A KEY DISTRIBUTION TECHNIQUE WITH STRONG AUTHENTICATION

BY

SABA TASNIM
ID: 192-25-771

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

JULY 2020

APPROVAL

The Thesis titled "**A Key Distribution Technique with Strong Authentication**" submitted by Saba Tasnim, ID No: 192-25-771 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 presentation has been held on9th July 2020.

BOARD OF EXAMINERS

Dr. Syed AkhterHossain **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Zahir

Gazi Zahirul Islam **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Abdus Sattar **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Saddam

Dr. Md. Saddam Hossain **External Examiner**
Assistant Professor
Department of Computer Science and Engineering
United International University

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:

Saba Tasnim

Saba Tasnim
ID: 192-25-771
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

To begin with, I express my heartiest thanks and gratefulness to all-powerful Allah (God) for His ideal blessing makes me possible to complete the M.Sc. proposition adequately.

I incredibly grateful and wish my critical my commitment to Dr. Md. Ismail Jabiullah, Professor, Department of CSE Daffodil International University, Dhaka. Significant Knowledge and obvious interest of my chief in the field of "Cryptography and Information Security" to finish this hypothesis. His ceaseless ingenuity, keen course, constant help, consistent and vivacious oversight, accommodating investigation, significant direction, scrutinizing various unsatisfactory draft and redressing them at all stage have made it possible to complete this suggestion.

I should offer my heartiest gratitude to Dr. Syed Akhter Hossain, Professor and Head, Department of CSE, for his mindful help to finish my proposition and moreover to other worker and the staff of CSE division of Daffodil International University.

I should thank my entire course mate in Daffodil International University, who took part in this discussion about while completing the course work.

Finally, I ought to perceive with due respect the predictable assistance and patients of my people.

ABSTRACT

In current correspondence age, security of electronic message exchange is the excitement of time. It is usually head in different edges. Right now a huge amount of secure information is transmitted over the open system or web or other correspondence channels typically. Without solid check, we can't shield this fragile data from toxic ambushes. Starting at now, it is principal stress to compel additional security organizations to the passing on message, correspondence channel and granting individuals. For this, an unmatched framework for electronic message exchange structure has been made C# programming language. It performs electronic message exchanges with all the key flow security necessities, which are secret, unwavering quality, attestation and non-renouncement for both offering message and passing on people. To do this, unmistakable cryptographic encryption and unraveling systems are utilized to the passing on messages. From the earliest starting point message is scrambles with the private key of sender PRa and the yield is again encodes with a shared puzzle key Ks that makes cipherext, this normal riddle key Ks that makes a code that fills in as message authenticator known as MAC, which is interfaces with the ciphertext and again encodes them with shared secret key Ks that fabricates the new cphertext, which is again scrambles with the finder's open key PUb to last ciphertext that will be send to the intendent recipient. In the not actually alluring end, to recover the message, beneficiary from the earliest starting point unravels the got data with his private key PRb and again unscrambles with the normal riddle key Ks that gives the ciphertext and MAC of the ciphertext, and affirmation just unwinds the MAC to make another ciphertext′ and multifaceted nature the new ciphertext′ and they got ciphertext that guarantees the ciphertext endorsement comparably as message check; on the off chance that ciphertexts are discovered same, by then interprets the ciphertext with shared secret key Ks and again translates with the sender open key PUa and recover the message; in any case dispose of it. This system can be applied any place of electronic exchanges an ensured way.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Introduction:

Solid confirmation is the strategy by which a master gets trust in the character of a correspondence accessory. Despite the way that major to enrolling practice, substance affirmation for the coursed condition lays on no satisfactory ordinary foundations. This is in excess of a scholastic protest; solid confirmation is where an easygoing approach has as often as possible lead to work which is considerably under the least positive conditions wrong, and, most ideal situation just for the most part analyzable. It is along these lines appealing that trust in a confirmation show ought to begin from more than a few people's feebleness to break it. In all honesty, each basic substance affirmation objective should be authoritatively described and any up-and-comer show should be exhibited to meet its goal under a standard cryptographic assumption. When in doubt, the solid validation process is joined with the assignment of a "meeting key" which the passing on associates may later use for message security, trustworthiness, or whatever else. This "confirmed key dispersion" objective might be considered significantly more significant practically speaking than the unadulterated solid confirmation objective. [1] As an issue, it is ambushed with the identical fundamental difficulties as the solid confirmation issue of which it is an extension. Affirmation and approved key dispersal issues arrive in a wide scope of flavors: there may be two get-togethers included, or more; the confirmation may be uneven or normal; social occasions may (the symmetric case) or may not (the awry case) share a mystery key. Here we revolve around two adjustment of the two-party, normal, symmetric case.

Our essential worry in this theory is to force a solid verification key circulation place which ensures that electronic data trade properly sends and got past the problematic direct in a secured way.

1.2 Motivation:

Electronic message exchange is the interest security in present day correspondence age. It is generally basic in different perspectives. Right now a lot of delicate information is transmitted over the open system or web or other correspondence channel every day [2]. System administration going to day is extremely wide. [3]. System application framework used to distinguish validation. So we can't ensure significant data without solid security. Right when servers check themselves to customers, open key confirmation gives a better affirmation than the server the customer expected to interface with a toxic customer can't act like a validate cut off without securing that servers have key. Science the customer would somehow be forewarned that the host unmistakable verification had changed [4]. Message imparting over the open system condition is presently in defenseless circumstance. To perform secure message exchange over the unprotected World Wide Web organize, there are numerous instruments are accessible. Right now, it is principle worry to force extra security administrations to the imparting message, correspondence channel and conveying members. In this postulation, our anxiety is creating validation framework about key circulation framework with solid confirmation which give privacy, trustworthiness and verification, Electronic business, Chip-based installment cards, Digital monetary standards, Computer passwords, and Military correspondences framework need solid verification.

Which utilized key appropriation method. Offer significant help in our everyday monetary and social framework.

1.3 Relational of the Study:

In the electronic correspondence age security is the prime idea in various perspectives. The electronic correspondence channel is weak against the affirmation based data trade. The affirmation of security of data much demandable to overcome the current issue. The arrangement holds the use of key dispersion place (KDC) that share a riddle key with each customer and movement secret gathering keys encoded with the expert key. An open key arrangement is used to spread the pro keys. Approval key deal with the issue of the checking keys of the person to whom some other individual taking to or endeavoring to talk. Cryptographic strategies are used to ensure the affirmation of electronic message trades. To do this, cryptographic fixings, cryptographic estimation, cryptographic instruments confirm term will be inspected, examined and made sense of it. Strong approval structure will be perused and obliged key transport organizations will be perceived and made sense of it. The purpose of this hypothesis is to propose a prevalent procedure for strong affirmation data trade with favored security benefits over the standard structure using cryptographic encryption and unscrambling process in key allotment system.

1.4 Research Questions

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

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

Q.3: How to perform strong authenticate encryption-decryption?

Q .4: How to implement the system?

1.5 Expected Output:

In this theory, we will attempt to force solid confirmation to imparting electronic information or message through cryptographic key dispersion open key encryption-unscrambling process.

Our principle point of this postulation is to guarantee solid validation of electronic information or message over the open key appropriation without permitting access to an assailant.

1.6 Report Layout:

This proposal report created five sections. The principal section is the Introduction, wherein examined about the inspiration and method of reasoning of the examination. This section additionally incorporates research questions, anticipated yield and report format at long last.

The Chapter 2 Background, which features the cryptographic foundation and regular frameworks. This part comprises of nine segments and they are presentation, validation forms model, key dispersion process age, mystery key cryptography, confirmation draws near, verification information move and

Resuscitated. Validate information checking by key appropriation forms. Confinement of the confirmation forms framework and rundown.

The Chapter 3 Research Methodology, in which represents of this examination. This part formed with six areas they are presentation, forms depiction of the proposed framework, key circulation encryption-unscrambling procedure and graphs of the proposed framework, calculation of the proposed framework, bit by bit stream chart of the proposed framework and synopsis.

The Chapter 4 is Experimental Results and Discussion, this part features the test results and framework validation. There are four area in this part, which are presentation, test results, elucidating examination, and synopsis.

The Chapter 5 is Impact society condition and maintainability.

The last one Chapter 6 is Summery, end, suggestion and Implication for future examination.

CHAPTER 2
BACKGROUND

2.1Preliminaries

Cryptography is connected with the path toward defending data and trades by encryption and decoding with key(s) so simply the affirmed customers can peruse and process it. Present day cryptography subject to complex numerical estimation and set of rules which are viewed as frameworks or counts to change message that are hard to comprehend.

2.2 Related Works

By and by a day's present cryptography uses the distinctive cryptographic terms. A portion of the accompanying cryptographic terms are utilized in this venture; Plaintext or comprehensible Data, Encryption Algorithm, Encryption Key, Cipher text, Decryption Algorithm, Decryption Cryptography, Cipher, key, Public key, Private key, Encryption , Deciphering , Decryption , Cryptography, Cryptanalysis, Cryptology, Code, Steganography, Digraphs, Homophones, Mono Alphabetic Substitution, Poly Alphabetic Substitution, Nomenclature, Null, Symmetric-Key cryptography, Public Key cryptography, Key dissemination Center, Authentication, Authorization, Substitution, Transposition, Hashing, Digital mark.

Plaintext or Clear text: The first message or information that can be straightforwardly comprehend by human or machine. Plaintext or Clear content is utilized as contribution to the encryption calculation and it tends to be in type of text, sound, video, picture and biometrics moreover.

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

Key for Encryption: Key fed in tothe 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 algorithm.

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

Key for Decryption: 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 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 human 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 with prior knowledge of the algorithms or keys used. This is done by the receiver.

Cryptography: Cryptography is the investigation of standards and procedures of changing over Intelligible Message into Unintelligible structure that is mixed up to people and machine; and afterward recouping that Plaintext from Cipher text that is its unique from. Figure 2.1 Shows Cryptographic System.

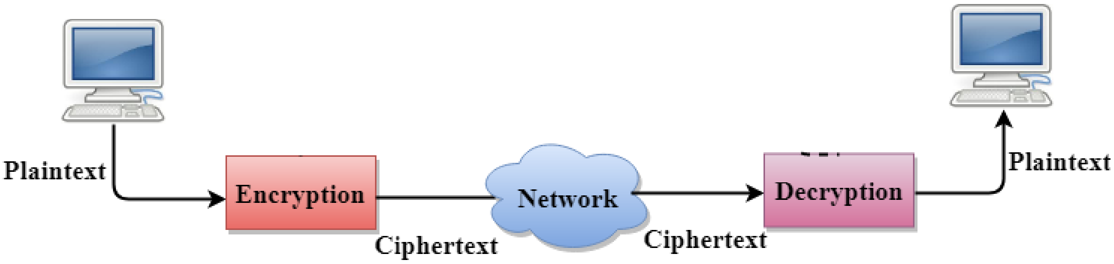


Figure 2.1: A Cryptographic System

Cryptanalysis: Cryptanalysis is the investigation of the rule and procedures of recuperating Plaintext from Cipher text without knowing the calculation the or keys utilized.

