Android based Secure End to End Encrypted SMS System.

Bekkem Sumanth Reddy[1]
Computer Science and Engineering
Lovely Professional University
Phagwara, India

Mohiddin Shaik[2]
Computer Science and Engineering
Lovely Professional University
Phagwara, India

Parihari Harish Seervi[3]
Computer Science and Engineering
Lovely Professional University
Phagwara, India

Savleen Kaur[4]
Assistant Professor, Department of Computer Science and Engineering,
Lovely Professional University,
Phagwara, India

---***---

Abstract— Encryption is especially important if confidential details will be transmitted over the internet. A text message is one of the main means of information trade between mobile users. SMS security is one of the major issues to be addressed during statistics transfer. Therefore, the use of Android technological know-how the system is developed by us that allows the sender to enter the code in the messages before it is sent over the internet for this reason, the encryption manner, as a cryptographic algorithm, we used the Advanced Encryption Standard (AES). The app permits the consumer to enter a key and Already Exists a message to encrypt and therefore generate encrypted messages that can be deleted in writing by the recipient. The encrypted text developed through the appeals resists Brute-Force attacks as we use AES.

Keywords—SMS, AES, Encryption, Decryption, Key (key words**)**

I. INTRODUCTION

The use of smartphones has flourished over the past decade. Strong growth is due to strong computer skills, great storage capacity and personal help instead of making calls or texting. The high performance and comfort of Smartphones helps people to access their information such as bank accounts, ship / get hold of emails, cellular payments, purchases, photos, stocks by phone. Screen lock is a crucial technology that protects sensitive information and prevents unauthorised use of Smartphones. After a period of inactivity, Android phones and Apple iPhones will lock themselves. Users' privacy can be protected using this form. Password, sample, and biometric authentication are the tools that can be used. Due to a lack of security, these approaches are not well supported. The iPhone normally uses a 4-digit password that can be broken by a powerful attack. Android systems use a geometric pattern of nine points. Encryption and encryption [1], we provide security for personal messages because if there is unauthorized access to your mobile devices. No one can get entry to encrypted messages without using a strong user-generated key. This application provides security using the Advanced Encryption Standard Algorithm which is the most secure and widely used algorithm for many applications and web pages to provide security [2]. In this application there is no button length.

A. *Motivation*

Smartphones store a lot of sensitive information. To protect data from tapping a new authentication method is required. The previous GSM SMS gadget is much less secure in transmitting messages without using the Internet. By using this application, we can send messages in a secure way, the message can be encrypted using this application and you can send the encrypted message via the GSM SMS system.

B. *Current Behavioral Characteristics*

Behavioural-based programs such as gait recognition, keystroke capabilities and phone usage statistics require a lot of time to determine user eligibility and have low accuracy. Many of the most current strip-based schemes on touch screens can achieve very high accuracy but require two-handed operation that limits the operating conditions. Open Sesame and Wave are two packages most closely related to our work. Open Sesame allows users to move or fold their phones without special requirements and acquires four types of geometric features with green axis acceleration for three. Solid electricity functions (PDFs) of these feature samples are used to train classifiers and validate the user. UWave can verify user competency by evaluating series of three-axis acceleration readings of a test action drawn from the pre-defined template library using dynamic time warping (DTW).

II. REVIEW OF LITERATURE

Jaya Bhattacharjee and Ankit Fadia [1] demonstrate how they can encrypt information in a way that keeps it safe from prying eyes. It explains how encryption works and the increasing need to protect one's privacy in communications and transactions by defining the terms encryption and encryption. William Stallings [2] describes a special section in his book: Part One: Provides a cross-sectional study, consisting of previous and present techniques. Emphasis on Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two very important algorithms (AES). Mark Stamp [3] describes statistics safety in four main categories: i) Encryption: Including classical cryptosystems, Public key cryptography, Symmetric key cryptography, random numbers, hash functions and encryption are some of the terms used to describe cryptography. Also, cryptanalytic techniques, which include cypher machine attacks as examples') Accessibility Control: Identifies and authenticates users, as well as password-based protection.

