International Journal of Information System & Technology
Vol. 3, No. 1, (2019), pp.131-139

Cryptographic Symmetry Analysis with AES Algorithm for Safeguarding Data at Government Agencies

Muhammad Rizal[1], Elviawaty Muisa Zamzami[2], Muhammad Zarlis[3]

[1,2,3] Universitas Sumatera Utara (USU), Medan - Indonesia
[1] rizaldal44@yahoo.com, [2] elvi_zamzami@usu.ac.id, [3] m.zarlis@yahoo.com

Abstract

Data is very confidential information because it contains important information about the company or agency. Therefore it is necessary to secure these important data, in order to avoid misuse, theft of information or manipulation by certain parties who are not responsible. To avoid theft and manipulation of data it is necessary to implement a computer-based security system. One of them is by using cryptography. Cryptography is the study of how to change information from a normal (understandable) state / form into an incomprehensible form. One method that can be used to secure messages or information is the Advanced Encryption Standard (AES). AES is a part of symmetry cryptography. The application of AES cryptographic algorithms in securing data at government agencies can produce encryption that cannot be understood by humans and produce decryption that is exactly the same as the initial plaintext inputted, so that important government data can be secured in such a way. This research will produce a program that can encrypt and decrypt data using the AES (Advanced Encryption Standard) algorithm which will be used to secure data at Government Agencies.

Keywords: *Cryptography, Symmetry, AES Algorithm, Data Security, Government Agencies*

1. Introduction

Data is important information which is one of the vital things in the ongoing of a company, educational institution or government agency. So that requires a variety of considerations for data storage, especially in terms of security and confidentiality. Very often there are cases of leakage of confidential data by unauthorized parties such as hackers or crackers that cause great losses to the owner of the data. Pematangsiantar Mayor's Office is a government office that has a lot of data, both employee data, financial data, population data, and local government data. This will certainly be a consideration in data storage because the protection of the authenticity of data and information is a very important need in the present and beyond.

From the author's observations, many offices of government agencies such as the Aceh Mayor's office have not yet implemented a data security system. The computer user can be accessed by anyone so it is very risky if there are people who are not responsible for accessing sensitive and valuable information. Another possibility is that the information contained therein may change, causing changes or damage to data and can be misused for the benefit of the data owner. Efforts to protect data can be done in various ways, one of which is by applying cryptography. Cryptography is a technique for securing and sending data in a form that is difficult to read so that it can secure important data both stored in storage media and transmitted through communication networks. Cryptography is the science of securing data with encryption techniques where the original data is encrypted using an encryption key into data that can only be understood by someone who has a decryption key. In classical criticism, the encryption technique used is symmetrical encryption where the key description is the same as the encryption key. The secret lies in several parameters used, so the key is determined by the parameter. The parameters that

ISSN : 2580-7250

determine the decryption key must be kept secret (the parameter becomes equivalent to the key.

Efforts to protect data can be done in various ways, one of them by applying the cryptographic field. Cryptography is a technique for securing and sending data in a form that is difficult to read, so that it can secure important data both stored in storage media and transmitted through communication networks. Cryptography is the science of securing data with encryption techniques where the original data is encrypted using an encryption key into data that can only be understood by someone who has a decryption key. In classical criticism, the encryption technique used is symmetrical encryption where the key description is the same as the encryption key. The secret lies in several parameters used, so the key is determined by the parameter. The parameter that determines the decryption key must be kept secret (the parameter becomes equivalent to the key) [1].

Previous research discusses the Application of AES Algorithm: Rijndael in Encrypting Confidential Data [2]. In this study discusses the application of Rijndael cryptographic algorithms in data security. It starts by analyzing the workings of the Rijndael algorithm and then designs an application that can encrypt and decrypt plaintext user input. The evaluation results show that the Rijndael algorithm can produce encryption that cannot be understood by ordinary people, and produces the exact decryption of the initial plaintext input by the user. Here the author applies a data security method namely AES (Advanced Encryption Standard) which is a symmetric key-encryption standard adopted by the United States government. AES Algorithm is a non-feistel block coding system because AES uses components that always have an inverse with a block length of 128. AES Algorithm uses a repetitive process called a round. the number of rounds used by AES depends on the length of the key used. Each round requires a round key and input from the next round [3]. Based on these problems, the authors conducted this research.

