BORANG PENGESAHAN STATUS TESIS*

JUDUL: SECURE SMS

SESI PENGAJIAN: SESI 2008/2009

Saya ROHAIZA BINTI ABU SEMAN
(HURUF BESAR)

Mengaku membenarkan tesis (PSM/ ~~Sarjana/ Doktor Falsafah~~) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

______	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau Kepentingan Malaysia seperti yang termaktup di dalam AKTA RAHSIA RASMI 1972)
______	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ badan di mana penyelidikan dijalankan)
/	TIDAK TERHAD	

Rohaiza.
(TANDATANGAN PENULIS)

Alamat tetap: 103 B KG. SRI INDAH,
47000 SG. BULOH, SELANGOR

Tarikh: 13 JULAI 09

(TANDATANGAN PENYELIA)

IRDA BINTI ROSLAN
Nama penyelia

Tarikh: 13 JULAI 09

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

© Universiti Teknikal Malaysia Melaka

SECURE SMS

ROHAIZA BINTI ABU SEMAN

This report is submitted in partial fulfillment of the requirements for the Bachelor of computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2009

© Universiti Teknikal Malaysia Melaka

DECLARATION

I hereby declare that this project report entitled

SECURE SMS

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ____________ DATE: 13 JULAI 09

(ROHAIZA BINTI ABU SEMAN)

SUPERVISOR: ____________ DATE: 13 JULAI 09

(CIK IRDA BINTI ROSLAN)

© Universiti Teknikal Malaysia Melaka

DEDICATION

Specially dedicated to my beloved father, mother and family,

For my supervisor, Cik Irda Binti Roslan

(UTeM)

And lastly to my beloved friends and who have encouraged, guided and inspired me through my journey in education

© Universiti Teknikal Malaysia Melaka

ACKNOWLEDGEMENTS

I would like expand my gratitude and heartfelt thanks to Universiti Teknikal Malaysia Melaka (UTeM) and Faculty of Information and Communication Technology (FTMK) for providing such a good environment for students in gaining knowledge and skills.

First of all, I am particularly grateful to my supervisor, Cik Irda Roslan for her advising and encouragement from the earliest beginning. Thank you for her teaching, guidance and help during this project. Thanks for the support, cooperative in leading way throughout the whole progress of the project.

Special thanks my parent, siblings and friend for their support, thoughts and advices. Nothing is possible without their support and they inspired me to move even further and ever.

Lastly, I would like to thank everyone who involve for helping in this project. One again, I would like to grant all of them with my greatest because they really reserve it.

© Universiti Teknikal Malaysia Melaka

ABSTRACT

This title of this project is Secure SMS. This application is build to securing SMS we send through the mobility network. The SMS will be encrypting before sender send the SMS. On the other side receiver need to have the same application to receive the SMS and decrypt it. Both sender and receiver send and receiver SMS using the same port number. Both sender and receiver need to have this application to allow the transmission happen. Mobile device that been used must support java program with Mobile Information Device Profile (MIDP) 2.0 profile. The application can run in all mobile operating system that support java program. User need to upload the ".jar" file for enable to run the application. The installation will be different depending on the operating system of the device. In this application there will be a few basic interfaces like SMS application we usually used so it's easy to used and simple.

© Universiti Teknikal Malaysia Melaka

ABSTRAK

Tajuk projek ini adalah “Secure SMS”. Aplikasi ini dibina adalah untuk menjamin keselamatan sms kita yang dihantar melalui rangkaian mobiliti. SMS akan diencrypt sebelum pengirim menghantar sms tersebut. Penerima memerlukan aplikasi yang sama untuk menerima SMS dan decrypt serta membaca SMS yang diterima. Kedua-dua pengirim dan penerima menghantar dan SMS penerima menggunakan port yang sama. Kedua-dua pengirim dan penerima memerlukan aplikasi ini untuk membolehkan penghantaran SMS berlaku. Perkakas mobiliti yang digunakan perlu menyokong program java dengan Mobile Information Device Profile (MIDP) 2.0 sebagai profil. Aplikasi ini boleh digunakan dalam semua perkakas mobility yang mempunyai system pengoperasian yang menyokong program java. Pengguna perlu memuat naik fail ".jar" untuk membolehkan pengguna menggunakan aplikasi ini. Pemasangan bergantung pada sistem pengoperaian yang digunakan perkakas mobiliti. Aplikasi ini mempunyai beberapa antaramuka yang sama dengan aplikasi SMS yang biasa digunakan oleh pengguna. Ini akan memudahkan penggunaan aplikasi ini.

