INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume 4, Issue 5)

Available online at: www.ijarnd.com

SMS security for Andriod platform by using RSA

Thandar Myint

Student, Technological University, Mandalay, Myanmar

ABSTRACT

The users of mobile based on Android were increasing every day. Mobile phone users send and receive a simple text message by using Short Message Service (SMS). When a user sends any confidential data through the message it is very difficult to protect it. SMS does not provide a secure medium. Information about every aspect of our lives needs to be kept secure from attackers and transfer safely over an insecure channel. Cryptography provides security services that enhance the security of data processing systems and transfers of information. Encryption, hiding or covering data provides data confidentiality. Asymmetric key cryptography algorithm RSA is used for encryption and decryption of the message. The user can obtain security of text message using RSA. In this system, the RSA algorithm is used for providing a secure medium on the mobile platform.

Keywords— *Android, Cryptography, RSA, SMS*

1. INTRODUCTION

Nowadays, SMS (Short Message Service) or messages are very common way of communication for mobile phone devices. Even the various instant messaging applications are available but SMS is stilled one of the popular ways of communication because it does not require an internet connection and of course sending an SMS is cheap, fast and simple. The majority of SMS are sending and receiving important data such social security numbers, bank account details, passwords, and so on and so forth. In some cases, this data may also include very private information reserved for the personal viewing of the legal recipient. So our aim is to provide SMS security that guarantees the provision of confidentiality, integrity, and authentication and non-repudiation service [9]. Data confidentiality and authentication are normally provided using cryptographic techniques.

Cryptography is a tool that provides privacy and security. It is a technique for the secrecy of communication. All business, government and academic organizations interconnect their private data by using a cryptographic algorithm to support the security services. Many different methods have been developed to encrypt and decrypt data in order to keep the data secret. Asymmetric key cryptography algorithm RSA is used for encryption and decryption of the message. The encrypted message is sent over the public network and is decrypted by the intended recipient. Message encrypt before transmission to ensure that the message is secure during transmit. The user can obtain strong security of text message using RSA. This system is a secure message on the mobile phone. One way to protect data is with a mobile encryption application to protect text messages from being read by friends or other people. Android is the most widely used on the mobile platform.

1.1 RSA Algorithm

RSA encryption algorithm, which is based on the idea of ensuring the secure transfer of data in the digital environment and the algorithmic difficulty of separating the integer factorization, is a type of public-key encryption method. Nowadays, it is also known as both the most commonly used encryption method and the method that allows digital signatures. It was created by Ron Rivest, Adi Shamir and Leonard Adleman [1] in 1978. Prime numbers are used for the key generation process in the RSA encryption method.

1.1.1 Algorithm Structure

Step 1: Choose two very large random prime integers: p and q.
Step 2: Compute n and $\Phi(n)$: $n = p \times q$ and $\Phi(n) = (p-1)(q-1)$
Step 3: Choose an integer e, $1 < e < \Phi(n)$ such that: gcd(e, Φ (n)) = 1 (where gcd means greatest common denominator)
Step 4: Compute d, $1 < d < \Phi(n)$such that: $ed \equiv 1 \pmod{\Phi(n)}$.

The public key is (n, e) and the private key is (n, d), the values of p, q and Φ (n) are private, e is the public or encryption exponent, d is the private or decryption exponent.

After creating public and private keys, information which must be sent is encrypted with the public key. Encryption and decryption processes are done as follows:

- The cypher text C is found by the equation $C = M^e \bmod n$ where M is the original message.
- The message M can be found from the cypher text C by the equation $M = C^d \bmod n$.
- A text encrypted with the public key can only be solved with the private key.

How the encryption and description process is done with the RSA algorithm is shown in figure 1.

