International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2020.33797

Volume 6, Issue 4
April - 2020

Secure SMS System using RSA Encryption Based on Android platform

Zarni Sann[1], Thi Thi Soe[2] and Moe Moe San[3]

Professor[12] and Assistant Lecture[3]

[13]Faculty of Computer Systems and Technologies

[2]Faculty of Computer Science

University of Computer Studies (Mandalay)

Mandalay, Mandalay Division

Myanmar

ABSTRACT

To send text messages free of charge using an existing mobile number, you can use this system like SMS messenger and install it on your mobile device. This apk is an application that enables you to text and sends small images to other this apk's users without charge. To send a secure message, secure sessions must exist between the sending device and all the recipient's devices. Asymmetric key cryptography algorithm RSA is used for encryption and decryption of the message. The user can obtain the security of text messages using RSA. This system provides a secure message on the mobile phone. Every SMS packet contains 140 bytes of effective data. Mobile users send short messages to the short message center through mobile terminals, and then the short message center transmits these short messages to target users.

Key Words: *Instance Message, Asymmetric Key Cryptography, RSA algorithm, Android Platform*.

1. INTRODUCTION

Users install instant messaging clients on their client machines: desktop computers, wireless devices, PDAs, and any mobile devices [1]. User communicates with an IM server in the messaging provider's infrastructure to locate other users and exchange messages. Firstly, user installs this mobile application (message apk) If user wants to send message to their friends, user must be known phone number or name of their friends. Cryptography provides security services that enhance the security of data processing systems and transfers of information. This system can support message sending with security by using RSA encryption and secret message communication. Message encrypt before transmission to ensure that the message is secure during transmit. Receiver receive encrypted message to get plain text by decrypting [2].

The user can obtain strong security of text message using RSA. Though Instant Messaging is an effective and easy means of network-based communication, it introduces a number of security risks if proper security measures are not applied. Users install instant messaging clients on their client machines: desktop computers, wireless devices, or PDAs. These clients communicate with an IM server in the messaging provider's infrastructure to locate other users and exchange messages [5, 9]. Cryptography provides security services that enhance the security of data processing systems and transfers of information. Message is encrypted before transmission to ensure that the message is secure during transmission. The SMS is a connectionless-oriented mobile data transmission model based on the store-forwarding technology. The Objectives and motivation of the system are: to provide an introduction to basic Short Message Service (SMS) concepts, to get cheap and easy communication for business purposes, to demonstrate small chat room mobile network, to provide integrity by protecting the transmitted message to be invisible and to provide privacy, confidentiality and security of messaging system by RSA. The motivations of the system are as follows: this system provides a secure and secret communication between different people. Mobile encryption application is one way to protect text messages from being read by friends or other peoples [4]. Today, most people are using SMS and this system makes SMS more secure.

2. SHORT MESSAGE SERVICE (SMS)

The Short Messaging Service, or SMS, is a bi-directional service to send text over wireless communication systems. SMS also guarantees delivery of the short message by the network. SMS is characterized by out-of-band packet delivery and low-bandwidth message transfer, which results in a highly efficient means for transmitting short bursts of data. SMS provides a convenient means for people to communicate with each other using text messages via mobile devices or Internet-connected computers. When confidential information is exchanged using SMS, it is very difficult to protect the information from SMS security as well as ensure that the message is sent by authorized senders. SMS security guarantees provision of confidentiality, authentication, and integrity service. Asymmetric key cryptography algorithm RSA is used for encryption and decryption of the data. The necessity of providing security to SMS has been imperative since a long time and many algorithms and techniques have been implemented in various platforms to try and provide security to the messages [5, 9].

2.1 Android Applications

Android has a large community of developers writing applications that extend the functionality of devices, written primarily in a customized version of the Java programming language. Android applications are authored as Java source code and then compiled to Dalvik byte code. This byte code is packaged with additional resources, such as images and configuration files into an application package (apk) file. When the user installs an application from Google Play, the apk is downloaded and installed on the user's system [10]. The Android platform is provided through open source licensing. Developers have unprecedented access to the handset features when developing applications. Android applications are free to develop. There are no licensing or royalty fees to develop on the platform. No required membership fees. No required testing fees. No required signing or certification fees. Android applications can be distributed and commercialized in a variety of ways [1, 10].

