Trinity International College

(Under the affiliation of Tribhuvan University)

Dillibazar Height, Kathmandu, Nepal

A Project Proposal on

"MESSAGE ENCRYPTION USING IDEA"

Submitted to:

Department of Computer Science and Information Technology

Trinity International College

By:

Bhubal Karki, 16092/074

Saajan Shrestha, 16118/074

Ujjwal Khanal, 16130/074

7th Semester

2074

June 29, 2021

TABLE OF CONTENT

1. INTRODUCTION

Looking at the present situation we are in the age where almost everything is transferred and transmitted digitally, making them vulnerable to any and every kind of security threats discovered. To prevent these kinds of vulnerabilities or threats the use of cryptographic methods is encouraged. Cryptography can be defined as a method of storing and transmitting data in such a way that only those for whom it is intended can read and process it.

IDEA-International Data Encryption Algorithm is one of the techniques which can be implemented to guarantee the security of data transmitted during the communication. IDEA is a block cipher algorithm and was designed by Xuejia Lai and James L.Massey of ETH-Zürich in 1991. [1] IDEA was developed to replace the usage of DES algorithm during the early to late seventies. IDEA was developed to a very strong algorithm and used even in PGP email and file encryption products as a result of its proven design and great reputation. IDEA operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a round) and an output transformation (the half-round). [2] As the cipher key size is 128bits, in that respect IDEA is too strong (having taken care for weak keys). [3]

IDEA is a patented, strongly believed and universally applicable and appreciated block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental reason for the rise of this cryptographic algorithm IDEA was to ensure the military strength for all security requirements and easy hardware and software implementation. [2]

This algorithm is widely distributed throughout several working and security fields all over the world ranging from banking to other various industrial operations. They predestine the algorithm for use in a great number of commercial applications. The IDEA algorithm can be used alongside any encryption algorithm. Hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. [2]

IDEA encrypts the text into an unreadable format and makes it secured in order to send it over to the internet. The IDEA encryption algorithm provides high level security not based keeping the algorithm a secret, but rather upon ignorance of the secret key. [2]

2. PROBLEM DEFINITION

In this modern age where every human being is dependent on machines and spend most of their time ahead of their computers, data security automatically becomes a huge necessity. From simple day to day greetings to immensely confidential communication is done digitally and are demanded to be secured so as they don't get pried by the unwanted eyes.

3. OBJECTIVE

1) To ensure the secure transmission of data from sender to recipient.
2) To ensure proper key generation.
3) To ensure client side encryption of the message and the recipient side decryption results in the original message.

4. RESEARCH METHODOLOGY

4.1. Requirement Identification

4.1.1. Literature review

In [2], for the secure transmission of the data in the internet high security measures are taken into account in the hardware and software. Fields like video conferencing, business TV, email, sensitive financial and commercial data, and other transmission links are required to be secured via different methodology from any security breach.

In [3], time taken for execution of the system is taken into consideration and parallelism in the system provides better performance of the system. Multiple steps of algorithm i.e. key generation, encryption and decryption method of the plain text execution time varies from one another due to the execution of arithmetic and logical operation i.e. multiplication modulo, addition modulo and bitwise XOR.

4.1.2. Requirement analysis

a. Functional requirement

- Two actors, server and client are present in the system.
- Here, encryption and decryption in the client side.
- Server side is responsible for transmission of data between clients.