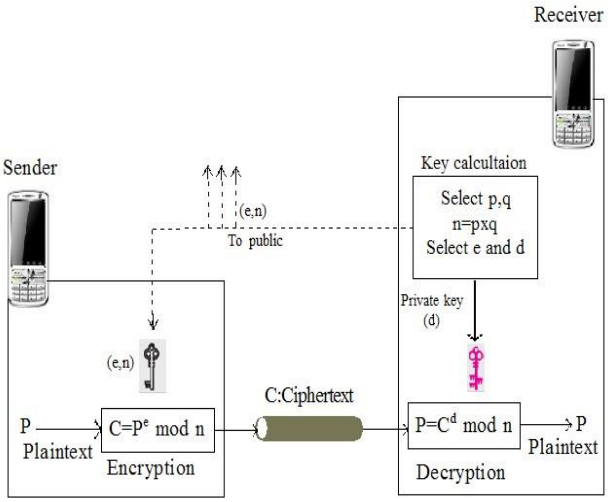

Fig. 1: Encryption, decryption and key generation in RSA

2. SHORT MESSAGE SERVICE (SMS)

Short Message Service (SMS) is a very popular and easy to use communications technology for mobile phone devices. Short Message Service (SMS) has become an extension of our lives and plays an important role in daily life. SMS is a popular medium for delivering Value Added Service and are suitable for mobile banking, payment reminders, stock and news alerts, railway and flight enquiries etc. [2]. Short Message Service (SMS) is the transmission of short text messages to and from a mobile phone, fax machine, and IP address. Messages must be no longer than 160 alphanumeric characters and contain no images or graphics. 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 the provision of confidentiality, authentication, and integrity service. Asymmetric key cryptography algorithm RSA used for encryption and decryption of the data.

2.1. Benefit of SMS

In today's competitive world, differentiation is a significant factor in the success of the service provider. Once the basic services, such as voice telephony, are deployed, SMS provides a powerful vehicle for service differentiation. If the market allows for it, SMS can also represent an additional source of revenue for the service provider. The benefits of SMS to subscriber's center on convenience, flexibility, and seamless integration of messaging services and data access [10]. From this perspective, the primary benefit is the ability to use the handset as an extension of the computer. SMS also eliminates the need for separate devices for messaging because services can be integrated into a single wireless device the mobile terminal. These benefits normally depend on the applications that the service provider offers.

At a minimum, SMS benefits include the following:

- Delivery of notifications and alerts
- Guaranteed message delivery
- Reliable, low-cost communication mechanism for concise information
- Ability to screen messages and return calls in a selective way
- Increased subscriber productivity

More sophisticated functionality provides the following enhanced subscriber benefits:

- Delivery of messages to multiple subscribers at a time.
- Ability to receive diverse information
- E-mail generation
- Creation of user groups
- Integration with other data and Internet-based applications

2.2. SMS Message Size

Short Message Service (SMS) has become a very popular way for mobile phone users to send and receive simple text messages to each other using mobile phones and portable devices. With SMS, users could send to or receive from a single person, or several persons, personal messages, email notifications, information services, job dispatches, stock alerts and so on. SMS is now more and more common among mobile phone users. Each message can contain at most 140 bytes (1120bits) [11] of data, the equivalent of up to 160 English characters, or 70 Chinese characters. A Short Message Service Centre (SMSC), usually owned and run by a telecommunication operator, is responsible for the routing and delivery of SMS. When an SMS message is delivered to the SMSC, a store-and-forward message mechanism is implemented, where the message is temporarily stored, then forwarded to the recipient's phone when the recipient device is available. Similar to email messages, an SMS message may pass through a number

of SMSC or other SMS gateways (which act as bridges between two or more SMSCs running different SMSC protocols2) before reaching the recipient's device. An SMSC helps route SMS messages and manage the process. If the intended SMS recipient is not online, the SMSC will keep the stored SMS message for a "validity period" before deleting it from storage. Short Message Service (SMS) has become a very popular way for mobile phone users to send and receive simple text messages to each other using mobile phones and portable devices.

3. ANDROID SYSTEM

Android becomes the world's most widely used smartphone platform and the software of choice for technology companies who require a low-cost, customizable, lightweight operating system for high techniques devices without developing one from scratch. As a result, despite being primarily designed for phones and tablets, it has seen additional applications on televisions, games consoles, digital cameras and other electronics. Android's open nature has further encouraged a large community of developers and enthusiasts to use the open source code as a foundation for community-driven projects, which add new features for advanced users or bring Android to devices which were officially released running other operating systems. [3]

Cryptography can also be used on android to keep the data secret. In addition to providing data isolation, supporting full-file system encryption, and providing secure communication channels, Android provides a wide array of algorithms for protecting data using cryptography [4]. In general, the user should try to use the highest level of pre-existing framework implementation that can support her use case. If a file is needed to be securely retrieved from a known location, a simple HTTPS URI may be adequate and requires no knowledge of cryptography. If a secure tunnel is needed, consider using Https URL Connection or SSL Socket, rather than writing the user's own protocol. If the user's own protocol is needed to be implemented, she should not implement her own cryptographic algorithms.

