An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm

Zaeniah
Academy of Computer Information Management Mataram
AMIKOM Mataram
Mataram, Indonesian

Bambang Eka Purnama
School of Information Management and Computer
"Nusa Mandiri", STMIK Nusa Mandiri
Jakarta, Indonesian

***Abstract*—Security of data in a computer is needed to protect critical data and information from other parties. One way to protect data is to apply the science of cryptography to perform data encryption. There are wide variety of algorithms used for encryption of data, this study used a one-time pad algorithm for encrypting data. Algorithm One Time Pad uses the same key in the encryption process and a decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. Therefore, analysis will be done for an application that implements a one-time pad algorithm for encrypting data. The application that implements the one time pad algorithm can help users to store data securely.**

Keywords—cryptography; algorithms One Time pad; encryption; Decryption

I. INTRODUCTION

Security of data in a computer is very important to protect the data from other parties that do not have the authority to determine the content of the data [1]. If the data has a very high value that has been stored in the computer and then opened by another party then it would be very detrimental.

One way to protect data is to password protect the data. But now to unlock the data that is already widely available password receipts of software that we can use. Another way that is used for encoding is to use the science of cryptography is to encrypt the data so that the data can not be read, deleted and changed by others[4].

Science of cryptography has been applied since ancient times to the present in accordance with technological developments. Various kinds of complex algorithm created as a tool to encrypt data one of which is the algorithm One Time Pad. The advantage of the one-time pad algorithm is to perform the encryption process and a decryption of each character plaintextnya use each character in the key. One Time Pad This algorithm uses the same key to encrypt and a decryption of the data. [1]

There are many algorithms are created to make applications in addition to data encryption algorithms One Time Pad one of which is the DES algorithm (Data Encryption Standard). DES is an algorithm that has the Feistel structure so that the structure of the encryption and the same decryption. But the DES key possessed only 56 bits that are considered unsafe[5]. Therefore, it will be created an application for data encryption as well as a decryption applying modern algorithm is an algorithm one time pad. One time pad algorithm is only used one time for one key encryption key then it will be destroyed and not used again to encrypt other data. In this study will be discussed regarding the encryption process and the decryption of data using one-time pad algorithm. This research is expected to be useful to be able to protect the data of those who do not have the authority to fill in the data so that data confidentiality is maintained properly.

II. REVIEW OF RELATED LITERATURE

Cryptography is derived from the Greek, crypto and Graphia. Crypto means confidential while Graphia means writing. In the term of the terminology, cryptography is the science and art that is used when a message is sent from one place to another to maintain the security of the message. Engineering data encryption (cryptography) is applied to the data and information, performed by encoding or hiding the original data. In cryptography, a message which will be kept secret called the plaintext and encrypted messages that have been called cipher text. In 1960s, the development of computers and communication systems has an impact on the demand of the parties - certain parties to provide various security services and protect information in digital form.

One-time pad (OTP) is a stream cipher encryption and decryption of one character each time. This algorithm was found in 1917 by Major Joseph Mauborgne as the improvement of the Vernam cipher to produce the perfect security. Mauborgne proposes the use of one-time pad (pad = paper notebooks) which contains the generation of random sequences of characters - a key character. To encrypt a message pad, it is simply used once (one-time), afterwards to encrypt messages, the pad that has been used cab be destroyed in order that no one can used it[12].

III. RESEARCH METHOD

The techniques of OTP algorithm uses a stream cipher manner in which the proceeds of the XOR cipher between plaintext bit and bit key encryption and XOR the hash value of the password.

For examples:

Samples are taken from a sentence "The World is wonderful" if it is represented into byte it would be "87 111 114 108 100 32 105 115 32 119 111 110 100 101 114 102 117 108 108 "(19 Byte without the quotes).

While each byte of data is read randomly generated bytes are used as keys, for example: "234 119 208 217 14 109 212 144 71 40 150 242 27 135 180 125 223 120 73 "(19 bytes without the quotes).