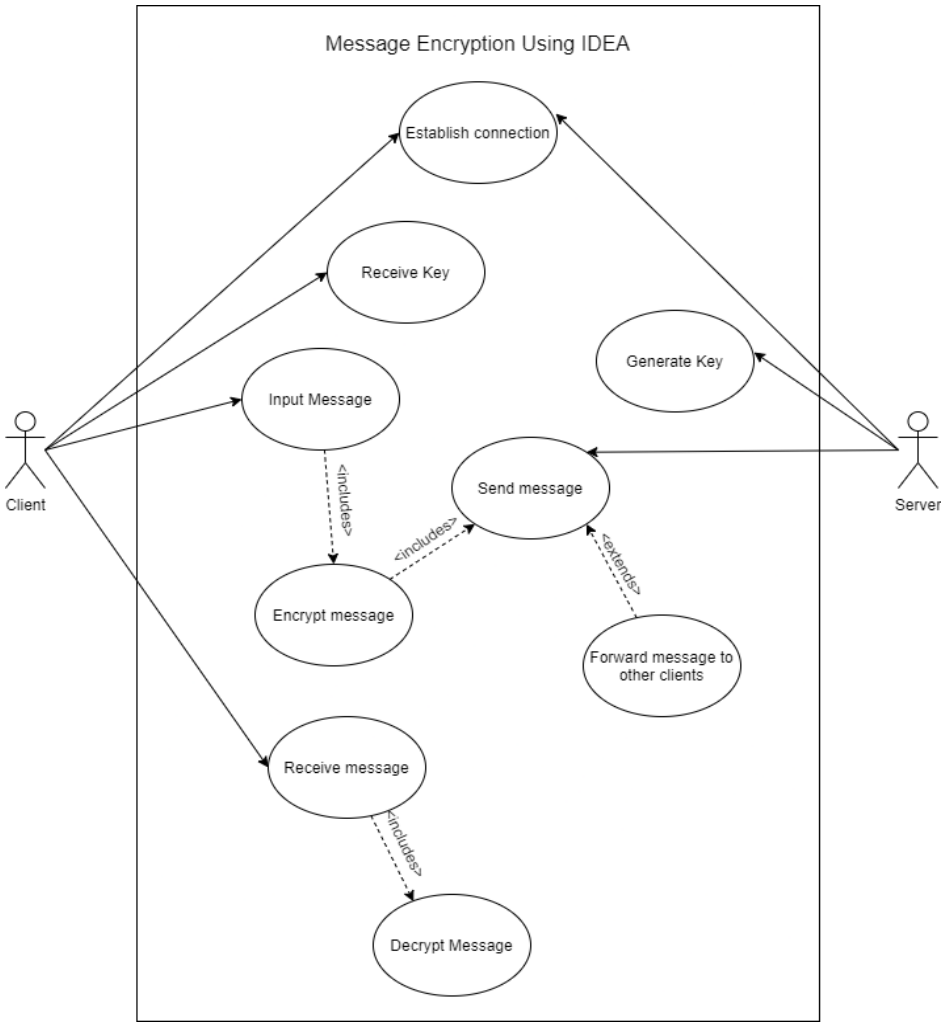

Figure 1: Use case of the system

b. Non-functional requirement

- Connection should be made between client and server before the encryption or decryption process
- Same key should be used by both clients [sender and receiver] during both encryption and decryption process.

4.2. Feasibility Study

4.2.1. Technical

The basic requirement for the implementation of the system can be general computer system that is capable of running basic programming scripts.

