KANTIPUR ENGINEERING COLLEGE

(Affiliated to Tribhuvan University)

Dhapakhel, Lalitpur

[Subject Code: CT755]

A MAJOR PROJECT FINAL REPORT ON

SECURE MESSAGING USING RSA AND AES CRYPTOGRAPHY ALGORITHM

Submitted by:

Angel Karki	[25759]
Anjali Mehta	[25761]
Manil Maharjan	[25786]
Sudip Rai	[25829]

A MAJOR PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR IN COMPUTER ENGINEERING

Submitted to:

Department of Computer and Electronics Engineering

March, 2022

SECURE MESSAGING USING RSA AND AES CRYPTOGRAPHY ALGORITHM

Submitted by:

Angel Karki	**[25759]**
Anjali Mehta	**[25761]**
Manil Maharjan	**[25786]**
Sudip Rai	**[25829]**

Supervised by:

Er.Bikash Shrestha

Senior System Engineer, Nepal Telecom

A MAJOR PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR IN COMPUTER ENGINEERING

Submitted to:

Department of Computer and Electronics Engineering

Kantipur Engineering College

Dhapakhel, Lalitpur

March, 2022

ACKNOWLEDGMENT

This project is prepared in partial fulfillment of the requirement for the bachelor's degree in Computer engineering. First and foremost, we would like to express our sincere gratitude towards Er. Bikash Shrestha, our project supervisor for his constant guidance, inspiring lectures and precious encouragement. Without his invaluable supervision and suggestions, it would have been a difficult journey for us. His useful suggestions for this whole work and cooperative behaviour are sincerely acknowledged.

We would like to thank the Department of Electronics and Computer Engineering for providing this opportunity of collaborative undertaking which has helped us developed a major project of our own that has greatly enhanced our knowledge and provided us a new experience of teamwork. The great need of research, time and sheer coding has allowed us to harness our skill, experience and knowledge. We would like to thank and express our gratitude to all our respective subject teachers for sharing their precious knowledge, constant and guidance.

Last but never the least we are thankful to all other people who contributed in preparation of this report. We have tried our best to make this report error free. Any error in this report is our own responsibility. Suggestions and comments from readers are highly appreciable.

Angel Karki	[25759]
Anjali Mehta	[25761]
Manil Maharjan	[25786]
Sudip Rai	[25829]

ABSTRACT

WHISPER is a standalone project which can be used to secure communication between two clients.The project mainly focuses to provide security between two clients communicating with each other through internet. However,web application can be easily divided that allows replacing the user interface by a different one.

The project demonstrates the process of creating the core of any application responsible for communication between two computer and secure communication was the most important part of it.It was achieved using RSA in combination with AES algorithm.

The result of this project is a functional web application able to ensure secure communication between two clients transimitting text messages over a computer that can be further implemented to run through internet. The project is shown with success to the project's supervisor.Nevertheless, further development would be required to make the application more secure and smooth.

Keywords$-Encryption, Cryptography, RSA, AES$

TABLE OF CONTENTS

Acknowledgment **i**

Abstract **ii**

List of Figures **v**

List of Abbreviations **vi**

1 Introduction **1**

1.1 Background 1

1.2 Problem Statement 2

1.3 Objectives 2

1.4 Applications 2

1.5 Project Features 3

1.6 Feasibility Analysis 3

1.6.1 Economic Feasibility 3

1.6.2 Technical Feasibility 3

1.6.3 Operational Feasibility 3

1.7 System Requirement 4

1.7.1 Software Requirement 4

1.7.2 Hardware Requirements 4

2 Literature Review **5**

2.1 Existing System 7

2.1.1 Description of Related Theory 7

2.1.2 Implementations Examples 11

2.2 Technology Used 11

2.2.1 Node JS 11

2.2.2 Vue Js 12

2.2.3 Socket.Io 12

3 Methodology **13**

3.1 Working Description 13

3.2 Algorithm Employed: 13

3.2.1 AES - Advanced Encryption Standard 13

3.2.2 RSA 16

3.3 Implementation Process 17

3.4 System Diagrams 18

3.4.1 System Flowchart 18

3.4.2 Usecase Diagram 19

3.4.3 Sequence Diagram 20

3.4.4 Activity Diagram 21

3.5 Software Development Model 22

4 Result and Discussion 23

4.1 Snapshots of Output 23

4.2 Work Schedule 24

5 Conclusion and Future Enhancement 25

5.1 Conclusion 25

5.2 Scope for future Enhancement 25

References 25

LIST OF FIGURES

2.1 Utilization Of Shared Key in Encryption And Decryption Of Symmetric Key Cryptography . . . 9

2.2 Utilization of Keys in Encryption and Decryption of Asymmetric Key Cryptography. . . . 10

3.1 Hybrid cryptosystem . . . 13

3.2 AES encryption and decryption . . . 16

3.3 Process of secure communication . . . 17

3.4 Flowchart of System . . . 18

3.5 Usecase diagram of System . . . 19

3.6 Sequence Diagram of System . . . 20

3.7 Activity diagram of System . . . 21

3.8 Software Development Model (Incremental Model) . . . 22

4.1 Chat room . . . 23

4.2 Chat room . . . 23

4.3 Encrypted message . . . 24

4.4 Gantt Chart . . . 24

LIST OF ABBREVIATIONS

AES-Advanced Encryption Standard

RSA-Rivest, Shamir, Adleman

CHAPTER 1
INTRODUCTION

”We live in a society that is awash with information but few of us really understand what information is”.

Nowadays people need to communication with each other all the time. Communication often takes place between people who are far from each other.They are exchanging information with significant value. This fact leads to the statement that the message they are exchanging should remain secret for other parties which are not authorized.Today, more and more sensitive data is stored digitally.As the data transference turned to be a major trend, the need for data security becomes vital and significant. Bank accounts, medical records,messages and personal emails are some categories of data that must be secure ; this has made cryptography an important research topic.Cryptography is one of the methods to protect and secure the data

1.1 Background

Since the world has become a global village with the help of internet. Using internet facility a person can communicate with any person that resides on any corner of the world where internet have been reached. To communicate with each other, person uses different form of communication like sending of data in text,audio,video format. So,our environment is surrounded by digital data that transit via networks. When data are important, they become vulnerable to external attacks which can be avoided by using cryptography which provides confidentiality, privacy and availability required to secure digital data during exchange of messages.With different forms of attack such as brute force attack,biclique attack and related key attacks,the security needed for every data had also arise and traditional encryption(Single data encryption)had eventually not been sufficient for the protection and security of every data.

1.2 Problem Statement

In recent years network security had become an important issue.Encryption has come up as a solution, and plays an important role in information security system.Moreover, some secure chatting app that offers storing the history of shared information on database may not be preferred by some users.

As the requirement for security arises,advancement of new,simple and effective security framework has been preferred by many people.One way to develop the security of data that can also answer today's problem in securiy is through hybridization of prevailing cryptographic algorithms.The present project focuses on cryptography which strongly ensures securing any type of text data to be transmitted in a network (LAN) implementing two encryption technologies such as AES algorithm and RSA algorithm , that combines the convenience of RSA algorithm with the efficiency of AES.

1.3 Objectives

The objectives are:

i. To implement a hybrid cryptosystem

ii. To realize a fast and reliable web app that allows secure communication between two clients.

1.4 Applications

The project assumed providing communication between two users at a time. Communication should take place via two different channels, one allowing to receive a text message, the other one to send them. Moreover, a third user trying to enforce him/her on a communicating channel is barred.