Taken a password for example: "ZAENIAH" after the one-way hash function obtained hash value is "3100" (4 bytes without the quotes).

The results of encryption are:

87 111 114 108 100 32 105 115 32 119 111 110 100 101 114 102 117 108 108
XOR 234 119 208 217 14 109 212 144 71 40 150 242 27 135 180 125 223 120 73
189 24 162 181 106 77 189 227 103 95 249 156 127 226 198 27 178 20 37
XOR 3100
3233 3076 3262 3241 3190 3153 3233 3327 3195 3139 3301 3200 3171 3326 3079 3246 3080 3129
(19 byte)

The results of encryption is "3233 3076 3262 3241 3190 3153 3233 3327 3195 3139 3301 3200 3171 3326 3079 3246 3080 3129" (19 bytes without the quotes).

The results of byte values obtained through XOR encryption between each plaintext byte and byte key value and the password hash value, then the creation of the software, which need to be considered in data decryption by using OTP algorithm that is a random number generator and key word.

For the random number generator, or in this case to obtain the encryption key, the process by means of a generator or random number generator (RNG) that generate a key from the keyboard and mouse input values and random noise. As for the management of this key, involved sub of the hash function is a one way hash operation performed in addition to the key XOR and AND already in the random pool.

Generally, the form of the algorithm or techniques of data encryption algorithm method One Time Pad (OTP) are as follows:

a) Open the application program encryption and decryption of data.

b) Enter the password program, then check it in the register. Whether the password is entered or entered in accordance with the password stored in the register.

- If the *passwords* do not match those stored in *registers* or no, the program will provide comments that *the password is* incorrect and automatically program cannot be used until a password is entered in accordance with the in- *registers.*
- If the *password* is entered or entered in accordance with the password that is stored in a register, then will be displayed program or *form* for the encryption and decryption of data.

c) In the Form encryption and decryption of data, Read Data / plaintext (data size, location of the data, the name data)

d) Create Key or key by using random (random noise and the input from the keyboard and mouse)

- Create output *key* (key) in the size of *the input* (data size / *plaintext)*
- Fill each *byte* with a random value (the value of which has been obtained through the hash between *random noise* and the *keyboard and mouse)*
- The key test, good or not
- Compress the key *(key),* the key here will be compressed, if the key size after compression> = the original data, the key is feasible to be used, otherwise if the key size after being compressed <of the original data, the key is not feasible to be used. As for some of the methods used to compress or calculate *the frequency of* occurrence of a character such method *Huffman, RLE, chi-square* etc.

e) Read per byte of data / plaintext and Key is already in Hash

f) Perform XOR operation on the data / plaintext with the key (key) which has been obtained and in XOR again with the hash key.

g) Finish (data encrypted / ciphertext).

While the algorithm to decrypt the encrypted data / ciphertext it is, basically the same as the encryption process, the general form of the algorithm is:

a) Open application program encryption and decryption of data.

b) Enter the password program, then check it in the register. Whether the password is entered or entered in accordance with the password stored in the register.

- If the *passwords* do not match those stored in *registers* or no, the program will provide comments that *the password is* incorrect and automatically program can not be used until *a password* is entered in accordance with the in- *registers.*
- If the password is entered or entered in accordance with the password that is stored in a *register,* then will be displayed program or *form* for the encryption and decryption of data.

c) In Form encryption and decryption of data, Read or download the encrypted data (ciphertext)

d) Take Key / key (key = key encryption)

e) Read per byte of data between the ciphertext with the key / lock

f) Perform XOR operation between the ciphertext with a hash key (hash value of the password) and XOR again with data key (encryption key).

g) Finish (data decrypted or original data / plaintext)

IV. Result and Discussion

The results of this study after testing the application that implements the one-time pad algorithm, we discussed password making when the application was first used until the encryption process and a decryption of the data and results. For

the first time use, it will displayed following message like figure 1.

