SECURE MESSAGE COMMUNICATION

An Android Application

Assistant Professor Tanya Singh
Uday H R
Master of Computer Application
In
Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India

***Abstract*:** Sharing crucial information over the digital medium has become very painful these days. As the technology grows even the risk like digital crime is also emerging more day by day. In that hacking is a one major thing which puts any system or organization in a great risk. So, to avoid such risk and protect confidential information that travels across public network encryption technique came to picture for ensuring end to end encryption of normal text into cipher text in more secure way. But, the application's that providing these kind of a facility are lagging with some advance features. So, to overcome that issue we have come up with new idea of building an application that provides more strong support for encryption for text messages that which helps to avoid of getting hacked by the third party who doesn't have the privilege to access that information. So, In this work, we are going to make one secure message communication app, where one user can send message to some other user. That message has to be encrypting using symmetric algorithm, and that encrypted message will send to other user and vice versa. This application helps user by providing special feature like multiple options of 4 different Algorithms in which user could select and use for the Encryption.

By doing this user will be provided with more options of encryption that which helps to keep their confidential text information safe and secure over the public network.

I. INTRODUCTION

The main goal of a cryptography is to transmit the plain text into cipher text(encrypt) and reverse of encrypting process(decrypt). The objective of transmitting the plain text to cipher text is to secure the original data from the anonymous user.

The Cryptography uses mathematics to encrypt and decrypt the information. it enables to user to transmission or storage of the message through insecure ways In the confidential message only the authorized receiver should be able to extract the content of ciphertext. The ciphertext is the major pristine in modern cryptography, data, and network security.

The primary goal of such ciphers is to provide confidentiality for data transmitted in insecure communication environments. The ciphertext is used to provide confidentiality for data transmitted over public network environments. A block cipher can also be used to build other secret-key cryptography archaic, such as stream ciphertext, hash functions features.

Cryptography is the process of encrypting the confidential information before transmitting them to another receiver or phone and then decrypting them when they reach the intended destination. when an information needs to be transmitted to represents different ways to make that transition of information from one computer another phone then it becomes vulnerable to the hackers. The cryptography to another computer safe, secure and unharmed. in this process Firstly, the message or information is scrambled by the sender. and, then the sender encrypts that message or information. when the information encrypted that message is sent to the sender.

The Cryptography uses mathematics to encrypt and decrypt the information. it enables user transmission or storage of the message through insecure ways such as the internet. thus, the message can flow from sender to receiver and it will be unreadable to another person, it can only be understood by its recipient. The cryptography strength this measured according to the resources and time required to retrieve the original plaintext through encrypted text. Cryptography services are capable to exchanging the information between participants in a way that prevents others from reading it. Cryptography that is based on representing the information as numbers and mathematical pattern operate these numbers.

II. OBJECTIVE

The objective and scope of this project are 'Secure message Communication' by using four different algorithms (i.e. AES, RSA, RC4, and BLOWFISH) that provided user data with protection by adding anyone algorithms amongst these to which user selects and transmitted to another user/device over the public network and vice versa.

III. SYSTEM ARCHITECTURE

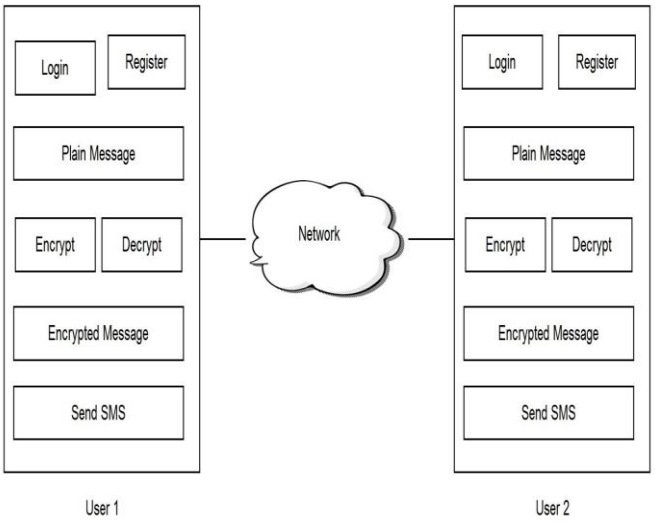


Figure-01

User has to register and login to access this application feathers. In this system architecture, user 1 is encrypting a plain message and he/she is sending that encrypted message to user 2by selecting anyone type of an algorithm that is present in the drop down list. Then user 2 has to copy that message and he/she has to decrypt that message by using that same algorithm, then user 2 can able to see the original message.

