SMS Security System on Mobile Devices Using Tiny Encryption Algorithm

M S Novelan, A M Husein, M Harahap and S Aisyah
Faculty of Technology and Computer Science, Universitas Prima Indonesia, Indonesia

E-mails: teknisiputra@gmail.com, amirmahmud@unprimdn.ac.id, mawaddah@unprimdn.ac.id, sitiaisyah@unprimdn.ac.id

Abstract. The development of telecommunications technology is so rapid has given such great benefits. With the telecommunication technology, distance and time no longer be a significant obstacle. One of the results of telecommunications technology that is well known is the Short Message Service. In this study developed an application on the mobile phone to modify the SMS message into ciphertext so that the information content of the SMS is not known by others. SMS delivery system for encrypting messages into ciphertext using a key that is entered by the sender then sends to the destination number. SMS reception system to decrypt it to others via SMS without the fear of information from these messages will be known by others. The method used in the system encrypt and decrypt the message is the algorithm Tiny Encryption Algorithm and implemented using the Java programming language. JDK 1.7 as the Java programming language ciphertext into plaintext using the key entered by the receiver and displays the original message to the recipient. This application can be used by someone who wants to send a confidential information and the Java compiler. Eclipse, a Java SDK and the Android SDK as a Java source code editor.

1. Introduction
Encryption is the process of converting an original message called plaintext into an unreadable code or code called ciphertext and can not be understood. To return a message to the original form as it needed a process called decryption. Encryption is intended to protect and conceal information so as not to be seen by parties or non-intended persons. Inside the computer security is known a cryptographic technique, which is used for message encoding. Based on the importance and confidentiality of a message it requires a way to secure a message or information using cryptographic techniques. One of the cryptographic techniques is using Tiny Encryption Algorithm (TEA) algorithm. TEA is a block cipher algorithm created by David J. Wheeler and Roger M. Needham from Cambridge University in 1994. The most prominent of the TEA is the simplicity of implementation, the absence of S-Box and P-Box and high speed.

2. Theoritical Basis

2.1 Security
The security of an android device is one of the hallmarks of this device, as it is well known that android devices have security designed for the convenience of users, but some services on certain features that do not have a method of security on the data it stores, one of which is the SMS service.
(Short Message Service) which on the android device by default does not have a security method at all. So it is needed to overcome the third-party software applications in securing the SMS service.

2.2 Cryptography
Cryptography comes from the Greek word from Crypto and Graphia which means secret writing. Cryptography is a science that studies the writing of a secret, in which the definition of cryptography according to (Schneier, 1996) is the science as well as the arts to maintain the security of messages (message) Cryptography is part of a branch of mathematical science called Cryptology. Cryptography aims to maintain the confidentiality of information contained in the data so that the information can not be known by unauthorized parties.

2.3 Encryption
Encryption is the process of securing an information by making the information unreadable without the help of knowledge and or special tools. The way used to perform encryption is to change a code from an understandable into a code that can not be understood. A coding system uses a table or dictionary that has been defined to replace the word of the information or piece of information sent. Encryption can be interpreted as a code or cipher. A cipher uses an algorithm that can encode all stream data streams from a message into an unintelligible cryptogram.

2.4 Description
Decryption is an algorithm or a way that can be used to read encrypted information for readability. In other words the description is the process of giving the result given from the encryption process into the initial form before the encryption.

2.5 Algoritma TEA (Tiny Encryption Algorithm)
TEA is a block cipher algorithm created by David J. Wheeler and Roger M. Needham from Cambridge University in 1994. The most prominent of the TEA is the simplicity of implementation, the absence of S-Box and P-Box and high speed. TEA operates in 64 bit block size and 128 bit key length. TEA is based on Feistel network and has 32 rounds. The K key will first be divided into 4 internal keys ie K [0..3] each length of 32 bits.

3. The Scheme Of System
The TEA encryption system uses a feistel network process by adding a mathematical function of addition and subtraction as an inverting operator other than XOR illustrated in the figure 1.
Figure 1. The structure of the Tiny Encryption Algorithm (TEA).

3.1 Cycle TEA (Tiny Encryption Algorithm)
The structure of the encoding with the algorithm for one cycle (two rounds) is illustrated in the figure 2:

Figure 2. One Cycle TEA (Two Rounds).

3.2 Flowchart Encryption
Flowchart for the encryption process illustrated in the figure 3:
Figure 3. Flowchart of the Encryption Process.

3.3 Flowchart Decryption
Flowchart for the encryption process illustrated in the figure 4.
4. User Interfaces

4.1 See the preview
Before the operation, the program will display a page like this:

![Figure 5. The main menu view.](image)

4.2 Display new message
Access view to write sms and send messages
4.3 List Message
The view a list of incoming messages, sent messages and saved messages

5. Conclusions
From the results of research and discussion undertaken conclusions can be drawn as follows:
1. The software designed can be used to process files that have been encrypted to mobile phone, can be done file decryption process to see the actual file.
2. The software can only perform encryption and decryption, done by using one time pad algorithm.
3. The key to decrypt an encrypted file must be the same as the key when the file was sent.
4. The speed of the encryption / decryption process depends on the size of the file, the larger the file size the more time it takes for encryption / decryption.

References
[1] M. Feldhofer, J. Wukerstorfer, and V. Rijmen, “AES Implementation on a Grain of Sand,” IEE Proc, vol. 152, no. 1, Oct. 2005, pp. 13-20.
[2] G. Leander et al., “New Lightweight DES Variants,” Proc. Fast Software Encryption (FSE 07), LNCS 4593, Springer-Verlag, 2007, pp. 196-210.
[3] S. Kumar et al., “Breaking Ciphers with COPACOBANA—A Cost-Optimized Parallel Code Breaker,” Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES 06), LNCS 4249, Springer, 2006, pp. 101-118.

[4] T. Good and M. Benaissa, “Hardware Results for Selected Stream Cipher Candidates,” Workshop Record State of the Art of Stream Ciphers (SASC 07), 2007, http://www.ecrypt.eu.org/stream/papersdir/2007/023.pdf.

[5] S. Kumar, “Elliptic Curve Cryptography for Constrained Devices,” doctoral dissertation, Electrical Engineering and Information Sciences, Ruhr University Bochum: Germany, 2006.

[6] L. Uhsadel, A. Poschmann, and C. Paar, “Enabling FullSize Public-Key Algorithms on 8-bit Sensor Nodes,” Proc. 4th European Workshop Security and Privacy in Ad hoc and Sensor Networks (ESAS 07), LNCS 4572, Springer-Verlag, 2007, pp. 73-86.