured message transactions with confidentiality, integrity, authentication and digital signature. This is most demandable for present Electronic Commerce (E-commerce), Electronic Banking (E-banking), Electronic Governance (E-governance), Telemedicine and so on.

1.3 Rationale of the Study

In electronic communication age security is the prime consideration in various aspects. The electronic communication channel is vulnerable to the message transactions. The security of the message transaction is very much demandable to overcome the existing problem. Cryptographic techniques are used to ensure the security of electronic message transactions. To do this, cryptographic ingredients, cryptographic dimensions, cryptographic mechanisms, and other related cryptographic terms will be studied, analyzed and realized. Conventional secured message transaction system will be studied and provided security services will be identified and realized. The aim of this thesis is to propose a better approach for secured message transactions with better security services than the conventional systems by using cryptographic encryption and decryption processes with keys.

1.4 Research Questions

Q.1: How to transmit electronic message over the open network without allowing access to an attacker?

Q.2: What is the procedure of the system?

Q.3: How perform encryption-decryption?

Q.4: How to implement the system?

1.5 Expected Output

In this thesis, we will try to impose additional security to the communicating electronic message through cryptographic public-private key encryption-decryption process.

Our main aim of this thesis is to ensure transmission of electronic message over the open network without allowing access to an attacker.

1.6 Report Layout

This thesis report composed with five chapters. The first chapter is the Introduction, in which discussed about the motivation and rationale of the study. This chapter also includes research questions, expected output and report layout in the end.

The Chapter 2 is Background, which highlights the cryptographic background and conventional systems. This chapter consists of nine sections and they are introduction, cryptographic terms, secure message transaction model, security services, secret key generation, random number generation, secret key cryptography, conventional approaches and summary.

The Chapter 3 is Research Methodology, in which illustrates the details of this research. This chapter composed with six sections and they are introduction, process description of the proposed system, encryption-decryption process and diagrams of the proposed system, algorithms of the proposed system, step-by-step flow diagram of the proposed system and summary.

The Chapter 4 is Experimental Results and Discussion, this chapter highlights the experimental results and system security. There are four sections in this chapter, which are introduction, experimental results, descriptive analysis, and summary.

The final one is Chapter 5, which consists of four sections and they are summary of the study, conclusions, recommendations and implication for further study.

CHAPTER 2

Background

2.1 Introduction

Cryptography is associated with the process of safeguarding information and communications by encryption and decryption with key(s) so that only the authorized users can read and process it [5]. Modern cryptography based on complex mathematical calculations and a set of rules which are called procedures or algorithms to transform messages that are difficult to understand [14].

2.2 Cryptographic Terms

Now a day's modern cryptography uses various cryptographic terms. Some of the following cryptographic terms are used in this project; Plaintext or Intelligible Message, Encryption Algorithm, Encryption Key, Cipher text, Decryption Algorithm, Decryption Key, Cipher, Key, Public Key, Private Key, Encryption, Deciphering, Decryption, Cryptography, Cryptanalysis, Cryptology, Code, Steganography, Digraphs, Homophones, Mono Alphabetic Substitution, Poly Alphabetic Substitution, Nomenclature, Nulls, Public-key cryptography, Private-key or Symmetric-key cryptography, Substitution, Transposition, Hashing, Authentication, Digital signature. Short description of the above cryptographic terms are as follows:

Plaintext or Clear text: The original message or data that can be directly understand by human or machine. Plaintext or Clear text is used as input to the encryption algorithm and it can be in form of text, audio, video, image and biometrics also.

Encryption Algorithm: It is a complex mathematical process that takes intelligible message and an Encryption key as input and gives Cipher text as output.

Key for Encryption: The key fed in to the encryption algorithm along with the Plaintext in order to determine the Cipher text.

Cipher text: The transformed message or data that cannot directly understand by human or machine. It is the incomprehensible output of the encryption algorithms.

Decryption Algorithm: It is a complex mathematical process that takes Cipher text and a decryption key as input and gives Plaintext as output.

Key for Decryption: The key fed in to the decryption algorithm along with the Cipher text in order to determine the Plaintext.

Cipher: A Cipher is a method responsible for converting Plaintext into Cipher text and reverting Cipher text to Plaintext.

Key: A Key is a value or some critical information that is fed in to the algorithm to transforming Clear text into Cipher text and reverting Clear text from Cipher text. The Key is known only to the sender or receiver or both depends on the types of key used.

Public Key: A Public Key, which may be known to anyone and can be used for encryption.

Private Key: A Private Key, which is only known to the owner and can be used for decryption.

Encryption: Encryption is a technique of converting Plaintext into Cipher text and that is unreadable to humans and machine without knowing the algorithm and decryption key.

Deciphering: The procedure of turning Cipher text to Plaintext with prior knowledge of the algorithms or keys used. This is done by the receiver.

Decryption: Decryption is the technique of turning Cipher text to Plaintext without knowing the algorithm or keys used. This is done by the interceptor or 'cracker'.

Cryptography: Cryptography is the study of principles and techniques of converting Intelligible Message into Unintelligible form that is unreadable to humans and machine; and then recovering that Plaintext from Cipher text that is its original form. Figure 2.1. Shows Cryptographic System:

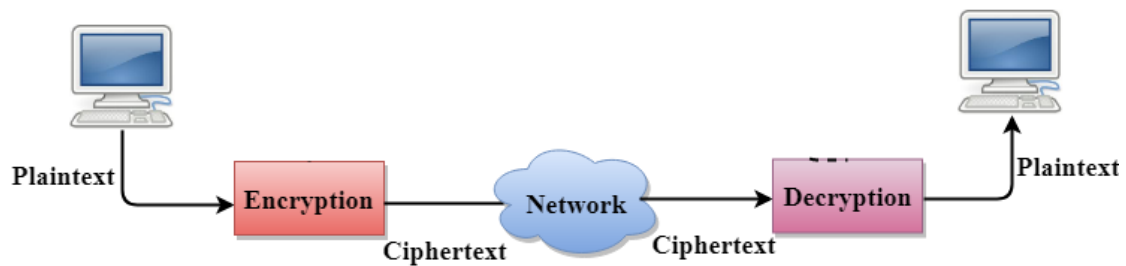


Figure 2.1: A Cryptographic System

Cryptanalysis: Cryptanalysis is the study of the principles and techniques of recovering Plaintext from Cipher text without knowing the algorithm or keys used.

Cryptology: The study of both Cryptography (Enciphering and Deciphering) and Cryptanalysis (Codebreaking or Cracking a cipher system or individual Cipher text).

Code: It is a process for transforming an unreadable information into a readable one using a code-book.

Steganography: It is the process of concealing a file, message, image or video within another file, message, image or video.

Digraphs: A Plaintext character coupling process that stops frequency predict of frequently occurring pairs like 'qu'.

Homophones: Some substitutional letters for the duplicate letter in Plaintext.

Substitution: Enciphering by change one character by another.

Mono Alphabetic Substitution: A Mono Alphabetic Substitution is a cipher where each event of a Plaintext character is replaced by a corresponding Cipher text character to generate Cipher text.

Poly Alphabetic Substitution: A Poly Alphabetic Substitution is a cipher where several Plaintext character is replaced by the corresponding Cipher text character to generate Cipher text.

Transposition: Enciphering by arranged letters in a different order.

Public Key Cryptography: It is also known as asymmetric key cryptography is a cryptographic system that uses two keys. The keys are mathematically linked, but not same, a public key which may be known by anyone where the private key is only known to the recipient. The public key is used for encryption where private key is for decryption. Figure 2.2. Shows Public Key Cryptography System:

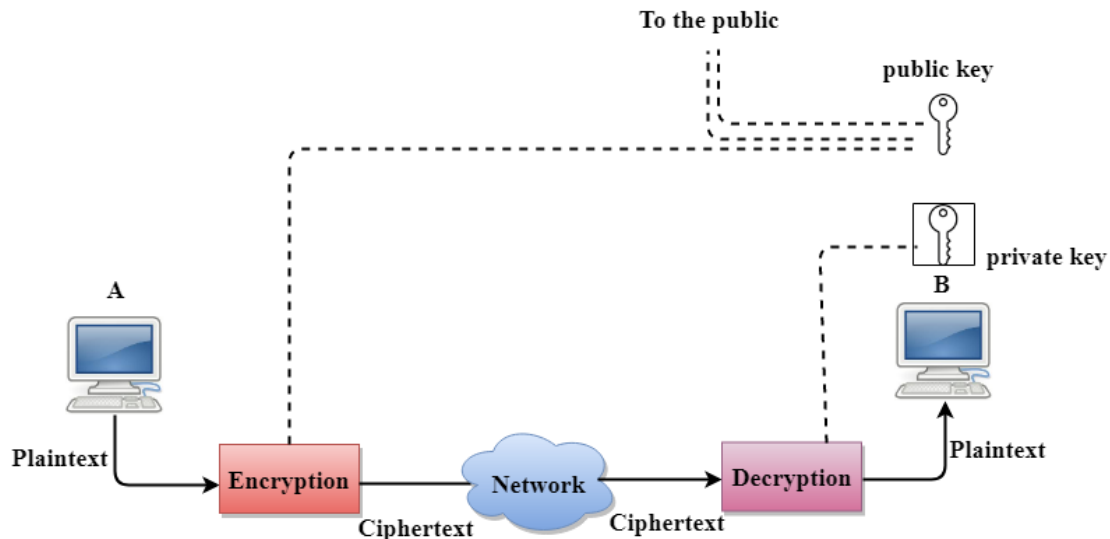


Figure 2.2: A Public Key Cryptography

Private Key Cryptography: A Private-key cryptography or Single-key cryptography also known as Symmetric-key cryptography uses one key shared by both sender and receiver. This common key is used for both encryption of the Plaintext and decryption of the Cipher text. Figure 2.3 Shows Private Key Cryptography System:

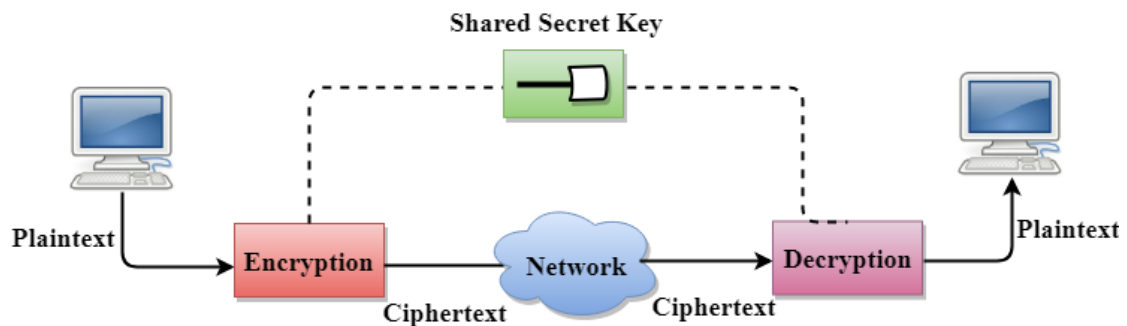


Figure 2.3: A Private Key Cryptography

Nomenclature: Combining code and cipher elements. The word ‘nomenclature’ sometimes used for a system that combines code elements and cipher.

Nulls: Dummy characters used to complicate by changing frequency distributions or predictability. Often used as padding to fill exact length of a message.

2.3 Secure Message Transaction Model

Security model of a message transaction using symmetric encryption. A symmetric encryption system has five components. Shows in Figure 2.3.1:

- **Plaintext:** The original information or data that can be directly understand by humans or machine. Plaintext or Clear text, which is used as input to the encryption algorithm and it can be in form of text, audio, video, image and biometrics also.
- **Encryption algorithm:** It is a complex mathematical procedure that takes intelligible message and an Encryption key as input and produces unintelligible message as output.
- **Secret Key:** A Key is a value or some critical information that is fed in to the algorithm to transforming Intelligible Message into Cipher text and reverting Cipher text to Intelligible Message. The Key is only known to the communicating parties.

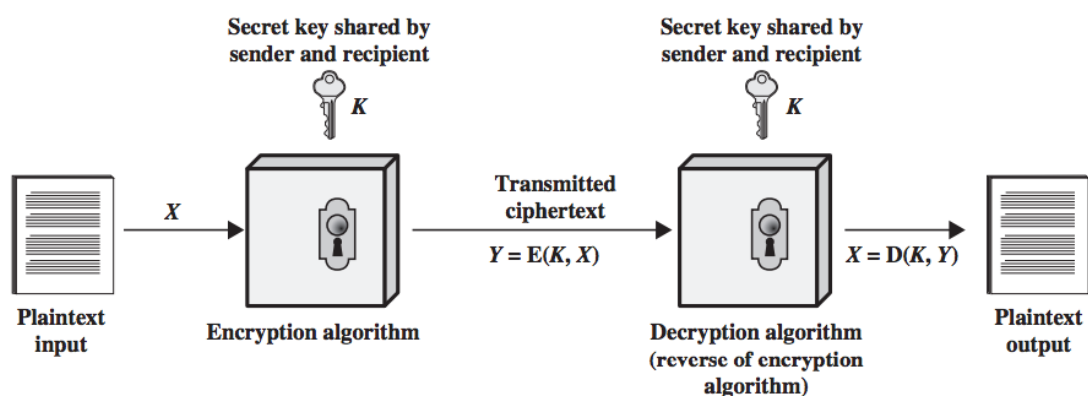


Figure 2.4: Simplified Model of Conventional Encryption

- **Cipher text:** The transformed information that cannot directly understand by human or machine without knowing the algorithm or secret key used. It is the incomprehensible output of the encryption algorithms.
- **Decryption algorithm:** It is basically the encryption process execute in reverse. It takes unintelligible Message and same secret key as input and provides initial intelligible Message as output.

There are two compulsory requirements for secure use of symmetric encryption:

1. First we require a strong encryption algorithm. At least, we would choose the algorithm to be such that an attacker should not be capable to decipher the unintelligible information or find out the key; even if attacker knows the algorithm and obtain one or more cipher text.
2. The sender and the receiver must have acquired the copies of secret key in a secure fashion and key must be kept secret. If this key is disclosed, communications are compromised.

2.4 Security Services

It ensures sufficient security for the systems and also for data transmissions [19]. This system provide a processing or communication service to ensure specific type of safeguard to resources. Security services usually development part of security policies and they are implemented through security mechanisms.

Security services are divided into five categories:

Confidentiality:

Confidentiality is the fundamental requirement for message or information security. Confidentiality means safeguard private information or data from unauthorized access, use, disclosure and modification it; to any unwanted users, systems or other entities. An organization or a person required to protection against malicious actions that is threat for the message or information confidentiality. In information age communication security of sensitive information is the major issue. For example, if your bank accounts information are posted on a public website, everybody can know your account number,

balance and other sensitive information. Those information cannot be removed from their minds, computers, papers and other places. Nearly all the crucial security occurrences reported in the media today include huge lack of confidentiality. Confidentiality not only used for message or information storage but also apply for message or information transmission technique [10].

Integrity:

Data integrity refers to the fact that data must be authentic and genuine; means that when a sender sends data, the receiver must receive exactly the same data as send by an authorized sender. Data must not be contain modification, insertion, deletion or no reply over its entire lifecycle [11].

Authentication:

The authentication technique guarantee that communication between a sender and receiver is genuine or authentic. Authentication service can be divided into two categories: (a) Peer entity authentication; which is used for identity confirmation of an association of peer entities. (b) Data source authentication; which ensure the origin of data. I does not serves as safeguard against the modification or duplication of data [11].

Non-repudiation:

Non-repudiation refers to the capability to ensure that a party to a communication or contract cannot successfully deny the authenticity of their signature on a document or the sending of a message that they originated. Digital signatures provide non-repudiation service.

Availability:

The characteristics of a system or a system resources or information being reachable and usable by permitted users when needed and also ensure that those system or system resources or information is unavailable for unauthorized users.

2.5 Secret Key Generation

The key generation technique is the procedure of creating key in cryptography. A key is used by the sender to encrypt data and by the receiver to decrypt data. A device or program which is used to create keys is called key generator. Present cryptographic systems involve symmetric-key algorithms like AES and DES and public-key algorithms like RSA. Symmetric-key algorithms use a secret single key shared only between communicating parties for keeping data secure. Public-key algorithms uses two keys one public-key and one private-key. The public-key may be known by anybody and private key is kept secret [1] [3].

In computer cryptography uses integers for generate keys. Sometimes keys are generated randomly using a random number generator (RNG) or pseudorandom number generator (PRNG).

The easiest process to read unintelligible encrypted message or information without actually decrypting it is called brute force attack; simply trying each number, up to the maximum size of the key. So, it is essential to use a sufficiently large key size; larger keys take exponentially longer to attack, rendering a brute force attack is not practical. Present-days, the symmetric key algorithms are commonly uses 128 bits long key and public-key algorithms uses the key lengths of 2048 bits.

2.6 Random Number Generation

A random number generator (RNG) is a system or program that produces a series of numbers or symbols that cannot be appropriately predicted than by a random chance. It can be a real hardware random-number generators (HRNG), which produce originally random numbers, or pseudo-random number generators (PRNG), which produce numbers that look random, but numbers are actually deterministic, and can be regenerated if the state of the pseudo-random number generator is known.

Several computational techniques for generation of pseudo-random number exist but they are not suitable for applications such as cryptography. Although, carefully developed cryptographically secure pseudo-random number generators (CSPRNG) also exist, with important characteristics particularly designed for use in cryptography.