2. Research Methodology

2.1. AES Algorithm Parameters

Following are the parameters in the AES algorithm:

a. *Plaintext: 16-byte array, which contains input data*.
b. *Ciphertext: 16-byte array, which contains the results of encryption*.
c. *Key: a 16-byte array, which contains a ciphering key (also called a cipher key)*.

With 16 bytes, 128-bit data blocks and keys can be stored in an array of 16 characters (16 x 8 = 128).

2.2. Symmetry Algorithm

Symmetry algorithm or also called classic algorithm, uses the same key for encryption and decryption activities. When sending messages using this symmetry algorithm, the recipient of the message must be notified of the key of the message in order to be able to decrypt the message sent. The security of this message depends on the key. If the key is known to someone else, then that person can encrypt and decrypt the message. According to [4] The weakness of this algorithm is that both the sender of the message and the recipient of the message must have the same key, so the sender of the message must find a safer way to notify the key to the recipient of the message.

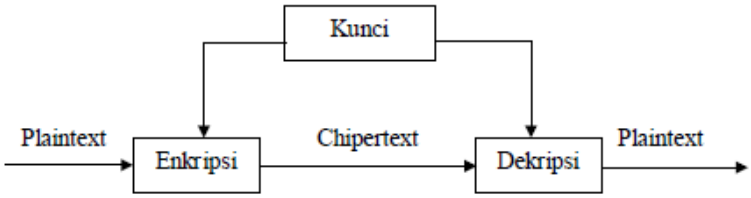

Figure 1. Symmetry algorithm

2.3. Advance Encryption Standard (AES) Algorithm

AES is a cryptographic algorithm named Rijndael that was designed by two cryptographers from Belgium, Vincent Rijmen and John Daemen. They were the winners of the Data Encryption Standard (DES) replacement cryptographic algorithm contest held by the National Institutes of Standards and Technology (NIST) in the United States on November 26, 2001. This Rijndael algorithm was later known as AES. On May 22, 2006 AES underwent a process of adjustment by NIST, then was appointed as a cryptographic algorithm measure [5]. According to [6] Rijndael has a key length of 128 to 256 bits with a 32-bit step. Because the AES Algorithm has three key choices namely type: 128, 192, and 256 and full support of the flexible Rijndael algorithm, AES is now known as AES-128, AES-192, AES-286.

2.4. Research Flowchart

The following is a diagram of the Encryption process diagram and a description of the Advance Encryption Standard (AES) Algorithm.