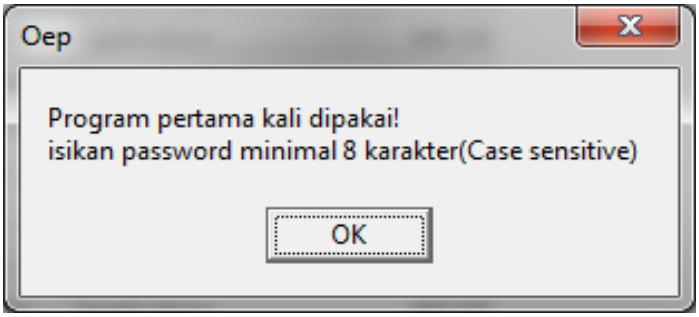

Fig. 1. Messages when the application is first used

To create a password, fill in the spaces at least 8 characters that consist of numbers and letters. Enter the password and then click the button confirm the entered password is stored into the register. If the password entered is correct, then the password is already registered in the register. If the password is wrong, it must be registered on the registration. The first Password is made is the first security level of the application as shown in Figure 2.

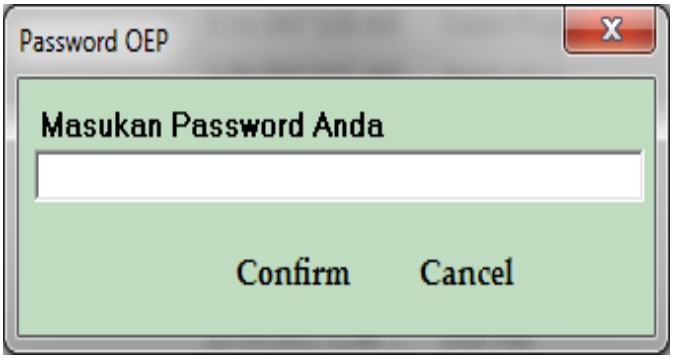

Fig. 2. The form of charging password

Data encryption process is done by taking a file that will then enter the password encryption to secure the data that has been encrypted files. Meanwhile, to make the decryption of the data is done by taking the files that have been encrypted using OTP app, enter the password that was used to encrypt the data, then grab the key that has been made time encryption key using the pick button then described.

A. A Test result on document formats doc

The encryption process is carried out in doc format documents with long file size of 835KB with the encryption process 31 milliseconds and the speed of the process is 27 581 bytes / mDtk as shown in Figure 3.

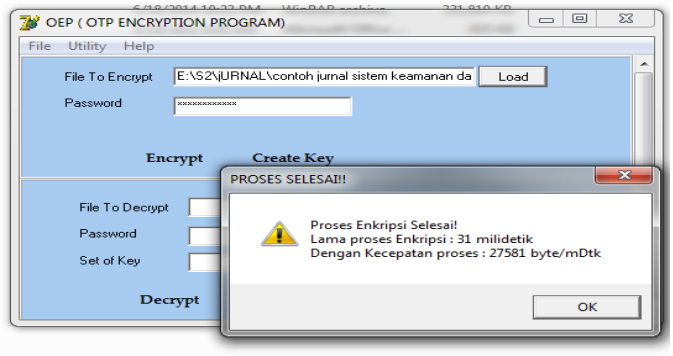

Fig. 3. Encryption processes with the doc format

After performing the encryption process, the application will change the original file of the document. Results encryption of documents with the doc format can be seen in Figure 4.