iii) Agreements: Focuses on standard authentication protocols and real-world security agreements, that are IPsec, SSL, GSM and Kerberos; Urs. E. Gattiker [4] provides comprehensive and easy-to-understand examples the general principles of infrastructure security and protection. Specific guidelines are supplied especially for students who have learned to understand cryptography journals or books, pc security, facts systems, on-site access control, as well as the related applied areas. The dictionary is also suitable for computer science, engineering, and science students in college. Our business protection directors, STEVEN FURNELL and PAUL DOWLAND [5], use email clients to enhance security, maintain confidentiality, and preserve our reputation of the company. The Fund Guide is a quick reference guide to the most important security issues that concern those who send and use email to help their businesses. e-mail for its significance in the context of the business, and focuses on why effective and safe policy is important in ensuring the smooth running of a business. David Harley et. al. [6] A information to protect our system from cyber threats. It presents the nutmeg soup, a whole physical analysis of system virus protection by providing: i) Current information on the growing computer viral domain; ii) Real-world research on viral infections, solutions) Problem analysis and application of modern viral threat solutions. Bradley Dunsmore et. al. [7] explores choices to protect a computer network from Internet attacks, Cisco, Symantec, Microsoft, and Check Point firewall solutions are highlighted. It describes what to do to set up a full security system in general terms. It ends with information on the suspension specifications for a variety of items. Fauzan Mirza [8] provides a primary introduction to preventing the formation and analysis of the cipher. It describes the diagram principles and standards of block ciphers, Particularly the Feistel cyphers, a type of block cypher. Some modern block cypher cryptanalysis methods are demonstrated using Simplified TEA (STEA), a delicate Feistel cypher based entirely on the Tiny Encryption Algorithm (TEA). Paul C. Kocher [9] describes how the attackers can find Diffe-Hellman's opponents, the RSA keys, and destroy different dimension systems by carefully measuring the time required to carry out confidential activities. I additionally outlined strategies to forestall attacks by RSA and Diffe-Hellman. Finally set the requirement that other cryptosystems be updated to prevent attacks, as nicely as new agreements and algorithms that include measures to prevent time attacks.

III. System Architecture

Cryptography is often regarded as a secret study. While encryption is the process of converting encrypted text into unreadable form, encryption is the manner of changing encrypted text to plain text [Figure 1]. The basic steps involved in a typical encryption model are:

- text messaging
- Convert the first message to a cipher text using a key and a specific algorithm
- The transmission of the cipher textual content in some way
- The cipher text at the end of the receiver is returned to the original message using the same algorithm as the key. In cryptography there are 5 primary objectives that should be held in mind in order to guarantee system confidentiality.
- **Verification:** Before sending or receiving data, verifying the sender's and receiver's identities.
- **Privacy:** The message can only be read by approved users.
- **Integrity:** The received message should not be altered in any way.
- **Non-disclosure:** It is a way of proving that the sender has actually sent a message that is not a sender or recipient who can falsely deny sending or sending a particular message.
- **Service Reliability and Availability**: Intruders do not impact the availability of the system or the type of service provided to the customer.

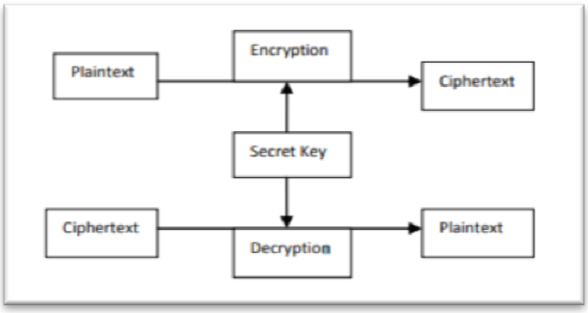


Fig 1: System Architecture

A. Real Implantation for SMS Encryption–Based on Android App.

They have used 3 cryptographic algorithms namely AES, DES, 3-DES. If you compare yourself on the basis of time delay. Therefore, it helps developers to pick the most effective and efficient cryptographic algorithm that will be used to deliver secure messages. SMS coding software operates via SMS mostly on Android operating system, with SMS being encrypted at the sender's end, electronically signed in the second stage, and sent in the final step .A coding of time delays is defined as a measurement of time determined by the transition from clear text to cypher text. Different SMS message sizes determined using the same algorithm's key length. SMS messages can be vulnerable to malicious attacks from unauthorised access, so users should be aware of this.