Mobile data collection (MDC) refers to the utilization of existing information technology products such as phones, smartphones, and tablets (hardware), and a number of different possible programs (software), for data gathering. Instead of recording information on printed paper using a pen, which is then manually entered into a database for analysis, data is input into a device which is then capable of exporting directly into a centralized database (which can be done using the Internet or a local computer) [6].

3. CRYPTOGRAPHY

Cryptography is a tool that provides privacy and security. It is a technique for secrecy of communication. All business, government and academic organizations interconnect their private data by using cryptographic algorithm to support the security services. Two type of techniques are Asymmetric key and Symmetric key cryptography. This system is applied Asymmetric key Cryptography or Public key Cryptography. Asymmetric key cryptography or public key cryptography uses two different keys: public key and private key. The private key is kept secret and the pubic key is distributed. Anyone can encrypt the message with the public key but only the one who knows the corresponding private key can decrypt it. An original message is plaintext. The encrypted message is known as cipher text. The process of converting from plaintext to cipher text is called encryption. The process of turning ciphertext back into plaintext is called decryption [2, 7].

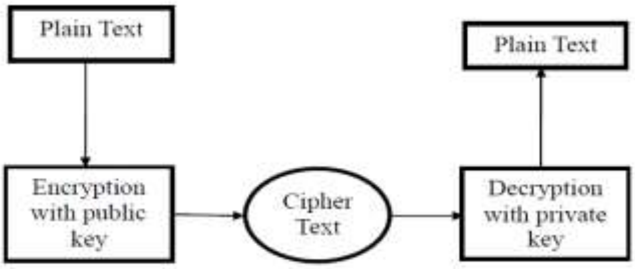


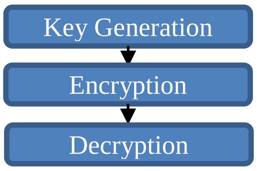
Figure1. Processes of Asymmetric Key Cryptography

3.1 Description of RSA Algorithm

RSA is made of the initial letters of the surnames of Ron Rivest, Adi Sharmir, and Leonard Adleman. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. Public key algorithm was invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adelman (RSA). It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments. Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modules in modular exponentiation is a technique to speed up the RSA decryption. By securing the data, we are not allowing

DOI: 10.31695/IJASRE.2020.33797

unauthorized access to it. RSA algorithm uses two different numbers but mathematically linked keys, one public and one private. Both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. Functioning of RSA is based on multiplication of two large prime numbers [3, 8]. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key. The two numbers that are used for multiplication-one of them is public other is private. RSA algorithm involves three steps:



3.1.1 Key Generation

A RSA public and private key pair can be generated by using the algorithm below:

1. Choose two random prime numbers *p* and *q* such that the bit length of *p* is approximately equal to the bit length of *q*.

   Compute N such that $N = p * q$ .... (1)
2. Compute *f (n)* such that $\varphi (n) = (p - 1)*(q - 1)$ ………… *(2)*
3. Choose a random integer e such that $e < \varphi (n)$ and $gcd (e, \varphi (n)) = 1$, then compute the integer d such that:

   $e*d = 1 \bmod \Phi(N)$ .... (3)
4. *(n, e)* is the public key, and *d* is the private key.

3.1.2 RSA Encryption

RSA is widely used in encrypted connection, digital certificates core algorithms. The security of RSA comes from integer to find. Generation of random prime numbers gives the algorithm extra strength and efficiency. In our system, we are applied RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

i. Consider the user A that needs to send A message to B in secured manner using RSA algorithm. (Public Key (*e*, *n*))
ii. *e* is B's public key. Since e is public, A is allowed access to *e*.
iii. For encryption the message *m* of A which is in the range $1<m<n$ is converted to cipher. $C = m^e \pmod n$ …… (4)
iv. Where the cipher text

3.1.3 RSA Decryption

The receiver B can recover *m* from *c* by using A' private key exponent *d* by the following computation: [3, 6]

$m = c^d \bmod n$ ………… (5)

Given *m*, the receiver A can recover the original message *m* by reversing the padding scheme.