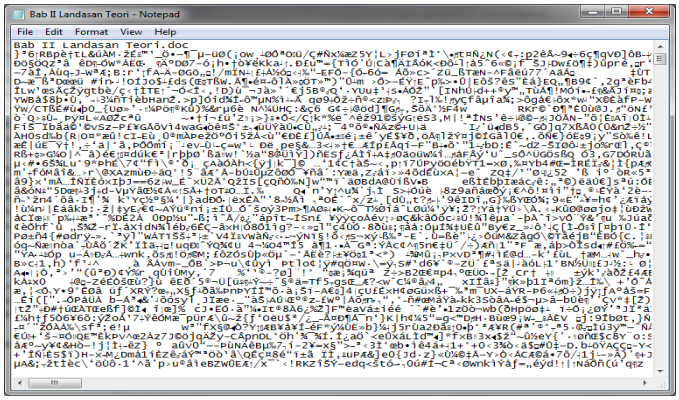

Fig. 4. Encrypted files with .doc format

To open a document that has been encrypted is then encrypted file must first be described in advanced. The process of Decryption file to doc format can be seen in Figure.5. The decryption of the process is done with a long process that is 16 milliseconds to speed the process 53 456 bytes / mDtk with 835KB file size.

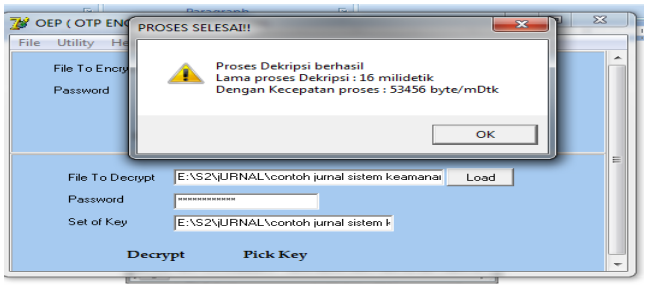

Fig. 5. Process decryption file to doc format

The decryption of the file to doc format can be seen in Figure 6.

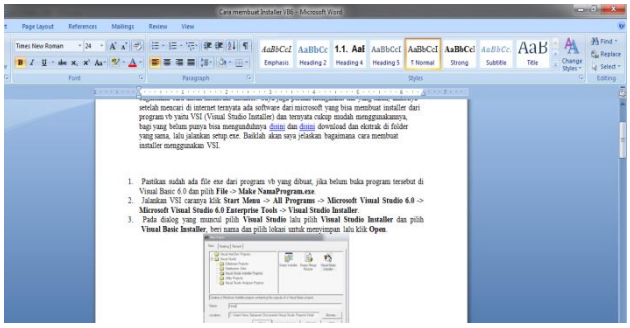

Fig. 6. The decryption of the file format doc

B. *Excel file encryption process*

The encryption process is carried out in a excel file with a file size of 256 KB to 16 milliseconds longer the encryption process and speed of 16352 bytes / mDtk as terliahat in Figure 7

