JurnalMantik
Volume 4, Number 3, Nov 2020, pp. 2348-2353 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik

Application of File Encryption and Decryption Using One Time Pad Algorithm

Muhammad Syahputra Novelan

Sistem Komputer, Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi Medan, Jl. Jenderal Gatot Subroto, KM 4,5Sei Sikambing 20122 Medan

Email : putranovelan@dosen.pancabudi.ac.id

ARTICLEINFO

Article history:
Received: 28/10/2020
Revised: 20/11/2020
Accepted: 30/11/2020

Keywords:
Kriptografi,OTP,Enkripsi, Dekripsi,Chipertext

ABSTRACT

In maintaining a system security, it is very important to pay attention to that, namely an authentication process. This process is carried out in order to ensure that users who access data or information are users who have the right and authority. In authentication, there are several methods, one of which is using data encryption techniques, namely cryptography. Cryptography is implemented in data and information by coding or hiding the original data so that only certain parts have a key that can access the data or information. This research will apply the One Time Pad (OTP) Algorithm based on android which includes data encryption and decryption which will be designed using Android Studio to carry out encryption of stored data or information. The data will be in the form of ciphertext so that the user gets an access key for the data or information. In making this application, it is hoped that it will be useful in maintaining data security and confidentiality.

1. Introduction

Technological advances in the field of computers allow thousands of people and computers around the world to connect in a virtual world known as cyberspace or the Internet. Likewise hundreds of organizations such as companies, state institutions, financial institutions, military and so on. But these technological advances are always followed by the downside of the technology itself. One of them is the vulnerability of data security, which raises challenges and demands for the availability of a data security system that is as sophisticated as advances in computer technology itself..

Nowadays, the effective security of a system is indispensable for daily business activities. A secure system can provide a high level of trust to users so that it can add value and usability to the system itself. Users will feel comfortable and safe when dealing with a system that can secure user data from attackers.

There are several ways to secure data through a channel, one of which is cryptography. In cryptography, highly confidential data will be disguised in such a way that even if the data can be read it cannot be understood by unauthorized parties. The data that will be sent and have not been encrypted is known as the term plaintext, and after being disguised by an encoding method, this plaintext will turn into ciphertext. One of the algorithms that can secure the data that the author discussed is the One Time Pad Algorithm, while the advantages of OTP are that it is easy to implement but difficult to penetrate.

2. Method

In Figure shown. Stage 1 is planning where step 1 identifies needs in the review literature. As determining the objectives of the literature review research, look for similar literature research on lecture schedulers, which have been discussed in the Introduction section. Step 2 compile an SLR protocol that contains a plan of procedures and methods selected in the study. Stage 2 is the implementation of the proceduresandmethodsspecifiedintheSLRprotocol,andPhase3istocreatereportontheresultsofthe Phase 1 and 2 research.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

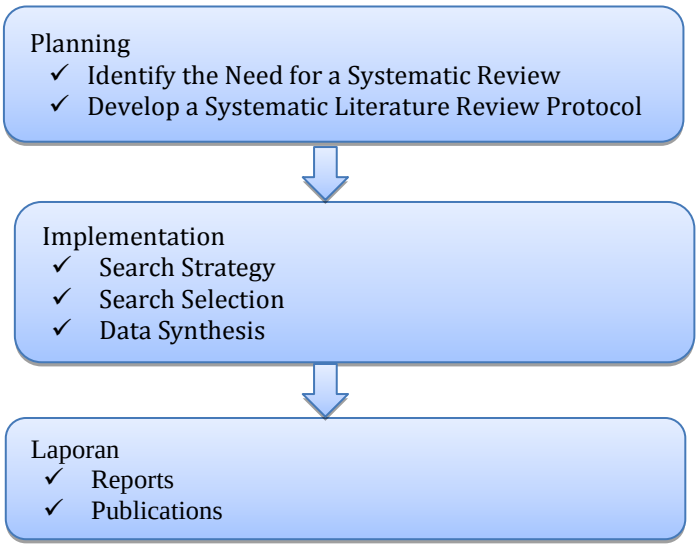

Fig1. SLR stages

In Figure shown. Stage 1 is planning where step 1 identifies needs in the review literature. As determining the objectives of the literature review research, look for similar literature research on lecture schedulers, which have been discussed in the Introduction section. Step 2 compile an SLR protocol that contains a plan of procedures and methods selected in the study. Stage 2 is the implementation of the procedures and methods specified in the SLR protocol, and Phase 3 is to create a report on the results of the Phase 1 and 2 researc.

3. Results and Discussion

A. Vernam Cipher Encryption Process

Data encryption is the initial part of the data security process. In this encryption process, the original data will be randomized with a predetermined algorithm, while the encryption process in Vernam Chiper can be done using the following formula:

C(i) = P(i) XOR K(i)**.....** **.....(1)**

In this case :

C = Chiper Text
P = Plain Text
K = Key
I = Character Index

B. One Time Pad Algorithm Encryption Process

Encryption is used to encode data or information so that it cannot be read by unauthorized people. With encryption, our data is encrypted (encrypted) using a key. To open (decrypt) the data, a key is also used which can be the same as the key to encrypt (private key) or with a different key (public key).