2.7 Secret Key Cryptography

With Secret key cryptography, which is also known as private-key cryptography or symmetric key cryptography, both communicating parties, sender and receiver, uses the same shared secret key for encryption and decryption as shown in Figure 2.5:

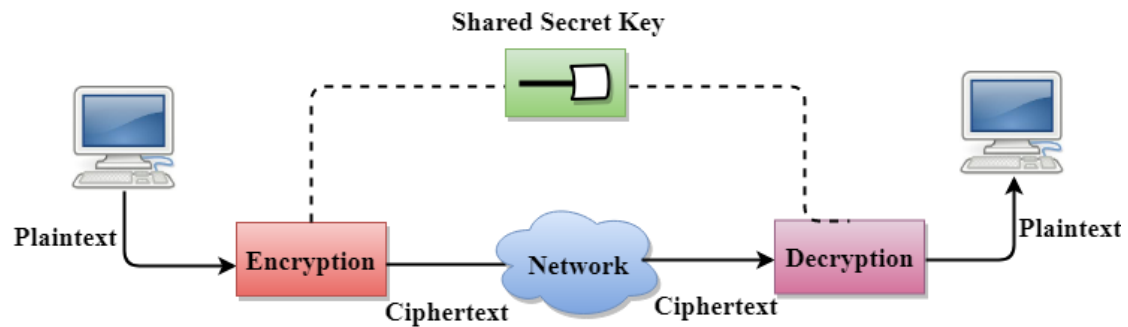


Figure 2.5: Secret Key Cryptography

Before any unintelligible encrypted information can be sent over the open network, both sender and receiver must have the key and agree on the cryptographic algorithm that they will need for encryption and decryption.

The biggest problem with private key cryptography is key distribution; how to receive the key from one party to the other without permitting access to an attacker. When the secret key distribution problem is solve, it can be a demandable tool. The algorithm ensure stronger security and faster encryption.

2.8 Conventional Approaches

Authentication can be easily ensure by using conventional encryption technique. If the secret key is known only to the sender and the receiver, then the legitimate sender can only allowed to encrypt a message for the receiver. Moreover, if a sequence number and an error-detection code is append to the message, the receiver is sure that no modifications occurred and the received sequence is correct. If the timestamp is append to the message, the receiver is also confirmed about message transmission time; whether the message delayed or take expected time for transit.

2.8.1 Convectional Message Authentication

Message authentication is a method that permits communicating parties to verify the integrity of a message (i.e. message is not modified in transmission) and authenticity of a message (i.e. message came from an authentic sender). Message Authentication normally achieved by using Message authentication codes (MACs). A MAC is cryptographic checksum generated based on a variable-length of message M using a secret key K shared only by sender and receiver. The process using MAC for authenticator is as follows:

$$\text{MAC} = E_k(M)$$

If the sender A wishes to send a message M to the receiver B, and secured it with a MAC, both communicating parties must need to share a secret key K and agree on the MAC algorithm. Then calculates the MAC as a function (agreed algorithm) of message M using shared secret key K. Then the sender A append the MAC with message M and transmitted to the receiver B. The receiver B calculates a new MAC called MAC' by performing the same calculations on the message M and using the same shared secret key K. Then the receiver B, compare the received MAC with new code MAC' to confirm the data integrity. As only communicating parties known the MAC algorithm and secret key; only the sender A is capable to calculate the MAC, hence the source authentication is also confirmed. Message authentication code (MAC) gives a systematic way to message authentication. MAC also divide the authentication from confidentiality. This feature is suitable for various applications where confidentiality is not mandatory. Message Authentication is the vital part of network security. I is a process to confirm that the received message is came from the stated source and message has not been modified. Message Authentication Code achieved by encrypt the message with shared secret key K depicted in Figure 2.6:

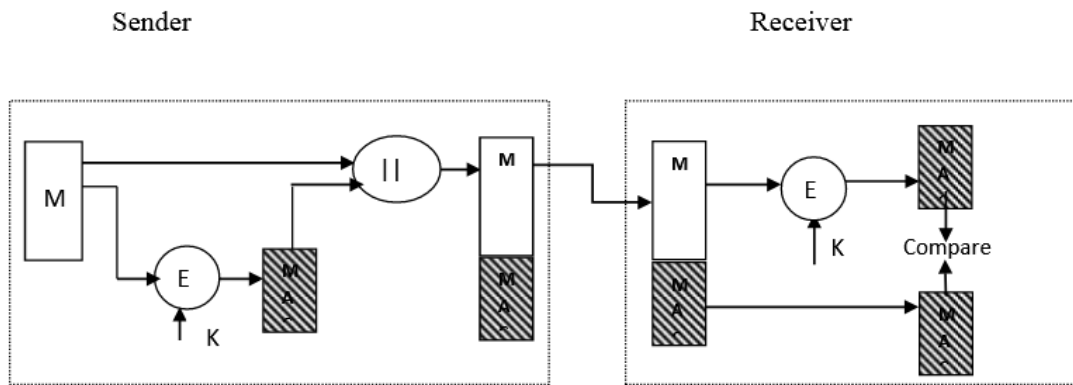


Figure 2.6: Secured Message Transmission with Message Authentication

Here, the sender generated the Message Authentication Code (MAC) by encrypt the message with shared secret key K and concatenated it with the message. Then the sender sent the message and MAC to the receiver. In the receiver end, the receiver again encrypt the message with the same shared secret key K to generate another new MAC which is called MAC' and compare it with the received MAC. If the MAC and MAC' are found same, then the receiver confirm that the received message came from the stated sender and has not been modified. It provide message authentication in a secure fashion. This procedure does not give confidentiality and non-repudiation security services. To ensure these security services, an additional security mechanism is required. If we suppose that the shared secret key K is only known to the sender and the receiver and the received MAC is found same with the new calculated MAC, then:

- a. The receiver is supposed that the message has not been modified. If an attacker modifies the message but doesn't modify the authentication code MAC, then the receiver's generated MAC does not match with the received MAC. Assumed that the attacker is not know the shared secret key. So, the attacker can't modify the MAC to correspond to the modifications in the message.
- b. The receiver is confirmed that the message came from the intended sender. Since only the sender and receiver knows the secret key, no one else could have generated the MAC that was sent by sender without genuine message and secret key.
- c. If the message contains a sequence number, then the receiver can be confirmed of the actual sequence because an attacker can't properly modify the sequence number.

2.8.2 Conventional Message Confidentiality Checking

Confidentiality refers to the process of protecting information or data from access, share and use it by an unauthorized user in the network. Cryptographic techniques allows to achieve confidentiality by using keys for encryption and decryption. Data integrity is the guarantee that the received message or data are totally same as sent by an authorized sender that is contain no modification, insertion, deletion or replay. One can calculate a MAC by applying an algorithm to the message, so that only genuine plaintext accept by MAC. The attackers can alter the message in a way which cannot be accepted by MAC. However encrypting the plaintext and its MAC as a whole seems to be a reliable approach for providing the mentioned security services. Like the MAC, we can encrypt the message with a secret key which produce code. If the attackers modify the message in a way without the key, it is impossible to matches with the encrypted message. To recognize the message authentication code (MAC) generating and verifying techniques several conventional approaches are studied. In this thesis, a better system for electronic message transaction has been developed in Python to provide the better security services of the secure message transaction system. A comparative study has also been performed and presented between the proposed system and conventional system.

In our research, we developed a system that provide two layer confidentiality to the communicating message; where first layer is achieved by encrypts the message with shared secret keys and second layer is achieved by encrypts the final ciphertext with receiver's public key.

2.8.3 Conventional Message Authentication and Confidentiality Checking

Conventional approaches has been reviewed to propose a better new strong message authentication system. This system provides a better strong message authentication and confidentiality checking feature for communicating parties. Here, the system uses two shared secret keys for message authentication and confidentiality checking. First, the intelligible message is encrypts with secret key K_2 , the output is called ciphertext, which is again encrypts with shared secret key K_1 , which generates an authenticator known as MAC that is appended with the ciphertext and sent to the intendent recipient. In the receiver side, the receiver calculate the new message authentication code (MAC') by encrypt the received ciphertext with the shared secret key K_1 . Then the calculated

MAC' is compared with the received MAC. If the MACs are found same, the receiver accept it and decrypt the received ciphertext with shared secret key K2 to get intelligible message; otherwise deny it. Hence the receiver confirmed that the message is not altered and came from the stated source. In this case, the shared secret key K2 is used for encryption and decryption to provide confidentiality of the message and the MAC. This provide a layer two security for the secure message transaction. Another part of the system establishes the message authentication for secured message transaction. Figure 2.7. Shows the message authentication and confidentiality where authentication is tied to ciphertext:

