# Secured Chat

Computer Networks CS2206

SUBMITTED TO A. PAWUT SATITSUKSANOH

Submitted by :
Sai Kham Lao 5748124
Deep Kumar 5818029
Nattalie Shinkoi 5835205

# Secured Chat

## Secured Chat

Chat rooms are online spaces where users can communicate with one another through text-based messages. The security element in chat room applications is important to ensure all message from users are protected from others. So, we need to provide some method to manage the security problem.

## Cryptography (Encrypt-Decrypt)

Cryptography is an important method to keep private data security in order to unauthorized access. In this project, We are working on the data encryption.

The architecture of the chat room application is divided into two parts. First is sender and second is receiver. This communication is connected via internet. In sender part, the sender is needed to enter a message using chat room interface. After that, the message will encrypt using encryption algorithm. Then, the message will send to receiver. In receiver part, decryption process will occur. The purpose of this decryption is to convert cipher text to plaintext.

In PKC Every user has a pair of keys which were related :

- Public key : known to everyone in the system with assurance
- Private key : known only by its owner

## Protocol

1. Connect both computer to the server.
2. Sender and Receiver agrees on a key.
3. Receiver sends his public key to Sender.
4. Sender encrypts the message with the receiver's public key and sends the ciphertext back.
5. Receiver decrypts the ciphertext using his private key.

# Facts

- Application is written in JAVA
- Chat implementation utilizes Socket IO (websocket + chat rooms)
- Divided into two sides. (Server : Client)
- Written using Eclipse program

# Function

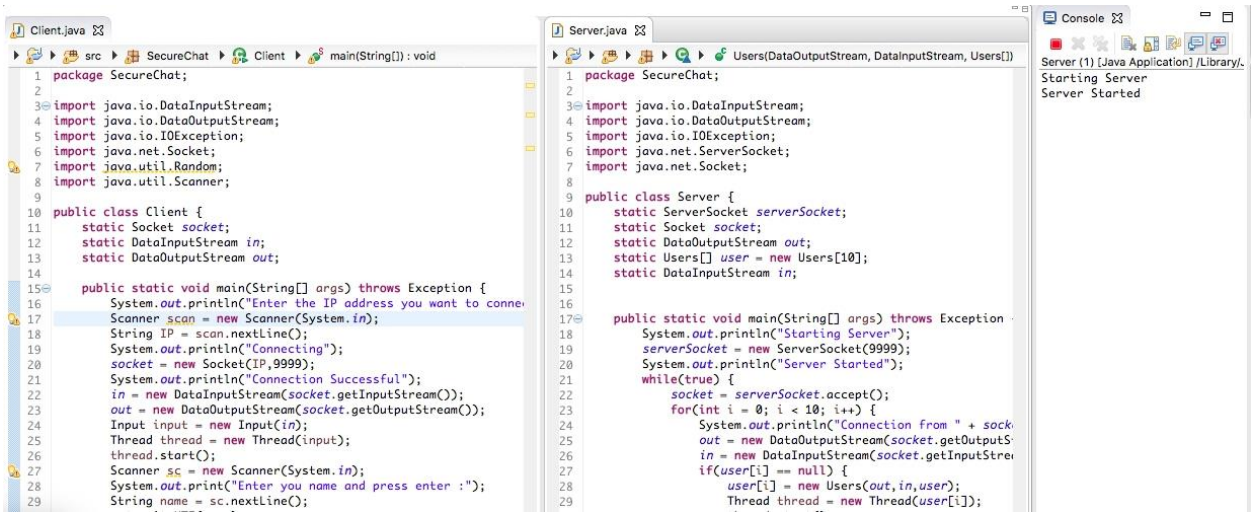
Server class :
Main, Users, Run()

Client class :
Main, EncryptMessage, ChangeKey, Run(), DecryptMessage, ChangeDecrypt

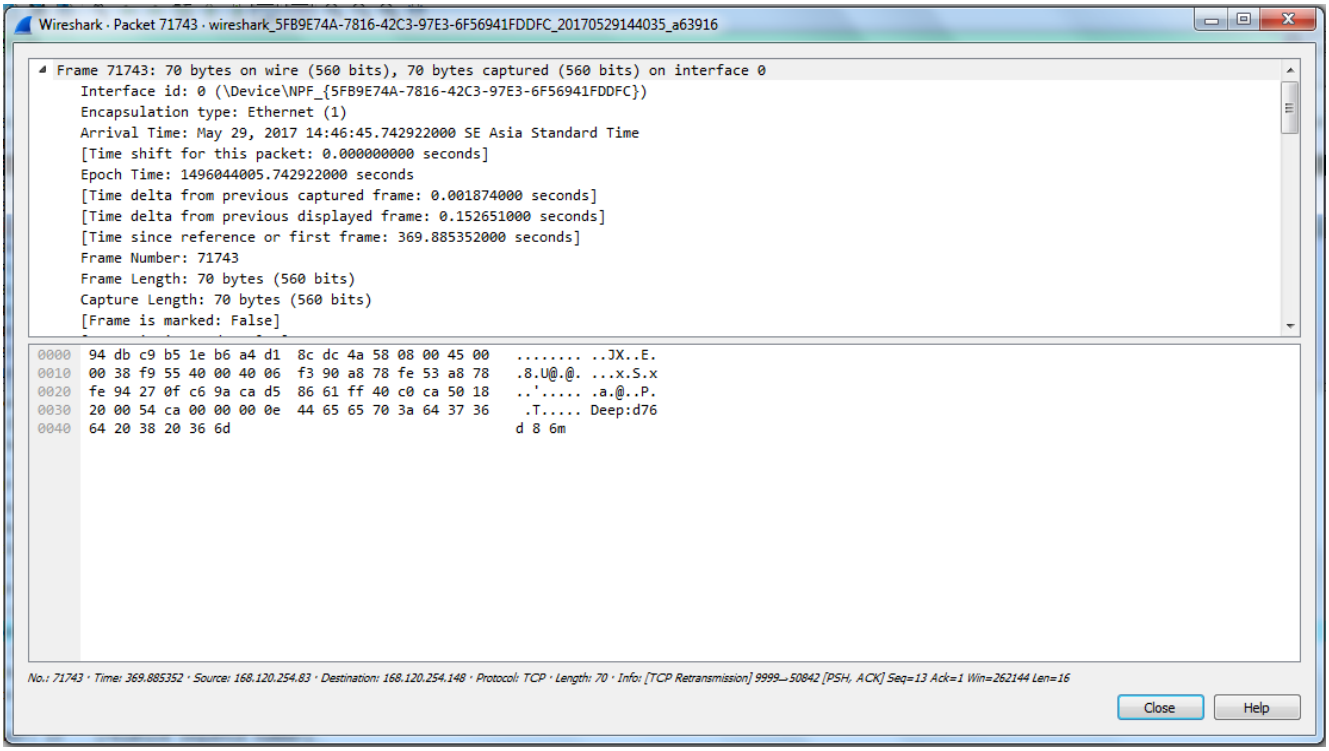
# Steps that are implemented for encryption

1. Define the logistic equation
2. Define sites for characters and vowels
3. Set the secret key

Start the application by running the console web-based program. Connect to the server.



Encrypt data at one end using the key, send it over the servers, and at the other end it can be read because the key is known.




The figure above show the message that has been sent from Deep. Once it's connected and sent out, It gets encrypt. The message has been converted to the other form and send over the network. (Last line)