IV. Performance Analysis of cryptographic algorithms with symmetric key

Cryptography is highly divided between two broad categories according to the type of security keys used in Symmetric and Asymmetric encryption. While Symmetric encryption also regarded as secret key use one encryption key and Asymmetric encryption also known as public key encryption uses two different keys for encryption and decryption. When performing encrypted encryption both the sender and the recipient must agree on the same encryption key, in unencrypted encryption there are two buttons: one public key that is public and used for encryption and another private key that the user knows and used to decrypt. It also discusses various encryption methods such as:

- **Advanced Encryption Standard**

Implementation on Android for Message Encryption.

There are various encryption algorithms available these days to perform encryption during private data transfer over a network. Privacy is accomplished by using encrypting messages. The latest business quality trends have created the need for mobile device security. The SMS enterprise that has grown so well is in danger of being attacked. Therefore, it is now very important to encrypt the SMS before it is sent. Encryption has been used via the navy for a long time and the government facilitates confidential communication.qEncryption.it is frequently used to defend facts between several styles of social programs. One learn about found that seventy-one audited firms used secret encryption for some of their information on the go and 53% for secret use in their other last data. AES requires very little RAM house and is very fast. For trained Pentium processors AES encryption requires only clock / byte cycles compatible with 11Mib / s output of 200 MHz processor. Their software gives a variety of functions such as chat view, inbox, drafts, backup, restore. The UI is made lightweight and with great importance given the functionality of the encryption and decryption process.

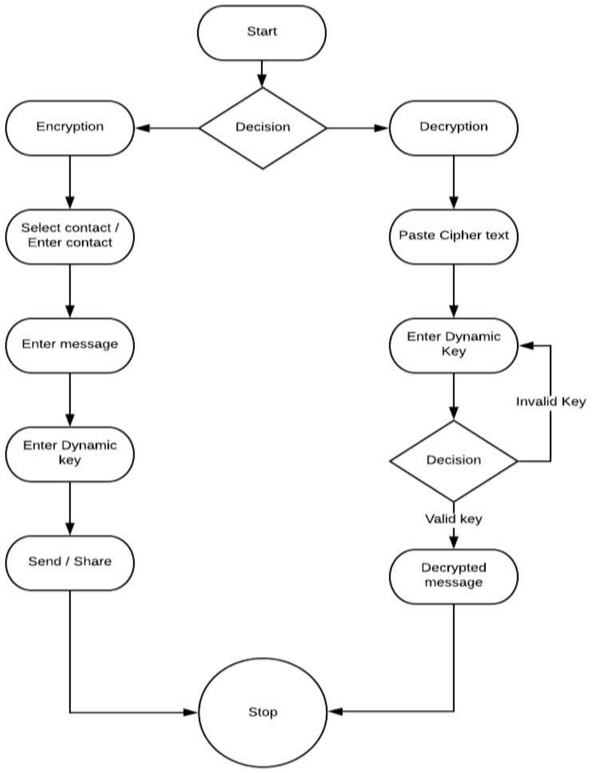


Fig 2: Activity Diagram for Overall Project

The complete transfer process is described in detail in Fig 2. The separate facilities receiving the BTS transfer were used to make the user's equipment and the network communicate offline. The MSC is in charge of routing voice, fax, and other service calls. MSC stands for "SMS Support Center." e that serves as an instant messaging service. It additionally notifies the sender whether the message has been delivered or not. They used AES (advanced encryption algorithm) for encryption and decryption. The AES has a most block size of 128bits and a key size of 128, 192, or 256-bit bits uses a number of encryption ideas that convert plain text into cipher text. The output of the complete round will be the input to the next round. The final world effect is the cipher text. The steps used in the algorithm are SubBytes,ShiftRows, Mix Columns, AddRoundKey. The Cipher key used is 128 bits. Any attacker test 2128 probabilities of breaking the cipher key. There are no patterns set in the algorithm. As a result, velocity and density requirements are met. The app size is bytes of 50 pounds and can be installed on a mobile phone running on an Android platform. The consumer does no longer experience any delays while using the system, This is a strong sign that the necessary speed has been met. The user interface is basic and easy to use.. For apps, where access control is important, our app can be used to verify the sender of the message aw. Also, it is possible to see, if the message was corrupted or changed during the transfer. Messages with sensitive information are stored securely and remain anonymous even if the device is detected by the enemy. A very one of a kind point to think about is the security of the data implicit in various attacks namely Brute Force attack, pattern assault etc..