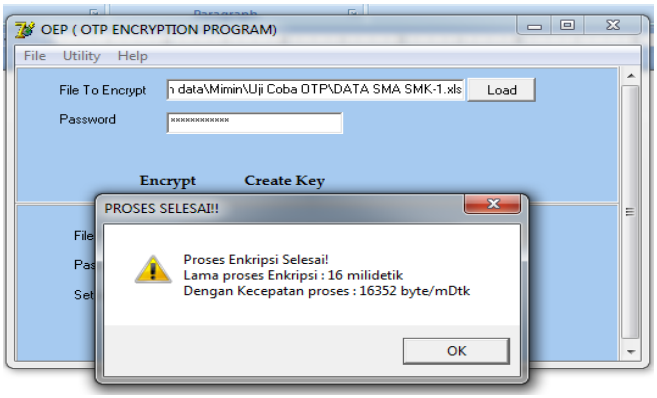

Fig. 7. Excel file encryption process

The Result of excel files stored encryption can be seen in Figure 8

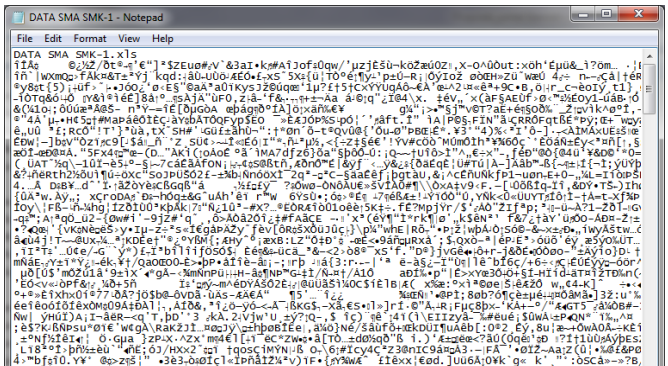

Fig. 8. Results excel file encryption

Process file decryption is conducted by the time the process is 16 milliseconds and the speed of the process is 16 368 bytes / mDtk with a 256 KB big file as shown in Figure 9.

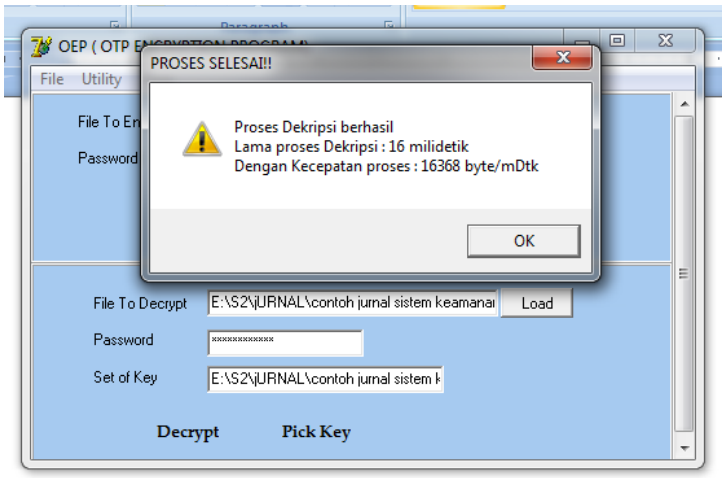

Fig. 9. Process decryptions excel file

The Result of excel file decryption can be seen in Figure 10

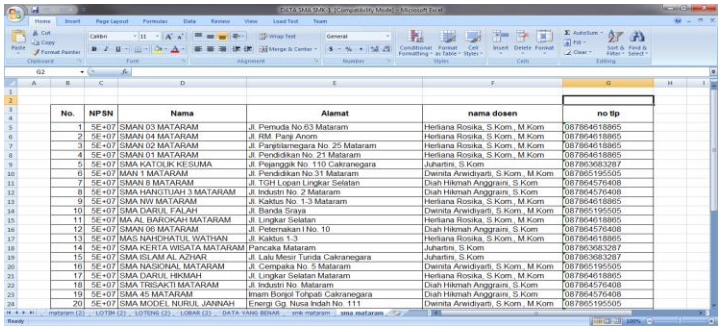

Fig. 10. Results excel file decryption

C. *A Test on an image file*

Encryption process of image files with file size 6715 KB, 125 milliseconds longer the encryption process with process speed 55 002 bytes / mDtk can be seen in Figure 11.

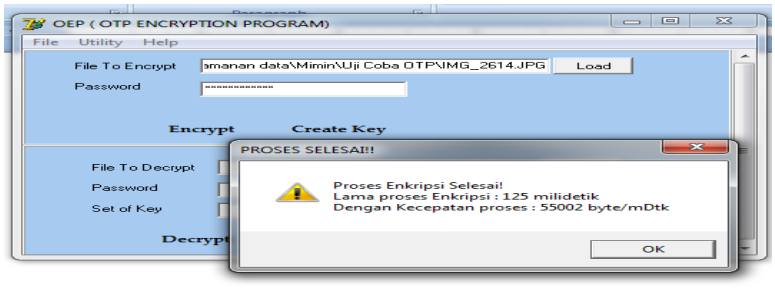

Fig. 11. Image file encryption process

Encryption results of image files can be seen in Figure 12

Fig. 12. Result image file encryption

Decryption process of image files can be seen in Figure 13 with 125 milliseconds long process decryption as well as the speed of 55 004 bytes / mDtk