1) The cipher text *c* is sent to B and A.

2) User B calculate the message with its private key (*d*, *n*), $m = c^d \pmod n$ .... (6)

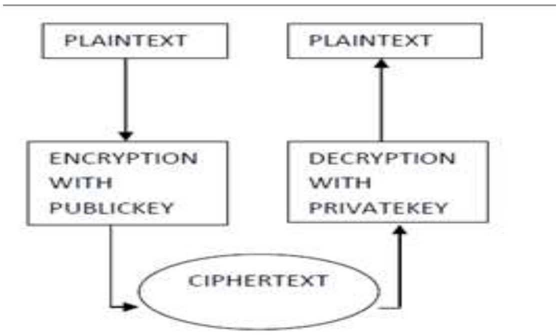


Figure2. RSA Process

4. SYSTEM DESIGN AND PROCESSING STATE

This system will implement four parts:

1. Installing apk to android to use message exchange
2. Implementing normal message communication session
3. Implementing secret message communication session and

DOI: 10.31695/IJASRE.2020.33797

4. Implementing secure message communication using RSA encryption.

In this system, the message is encrypted with RSA algorithm. The sender sends an encrypted message to the receiver on android platform. The message is encrypted by using the public key from key generation. The message or plaintext is encrypted to be a ciphertext or an encrypted message as shown in Figure 3. The receiver gets the encrypted message and decrypts it by using private key from key generation. The encrypted message or ciphertext is decrypted by the receiver to get the original message or plaintext.

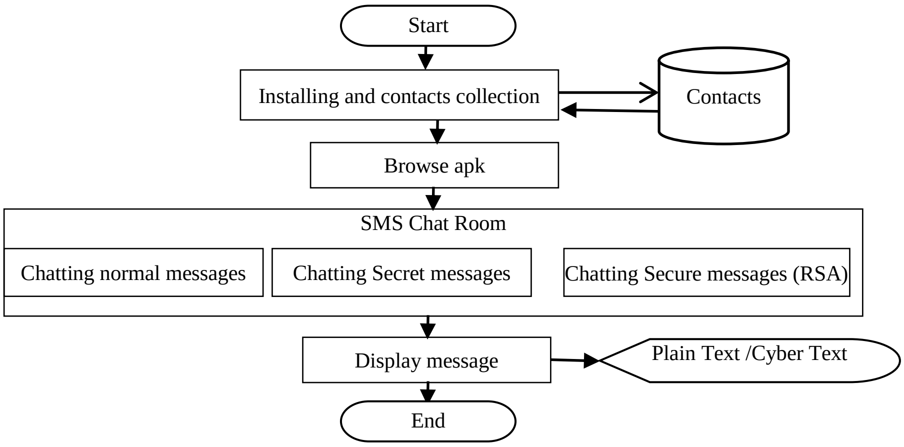
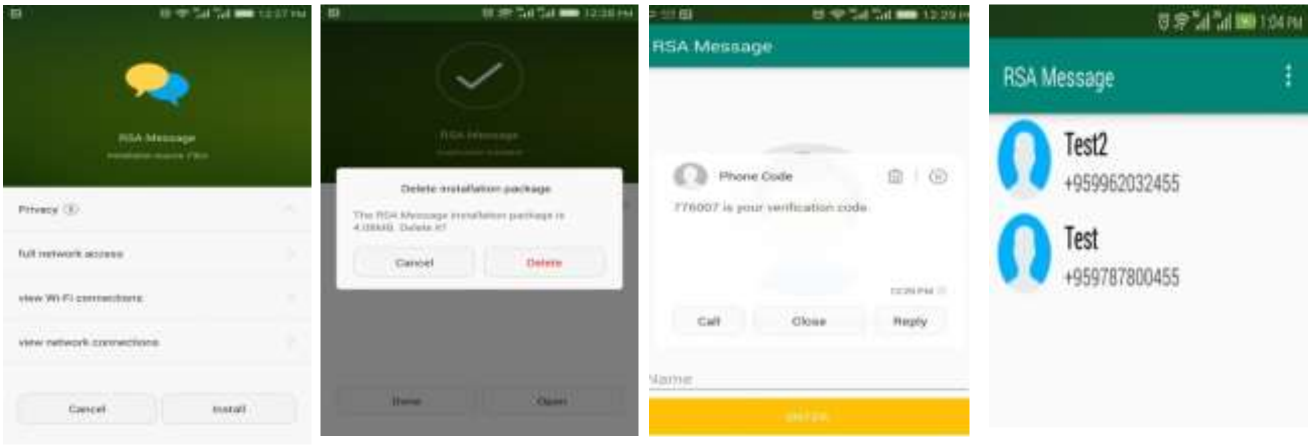