3.1 Architecture for Android System

There are a number of components that makeup the Android application and android operating systems architecture**.** These are:

(a) The Applications part is the highest layer in the Android system architecture. This part represents the basic applications that can be found for devices that are represented such as telephone calls, email client, SMS program, calendars, browsers, and others. That is written in Java language and other languages [5].

(b) Application Framework is a layer higher than the system structure. It is the framework or the way the developer follows it through application development. The developer fully accesses the same framework as used by the previous layer [5,6].

(c) Libraries area layer contain software libraries, written in Java for the development of Android applications. A different of libraries, from surface manager to lib c, are written in different languages and these libraries are available for the developer to be used through the Framework application [7].

(d) Android Runtime is the fourth layer in android system architecture. This layer contains the so-called Dalvik Virtual Machine which is a type of JVM has been improved and modified to suit the Android system.[7].

(e) Linux kernel is a layer at the bottom of the structure which is responsible for handling its own hardware. Android relies on Linux for basic system services such as memory management, power management software and a number of other services [8].

4. GENERAL STRUCTURE OF THE SUGGESTED APPROACH

In this system, the message is encrypted with the RSA algorithm. The sender sends an encrypted message to the receiver on the Android platform. The message is encrypted using the public key from the key generation. The receiver gets the encrypted message and decrypts it using the private key from the key generation. The encrypted message or cipher text is decrypted by the receiver to get the original message or plaintext. The process is shown in figure 2 and figure 3.

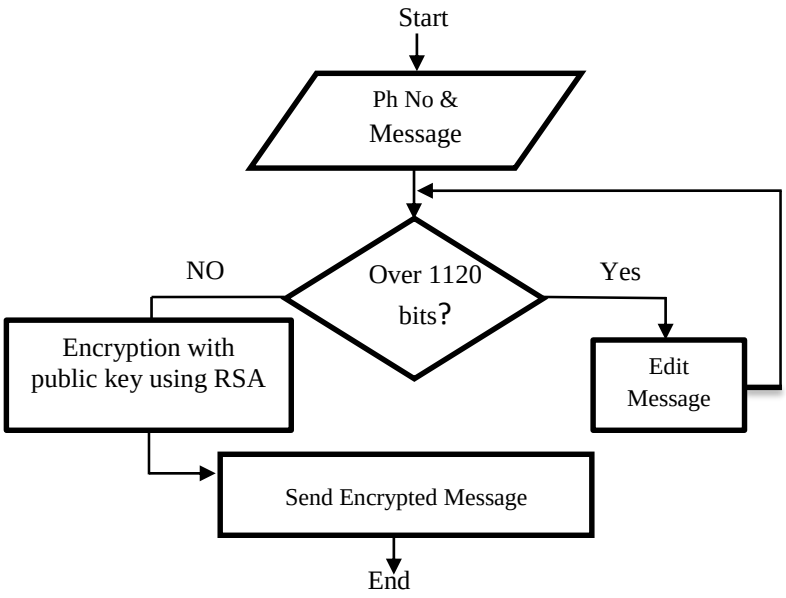

Fig. 2: System design of encryption in the sender side

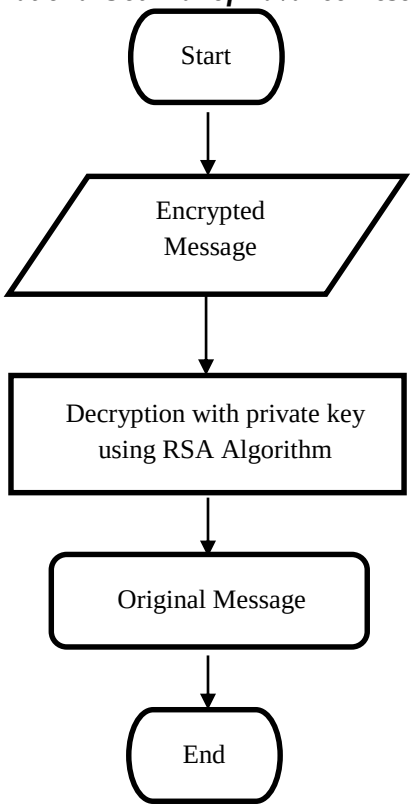

Fig. 3: System design of decryption in the receiver side

4.1. Implementation of the System

This system is implemented for the security of messages on android using RSA algorithms. It is developed by using Java Programming Language. First, the system runs on a computer using a java devolvement tool (Eclipse). After running on a computer, the RSA_Key_SMS.apk is released. This apk can be sent to android phones by using Bluetooth, USB debugging and so on. Both sender and receiver have to install this apk on their android phones. When using this app, this is opened by both sides. After installing and opening the application, the splash screen will appear as shown in figure 4.