1.5 Project Features

The different features of this project are:

i Exchange of information over a secure channel

ii Allow realization of complex hybrid algorithm

iii Utmost privacy is maintained

1.6 Feasibility Analysis

i Feasibility Analysis

ii Economic

iii Technical

iv Operational

The key consideration involved in the feasibility study are described below:

1.6.1 Economic Feasibility

This project will be economically feasible as it only requires mobile/laptops to enter a web browser.

1.6.2 Technical Feasibility

The technical requirements of the project is simple.The use of Node.js for programming which has amazing and powerful opensource libraries has made the technical requirements easy and simple.Hence,the project is technically feasible.

1.6.3 Operational Feasibility

This project will be operationally feasible as it helps for communication between clients.

1.7 System Requirement

1.7.1 Software Requirement

i PC: Windows 7, Windows 8, Windows 10 with IE 11*

ii Mac: OS 10(Safari 9, Chrome 43+)

iii Arch 4.0.0(Chrome 43+)

1.7.2 Hardware Requirements

i Minimum 1 GB RAM and Intel core 2 duo processor

ii Recommended 2 GB RAM and Intel i3 processor or higher

CHAPTER 2
LITERATURE REVIEW

In this section, we try to explain the information we achieved from the previous researchers in the field of cryptographic algorithm.

Hua Li ab1 *et al.* explained new compact dual-core architecture used in AES. The practise of using a new compact dual-core architecture started that consisted of two independent cores that practice encryption and decryption simultaneously. In order to provide round keys for encryption and decryption, proposed key generation unit with 32-bit data path was explored. The concept used to implement shift rows was the important design which helps to increase the encryption time. The major limitation was that in comparison to the other design, this design also requires fewer more hardware resources.[1]

H. C. Williams modified the RSA public-Key encryption algorithm. He suggested that if the encryption procedure was broken into a certain number of operations than remainder used as modulus could be factored after few more operations. This technique was in similar appearance of RSA so as produce digital signatures. The main limitation of this scheme was that very large prime numbers were used and generated mathematical errors were observed.[2]

Adam J. Elbirt *et al.* explained the AES block cipher algorithm using FPGA based kit. They proposed that for hardware implementation of encryption algorithms, reprogrammable devices were the best choice. The disadvantage was that when the implementation size was increased then the number of rounds unrolled also enhanced and this increase was partially offset by the packing of the round keys within the round structure.[3]

Martin E.Hellman extended the shannon theory approach to cryptography. He discussed about Shannon's random cipher model which was conservative than in such case when a randomly chosen cipher was considered, the security falls significantly. The concept of matching a cipher to a language and the trade-off between local and global uncertainty were also developed. The limitation of this approach is that it is not directly applicable to designing practical cryptographic systems.[4]

Hung-Min Sun *et al.* proposed dual RSA algorithm and also did the acute analysis of the security of the algorithm. Dual RSA was a variant of RSA which is helpful in some specific situations that require two instances of RSA with the advantage of reducing the storage requirements for the keys. The main drawback of using dual RSA was that the computational complexity of the key generation algorithms was also optimised.[5]

Mao-Yin Wang *et al.* configured single and multi-core AES architectures for flexible security. According to them the major building blocks for the architecture of AES was a group of AES processors. Each AES processor provides a block cipher scheme with a novel key expansion design approach for the original AES algorithm. In this multi core architecture the memory controller of each AES processor was designed for the maximum overlapping between data transfer and encryption and thus reducing interrupt handling load of the host processor.[6]

Chong Hee Kim *et al.* improved differential fault analysis on AES key schedule. Proposed advanced encryption standard for which the main target is known DFA. Implementation of AES is known to be vulnerable to DFA which could be split into two categories depending on the fault location that has the DFA on the state and the DFA on the key schedule. The major limitation is that if the key schedule is not redone for recomputation then it cannot prevent DFA on the AES Key Schedule. The major problem was that if the key schedule was not done again for recomputation then it cannot prevent DFA on the AES Key Schedule.[7]

Ho Won Kim *et al.* designed and implemented a private and public key crypto processor and its application to a Security System. A special-purpose microprocessor was optimized for the execution of cryptography algorithms. This crypto processor could be used for various security applications such as storage devices, embedded systems, network routers, security gateways using IP Sec and SSL protocol, etc. They had presented the design and implementation of a crypto processor composed to a 32-bit RISC processor and coprocessor blocks dedicated to the AES, KASUMI, SEED, triple- DES, ECC and RSA crypto algorithms.[8]

2.1 Existing System

2.1.1 Description of Related Theory

Authentication

Authentication is one of the most important aspects of security, where an entity should identify itself before or during the communication. This avoids any type of attack or malicious activity by which a malicious user impersonates the user and identifies himself as the real user to the server. There two types of authentication schemas knows as weak authentication and strong authentication. Weak authentication (one factor authentication) means that the user uses only one type of identify credential such as a PIN or password authentication. While in strong authentication the client needs to provide his identify and verify himself of the server with multiple factors.

Privacy

In a digital word, privacy of a user means the power to select what type of information to be shared or be accessible by other entities including governments, service provides etc. Unfortunately privacy is one of the factors that is getting sacrified in the current applications. Many applications grab metadata of the user and send these information to their servers even without the knowledge of the user.

Confidentiality: Confidentiality means messages which are exchanged by two parties through a communication channel should be readable only to the intended parties. In order to achieve such a goal, encryption is the mechanism that provides confidentiality between two parties. A message is encrypted by a cryptographic technique and this encrypted message can only be readable by the intended party.

Security Service for Mobile Instant Messaging

In order to evaluate any chat application from the security point of view, relevant threats to such application should be identified and described. Security has three key aspects. Confidentiality, integrity and availability.

Cryptography

The conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text (”plaintext”) is turned into a coded equivalent called ”ciphertext” via an encryption algorithm.

Symmetric Key Cryptography: Symmetric key cryptography or the shared key cryptography utilizes a single same key for encryption and decryption process.

For instance, the message that will be sent by the sender is encrypted using a private (secret) key and will be received by the receiver which is decrypted using the same secret key.

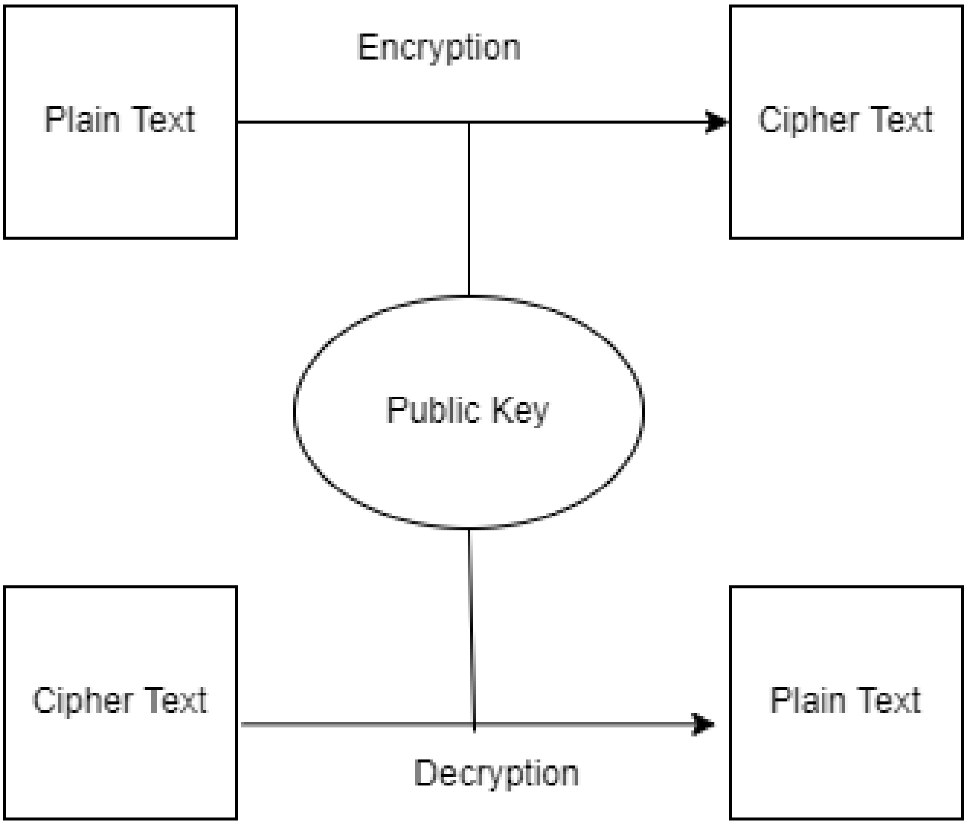


Figure 2.1: Utilization Of Shared Key in Encryption And Decryption Of Symmetric Key Cryptography
Source:Source: https://www.researchgate.net

