Stronger Message Authentication and Confidentiality Checking Through Authentication Code Tied To Cipher Text

BY

MD ARIFUL HAQUE
ID: 112-25-208

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

Supervised By

Professor Dr. Md. Ismail Jabiullah
Head
Department of Computer Science And Engineering
Hamdard University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2013

APPROVAL

This Thesis/Project titled **"STRONGER MESSAGE AUTHENTICATION AND CONFIDENTIALITY CHECKING THROUGH AUTHENTICATION CODE TIED TO CIPHER TEXT**", submitted by **Md. Ariful Haque** 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 CSE and approved as to its style and contents. The presentation has been held on 28.01.2013.

BOARD OF EXAMINERS

_____

Dr Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr Yousuf Mahbubul Islam — **Internal Examiner**
Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr Md Kabirul Islam — **Internal Examiner**
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr Mohammad Shorif Uddin — **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

We hereby declare that, this thesis has been done by us under the supervision of **Professor Dr. Md. Ismail Jabiullah,** Head, Department of Computer Science And Engineering **,**Hamdard University. We also declare that neither this project nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:

_____

Professor Dr. Md. Ismail Jabiullah
Professor,Head
Department of Computer Science And Engineering
Hamdard University

Submitted by:

_____

(MD. ARIFUL HAQUE)
ID: 112-25-208
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to almighty Allah for His divine blessing makes me possible to complete this project successfully.

I fell grateful to and wish my profound my indebtedness to **Professor Dr. Md. Ismail Jabiullah**, Head, Department ofComputer Science And Engineering, Hamdard University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of network security influenced me 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 **Professor Dr. Syed Akter Hossain**, Professor and Head**,** Department of Computer Science and Engineering (CSE), for his kind help to finish our thesis and also to other faculty members and the staffs 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.

(Md. Ariful Haque)
ID: 112-25-208
Department of Computer Science and Engineering
Daffodil International University

ABSTRACT

Message Authentication and confidentiality checking of a message are demanding issues for secured electronic transactions. A stronger message authentication and confidentiality checking technique has been designed, developed and implemented using Java programming language. For this, existing approaches have been studied, realized and analyzed with their limitations, advantages and applications. In this process, a message is encrypted with a secret key K_1 that produces message authentication code (MAC), which is concatenated with the message and again encrypted with another secret key K_2 and again encrypted the output with key K_1 that builds the ciphertext that is to be sent to the destination. In the receiving end, first decryption is performed with the secret key K_1 and then again decrypted the output with the secret key K_2 that produces thecipher' and the MAC of the message, and then the message is only decrypted to produce Cipher'; and the new cipher' is compared with received message authentication code (MAC) that ensures the authentication of the message. Here, encryption/decryption key values ensure the stronger authentication and also the confidentiality of the communicating message. It can be applied where higher-level security services of the communicating messages are needed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Introduction

Message transactions are very much important issue in electronic communications era. Messages are communicating through e-mail in network environment is now in vulnerable situation. There are much more mechanisms for doing secured electronic message transactions in the vulnerable worldwide network Internet. Now-a-days, it is prime concern to impose more security services in the communicating message, communicating participants and the communication route. The message communication through the world wide network Internet which is very insecure. In electronic message transaction the sender transmits a message to the receiver through a communication channel. In this process the intended receiver might not get the original message sent by the sender due to insecure channel. The intruder may alter the message as a malicious act.

Secure electronic message transactions is now-a-days an important ingredient of electronic commerce. Without strong security, the benefit of the merchant, the consumer, and the credit or economic institution cannot be served properly. Privacy of transactions, integrity and authentication of all parties, is important for achieving the height of trust that will boost the transactions. The cryptographic techniques are used to provide the security to the messages. It is important that the encryption algorithms and increased complexity is robust enough to prevent observation by the intruders. The ideal of the secure electronic message transactions is important for the success of electronic commerce. In cryptographic message transactions, messages are transformed into an encrypted form by using some cryptographic technique and some cryptographic keys and then sent to the destination by the insecure channel that may be any public network channel. In the destination, the received encrypted message is not clear to the receiver. He/she should do the related cryptographic technique with the related cryptographic keys and then retrieve the clear message from the ciphertext. This clear message is then intelligent to the receiver and performs the security for the message and the communicating parties.

Our prime concern in this thesis is to impose more security services to the communicating messages and stronger security approaches by using the same methods, encryption-decryption processes and the encryption-decryption keys.

1.2 Aim of the Work

In modern electronic communication era security is the key consideration for many reasons. The electronic media is vulnerable to the message transactions. To overcome the existing problem, the demand of message security is growing. To ensure the message security various cryptographic techniques are employed. For this, cryptographic dimensions, cryptographic mechanisms, cryptographic key considerations and related issues will be studied, realized and analyzed. Existing systems for secured message transactions will be studied and the established security parameters will be identified and realized. The main objective of this thesis is to propose an improved method for secured message transactions with stronger security services than the existing systems to the messages transactions using cryptographic encryption and decryption methods and the cryptographic keys.

1.3 Motivation

Secure electronic message transactions is now-a-days an important ingredient of electronic commerce. Without strong security, the benefit of the merchant, the consumer, and the credit or economic institution cannot be served properly. Privacy of transactions, integrity and authentication of all parties, is important for achieving the height of trust that will boost the transactions. The cryptographic techniques are used to provide the security to the messages. It is important that the encryption algorithms and increased complexity is robust enough to prevent observation by the intruders. The ideal of the secure electronic message transactions is important for the success of electronic commerce. In cryptographic message transaction, messages are transformed into an encrypted form by using some cryptographic technique and some cryptographic keys and

then sent to the destination by the insecured channel that may be any public network channel.

Messages are communicating through e-mail in network environment is now in vulnerable situation. There are much more mechanisms for doing secured message transactions in the vulnerable world wide network Internet. Now-a-days, it is prime concern to impose more security in the communicating message, communicating participants and the communication route. In this thesis, it is our interest to establish an electronic transaction system that performs secured message transactions with the fundamental security services: authentication, confidentiality, integrity and non-repudiation both on communicating messages and also on the communicating parties. This is very much desirable for current e-commerce, e-banking, e-marketing, e-management, e-governance etc.

1.4 Organization of the Thesis

The thesis is organized in seven chapters. The first chapter introduces the aims and objectives of the current research work after a brief introduction of the secured message transactions, and the last chapter i.e., Chapter 7 is the conclusion of the thesis and it also gives the indication of the future work.

Chapter 2 introduces cryptographic background, security requirements and services, Secret key or Symmetric key and Asymmetric key, PGP and the necessary mathematical background for cryptographic techniques. Chapter 3 introduces the RSA encryption and decryption processes, prime number generation and RSA key generation techniques. Chapter 4 introduces the Tri-level Cryptographic Technique for Secured Message Transactions as proposed system for increased security for message transactions, data flow diagram and the algorithms for encryption and decryption processes. Chapter 5 is the implementation of the proposed system for experimental verification of the total process in java programming language. Chapter 5 also analyzes the input and output of

the system. Chapter 6 is a comparative analysis of the proposed system with the PGP and gives various statistics of their security services.

CHAPTER 2: BACKGROUND STUDY

2.1 Introduction

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptology prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Since WWI and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Alongside the advancement in cryptology-related technology, the practice has raised a number of legal issues, some of which remain unresolved.

2.2 Cryptographic Terms

In modern day cryptography the several cryptographic terms are used. In this project the flowing cryptographic terms used; cipher, code, commercial code, cryptanalysis, cryptography, cryptology, deciphering, decryption, digraphs, encryption, homophones key, mono alphabet, nomenclature, nulls, plaintext, poly alphabet, public key, cryptosystem, steganography, substitution, symmetric key cryptosystem, transmission security, transposition. Definitions of some of the cryptographic terms are given below.

Cipher: A mapping algorithm that is applied to a fixed number of characters at a time with an intent of concealing the contents of the message.