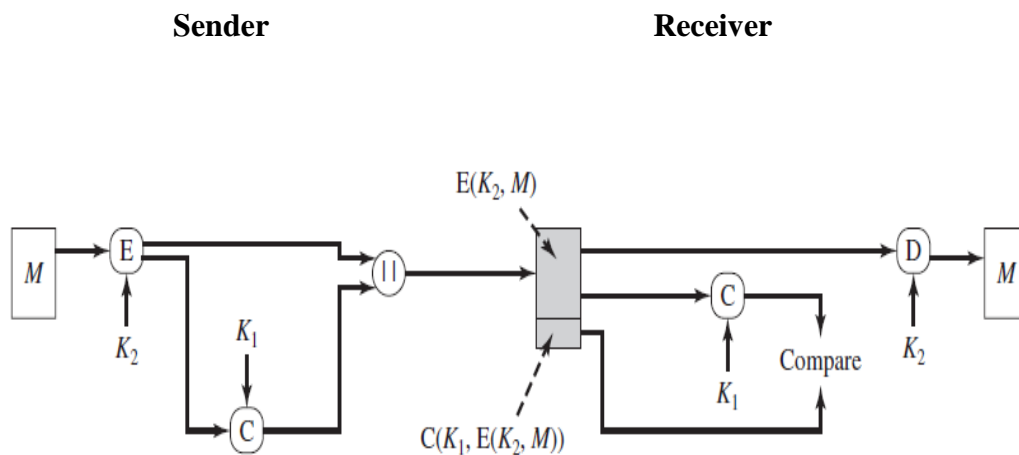


Figure 2.7: Message Authentication and Confidentiality; Authentication Tied to Ciphertext

2.8.4 Identified Limitations of the Conventional System

Conventional system for message authentication and confidentiality has been reviewed to identify its benefits, limitations and applications. After review the conventional systems some limitations are identified, which are summarized below:

- **Encryption-Decryption with a Single Key:** In this procedure, to generate message authentication code (MAC), a shared single secret key is used for encryption in the sender end and the same key is used for decryption in the receiver end. If the shared secret key is disclosed the security of the system may be at risk and communications are

compromised. The system confidentiality totally depends on the key used for encryption-decryption in the security system.

- **Message is not Encrypted with Stronger Way:** The conventional system for message authentication and confidentiality, encrypt the message one time to produce ciphertext and again encrypt to generate the MAC, which is concatenate with the ciphertext and directly send to the sender. If the system generate a new ciphertext after concatenation by encrypt the information with another key and send it to the intended sender, then the system uses two keys for performing two different encryption that provide the strong message authentication and confidentiality.

2.9 Summary

In this chapter, cryptography, cryptographic terms, cryptography component, secure message transmission model, security services and the secret key cryptography are reviewed and presented. And the last section of this chapter, conventional approach of message authentication, message authentication and confidentiality checking for conventional system, and limitations of the conventional system are identified, discussed, analyzed and presented.

CHAPTER 3

Research Methodology

3.1 Introduction

A double key based encryption-decryption process for secured message transaction has been designed, developed, implemented and analyzed.

3.2 Process Description of the Proposed System

In this system, simple cryptographic encryption and decryption techniques are used to the communicating messages. At first message is encrypts with the private key of sender PR_a and the output is again encrypt with a shared secret key K_1 which produces cipherext, that is again encrypts with another shared secret key K_2 that generates a message authenticator known as MAC, which is concatenate with the ciphertext and again encrypts them with shared secret key K_1 that generates the new ciphertext, which is finally encrypts with the receiver's public key PU_b that is to be send to the intendent recipient. In the recipient end, to retrieve the message, at first decrypts the received information with receiver's private key PR_b and, which is again decrypts with shared secret key K_1 that produces the ciphertext and MAC of the ciphertext, and then only decrypts the MAC to produce a new ciphertext' and compare the new ciphertext' with received ciphertext that ensures the ciphertext authentication as well as message authentication; if ciphertexts are found same, then decrypts the ciphertext with shared secret key K_1 and again decrypts with the sender public key PU_a and retrieve the message; otherwise discard it. Here, key values ensure the confidentiality, integrity, authentication and digital signature of the communicating message.

3.3 Encryption-Decryption Process and Diagrams of the proposed System

Encryption Process:

At the sender end, first message is encrypts with the private key of sender PR_a and the output is again encrypts with a shared secret key K_1 which produces cipherext, that is

again encrypts with another shared secret key K_2 that generates a message authenticator known as MAC, which is concatenate with the ciphertext and again encrypts them with shared secret key K_1 that generates the new ciphertext, which is finally encrypts with the receiver's public key PU_b that is to be send to the intendent recipient; as shown in Figure 3.1:

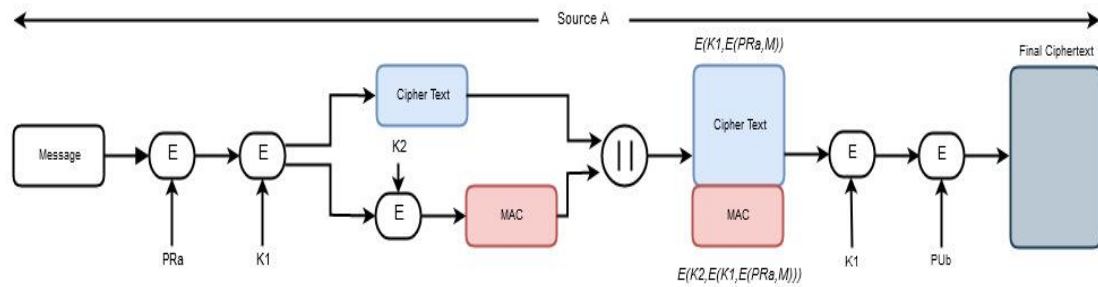


Figure 3.1: Encryption Process of the Proposed System

Decryption Process:

In the receiving end, to retrieve the message, at first decrypts the received information with receiver's private key PR_b and, which is again decrypts with shared secret key K_1 that gives the ciphertext and MAC of the ciphertext, and then only decrypts the MAC to produce a new ciphertext' and compare the new ciphertext' with received ciphertext that ensures the ciphertext authentication as well as message authentication; if ciphertexts are found same, then decrypts the ciphertext with shared secret key K_1 and again decrypts with the sender public key PU_a and retrieve the message; otherwise discard it; as shown in Figure 3.2:

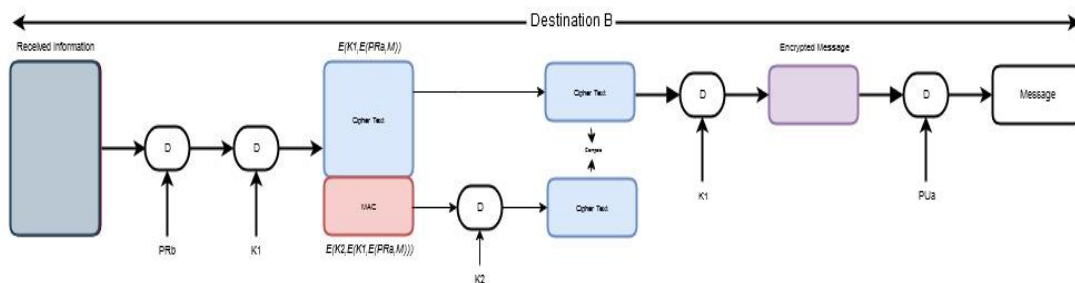


Figure 3.2: Decryption Process of the Proposed System

3.4 Algorithms of the Proposed System

Algorithmic processes of the proposed system for secured message transaction are formulated and demonstrated. The encryption algorithm is performed by the sender and decryption algorithm is performed by the receiver. Description of the encryption and decryption algorithms are given below.

Encryption Algorithm:

The proposed system encryption algorithm consists of the five steps:

- Step 1: Sender encrypts the message with his private key PR_a using RSA algorithm which produce an encrypted output.
- Step 2: Output is again encrypts with shared secret key K_1 which produce a ciphertext.
- Step 3: Ciphertext is again encrypts with another shared secret key K_2 that generates a message authenticator known as MAC.
- Step 4: MAC is concatenates with the ciphertext to compose into a single block.
- Step 5: Again encrypts them with shared secret key K_1 that generates the new ciphertext.
- Step 6: Finally, the new ciphertext is again encrypts with the receiver's public key PU_b that produce the final ciphertext, which is to be send to the intendent recipient.

Decryption Algorithm:

The proposed system decryption algorithm consists of the four steps:

- Step 1: Receiver at first decrypts the received information with his private key PR_a that produce the ciphertext of the concatenated value of ciphertext and MAC.
- Step 2: Which is again decrypts with the shared secret key K_1 that gives ciphertext and MAC of the ciphertext.
- Step 3: Then only decrypts the MAC to produce a new Ciphertext'; and compare it with the received ciphertext that ensures the ciphertext authentication as well as message authentication.
- Step 4: If ciphertexts are found same, then decrypts the cipherext to produce encrypted message; otherwise discard it.
- Step 5: Finally, decrypts the encrypted message with the sender's public key PU_a that establishes the digital signature.

3.5 Step-by-Step Flow Diagram of the Proposed System

Step wise flow diagrams of the proposed system for secured message transaction are demonstrated.

