

RSA Secure Chat Application

Avish Jain

Ajay Krishnan

Roshan John

Swattik Maiti

18BCE0421

18BCE0652

18BCE0975

18BCE0995

Vellore Institute of Technology, Vellore

Abstract

The aim of this project is to build a Chat application which is capable of sending messages with end to end encryption. This makes the messages secure and even if the message was intercepted by someone you won't be able to uncover the original message.

Keyword: Google Firebase Authentication, React Components, Hashing

1. Introduction

Communication is a mean for people to exchange messages. It has started since the beginning of human creation. Right now as technology has evolved people are using mobile phones to chat. But safety is of utmost importance. People want a safe medium to communicate. They do not want anyone else reading their messages. Hence we decided to make this project. This project is a Chat application secured using the RSA algorithm. RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. It is also a key pair (public and private key) generator. So in this application one can generate a room where multiple can join in by using room number. The first user will be the one who creates the room. And this chat application is highly secure so no one will be able to get information as we are using RSA algorithm to secure it. In order to read the message one will need both the public key as well as private key.

2. Literature Survey

S. no.	Title	Author	Published	Description
1.	UDP based chat application	Malhotra A., Sharma V., Gandhi P., Purohit N.	Published in 2nd International Conference on Computer Engineering and Technology April 2010	In this paper, a method was proposed to make a chat room using socket based on User Datagram Protocol (UDP) which enables the feature of acknowledgments after every message sent. It is equivalent to a dedicated chat server having a Server and n number of Clients[1].
2.	Design of Chatting Application Based on Android Bluetooth	Nikita Mahajan, Garima Verma, Gayatri Erale, Sneha Bonde, Divya Arya	Published in International Journal of Computer Science and Mobile Computing March-2014	Nikita Mahajan et al. proposed their research paper on design of chatting application based on android Bluetooth. Since the Bluetooth technology consumes low cost and power, they incorporated a system that enables the user to chat with each other over a Bluetooth connection. But this method might also face constraint as the range of the Bluetooth connection is restricted[2].
3.	Development of a real time chat application on intelligent network based on fuzzy logic	Kaur D., Dhanda P., Mirchandani M.	Published in Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems Aug. 2000	This paper describes the implementation of an intelligent chat group based on fuzzy logic. The chat group is based on client server model. The expert system based on fuzzy logic is developed in Java and monitors parameters, like number of clients, the idle time of each client etc., and then determines the priority of each client[3].

4.	Android Based Instant Messaging Application Using Firebase	Sai Spandhana Reddy Emmadi, Sirisha Potluri	International Journal of Recent Technology and Engineering (IJRTE), Jan 2019	The main objective of this paper is to present a software application for the launching of a real time communication between operators/users. The system developed on android will enable the users to communicate with another users through text messages with the help of internet. The system requires both the device to be connected via internet. This application is based on Android with the backend provided by google Firebase[4].
5.	Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application	Hüseyin Bodur and Resul Kara	Published in Proceedings.3RD International Symposium on Innovative Technologies in Engineering and Science at Valencia, June 2015	In this study, how RSA encryption algorithm and the secure messaging process on the SMS channel are realized in the devices with the Android operating system is examined thanks to the developed application. The application is tested with different key sizes for fast and powerful messaging. The different key sizes which can be used for key generation processes and changes occurring on encrypted messages are mentioned[5].

3. Proposed Method (or) System Design

3.1 RSA Encryption and Decryption

RSA works by generating a public and a private key. The public and private keys are generated together and form a key pair.

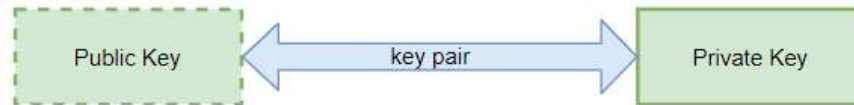


Fig. 3.1.1 Public key and Private key Generation

The public key can be used to encrypt any arbitrary piece of data, but cannot decrypt it.