Asymmetric key cryptography: Asymmetric key cryptography or the public key cryptography comprises a pair of key for encryption and decryption process. Here, public key is recognized by everyone while the private key is kept confidential by receiver.

For instance, the message is encrypted with the public key of the receiver then in order to decrypt the cipher text, private key of the same receiver is always required.

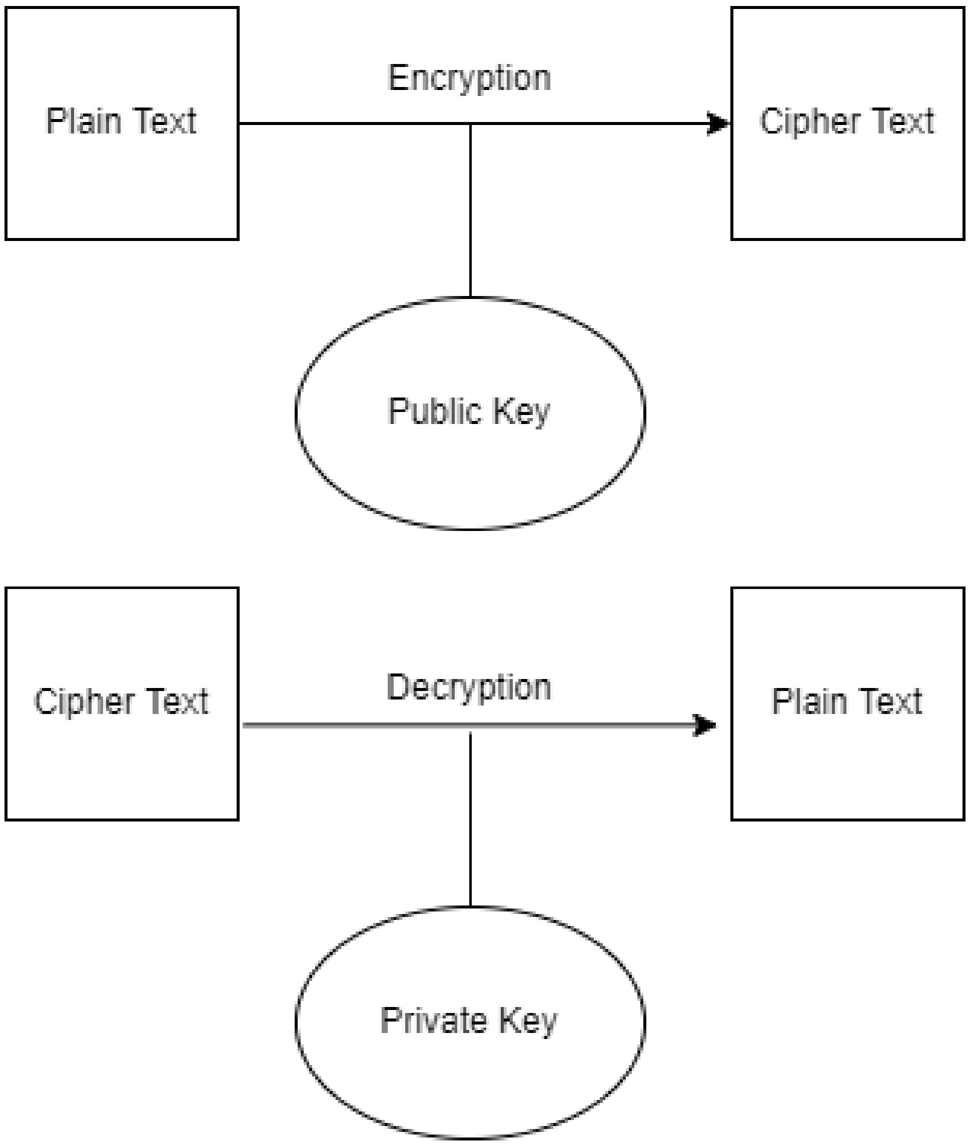


Figure 2.2: Utilization of Keys in Encryption and Decryption of Asymmetric Key Cryptography.
Source: https://www.researchgate.net

Rivest-Shamir-Adleman (RSA), Elgamal, Diffie-Hellman exchange method, Digital signature tandard (DSA), etc. are the examples of protocols using asymmetric key cryptography.

Hybrid Cryptosystem: Both symmetric and asymmetric cryptography techniques presents their own pros and cons. Symmetric cryptography are significantly faster and is used for transfer of large amount of data where as it only provides confidentiality. On the other hand, asymmetric cryptosystem is used to transfer small amount of data and provides confidentiality, authenticity and non-repudiation.

A hybrid cryptosystem combines the symmetric and asymmetric cryptographices in order to benefit from the rapidity of one and security of the other. It offers better efficiency and performance. Different hybrid cryptosystem can be formed to attain required level of security, resource utilization etc.

2.1.2 Implementations Examples

WeChat

Wechat does not provide end to end encryption meaning that is based on public-key encryption, user needs to trust the wechat servers.

imessage

It is an end-to-end encryption but there is still a possibility for the server owners to read their customer message in case they want to perform such as task.

Viber

Viber uses end-to-end encryption. Viber does not store any of the conversation on it's server.

2.2 Technology Used

2.2.1 Node JS

Node.js have made full stack developer's job a dream come true. In absence of node.js, it was hard for a developer to learn several different languages and environment to manage the complete system at server side and client side. Organization and developer can now with the invent of node.js build highly load bearable and fast applications and by using single page applications (SPA) now the server calls are reduced and the application are more friendly and faster. It can be reliable used in every field where the file sizes are high or the network bandwidth is highly consumed. Node.js will make such operation faster with less need of bandwidth.

Thus Node.js offers client-server development integration, aiding code reusability in web applications and is perfect tool for developing fast and scalable network.

2.2.2 Vue Js

Vue is an open source progresive framework that is deligned to be incrementally adoptable, as the core library is focused around the view layer. Orginally, Vue.js was developed as a way to take the best parts of the angular. Vue.js is primarily used to build web interfaces and one-page applications.Thus, it is a view-oriented product. The view is the seential part of everything that occurs inside the system and all information is only validated if it interacts with views correctly.

2.2.3 Socket.Io

Socket.Io enables real-time bidirectional event-based communication between browser and server. It consists of a node.js server, node.js client or a javascript client library for the browser. Its main feature are reliability, auto-reconnection support, disconnect detection, simple and convenient API etc. Websocket is the technology while socket.io is a library for web sockets. It supports fallback options. It also supports broadcasting. A room is an arbitary chamel that sockets join and leave. It can be used to broadcast events to a subset of clientts.

