Encryption and Decryption for Secure Communication

Charu Rohilla
Research Scholar, M.TECH CSE Dept.
PDMCE, B.Garh

Rahul Kumar Yadav
Asst. Prof. IT Dept.
PDMCE, B.Garh

Sugandha Singh
Asso. Prof. CSE Dept.
PDMCE, B.Garh

ABSTRACT
In modern era, conferencing has become a mode of communication. Conferencing is a form of real-time communication in which all the computer users see the same screen at all the time in their web browsers. Conferencing are of many types like text, audio, video, web, teleconferencing. Conferencing means communication between local as well as remote locations. It includes reduction in travelling costs and ability to streamline decision making processes among geographically distributed teams. But conferencing still an imperfect substitute for face to face communication. The authors tend to be influenced more by speaker’s like ability than by the quality of his or her arguments. Also conferencing becomes insecure due to attacks like virus, information theft, unauthorized access, security attacks, etc. So there is a need to have secure communication. We have implemented a new system which includes text, audio and video conferencing system along with several other interactive features. Security is achieved by encrypting the data using playfair cipher substitution algorithm. The source code makes use of Java swings and JAR related application programming interfaces. To know the IP address of a particular machine jdk1.6 is used.

Keywords
SIP, PC, API, JAR

1. INTRODUCTION
Conferencing allow two or more locations to communicate simultaneously by two way text, audio and video transmissions. Conferencing is a form of communication between local as well as remote locations. A network socket is an endpoint of inter-process communication. Today most communication between computers is based on Internet Protocol so network sockets are Internet sockets. Socket address is the combination of IP address and port number. IP address is a 32 bit binary address and port number is a 16 bit integer. Sockets provide communication mechanism between two systems using TCP. TCP establishes connection and provides reliable service. Communication takes place in the form of streams. There are two types of streams which are Input stream to read data on socket and Output stream to write data on socket. Communication over network must be secure. Security consists of provisions and policies adopted by network administrator to prevent and monitor unauthorized access. For security the concept of port scanning is used. A port is an application specific and process specific software construct servicing as a communication endpoint in a computer host’s operating system. A port scanner is a software application designed to probe a server or host for open ports. The result of scan on the port is categorized into open, close and filtered ports. Although this system includes data transmission over network with port scanning but it does not provide advanced level of security. It only identifies for open and close ports but not identified as a percentage of overall traffic and not categorize on the basis of its contribution to network congestion and resource consumption. Currently client program and server program do not distinguish between client address extracted from log entries and IP address decrypted from the port knock sequence.

1.1 Encryption
Encryption is the process of encoding the messages or information in such a way that only the authorized party can read it. In an encryption the message or information is referred to as plain text, is encrypted using an encryption algorithm generating cipher text that can only be read if
decrypted. Decryption is the process of decoding data that has been encrypted into secret form. Encryption and Decryption is shown in Fig 1. There are two types of encryption and decryption known as symmetric key and asymmetric key encryption and decryption. In symmetric key encryption and decryption keys are the same. In asymmetric key, one key is used for encryption and other is for decryption.

![Fig 1: Encryption & Decryption Process](image)

1.2 Playfair Cipher
The playfair cipher is a symmetric encryption technique. The scheme was invented in 1854 by Charles Wheatstone but bears the name of Lord Playfair who promoted the use of cipher. The technique encrypts pair of letters. It uses a 5 by 5 table containing a phrase or keyword. To generate the key table first fill in the spaces in the table with the letters of keywords, then fill the remaining spaces with the rest of letters of alphabet in order.