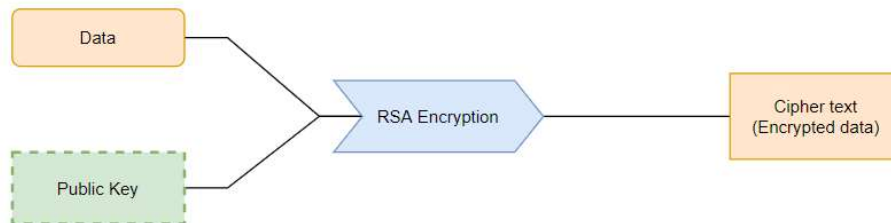


Fig. 3.1.2 Encryption using Public key

The private key can be used to decrypt any piece of data that was encrypted by its corresponding public key.

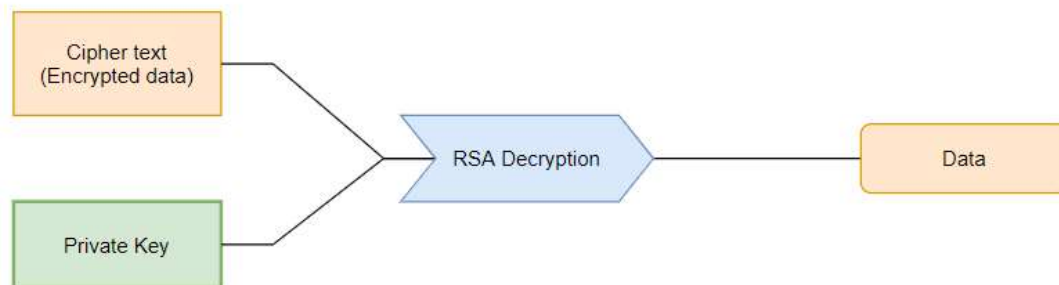


Fig. 3.1.3 Decryption using Private key

This means we can give our public key to whoever we want. They can then encrypt any information they want to send us, and the only way to access this information is by using our private key to decrypt it.