Code: A mapping algorithm that is applied to a variable number of characters (according to linguistic entities) at a time with an intent of concealing the contents of the message.

Commercial Code: A code used in business primarily to reduce cost by shortening messages. It involves no secrecy. The prime example is the 'Philips' Code.

Cryptanalysis: The study of methods of reading enciphered and encoded messages without original knowledge of the cipher method used or the current keys.

Cryptography: The study of methods of enciphering and deciphering messages to

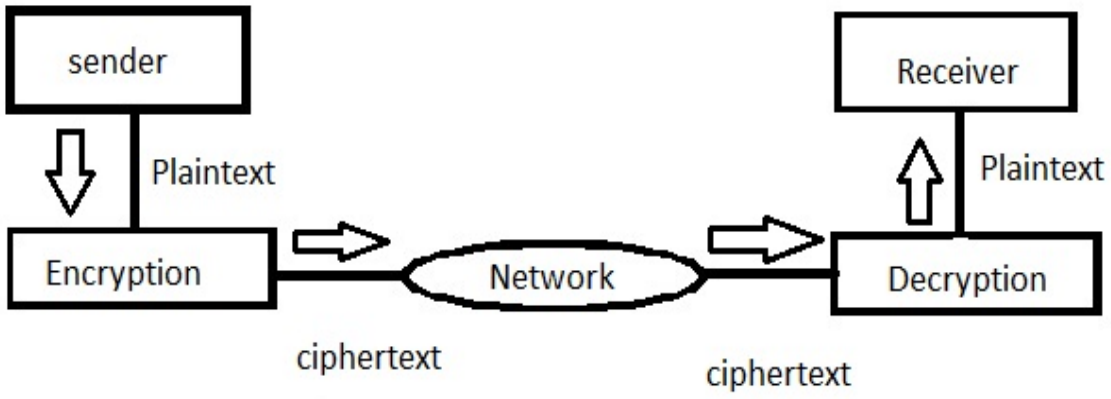


Figure 2.1: A Cryptographic System

conceal the contents of a message.

Cryptology: The study of both cryptography (enciphering and deciphering) and cryptanalysis (breaking or cracking a code system or individual messages).

Deciphering: The procedure of turning enciphered text into plain text **with** prior knowledge of the algorithms or keys involved. This is what the intended message receiver does.

Decryption: The science of turning enciphered text into plain text **without** prior knowledge of the algorithms or keys involved. This is what the interceptor or 'cracker' does.

Digraphs: A plaintext character pairing technique that prevents frequency analysis of commonly occurring pairs such as 'qu'. Note that trigraph (three characters at a time) is an extension of the theme.

Encryption: In cryptography, **encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as cipher text). In many contexts, the word **encryption** also implicitly refers to the reverse process

Homophones: Several replacement letters for the same letter in plaintext

Key: A sequence of symbols that controls the operation of a cryptographic transformation, e.g., encipherment, decipherment. In practice a key is normally a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. The key should be the only part of the algorithm that it is necessary to keep secret.

Mono alphabet: A single mapping of plaintext letters to cipher text letters.

Nomenclature: Half code and half cipher, it was a list of word/syllable substitutions and cipher alphabet with homophones.

Nulls: Meaningless letters used to confuse by modifying frequency distributions or predictability. Sometimes used to fill a message to a specific length.

Plaintext: The original message to be encoded or enciphered

Poly alphabet: A method where several mappings of plaintext letters to ciphertext letters occur in a message.

Public Key Cryptosystem: A system where a pair of keys are used, one freely distributed and the other known only to the recipient.

Steganography: The art of concealing a message's existence. One example would be through the use of photographic microdots.

Substitution: Enciphering by replacing one letter by another.

Symmetric Key Cryptosystem: A system where both sender and receiver use the same key for enciphering and deciphering.

Transmission Security: The art of concealing an electrically transmitted message through burst encoding or spread spectrum methods.

Transposition: Enciphering by shuffling the order of letters.

2.3 Secured Message Transaction Model

A message transaction security model using the symmetric encryption scheme has five ingredients [14]**:**

- **Plaintext Message:** This is the original intelligible message or data that is fed into the encryption algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions

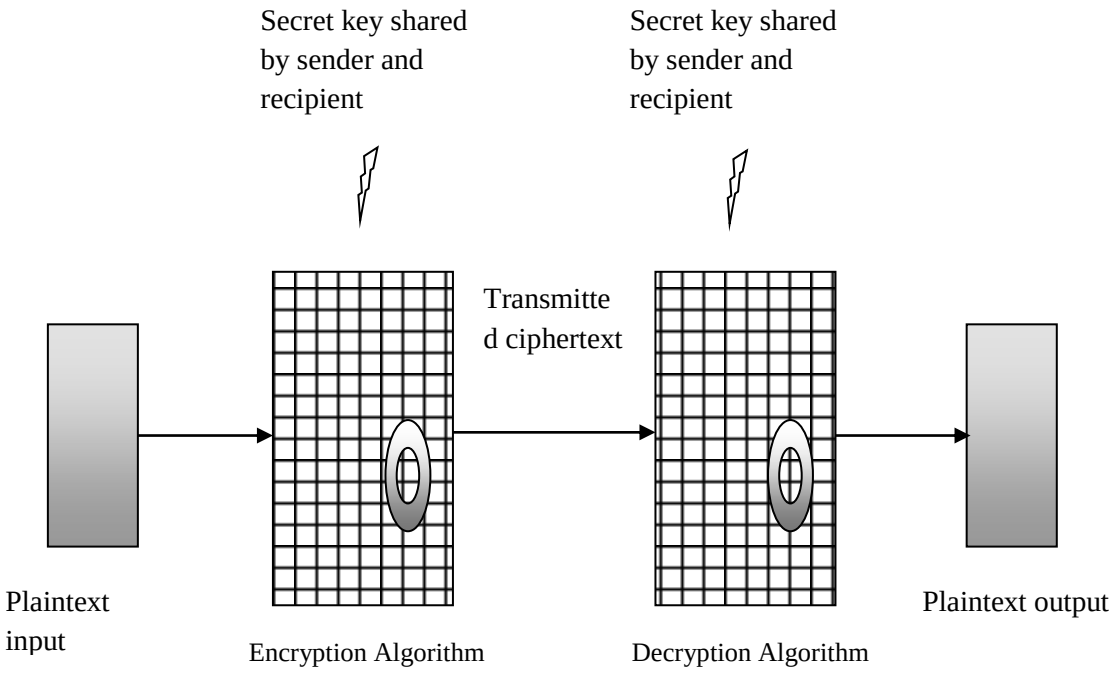


Figure 2.2: Simplified Model of Conventional Encryption Process

and transformations on the plaintext.

- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

2.4 Security Services

A security service is a service provided by a protocol layer of security communicating open system which ensures adequate security of the systems or of data transfers. It provides a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies, and are implemented by security mechanisms.

We are living in the information age. Now-a-days, we communicate each other through electronic message. As a result, we need to keep information secured from unauthorized access and protect from unauthorized change.

There are five categories of security services provided by the secured electronic transaction system and they are presented below.

Confidentiality: Confidentiality is the most common aspect of message or information security. An individual or organization need to guard against the malicious actions endangered to the confidentiality of the message or information. In modern days communication concealment of sensitive information is the major concern. In business arena, hiding information from competitors is crucial to the smooth operation of the organization e.g. the customers' accounts of a bank need to be kept secret. Confidentiality no only applies to the storage of information but also can be used to the message transmission methods.

Integrity: The integrity provides the assurance that data received are exactly the same as sent by the sender i.e. it ensures no modification, insertion, deletion, or replay. It also means that only authorized changes to the message can be performed. To ensure integrity, the sender of a message uses a hash function, a mathematical algorithm that creates a unique summary of a message known as a message digest and transmits it along with the message. When the recipient decrypts the message, he uses the same hash function to create his own version of the message digest and then compares it to the digest transmitted with the message. If the two digests match, the recipient knows that the integrity of the message is preserved. If the digests differ, someone altered the message along the way.