a. AES Algorithm Encryption Process Flowchart

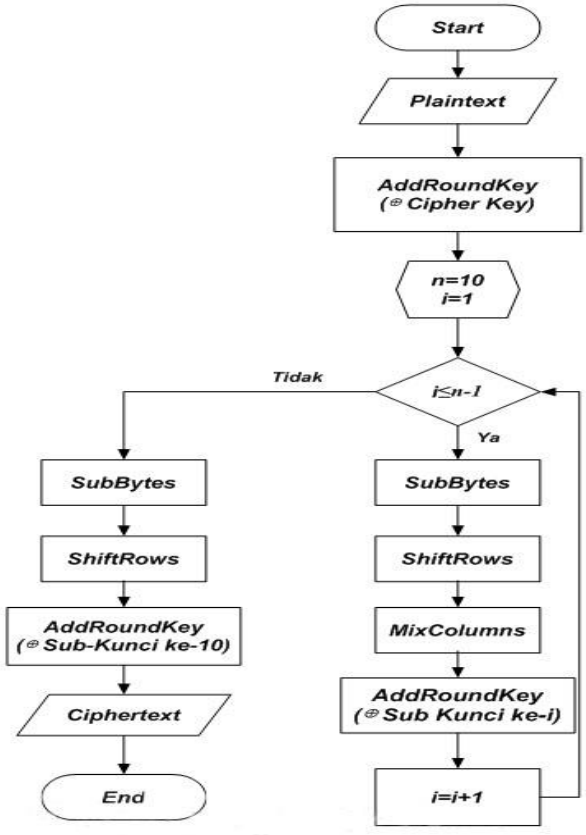

Figure 2. AES Algorithm Encryption Process Diagram

b. AES Algorithm Decryption Process Flowchart

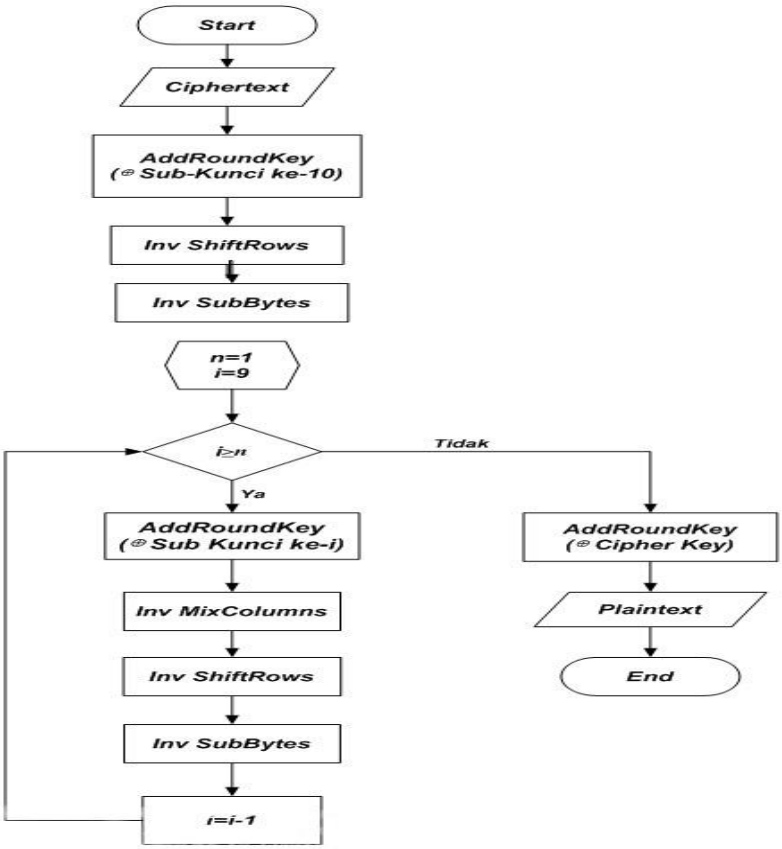

Figure 3. AES Algorithm Decryption Process Diagram

3. Results and Discussion

3.1. File Encryption

There are 2 main functions in this application, namely the encryption function and the decryption function, both of which we can access through the main menu, as shown below.

Figure 4. Main Menu Display

The process of encrypting files using this cryptographic program include: On the main menu there is a 'ENCRYPTION' button and when this button is clicked, a display like the following figure will appear.

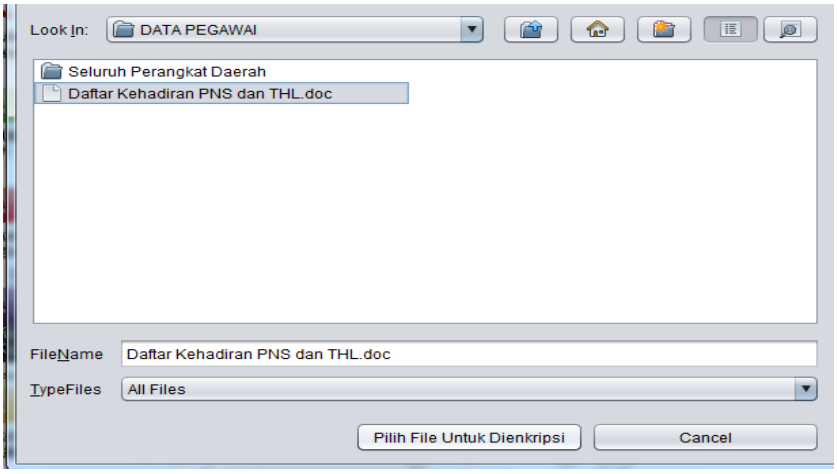

Figure 5. Display Select File to Encrypt

After selecting the file to be encrypted, then enter the menu list of files to be encrypted as shown below.

