Abstracts

4th ICIBA

3rd International Conference on Information Technology and Engineering Application

February 20 - 21, 2015

iT & Engineering For a Better Life

PALEMBANG - INDONESIA

Hosted by

Universitas Bina Darma

Program Pascasarjana

Ir. Cooperation with

UTM

Telepon : 0711-515679, 515582
: 0711-515582
Website : http://iciba.binadarma.ac.id
mail : iciba@binadarma.ac.id

SMS SECURITY SYSTEM WITH ENCRYPTION DECRYPTION BLOWFISH ALGORITHM BASED ON MOBILE ANDROID

Fitri Andiyani, Yesi Novaria Kunang, Evi Yulianingsih

Universitas Bina Darma
fitriandiyani26@gmail.com
yesi_kunang@mai.binadarma.ac.id
evi_yulianingsih@mail.binadarma.ac.id

Abstract

Short Message Service is known as the facilityto send and receiving short message which contain text (short text message) through the nircable ware, communication device called mobile phones. Although own so many advantages for people, SMS itself also own a minus or weakness in the progress. Build with the same systems a.... Short Message Service is known as the facility to send and receiving short message which contain text (short text message) through the nircable ware, communication device called mobile phones. Although own so many advantages for people, SMS itself also own a minus/weakness in the progress. Build with the same systems and programs possibly made what-so-called Roaming from the local channel/net until to strange/unknown channel/net happen, which affected to shaped SMS Spoofing in the manipulation form. One of the way out is using SMS protector with sms chriptography what take benefit from/using keys to describe enscripted SMS. One of the method to enscripted data or message is Algoritma Blowfish. Algoritma Blowfish is included as key-symmetric algoritma what own the same keys to enscripted a data. Algoritma Blowfish is also included as The Chiper Block what until now still can be claimed as the safe one caused by no attacker who really succeed on solve the Algoritma Blowfish existed till now.

Keywords : *Algoritma Blowfish, Dekripsi, Enkripsi, SMS.*

GEOGRAPHIC INFORMATION SYSTEM FOR MONTHLY RAINFALL FORECAST MAPPING USING ARIMA(AUTO REGRESSION INTEGRATED MOVING AVERAGE)

Bambang Beny Setiaji

Binadarma University
cuacawan@gmail.com

Abstract

Kenten Climatology Station as one of stations of Indonesia Agency for Meteorological, Climatological and Geophysicsknown as BMKG serve public for climatology service in collecting and processing rainfall data only in desktop computer so solution for this this paper will review about web base. Geographic Information System (GIS) in collecting and processing rainfall data moreover for forecasting using ARIMA (Auto Regression Integrated Moving average) method. The conclusion of this paper is a geographic information system that can be accessed from internet and produce time series rainfall forecasting with ARIMA (1,0.1) model for 24 (twenty four) data samples and ARIMA (1,1,1)model for 3 (three) data samples. Data samples are obtained from 27 (twenty seven) rainfall stations and posts which spread out over South Sumatera.

Keywords:Rainfall, GIS, ARIMA.

SMS SECURITY SYSTEM WITH ENCRYPTION DECRYPTION BLOWFISH ALGORITHM BASED ON MOBILE ANDROID

Fitri Andiyani, Yesi Novaria Kunang, Evi Yulianingsih

Universitas Bina Darma
e-mail:
fitriandiyani26@gmail.com
e-mail:
yesi_kunang@mai.binadarma.ac.id
e-mail:
evi_yulianingsih@mail.binadarma.ac.id

Abstract

Short Message Service is known as the facilityto send and receiving short message which contain text (short text message) through the nircable ware, communication device called mobile phones. Although own so many advantages for people, SMS itself also own a minus or weakness in the progress. Build with the same systems a Short Message Service is known as the facility to send and receiving short message which contain text (short text message) through the nircable ware, communication device called mobile phones. Although own so many advantages for people, SMS itself also own a minus/weakness in the progress. Build with the same systems and programs possibly made what-so-called Roaming from the local channel/net until to strange/unknown channel/net happen, which affected to shape SMS Spoofing in the manipulation form. One of the way out is using SMS protector with sms chriptography what take benefit from/using keys to describe enscripted SMS. One of the methods to enscripted data or message is Blowfish algorithm. Blowfish algorithm is included as key-symmetric algorithm what own the same keys to encrypt data. Blowfish algorithm is also included as The Chiper Block what until now still can be claimed as the safe one caused by no attacker who really succeed on solve the Blowfish algoorithm existed till now.