Authentication: The authentication service ensures that a communication between a sender and receiver is authentic. The authentication is of two types (i) Peer entity authentication: Provides for the confirmation of the identity of a peer entity in an association. It is provided for use at the establishment of connection or at times during the data transfer phase. It assures that an entity is not performing either a masquerade or an unauthorized replay of a previous connection. (ii) Data origin authentication: Provides for the confirmation of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like

electronic mail where there are no prior interactions between the communicating entities.

Non-repudiation: It prevents either sender or receiver from denying a transmitted message. As a result, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

2.5 Secret Key Generation

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. Modern cryptographic systems include symmetric key or secret key algorithms such as DES and AES and public key algorithms such as RSA. Symmetric key algorithms use a single shared key for keeping data secret.

In computer cryptography keys are integers. In some cases keys are randomly generated using a random number generator (RNG) or pseudorandom number generator (PRNG). The simplest method to read encrypted data is a brute force attack that means attempting every number, up to the maximum length of the key. Therefore, it is important to use a sufficiently long key length; longer keys take exponentially longer to attack, rendering a brute force attack impractical. Currently, key lengths of 128 bits (for symmetric key algorithms) and 1024 bits (for public key algorithms) are common.

2.6 Random Number Generation

Random number is a number chosen as if by chance from some specified distribution such that selection of a large set of these numbers reproduces the underlying distribution. Such numbers are always required to be independent, so that there are no correlations between successive numbers. Computer-generated random numbers are sometimes called

pseudorandom numbers, while the term "random" is reserved for the output of unpredictable physical processes. It is impossible to produce an arbitrarily long string of random digits and prove it is random. There are a number of common methods used for generating pseudorandom numbers, the simplest of which is the linear congruence method. Most random number generators require specification of an initial number used as the starting point, which is known as a "seed." The goodness of random numbers generated by a given algorithm can be analyzed by examining its noise sphere.

There are two principal methods used to generate random numbers. One measures some physical phenomenon that is expected to be random and then compensates for possible biases in the measurement process. The other uses computational algorithms that produce long sequences of apparently random results, which are in fact completely determined by a shorter initial value, known as a seed or key. The latter types are often called pseudorandom number generators

2.7 Secret Key Cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers

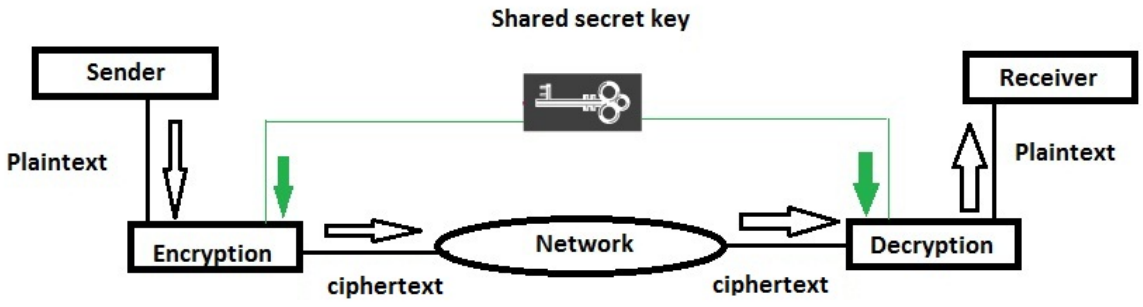


Figure 2.3: Shared Secret Key Cryptographic System

of people. In addition, there is also the problem of how you communicate the secret key securely.

In this present research work, shared secret key cryptographic model is used for generating message authentication code (MAC) in both sender site and also in receiver site.

2.8 Summary

In this chapter, cryptography, some cryptographic terms, components of cryptographic system, message security models, message security services and the shared secret key cryptography have been studied and presented.

CHAPTER 3: CONVENTIONAL APPROACH

3.1 Introduction

Message Authentication and Confidentiality checking is a general security services for secured electronic transactions. Here, first conventional message authentication with its diagram is described clearly, then conventional message confidentiality checking approach is analyzed with its pictorial presentation and then conventional message authentication and confidentiality checking approach is analyzed with its pictorial presentation. Finally, a summary is given regarding the present security services approaches.

3.2 Conventional Message Authentication

Message authentication is a procedure that allows communicating parties to verify that received message is authentic and a message is said to be authentic when it is genuine and comes from its alleged source. Essentially, the MAC is a small fixed-size block of data that is generated based on a message M of variable length using secret key K as follows [1]:

$$MAC = E_K(M)$$

If a party A wishes to send party B a message M, and protects it via a MAC, they first need to share a secret key K. Then A calculates MAC as a function of M and K. Then the message M plus the MAC are transmitted to B. B performs the same calculation on M, using K to generate a new code MAC′. The received MAC is compared to the calculated MAC′ to verify the data integrity [2]. As only A is able to generate MAC, source authentication is also achieved. MAC provides an efficient way to message authentication. It also separates the authentication function from confidentiality [3]. This is an attractive feature for many applications where confidentiality is not necessary. Message Authentication is one of the demanding areas of network security. Message

authentication is a process to verify that the received message come from the alleged source and have not been altered. The diagram of the message authentication using message encryption with a shared secret key is depicted in Fig. 3.1..

Sender Receiver

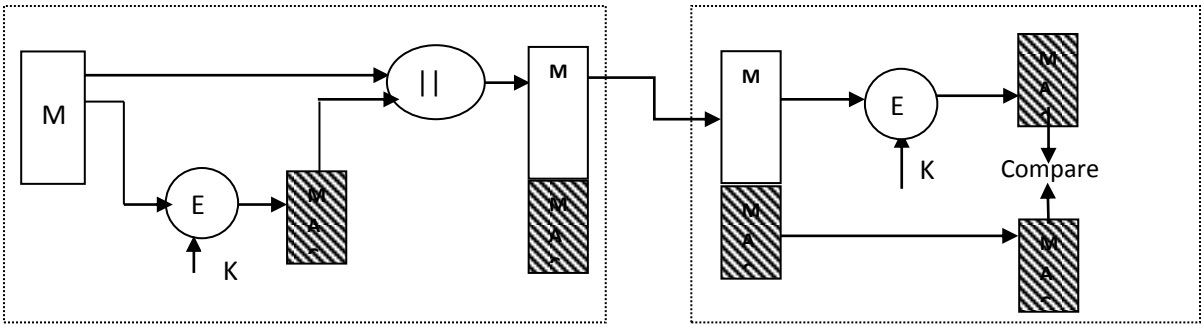


Fig. 3.1: Secured Message Transactions with Message Authentication

Here, message is encrypted with a shared secret key K to produce a MAC and which is concatenated with the message. Then the message plus the message digest is sent to the destination. In the receiving end, the message is again encrypted with the same shared secret key K and to produce another message authentication code MAC' and which is compared with the received MAC. If the MACs are the same, then the receiver assures that the received message came from the alleged source and the message is not altered. It establishes secured message transactions with message authentication. The communicating message has not been altered in the transition. This process does not provide confidentiality, integrity and non-repudiation security services [5]. To provide these security services, another layer of security mechanism is needed. If we assume that only the receiver and the sender know the identity of the secret key, and if the received MAC matches the calculated MAC, then:

(a) The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the MAC, then the receiver's calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to

know the secret key, the attacker cannot alter the MAC to correspond to the alterations in the message.

(b) The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper MAC.

(c) If the message includes a sequence number, then the receiver can be assured of the proper sequence because an attacker cannot successfully alter the sequence number.