© Universiti Teknikal Malaysia Melaka

TABLE OF CONTENTS

© Universiti Teknikal Malaysia Melaka

© Universiti Teknikal Malaysia Melaka

© Universiti Teknikal Malaysia Melaka

© Universiti Teknikal Malaysia Melaka

LIST OF TABLES

© Universiti Teknikal Malaysia Melaka

LIST OF FIGURES

© Universiti Teknikal Malaysia Melaka

© Universiti Teknikal Malaysia Melaka

CHAPTER I

INTRODUCTION

1.1 Project Background

Short Message Service (SMS) is a communications protocol allowing the interchange of short text messages between mobile telephone devices. It is a store and forward way of transmitting messages to and from mobiles. The message (text only) from the sending mobile is stored in a central short message center which then forwards it to the destination mobile. This means if happen that the recipient is not available, the short message is stored and can be sent later.

Lately, SMS has replaced the traditional way of human communication. The change is caused by the changing lifestyle, flexibility of network and advance technology in mobile device. SMS is one of the communication protocols that used to exchange information in text message between mobile handsets. SMS is transformed into data packet when travel in GSM/UMTS network and this technology operates approximately in real time mode.

The previous use of SMS is for one way communication such as news, stocks report, and weather forecast. Today, SMS is practiced as the easiest, fastest and cheapest daily communication tool. The usage of SMS expands greatly by the rapid growth of mobile system. SMS has switched from conventional human communication to system

© Universiti Teknikal Malaysia Melaka

device communication. Some of the software systems are programmed to send alert to mobile device and receive control command from particular handset in SMS. For example, vehicle tracking service uses the SMS to notify car stolen cases and uses the mobile SMS to remotely control home appliances.

SMS are sometimes used for the interchange of confidential data such as social security number, bank account number, password etc. A typing error in selecting a number when sending such a message can have severe consequences if the message is readable to any receiver. Most mobile operators encrypt all mobile communication data, including SMS messages but sometimes this is not the case, and even when encrypted, the data is readable for the operator.

So solution for this problem is to encrypt the message sender want to send. And receiver will decrypt back the message to read it. This system has both functions that can encrypt the plaintext to cipher text and decrypt back the cipher text to the plaintext. With this function the message cannot be read by the third party like the operator.

1.2 Problem Statement

Today everyone loves mobile phone text messages or mostly knows as Short Message Service (SMS). These short text messages are discreet, direct, and instantaneous but at the same time, surprisingly insecure. The contents of SMS messages are known to through network operator's applications and personnel. Therefore, SMS is not an appropriate technology for secure communications.

© Universiti Teknikal Malaysia Melaka

1.3 Objective

- Provide sent and receive message between mobile users.
- To secure the message from sender to receiver been read by the third party.
- To create a new idea of secure message in system telecommunication.

1.4 Scope

The scope of this system is the user of mobile phone. This system using java program that supported for most of mobile device.