Step wise flow diagrams of the proposed system:

Step 1: Sender encrypts the message with his private key PR_a using RSA algorithm which produce an encrypted output; as shown in Figure: 3.3.

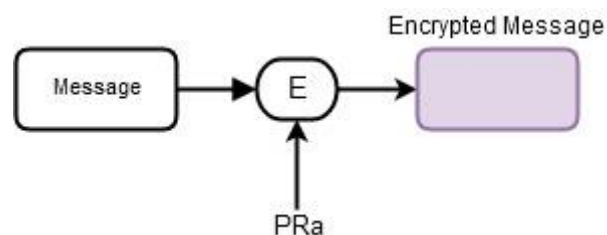


Figure 3.3: Encryption of Intelligible Message with Sender's Private Key

Step 2: Output is again encrypt with shared secret key K_1 which produce a ciphertext; as shown in Figure 3.4.

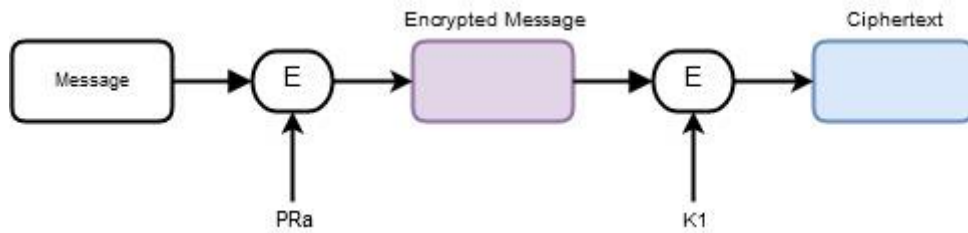


Figure 3.4.: Encryption of Encrypted Message with Shared Secret Key K_1

Step 3: Ciphertext is again encrypts with another shared secret key K_2 that generates a message authenticator known as MAC; as shown in Figure 3.5.

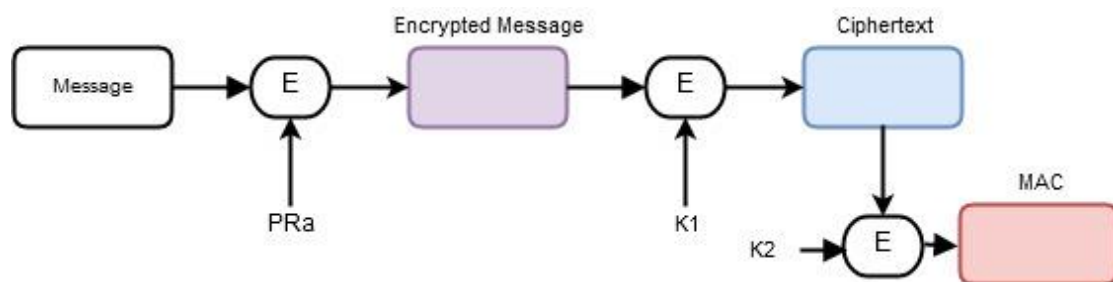


Figure 3.5: Generation of MAC

Step 4: MAC is concatenates with the ciphertext to compose into a single block; as shown in Figure 3.6.

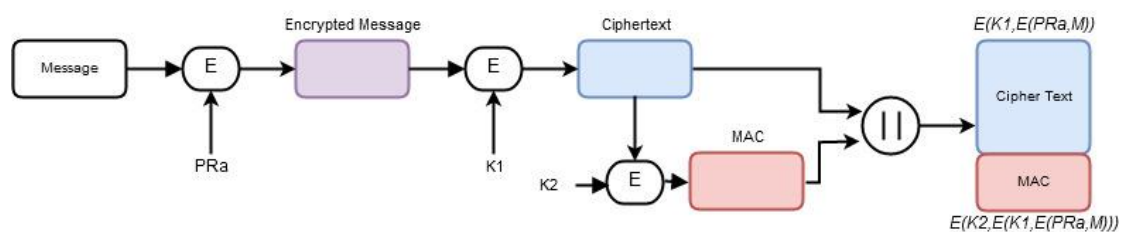


Figure 3.6: Concatenation of Ciphertext and MAC

Step 5: Again encrypts them with shared secret key K_1 that builds the new ciphertext; as shown in Figure 3.7.

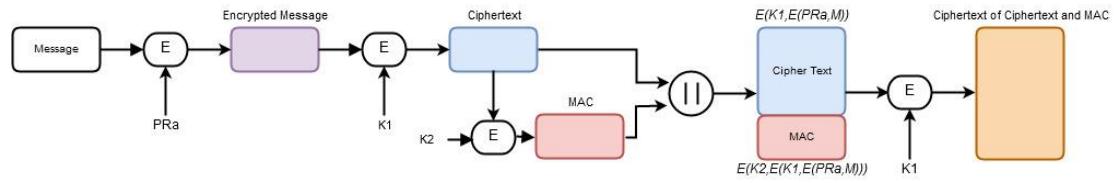


Figure 3.7: Encryption of Concatenated Ciphertext and MAC

Step 6: Finally, encrypts the ciphertext of the concatenated value with the receiver's public key KU_b that produce a final ciphertext that is to be send to the destination; as shown in Figure 3.8.

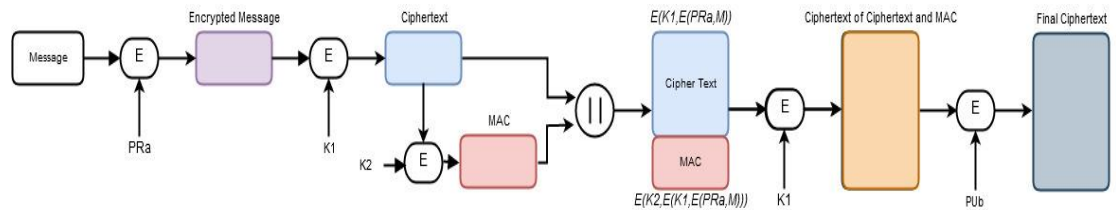


Figure 3.8: Final Ciphertext

Step 7: In the receiving end, receiver at first decrypts the received information with his private key PR_b that produces ciphertext of the concatenated value; as shown in Figure 3.9.

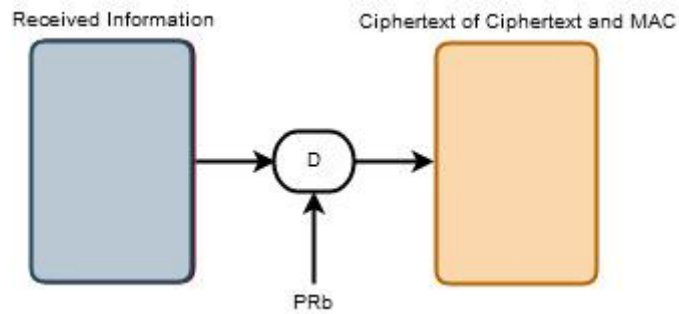


Figure 3.9: Decryption of Received Information with Receiver's Private Key

Step 8: Again decrypts the ciphertext of concatenated value with shared secret key K_1 that gives concatenation of ciphertext and MAC of the ciphertext; as shown in Figure 3.10.

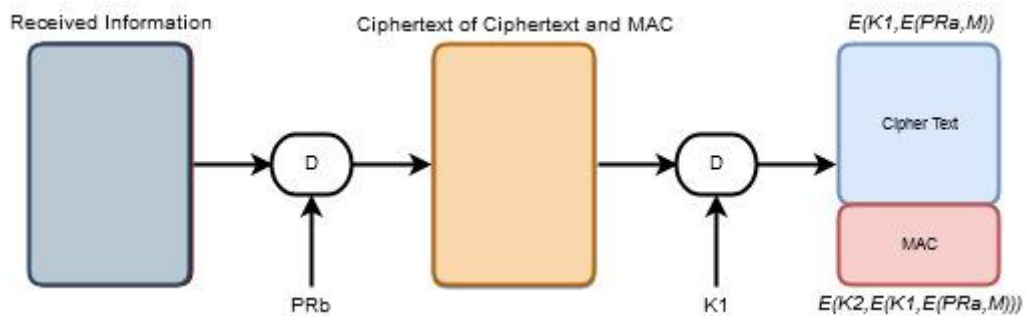


Figure 3.10: Retrieval of Concatenated Ciphertext and MAC

Step 8: Then only decrypts the MAC to produce a new Ciphertext'; and compare it with the received ciphertext that ensures the ciphertext authentication as well as message authentication; as shown in Figure 3.11.