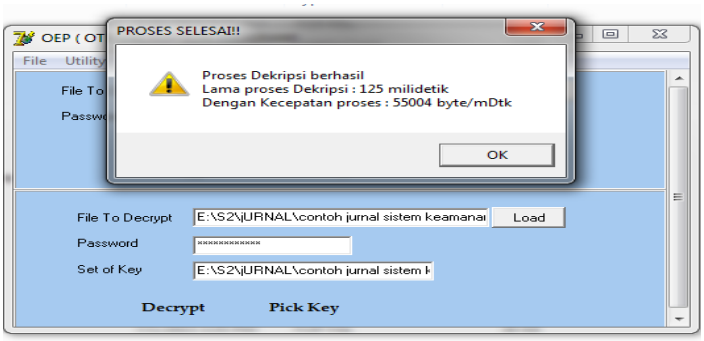

Fig. 13. The process decryption file image

The Results of Decryption on image files can be seen in Figure 14

Fig. 14. The decryption of the image file

D. A Test on a PDF file

The encryption process is performed on a file with a size of 1786 KB with the old encryption process 62 milliseconds to speed the process 29 489 bytes / mDtk as shown in figure 4.14.

Fig. 15. Pdf file encryption process

Encrypted file after the encryption process is shown in Figure 16

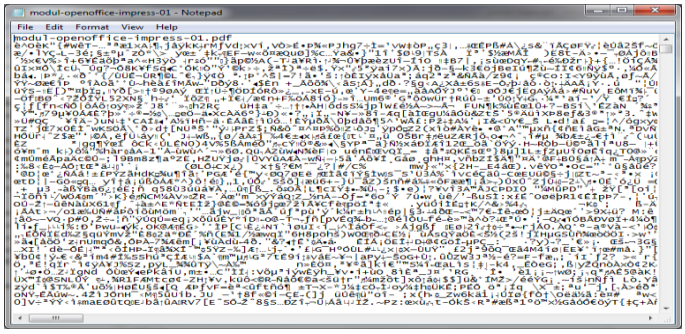

Fig. 16. The results of pdf file encryption

Decryption process lasted 62 milliseconds and with speed process 29 493 bytes / mDtk as shown in figure 17.

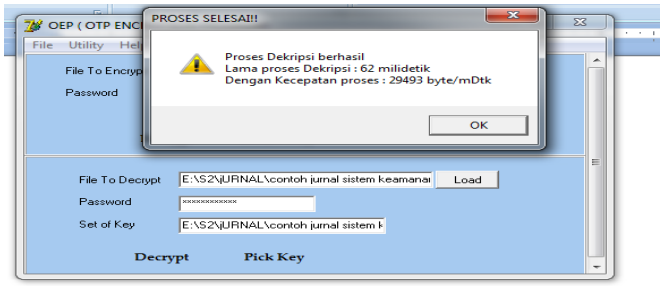

Fig. 17. Process decryption pdf file

The result decryption that is stored can be seen in Figure 18

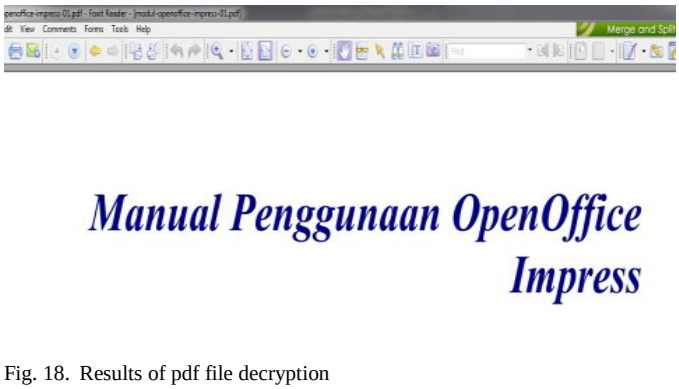

Fig. 18. Results of pdf file decryption

Experiment has been conducted on various types of file formats such as doc, pdf, ppt, and image file formats. Tests were also conducted on various types of file size.