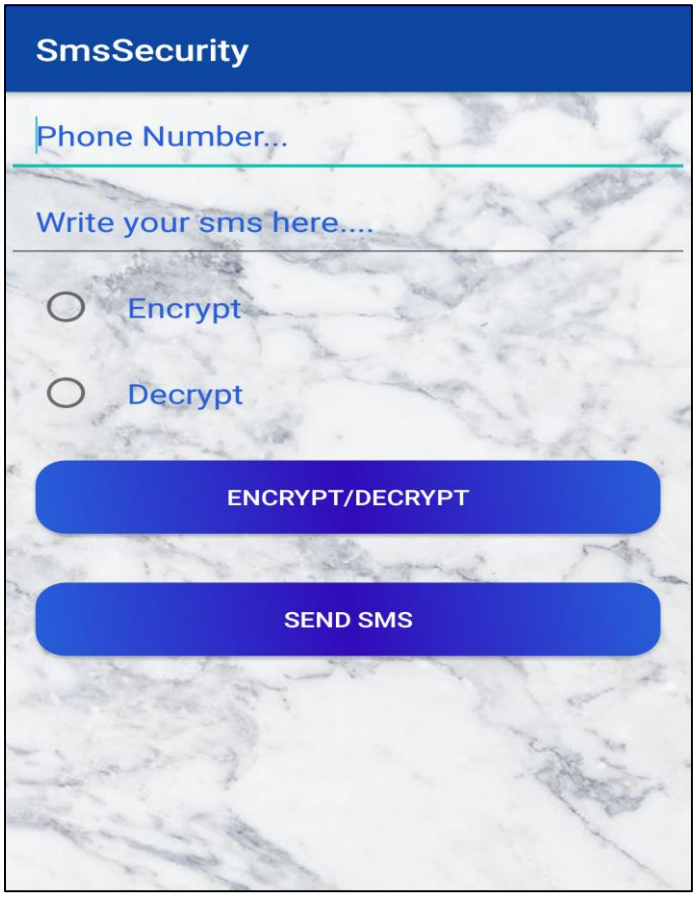

Fig. 4: Main Page of the System

The sender encrypts the original message and sends the encrypted message to the receiver as shown in Figure.5.

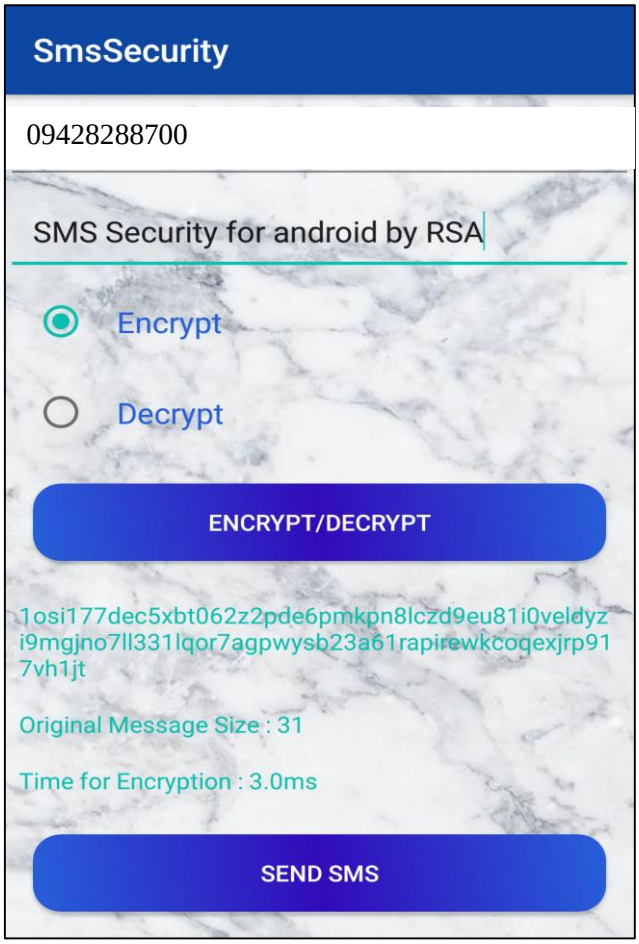

Fig. 5: Send the encrypted message to the receiver

However, if the message is over 64 words including space, the encrypted character is over original message 160 characters. So, the message will not send to the receiver. Then, the notice message will be displayed as shown in figure 6.