Keywords : *Algoritma Blowfish, Dekripsi, Enkripsi, SMS.*

1 INTRODUCTION

The last few years, there have been very rapid development in mobile phone technology (cell phones). One is started popping smart phone with a variety of features and has complex operating systems like computers. Starting from a phone that can only be used to talk and sms to "smart phones" (smartphone) which has various functions such as multimedia, multiplayer games, data transfer, video streaming and others. A variety of operating systems for mobile phones were introduced, including a fairly well known is Android.

One of the facilities used in mobile phones for sending data in the form of short messages via short message service (SMS). However, the SMS facility itself has many weaknesses that SMS is built with the same systems and programs, and SMS itself can roam the local network to the foreign network that SMS spoofing is possible in the form of disguise or manipulation of information such as addresses or other data that resemble users in general.

Other SMS weakness is the content of SMS messages sent in the open system service providers and employees. Abroad use SMS to send a secret message had already been developed. For example, in the UK a mobile operator, staellium UK, issued a service called "stealth text" that can be used to send messages securely, ie by deleting messages automatically as soon as 40 seconds the message is read or known by the name of self-destruct text message. There are also security sms sms using that utilizes cryptographic key to decrypt the text that has been in encryption. One method of data encryption or message is Blowfish algorithm.

Blowfish algorithm including symmetric key algorithms that have the same key to encrypt the data. Through encryption, the data that is important to be encoded by using a key that the key will also be used in the process of reading the data (descript). Based on this, the authors make the application design SMS encryption and decryption using the Blowfish algorithm. Blowfish algorithm including a block cipher and is still considered safe because no attacker who actually broke the Blowfish algorithm. Therefore, the authors will try to make a security sms with Blowfish method to encrypt the data that runs on Android operating system so that owners of Android-based mobile phone that can perform data exchange SMS with a more secure and comfortable.

Problem to be addressed in this research is limited encryption and decryption are performed is SMS data. Two sides users are required to use encryption on the mobile application being used. Mobile devices are used is a phone with Android operating system.

2 RESEARCH METHODOLOGY

2.1 Place and Time Research

This research was conducted at the University of Bina Darma Palembang in September 2014 through December 2014.

2.2 Research Methods

The method used in this study using the research method Unifed Rational Process (RUP), while the four-phase conducted in this study are as follows.

1. *Inception,* In this phase, the authors analyze the system, including the determination of the scope, the user needs is divided into two, namely the functional requirements described through the use case diagrams and non-functional requirements, analysis and problem solving procedural logic system with the activity diagram.

2. *Elaboration*, Based on the analysis results obtained from the analysis phase (Inception), the authors began to design a complete system. Start of designing a package diagram, the display (Interface) as the initial appearance design, design class diagrams, sequence diagrams and design the display interface.

3. *Construction,* At this stage the author to re-examine the results of the two previous stages, namely stages of analysis and design phase. Is it in accordance with the analysis that has been done. After appropriate then the author will start to implement the making of an application on a hardware design.

   Transition, Once the design is completed application is implemented, the authors submit the application to the user (user) that is the target of designing an application that made the author. Furthermore, the authors carried out tests on the application by requesting a response from the user (user), on application use of questionnaires as a medium to see the response from the user (user).

2.3 Analysis System

Before starting the design phase of the system (System Design) first performed the analysis system. At this stage will be determined the scope, the user needs is divided into two, covering functional requirements described in the use case diagrams and non-functional requirements, procedural logic system with the activity diagram.

2.4 Problems Analysis

At this stage of the design development application SMS encryption and decryption using the Blowfish algorithm, the authors found some problems to be analyzed, among others:

1. How to maintain the confidentiality of the data in the SMS using the Blowfish algorithm.

2. Implement the Blowfish algorithm in Android-based mobile.

2.5. Requirement Analysis

Analysis of user needs is divided into two groups: functional requirements analysis and analysis of non-functional requirements.

1. The non-functional Requirement is a requirement that support the work of a system, but does not bring direct influence on the performance of the system itself.

2. Functional requirement provides an overview of system services is available, who begin and how the system responds to this.

2.6. Blowfish algorithm

Blowfish is a symmetric key cryptography algorithm is a block cipher with a block length of 64 bits fixed throughout. The algorithms also apply any technique sized keys. Key size that can be accepted by blowfish is between 32 to 448 bits, with a standard size of 128 bits. Blowfish utilizes the bit manipulation techniques and playback techniques and key rotation performed 16 times. The main algorithm is divided into two main sub-algorithms, namely the expansion and part of the encryption key and a description of the data. Key expansion is done at the beginning of the input of a key with a length of 32 to 448 bits, and the output is an array of sub-keys with a total of 4168 bytes. Part of encryption and decryption of data occurs by utilizing a looping 16 times against Feistel network. Each iteration consists of permutations with the input is the key, and the substitution of data. All operations are performed by using xor operations and additions. Additions made to the four lines lookup is done each revolution, (Teak Revelation Aji: 4, 2011)

3 RESULTS

3.1. Stages Running Programs

The initial phase should be done for the user running the application encryption and decryption of this SMS is choose the applications you have installed on the phone and then the user can start the application.