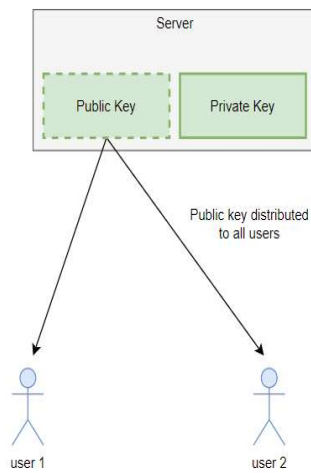


Fig. 3.1.4 Public key distribution

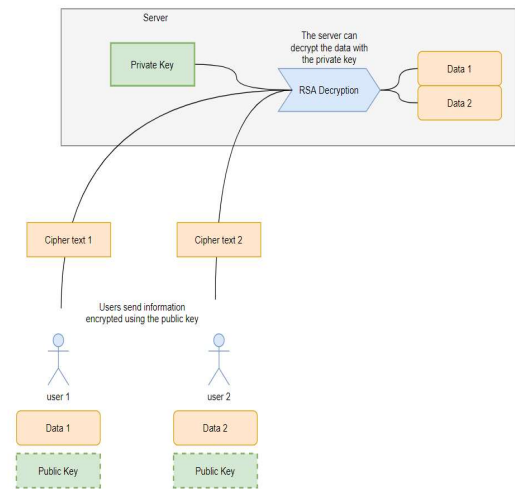


Fig. 3.1.5 Server decrypts data sent by the user using the private key

3.2 ER Diagram

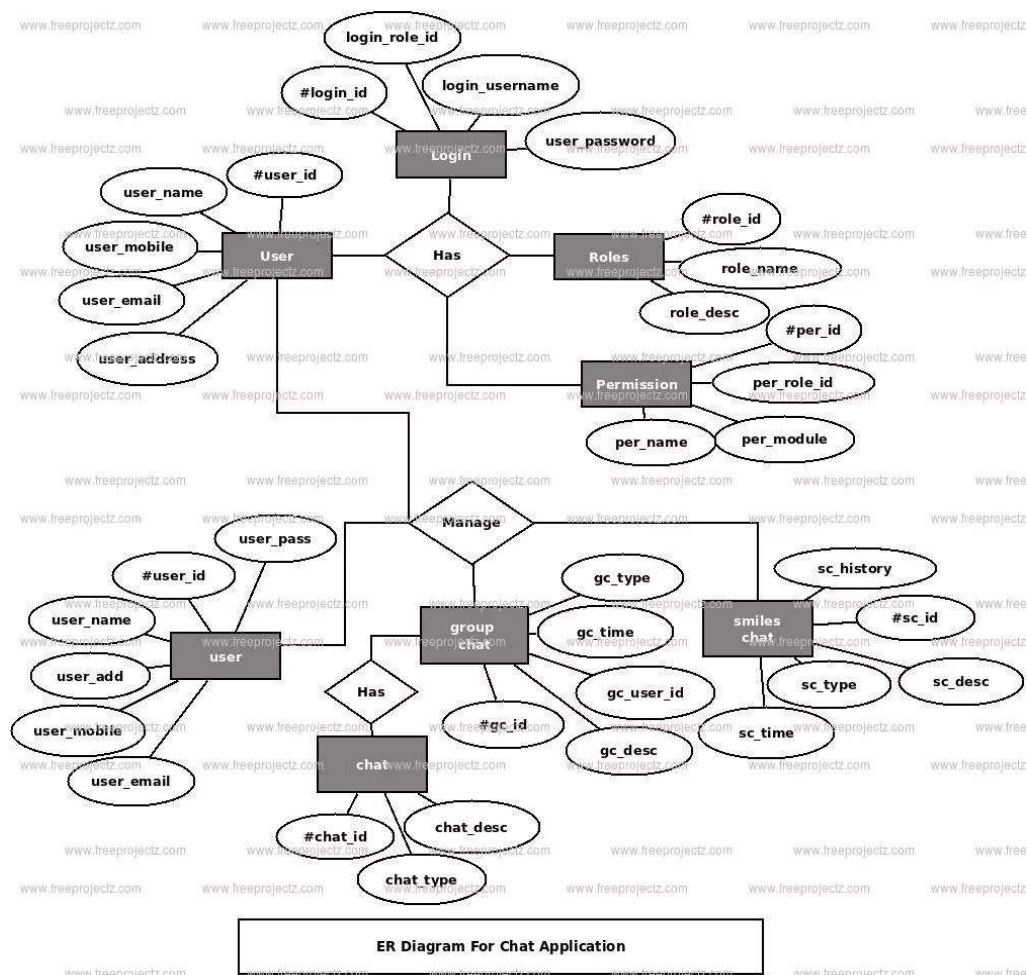


Fig. 3.2.1 ER Diagram

3.3 Functional Requirements

- The product shall have a user registration form
- The product shall have a database to store user information
- The product shall have a login system to log in the user
- Every user shall be assigned roles and permissions by admin
- Every user and admin shall be given access to change his user_id, password at any point of time
- Every user shall be able to access group chat and smiles chat
- Admin shall have the permission to remove a user.
- Every message passed between every user shall be encrypted such that confidentiality of the message is protected.

3.4 Non – Functional Requirements

Reliability

The system provides storage of all databases on redundant computers with automatic switchover. The reliability of the overall program depends on the reliability of the separate components. The main pillar of reliability of the system is the backup of the database which is continuously maintained and updated to reflect the most recent changes. Thus, the overall stability of the system depends on the stability of container and its underlying operating system.