CHAPTER 3
METHODOLOGY

3.1 Working Description

The model proposed is a hybrid cryptosystem based on RSA and AES algorithm . A 256 bit AES key has comparable strength with RSA 2056 bit key.

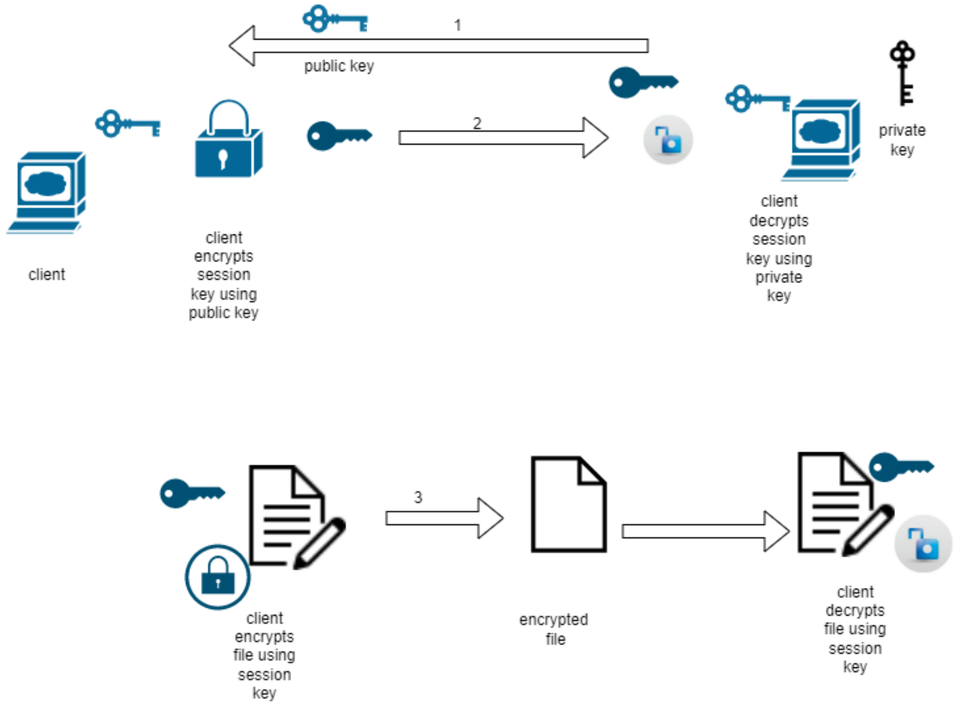

1
public key
2
private key
client
client encrypts session key using public key
client decrypts session key using private key
3
client encrypts file using session key
encrypted file
client decrypts file using session key

Figure 3.1: Hybrid cryptosystem
Source:https://www.researchgate.net/publication/336170348 Secure Hybrid Crypto system AESRSA on FPGA for Data Communication

.

3.2 Algorithm Employed:

3.2.1 AES - Advanced Encryption Standard

The AES algorithm (also known as the Rijndael algorithm) is a protocol standard for a symmetric cryphotyographic system. It is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0. Number of rounds, N$_r$ $= S_k/32 + 6$

Algorithm Steps

These steps used to encrypt 128-bit block:

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9 :
    i. Sub Bytes
    ii. Shift Rows
    iii. Mix Columns
    iv. Add Round Key , using K(round)
4. Execute Final Round :
    1. Sub Bytes
    2. Shift Rows
    3. Mix Columns
5. Corresponding cipher text chunk output of Final Round Step

Encryption

Each round consists of the following four steps:

i. Sub Bytes : In S-Box transformation, each element (byte) of input data is substituted with another data (byte) using precomputed look-up tables (LUTs).

ii. Shift Rows : The transformation is used to create diffusion in cipher text by shifting of elements by one byte. The bytes in the first row remain unchanged whereas the second, third and fourth rows are shifted to the left by 1, 2, 3 bytes, respectively.

iii. Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.This transformation is used for attaining diffusion in the block cipher.

iv. Add Round Key : Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XORing the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the Mix columns step.

Decryption

Decryption involves reversing all the steps taken in encryption using inverse functions like:

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key, and
4. Inverse mix columns.

The third step consists of XORing the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the Inverse mix columns step.

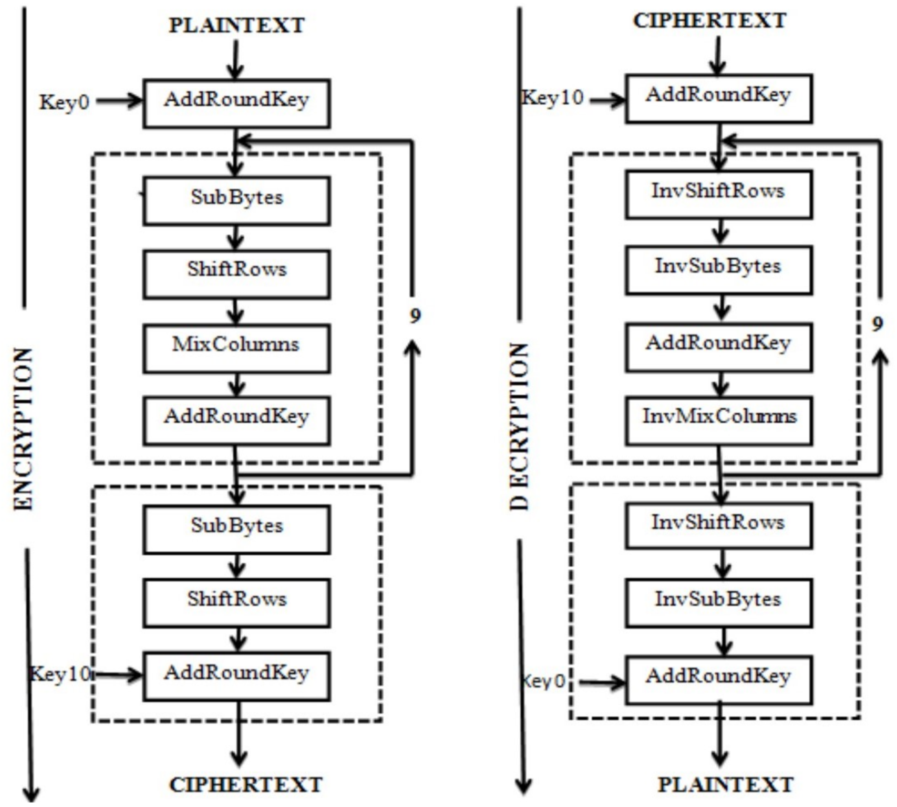


Figure 3.2: AES encryption and decryption
Source:https://www.scirp.org

3.2.2 RSA

RSA asymmetric key cryptography. The public key is used for encryption of message and as the name suggest is known to the public. The private key remains hidden from anyone but the user.

Algorithm

It comprises of three step:-

Key Generation:-Before the data is encrypted key generation is to be done.

1. select two large prime number 'p' and 'q' randomly
2. solve n=p*q
3. solve Euler function value for $\phi(n) = (p-1).(q-1)$
4. choose number e such that 1 < e < $\phi(n)$ relatively prime with $\phi(n)$

5. solve d from d=e$^{-1}mod\ \phi(n)$ such that d*e=$\phi(n)$.

public key is defined as number pair(n,e) while private key is defined as pair (n,d)

Encryption : To encrypt with RSA algorithm, message have to be divided into m; blocks of value not larger than n and then cipher with pattern: c=m^{e}mod n.

Decryption : To decrypt with RSA algorithm, every c block had to be transform like this: m=c^{d}mod n.

3.3 Implementation Process

Implementation of methodology proposed provides the combination of asymmetric and symmetric encryption into one which intends to provide a comprehensive yet secure encryption method. In order to confuse hacker the proposed model is further diversified with AES.