Cryptology: The investigation of both Cryptography (Enciphering and Deciphering) and Cryptanalysis (Codebreaking or Cracking a figure framework 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 way toward hiding a record, message, picture or video inside another document, message, picture or video.

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

Public Key Cryptography: It is otherwise called uneven key cryptography is a cryptographic framework that utilizes two keys. The keys are scientifically connected, however not same, an open key which might be known by anybody where the private key is just known to the beneficiary. The open key is utilized for encryption where private key is for decoding. Figure 2.2 Shows Public Key Cryptography System:

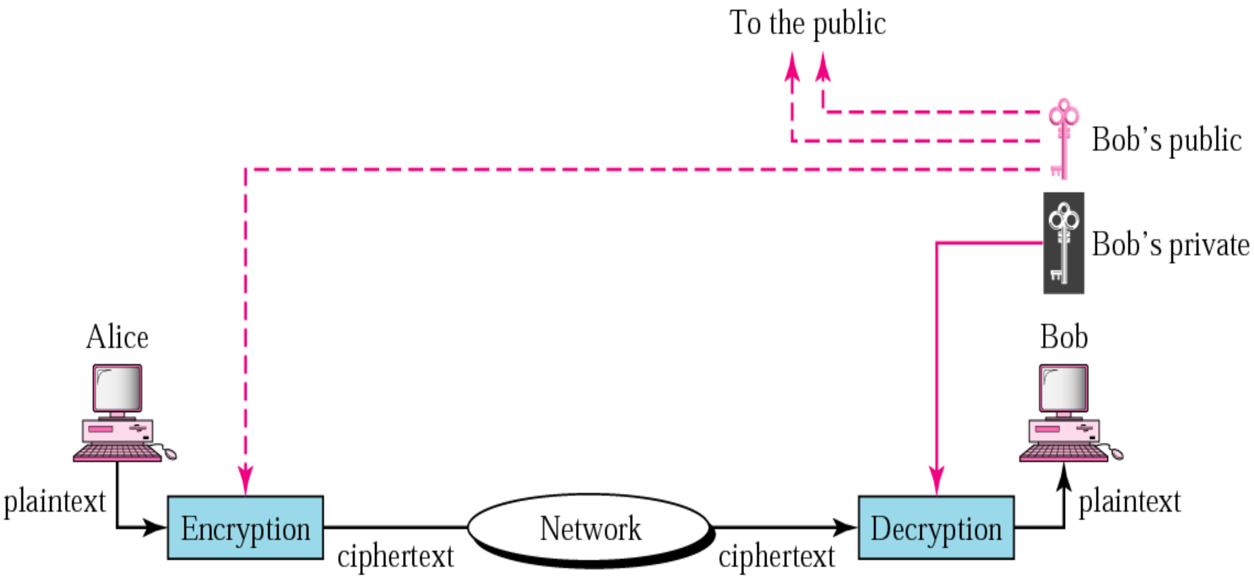


Figure 2.2: A Public Key Cryptography

Private key Cryptography: A Private-key cryptography or Single-key cryptography otherwise called Symmetric-key cryptography utilizes one key shared by both sender and collector. This normal key is utilized for the two encryptions of the Plaintext and decoding of the Cipher text. Figure 2.3 Shows Private Key Cryptography System.

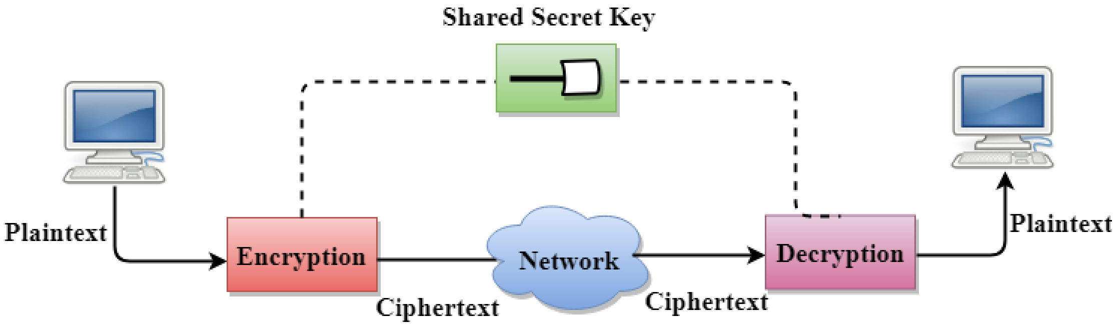


Figure 2.3: A Private Key Cryptography

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 message.

Key Distribution Center: A key distribution center (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data.

Authorization: Approval is a security component used to decide client/customer benefits or access levels identified with framework assets, including PC programs, records, administrations, information and application highlights. Approval is typically gone before by validation for client character check.

Authentication: Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. Identification phase provides a user identity to the security system.

Hashing: A hashing algorithm is a cryptographic hash function. It is a mathematical algorithm that maps data of arbitrary size to a hash of a fixed size. It's designed to be a one-way function, infeasible to invert.

Digital signature: Computerized marks are the open key natives of message validation. In the physical world, it is entirely expected to utilize written by hand marks on manually written or composed messages. Advanced mark is a cryptographic worth that is determined from the information and a mystery key known uniquely by the endorser.

2.3 Comparative Analysis and Summary:

Key distribution model of a secure strong authentication using symmetric encryption or public key authentication. A public key encryption system has five components. Shows in Figure 2.3.1

Plaintext: The first data or information that can be legitimately comprehended by people or machines. Plaintext or Clear content, which is utilized as a contribution to the encryption calculation and it tends to be in the type of content, sound, video, picture, and biometrics too.

Encryption algorithm: It is the complex numerical strategy that takes the clear message and an Encryption key as information and produces unintelligible message as output.

Secret Key: A key is a worth or some basic data that is taken care of into the algorithm to changing intelligible information into cipher text and returning cipher text to intelligible data. The key is just known to the correspondence parties.

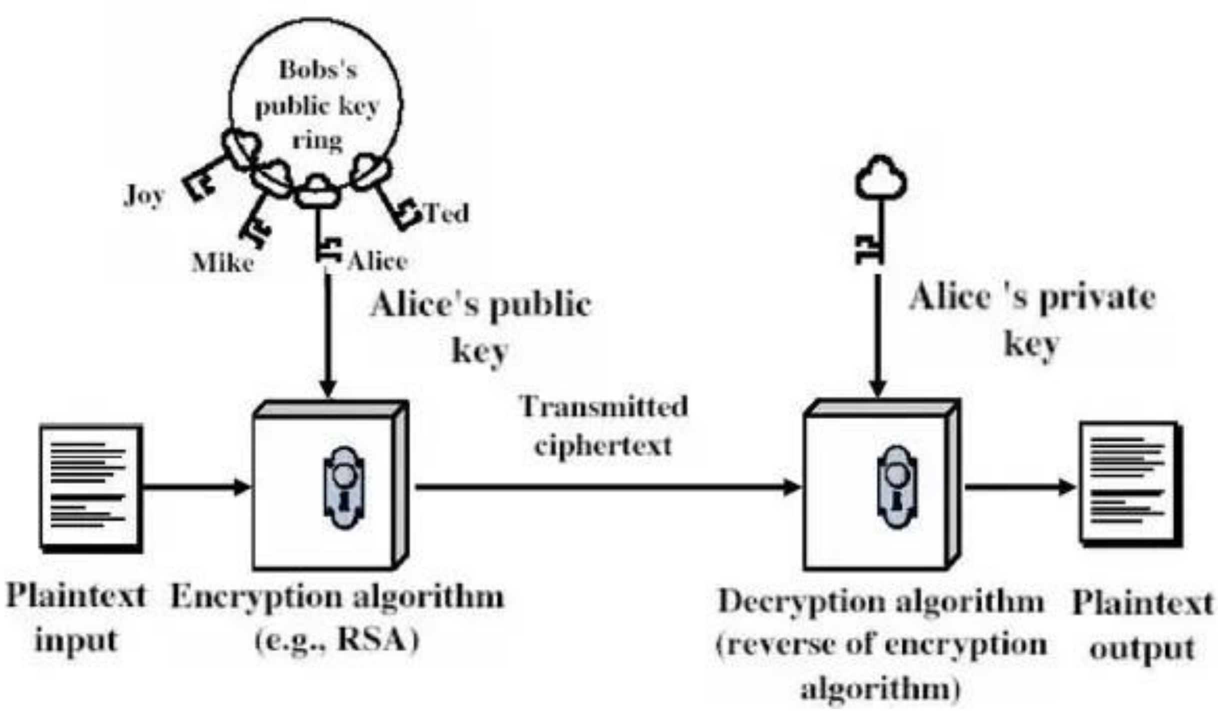


Figure 2.4: Simplified Model of Public Key Encryption

Cipher text: The transformed information that cannot directly understand by human or machine without knowing the algorithm or secret by used. It is the incomprehensible output of the encryption algorithms.

Decryption algorithm: It is fundamentally the encryption procedure execute backward. It takes incoherent Data and same key as info and gives starting understandable information as yield.

There are two necessary prerequisites for Key appropriation secure utilization of symmetric encryption:

1.First we require a solid encryption calculation. In any event, we would pick the calculation to be to such an extent that an aggressor ought not be proficient to decode the incomprehensible data or discover the key; regardless of whether assailant knows the calculation and acquire at least one figure text.

2.The sender and the beneficiary probably obtained the duplicates of mystery key in a safe manner and key must be left well enough alone. On the off chance that this key is revealed, interchanges are undermined.

2.3.1 Key Distribution Center (KDC):

A typical action with a KDC incorporates a requesting from a customer to use some assistance.

- The KDC will use cryptographic techniques to check referencing customers as themselves. It will in like manner check whether an individual customer has the benefit to get to the organization referenced.

- On the remote possibility that the confirmed customer meets each suggested condition, the KDC can give a ticket permitting access.

- KDC generally work with symmetric encryption. In most (yet not all) cases the KDC bestows a key to all of the different social occasions.

- The KDC produces a ticket subject to a server key.

The customer gets the ticket and submits it to the proper server. The server can check the submitted ticket and award access to the client submitting it.