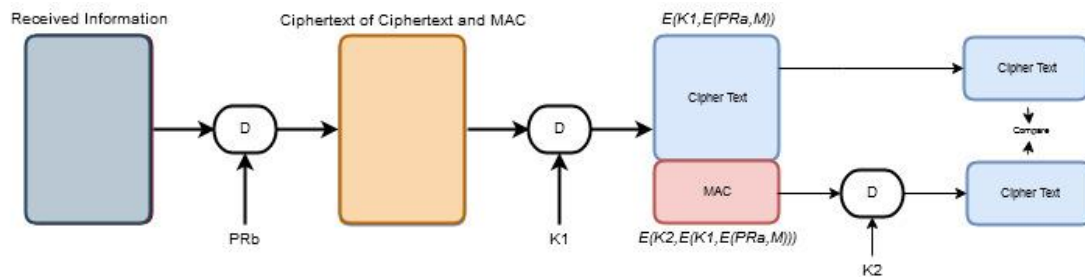


Figure 3.11: Generation of new Ciphertext and Compression with Received Ciphertext

Step 10: If ciphertexts are found same, then decrypts the ciphertext to produce encrypted message; otherwise discard it; as shown in Figure 3.12.

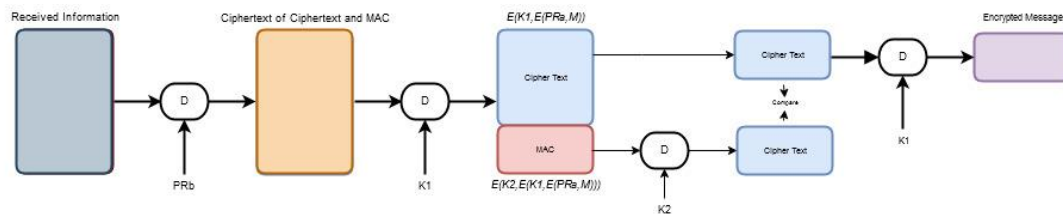


Figure 3.12: Decryption of Ciphertext with Shared Secret Key K_1

Step 11: Finally, decrypts the encrypted message with the sender's PU_a that establishes the digital signature; as shown in Figure 3.13.

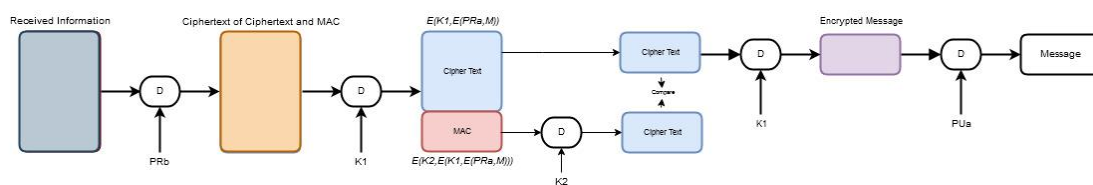


Figure 3.13: Retrieval of Message with Sender's Public Key PU_a

3.6 Summary

In this chapter, an introduction of the proposed system, process description, diagrams, encryption algorithm and decryption algorithm of the proposed system are formulated and demonstrated.

CHAPTER 4

Experimental Results and Discussion

4.1 Introduction

Our proposed system for secured message transaction has been developed using Python programming language Version 3.6. The main aim of our implemented system is to ensure security of the communicating messages. The system is mainly divided into two side one is sender end known as “Encryptor” and another is receiving end, which is known as “Decryptor”. We also developed a key generator for generate RSA public-private key pair. We run the system many times for different messages with different 16 bytes shared secret keys and public-private key pairs. We found the results of the system is good.

4.2 Experimental Results

The experimental input and output results of our developed system are as follows:

In our experiment, the intended message is “Muhammad Rashiduzzaman M.Sc. in CSE, Daffodil International University”, which is to be send to the destination after performing some encryptions. For this, at first sender generate his public-private key pair using RSA algorithm; as shown in Figure 4.1.

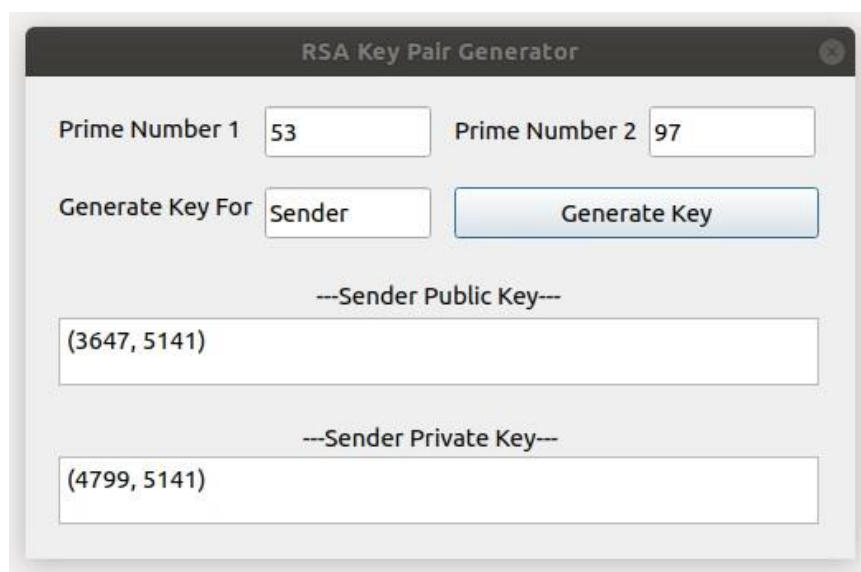


Figure 4.1: RSA Public-Private Key Generation for Sender

The sender publishes his public key (3647, 5141) and keeps a secret private key (4799, 5141). Then he encrypts the intended message with his private key (4799, 5141) and again encrypts with 16 bytes shared secret key K_1 "Diu123@Mij#Sah\$F", which produces ciphertext; as shown in Figure 4.2.

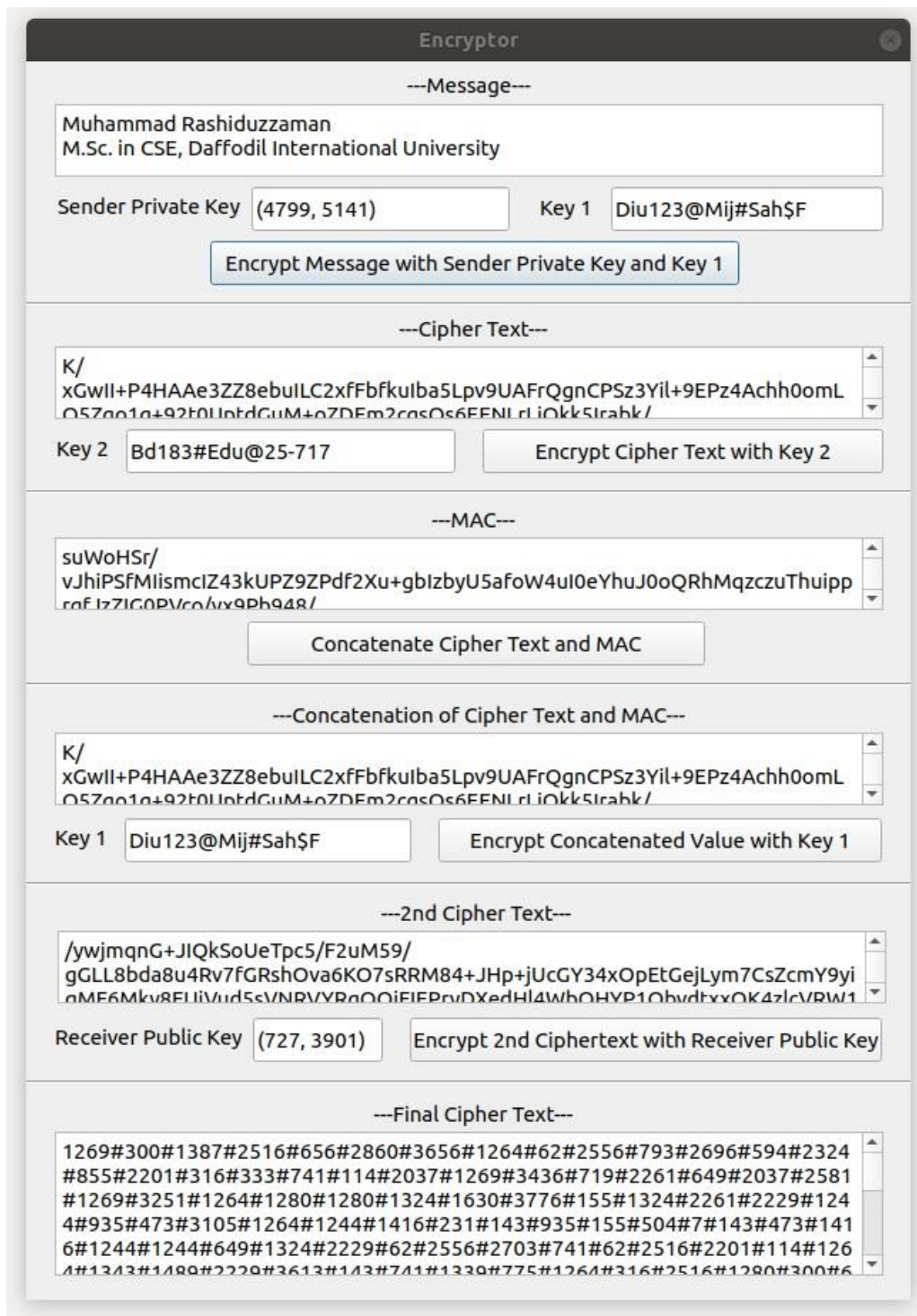


Figure 4.2: Encryption Process in the Sender End

Ciphertext is again encrypts with 16 bytes shared secret key K_2 “Bd183#Edu@25-717” that generates MAC. Then concatenate the ciphertext and MAC. The concatenated value is again encrypts with the 16 byte shared secret key K_1 “Diu123@Mij#Sah\$F”, that builds the 2nd ciphertext, which is again encrypts with the receiver’s public key (727, 3901) that produce the final ciphertext, which is send to the destination.