IV. HARDWARE & SOFTWARE REQUIREMENTS

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 500 GB.
- Ram : 4 GB
- Any System/Laptop with the above mentioned configuration

SOFTWARE REQUIREMENTS:

- Operating system : Windows7/8
- Coding Language : Java (Jdk 1.7)
- Database : SQLite
- Android : ADT bundle
- One Smart Phone

V. PROBLEM STATEMENT

The current messaging applications are unaware about the security threats and losses that could occur while sharing the data/information over public network due to lack of protection. So, when the privacy is highly valued, it's resulted in developing an android based secure messaging application that will ensure confidentiality, integrity and the availability of the SMS sent via public/GSM network.

VI. EXISTING SYSTEM FEATURES

- The innovation of text Messaging service has extensively evolved the nature of communication and information sharing.
- Lakhs/Millions of text messages that are exchanged daily across the world are done in the form of transparent text format and hence user privacy and security is under threat.
- Current Application are not providing multiple encryption option
- Current Application are not providing much information about the Algorithms that they use

VII. FEATURES OF PROPOSED SYSTEM

In this system, we propose a secure message communication using encryption technique which provides security to both the user. Here we are developing one android application, which will install to the user android device when some user wants to communicate with some other user, the sender has to encrypt the message and he/she has to send an encrypted message to the receiver mobile number. When receiver will receive the encrypted message then he/she has to decrypt and then the original message will display.

VIII. CONTEXT DIAGRAM

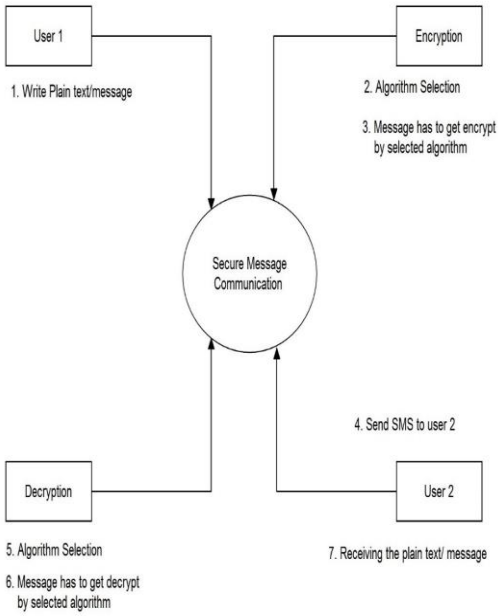


Figure-2

IX. USE CASE DIAGRAM

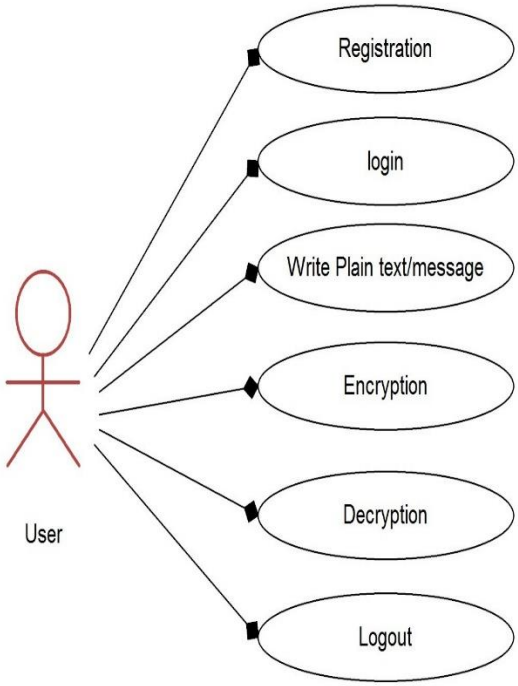


Figure-03

X. TEST CASES RESULTS

TEST CASES:

TEST 1:

Scenario: when you try to log in without doing the registration.

Description: it must show the error.

Status: Pass

TEST 2:

Scenario: when you try to register using the same information which already exists in the database

Description: It will throw an error.

Status: Pass

TEST 3:

Scenario: when you try to send message without selecting algorithm it throws an error

Description: it throws an error.