Security

The system must automatically log out all customers after a period of inactivity. The system should not leave any cookies on the customer's computer containing the user's password. The system's back-end servers shall only be accessible to authenticated administrators. Sensitive data will be encrypted before being sent over insecure connections like the internet.

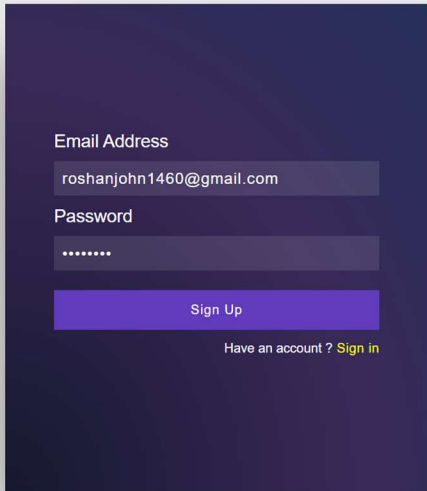
Maintainability

A commercial database is used for maintaining the database and the application server takes care of the site. In case of a failure, a re-initialization of the program will be done. Also, the software design is being done with modularity in mind so that maintainability can be done efficiently.

Portability

The application is HTML and scripting language based. So the end-user part is fully portable and any system using any web browser should be able to use the features of the system, including any hardware platform that is available or will be available in the future. An end-user uses this system on any OS; either it is Windows or Linux. The system shall run on PC, Laptops, and PDA etc.

4. Experimental Results and Analysis



A user authentication form with a dark purple background. It contains two input fields: 'Email Address' with the value 'roshanjohn1460@gmail.com' and 'Password' with masked characters '.....'. Below the password field is a purple 'Sign Up' button. At the bottom, there is a link that says 'Have an account ? Sign in'.

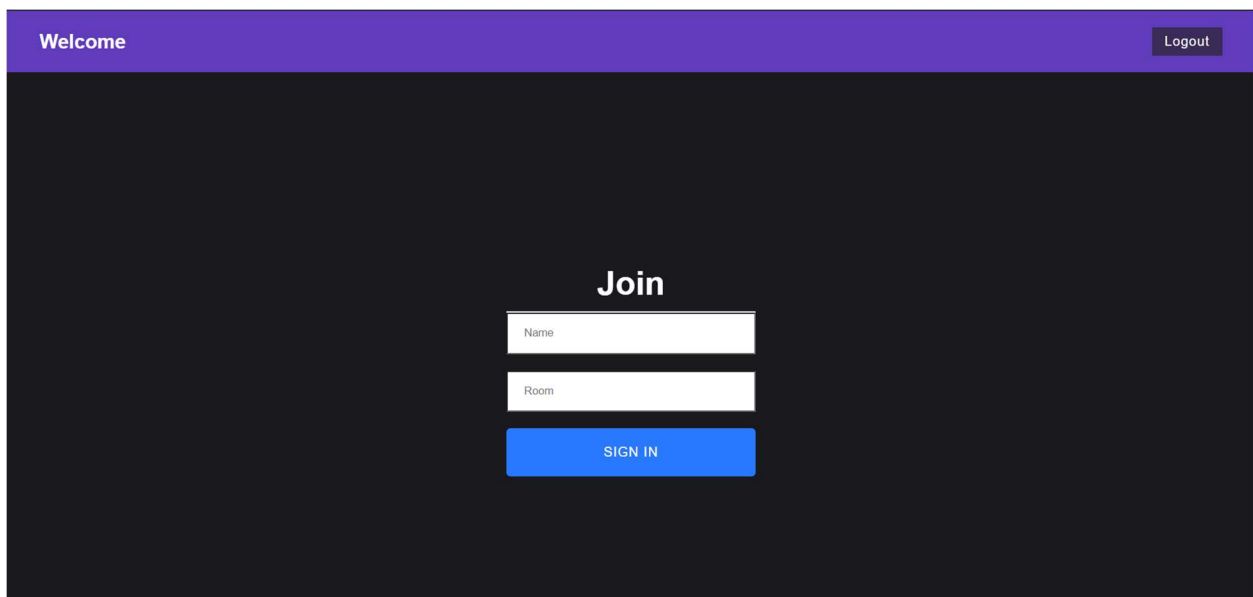
Email Address
roshanjohn1460@gmail.com

Password
.....