4.2.2. Gantt chart

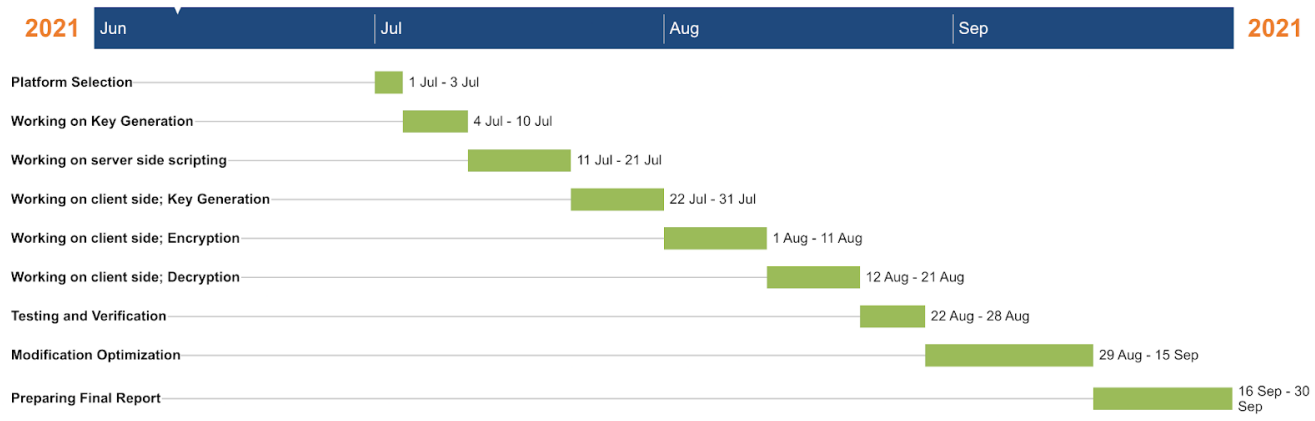

Figure 2: Gantt chart of the project work

4.3. Flow Diagram

a. Flow diagram of server system

With the starting of the server system a key is generated for both the encryption and decryption processes. It then waits for the client network for connections and once connected sends a key to the user. If the client is the sender, then it receives the encrypted message from the client and if receiver then the server sends the encrypted message to it.

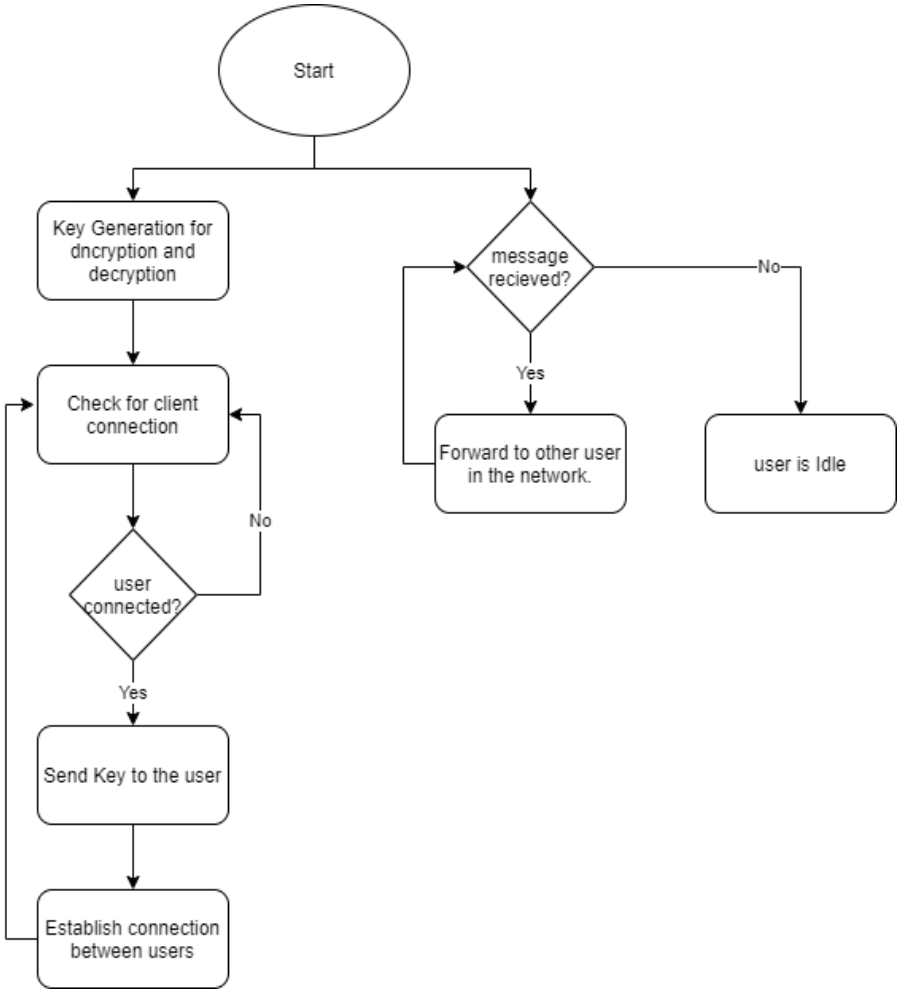

Figure 3: Flow diagram of server system

b. Flow diagram of client system

For the client system once connected to the server receives the key for communication from the server. If the connected user is the sender, then the sender encrypts the message using the key provided by the server and forward to the server. The receiver receives the encrypted message from the server and decrypts with the help of a key provided by the server and displays it to the user.