Status: Pass

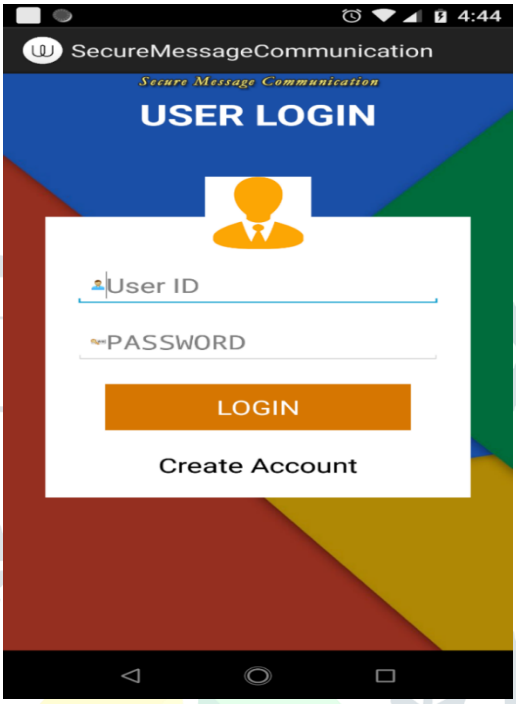
TEST 4:

Scenario: When you do mistake while entering phone no.

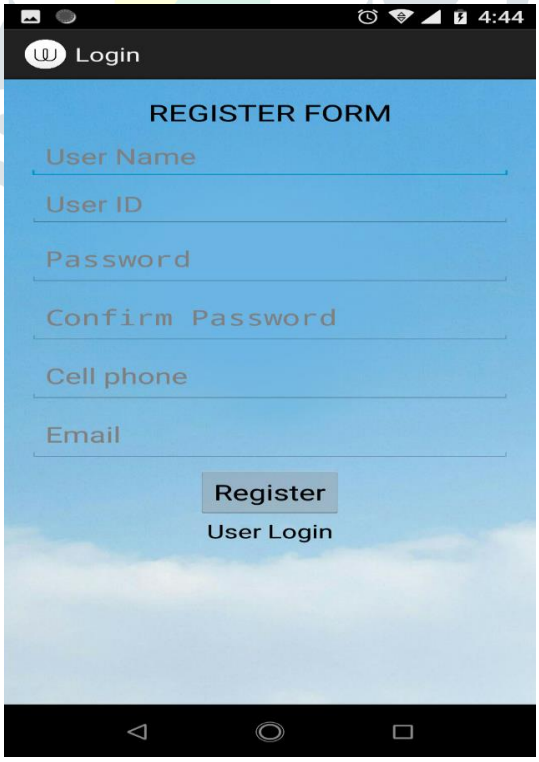
Description: it throws an error.