Sign Up

Have an account ? [Sign in](#)

Fig. 4.1 User Authentication



A 'Join Chat Room' form with a dark blue background. At the top, there is a purple header bar with 'Welcome' on the left and a 'Logout' button on the right. The main form area has the title 'Join' in white. Below the title are two white input fields: 'Name' and 'Room'. At the bottom is a blue 'SIGN IN' button.

Welcome Logout

Join

Name

Room

SIGN IN

Fig. 4.2 Join Chat Room

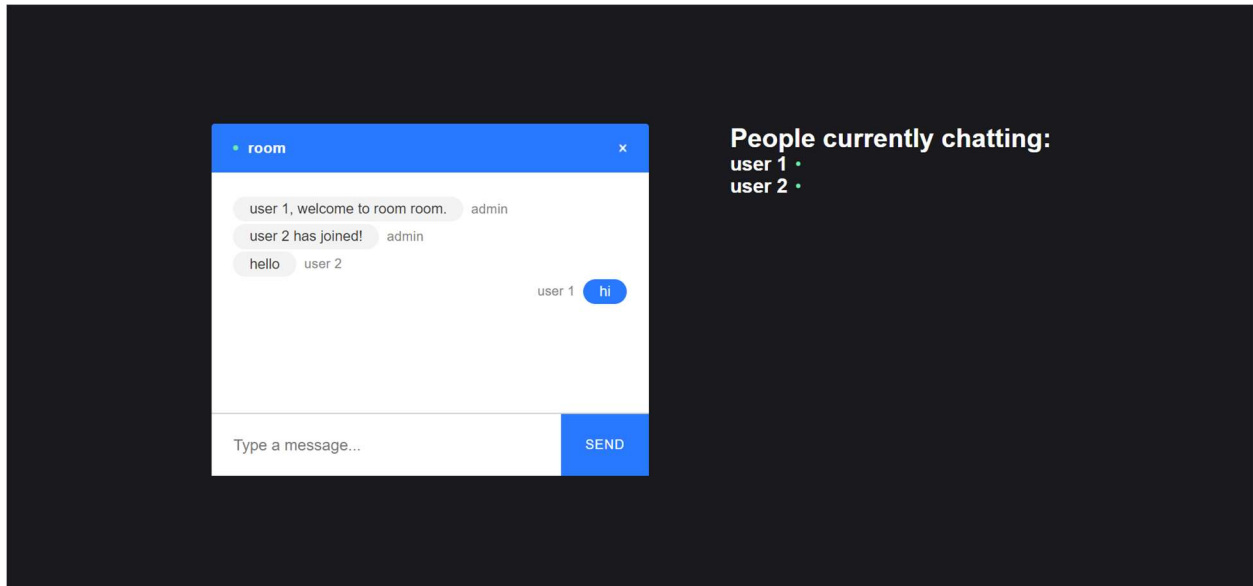


Fig. 4.3 Chat Room

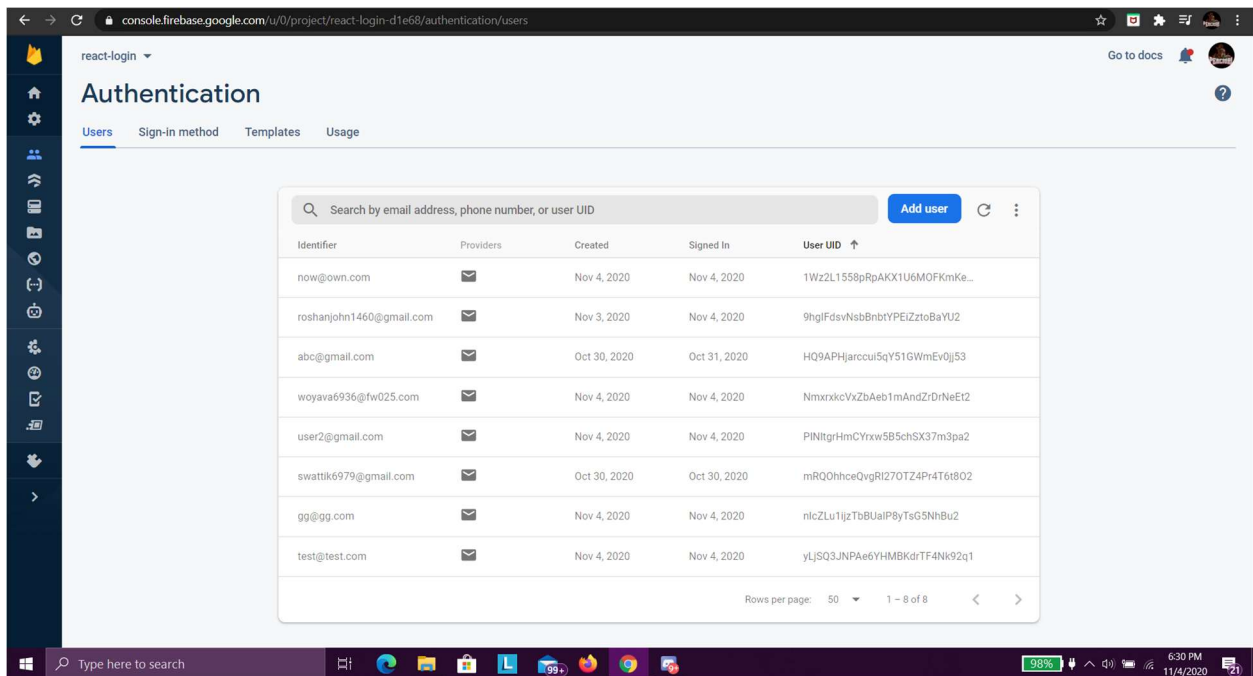


Fig. 4.4 Firebase Authenticated Users.


```
[
{
  id: 'HacIIsJwvAIhgq_2AAAB',
  name: 'user 1',
  room: 'room',
  publicKey: '-----BEGIN PUBLIC KEY-----\n' +
'MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKcAgEAvCQFMav+6bggIlsEebem\n' +
'xky0Q/hdjNuBTwO6Prv/mJLHT79nrkR3tuEsCB+ADqYAXekvt4YmDQLzkCDZTGHw\n' +
'wML10a9LppA1UQjhvooHKZH9mmO7smkYirfMDom7lMdtY5Au1MBQFcNLBRZDk3jI\n' +
'aoQ9883MRpYn1U7PY9/bIxhp/oFlV9JP7de1+dRUCJwKgsPzr8t8/nngBCKwjRAu\n' +
'gRUAP6IIoL0HokstgTGy3QMt8hzOR9cxLWEJ5A3QjVc8NOu1ZGmt6M9hBwZJPu\n' +
'F2NH5CUMm2Tbq0smoiQjx3aZ7RAHE3SIMLDwkoBVJhD9qo7CIM+vUD5x8hKUuZC\n' +
'qse2SWDU7NY+SyVXMzm1dcLm5VlFImKUK6rCyIJbPbU5GcKFsGv3QwGcOM7ov05I\n' +
'wh9FVzMOEsLOP/y4xe79nHgKjarGGGnz/+mr3D4MxT2G1npVC416uAzPgdoHgM17\n' +
'gYlEa8km1r4fd+z1GIEIkmn9UncXt+81p+TrarELMhnkaB3bV5HD116k2rNrN1b\n' +