A. SOFTWARE TESTING TECHNIQUES

Software testing is a complicated technique that incorporates multiple functions, software enhancement The final analysis of the specification, design, and coding is represented by these elements. Technology research shows a plethora of intriguing software developer variants.

- **Test Objectives**

Examining a set of steps that include running a programme with different inputs with the aim of identifying inputs and forcing the developer to correct mistakes. A thorough software programme analysis case is something that has a chance of uncovering a flaw that isn't present in the intended programme. Successful software testing reveals an error that is hidden or undetectable.. The following goals necessitate a significant shift in the viewing port. Testing process is a step by step process that cannot demonstrate the absence of errors or errors in the software or programme, but can only show the different errors contained in it.

- **White Box test**

The Open or Glass Box test is another name for the White Box test. A White Box test may be conducted by locating a particular programme or function that a software product or software programme is built or created to perform or performed to show each system or function fully simultaneously detecting errors in every system. A glass field or open check case machine that uses extensive control in the process design and design to detect and run check cases. Tasks for trying out how to start a white field test.

- **Black Box Testing**

A Black Box check may be performed during a Black Box test to ensure that all gears and internal components of the product, machine, or system are checked. Internal functionality is provided to track the performance including specificity among all frequently used internal processes. The Black Box check focuses on overall performance requirements and software requirements.

The procedures to be followed in developing a black box test case are:

- Graphical assessment techniques
- Equality distribution
- Boundary number analysis
- Comparing tests
- Graphic graph

B. *SOFTWARE TESTING APPROACH*

Software test cases are incorporated into a sequence of well-planned steps and systematic processes that contribute to effective software creation, construction, and execution by the Software Testing System. Authentication and validation can be done using a number of software testing methods. Software validation refers to a set of duties in tasks and programs designed to ensure that the software or product is performing the specific task or outcome required. Software Verification is a collection of functions that ensures that the software, product, or application is configured to meet the needs of the user, allowing them to enter valid data and freeing up space in the Data store.

- **Unit Testing**

Unit testing is a form of software testing that focuses on the verification of the smallest unit of a programme or software creation, also known as a module. Unit testing focuses on control methods to search for errors made in software built within the module parameters, using the design or operation of the device as a reference. A series of steps may be conducted in combination with or similarity of several modules or functions in software unit testing, which is typically a white box or open test.

- **Integration of testing**

Integration testing is a systematic test with a software framework that integrates that creates system structure and allows flow of data among functions, although it also includes the identification of errors associated with different combinations. The key goal is to apply the methods evaluated by the unit and the activities to build the system structure proposed by the project.

- **Top-Down Integration**

The next step to test the top-down integration is the sequence of design and the testing evaluation of system structure. Various modules are incorporated in software, a product, or an application by navigating across a structured control system among modules, beginning with the main control, domestic control system, or reference system. Various master plan-related activities or modules will be included in the project design, the first breath, or the first approach.

- **Verification testing**

Testing to ensure that fully integrated software as a kit passes the integration test verification testing will be the next step in the testing process, and it is characterised as an effective testing process for software tasks that meets the customer's expectations.

- **System testing**

To evaluate computer-related program activities we consider system tests that are actually a sequence of various tests which its main goal is to test the performance of a computer-based program. Although every test has a different motive for testing product validation and integration, all function is to ensure that all system components and system functions are properly integrated to perform shared functions.

- **Security Inspection**

Efforts to ensure security and safety measures are built into the data protection system, system and other system-related integrations.

- **Performance testing**

In software engineering, performance appraisal is considered for load testing, program usage, Efficiency in memory, encoding, networking, and other areas of the system. It could also be used to investigate and test a program's structure and processes within a system, as well as checking or validating other system quality features like robustness, reliability, and resource utilisation.

TABLE I: Test case results

Test S.No.	Input	Expected Behavior	Observed behavior	Status P = Passed F = Failed
1	Select Encrypt option on the home screen	Encryption page should be displayed to the user	Encryption page is displayed	P
2	Select Decrypt option on the home screen	Decryption page should be displayed to the user	Decryption page is displayed	P
3	Select on share option	Availability of other applications should be displayed	Applications are displayed which are able to share	P
4	Inbox	Click on message to copy the message into clipboard	Message copied	P

5	Sent	Click on sent message to add into favorites	Message added to favorites	P

V. RESULT

Below attached these are the screen shots of User Interface(UI). Which shows how the UI inside the application look and what are the buttons, functions, Photos used in the UI to make the app look modern. This Fig 3 below is the start-up page of the app where when we open the app n the mobile. The starting page we will see is the page attached below.