2.3. 2 Key Distribution Working Process:

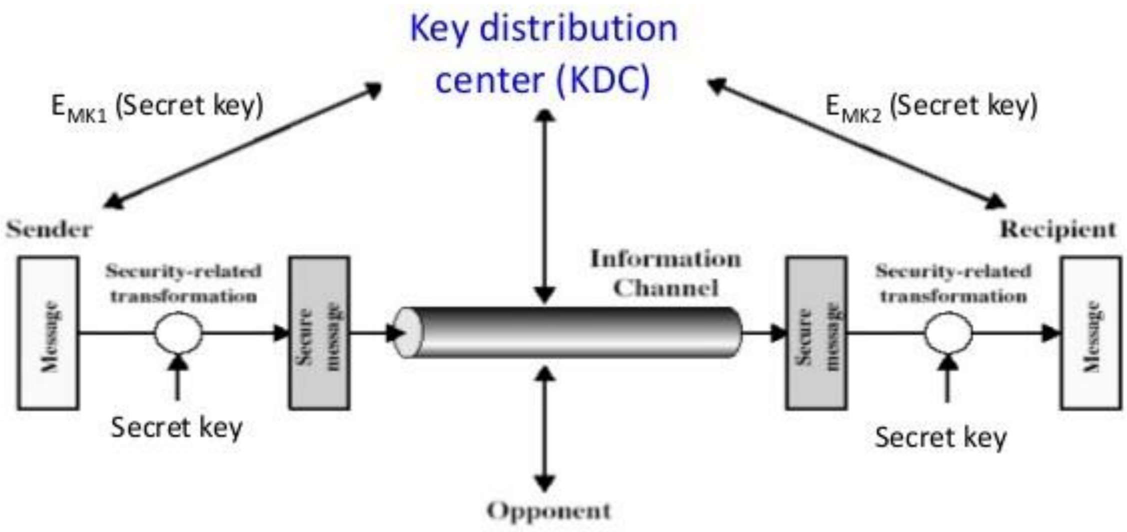


Figure 2.5: KDC working processes

2.3.3 Symmetric Key Encryption with KDC:

The nature of any cryptographic system rests with the key flow strategy, a term that insinuates the strategies for passing on a key to two social affairs who wish to exchange data without allowing others to see the key. For two social affairs A and B, key spread can be cultivated in different habits, as follows:

- A can choose a key and genuinely convey it to B.
- A outsider can choose the key and genuinely convey it to A and B.
- If A and B have beforehand and as of late utilized a key, one gathering can transmit the new key to the next, scrambled utilizing the old key.
- If A and B each has an encoded association with an outsider C, C can convey a key on the scrambled connects to A and B.

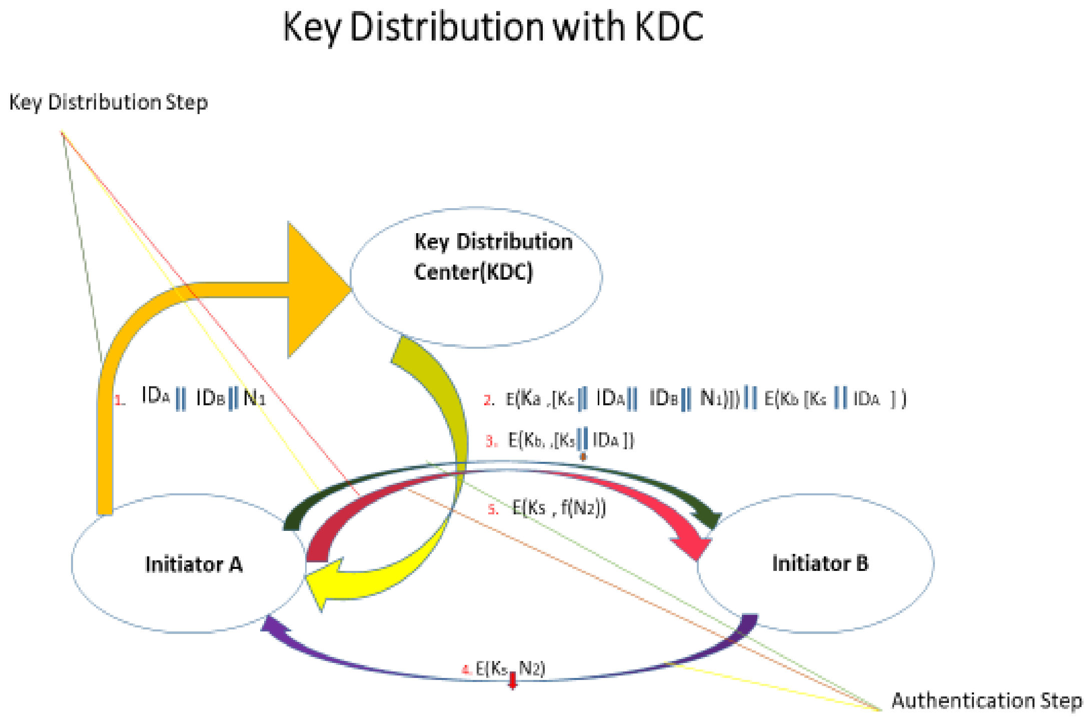

Key Distribution with KDC
Key Distribution Step
Key Distribution Center(KDC)
1. $ID_A || ID_B || N_1$
2. $E(K_a ,[K_s || ID_A || ID_B || N_1]) || E(K_b [K_s || ID_A])$
3. $E(K_b, ,[K_s || ID_A])$
5. $E(K_s , f(N_2))$
Initiator A
Initiator B
4. $E(K_s, N_2)$
Authentication Step

Figure 2.6: Symmetric key encryption technique with KDC

2.3.4 Strong Authentication Processes by KDC:

Solid verification is the strategy by which an expert in a scattered structure gains gather in the character of a correspondence accomplice. When in doubt, the solid validation process is joined with the transport of a \session key" which the assistants can later use for message classification, trustworthiness, or whatever else. These are central issues in handling practice, for without their objectives scattered figuring can't for all intents and purposes get the ground.

However solid confirmation for the disseminated condition lays on no agreeable proper establishments. This is in excess of a scholastic grumbling. We are talking about a region in which a casual methodology has frequently lead to work which is at the very least off-base, and, best case scenario just in part analyzable. Specifically, a disturbing division of proposed verification conventions have in this manner been seen as awed. It is in this way attractive that consolidate in a verification convention should originate from in excess of a couple of individuals' failure to break it. Indeed, in the custom of provable security examined over, each noteworthy substance confirmation objective ought to be officially characterized and any applicant convention ought to be demonstrated to meet its objective under a standard cryptographic supposition. Obviously the definition should appropriately demonstrate this present reality attributes of the current issue, the conventions must be viable, and the evidences must be \meaningful" for training. [4].

2.3.5 Secret key Generation:

The key age strategy is the methodology of making key in cryptography. A key is utilized by the sender to scramble information and by the collector to decode information. A gadget or program which is utilized to make keys is called key generator. Present cryptographic frameworks include symmetric-key calculations like AES and DES and open key calculations like RSA. Symmetric-key calculations utilize a mystery single key shared distinctly between imparting parties for keeping information secure. Open key calculations utilize two keys one open key and one private-key. The open key might be known by anyone and private key is stayed discreet [1] [3].

In PC cryptography utilizes whole numbers for create keys. At times keys are created arbitrarily utilizing an arbitrary number generator (RNG) or pseudorandom number generator (PRNG).

The most straightforward procedure to peruse incomprehensible encoded message or data without really unscrambling it is called savage power assault; basically attempting each number, up to the greatest size of the key. Along these lines, it is basic to utilize an adequately huge key size; bigger keys take exponentially longer to assault, rendering a savage power assault isn't viable. Present-days, the symmetric key calculations are generally utilizing 128 bits in length key and open key calculations utilizes the key lengths of 2048 bits.

2.3.6Secret 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 2.8:

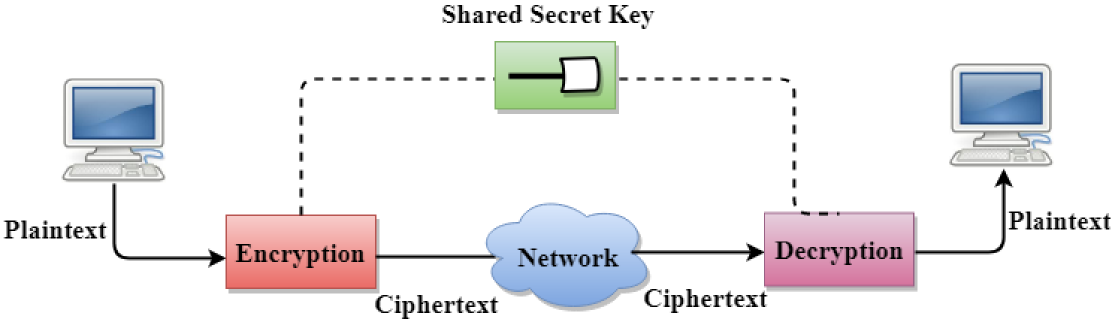


Figure 2.7: Secret Key Cryptography

Before any confused encoded data can be sent over the open system, both sender and collector must have the key and concede to the cryptographic calculation that they will requirement for encryption and decoding.

The most concerning issue with private key cryptography is key spread; how to get the key starting with one assembling then onto the next without permitting access to an aggressor. Right when the puzzle key flow issue is understanding, it might be a dependable gadget. The count ensures more grounded security and speedier encryption.

Summary:

In this chapter, cryptography, cryptographic terms, cryptography component, Key distribution, symmetric encryption and the secret key cryptography are reviewed and presented. And the last section of this chapter, conventional approach with key distribution, conventional key distribution with message authentication and confidentiality checking, Identified Limitations of the Conventional System with KDC, analyzed and presented.

2.4Scope of the Problem of the Conventional System with KDC

Ordinary framework for message validation and privacy has been minded to perceive its points of interest, impediments and applications. After audit the ordinary frameworks a few constraints are distinguished, which are summed up beneath:

- **Encryption-Decryption with a Single Key:** In this strategy, to make message check code (MAC), a typical single mystery key is utilized for encryption in the sender end and a comparative key unscrambling in the collector end. If the wrongdoing key is single key uncovered the security of the structure may be at serious risk and exchanges are undermined. The structure arrangement totally relies upon the key utilized for encryption-decoding in the security system.
- **Message is not Encrypted with Stronger Way:** The regular framework for message validation and privacy, encode the message one opportunity to convey ciphertext and scramble to create the MAC, which is interface with the ciphertext and straightforwardly send to the sender. If the system makes another ciphertext after connection by scramble the information with another key and send it to the normal sender, by then the structure uses two keys for performing two unique encryptions that give the solid message verification and classification.

2.4 Challenges

Mystery key verification is the endeavor of one social occasion showing to another get-together that they share a similar key. The issue has starting late pulled in extensive energy in view of the nearness of lightweight conventions amiable to usage on basic models. Enhances the huge assemblage of work on mystery key verification in two unique manners. On the definition side, we show that the idea of dynamic security, the most grounded accomplished by existing lightweight shows, is unnecessarily weak and can be satisfied by shows absolutely unstable with respect to obviously significantly increasingly defenseless considerations. We give new, continuously skilled implications of dynamic security. Moreover, investigate relations among them, inside another general structure for fine-grained exhibiting of the security of mystery key verification conventions of autonomous premium. Our new definitions as long as they are viably secure in regards to the past one.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Research Subject and Instruction

A Key dissemination strategy with solid validation process for made sure about message exchange has been structured, created, actualized and examined.

3.1.1. Secret Key Distribution Analysis

In this framework, straightforward cryptographic encryption and unscrambling procedures are utilized to the conveying messages. In this framework sender A creates an open key pair {Pa, Pb} and transmits a message to beneficiary B comprising of PUa and an identifier of An, Ida. B creates a mystery key, Ks and transmits it to A, scrambled with An's open key. A figures D (PRa E (PUa ,Ks)) to recoup the mystery key .Because just An and B will know the personality of Ks. A disposes of PUa and PRa and B disposes of PUa.