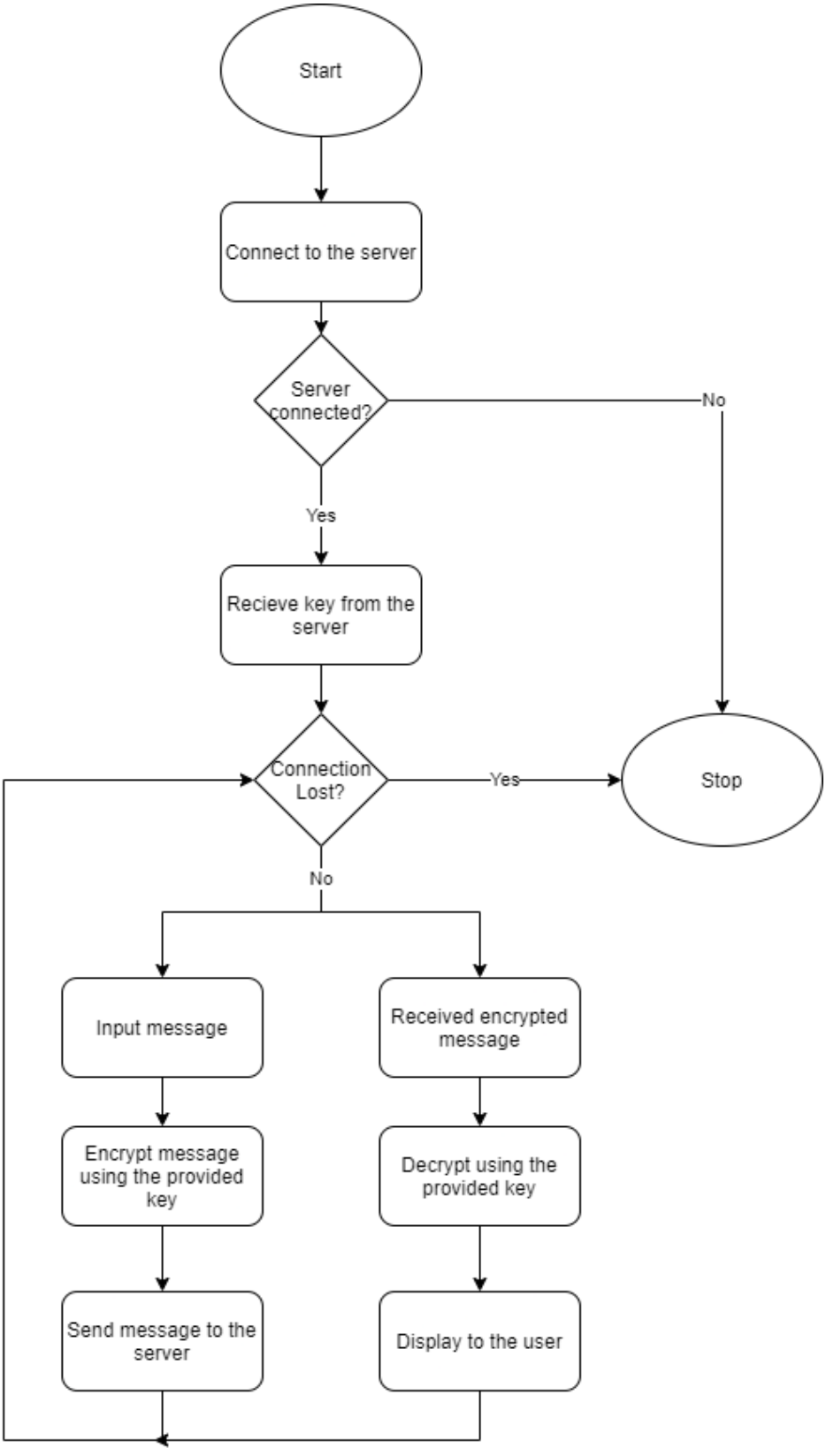

Figure 4: Flow diagram of client system

4.4. Algorithm

International Data Encryption Algorithm (IDEA)

IDEA is a block cipher algorithm. It is an encryption algorithm that operates on 64-bit plaintext and produces 64-bit cipher text using the key of 128 bit. It consists of a total of eight identical complete rounds and an output transformation of half round. [2]

There are 3 distinct operation performed in this algorithm [2]:

1. Bitwise XOR ($\oplus$)
2. Addition modulo ($\boxplus$)
3. Multiplication modulo ($\odot$)

Key generation steps of IDEA [2]

a. A 128-bit key is selected.

b. Then, the 128 bit of key is partitioned into eight 16-bit sub blocks.

c. The 8 blocks are directly used as the first eight key sub blocks.

d. Then, the 128-bit key is then shifted cyclically to the left by 25 position, after which the resulting 128-bit block is partitioned into eight 16-bit sub blocks to be used as next key sub blocks.

e. This cyclic shift is performed until all 52 16-bit sub blocks are generated.

Encryption of IDEA

The encryption process consists of eight identical rounds followed by an output transformation. First the plaintext is divided into 4 blocks. Each rounds consists of the following steps:

First keys are generated by using the key generation method described above for each round. Let the keys be K1, K2, K3, K4, K5, K6. and the input 4 blocks of plaintext be P1, P2, P3, P4.

1. D1 = P1 $\odot$ K1
2. D2 = P2 $\boxplus$ K2
3. D3 = P3 $\boxplus$ K3

4. D4 = P4 ⊙ K4

5. D5 = D1 ⊕ D3

6. D6 = D2 ⊕ D4

7. D7 = D5 ⊙ K5

8. D8 = D6 ⊞ D7

9. D9 = D8 ⊙ K6

10. D10 = D7 ⊞ D9

11. D11 = D1 ⊕ D9