'znrAtHTyqpREK0+NDzCdXtTvGwTo0A3iERHApqmI6qTdsZXEkY51czcVfwyHF95\n' +
'USHgi1AegGPq4D39hc8NIY4LdgQJAMh7v0tSeHCjAkYCh59buHj3kbAWAapEfH8A\n' +
'gbPiBK2QpQ1zPKdAbiD/i10CAWEAAQ==\n' +
'-----END PUBLIC KEY-----\n',
  privateKey: '-----BEGIN PRIVATE KEY-----\n' +
'MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkPAgEAAoICAQC9xAUxq/7puCAi\n' +
'wwR5t6bGTLRD+F2M24FPA7o+u/+YksdPv2euRHe24SwIH4A0pgBd6S+3hiYNvAOQ\n' +
'IN1MaHBYwvXRR0umkCVRCOG+igcpkf2aY7uyaRiKt8w0ibuUx21jkC6UwFAVw0sF\n' +
'FkoTEmhqhD3zzcxG1ifVts9j39sjGgn+gWVX0k/t16X51FRwnAqCw/Ovy3z+eeAE\n' +
'KTCNEC6BFQA/ogigvQeiSy2BMBLdAy3yHM5H1zEsZYQnkDdCNVzw066VmAy3oz2E\n' +
'Hbkk+40XY0fkJQybZNurSyaiJCPHdpntEAcTDIgwsPCSGFUMEP2qjsIgz69QPnEP\n' +
'yEpS5kKqx7ZJYNTs1j5LJVcz0aV1wub1wV8iYpSTqsLIgls9tTkZwoWwa/dDAZw4\n' +
'zui/TkjCH0VXMw4Sws4//LjETv2ceAqNqsYaA3P/6avcPgZFPYaWe1ULjXq4DM+B\n' +
'2iGAYXuBiURrySawvh937PUYh4iSaf1Sdxe37zWn50tqsQsyGeRoHdtXkc0XXXqT\n' +
'as2s2Vv0esC0dPKq1EQrT40PMJ1e108bB0jQDeIREcCmqYjqpN2x1eQSRjmVzNxV\n' +
'/DicX3lRKEALUB6AY+rgPf2ELw0hjgt2BAkAyHu/S1J4cKMCRgKHn1u4ePeRsBYB\n' +
'qkR8fwCBs+IERZCLDXM8p0BuIP+KLQIDAQABaoICAFApPIfBgebrwtp6nrqIvFY40\n' +
'zu307t1FV35F0F5DQ6t1gvBDySoGBONkTI3KNEDGZjZX+xv9FfPtDA4HGICG4b/o\n' +
'YyXb1rcsxhqtMkAMvJjU+hSzAJcgAzXNK1Yhb6EpWfiOE82sPEtcniH+uAwE4xs\n' +
'JPgbfM/EioXeXoC/DrDR204gyB/nw519uN4mg3SDY56Zrwh8Er1LZ6eT2EXdB8sI\n' +