3.1.2 Strong Authentication Analysis Technique in Key Distribution

3.2 Algorithms of the Proposed System or Data Utilization System:

In this proposed framework we use RSA calculation for solid verification. For this situation, A prepares a message to B and scrambles it using A's private key before transmitting it. B can unscramble the message utilize A s open key. Since the message was encoded using A's private key, only A could have orchestrated the message. The entire encoded message fills in as an automated mark. Moreover, it is hard to modify the message without access to A's private key, so the message is verified both viewing source and to the extent data trustworthiness. the entire message is encoded, which, albeit endorsing both maker and substance, requires a great deal of limit. Each report must be kept in plaintext to be used for reasonable purposes. A copy furthermore ought to be taken care of in ciphertext so the start and substance can be affirmed if there ought to emerge an event of a contest. An inexorably capable strategy for achieving comparative results is to encode somewhat square of bits that is a segment of the report. Such a square, called an authenticator, must have the property that it is infeasible to change the file without changing the authenticator. In case the authenticator is scrambled with the sender's private key, it fills in as an imprint that affirms beginning stage, content, and sequencing.

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 bellow.

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 encrypting with shared secret key K_s which produce a ciphertext.

Step 3: Ciphertext is again encrypts with another shared master key K_a and Kb that generates a message authenticator known as MAC.

Step 4: MAC is concatenating 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_s 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 ciphertext are found same, then decrypts the ciphertext 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.

3.3Statistical Analysis:

A mystery Key dispersion depends on solid security. It has been pointed. Out in a difficult situation in setting up establishments for element verification and validated key dissemination conventions has been the nonattendance of a proper correspondences model for confirmation in the conveyed condition I Here we determine such a model. To be totally wide, we expect that all correspondence among teaming up parties is under the adversary's control. Somebody can examine the messages conveyed by the get-togethers, give messages of her own to them, modify messages before they show up at their objective, and concede messages or replay them. Specifically, the foe can start up totally new "cases" of any of the social events, showing the limit of passing on administrators to at the same time partake in various gatherings immediately. Authoritatively, each gathering will be displayed by a limitless assortment of prophets which the enemy may run. Interface with the adversary, they never honestly partner with one another.

3.4. Proposed Methodology and Step by Step Mechanism:

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

Step wise flow diagrams of the proposed system:

Let us expect that client A desires to build up a logical connection with B and requires a one-time session key to secure the information transmitted over the association. A has an ace key, Ka, known uniquely to itself and the KDC; correspondingly, B shares the master key Kb with the KDC. The following steps occur:

Step 1: An issues a request to the KDC for a session key to ensure a logical connection with B. The message incorporates the character of A and B and an extraordinary identifier, N1, for this exchange, which we refer to as a nonce. The nonce might be a timestamp, a counter, or a random number; the base prerequisite is that it varies with each request. Likewise, to prevent masquerade, it should be difficult for an opponent to guess the nonce. Thus, a random number is a good choice for a nonce.

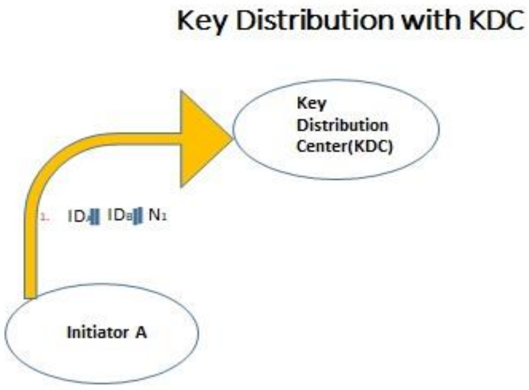


Figure 3.1: Sender send Value to the key distribution Center

Step2: The KDC reacts with a message encrypted using Ka Thus, A is the one in particular who can successfully read the message, and A realizes that it started at the KDC. The message incorporates two things proposed for A:

- The one-time session, Ks, to be utilized for the meeting

- The original request message, including the nonce, to enable A to coordinate this reaction with the appropriate request.

Along these lines, A can check that its original request was not changed before gathering by the KDC and, due to the nonce, this isn't a replay of some previous request. Moreover, the message incorporates two things proposed for B:

- The one-time session key, Ks to be used for the session
- An identifier of A (e.g., its system address), IDA

These last two things are encrypted with Kb (the master key that the KDC shares to B). They are to be sent to B to set up the association and demonstrate A's personality.

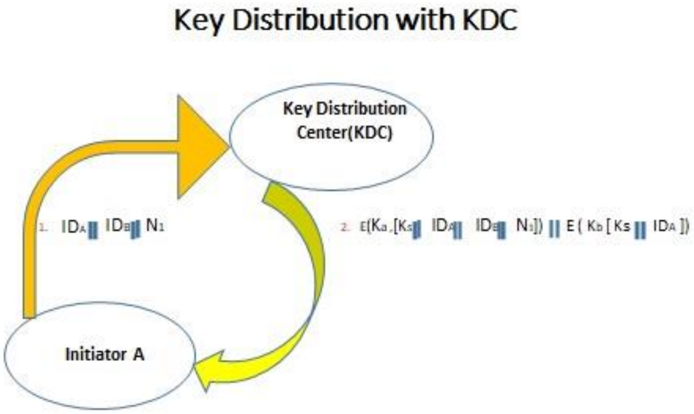

Key Distribution with KDC
Key Distribution Center(KDC)
1. $ID_A || ID_B || N_1$
2. $E(K_a, [K_s || ID_A || ID_B || N_1]) || E(K_b [K_s || ID_A])$
Initiator A

Figure 3 2: Key distribution Center Send Value to the sender A.

Step 3:A stores the meeting key for use in the best in class meeting and advances to B the information that began at the KDC for B, specifically, E (Kb, [Ks || IDA]). Since this information is encoded with Kb, it is shielded from tuning in. B by and by understands the meeting key (Ks), understands that the other party is A (from IDA), and understands that the information began at the KDC (in light of the fact that it is scrambled using Kb). Presently, a meeting key has been securely conveyed to An and B, and they may start their ensured trade.

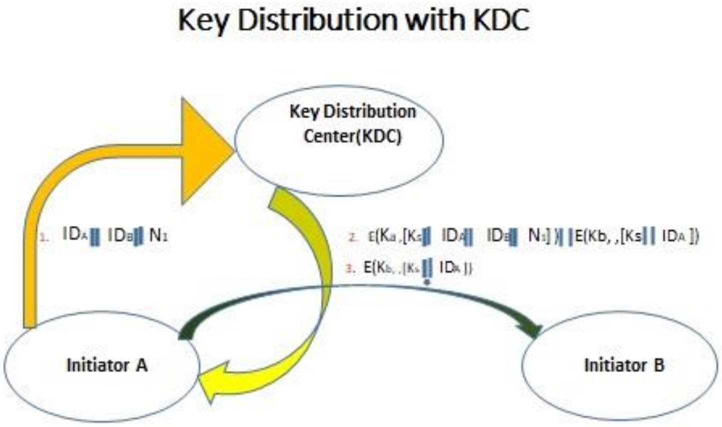

Key Distribution with KDC
Key Distribution Center(KDC)
1. $ID_A || ID_B || N_1$
2. $E(K_a, [K_s || ID_A || ID_B || N_1]) || E(Kb, , [Ks || ID_A])$
3. $E(K_b, , [K_s || ID_A])$
Initiator A
Initiator B

Figure 3.3: Sender A Send data to the Receiver B

Step 4: Using the recently printed session key for encryption, B sends a nonce, N2, to A.

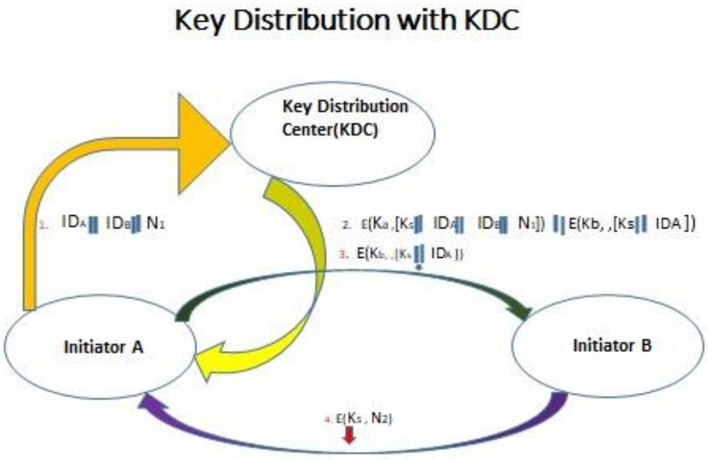

Key Distribution with KDC
Key Distribution Center(KDC)
1. IDA || IDB || N1
2. E(Ka ,[Ks || IDA || IDB || N1]) || E(Kb, ,[Ks || IDA])
3. E(Kb, ,[Ks || IDA])
Initiator A
Initiator B
4. E(Ks , N2)

Figure 3.4: Receiver B send request to the sender A.

Step5: Likewise using Ks, A responds with f(N2), where f is a limit that plays out some change on N2 (e.g., including one).

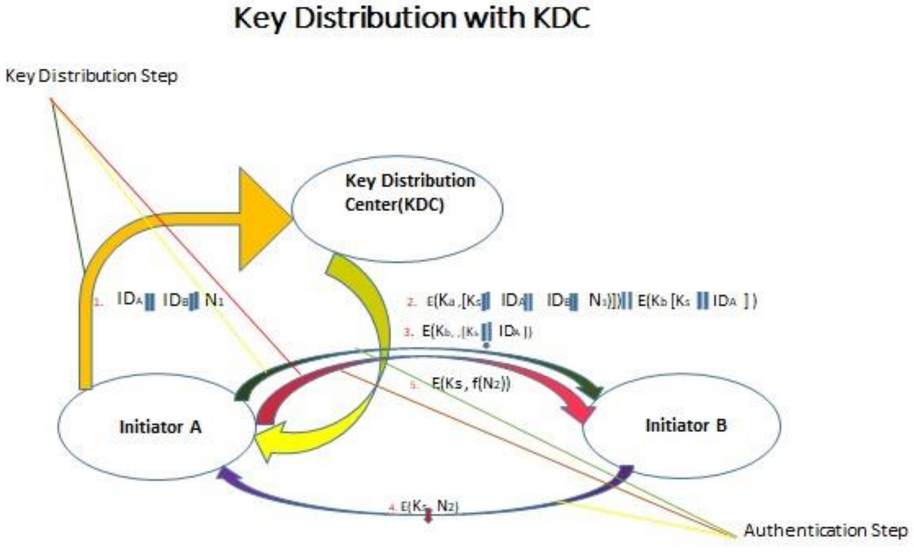


Figure 3.5: Process are all completed.