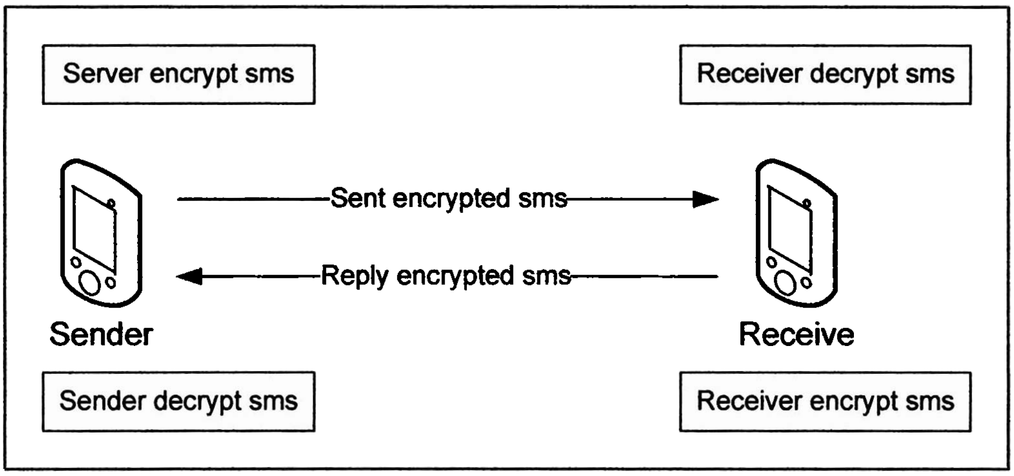

Figure 1.1 Preview design for the Secure SMS system

Refer to figure 1.1, this system is one-to-one system means that sender encrypt the message then send it to receiver. Then receivers will receive the message and decrypt it. Both user need to install the system to allow user to read the message. Both user also have to use mobile device with Mobile Information Device Profile (MIDP) 2.0, the system will only can operates in device with MIDP 2.0.

© Universiti Teknikal Malaysia Melaka

1.5 Project Significance

SMS today is important way to communicate between people. SMS increases the amount of voice calling by providing a mechanism for voice mail notification to the handset. SMS provides a convenient, low-cost mechanism for non-voice communication. SMS provides a mechanism for enabling various other systems such as prepaid. User also sometimes used SMS to exchange private or confidential information with others.

Most of the technology today encrypt message been send but it still readable by the operator. In any case one user send his/ her bank account number to the receiver it can be read by anyone if the sender mistakenly sends the SMS. With this project the SMS message will be encrypt by the sender and send the cipher text through the network. Event the third party stole the message it still cannot be read because of the cipher text. The message will be decrypt back to the plain text when receiver receives the SMS.

1.6 Expected Output

The expected output can be concluding from this project is the SMS message been send through network securely. Using Netbeans 6.5 Java 2 Micro Edition as IDE to build the system with the appropriate security algorithm to create a system that can be used for the above proposes. To reduce the possibility wrong sending private information and been read by other people.

Then message (data) will be encrypt to cipher text and send to the receiver. When receivers receive the message it will come in cipher text before receiver decrypt it into plain text. The database will show what message been sent and what type is the receivers receive the message.

© Universiti Teknikal Malaysia Melaka

1.7 Conclusion

Most mobile operators encrypt all mobile communication data, including SMS messages but sometimes this is not the case, and even when encrypted, the data is readable for the operator. Among others these needs give rise for the need to develop additional encryption for SMS messages, so that only accredited parties are able to engage communication. An approach to this problem is to develop an system that can be used in mobile devices to encrypt messages that are about to be sent. Naturally decryption for encrypted messages is also provided.

This system act as firewall before the message been seen and receive. Before the message had been sent it will be encrypt to the cipher text and the receiver will decrypt back to the plain text to read it. If the users send private information it will be secure from others event the operator.

In the future, maybe the secure SMS message can be encrypt using key. Means every user has their own key and when the sender wants to send the message, key receiver will be used to encrypt the message.

© Universiti Teknikal Malaysia Melaka

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter is to discuss and study about Secure SMS issue and development process includes programming tools and system features. To develop a project, it need more research and information about the project as a guideline to make sure that the project will be execute successfully. The research that needs to make is about the scope of the project, the main objective, understands about the system requirement and a comparison with the existing system.

To gain the requirement to execute the project, there are several task has to been done such as review on related books, internet and study the existing system. Mostly the internet and books resources are referred to get more idea and source to develop the project.

© Universiti Teknikal Malaysia Melaka

2.2 Literature Review

2.2.1 Domain

Information and Communication Technology (ICT) in Defense introduce to provide security in ICT. Now days most of our work can be done online such as paid bills, register account, send email including using mobile to communicate. With this user personal details vulnerable to danger.

In this project the system will provide security for the message. In the term of defense this system avoid private message been stolen and read by the third party. In some case user needs to send personal message to receiver and to keep the message private between sender and receiver this system can be used.