Figure3. Overview of Process Flow

5. IMPLEMENTATION FOR MESSAGE SECURITY

This system is implemented for security of messages on android using RSA algorithms. It is developed by using Java Programming Language. First, the system runs on computer using a java devolvement tool (Eclipse). After running on computer, the RSA_Key_SMS.apk is released. When user is using this apk, this application is opened by both sides. Step-by-step installing processes are shown below:

1. Download the RSA message application icon.
2. Tap on Install. The welcome screen opens.
3. Delete or cancel Installation Package and Tap Open.
4. Tap a phone number with a country code to receive verification code. *Phone Number Verification* dialog box opens. Apk sends you a text message with your verification code.
5. Tap Enter. And Type Name and after installing and opening the application, the splash screen will appear as shown in Figure 4.



The RSA Message installation package is 4.08MB. Delete it?

776007 is your verification code.

Test2
+959962032455

Test
+959787800455

Figure4. RSA Message's apk Installation process

DOI: 10.31695/IJASRE.2020.33797

Normal message communication process for sender and receiver side can be seen as shown in Figure 5.

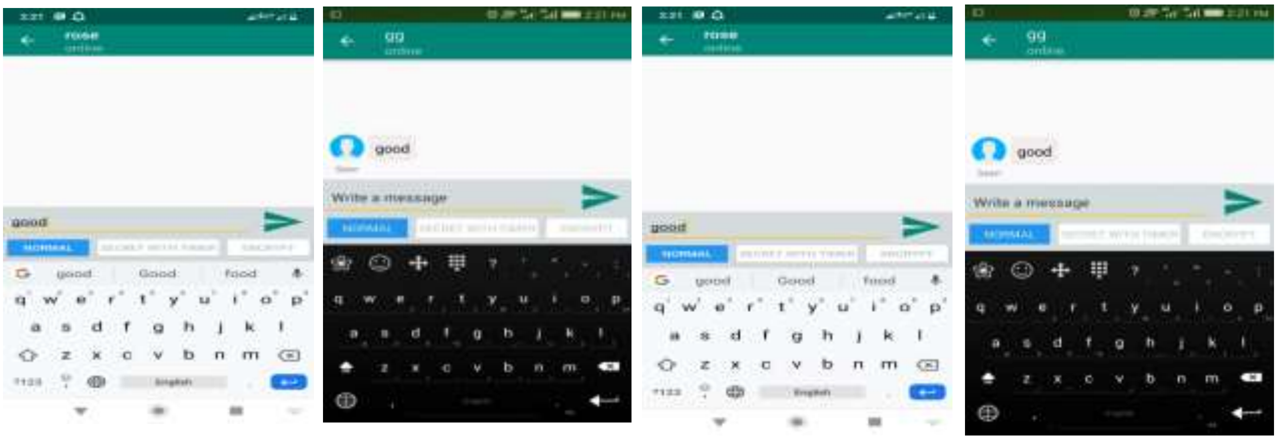


Figure5. Normal Message Communications Process in Sender and Receiver Side

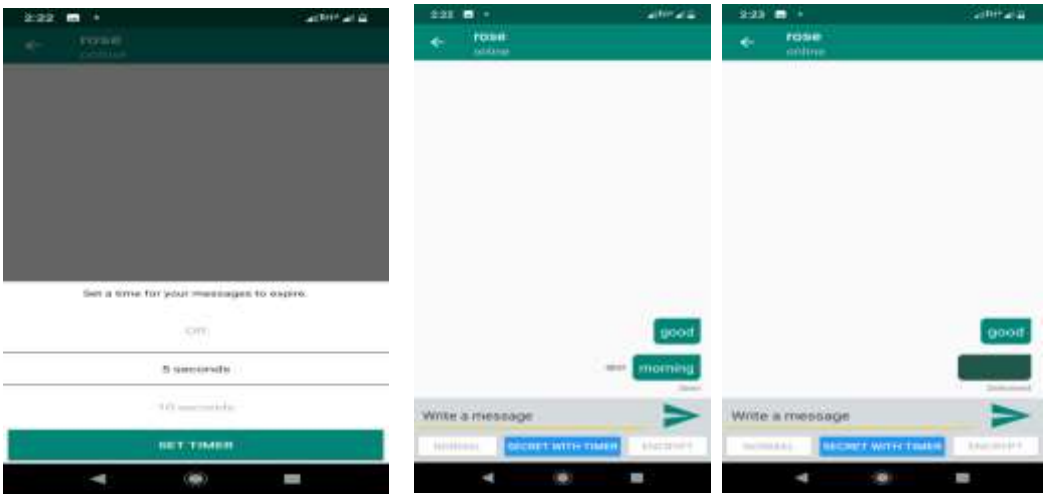
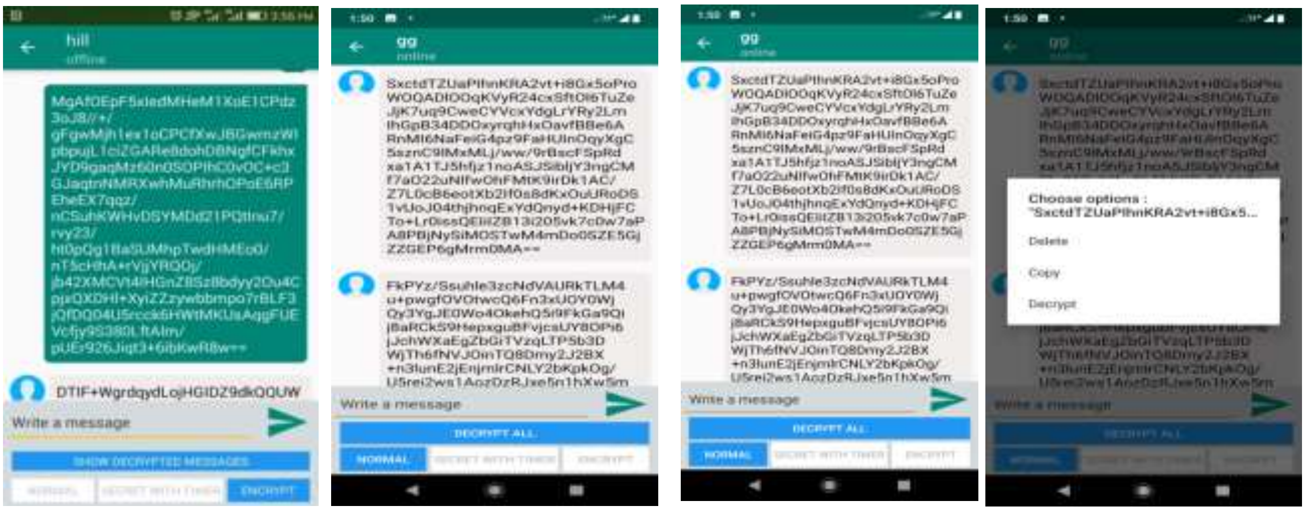


Figure6. Secret Message Receiving before Timeout and after Timeout

If user wants to communicate with secret message to their friend, firstly, user must be setting up Timer with specific time to display message and secret message communication process in sender and receiver side as shown in Figure 6.