Note that the actual key distribution involves only steps 1 through 3 but that steps 4 and 5, as well as 3, perform an authentication function.

3.5 Implementation Requirements:

In this part, a presentation of the proposed framework, process portrayal, Secret key circulation examination, solid verification investigation strategy in Key Distribution, charts, encryption calculation and unscrambling calculation of the proposed arrangement of Key appropriation and validation are planned and illustrated.

Techniques:

Key appropriation with Symmetric Encryption.

- Encrypted and Decrypted key appropriation use RSA calculation.

- C# Programming Language use for programming age.

- Hardware security keys (additionally called security keys, U2F keys, or physical security keys) include an additional layer of security to your online records.

They ensure against computerized bots and focused on assaults by utilizing cryptography to check your character and the URL of a login page.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

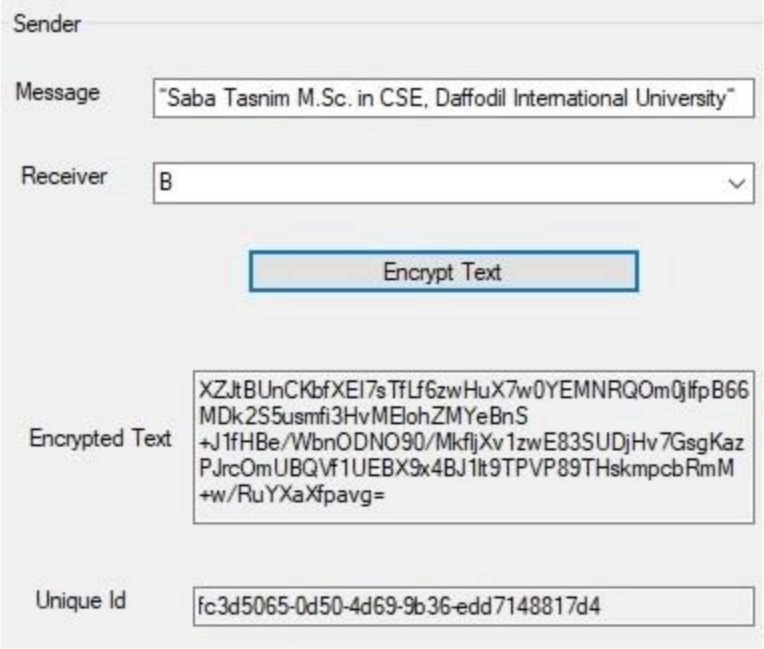
4.1 Experimental Setup:

Our proposed framework for made sure about message exchange has been created utilizing C# programming language. The fundamental point of our actualized framework is to guarantee key conveyance with solid validation for security of the imparting messages. The framework is mostly partitioned into two side one is sender end known as "Encryptor" and another is getting end, which is known as "Decoding". We additionally built up a key generator for produce RSA open private key pair. We run the framework ordinarily for various messages. Where sender send information or message and beneficiary acknowledge a similar message and got the message effectively. We found the consequences of the framework is acceptable.

4.2 Experimental Results and Analysis:

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

In our experiment, the intended message is “Saba Tasnim 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.



Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

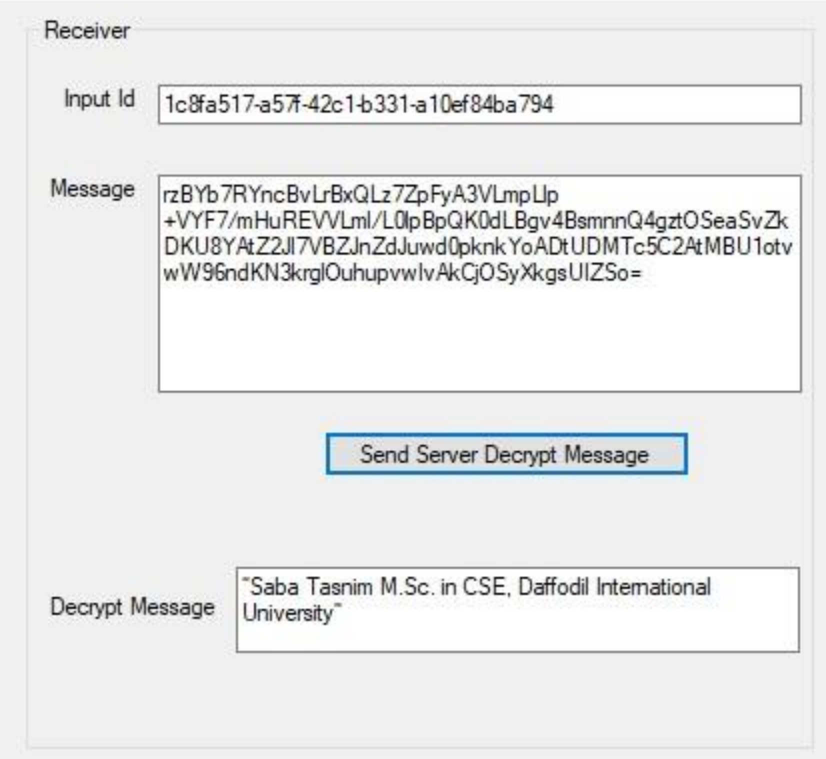
Receiver: B

Encrypted Text: XZJtBUnCKbfXEI7sTfLf6zwHuX7w0YEMNRQOm0jlfpB66
MDk2S5usmfi3HvMElohZMYeBnS
+J1fHBe/WbnODNO90/MkfljXv1zwE83SUDjHv7GsgKaz
PJrcOmUBQVf1UEBX9x4BJ1lt9TPVP89THskmpcbRmM
+w/RuYXaXfpavg=

Unique Id: fc3d5065-0d50-4d69-9b36-edd7148817d4

Figure 3.6: Sender Send Message to the Receiver

Message are send by any receiver B, C, D. After encryption using RSA algorithm Encrypted text are generated and also a unique ID is generated.



Input Id: 1c8fa517-a57f-42c1-b331-a10ef84ba794

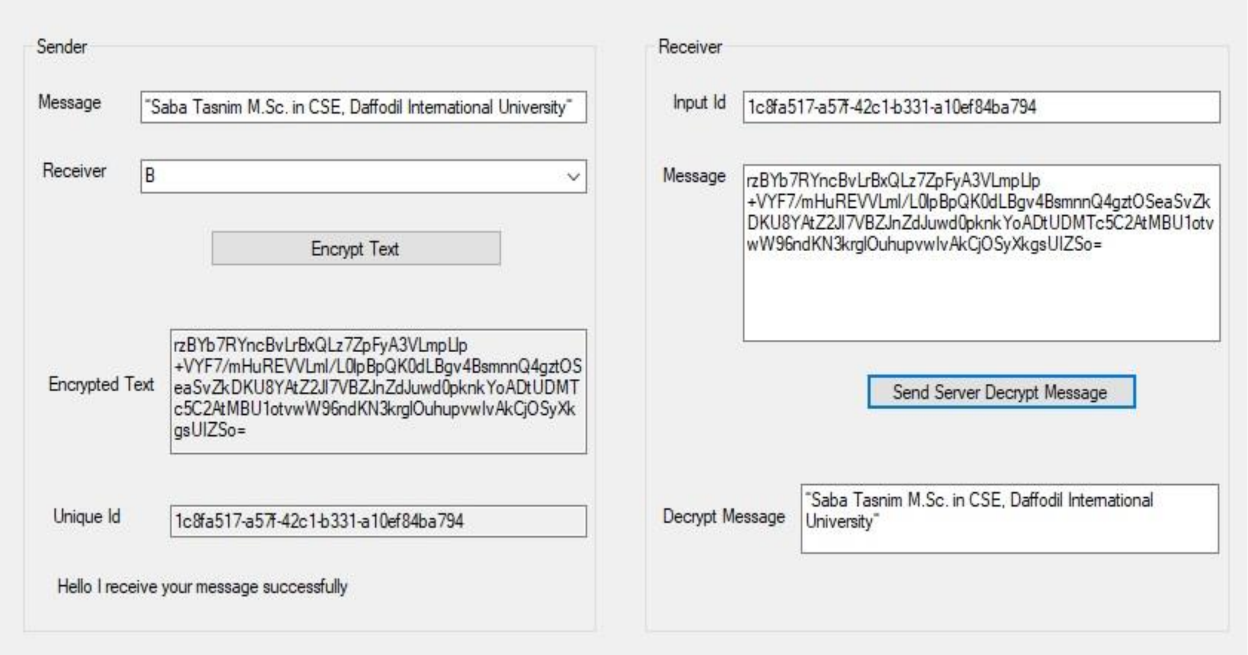
Message:

```
rzBYb7RYncBvLrBxQLz7ZpFyA3VLmpLlp
+VYF7/mHuREVVLml/L0lpBpQK0dLBgv4BsmnnQ4gztOSeaSvZk
DKU8YAtZ2Jl7VBZJnZdJuwd0pknkYoADtUDMTc5C2AtMBU1otv
wW96ndKN3krglOuhupvwlvAkCjOSyXkgsUIZSo=
```

Decrypt Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

Figure 3.7: Receiver Accept the same message.

In this system sender Unique ID is receiver Input ID. Sender encrypted message is receiver message. After decrypted the message by sender server same message is received by the receiver.


Sender

Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

Receiver: B

Encrypted Text:
rzBYb7RYncBvLrBxQLz7ZpFyA3VLmpLlp
+VYF7/mHuREVVLml/L0lpBpQK0dLBgv4BsmnnQ4gztOS
eaSvZkDKU8YAtZ2JI7VBZJnZdJuwd0pknkYoADtUDMT
c5C2AtMBU1otvwW96ndKN3krglOuhupvwlvAkCjOSyXk
gsUIZSo=

Unique Id: 1c8fa517-a57f-42c1-b331-a10ef84ba794

Hello I receive your message successfully

Receiver

Input Id: 1c8fa517-a57f-42c1-b331-a10ef84ba794

Message:
rzBYb7RYncBvLrBxQLz7ZpFyA3VLmpLlp
+VYF7/mHuREVVLml/L0lpBpQK0dLBgv4BsmnnQ4gztOSeaSvZk
DKU8YAtZ2JI7VBZJnZdJuwd0pknkYoADtUDMTc5C2AtMBU1otv
wW96ndKN3krglOuhupvwlvAkCjOSyXkgsUIZSo=

Decrypt Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

Figure 3.8: Message generated

Then the following system generate **Hello I received your message successfully**.