The receiver generated his public-private key pair using RSA algorithm and published public key (727, 3901) and kept secret private key (1707, 3901); as shown in Figure 4.2.3.



Figure 4.3: RSA Public-Private Key Pair Generation for Receiver

The receiver decrypts the received information with his private key (1707, 3901) that produces 2nd ciphertext, which is again decrypts with the 16 bytes shared secret key K_1 “Diu123@Mij#Sah\$F” that produces concatenation of ciphertext and MAC. Then only decrypts the MAC with 16 bytes shared secret key K_2 “Bd183#Edu@25-717”, which generate the new ciphertext and compared with the received ciphertext; if the ciphertext and decrypted MAC are found same, then decrypts the ciphertext with the 16 bytes shared secret key K_1 “Diu123@Mij#Sah\$F” and again decrypts with the sender’s public key (3647, 5141) that produces the original message “Muhammad ©Daffodil International University

Rashiduzzaman M.Sc. in CSE, Daffodil International University”; the whole decryption process as shown in Figure 4.4.



Figure 4.4: Decryption Process in the Receiving End

4.3 Descriptive Analysis

Some fundamental security services such as confidentiality, integrity, authentication and non-repudiation are the essential ingredients for any secured electronic transaction system. A comparative study between the proposed system and the two conventional systems for secured electronic message transaction has been performed demonstrated, where our proposed system performs all the fundamental security services; as shown in Table 4.1.

Table 4.1: Comparative Security Services between two Conventional Systems and Proposed System

Approaches	Confidentiality	Integrity	Authentication	Non-repudiation
Conventional System 1	Yes	No	No	No
Conventional System 2	Yes	Yes	Yes	No
Proposed System	Yes	Yes	Yes	Yes

The proposed system ensures all the fundamental security services which are analyzed in the following:

- 1. Confidentiality:** The proposed system at first encrypts the information with sender's private key and again encrypts the encrypted information two times with the shared secret keys that establishes first layer confidentiality on the communicating message. Finally, the system encrypts the final ciphertext with receiver's public key, which is must be decrypt with receiver's private key; but only receiver is known his private key that establishes second layer confidentiality of the transaction.
- 2. Integrity:** The system generates a Message Authentication Code (MAC) by encrypts the ciphertext with shared secret key for integrity check of the ciphertext as well as message. Finally the system encrypts the final encrypted information with receiver's public key and send to the destination. Hence, only receiver can decrypts the information, since receiver is only know his private key that establishes first layer integrity. Again the receiver decrypts the received information two times with shared secret keys and compare the ciphertext with generated ciphertext; if the ciphertexts are found same, the receiver accept for

retrieve message; otherwise discard it. Hence, establishes the layer two integrity of the communicating message.

- 3. Authentication:** In the sender end, the system encrypts the message with sender's public key and again encrypts the message two times with shared secret keys and finally encrypts with receiver's public key and send to the destination. The system decrypts the received information in the receiving end. For this, first decrypts the received information with receiver's private key and then decrypts two times with shared secret keys and finally retrieve the message with sender's public key. Hence, the sender and the receiver could not deny the communication due to the received information is at first decrypts with the receiver's private key, which is related with his public key that is used to encrypts the information in the sender side and finally retrieve the message with sender's public key similarly, it is related with sender's private key that is used to encrypts the message. Since, the private key is only known to the owner; hence, it establishes authentication for both the sender and the receiver of the communicating message.
- 4. Non-repudiation** The system encrypts the message with sender's public key and again encrypts the message two times with shared secret keys and finally encrypts with receiver's public key and send to the destination. Hence, the sender and the receiver could not repudiate the communication due to the received information is at first decrypts with the receiver's private key, which is related with his public key that is used to encrypts the information in the sender side and finally retrieve the message with sender's public key similarly, that is related with sender's private key that is used to encrypts the message. Since the private key is only known to the owner and hence, it establishes non-repudiation for both the receiver and the sender of the communicating message.

4.4 Summary

In this chapter, experimental results are analyzed and briefly described input and output results of the developed system. A comparative security analysis between our developed system and conventional systems is also demonstrated, in which our developed system successfully fulfilled the fundamental security requirements.

CHAPTER 5

Summary and Conclusion

5.1 Summary of the Study

Cryptographic ingredients, cryptographic dimensions, cryptographic mechanisms, and other related cryptographic terms are studied, reviewed, analyzed and realized.

An introduction of the conventional approach for message authentication, where message authentication code (MAC) is tied to the ciphertext; has been studied, reviewed and its limitations are identified and discussed.

In our proposed system, we offer a better approach for secured message transactions with better security services than the conventional systems.

An introduction of the proposed system, process description, diagrams, encryption algorithm and decryption algorithm of the proposed system are formulated and demonstrated.

Security mechanisms are required to ensure fundamental security services: Confidentiality, Integrity, Authentication and Non-repudiation of the communicating message and participants. A comparative study between the conventional systems and proposed system has been performed, where the proposed system performs all the mentioned fundamental security services.

5.2 Conclusions

A better approach for electronic message transaction system has been developed using Python programming language. It performs electronic message transactions with all the fundamental security services, which are confidentiality, integrity, authentication and non-repudiation for both communicating message and communicating participants. For this, simple cryptographic encryption and decryption techniques are used to the communicating messages. At first message is encrypted with the private key of sender PR_a and the output is again encrypted with a shared secret key K_1 that generates ciphertext, which is again encrypted with another shared secret key K_2 that generates a code that serves as message authenticator known as MAC, which is concatenate with

the ciphertext and again encrypts them with shared secret key K_1 that builds the new ciphertext, which is again encrypt with the receiver's public key PU_b to produce final ciphertext, which is to be send to the intendent recipient. In the receiving end, to retrieve the message, receiver at first decrypts the received information with his private key PR_b and again decrypts with the shared secret key K_1 that gives the ciphertext and MAC of the ciphertext, and then only decrypts the MAC to generate a new ciphertext' and compare the new ciphertext' with the received ciphertext that ensures the ciphertext authentication as well as message authentication; if ciphertexts are found same, then decrypts the ciphertext with shared secret key K_1 and again decrypts with the sender public key PU_a and retrieve the message; otherwise discard it. This technique can be applied anywhere of electronic communications in a secure fashion.

5.3 Recommendations

In modern electronic communication age, security of the electronic message transactions are the crucial issues and prime concern and it is very demandable. Security of electronic message transactions depends on the key values of the cryptosystem and various cryptographic techniques. So, cryptographic key generation, key exchange, cryptographic security mechanisms, cryptography security services are the concern areas for future research work.

Key generation for the various cryptographic applications such as E-commerce, E-transactions, E-banking, E-payments, E-governance, Telemedicine, Exam Questions Transmissions and so on; Group Key generation, Group Key Exchange and Key distribution without third party are the cryptographic research field.

5.4 Implication for Further Study

In this thesis, we proposed and developed a system for transmission of electronic message in a secure fashion. This thesis can be very helpful to further research and project related to cryptography, especially for whom, who want to research with security of electronic transactions. The people who interested to study on information security can be also benefited from this thesis.

References

- [1] Kaufman, Charlie, Radia J. Perlman and Mike Speciner. "Network security - private communication in a public world." Prentice Hall series in computer networking and distributed systems (1995).
- [2] W. Stallings, *Cryptography and Network Security Principles and Practice*, 5th ed., Prentice Hall Press, Upper Saddle River, NJ, USA, 2010.
- [3] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Education Private Limited, 2011.
- [4] Bruce Schneier, "Applied Cryptography", 2nd Edition, 2003, ISBN: 9971-51-348-X.
- [5] C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-5.
- [6] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5.
- [7] M. Ismail Jabiullah, Abdullah Al-Shamim and M. Lutfar Rahman, "Improved Message Authentication and Confidentiality Checking", *Journal of Science and Applications*, Bangladesh Atomic Energy Commission, Dhaka, Bangladesh, Vol. 14, No.1, June 2005, ISSN: 1016-197X, pp: 1-5.
- [8] M. Ismail Jabiullah and M. Lutfar Rahman, "Review on Session-keys and Their Importance for Secured Electronic Transactions", *International Journal of Soft Computing*, Medwell Online, Pakistan, <http://www.medwellonline.net>, Volume 1, Issue Number 3, June-July, 2006 ISSN: 1816-9503, pp: 220-224.
- [9] M. Ismail Jabiullah, Kamrul Ahsan, Jahangir Alam, ANM Khaleqdad Khan and M. Lutfar Rahman, "Elliptic Curve Cryptographic Technique Implementation of Textmessage (SMS) Transaction in Mobile Phone", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 70, May 04-05, 2007.
- [10] M. Ismail Jabiullah, ANM Khaleqdad Khan and M. Lutfar Rahman, "An Improved Session-key Distribution Technique for the Key Distribution Center (KDC)", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 73, May 04-05, 2007.