MgAfOEpF5xledMHeM1XoE1CPdz
3oJ8//+/
gFgwMjh1ex1oCPCfXwJBGwmzWl
pbpujL1ciZGARe8dohDBNgfCFkhx
JYD9gaqMz60n0SOPlhC0vOC+c3
GJaqtnNMRXwhMuRhrhOPoE6RP
EheEX7qqz/
nCSuhKWHvDSYMDd21PQtlnu7/
rvy23/
ht0pQg1BaSUMhpTwdHMEo0/
nT5cHhA+rVjjYRQ0j/
jb42XMCVt4lHGnZ8Sz8bdyy2Ou4C
pjzQXDHI+XyiZZzywbbmpo7rBLF3
jQfDQ04U5rcck6HWtMKUsAggFUE
Vcfjy9S380LftAlm/
pUEr926Jiqt3+6ibKwR8w==

DTIF+WgrdqydLojHGIDZ9dkQQUW

SxctdTZUaPlhnKRA2vt+i8Gx5oPro
WOQADIOOqKVyR24cxSftOl6TuZe
JjK7uq9CweCYVcxYdgLrYRy2Lm
lhGpB34DDOxyrghHxOavfBBe6A
RnMl6NaFeiG4pz9FaHUlnOqyXgC
5aznC9lMxMLj/ww/9rBscFSpRd
xa1A1TJ5hfjz1noASJSibljY3ngCM
f7aO22uNlfwOhFMtK9irDk1AC/
Z7L0cB6eotXb2lf0s8dKxOuURoDS
1vUoJ04thjhnqExYdQnyd+KDHjFC
To+LrOissQEIIZB13l205vk7cDw7aP
A8PBjNySiMOSTwM4mDo0SZE5Gj
ZZGEP6gMrmDMA==

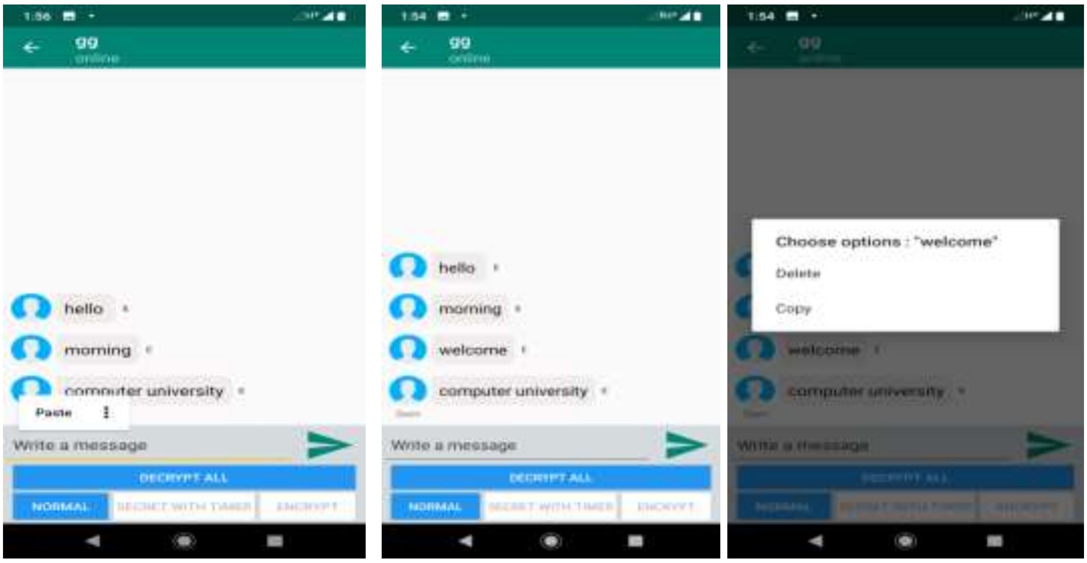
FkPYz/Ssuhle3zcNdVAURkTLM4
u+pwgfOVOtwcQ6Fn3xUOY0Wj
Qy3YgJE0Wo4OkehQ5l9FkGa9Qi
jBaRCk59HepxguBFvjcsUY8OPi6
jJchWXaEgZbGiTVzqLTP5b3D
WjTh6fNVJOinTQ8Dmy2J2BX
+n3lunE2jEnjmlrCNLY2bKpkOg/
U5rei2ws1AozDzRJxe5n1hXw5m