3.3 Conventional Message Confidentiality Checking

Confidentiality is the protection of transmitted data or message from unauthorized disclosure. Cryptographic techniques provide confidentiality by virtue of the keys used for encryption-decryption. Data integrity provides the assurance that the message or data received are exactly as sent by an unauthorized entity i.e., contains no modification, insertion, deletion, or replay [6]. One can apply a process to generate a MAC to the message so that only legitimate plaintext can pass the MAC detection. The attackers can manipulate the message in a way which cannot be detected by MAC. Although encrypting the message and its MAC as a whole seems to be a valid approach for establishing the mentioned security services [7]. In light of MAC, we can design a code that uses a secret key. Without the key, modifying the message in a way that it matches the code is impossible. To realize the processes of the message authentication code generating and verifying two conventional approaches are studied. In this paper, an improved approach for message authentication and confidentiality checking has been designed, developed and implemented in Java for achieving the better security services of the message transaction system [8]. A comparative study on the proposed system and the conventional system has also been performed and presented.

In our research, a stronger approach has been established for message authentication and confidentiality checking where message authentication code (MAC) is concatenated with the ciphertext of the communicating message by using two secret shared keys.

3.4 Conventional Message Authentication and Confidentiality Checking

To propose a new stronger message authentication process, conventional approach has been studied, realized and analyzed. This approach establishes a stronger message authentication and confidentiality checking between the communicants. Here, message is encrypted with a shared secret key K_1 that produces a message authentication code (MAC) and which is again encrypted by secret key K2 and get cipher. Then the MAC and the cipher is concatenate with one another.. The output is sent to the destination. In the receiving end, the received information is decrypted with the secret key K_1 that produces the cipher' and the MAC of the message . Then the cipher is then compared with the received cipher . If the cipher s are the same, then the receiver assured that the received message came from the alleged source and the message is not altered. In this case, encryption-decryption with the shared secret key K_2 assures the confidentiality of the message and the message authentication code (MAC) . This is a layer-two security of the communicating message in the transaction . And the other part of the process establishes secured message transactions with message authentication. The diagram of the message authentication with more confidentiality in the message using message encryption with two shared secret keys is depicted in Fig. 3.2.

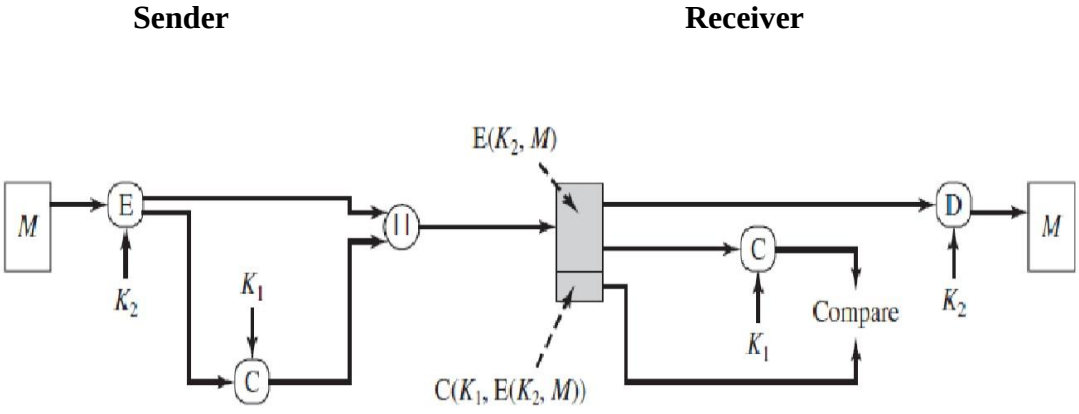


Fig 3.2: Message authentication and confidentiality authentication tied to ciphertext

3.5 Identified Limitations of the Conventional System

Conventional message authentication and confidentiality technique has been studied, realized and analyzed to find its limitations, benefits and application areas. The identified limitations of the conventional system are summarized below.

- **Single Encryption/Decryption:** In this process, to prepare a message authentication code (MAC), a single key K is used for performing encryption in the sender side and decryption in the receiver side. If the key is compromised the security of the system may be vulnerable. The confidentiality of the system is fully depends on the encryption/decryption key of the security system.
- **Message is not Encrypted with Stronger Way:** The conventional process for message authentication and confidentiality checking is only encrypted one time and produce MAC and concatenated it with message and again encrypted with another key to produce the ciphertext that is to be sent to the destination. The keys are used for encryption for two separate encryption processes that establishes the strong message authentication and message confidentiality.

3.6 Summary

In this chapter, an introduction of the convention message authentication system, message authentication of the convention process where message authentication code (MAC) is tied to the ciphertext, limitations of the conventional system are discussed, analyzed and presented. In our proposed system, an improved security service can be performed to impose better security services where needed.

CHAPTER 4: IMPROVED APPROACH

4.1 Introduction

A stronger message authentication and confidentiality checking system has been designed, developed and analyzed that is using with ciphertext tied to the context. In this chapter, process of the proposed, diagram of the proposed system, encryption algorithm, decryption algorithm and a summary of the system are presented.

4.2 Process Description of the Proposed System

Consider the straight forward secret-key encryption-decryption process on the transmitted messages. A message M transmitted from source A to the destination B is encrypted by a conventional cryptographic mechanism using a secret key shared by the sender A and as well as receiver B. If no other party knows the secret key K and no other party can decrypt the transmitted message, then the confidentiality is provided [10]. Here, a message is encrypted with a key K_1 that produces MAC which is encrypted again by secret key K2.Then the cipher and the MAC will concatenate with one another and encrypt again bye secret key K1. In the receiving end, first decryption is performed with the key K_1 and then again the output is decrypted with key K_1 that produces the cipher' and the message authentication code (MAC).Then the cipher' and the main cipher wil be compared and if the cipher' is alleged with proper cipher then the cipher' will decrypt and get MAC.At last the MAC will decrypt by secret key K1and get an authenticated proper message. Here, key values ensure the strong authentication and also confidentiality of the communicating message.

4.3 Diagram of the Proposed System

A message is encrypted with a key K_1 that produces MAC which is concatenated with the message and again encrypted with key K_2 and again encrypted the output with key K_1 which builds the ciphertext that is to be sent to the destination. In the receiving end, first decryption is performed with the key K_1 and then again the output is decrypted with key K_2 that produces the message and the message authentication code (MAC) of the message, and then the message is only decrypted to produce message authentication code (MAC'); and the new message authentication code MAC' is compared with received message authentication code MAC that ensures the authentication of the message.

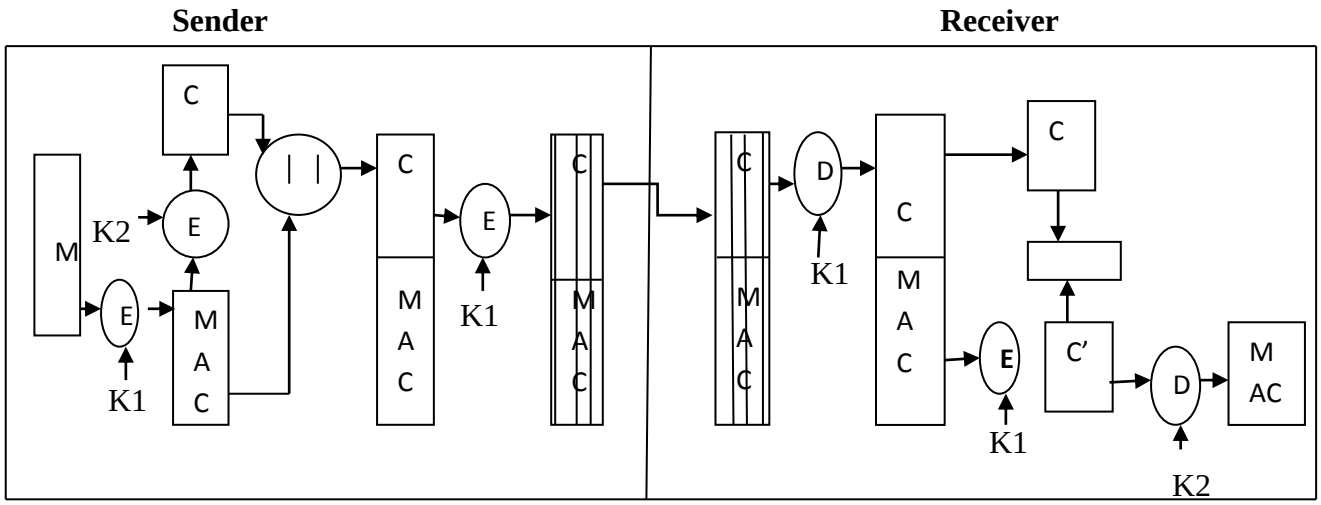


Fig 4.1: Strong message authentication and confidentiality checking by MAC encryption