Status: Pass

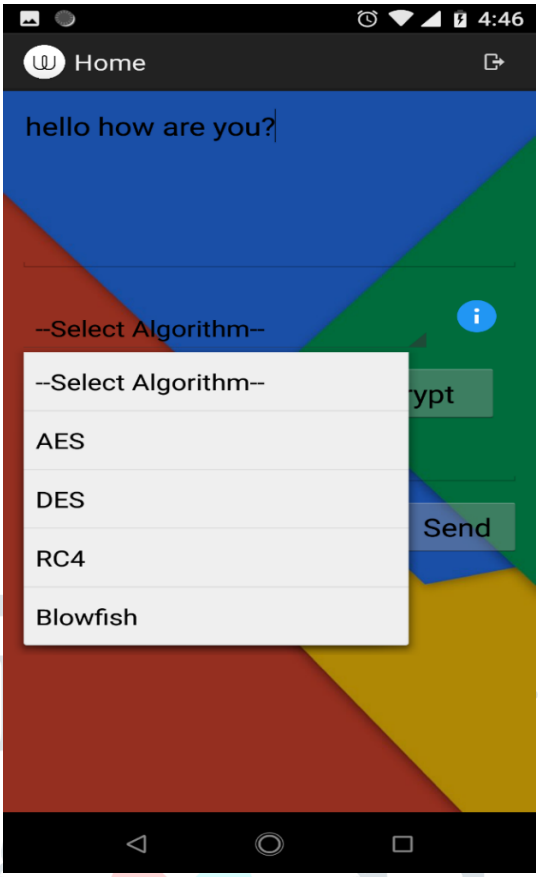
XI. SCREENSHOTS



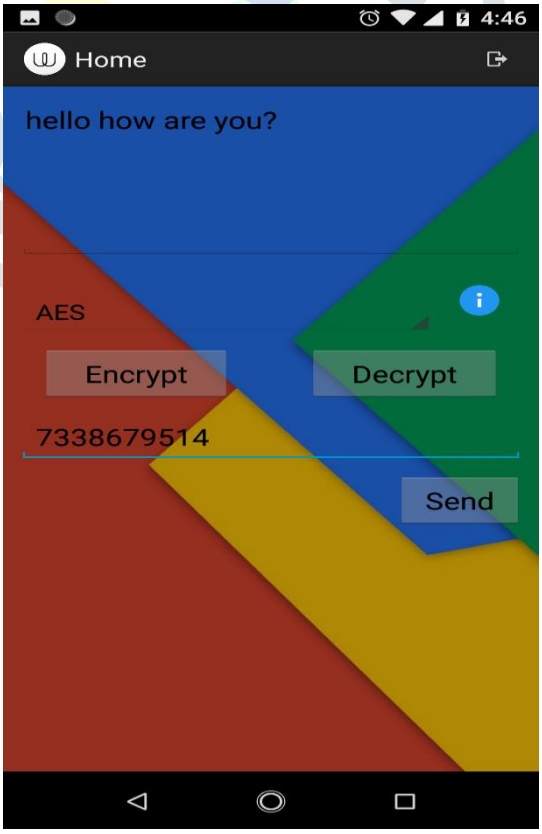
Screenshot-01



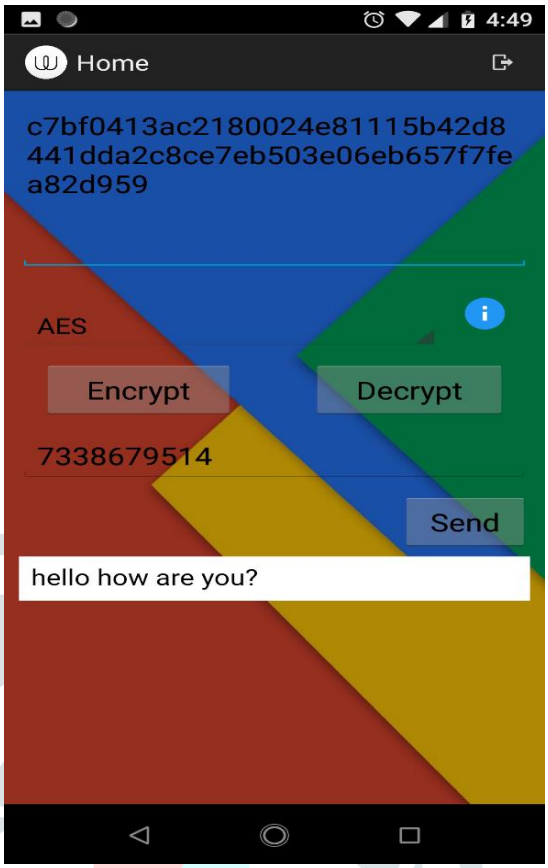
Screenshot-02



Screenshot-03



Screenshot-04



Screenshot-05

XII. FUTURE ENHANCEMENT

1. Planning to ADD more features for encryption like Image encryption, Video encryption, and chat room.

2. Adding such features will increase the flexibility of the Applications

3. We will be working on UI as well to make it to look more premium and topnotch.

XIII. CONCLUSION

To conclude, Project "Secure Message Communication" which has been developed using Android. This project helps users to secure the data communication by hiding the original content of the data in an encrypted format which helps users to hide their confidential and private data by selecting any Algorithm from the drop down menu. Which provides Easy implementation and Generate output flexibly. Thus, the project entitled 'SECURES_MESSAGE_COMMUNICATION' should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project.

Key features of this application

It is easy to encrypt and decrypt. User friendly environment. Generates PUBLIC and PRIVATE key Using multiple algorithm technique.

- Generates Symmetric keys.
- Provides secure communication between two registered users/smartphones.

XIV. Bibliography

Review through Books

[1].Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.

[2].Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: Prentice-Hall, 2001

[3].Hoffstein, Jeffery, Pipher, Jill and Silverman, Joseph H. NTRU: A Public Key Crypto

[4].http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU

[5].Kurose, James F., Ross, Keith W., Computer Networking: A top Down Approach Featuring the Internet. 2nd edition. Addison Wesley 2002.

[6].www.cdt.luth.se/~peppar/docs/lic/html/ node66.html

[7]. www.codenotes.com

[8]. www.dotnetspider.com

[9]. www.gotdotnet.com

[10]. msdn.microsoft.com

[11]. www.dotnet247.com

[12]. www.cs.columbia.edu

I. Biography

ASST. Prof. TANYA SINGH
Faculty & Guide Department of Computer Science & IT-MCA
Jain (Deemed-to-be University) Bangalore, India

Uday H R
Master of Computer Application in Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India