4.3 Discussion

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 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 framework from the outset scrambles the data with sender's private key and again encodes the encoded data with the common mystery keys that sets up first layer secrecy on the conveying message. At long last, the framework scrambles the last ciphertext with recipient's open key, which is must be unscramble with beneficiary's private key; yet just collector is realized his private key that builds up second layer classification of the exchange.
2. **Integrity:** The framework produces a Message Authentication Code (MAC) by encodes the ciphertext with shared mystery key for trustworthiness check of the ciphertext just as message. At long last, the framework encodes the last scrambled data with recipient's open key and send to the goal. Thus, no one but collector can decode the data, since beneficiary is just realizing his private key that sets up first layer uprightness. Again the recipient unscrambles the got data with shared mystery keys and contrast the ciphertext and created ciphertext; if the ciphertexts are discovered same, the collector acknowledges for recover message; in any case dispose of it.
3. **Authentication:** In the sender end, the framework scrambles the message with sender's open key and again encodes the message multiple times with shared mystery keys lastly scrambles with collector's open key and send to the goal. The framework unscrambles the got data in the less than desirable end. For this, first decodes the got data with beneficiary's private key and afterward unscrambles with shared mystery keys lastly

recover the message with sender's open key. Thus, the sender and the collector couldn't deny the correspondence because of the got data is from the outset decodes with the recipient's private key, which is connected with his open key that is utilized to encodes the data in the sender side lastly recover the message with sender's open key correspondingly, it is connected with sender's private key that is utilized to scrambles the message. Since, the private key is just known to the proprietor; consequently, it builds up confirmation for both the sender and the collector of the imparting message.

4. **Non-repudiation:** The framework encodes the message with sender's open key and again scrambles the message with shared mystery keys lastly encodes with collector's open key and send to the goal. Consequently, the sender and the collector couldn't renounce the correspondence because of the got data is from the start decodes with the recipient's private key, which is connected with his open key that is utilized to encodes the data in the sender side lastly recover the message with sender's open key likewise, that is connected with sender's private key that is utilized to scrambles the message. Since the private key is just known to the proprietor and consequently, it sets up non-disavowal for both the beneficiary and the sender of the imparting message.

In this part, trial results are dissected and quickly portrayed info and yield aftereffects of the created framework. A relative security investigation between our created framework and customary frameworks is likewise illustrated, in which our created framework effectively satisfied the central security necessities.

CHAPTER 5
IMPACT SOCIETY ENVIRONMENT AND SUSTAINABILITY

5.1 Impaction on Society:

Key confirmation with Secure Shell is more secure than mystery word approval, as it gives much more grounded character checking. A substance must have both the private key and the privilege passphrase to confirm itself to another component.

An open key foundation or Key dissemination offers a scope of administrations that radically decrease security dangers related with business forms. A Key dispersion offers the accompanying administrations:

Advanced validation univocal guarantees a component's character and characteristics. In spite of the way that the character outfits us with the name of an individual or machine, the characteristics offer us data in regards to their ability to rehearse as a certified proficient, credit limits, date of birth, and so on.

Information honesty is the administration that perceives any movements that may have happened by chance or purposely while data is taken care of or transmitted over the Internet. Approval and decency organizations are the reason of electronic imprints, which can be differentiated and composed by hand stamps, in this manner emptying the prerequisite for paper.

The classification administration empowers data (records and correspondences) to be made sure about, and controls access to the data by applying key dissemination with based strong approval frameworks.

5.2 Impact On Environment:

Without vitality or transfer speed imperatives, the present (fixed line) systems will in general imitate multicasting by a large number of unicasts lessening bunch the executives to straightforward usefulness on head of point-to-point correspondence. Shockingly, vitality, data transfer capacity and register power is critical, particularly in compelled conditions and remote sensor systems (WSN). Subsequently, multicasting is intended to turn out to be progressively significant, as it intensely lessens arrange overhead and both, the required for CPU force and vitality utilization. As an outcome, the requirement for secure gathering the board and secure gathering key circulation in obliged conditions increments and isn't yet settled fittingly – neither in norms, nor in the writing and not as a reasonable execution. In a meaning of secure gathering correspondence in obliged conditions is given. It is demonstrated that both sender confirmation and secure gathering the board for the most part address secrecy during transport, yet neither validation nor secure key trade or secure gathering the executives are thought of.

5.3 Ethical Aspects On Message Authentication with KDC:

MAC algorithm is a symmetric key cryptographic procedure to give message authentication. For building up MAC process, the sender and receiver share a symmetric key K. Basically, a MAC is an encrypted checksum produced on the fundamental message that is sent along with a message to guarantee message authentication.

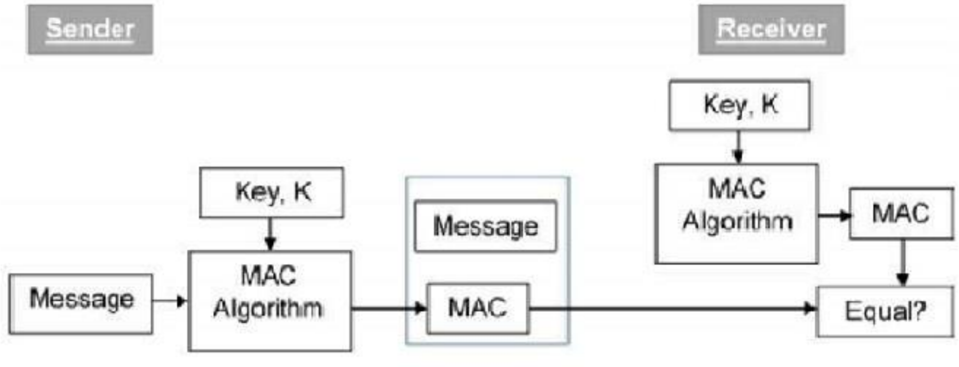


Figure 5.1: Authentication procedure at KDC

Let us currently attempt to comprehend the whole procedure in detail −

- The sender utilizes some openly known MAC calculation, inputs the message and the secret key K and produces a MAC value.
- Like hash, MAC function also compresses an arbitrary long input into a fixed length output. The significant distinction among hash and MAC is that MAC uses secret key during the compression.
- The sender forwards the message alongside the MAC. Here, we accept that the message is sent free, as we are worried of giving message cause confirmation, not privacy. On the off chance that privacy is required, at that point the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.

In the event that the processed MAC doesn't coordinate the MAC sent by the sender, the beneficiary can't decide if the message has been adjusted or the starting point has been distorted. As a main concern, a beneficiary securely expect that the message isn't the real.

5.4: Sustainability Plan for Key Distribution with Message Authentication and Confidentiality Checking:

Ordinary methodologies have been inspected to propose a superior new solid message confirmation framework. This system gives a predominant solid message validation and privacy checking highlight for conveying parties. Here, the structure uses two shared two shared mystery keys for message validation and grouping checking. To begin with, is scrambles with mystery key K2, the yield is called ciphertext, which is again encodes with shared mystery key Ks, which delivers an authenticator known as MAC that is appended with the ciphertext and sent to the intendent beneficiary. In the recipient side, the collector ascertains the new back rub validation code (MAC′) by scramble the got figure text with the common mystery key Ks. By then the decided MAC′ is contrasted and the got MAC. If the MACs are found same, the recipient acknowledge it and unscramble the got ciphertext with shared mystery key Ks to get comprehensible message; regardless deny it. Subsequently the recipient affirmed that the message isn't modified and originated from the expressed source. This give a layer two security to the protected message trade. Another bit of the system develops the message check for ensured about message trade. Figure 3.10. Shows the message check and grouping where affirmation is joined to ciphertext:

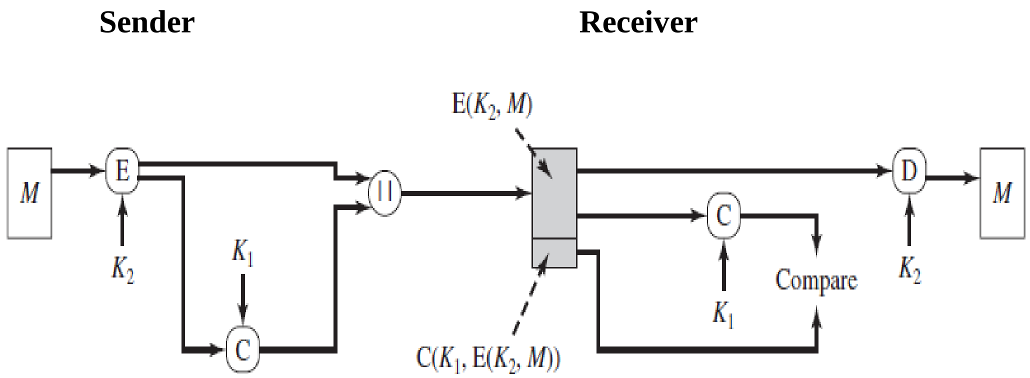


Figure 5.2: Message Authentication and Confidentiality

CHAPTER 6
SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

Cryptographic fixings, cryptographic estimations, cryptographic instruments, and other related cryptographic terms are thought of, inspected, reviewed, dismembered and made sense of it.

A presentation of the normal ordinary philosophy for message affirmation, where message endorsement code (MAC) is joined to the cipherext has been inspected, explored and its limitations are perceived and discussed.

In our proposed structure, we offer an unrivaled procedure for ensured about message trades with ideal security organizations over the customary systems.

A presentation of the proposed structure, process depiction, diagrams, encryption count and unscrambling estimation of the proposed system are arranged and represented.

Security structures are required to guarantee key scattering security associations: Confidentiality, Integrity, Authentication and Non-refusal of the offering message and people. An equivalent report between the standard frameworks and proposed structure has been performed, where the proposed structure plays out all the referenced head security organizations.

6.2 Conclusions

An unrivaled methodology for electronic message trade structure has been made utilizing C# programming language. It performs electronic message trades with all the fundamental security organizations, which are classification, respectability, verification and non-denial for both imparting message and conveying members. For this, straightforward cryptographic encryption and decoding strategies are utilized to the imparting messages. From the start message is scrambles with the private key of sender PRa and yield is again encoding with a mutual mystery key Ks that creates cipherext, that creates a code that fills in as message authenticator known as

MAC, which is connect with the ciphertext and again scrambles them with shared mystery key K1 that fabricates the new ciphertext, which is again scramble with the beneficiary's open key PUb to deliver last ciphertext, which is to be send to the intendent beneficiary. In the not exactly alluring end, recover the message, beneficiary from the start unscrambles the got data with his private key PRb and again decodes with the common mystery key Ks that and MAC of the ciphertext, and a while later just unravels the MAC to make another ciphertext′ and differentiation the new ciphertext′ and they got ciphertext that ensures the ciphertext approval similarly as message confirmation; in case ciphertexts are found same, by then interprets the ciphertext with shared puzzle key K1 and again translates with the sender open key PUa and recuperate the message; regardless discard it. This strategy can be applied wherever of electronic correspondences in a safe manner.

6.3 Recommendations

In current electronic correspondence age, security of the electronic message exchanges are the vital issues and prime concern and it is entirely demandable. Security of electronic message exchanges relies upon the key estimations of the cryptosystem and different cryptographic procedures. In this way, cryptographic key age, key trade, cryptographic security instruments, cryptography security administrations are the worry regions for future examination work.

Key age for the different cryptographic applications, for example, E-trade, E-exchanges, E-banking, E-installments, E-administration, Telemedicine, Exam Questions Transmissions, etc; Group Key age, Group Key Exchange and Key conveyance without outsider are the cryptographic examination field.

6.4 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 the thesis.