'Lm4izi0mIJjL0jmGXRbH4g1Nu1fj0VcFJPIV8+FbbBcTX1b5ACw8S/yQKHxc3qKkT\n' +
'7BSocks261HaJDXr8f/+Safgkv557skEBBpIekkan1q7WVI4oNYiacuTKZYFjozt\n' +
'QIU+401m5NghvbnDk/VAuLnpmXFTgQSSAb7SXYCo/hHPFqi30X1+va07VZ1QWfr5\n' +
'zuJ2wG+0jgfoDUxY416XS1TYBWjaTF3fn1P42MdRJUq3W5fk8fVD6tQzD3C4fZLo\n' +
'ZsiTYr753N+uohtYaqgRiIE3IEvrtcONhzL3pr31h13PwxzFV8E9Fa7vD09dDTe\n' +
'plmdY/UMBS2TQzUdp2dj5YDtcIwwojs1h3iebdSB4zr1BtPSj/hkbTPBGR9qYA+t\n' +
'a8AVYL1g+k97IwbaYqjerwb2wSwq3+SguDZ1+9BGtAjXxoKzSdKXawtpQcJv4Piz\n' +
'Z6GEQ8n6UNvNdpnIApohAoIBAQDe1bRILn60Yd2jg2MLr4hGTeptrCURkgHtmeCe\n' +
'5ayuQMUTogD8N+F8mTa1SuAM2L5xfx0Xhz2V6R49fXxNKOga8xgIMENGnrHpP+lZ\n' +
'jw8UFp6dXINwAXZ20dwoM1xwLwUfquJOAyJ31HWRZoaeQ0VBil3ReAHRA8dyi3CR\n' +
'wY8nPpp05YTrx/wiILMm1aygOivR2ugJ1XMAJZX+e9nPwGPVD3IW8UKnjSFZVU1W\n' +
'1v73f4Sf/+17npLON104o4z0CkKQ1twR59wzH7fwxVGCIE6+TOH1wob1iV3uWuGf\n' +
'/BaMcIL2GPGRUpjZLDEZOnedevoFNF2g6sZIUpo7R+vBZPcXAOIBAQDaAlDQnSW9\n' +
'LyU86MYAlzVFH+Dct46PGubmXRe8ZbwAWxY616g9KL8MwhTHT1rYTTld0Tk4xMNL\n' +
'N21ScJICGH1AlcdIWNuZqqgtessHUUrvPuVUU3iugxUuV8ybcNdFPzVf1GNZFEIt0\n' +
'8xa6Qum9q1X6ceCIQFvUU7Fgfe1hoy1bUkNZ4vfSHEDTzxUyjqKzuIAC1CcI7r4a\n' +
'480Qpp7oEuupBIw+ByM4xer/9Qno+cind4Uct01a36kqSSjBEFw/YmGvklY6NKar\n' +
'QPRPKquDuMirf/V5DTEMPE4TEo22dnawz74evSYP4Ta/Ir1guNpuL3ht8A4xAdez\n' +
'qDnAwngFGxNbAoIBAQDHyy8Sw0/wdQ9N7RV18mWcisFV6u+sPhotkT+Uzmvp65jC\n' +