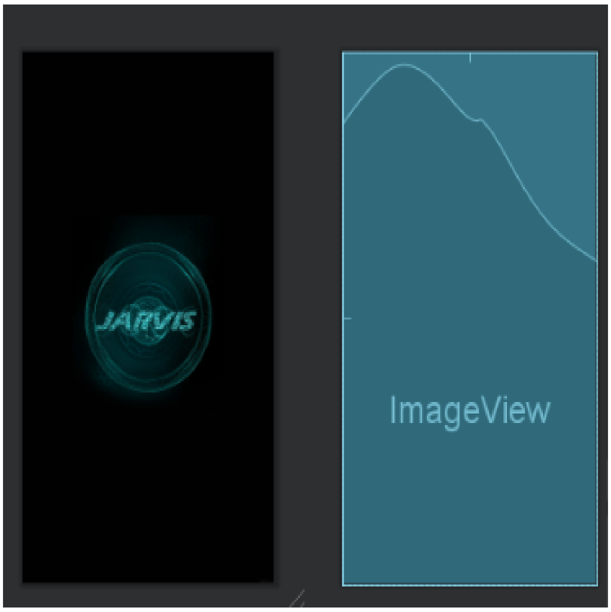


Fig 3. Startup page of Application

The Fig 4 below shows the main page of the application. In this Page user can Encrypt and Decrypt the data. Where sender can encrypt the data, while receiver can decrypt the data by clicking the Encrypt and Decrypt buttons. This page is the main page of the project.

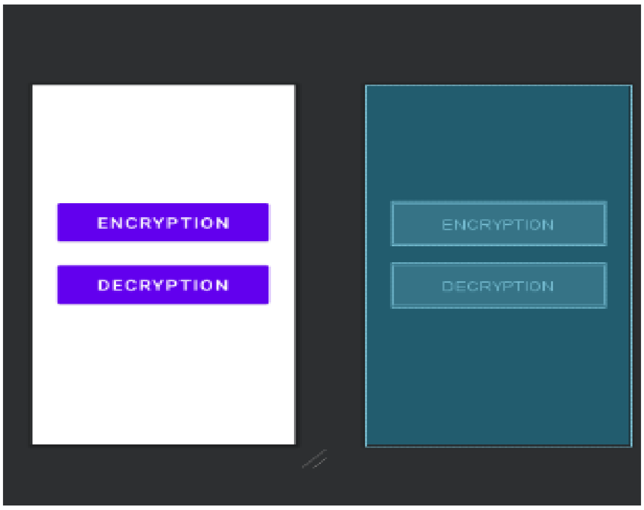


Fig 4: Home Page of Application

In this following Fig 5 when the user click on the Encrypt button the user will be redirected to the following page where user need to select the number from contacts(To whom The sender wants to send the message to) And then there after the sender need's to enter the message that he wish to send to the receiver along with the Private key which will solely know to the sender only. After filling the all details the sender needs to click on send button, after that the application will send an encrypted SMS to the receiver's mobile

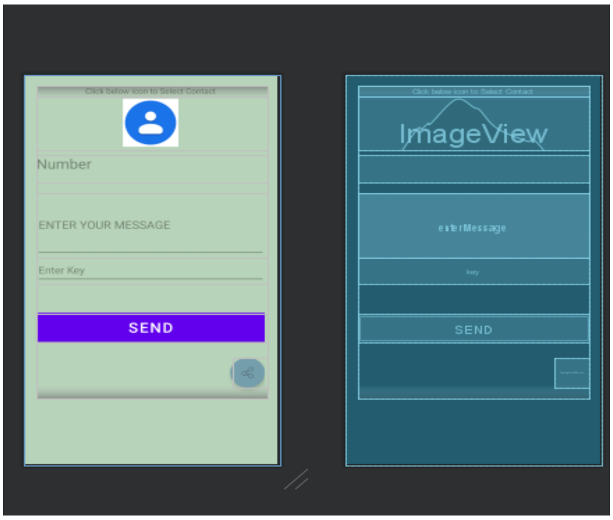

Click below icon to Select Contact
Number
ENTER YOUR MESSAGE
Enter Key
SEND
Click below icon to Select Contact
ImageView
enterMessage
key
SEND

Fig 5: Encryption Page of Application

In this below Fig 6 we are seeing the page of decryption. When the user click on decryption button he will be redirected to the following page where the receiver needs to enter the Encrypted message(Cipher Text) received from the sender in the 1 text field, and then after he needs to enter the private key which is only known to the sender of the message. After entering the private key when the user clicks on Decrypt button, The application decrypt's the message and shows the message in the message field.