2.2.2 Keyword

2.2.2.1 Short Messaging Service (SMS)

SMS is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems. SMS provides a mechanism for transmitting short messages to and from wireless devices.

The service makes use of a Short messaging service center (SMSC), which acts as a store-and-forward system for short messages. The wireless network provides the mechanisms required to find the destination station(s) and transports short messages between the SMSCs and wireless stations.

© Universiti Teknikal Malaysia Melaka

SMS supports several input mechanisms that allow interconnection with different message sources and destinations. SMS also guarantees delivery of the short message by the network. Temporary failures due to unavailable receiving stations are identified, and the short message is stored in the SMSC until the destination device becomes available.

The benefits of SMS to subscribers center on convenience, flexibility, and seamless integration of messaging services and data access. From this perspective, the primary benefit is the ability to use the handset as an extension of the computer. SMS also delivery of notifications and alerts, guaranteed message delivery, reliable and low-cost communication mechanism for concise information.

2.2.2.2 Cipher

Cipher is a complicated computer software algorithm that is used to perform digital encryption and decryption (Bauchle, et al. 2006). The plain text (message) is transformed by the cipher throughout a repetition of processing steps into cipher text. The reverse process converts the cipher text back to the original message.

There are three types of cipher which are *symmetric*, *asymmetric*, and *hybrid* (Knudsen, 1998:89). The symmetric cipher uses one secret key, known as private key and used to perform encryption and decryption. Pairing keys are needed for asymmetric cipher. Public key is for encryption purpose while private key is required for decryption. Hybrid cipher is the effort of combination of symmetric and asymmetric ciphers.

Asymmetric cipher takes longer time to practice the encryption and decryption process when compared to symmetric cipher. In hybrid system, asymmetric key pair is used for distributing the symmetric key. Some of the popular cipher algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), ElGamal, and RSA. Table 2.1 below shows comparison between symmetric algorithm and asymmetric algorithm.

© Universiti Teknikal Malaysia Melaka

Comparison	Encryption algorithm	
	Symmetric algorithm	**Asymmetric algorithm**
Key used	Secret key	Public key and private key
Key distribution	Private domain	Public domain
Speed	Fast	Slow
Security	Encryption/ decryption	Authentication

Table 2.1 Symmetric algorithm versus Asymmetric algorithm

2.2.2.3 Encryption

The safest way to ensure all confidential data, file and message are unreachable by adversary or unauthorized person is encryption. Encryption is the conversion of plain text into unreadable cipher text. This conversion is done after undergoing a series of complex mathematical transformational steps. Therefore, it can prevent eavesdrop activity.

The security of encryption depends on the decided key length and algorithm used. According to National Security Agency (NSA), the key length falls between 192 to 256 bits is considered as TOP SECRET level (Fact Sheet NSA Suite B Cryptography, 2008). If the encryption algorithm is more complex, the produced cipher text may be harder to be broken. However, the implementation cost will be more expensive and decrease the speed of the performance.

2.2.2.4 Decryption

The procedure that needs to transform the cipher text to the original message is called decryption. The actual message can only be read when the correct key is given. Same key is used for symmetric encryption and decryption. Furthermore, same

© Universiti Teknikal Malaysia Melaka

algorithm that applies for encryption must be used for decryption. Asymmetric encryption/decryption also execute in the same manner.

2.2.2.5 Symmetric Algorithm

There is a lot of symmetric algorithm available for cryptography purpose. As mentioned before, the security of algorithm depends on the chosen algorithm and decided key length. Generally, the algorithm uses a secret key to change the normal text into unreadable cipher text (encryption) and then use back the same key and algorithm to get back to the original text.

Figure 2.1 below shows the encryption and decryption operation of symmetric algorithm. Symmetric encryption is simple, fast, and easy to apply on digital message. This is the main reason why it is so popular in electronic commerce (E-commerce). The execution speed on performing encryption and decryption is within 10 milliseconds with minimal computer power.

The mobile devices such as cell phone and Personal Digital Assistance (PDA) phone take longer time (within 100 milliseconds) due to low processor power. The publicly used symmetric algorithms are DES, Triple DES, AES, Blowfish and RC4.

© Universiti Teknikal Malaysia Melaka