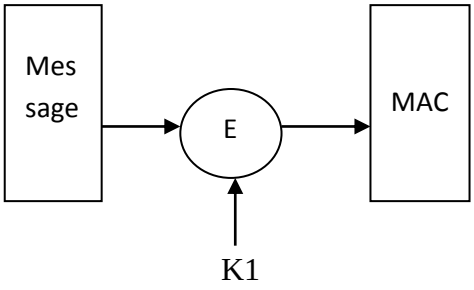
Here, key values ensure the strong authentication and also confidentiality of the communicating message. The diagram of the message authentication with more confidentiality in the message using message encryption with two shared secret keys. The whole process is depicted in Fig. 4.1.

4.4 Step-by-Step Flow diagram of the Proposed System

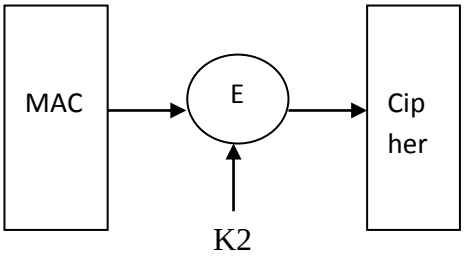
Diagrammatic flow approach of the proposed system for message authentication and confidentiality checking through authentication code tied to plaintext are formulized and presented. The segmented flow diagram of the algorithms is given here in step-wise.

Step by step flow diagram of proposed system:

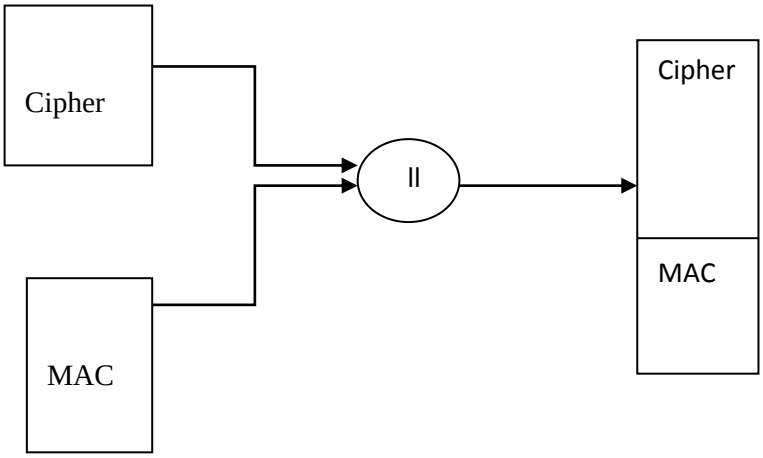
Step 1: Perform an encryption process on the block of message using the secret key K1 what produces the message authentication code MAC or check sum.



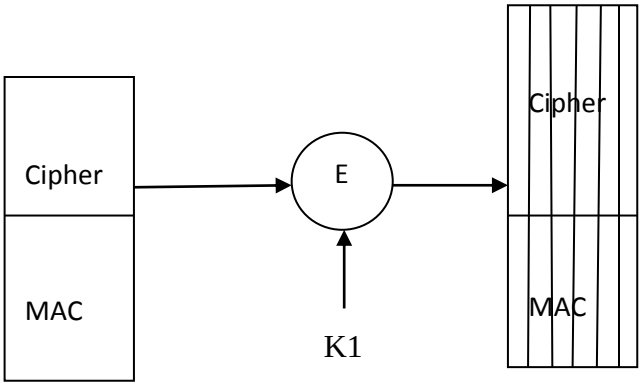
Step 2: Then the MAC is encrypted by an another key K2 what produces a ciphertext.



Step 3: Ciphertext and MAC is concatenate where produced a big block of message as merged .

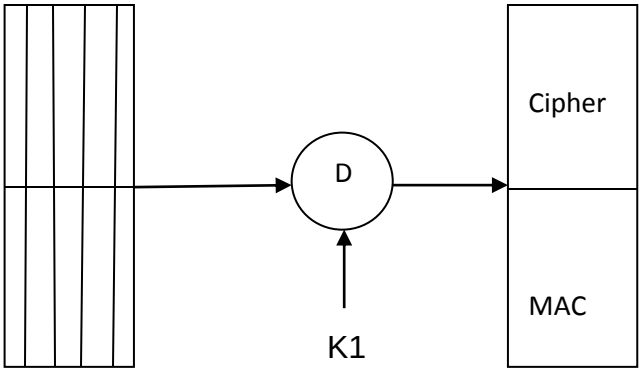


Step 4: Encrypt that merged message with the secret keyK1 that produces the ultimate protected message.

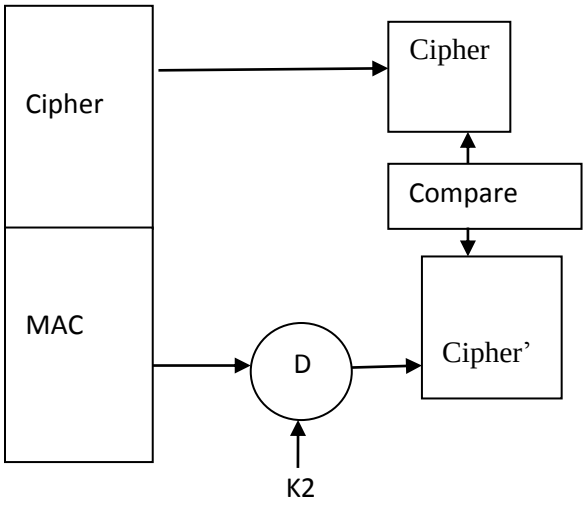


The output is then sent to the desired destination.

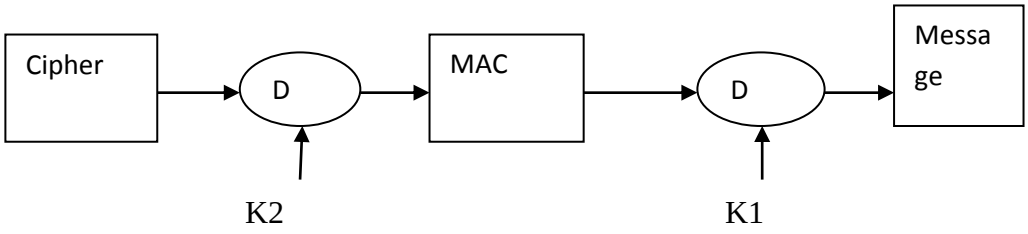
Step 5: In the receiving end, the received information is first decrypted using the secret key K_1 that produces the encrypted message and the MAC of the message.



Step 6: Now encrypt the using the secret key K_1 that produces a MAC and then compare it with the received MAC of the message.



Step 7: Then separate the message and the MAC. The retrieved information is again decrypted using the secret key K_2 that produces the original message and the MAC of the message.



Here, if the generated MAC and the Received MAC is found same, then it is concluded that the message is not altered in the route.

4.5 Algorithms of the Proposed System

Algorithmic approaches of the proposed system for message authentication and confidentiality checking through authentication code tied to ciphertext are formulized and presented. The encryption algorithm that is done in the sender site is given here in step-wise.

Description of the Encryption Algorithm:

The encryption algorithm of the proposed system is composed of the following steps.

Step 1: Sender selects the message and divides it into block of messages of key length. Padding is used if necessary.