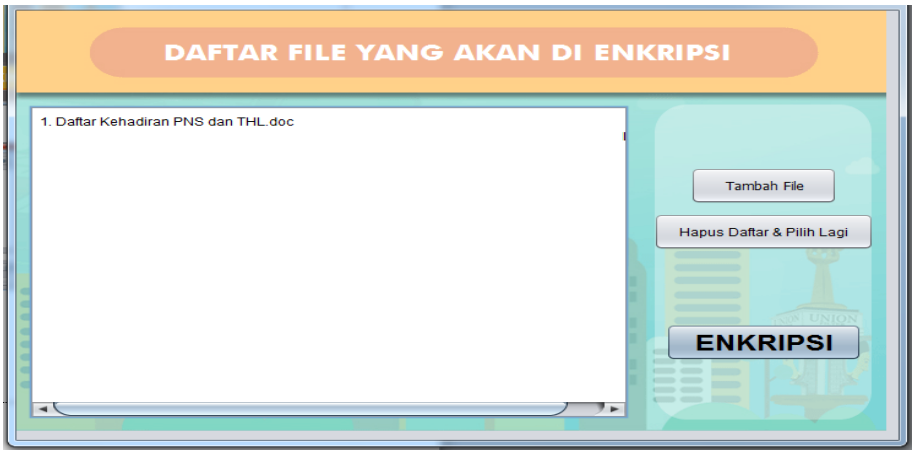

Figure 6. Display List Of Files To Be Encrypted

Press the 'ENKRIPSI' button and a menu will appear for inputting keys such as the following Figure.

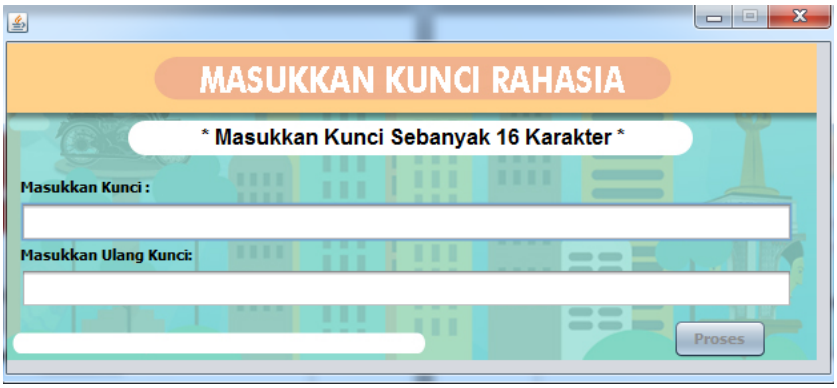

Figure 7. Display Enter Key

The key length entered must match the specified key length. For AES 128 bits long it means 16 bytes (16 characters). If the key lengths entered do not match, the program will issue the message "Key length must be 16 characters". And then we will be asked to re-

enter the same key for the verification process, if the key entered is different then the message "Two keys are different!" Will appear. After the two keys are the same, the encryption process will be performed and a menu will appear stating the encryption process was successful.

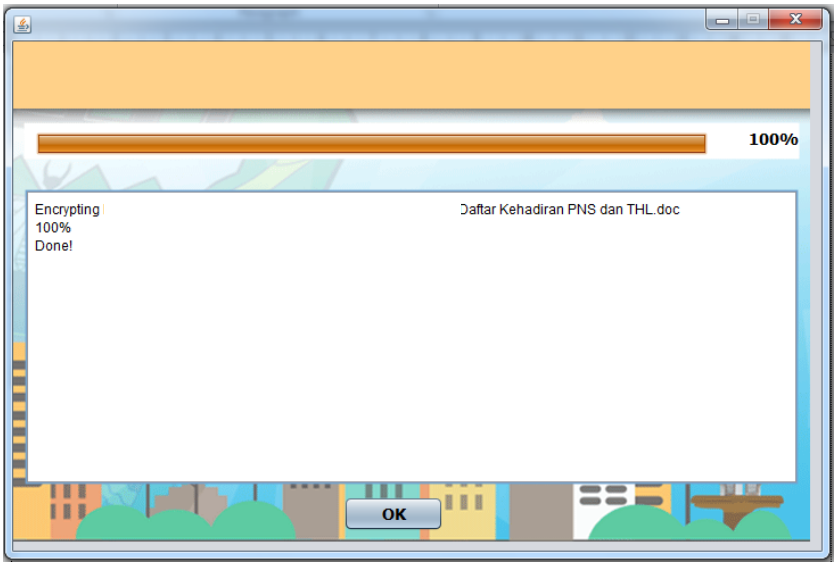

Figure 8. Display Encryption Process Successfully

3.2. File Decryption

The process of decrypting files using this cryptographic program is as follows: In the main menu there is a 'DEKRIPSI' option and when this menu is clicked, a display will appear as follows.