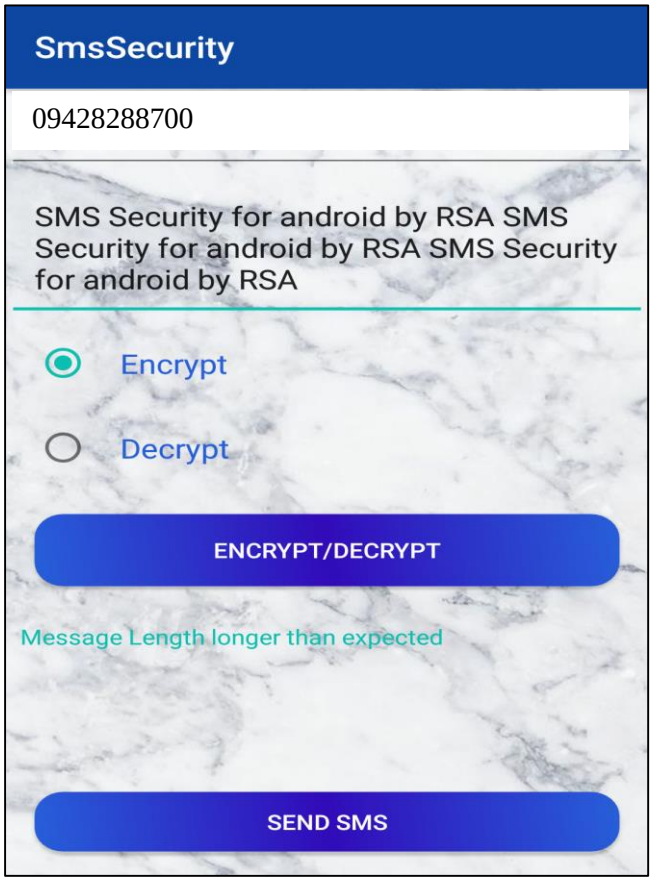

Fig. 6: The notice message

At the receiver side, incoming encrypted messages will be displayed as shown in figure 7.

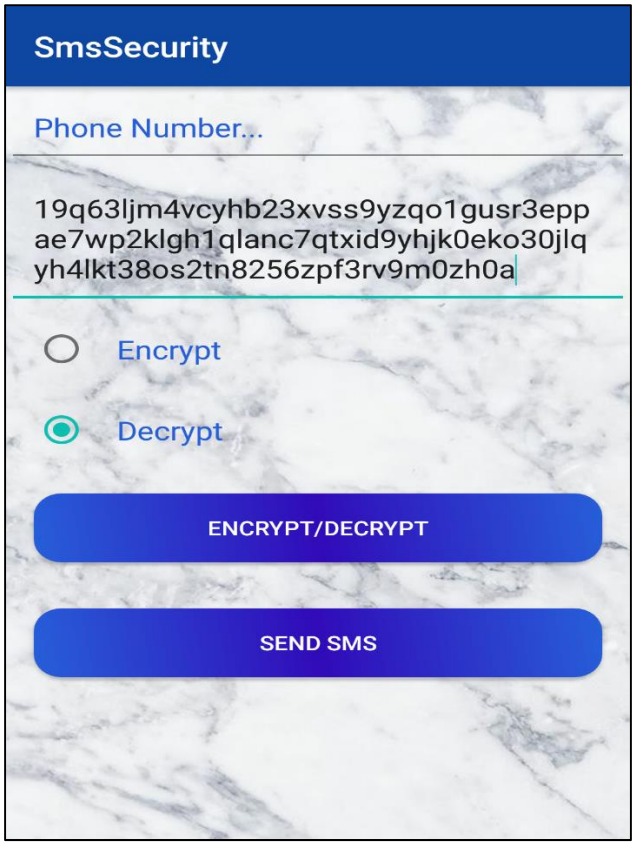

Fig. 7: The incoming message displayed

Then, the receiver decrypts the encrypted message by using the private key as shown in figure 8.