Step 2: Performs encryption process on the block of messages using the secret key K_1 that produces the message authentication code, MAC, or check sum. again encrypt MAC with another secret key K_2 and the output is concatenate with encrypted cipher text and encrypted with the secret key K_1 which builds the ciphertext that is to be sent to the destination.

Step 3: In the receiving end, first receiver performs decryption with the secret key K_1 .

Step 4: Then the receiver encrypts the message only to produce a new message authentication code MAC'; and the newly generated MAC' is compared with the received MAC. This ensures the authentication of the message. Then the output is again decrypted with the secret key K_2 that produces the message and the message authentication code MAC of the message. Here, using the two secret key values ensures the strong authentication and two times encryption-decryption establishes the confidentiality of the communicating messages.

Then, the decryption algorithm is formulized as algorithmic approach which is performed in the receiver site is given below as step-wise.

Description of the Decryption Algorithm:

The decryption algorithm of the proposed system is composed of the following steps.

Step 1: After receiving the ciphertext receiver first performs decryption with the secret key K1

Step 2: Then the output is again decrypted with the secret key K2 that produces the message and the message authentication code MAC of the message.

Step 3: Finally the receiver encrypts the message with K1 only to produce a new message authentication code MAC.

Step 4: The newly generated MAC is compared with the received MAC. This ensures the authentication of the message. Here, using the two secret key values ensures the strong authentication and two times encryption-decryption establishes the confidentiality of the communicating messages.

Notation of the Decryption Algorithm:

The notation of the decryption algorithm of the proposed system is composed of the following steps.

4.6 Summary

In this chapter, an introduction about the proposed system, process of the proposed system, proposed system diagram, encryption algorithm and decryption algorithmic process of the proposed system are analyzed and presented.

CHAPTER 5: IMPLEMENTATION OF THE PROPOSED SYSTEM

5.1 Introduction

Any proposed method is implemented in a programming language to measure its justification for input and output conditions. In this chapter, the implemented input-output analysis of the proposed system and a discussion are presented.

5.2 Implementation on Java

The proposed method has been implemented using the Java programming language because of its simplicity, better security and its better interactive property with the users. For this Java software JbK-6u21-windows-i586 is installed in C drive of the system. The implemented program is tested and analyzed and for several inputs. The proposed system has been found justified conditions with its identified security services.

5.3 Input / Output Analysis

The proposed encryption / decryption system has been implemented in Java programming language with several inputs. The implemented input / output analysis has been presented here. For example, first intended message "Send more money immediately" is taken as the plaintext shown in Fig. 5.1.

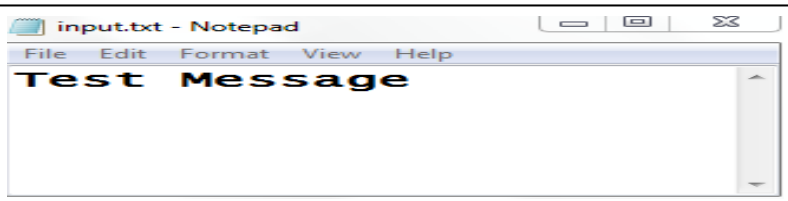


Fig. 5.1: Input Message

Then, "-1019039863" has taken as the secret key K_1 used for encryption in the proposed system shown in Fig. 5.2. Then "OK" button has been pressed and the encrypted output is generated by the system.

Fig. 5.2: Secret Key K_1

The process produces the ciphertext and the produced ciphertext is used as the message authentication code (MAC) which is given in Fig. 5.3.

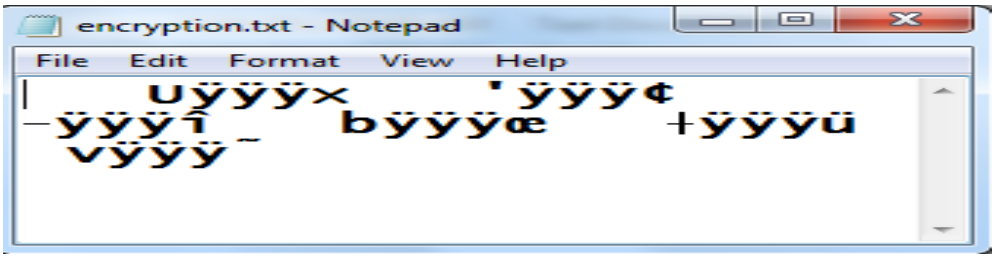


Fig. 5.3: MAC by K_1

Then the number 9887 is used here as another secret key K_2 depicted in the Fig. 5.4 is used for encryption on the message to produce the second ciphertext. The OK button is pressed to produce the encrypted message and the MAC.

Fig.5.4: Secret Key K_2

This output is again encrypted with the secret key K_1 to produce the final ciphertext depicted in Fig. 5.5 and that is to be sent to the destination.

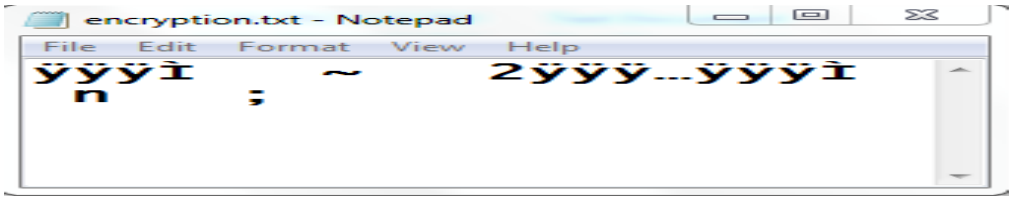


Fig. 5.5: Ciphertext is sent to the Destination

In the receiving end, the received ciphertext is first decrypted by using the secret key K_1 that produces the intermediary ciphertext from the retrieved ciphertext which is given in Fig. 5.6. This is the encrypted message and the MAC of the message.

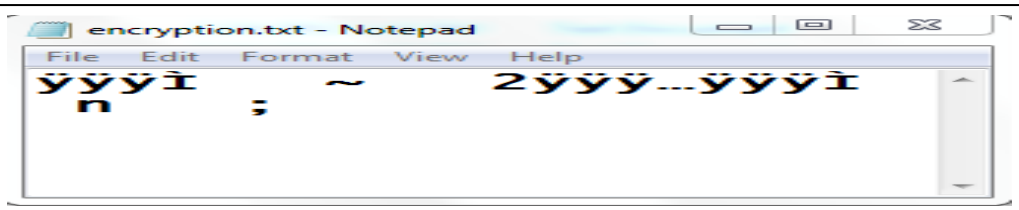


Fig. 5.6: Retrieved Ciphertext in the Destination

After that, the intermediary ciphertext is again decrypted by the secret key K_2 to retrieve the plaintext and the MAC. Now separate the message and the MAC. This establishes the confidentiality of the message transactions. Now for message authentication, the message is again encrypted with the secret key K_1 that produces the MAC and is compared with the received MAC. This establishes stronger message authentication

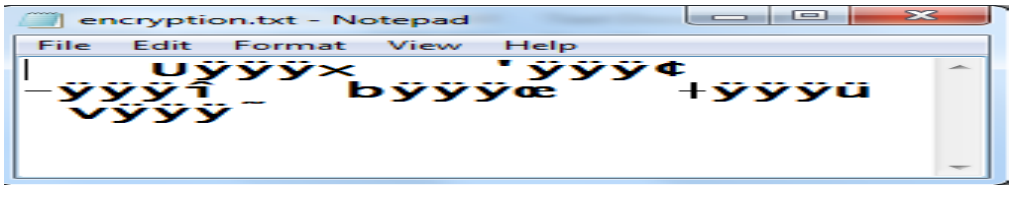


Fig. 5.7: Retireved MAC

.If the produced MAC is matched to the received MAC, the message is not altered in the transition, i.e. the message is found in the receiving end with full authentication. Here, uses of two times encryption perform for stronger confidentiality. Use of two separate keys encryption ensures the stronger message authentication. The process was implemented in Java programming language for several times for different messages and was found to produce satisfactory results.