12. D12 = D3 ⊕ D9

13. D13 = D2 ⊕ D10

14. D14 = D4 ⊕ D10

15. P1 = D1, P2 = D13, P3 = D12, P4 = D4

The above step is repeated for 7 additional rounds with the respective generated keys. For the output transformation round, the first 4 steps from above are performed and combined to get the cipher text. [1]

Decryption of IDEA

The operation for decryption is the same as the encryption method. The only difference is that each of the 52 16-bit key sub- blocks used for decryption is the inverse of the key sub-block used during encryption i.e. key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process. [2]

5. TESTING AND VERIFICATION

The outcome is tested as to know whether our message i.e. plaintext gets encrypted with the help of key on the sender side and the encrypted message could be successfully decrypted in the receiving side.

6. EXPECTED OUTPUT

The expected output of the system is that the user message will be encrypted and transmitted to another user who will decrypt the message without losing the original meaning.

7. REFERENCE

[1] Ms Snehal Patil, Prof.Vrunda Bhusari, *An Enhancement In International Data Encryption Algorithm For Increasing Security*, Volume 3, Issue 8 (International Journal of Application or Innovation in Engineering & Management, 2014), 64-70.

[2] S. Artheeswari, Dr. RM. Chandrasekaran, *INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) FOR DATA SECURITY IN CLOUD*, Volume 8, No 1 (International Journal of Technology and Engineering System, 2016), 6-11.

[3] Sandipan Basu, *INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION*, Volume 2, No 7 (Journal of Global Research in Computer Science, 2011), 116-118.