- [11] Sydul Islam Khan, Md. Ismail Jabiullah and M. Lutfar Rahman, “An Approach for Strong Message Authentication and Confidentiality Checking”, The 22nd Bangladesh Science Conference organized by Bangladesh Association for Advancement of Science (BAAS) and Bangladesh Council of Scientific and Industrial Research (BCSIR), Dhaka, Bangladesh on 27-29 September, 2012
- [12] Md. Monowar Hossain, Anisur Rahman, Sydul Islam Khan and M. Ismail Jabiullah, “Improved CBC-Based Cryptographic Process for Message Transactions”, National Conference on Communication and Information Security (NCCIS 2012), held at 31 March 2012, at the Auditorium, Daffodil International University, Dhaka-1000, Bangladesh, Pages: 59-63.
- [13] Mago, Neeru. “PMAC : A Fully Parallelizable MAC Algorithm.” (2016).
- [14] Semantic Scholar, <https://www.semanticscholar.org/paper/PMAC-%3A-A-Fully-Parallelizable-MAC-Algorithm-Mago/583789c89b0f8abfe0751679a4a330121b9b7f4c>
- [15] Manning’s Inovative Online Reader, <https://livebook.manning.com/book/real-world-cryptography/chapter-3/v-1/27>
- [16] Brain Kart.com, http://www.brainkart.com/article/Pretty-Good-Privacy_8491
- [17] Tutorials Point, <https://www.tutorialspoint.com/cryptography/index.htm>
- [18] Learn Cryptography, <https://learncryptography.com>
- [19] Wikipedia, <https://en.wikipedia.org/wiki/Cryptography>
- [20] ScienceDirect, <https://www.sciencedirect.com/topics/computer-science/encryption-process>

Plagiarism Report

A Double Key

by Muhammad Rashiduzzaman

Submission date: 08-Dec-2019 11:28AM (UTC+0600)

Submission ID: 1229594210

File name: crypton-Decryption_Process_for_Secured_Message_Transactions.pdf (816.33K)

Word count: 7258

Character count: 40368

A Double Key

ORIGINALITY REPORT

19%

SIMILARITY INDEX

7%

INTERNET SOURCES

6%

PUBLICATIONS

16%

STUDENT PAPERS

PRIMARY SOURCES

1 en.wikipedia.org
Internet Source

1%

2 docplayer.net
Internet Source

1%

3 Submitted to Trident University International
Student Paper

1%

4 unina.stidue.net
Internet Source

1%

5 Submitted to Runshaw College, Lancashire
Student Paper

1%

6 Submitted to Daffodil International University
Student Paper

1%

7 Submitted to iGroup
Student Paper

1%

8 Submitted to American Intercontinental
University Online

1%

Student Paper

9 Submitted to Higher Education Commission

Pakistan

Student Paper

1%

10

Submitted to University of Sunderland

Student Paper

1%

11

Aiqing Zhang, Abel Bacchus, Xiaodong Lin.

"Consent-based access control for secure and privacy-preserving health information exchange", Security and Communication Networks, 2016

Publication

<1%

12

Submitted to Visvesvaraya Technological University

Student Paper

<1%

13

passhojao.com

Internet Source

<1%

14

Submitted to New Bulgarian University

Student Paper

<1%

15

Submitted to Pathfinder Enterprises

Student Paper

<1%

16

Submitted to Indian Institute of Technology, Kanpur

Student Paper

<1%

17

Submitted to INTI University College

Student Paper

<1%

Submitted to Canterbury College, Kent

18

Student Paper

<1%

19

J. Rosenberg. "Embedded security", Elsevier
BV, 2017

Publication

<1%

20

"Engineering Information Security", Wiley, 2015

Publication

<1%

21

Submitted to Royal Holloway and Bedford New
College

Student Paper

<1%

22

www.testingexcellence.com

Internet Source

<1%

23

Submitted to CAVAL Ltd.

Student Paper

<1%

24

Submitted to NCC Education Services

Student Paper

<1%

25

m.rbi.org.in

Internet Source

<1%

26

Submitted to University of Wales, Bangor

Student Paper

<1%

27

www.gratisexam.com

Internet Source

<1%

28

Submitted to Kwame Nkrumah University of
Science and Technology

<1%

29 Submitted to De Montfort University <1 %
Student Paper

30 Submitted to Anglo-Chinese School (Independent) <1 %
Student Paper

31 Submitted to Petroleum Research & Development Center <1 %
Student Paper

32 snap.nlc.dcccd.edu <1 %
Internet Source

33 Stallings, William. "E-mail Security Using Pretty Good Privacy", Information Security Management Handbook Four Volume Set, 2000. <1 %
Publication

34 Submitted to University of Hertfordshire <1 %
Student Paper

35 Submitted to Kaplan College <1 %
Student Paper

36 Submitted to SASTRA University <1 %
Student Paper

37 Submitted to University of Maryland, University College <1 %
Student Paper

Submitted to University of British Columbia

38

Student Paper

<1%

39

www.ucalgary.ca

Internet Source

<1%

40

Submitted to SUNY Institute of Technology at
Utica/Rome

Student Paper

<1%

41

ir.library.oregonstate.edu

Internet Source

<1%

42

Submitted to CSU, San Francisco State
University

Student Paper

<1%

43

Shuang-Hua Yang. "Chapter 9 WSN Security",
Springer Science and Business Media LLC,
2014

Publication

<1%

44

www.apriorit.com

Internet Source

<1%

45

amsdottorato.unibo.it

Internet Source

<1%

46

www.researchgate.net

Internet Source

<1%

47

Zhuo Lu, Wenye Wang, Cliff Wang.

"Camouflage Traffic: Minimizing Message Delay
for Smart Grid Applications under Jamming",

<1%

IEEE Transactions on Dependable and Secure Computing, 2015

Publication

48 [archive.org](#)
Internet Source

<1%

49 Submitted to Metropolitan State University
Student Paper

<1%

50 Y.-C. Hu, A. Perrig, D.B. Johnson. "Packet leases: a defense against wormhole attacks in wireless networks", IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), 2003

<1%

Publication

51 Jing Liu, Yang Xiao. "Temporal Accountability and Anonymity in Medical Sensor Networks", Mobile Networks and Applications, 2010

<1%

Publication

52 Bill Hancock. "IPV6 security enhancements still not everything you need", Network Security, 1998

<1%

Publication

53 Umesh Hodeghatta Rao, Umesha Nayak. "The InfoSec Handbook", Springer Nature America, Inc, 2014

<1%

Publication

54 Submitted to Universiti Malaysia Sarawak

Student Paper

<1%

55 Submitted to George Mason University

Student Paper

<1%

56 Submitted to Kingston University

Student Paper

<1%

57 Submitted to University of Northumbria at
Newcastle

Student Paper

<1%

58 Submitted to MCAST

Student Paper

<1%

59 Submitted to University of Bristol

Student Paper

<1%

60 I. Henning, S. Sim, C. Gibbings, M. Russell, P.
Cochrane. "A testbed for the twenty-first
century", Proceedings of the IEEE, 1997

Publication

<1%

61 www.cqu.edu.au

Internet Source

<1%

62 www.mathworks.com

Internet Source

<1%

63 Submitted to Guru Nanak Dev Engineering
College

Student Paper

<1%

64	Submitted to Rochester Institute of Technology Student Paper	<1%
65	flylib.com Internet Source	<1%
66	Submitted to (school name not available) Student Paper	<1%
67	Submitted to Limerick Institute of Technology Student Paper	<1%
68	Submitted to University of Teesside Student Paper	<1%
69	"Social Transformation – Digital Way", Springer Science and Business Media LLC, 2018 Publication	<1%
70	Submitted to The State University of Zanzibar Student Paper	<1%
71	"Advanced Hybrid Information Processing", Springer Science and Business Media LLC, 2019 Publication	<1%
72	Hong Heather Yu, Peng Yin, Xiaolong Yu. "Joint content authentication and error control for wireless multimedia communications", 2003 International Symposium on VLSI Technology, Systems and Applications. Proceedings of Technical Papers. (IEEE Cat. No.03TH8672),	<1%

2004

Publication

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off