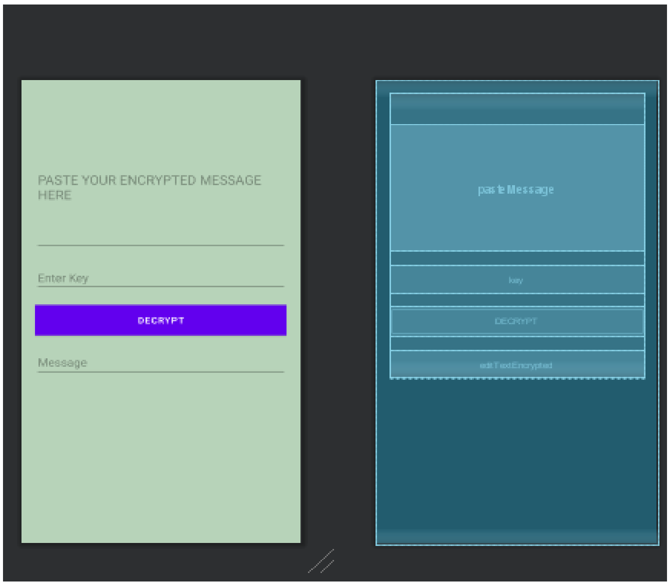
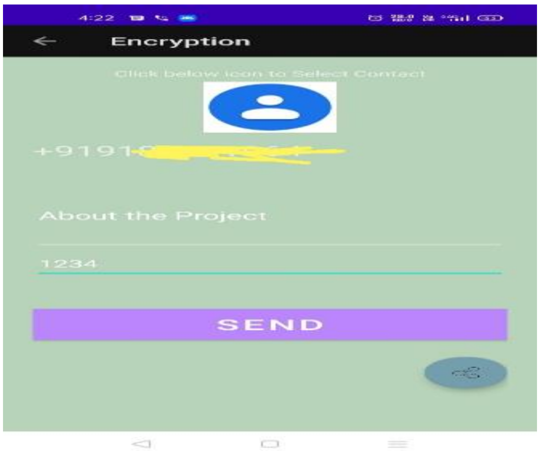


Fig 6: Decryption Page of Application

- *On Senders Mobile:*

In the below Fig 7 is the practical implementation of the Encryption from sender's mobile. The sender first selected a mobile number from the contacts, And then he wrote a message(About the project) that he wants to send to the receiver, and then in the next field he used a private password(1234) which is only known to the sender to protect the text he entered. Then after the sender hits the send button in the application.



+9191[redacted]

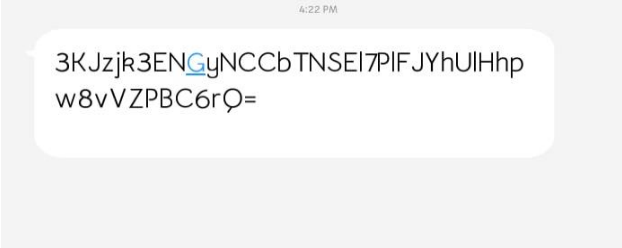
About the Project

1234

Fig 7: Process of Encryption

- *On Receivers Mobile*

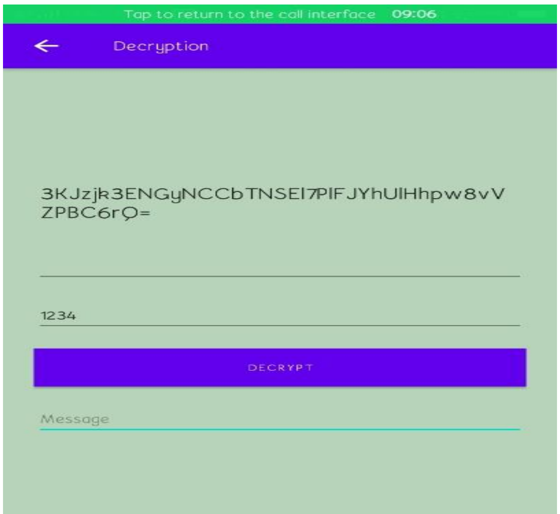
The Fig 8 we see below is the encrypted version of the message sent by the sender. This SMS is received by the receiver mobile using the senders network carrier.