5.4 Discussions

Message authentication and message confidentiality are very much important issues regarding network security services.

CHAPTER 6: SECURITY ANALYSIS

6.1 Introduction

The security mechanisms needed to cope with unwanted access fall into different basic security services and they are confidentiality, authentication, integrity checking and non-repudiation. Security services are implemented by security policies and then are implemented by security mechanisms. In this chapter, a comparative study between the conventional system and the proposed system for message authentication and confidentiality checking through authentication code tied to ciphertext has been performed and presented.

6.2 Comparative Security Analysis

Any security system performs the fundamental security services which are confidentiality, authentication, integrity checking and non-repudiation. The proposed system performs all the security services and is shown in Table 6.1.

Table 6.1: Comparison Chart between the Conventional and the Proposed System

Approaches	Confidentiality	Authentication	Integrity	Non-repudiation
Conventional Approach	Yes	Yes	No	Yes
Proposed Approach	Yes	Yes	Yes	No

The security services performed by the proposed system are analyzed in the following:

- **Confidentiality:** The system performs encryption with the sender's private key that is not compromised by anyone in the communication and so it establishes first layer confidentiality of the message transaction. Since the system finally again encrypts the ciphertext with the shared secret key for the communicants. Hence, it establishes second layer confidentiality in the communicating message.
- **Authentication:** The system performs encryption with the sender's private key and then again encrypts them with receiver's public key in the sender site. It is decrypted with sender's public key in the receiver's site, so sender cannot deny that is not sent by the sender. Since, the message is decrypted with the receiver's private key that is related with the receiver's public key that is used in the sender's site for encryption. No one can decrypt the ciphertext other than the intended receiver, since the receiver's private key is not compromised. Hence, it establishes the both way authentication for the communicating message.
- **Integrity:** The system encrypts the message contents through the sender's private key related to his public key. So, anyone who knows the sender's public key can decrypts the ciphertext and retrieves the message. But the system again encrypts the ciphertext by using the receiver's public key and so none other than the intending receiver cannot decrypt the received ciphertext and hence cannot retrieve the message. So, thus it establishes integrity in the communicating message.
- **Non-repudiation:** The proposed system first encrypts the message with sender's private key, then encrypts with receiver's public key and finally encrypts the contents with a shared secret key. One can compromise the shared secret key and retrieves the ciphertext that needs to retrieve the receiver's private key and that is not possible. Since it requires retrieving the message the receiver's private key, sender's public key and a sender-receiver shared secret key, so it is impossible to repudiate the transaction to each of the participants simultaneously. Hence, it establishes non-repudiation in the communicating message.

Finally, the desired plaintext is found again that is given as input. Here, the retrieved output is also found as plain text file in project folder. For the proposed system, it is tried to implement the process in Java language because of stronger security. The proposed system was run satisfactorily in this program. Several different inputs are analyzed for this program and every one of them produced correct output. It can be observed that the program can be used for variable length file transfer. Some difficulties are faced to implement the program in Java language, because Java language has some limitations. To overcome these difficulties further research in future will be required.

6.3 Summary

Any improved process is desired for the betterment of the security services of the secured electronic transaction system. In this chapter, a comparative analysis has be done and presented with clear comparison between the conventional system and the proposed system. The comparison of the security systems is performed on the fundamental security services which are confidentiality, authentication, integrity checking and non-repudiation.

CHAPTER 7: CONCLUSIONS AND FUTURE WORKS

7.1 Summary

An introduction of the convention message authentication system, message authentication of the convention process where message authentication code (MAC) is tied to the ciphertext, limitations of the conventional system are discussed, analyzed and presented. In our proposed system, an improved security service can be performed to impose better security services where needed.

An introduction about the proposed system, process of the proposed system, proposed system diagram, encryption algorithm and decryption algorithmic process of the proposed system are analyzed and presented.

The security mechanisms needed to cope with unwanted access fall into different basic security services and they are confidentiality, authentication, integrity checking and non-repudiation. Security services are implemented by security policies and then are implemented by security mechanisms. In this chapter, a comparative study between the conventional system and the proposed system for message authentication and confidentiality checking through authentication code tied to ciphertext has been performed and presented.

Any improved process is desired for the betterment of the security services of the secured electronic transaction system. In this chapter, a comparative analysis has be done and presented with clear comparison between the conventional system and the proposed system. The comparison of the security systems is performed on the fundamental security services which are confidentiality, authentication, integrity checking and non-repudiation.

7.2 Conclusions

An improved message transaction technique has been designed, developed and implemented using Java programming language. It performs stronger authentication of the message transaction and preserves better confidentiality checking services. For this process, first message is encrypted with a secret key K_1 to produce MAC, which is concatenated with the message and again encrypted with another secret key K_2 and again encrypted the output with key K_1 that builds the ciphertext that is to be sent to the destination. In the receiving end, first decryption is performed with the secret key K_1 and then again decrypted the output with the secret key K_2 that produces the message and the MAC of the message, and then the message is only decrypted to produce message authentication code MAC'; and the new MAC' is compared with received message authentication code MAC, to ensure the authentication of the message. In this method, key values that are used for encryption / decryption ensure the stronger authentication, and crossed application of the two keys K1 and K2 for performing encryption-decryption establishes the stronger confidentiality of the communicating message. It can be applied where higher-level of security services of the communicating messages are needed.

7.3 Future Works

In the current era of electronic communication, message security issues are the top and central concern and thus are in high demand. Security of message in electronic transactions fully relies on the key value of the cryptosystem and also the different cryptographic techniques. So the key generation techniques, Cryptographic mechanisms and the cryptographic policies for security services are the concern areas as the future works. Following are the cryptographic areas of the research.

- Key Generation for cryptographic application in the transaction of
    - E-commerce,
    - E-payments,
    - E-banking,
    - E-transactions,
    - E-marketing,
    - E-management,etc.
- Group Key Generation
- Key Distribution without the third party
- Group key exchange, etc.

The following areas can be considered as the further area of research: Electronic Funds Transfers (EFT), whose short term security is essential but whose exposure is brief. A company's strategic corporate plans, whose confidentiality must be preserved for a small number of years; a proprietary product that needs to be protected over its useful life, often decades, and information private to an individual, medical condition, employment evaluation that may need protection for the lifetime of the individual.

REFERENCES

[1] Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security Private Communication in a Public World", 2nd Edition, 2003, ISBN: 81-7808-790-1.

[2] Behrouz A. Forouzan, "Cryptography & Network Security", 1st Edition, 2007, ISBN-13: 978-0-07-066046-5. Accessed on January 05, 2011.

[3] William Stallings, "Cryptography and Network Security – Principles and Practice", 4th Edition, 2006, ISBN: 978-81-203-3018-4.

[4] Bruce Schneier, "Applied Cryptography", 2nd Edition, 2003, ISBN: 9971-51-348-X.

[5] Wikipedia, http://en.wikipedia.org/wiki/Initialization_vector, Accessed on December 02,2010.

[6] Wikipedia, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, Accessed on December 03,2010.

[7] Citrix Product, http://support.citrix.com/proddocs/index.jsp?topic=/access-gateway-46/ag-appendix-types-cryptography-con.html, Accessed on December 12, 2010.

[8] Crypt::C,http://search.cpan.org/~lds/Crypt-CBC-2.12/CBC.pm#LIMITATIONS , Accessed on December 22, 2010.

[9] 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.

[10] 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.

[11] C. Kaufman, R. Perlman and M. Speciner, "Network Security Private Communication in a Public World", Second Edition, Pages: 406-407, ISBN 81-7808-790-1, Indian Reprint, 2003.

[12] C. Radu, "Analysis and Design of off-line Electronic Payment Systems", Ph.D Thesis.

[13] A. Menezes, P. Van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Inc., 1997.