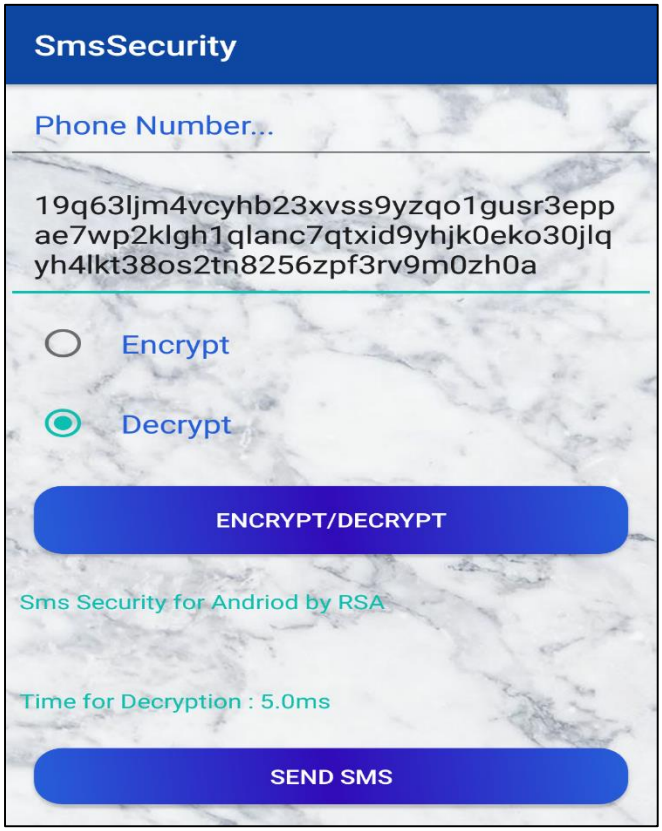

Fig. 8: Original message displayed

5. CONCLUSION

In this system, I will discuss the security of the relay SMS in mobile and how to encrypt and decrypt them, programming platforms of all kinds for the mobile phones and RSA Algorithm. This approach presents a method for encryption SMS messages of mobile in the Android operating system environment. The application is running on the mobile phone and does not require any additional encryption devices. The result showed that suitable and easy to implement in a mobile device for the proposed scheme. But the biggest dilemma at this point is that the size of the message which can be transmitted via SMS is limited. In future work, I

will use the other cryptography algorithm to encryption and decryption SMS and implement from through mobile and compared with traditional encryption in terms of time and speed in encryption and decryption operations for testing purposes.

6. REFERENCES

[1] RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Len. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM; 1978; 21.2: 120-126.
[2] http://en.Wikipedia.org/wiki/Short _Message_ Service
[3] htttp://en.Wikipedia.org/ wiki/ Andriod_28 % operating system%29
[4] William Stallings: Cryptography and Network Security Principles and Practice, Fifth Edition, (2011).
[5] Jianye Liu, " Research on Development of Android Applications" Fourth International Conference on Intelligent Networks and Intelligent Systems, IEEE 978-0-7695-4543-1, Volume 3, pp 69-72,2011
[6] Chao Wang, Wei Duan, Jianzhang Ma and Chenhuri Wang, "The research of Android System architecture and application programming" Computer Science and Network Technology International Conference (ICCSNT), Volume 2, pp 785 – 790, 2011.
[7] Huang, Qing: An extension to the Android access control framework, 2011
[8] Vaibhav Kumar Sarkania, "Android Internals" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 128X, Volume 3, Issue6, pp 143-147, 2013.
[9] D. Lisonek and M. Drahansky, Sms encryption for mobile communication, Proc International Conference on Security Technology, 2008. SECTECH'08, 2008, 198-201.
[10] Dr Chukwman Ezeobika: The Advantages and Disadvantages of the message encryption method, Created on September 20, 2012, www.helium.com.
[11] PEERSMAN, Gert, et al. A tutorial overview of the short message service within GSM. Computing & Control Engineering Journal; 2000; 11.2: 79-89.

BIOGRAPHY

Thandar Myint
Student
Technological University, Mandalay, Myanmar