3KJzjk3ENGyNCCbTNSEI7PIFJYhUIHhp
w8vVZPBC6rQ=

Fig 8: Output of Encrypted Message

In this following Fig 9 shows the Practical implementation of the Decryption Process, where receiver needs to copy the text he received from the sender and paste it in the Message field, And then he needs to enter the private key which is only known to sender of the message to decrypt the message. After entering the key and cipher test the user(receiver) need's to hit the Decrypt button to Decrypt the cipher text.

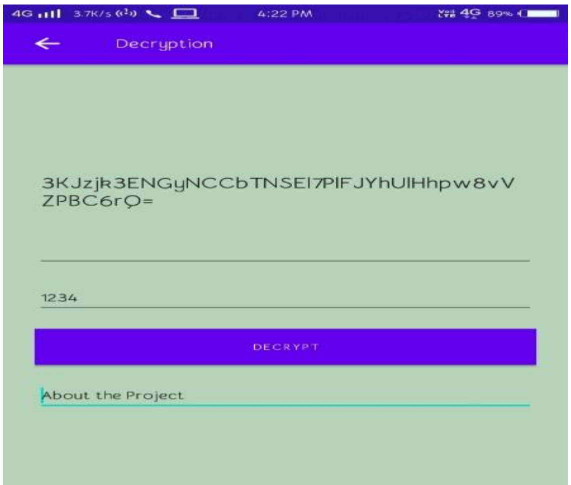


3KJzjk3ENGyNCCbTNSEI7PIFJYhUIHhpw8vV
ZPBC6rQ=

1234

Fig 9: Decryption Process

The Fig 10 we see below is the output of the encrypted message. After entering the correct details by the user when he hits the decrypt button the application will process the details in the background and show the output in message section. Which is the plain text from(Human Readable form).



3KJzjk3ENGyNCCbTNSEI7PIFJYhUIHhpw8vV
ZPBC6rQ=

1234

About the Project

Fig 10: Output of Decrypted Message

VI. CONCLUSION

In this project, we have proposed a secure messaging system, in case a message is stolen by a third party without the user's knowledge, the message will not be able to be understood by a third party because the message will be transmitted via GSM SMS in text format. Without entering the correct key provided by the third party the cypher text will not be able to be converted to plain text by the user. The user should remember the key to convert cipher text into plain text, without a key it is impossible to convert. The feature when sending a text message using the GSM SMS system is the message will be converted into a cipher text and go through the network and when the recipient receives the message the message will be converted to clear text. This enables the user to easily send the message through secure sending.

REFERENCES

[1] Ankid Fadia, Jaya Bhattacharjee, "Encryption, Protecting Your Data", Vikash Publishing House Pvt Ltd,2007, ISBN: 812592251-2

[2] William Stallings, "Cryptography and Network Security", Fifth Edition, Person,2011, ISBN 978-81-317-6166-3

[3] Mark Stamp, "INFORMATION SECURITY Principles and Practice", Second Edition, A JOHN WILEY & SONS INC. PUBLICATION,2011,

[4] Us E. Gattiker, International School of New Media, "THE INFORMATION SECURITY DICTIONARY", KLUWER ACADEMIC PUBLISHERS, ISBN: 1-4020-7889-7

[5] STEVEN FURNELL, PAUL DOWLAND, "E-mail Security A Pocket Guide", IT Governance Publishing, 2010, ISBN 978-1-84928-097-6

[6] David Harley, Robert Slade, Urs Gattiker, "Viruses Revealed", Osborne/McGraw-Hill

[7] Bradley Dunsmore, Jeffrey W. Brown, Michael Cross, "MISSION CRITICAL! INTERNET SECURITY", Syngress Publishing Inc., 2001, ISBN: 1-928994-20-2

[8] Fauzan Mirza, "Block Ciphers and Cryptanalysis" PhD Thesis, Department of Mathematics, Royal Holloway University of London, 2001

[9] Paul C. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems", Cryptography Research Inc., San Francisco, USA.