REFERENCES

1. Kaufman, Charlie, Radia J. Pelman and Mike Speciner. “Network security –private communication in a public world”. Prentice Hall series in computer networking and distribution system (1995).

2. Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Education Private Limited, 2011.

3. W. Stallings, Cryptography and Network Security Principles and Practice, 5th ed., Prentice Hall Press, Upper Saddle River, NJ, USA, 2010.

4. 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.

5. Bruce Schneier, “Applied Cryptography”, 2nd Edition, 2003, ISBN: 9971-51-348-X.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

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. Manning’s Inovative Online Reader, https://livebook.manning.com/book/real-world-cryptography/chapter 3/v-1/27

13. Mago, Neeru. “PMAC : A Fully Parallelizable MAC Algorithm.” (2016).

14. Brain Kart.com, http://www.brainkart.com/article/Pretty-Good Privacy_8491

15. Semantic Scholar, https://www.semanticscholar.org/paper/PMAC-%3A-A-Fully Parallelizable-MAC-Algorithm Mago/583789c89b0f8abfe0751679a4a330121b9b7f4c

16. Tutorials Point, https://www.tutorialspoint.com/cryptography/index.htm

17. Learn Cryptography, https://learncryptography.com

18. ScienceDirect, https://www.sciencedirect.com/topics/computer-science/encryption-process

19 .Wikipedia, https://en.wikipedia.org/wiki/Cryptography

APPENDICES

Appendix A

This is in excess of a scholastic objection; solid verification is where an easygoing procedure has much of the time lead to work which is significantly under the least positive conditions wrong, and, most ideal situation just for the most part analyzable. It is along these lines alluring that trust in a confirmation show ought to start from more than several people's frailty to break it. Believe it or not, each basic substance affirmation objective should be authoritatively described and any up-and-comer show should be shown to meet its goal under a standard cryptographic assumption.

Appendix B

In this postulation, we will attempt to force solid confirmation to conveying electronic information or message through cryptographic key dissemination open key encryption-decoding process.

Our primary point of this proposition is to guarantee solid validation of electronic information or message over the open key conveyance without permitting access to an assailant.

Appendix C

2.3. 2 Key Distribution Working Process:

Key Distribution Center (KDC)

- ❖ A typical movement with a KDC incorporates a sales from a customer to use some assistance.

- ❖ The KDC will use cryptographic methodologies to confirm referencing customers as themselves. It will similarly check whether an individual customer has the benefit to get to the organization referenced.

- On the remote possibility that the confirmed customer meets each suggested condition, the KDC can give a ticket permitting access.

- KDC generally work with symmetric encryption. In most (yet not all) cases the KDC grants a key to all of the different social events.

- The KDC produces a ticket reliant on a server key.

The customer gets the ticket and submits it to the suitable server. The server can confirm the submitted ticket and award access to the client submitting it.

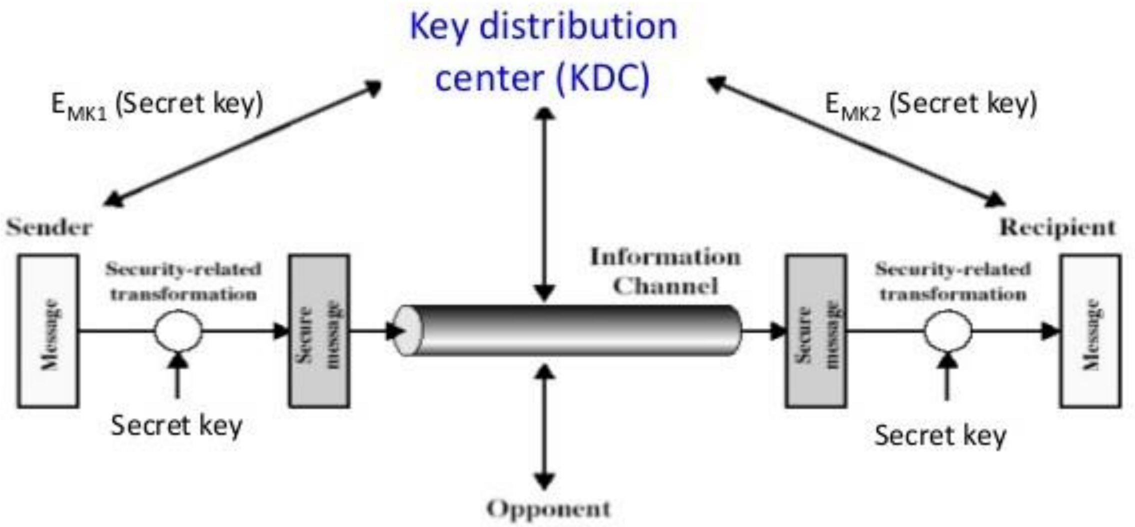


Figure2.5: KDC working processes

Appendix D

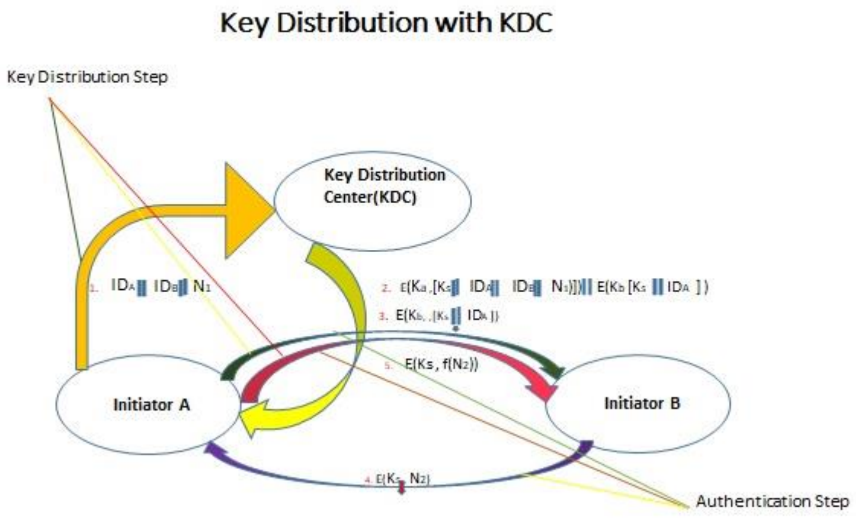
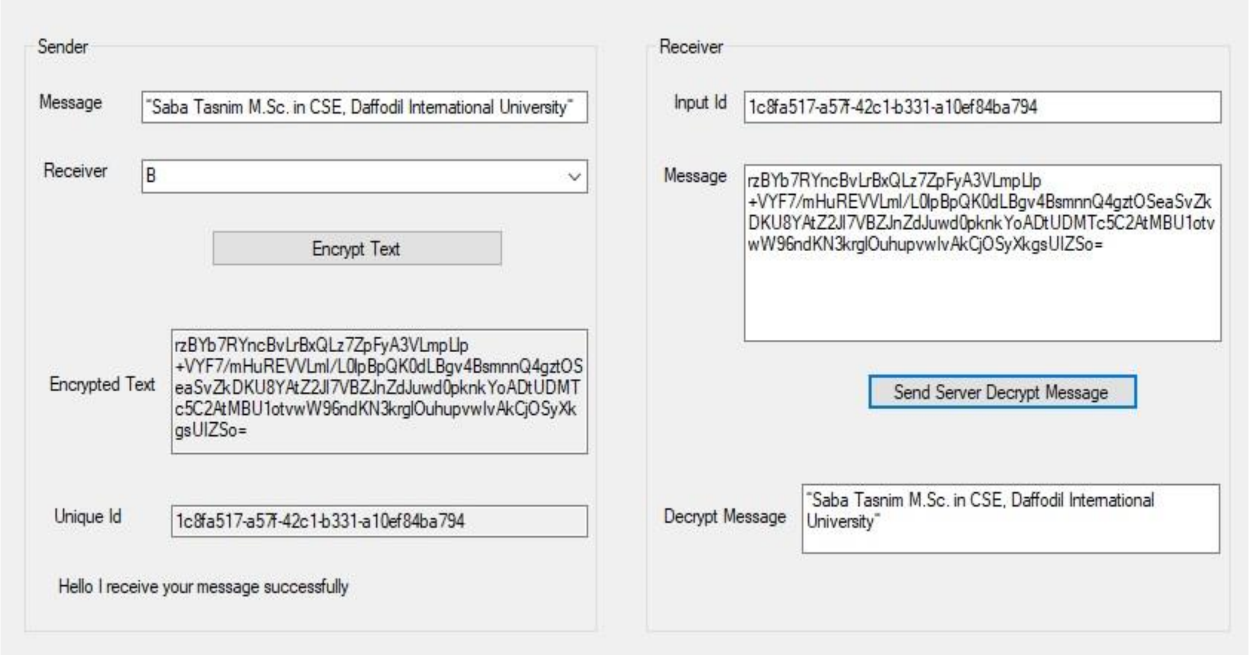

Key Distribution with KDC
Key Distribution Step
Key Distribution Center(KDC)
1. ID_A ‖ ID_B ‖ N_1
2. E(K_a ,[K_s ‖ ID_A ‖ ID_B ‖ N_1)])‖ E(K_b [K_s ‖ ID_A])
3. E(K_b, ,[K_s ‖ ID_A])
5. E(K_s , f(N_2))
Initiator A
Initiator B
4. E(K_s, N_2)
Authentication Step

Figure 3.5: Process are all completed

Appendix E



Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

Receiver: B

Encrypted Text:
```
rzBYb7RYncBvLrBxQLz7ZpFyA3VLmpLlp
+VYF7/mHuREVVLml/L0lpBpQK0dLBgv4BsmnnQ4gztOS
eaSvZkDKU8YAtZ2Jl7VBZJnZdJuwd0pknkYoADtUDMT
c5C2AtMBU1otvwW96ndKN3krglOuhupvwlvAkCjOSyXk
gsUIZSo=
```

Unique Id: 1c8fa517-a57f-42c1-b331-a10ef84ba794

Hello I receive your message successfully

Input Id: 1c8fa517-a57f-42c1-b331-a10ef84ba794

Message:
```
rzBYb7RYncBvLrBxQLz7ZpFyA3VLmpLlp
+VYF7/mHuREVVLml/L0lpBpQK0dLBgv4BsmnnQ4gztOSeaSvZk
DKU8YAtZ2Jl7VBZJnZdJuwd0pknkYoADtUDMTc5C2AtMBU1otv
wW96ndKN3krglOuhupvwlvAkCjOSyXkgsUIZSo=
```

Decrypt Message: "Saba Tasnim M.Sc. in CSE, Daffodil International University"