[14] B. Schneir, "Applied Cryptography", John Wiley, ISBN: 9971-51-348-X, Pages: 169-180, 2nd Edition, 1996.

[15] M. Bellare and P. Rogaway, "Introduction to Modern Cryptography", Department of Computer Science and Engineering, University of California, San Diego, USA, November, 2002, Web: http://www-cse.ucsd.edu/users/mihir

[16] P.F. Syverson, "Adding Time to a Logic Authentication", Naval Research Laboratory, Washington, In the Proceedings of the First ACM Conference and Communication Security, Fairfax, Virginia, November, 1993.

[17] L. Weimin, Y. Zongkai, C. Wenqing and T. Yunmeng, "Research on the Security in Wireless Sensor Network", Asian Journal of Information Technology, Volume 5(3), Pages: 339-345, Medwell Online, http://www.medwellonline.net, 2006.

[18] A. C. Yao, "Theory and Applications of Trapdoor Functions", In the Proceeding of the 23rd IEEE Symposium on Foundations of Computer Science, Pages: 80-91, Chicago, 1982.

[19] R.W. Jones, "Some Techniques for Handling Encipherment Keys", ICL Technical Journal, 3(1982), Pages: 175-188, 1982.

[20] ACM Transactions on Information and System Security, August 1999, pp. 230-268.

[21] Advanced Encryption Standard (AES), FIPS 197, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, Nov. 2001.

[22] W. Küchlin, "Public Key Encryption," ACM SIGSAM Bulletin, August 1987, pp. 69-73.

[23] S. M. Bellovin and M. Merritt. "Encrypted Key Exchange: Password based protocols secure against dictionary attacks". In Proceedings 1992 IEEE Symposium on Research in Security and Privacy, pp: 72–84. IEEE Computer Society, May 1992.

[24] Menezes, A.J., van Oorschot, P.C., and Vanstone, S.A., "Handbook of Applied Cryptography", CRC Press, 1997.

[25] Kumar, I. Cryptology. Laguna Hills, "Certificate Authority", Aegean Park Press, 1997.

[26] Hankerson, D., Menezes, A., and Vanstone, S., "Guide to Elliptic Curve Cryptography", Springer, 2004.

[27] Kimmo J¨ arvinen "Studies on Efficient Implementation of Cryptographic Algorithms", Ph.D. thesis, Helsinki University of Technology

[28] Shai Halevi and Hugo Krawczyk, “Public-key cryptography and password protocols,” http://portal.acm.org/citation.cfm?id=322514

[29] W. Stallings, "Cryptography and Network Security", Principles and Practice, 3rd Edition, ISBN: 81-7808-902-5, Pearson and Education, 2003, 4th Indian Reprint, 2004.

[30] http://www.rsa.com/rsalabs/node.asp?id=2166

[31] http://java.sun.com/j2se.s

[32] http://www.asciitable.com

[33] A. Tanenbaum, "Computer Network", 4th Edition, 2003.

[34] B.A. Forouzan, "Data Communications and Networking", 3rd Edition, Tata-McGraw Hill, 2004.

[35] Crandall, R., and Pomerance, C. Prime Numbers: A Computational Perspective. New York: Springer-Verlag, 2001.

[36] Diffie, W., and Hellman, M. “Privacy and Authentication: An Introduction to Cryptography.” Proceedings of the IEEE, March 1979.

[37] Popek, G., and Kline, C. “Encryption and Secure Computer Networks.” ACM Computing Surveys, December 1979.

[38] Robshaw, M. Block Ciphers. RSA Laboratories Technical Report TR-601, August 1995.

[39] Bellare, M, and Rogaway, P. “Optimal Asymmetric Encryption: How to Encrypt with RSA.” Proceedings, Eurocrypt ’94, 1994.

[40] Denning, D. Cryptography and Data Security. Reading, MA: Addision-Wesley, 1982.

[41] Gollmann, D. Compuer Security. New York: Wiley, 1999.

[42] Javitz, H., and “Valdes, A. “The SRI IDES Statistical Anomaly Detector.” Proceedings, 1991 IEEE Computer Society Symposium on Research in Security and Privacy, May 1999.

[43] Merkle, R., and Hellman, M. “On the Security of Multiple Encryption” Communications of the ACM, July 1981.

[44] Koblitz, N. Acourse in Number Theory and Cryptography. New York: Springer-Verlag, 1994.

[45] 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.

[46] M. Ismail Jabiullah, Shamima Ahsan, ANM Khaleqdad Khan and M. Lutfar Rahman, "Emerging Applications of Cryptography in Bluetooth Networks", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 71, May 04-05, 2007.

[47] M. Ismail Jabiullah, Ahmed Fazle Rabbi and Shahida Rafique, "Privacy Mechanisms for Session Initial Protocol Message Over VoIP", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 71, May 04-05, 2007.

[48] M. Ismail Jabiullah, ANM Khaleqdad Khan and M. Lutfar Rahman, "Secured Session-key Distribution through Prime Field Elliptic Curve Cryptography", In the Proceedings of the Annual Conference, Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, Page: 73, May 04-05, 2007.

[49] 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.

[50] Md. Monowar Hossain, Anisur Rahman, Sydul Islam Khan, **M. Ismail Jabiullah** 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.

[51] Md. Monowar Hossain, Anisur Rahman, **M. Ismail Jabiullah** and M. Lutfar Rahman, *"CBC-Based Cryptographic Technique for Secured Message Transactions",* International Conference on Physics of Today, held at 15-16 March 2012, at Central Auditorium, Bangladesh University of Engineering and Technology (BUET), Dhaka-1000, Bangladesh, SSI-VI-A 04, Page: 86.

[52] 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

[53] Sydul Islam Khan, Md. Alamgir Kabir, Md. Ismail Jabiullah and M. Lutfar Rahman, "Study of the Message Authentication Techniques for Secured Electronic Transactions", Proceedings of the National Seminar on Electronics and ICT for National Development organized by Bangladesh Electronics Society (BES), Dhaka, Bangladesh on 3-4 October, 2012.

[54] M. Ismail Jabiullah, Taposhi Rabeya, A.N.M. Khaleqdad Khan and M. Lutfar Rahman, "A Novel Key Distribution Approach through Certified Authority", In the Proceedings of the National Conference on Electronics, Information and Telecommunication, Rajshahi University, Rajshahi, Bangladesh, A-125, ISBN: 984-300-000645-7, Page: 201, June 29-30, 2007.

[55] A.N.M. Khaleqdad Khan, M. Ismail Jabiullah, Rosy Sharmin and M. Lutfar Rahman, "A Trusted-Based Novel Approach for Secured Mutual Distributions of Session-key and Message", In the Proceedings of the National Conference on Electronics, Information and Telecommunication, Rajshahi University, Rajshahi, Bangladesh, A-132, ISBN: 984-300-000645-7, Page: 206, June 29-30, 2007.

[56] M. Ismail Jabiullah and M. Lutfar Rahman, "Approaches of Session-key Generations for Secured Electronic Transactions", In the Proceedings of the National Conference on Electronics, Information and Telecommunication, Rajshahi University, Rajshahi, Bangladesh, A-132, ISBN: 984-300-000645-7, Page: 194, June 29-30, 2007.

Some Other Instruction

Thesis/Project Size: 50-60 page limit for Bachelor program

70-80 page limit for Masters Program

Page Setup: Left- 1.25"

Right-1.25"

Top: 1.0-1.25"

Bottom-1.0-1.25"

Orientation- Portrait

Paragraph Line Spacing: 1.5
Font: Time New Roman
Header: Bold, Capital letter, Alignment-Center, Font-14
Inner Text: Font-12, Plain text
Figure caption: Font-12, Bottom, Center
Table caption: Font-12, Top, Left
Reference: Font-11 [1] *Author, "Paper Title", Conference/Journal, Volume, page number, Month Year* ; [2] *Author, Book Title, Publisher, Volume, page number, Month Year;* [3] *web site address;*