TABLE I. File Size and Time Process

File Size	Time Process
1 KB	16 Milidetik
835 KB	31 Milidetik
1599KB	62 Milidetik
6715 KB	125Milidetik

From Table 1, we can see some test results influence the file size of the processing time required, the time required performing the encryption or decryption process also depends on the speed of the computer used. Meanwhile, to make the process of file encryption and file decryption does not change the size of the file.

From the test results that have been done, it can be seen the advantages of using the application of algorithm on One Time Pad

- It helps the users to store data securely because the password used to encrypt the file must be the same as the password used to decrypt the file so that the right to open the files you have encrypted the only person who has the right to open it.
- Data security when it is encrypted is quite reliable because it uses the algorithm is the result of one-time pad encryption in the fox into cipher text that is very different from the original file.
- By using this application, it can encrypt and describe the various types of file formats such as doc, pdf, ppt and image files.

While the limitations of the application that implements the algorithm one time pad is between the length of a key must be equal to the length of plaintext (original message). This thing can cause the application to run less efficiently because of a long encryption on a long message.

V. Conclusions and Suggestions

From various experiments performed on One time pad algorithm implementation, it can be concluded that this application can protect data properly. Applications that implement the one time pad algorithm can help the users to save data and information from those who do not have the authority. This application can encrypt and decrypt the data in various file formats and file size does not change when performing the encryption process and a decryption of the document.

Developing of this application can increase the security level of the encrypted document and create more interesting design.

References

[1] S. P. Agustanti, "Pengamanan Kunci Enkripsi One-Time Pad (Otp) Menggunakan Enkripsi Rsa", Vol. 7, No. 1, pp. 95-100, 2010.

[2] I. R. Widiasari, "Combining Advanced Encryption Standard (AES) and One Time Pad (OTP) Encryption for Data Security", Vol. 57, No. 20, pp. 1-8, 2012.

[3] M. A. Muda, M, Komarudin and Y. Susanty, "Rancang Bangun Sistem Enkripsi Sebagai Security Komunikasi Handie-Talkie Menggunakan Mikrokontroler Avr Seri", Vol. 1, No. 1, pp. 25-37, 2007.

[4] R. Primartha, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)", Vol. 3, No. 2, 2011.

[5] Y. Kurniawan, A. S. Ahmad, M. S. Mardiyanto, I. Supriana dan S. Sutikno, "Analisis Sandi Diferensial terhadap AES, DES dan AE1", Vol. 38 A, No. 1, pp. 73-88. 2006.

[6] E. Sitohang, "Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook dengan Algoritma DES", Vol. 5, No. 3, 2013.

[7] M. Sholeh dan J. V. Hamokwarong, "Aplikasi Kriptografi dengan Metode Vernam Cipher dan Metode Permutasi Biner", Vol. 7, No. 2, pp. 8-13, 2011.

[8] D. Wirdasari, "Prinsip Kerja Kriptografi Dalam Mengamankan Informasi", Vol. 5, No. 2, 2008.

[9] M. Fairuzabadi, "Implementasi Kriptografi Klasik Menggunakan Borland Delphi", Vol. 4, No. 2, pp. 65-78, 2010.

[10] Inayatullah, "Analisis Penerapan Algoritma MD 5 Untuk Pengamanan Password", Vol. 3, No. 3, 2007.

[11] F. W. Nurwiyati dan I. Yatini B., "Enkripsi Dekripsi Data Menggunakan Metode Stream dan Vigenere Cipher", Vol. 3, No. 23, 2013.

[12] R. Munir, "Algoritma Enkripsi Citra dengan Pseudo One-Time Pad yang Menggunakan Sistem Chaos", 2011.