2. RELATED RESEARCH
First research made an attempt to introduce sockets and its deployment pertaining to network programming. Sockets play a vital role in client server applications. The client and server communicate by writing to and reading from these sockets. Sockets works with TCP which provides a reliable and connection oriented service. Socket programming over Java has been preferred. When communication over network takes place, Java technology uses stream model. In the second research the attempt was made to investigate Remote Method Invocation. The advantages of socket programming over remote method invocation has been discussed. RMI is a technique to call a method or object of class from a remote location. It serves as a client server relationship. When a client port wants to invoke a remote method on a remote object, it actually calls an ordinary method of java program language that is encapsulated in a packaged object called stub. It resides on client machine, not on server. RMI programming is like programming in high level language. RMI limit us to client to needing to be another Java application. Sockets have tighter control over what is sent. RMI is strictly in Java. This can be fixed by socket programming. RMI can not guarantee that a client will always use the same thread in consecutive calls. The next research discusses Session Initiation Protocol, its capabilities, components and infrastructure. SIP is used to establish, modify and terminate a multimedia sessions. SIP provides new ways to develop presence based applications. SIP is an application layer protocol and incorporates many elements of HTTP and SMTP. SIP architecture consists of four layers which are syntax and encoding layer, transport layer, transaction layer and transaction user layer. SIP uses its request and response parameters. The various components of SIP are user agent, proxy server, registrar server, redirect server, location server, application server, session border controller, presence server, etc. Also to provide communication between two systems, SIP has its communicator known as Jitsi which is a free and open source multiplatform voice VoIP, videoconferencing and instant messaging application. The next research discusses the encryption and decryption technique. Encryption is the process of
converting a plain text into cipher text. Decryption is the process of converting a cipher text into plain text. The paper discusses the playfair cipher symmetric key encryption and decryption technique. In symmetric key process the encryption and decryption keys are the same. The playfair is harder to break since the frequency analysis of digraphs is more difficult. The playfair uses the 5 by 5 table containing a keyword or phrase. Memorization of keyword and four simple rules was all that was required to create the 5 by 5 table and use the cipher. The next research made an attempt to define swings. Swing is built on the foundation of AWT. Swing is the primary Java GUI widget toolkit. Swings provides a native look and feel. Swing has powerful components which are not implemented by platform specific code. Instead they are written entirely in Java and are platform independent. Swing defines a separate model interface for each component that has a logical data or value abstraction. This separation provides programs with the option of plugging in their own model implementations for swing components.

3. PROPOSED WORK
In the proposed work SIP in conjunction with TCP will be used to provide communication over the network. For the implementation of system eclipse software will be used. There will be addition of audio and video conferencing along with several other interactive features like call history, profile picture setting, status messages, screen sharing, etc. Communication will take place with the help of SIP communicator known as Jitsi. JAR related API and java swings will be used to implement the system. To make a contact with another machine jdk 1.6 will be used. The playfair cipher will be used to implement security in the system. This is symmetric key encryption and decryption technique in which same key will be used for both encryption and decryption. The system will have a well defined interface. The playfair algorithm algorithm will work by using a 5 by 5 table. To encrypt the message we have to break the message into digraphs and map them out on the key table. Z is added to complete the final digraph if needed. The two letters of the digraph are considered as the opposite corners of the rectangle in the key table. Note the relative position of the corners of rectangle. Then apply following four rules:
1. If both letters are the same then add after the first letter. Encrypt the new pair and continue.
2. If letters are on the same row then replace them with letters of their immediate right.
3. If letters appear in the same column replace them with letters immediately below respectively.
4. If letters are not on the same row or column replace them with letters of same row but at the other corners of the rectangle defined by the original pair.

4. RESULT ANALYSIS
We have implemented a secure communication system. For the implementation of system eclipse is used.
1. The Fig 2 below shows all the communication methods in the system like text, audio, video and screen sharing.
2. The Fig 3 shows the call from one person to another

![Fig 3: Call from one person to another](https://via.placeholder.com/150)

3. The Fig 4 shows a person who is online.

![Fig 4: Online](https://via.placeholder.com/150)

4. The Fig 5 shows the call history and has parameters like-
   1. Time of calls
   2. Type of calls
   3. Person with which call was made.
   4. All call history stored with login ID.

![Fig 5: Call history](https://via.placeholder.com/150)
5. The Fig 6 below shows the file menu and its options are:
1. Add new account
2. Add contact
3. Quit

![Fig 6: File Menu](image)

6. The Fig 7 below shows the picture option and it has the parameter
1. Image capture from webcam.

![Fig 7: Picture Option](image)

5. CONCLUSION
Communication over network must be secure so that it can reach to its destination without any harm. Communication with only port scanning could not provide secure communication. So we add encryption technique to achieve advanced level of security. The playfair cipher symmetric key encryption technique is used. Also in addition to text the audio and video conferencing is added to the system along with other interactive features. The eclipse software has been used for the implementation of system. The system makes use of Session Initiation Protocol and JAR related API to provide communication over the network.
6. REFERENCES