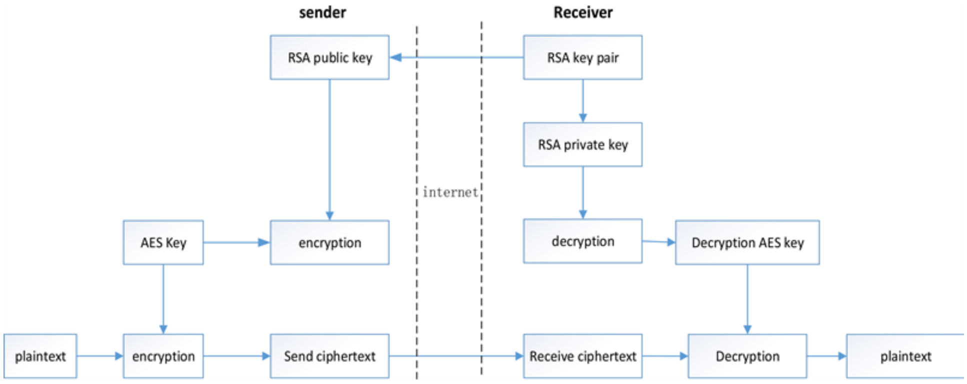


Figure 3.3: Process of secure communication
Source:https://www.scirp.or

Steps Involved :

1. Client2 generates RSA key pair, saves the private key and sends the RSA public key to client1
2. Client1 encrypts AES key with the RSA public key sent by client2.
3. Client1 encrypts plain text data to be sent with the AES key.
4. After receiving the cipher text and encrypted AES key, client2 decrypts AES key by using saved RSA private key and decrypts received cipher text with AES key

to obtain plain text.

3.4 System Diagrams

3.4.1 System Flowchart

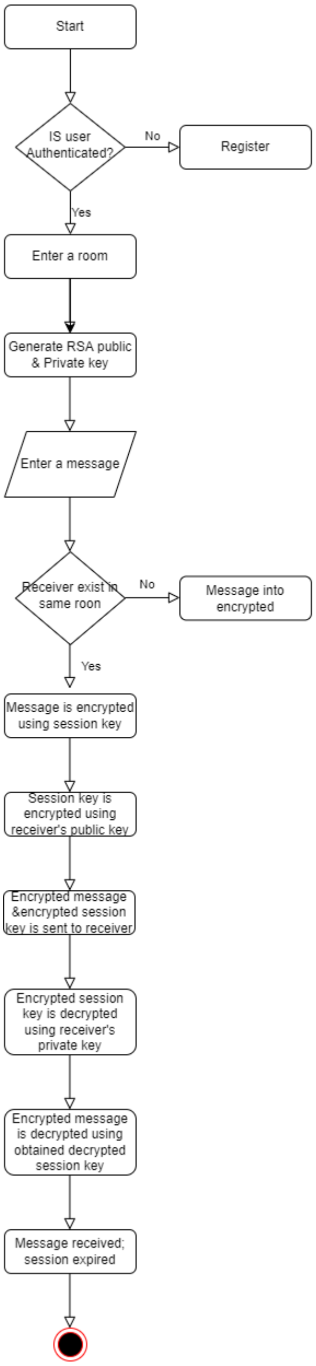

Start
IS user Authenticated?
No
Register
Yes
Enter a room
Generate RSA public & Private key
Enter a message
Receiver exist in same roon
No
Message into encrypted
Yes
Message is encrypted using session key
Session key is encrypted using receiver's public key
Encrypted message &encrypted session key is sent to receiver
Encrypted session key is decrypted using receiver's private key
Encrypted message is decrypted using obtained decrypted session key
Message received; session expired