Choose options :
"SxctdTZUaPlhnKRA2vt+i8Gx5...
Delete
Copy
Decrypt

Figure7. Encrypted and decrypted Message Sending and Receiving Process

DOI: 10.31695/IJASRE.2020.33797

Message encrypted and decrypted process as shown in figure 7. In this application, user can use message copying the same message that wants to send and deleting when the message is not need. This process is shown in figure 8.



hello

morning

welcome

computer university

Choose options : "welcome"

Delete

Copy

Figure8. Message Copying and Deleting Process

6. CONCLUSION

Many SMS messages are alerts of one kind or another, used to notify the recipient of an event. This defines the upper bound of an SMS message to be 160 characters using 7-bit encoding. The system can use Myanmar and English language at the sending of the message. This application can easily be used for the purpose of communication with a high security. To deliver and store the message securely and authenticity is one of the major aims of phone number and communication security research. The security for SMS is a must for preventing message from different attacks. This system can use mobile-based secure message communication. Mobile security is one of the key issues in the SMS industry applications. It is necessary to avoid message to be interrupted by third person other than sender and receiver. Hence, using cryptographic algorithm, RSA provides SMS security solution in mobile security system. It provides security services such as confidentiality, authentication, integrity and non-repudiation. RSA encryption is faster than RSA decryption. Using android technology is following current market trend. This system can be used by high level organizations, business organization and military people for sharing their confidential data.

This study could be extended by comparing other Public Key Cryptography systems such as ElGamal, Pretty Good Privacy (PGP), Elliptic-curve cryptography (ECC), etc. This defines the upper bound of an SMS message to be 160 characters using 7-bit encoding. SMSs are generated from mobile phones which generally have very low processing capacities and also low memory and battery capacity. RSA are conventional algorithms with large key sizes which require higher memory capacities and high processing powers.

REFERENCES

1. A. Singh, S. Maheshwari, S. Verma, and R. Dekar, Peer to Peer Secure Communication in Mobile Environment: A Novel Approach, International Journal of Computer Applications, vol. 52, 2012 24-29.
2. H. Mathkour, G. Assassa, A. Al-Muharib, and A. Jumaíh, A Secured Cryptographic Messaging System Proc. International Conference on Machine Learning and Computing (ICMLC), 2009.
3. Kriti Singhal, Secure Communication using RSA Algorithm for Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vol. 4, Issue 11, November 2016
4. Neidhardt, Eric. Asymmetric Cryptography for Mobile Devices.
5. PEERSMAN, Gert, et al. A tutorial overview of the short message service within GSM. Computing & Control Engineering Journal; 2000; 11.2: 79-89.
6. Satterlee E., Leela McCullough, Michael Dawson, and Kelly Cheung, PAPER -TO –MOBILE DATA COLLECTION, Layout and Design by FHI 360 Design Lab.

DOI: 10.31695/IJASRE.2020.33797

7. William S, Cryptography and Network Security Principles and Practice fifth edition. 2011.
8. http://en.wikipedia.org/wiki/RSA
9. http://en.wikipedia.org/wiki/Short_Message_Service
10. http://en.wikipedia.org/wiki/Android_%28operating_system%29

DOI: 10.31695/IJASRE.2020.33797