'9CDHjftCeXejVmEN/a7CfXv5fpCTn+joGm1r2UwTURFS2mSIPx1wWTiiYdrfhdHf\n' +
'G1wd1ifdyBMXgKCH3PrXsB8YsONZXmSoerW/z0+eSoHSGXB/A9KN4skSEsDV28V3\n' +
'DZwXIXWxLOIoh0rUf9K+4II5eR1Sq08AS6/EniB2F4D9mFj1sa+CcLpofQ5DpT11\n' +
'sRm9QFGZ5LkbIfSutC2FzktSVkYJFLuQ2+4n4mKZErYa0SnFH1oGghnC/lzqww3b\n' +
}
```

Fig. 4.4 (a)

Reference

1. Malhotra A., Sharma V., Gandhi P., Purohit N., UDP based chat application, Published in 2nd International Conference on Computer Engineering and Technology April 2010
2. Nikita Mahajan, Garima Verma, Gayatri Erale, Sneha Bonde, Divya Arya, Design of Chatting Application Based on Android Bluetooth, Published in International Journal of Computer Science and Mobile Computing March-2014
3. Kaur D., Dhanda P., Mirchandani M., Development of a real time chat application on intelligent network based on fuzzy logic, Published in Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems Aug. 2000
4. Sai Spandhana Reddy Emmadi, Sirisha Potluri, Android Based Instant Messaging Application Using Firebase, International Journal of Recent Technology and Engineering (IJRTE), Jan 2019
5. Hüseyin Bodur and Resul Kara, Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application, Published in Proceedings.3RD International Symposium on Innovative Technologies in Engineering and Science at Valencia, June 2015