Figure 3.4: Flowchart of System

3.4.2 Usecase Diagram

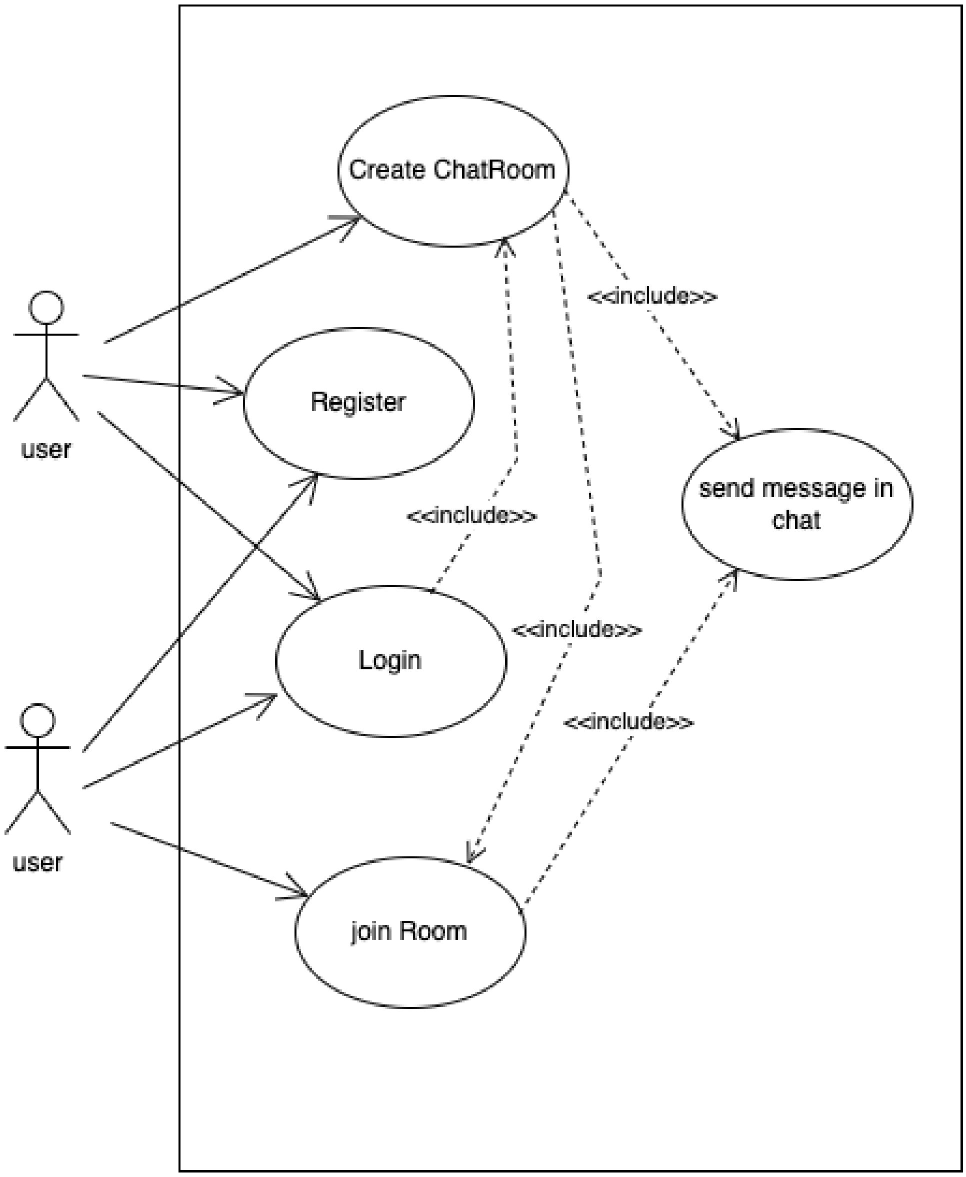


Figure 3.5: Usecase diagram of System

3.4.3 Sequence Diagram

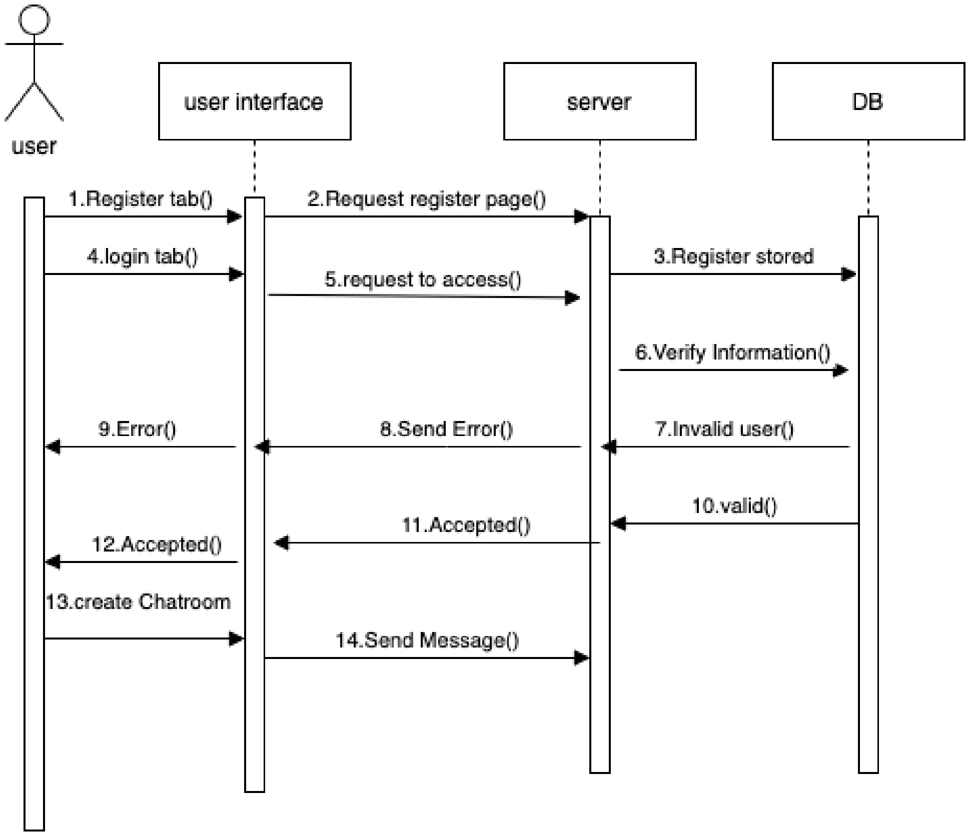


Figure 3.6: Sequence Diagram of System

3.4.4 Activity Diagram

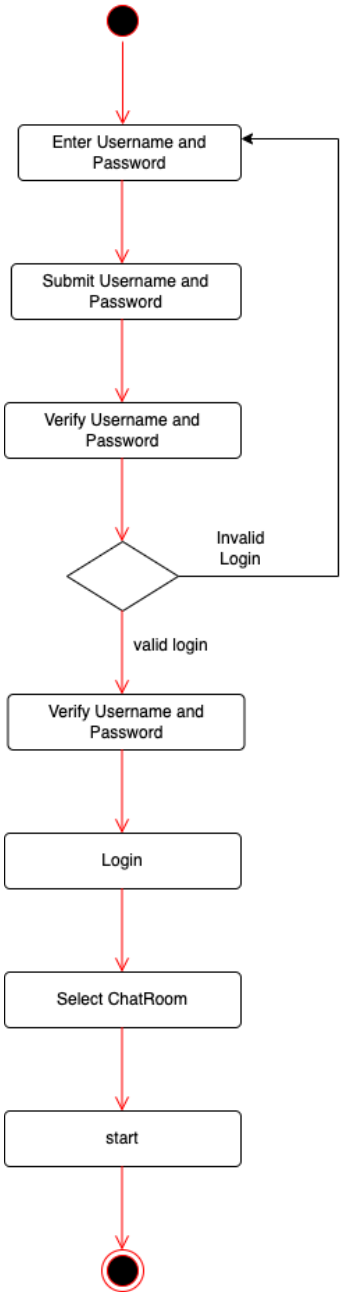

Enter Username and Password
Submit Username and Password
Verify Username and Password
Invalid Login
valid login
Verify Username and Password
Login
Select ChatRoom
start

Figure 3.7: Activity diagram of System

3.5 Software Development Model

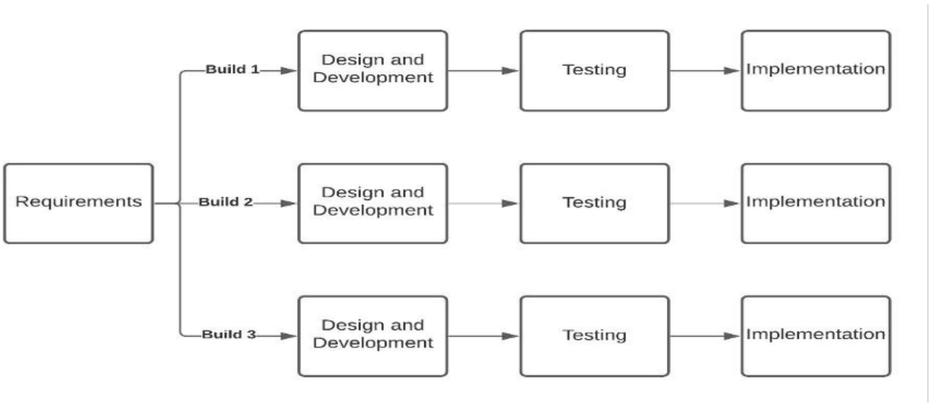


Figure 3.8: Software Development Model (Incremental Model)

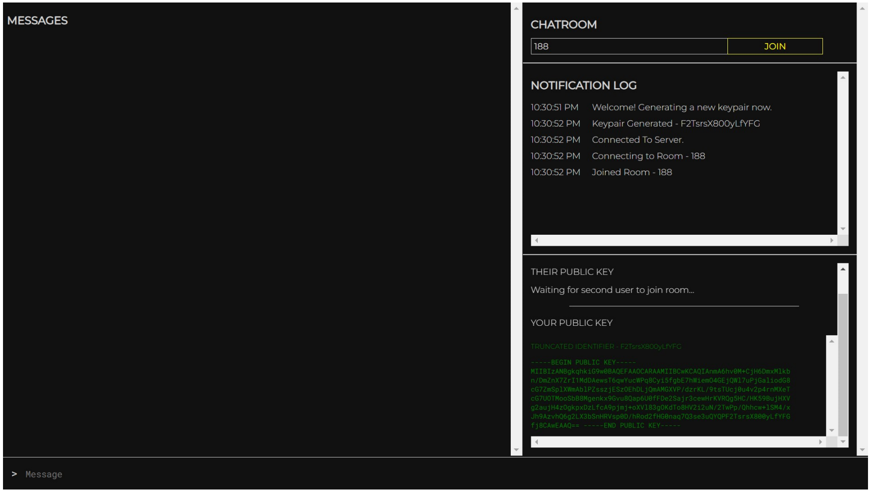
The project followed the incremental model of software development. At any time, the plan was made just for the next increment and not for any kind of long-term plan. Therefore, it was easier to modify the version as per our need. Each incremental version was developed using an iterative waterfall model of development. Each version of the software added more additional features than the previous ones. This model gave us the advantage of error reduction.