3.2. Running Programs Menu Display

Menu display page is the page where the user can begin to access the application, by selecting one of the menu, among others, Send SMS and Read Messages. Display menu page can be seen in Figure 3.1.
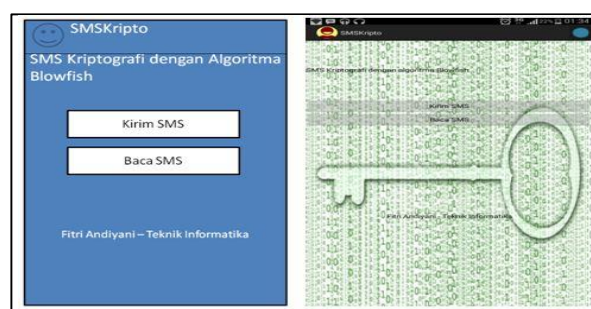
Picture 3.1 Display *Menu*

3.3. Starting the Display Program Send SMS

Page send a message is a page where users can write a message to be sent. On this page the user can enter the destination number, contents and key messages. On this page there is an option to send a message and automatically after the user selects the Send SMS will display a message that has been encrypted in the input plaintext form. Pageviews send a message can be seen in Figure 3.2.
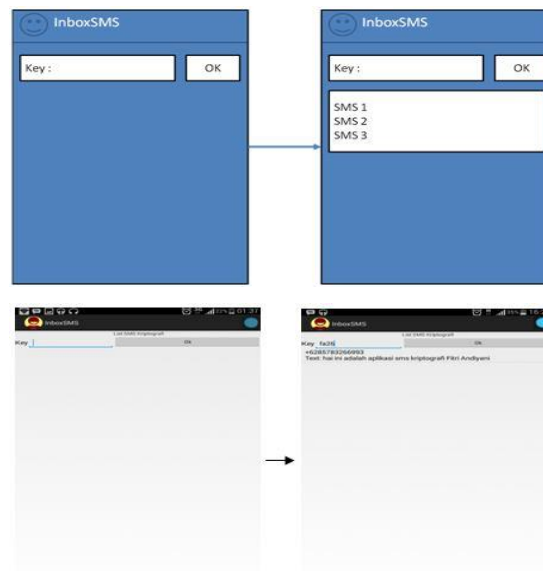
Picture 3.2 Send Message Display

3.4. Running Programs Display Read Message

Read display page is a page message contains the messages received by the user. Read a message directly connected to the SMS Inbox and to access the SMS inbox first user must perform key input. After the user input the key it will show the contents of incoming messages. Display read SMS inbox messages and can be seen in Figure 3.3.

Picture 3.3 Read Message Display.

4 CONCLUSION

Based on the results of the discussion in the previous chapters in this thesis report, it can be concluded as follows :

1. Blowfish algorithm can be applied to applications based on Android SMS Cryptography.
2. SMS Cryptography Applications can be run on Android version 4.2.2 (Kitkat), the Android version 4.1.2 (Jelly Bean), Android Version 3.2 (Icecream Sandwich), the Android version 3.0 (Honey Comb), Android Version 2.3 (Ginger Bread).

5 REFERENCES

Ariyus, Doni. (2006), "*Kriptografi Keamanan Data dan Komunikasi*", Penerbit Graha Ilmu, Yogyakarta.

Ariyus, Dony. (2009), "*Keamanan Multimedia*", Penerbit Andi, Yogyakarta.

H, Nazruddin Safaat. (2012), "*Android Pemprograman Aplikasi Mobile, Smartphone dan Tablet PC Berbasis Android*", Penerbit Informatika, Bandung.

Kadir, Abdul. (2004), "*Dasar Pemprograman Java 2*", Penerbit Andi, Yogyakarta.

Kurniawan, Yusuf. (2004), "*Kriptografi Keamanan Internet dan Jaringan Komunikasi*", Penerbit Informatika, Bandung.

Munir, Rinaldi. (2006), "*Kriptografi*", Penerbit Informatika, Bandung.

Sadikin, Rifki. (2012), "*Kriptografi Untuk Keamanan Jaringan*", Penerbit Andi, Yogyakarta.

Utomo, Eko Priyo. (2013), "*Cara Cepat dan Mudah Belajar Java*", Penerbit Andi, Yogyakarta.

Wahana Komputer Semarang. (2003), "*Memahami Model Enkripsi dan Security Data*", Penerbit Andi, Yogyakarta.