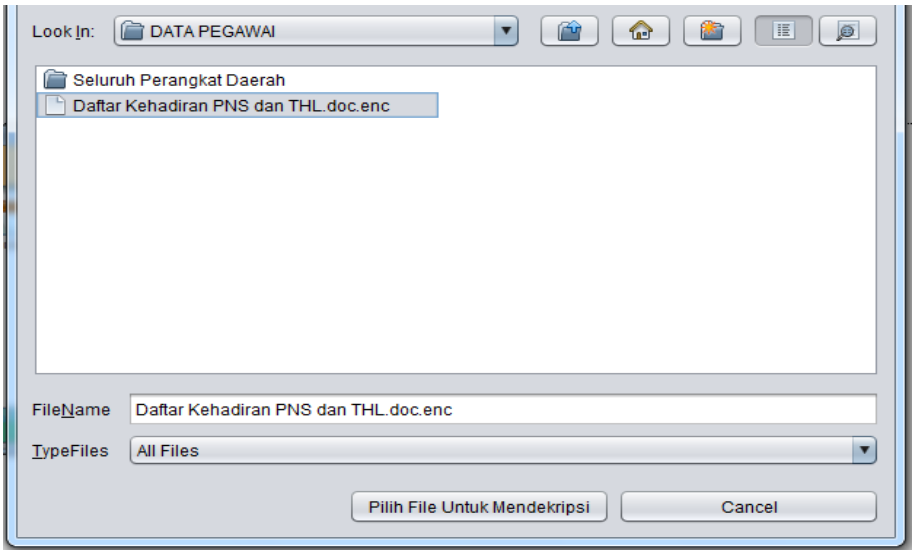

Figure 9. Display Select File to Decrypt

After selecting the file and pressing the select file button to decrypt, then enter the file list menu to be encrypted.

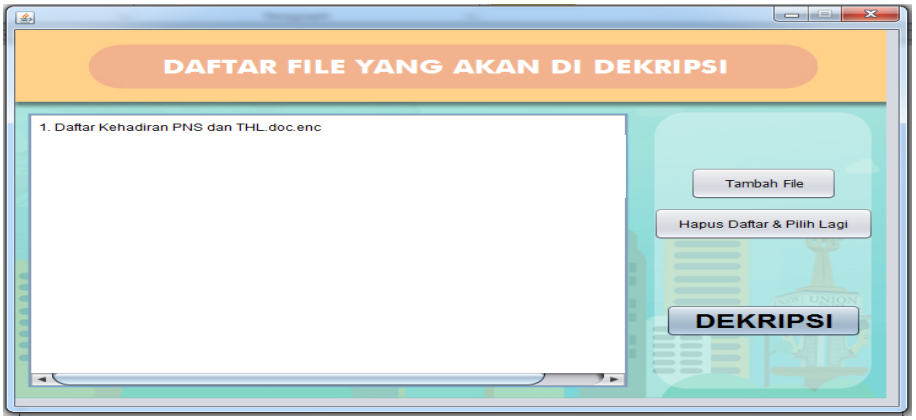

Figure 10. Display List of Files to be Decrypted

After pressing the 'DEKRIPSI' button, a form will appear to enter a key like the following Figure.

Figure 11. Display Enter Decryption Key

The key entered must match the key entered during the encryption process. If the key entered is different then the 'process' button cannot be clicked. After the keys match, the decryption process will be performed and a menu will appear stating the decryption process was successful.

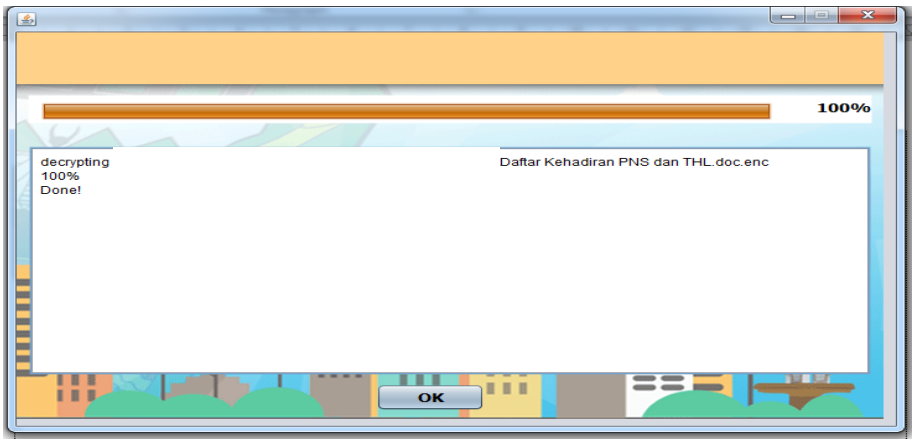

Figure 12. Display Decryption Process Successfully

If the keys do not match then the decryption process will not be performed and a menu appears stating the process failed.