CHAPTER 4

RESULT AND DISCUSSION

4.1 Snapshots of Output

User interface for messaging:



188

```
10:30:51 PM   Welcome! Generating a new keypair now.
10:30:52 PM   Keypair Generated - F2TsrsX800yLfYFG
10:30:52 PM   Connected To Server.
10:30:52 PM   Connecting to Room - 188
10:30:52 PM   Joined Room - 188
```

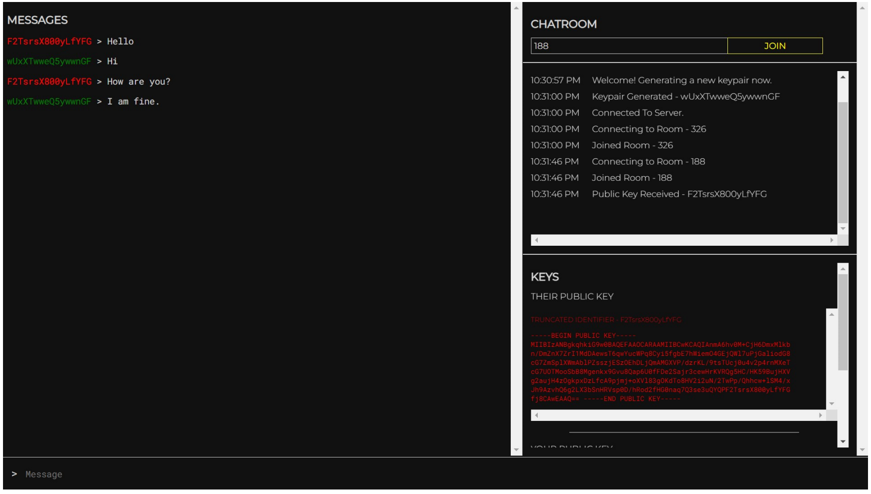
Waiting for second user to join room...

TRUNCATED IDENTIFIER - F2TsrsX800yLfYFG

```
-----BEGIN PUBLIC KEY-----
MIIBIzANBgkqhkiG9w0BAQEFAAOCARAAMIIBCwKCAQIAnmA6hv0M+CjH6DmxMlkb
n/DmZnX7ZrI1MdDAewsT6qwYucWPq8Cyi5fgbE7hWiemO4GEjQWl7uPjGaliodG8
cG7ZmSplXWmAblPZsszjESzOEhDLjQmAMGXVP/dzrKL/9tsTUcj0u4v2p4rnMXeT
cG7UOTMooSbB8Mgenkx9Gvu8Qap6U0fFDe2Sajr3cewHrKVRQg5HC/HK59BujHXV
g2aujH4zOgkpxDzLfcA9pjmj+oXVl83gOKdTo8HV2i2uN/2TwPp/Qhhcw+lSM4/x
Jh9AzvhQ6g2LX3bSnHRVsp0D/hRod2fHG0naq7Q3se3uQYQPF2TsrsX800yLfYFG
fj8CAwEAAQ== -----END PUBLIC KEY-----
```

Figure 4.1: Chat room

Client side interface for messaging:



```
F2TsrsX800yLfYFG > Hello
wUxXTwweQ5ywwnGF > Hi
F2TsrsX800yLfYFG > How are you?
wUxXTwweQ5ywwnGF > I am fine.
```

188

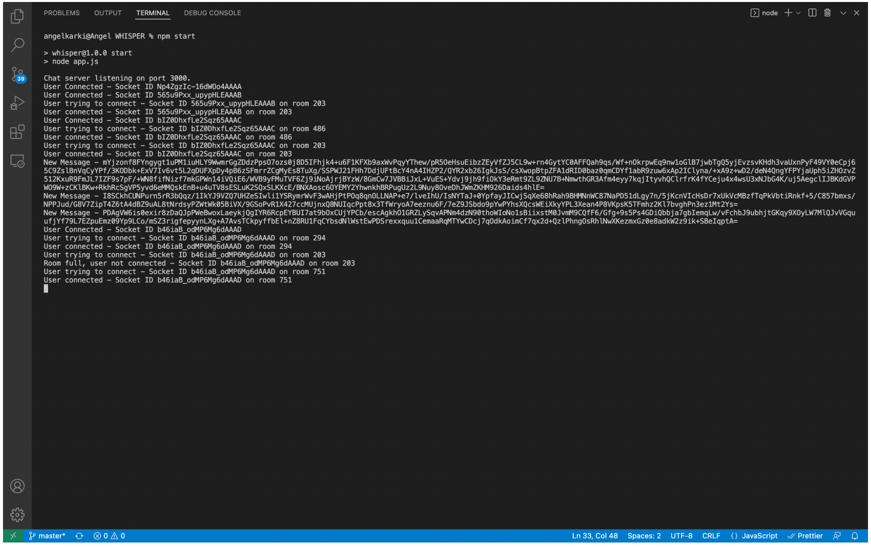
```
10:30:57 PM   Welcome! Generating a new keypair now.
10:31:00 PM   Keypair Generated - wUxXTwweQ5ywwnGF
10:31:00 PM   Connected To Server.
10:31:00 PM   Connecting to Room - 326
10:31:00 PM   Joined Room - 326
10:31:46 PM   Connecting to Room - 188
10:31:46 PM   Joined Room - 188
10:31:46 PM   Public Key Received - F2TsrsX800yLfYFG
```

TRUNCATED IDENTIFIER - F2TsrsX800yLfYFG

```
-----BEGIN PUBLIC KEY-----
MIIBIzANBgkqhkiG9w0BAQEFAAOCARAAMIIBCwKCAQIAnmA6hv0M+CjH6DmxMlkb
n/DmZnX7ZrI1MdDAewsT6qwYucWPq8Cyi5fgbE7hWiemO4GEjQWl7uPjGaliodG8
cG7ZmSplXWmAblPZsszjESzOEhDLjQmAMGXVP/dzrKL/9tsTUcj0u4v2p4rnMXeT
cG7UOTMooSbB8Mgenkx9Gvu8Qap6U0fFDe2Sajr3cewHrKVRQg5HC/HK59BujHXV
g2aujH4zOgkpxDzLfcA9pjmj+oXVl83gOKdTo8HV2i2uN/2TwPp/Qhhcw+lSM4/x
Jh9AzvhQ6g2LX3bSnHRVsp0D/hRod2fHG0naq7Q3se3uQYQPF2TsrsX800yLfYFG
fj8CAwEAAQ== -----END PUBLIC KEY-----
```