Figure 3.8: Message generated

Appendix F

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

Appendix G

Sender **Receiver**

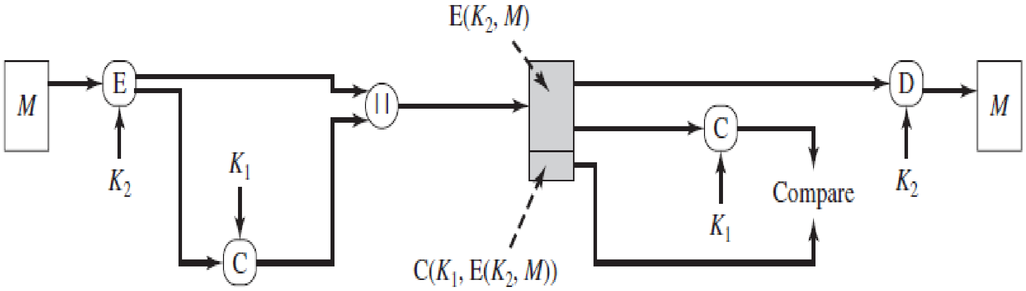
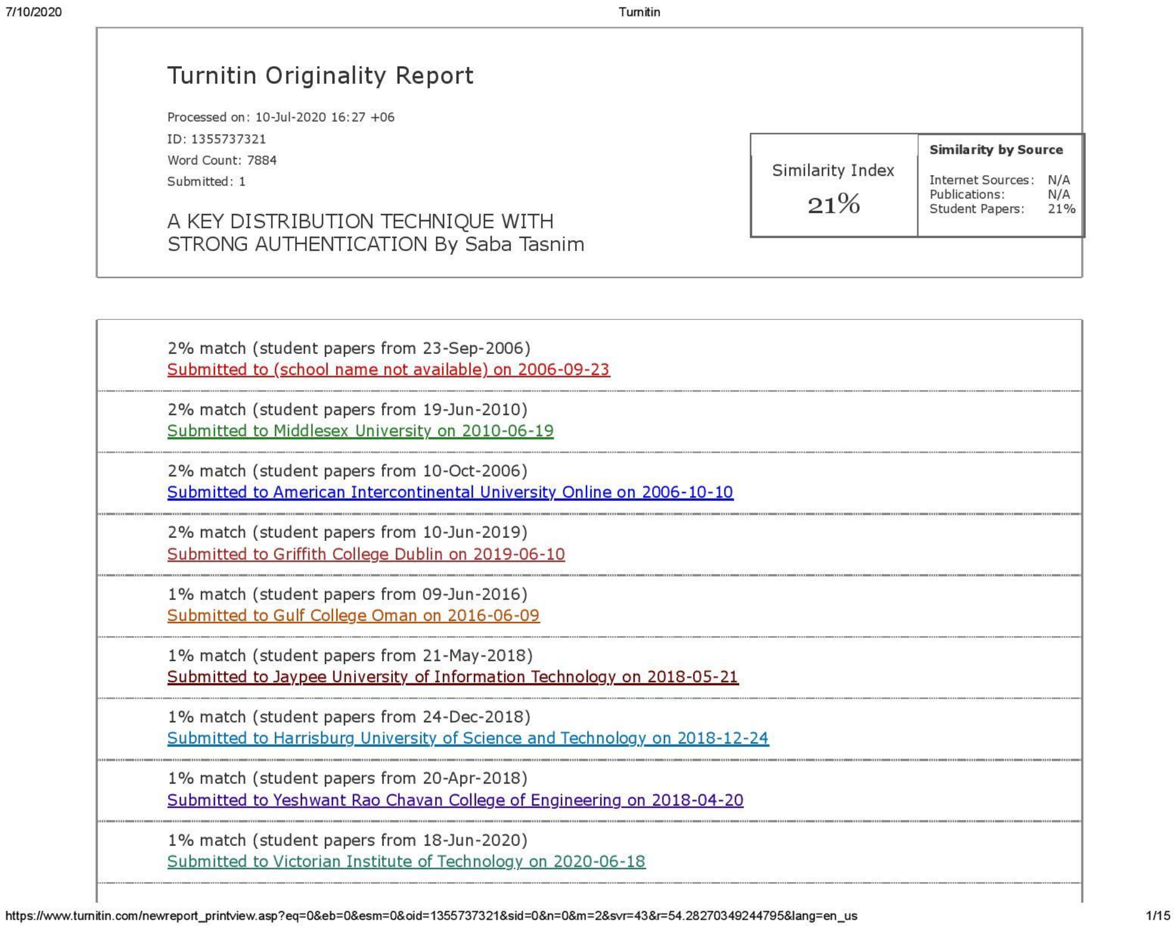


Figure 2.9: Message Authentication and Confidentiality

Plagiarism Report



7/10/2020 Turnitin

Turnitin Originality Report

Processed on: 10-Jul-2020 16:27 +06
ID: 1355737321
Word Count: 7884
Submitted: 1

A KEY DISTRIBUTION TECHNIQUE WITH STRONG AUTHENTICATION By Saba Tasnim

Similarity Index	Similarity by Source	
21%	Internet Sources:	N/A
	Publications:	N/A
	Student Papers:	21%

2% match (student papers from 23-Sep-2006)
Submitted to (school name not available) on 2006-09-23

2% match (student papers from 19-Jun-2010)
Submitted to Middlesex University on 2010-06-19

2% match (student papers from 10-Oct-2006)
Submitted to American Intercontinental University Online on 2006-10-10

2% match (student papers from 10-Jun-2019)
Submitted to Griffith College Dublin on 2019-06-10

1% match (student papers from 09-Jun-2016)
Submitted to Gulf College Oman on 2016-06-09

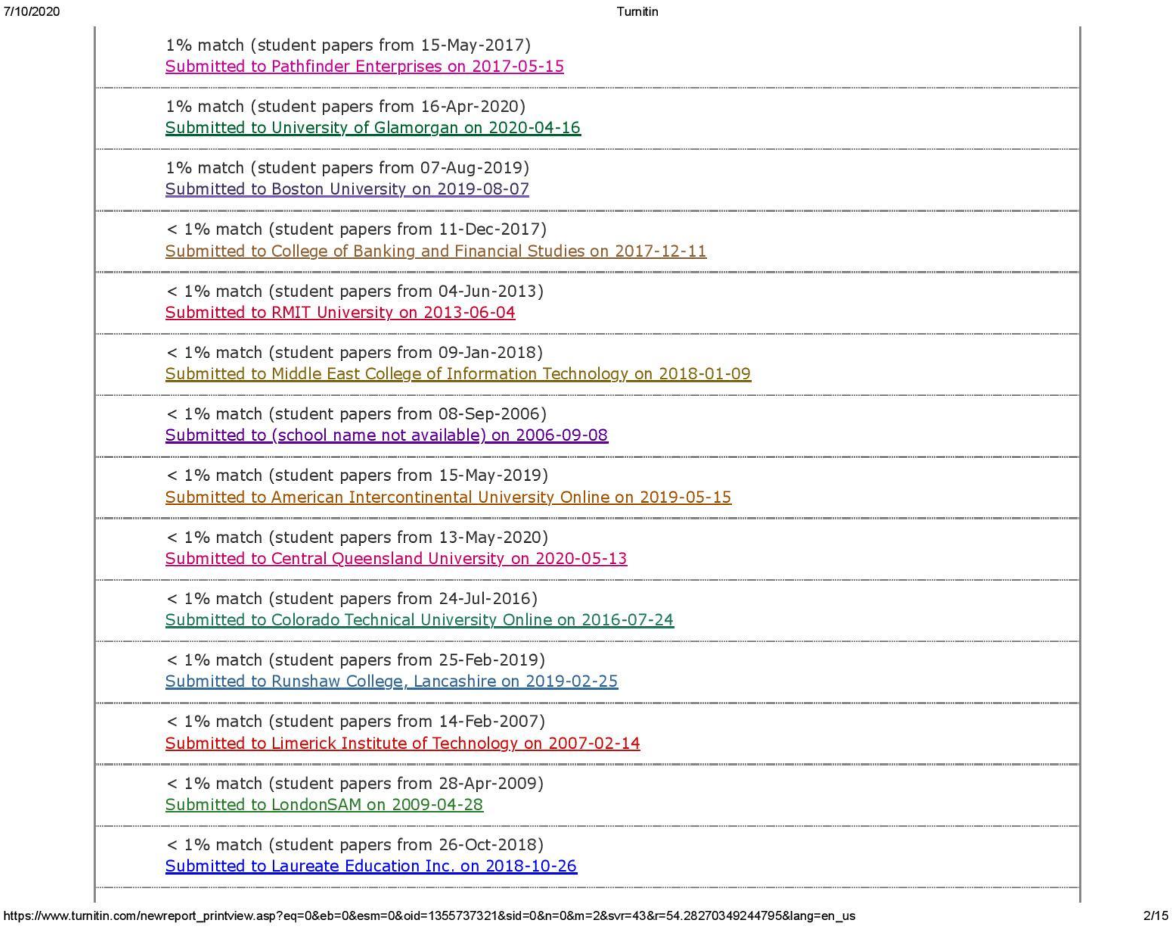
1% match (student papers from 21-May-2018)
Submitted to Jaypee University of Information Technology on 2018-05-21

1% match (student papers from 24-Dec-2018)
Submitted to Harrisburg University of Science and Technology on 2018-12-24

1% match (student papers from 20-Apr-2018)
Submitted to Yeshwant Rao Chavan College of Engineering on 2018-04-20

1% match (student papers from 18-Jun-2020)
Submitted to Victorian Institute of Technology on 2020-06-18

https://www.turnitin.com/newreport_printview.asp?eq=0&eb=0&esm=0&oid=1355737321&sid=0&n=0&m=2&svr=43&r=54.28270349244795&lang=en_us 1/15



7/10/2020 Turnitin

1% match (student papers from 15-May-2017)
Submitted to Pathfinder Enterprises on 2017-05-15

1% match (student papers from 16-Apr-2020)
Submitted to University of Glamorgan on 2020-04-16

1% match (student papers from 07-Aug-2019)
Submitted to Boston University on 2019-08-07

< 1% match (student papers from 11-Dec-2017)
Submitted to College of Banking and Financial Studies on 2017-12-11

< 1% match (student papers from 04-Jun-2013)
Submitted to RMIT University on 2013-06-04

< 1% match (student papers from 09-Jan-2018)
Submitted to Middle East College of Information Technology on 2018-01-09

< 1% match (student papers from 08-Sep-2006)
Submitted to (school name not available) on 2006-09-08

< 1% match (student papers from 15-May-2019)
Submitted to American Intercontinental University Online on 2019-05-15

< 1% match (student papers from 13-May-2020)
Submitted to Central Queensland University on 2020-05-13

< 1% match (student papers from 24-Jul-2016)
Submitted to Colorado Technical University Online on 2016-07-24

< 1% match (student papers from 25-Feb-2019)
Submitted to Runshaw College, Lancashire on 2019-02-25

< 1% match (student papers from 14-Feb-2007)
Submitted to Limerick Institute of Technology on 2007-02-14

< 1% match (student papers from 28-Apr-2009)
Submitted to LondonSAM on 2009-04-28

< 1% match (student papers from 26-Oct-2018)
Submitted to Laureate Education Inc. on 2018-10-26

https://www.turnitin.com/newreport_printview.asp?eq=0&eb=0&esm=0&oid=1355737321&sid=0&n=0&m=2&svr=43&r=54.28270349244795&lang=en_us 2/15