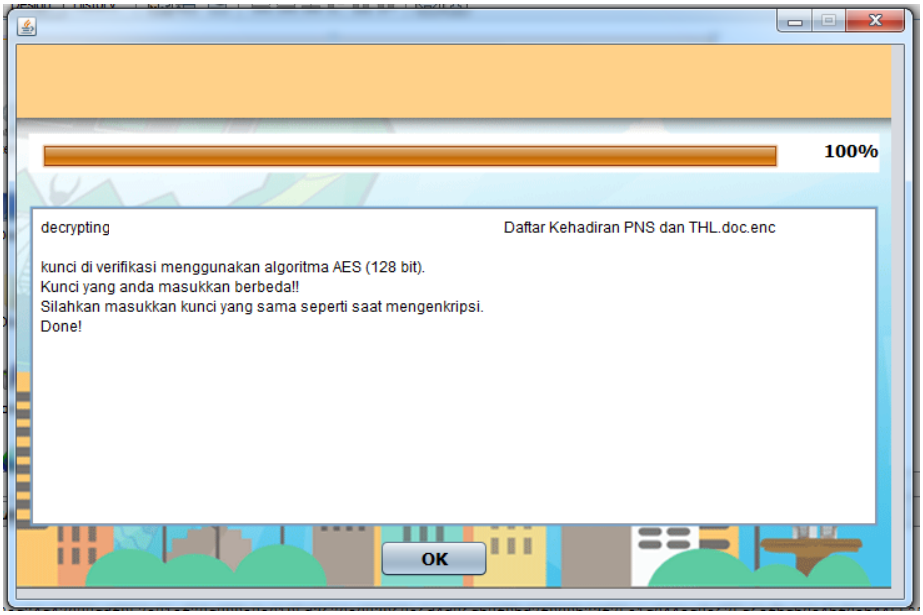

Figure 13. Display Decryption Process Failed

4. Conclusion

a. AES algorithm was successfully applied to encrypt files with various extensions such as: .doc, .xls, .ppt, .pdf, .jpg, .png. . MP4, and .Mp3 and can restore plaintext the same as the original file.
b. Data that is secured through the AES cryptographic method does not become damaged with the condition that no editing includes adding or deleting text, cropping, adding brightness, and other things that can change the encrypted data.

References

[1] A. Fauzi, Novriyenni, Y. Maulita, and A. M. H. Pardede, "Analisis Hybrid Cryptosystem Algoritma Algoritma Rsa Dan Triple Des," vol. 1, no. 2, pp. 36–44, 2017.
[2] D. Alyanto, "Pengenkripsian Data Rahasia," 2016.
[3] R. R. M, "Desain Dan Implementasi Aplikasi Sms (*Short Message Service*) Pada Android Menggunakan Algoritma AES," vol. 2, no. 2, pp. 3318–3326, 2015.
[4] D. Atika, "Implementasi Algoritma Spritz dan Algoritma RC4A Dalam Skema Three-Pass Protocol Untuk Pengamanan Data," 2018.
[5] D. Kurniawan, R. Afyenni, and R. Hidayat, "Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan Cloud Storage Berbasis Android," no. September, pp. 237–245, 2018.
[6] P. Arif, ahmad; Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (aes) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android," vol. 4, no. 1, 2016.

Authors

1st Author
Muhammad Rizal
Student of Universitas Sumatera Utara. Medan - Indonesia
rizaldal44@yahoo.com

2nd Author
Elviawaty Muisa Zamzami
Lecturer of Universitas Sumatera Utara. Medan - Indonesia
elvi_zamzami@usu.ac.id

3rd Author
Muhammad Zarlis
Lecturer of Universitas Sumatera Utara. Medan - Indonesia
m.zarlis@yahoo.com