Figure 4.2: Chat room

Server side demonstration:



```
angelkarki@Angel WHISPER % npm start

> whisper@1.0.0 start
> node app.js

Chat server listening on port 3000.
User Connected – Socket ID Np4ZgzIc-16dWOo4AAAA
User Connected – Socket ID 565u9Pxx_upypHLEAAAB
User trying to connect – Socket ID 565u9Pxx_upypHLEAAAB on room 203
User connected – Socket ID 565u9Pxx_upypHLEAAAB on room 203
User Connected – Socket ID bIZ0DhxfLe2Sqz65AAAC
User trying to connect – Socket ID bIZ0DhxfLe2Sqz65AAAC on room 486
User connected – Socket ID bIZ0DhxfLe2Sqz65AAAC on room 486
User trying to connect – Socket ID bIZ0DhxfLe2Sqz65AAAC on room 203
User connected – Socket ID bIZ0DhxfLe2Sqz65AAAC on room 203
New Message – mYjzonf8FYngygt1uPM1iuHLY9WwmrGgZDdzPps07ozs0j8D5IFhjk4+u6F1KFXb9axWvPqyYThew/pR5OeHsuEibzZEyVfZJ5CL9w+rn4GytYC0AFFQah9qs/Wf+nOkrpwEq9nw1oGlB7jwbTgQ5yjEvzsvKHdh3vaUxnPyF49VY0eCpj6
5C9ZslBnVqCyYPf/3KODbk+ExV7Iv6vt5L2qDUFXpDy4pB6zSFmrrZCgMyEs8TuXg/SSPWJ21FHh7DdjUFtBcY4nA4IHZP2/QYR2xb26IgkJsS/csXwopBtpZFA1dRID0baz0qmCDYf1abR9zuw6xAp2IClyna/+xA9z+wD2/deN4QngYFPYjaUph5iZHOzvZ
512KxuR9FmJL7IZF9s7pF/+WN8fifNizf7mkGPWn14iVQiE6/WVB9yFMuTVF6Zj9iNoAjrjBYzW/8GmCw7JVBBiJxL+VuES+Ydvj9jh9fiOkY3eRmt9ZL9ZNU7B+NmwthGR3Afm4eyy7kqjItyvhQClrfrK4fYCeju4x4wsU3xNJbG4K/uj5AegclIJBKdGVP
WO9W+zCKlBKw+RkhRcSgVP5yvd6eMMQskEnB+u4uTV8sESLuK2SQxSLKXcE/BNXAosc6OYEMY2YhwnkhBRPugUz2L9Nuy8OveDhJWmZKHM926Daids4hlE=
New Message – I8SCkhCUNPurn5rR3bQqz/1IkYJ9VZQ7UHZeSIwli1YSRymrWvF3wAHjPtPOq8qnOLLNAP+e7/lveIhU/IsNYTaJ+0YpfayJICwjSqXe68hRah9BHMNnWC87NaPD51dLgy7n/5jKcnVIcHsDr7xUkVcMBzfTqPkVbtiRnkf+5/C857bmxs/
NPPJud/G8V7ZipT4Z6tA4dBZ9uAL8tNrdsyPZWtWk05BiVX/9GSoPvR1X427ccMUjnxQ8NUIqcPpt8x3TfWryoA7eeznu6F/7eZ9JSbdo9pYwPYhsXQcsWEiXkyYPL3Xean4P8VKpsK5TFmhz2Kl7bvghPn3ez1Mt2Ys=
New Message – PDAgVW6is0exir8zDaQJpPWeBwoxLaeykjQgIYR6RcpEYBUI7at9bOxCUjYPCb/escAgkh01GRZLySqvAPNm4dzN90thoWIoNo1sBiixstM0JvmM9CQfF6/Gfg+9s5Ps4GDiQbbja7gbIemqLw/vFchbJ9ubhjtGKqy9XOyLW7MlQJvVGqu
ufjYf79L7EZpuEmz09Yp9LCo/mSZ3rigfepyynLXg+A7AvsTCkpyffbEl+nZ8RU1FqCYbsdNlWstEwPDSrexxquu1CemaaRqMTYwCDcj7qOdkAoimCf7qx2d+QzlPhngOsRhlNwXKezmxGz0e8adkW2z9ik+SBeIqptA=
User Connected – Socket ID b46iaB_odMP6Mg6dAAAD
User trying to connect – Socket ID b46iaB_odMP6Mg6dAAAD on room 294
User connected – Socket ID b46iaB_odMP6Mg6dAAAD on room 294
User trying to connect – Socket ID b46iaB_odMP6Mg6dAAAD on room 203
Room full, user not connected – Socket ID b46iaB_odMP6Mg6dAAAD on room 203
User trying to connect – Socket ID b46iaB_odMP6Mg6dAAAD on room 751
User connected – Socket ID b46iaB_odMP6Mg6dAAAD on room 751
```

Figure 4.3: Encrypted message

4.2 Work Schedule

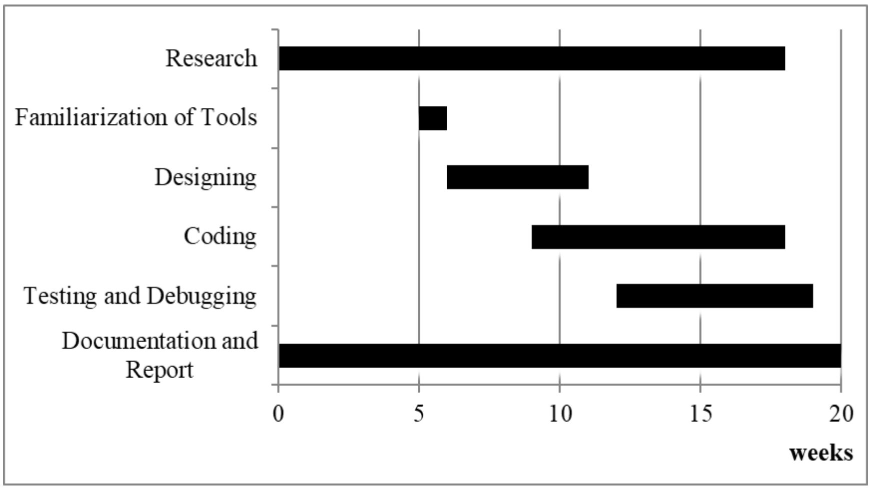


Figure 4.4: Gantt Chart

CHAPTER 5
CONCLUSION AND FUTURE ENHANCEMENT

5.1 Conclusion

Immense grown in computer technology has its own vulnerabilities. Thus, security would always remain an important issue. There have been huge amount of research in this sector to ensure a whole lot of community that expects to address their privacy policy. The main focus of project was to define requirements and parameters of a secure chat application which provides to users different aspects of security such as confidentially, cryptography, authentication, privacy. This application is able to work in real time and provides acceptable range of encryption and decryption time and provide a secure channel for communication. While working on this project, we learned various technique used for encryption of messages and the approach to hybrid cryptosystem. We successfully implemented few of them. But from our experiences, it was found that hybrid cryptosystem is more than secure to send a text message whereas it can be deployed to send files over the cloud and such security applications.

Thus, immense research in the field of computer security was done, realized different algorithms, implement them using a web chat application and have achieved objectives of this project.

5.2 Scope for future Enhancement

There are lots of scope for future enhancements in this system.The proposed application can be deployed to provide communication message security for another chat applications by just replacing the user interface by another one. Further work can be done to enhance the system by introducing group chat feature. Moreover,offline storage of the shared data can be maintained but needs to be encrypted to protect user's privacy.

REFERENCES

[1] H. Li and J. Li, “A new compact dual-core architecture for aes encryption and decryption,” *IEEE Canadian Journal of Electrical and Computer Engineering*, vol. 33, pp. 209–213, 2009.

[2] H. C. Williams, “A modification of the rsa public-key encryption procedure,” *IEE Transactions on Information Theory*, vol. 26, pp. 726–729, 2020.

[3] B. C. A.J. Elbirt, W. Yip and C. Paar, “An fpga based performance evaluation of the aes block cipher candidate algorithm finalists,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 9, pp. 545–557, 2001.

[4] M. E. Hellman, “An extension of the shannon theory approach to cryptography,” *IEEE Transactions on Information Theory*, vol. 23, pp. 289–294, 1997.

[5] A. S. K. Bhatele and M. Pathak, “a novel approach to the design of a new hybrid security protocol architecture,” *IEEE International Conference on Advanced Communication Control and Computing Technologies*, pp. 429–433, 2012.

[6] C. L. H. C. W. M. Y. Wang, C. P. Su and C. T. Huang, “Single and multi-core configurable aes architectures for flexible security,” *IEEE Transactions on Very Large Scale Integration Systems*, vol. 18, pp. 541–552, 2010.

[7] C. H. Kim, “Improved differential fault analysis on aes key schedule,” *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 41–50, 2012.

[8] H. W. Kim and S. Lee, “Design and implementation of a private and public key crypto processor and its application to a security system,” *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 214–224, 2004.