The security of encryption depends on several factors. First, the encryption algorithm must be strong enough so that it is difficult to decrypt cipher text based on the cipher text. Furthermore, the security of the encryption algorithm relies on the confidentiality of the key not the algorithm, that is, on the assumption that it is impractical to deycrypt information on the basis of cipher text and knowledge of the decryption or encryption algorithm. Or in other words, we do not need to maintain the confidentiality of the algorithm but rather the secret of the key. This image is used to explain the encryption process in the form of a flowchart whose image is as shown below.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

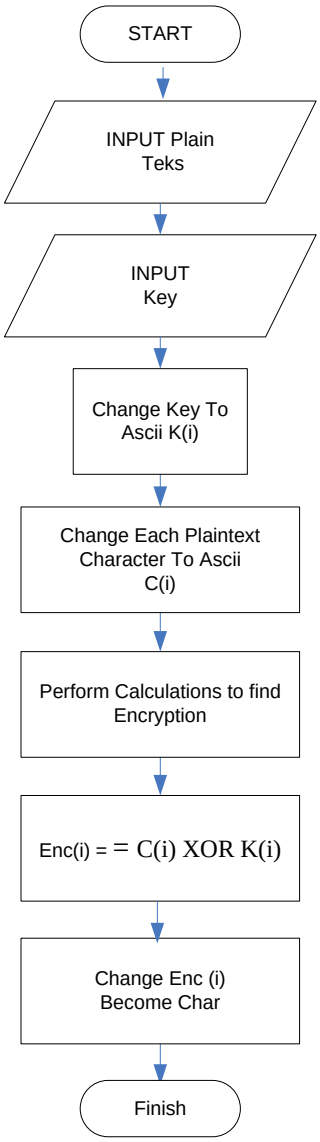

Fig 2. One Time Pad Encryption Process

Information :
Input Plain Text, Key
Take the Number of Key Characters
Change Key To Ascii
Change Every Plain Text Character To Ascii
Perform calculations to find encryption using the formula Enc (i) = = C (i) XOR K (i)
Change Enc (i) to Char
Finish

C. One Time Pad Algorithm Decryption Process

Decryption is used to return data or information so that it can be read by the authorized person. With decryption, the data is returned to its original form so that it can be read properly, while the encryption flowchar can be seen as shown below.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

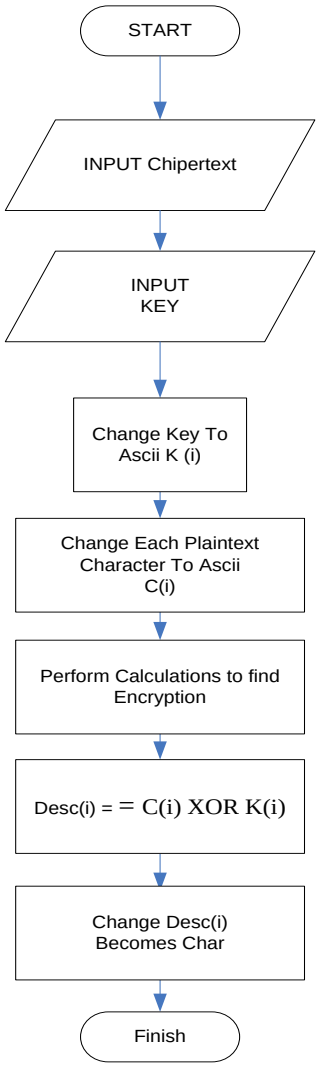

Fig 3. One Time Pad Decryption Process

Keterangan :
Input Chiper Text, Key
Take the Number of Key Characters
Change Key To Ascii
Change Every Text Chiper Character To Ascii
Perform calculations to find a description using the formula Desc (i) = = C (i) XOR K (i)
Change Desc (i) to Char
Finish

In writing this thesis, the Vernam Cipher algorithm analysis will be discussed. For example, when sending a file to someone, it must be confidential. In this discussion, Vernam Cipher will encrypt the files so that they are safe. Below will explain an example of using the Vernam Cipher algorithm.

For example: A "**JALAN**" will be encrypted with the key "**BINJAI**" with the following calculations, it will get the following results:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Table 1
Ascii Messages

Plain Teks	Ascii
J	74
A	65
L	76
A	65
N	78

Table 2
Key Ascii

Teks Kunci	Ascii
B	66
I	73
N	78
J	74
E	69

From the table above, it can be concluded as follows :

Table 3
Encryption Calculations

Pesan	**74**	**65**	**76**	**65**	**78**
Kunci	**66**	**73**	**78**	**74**	**69**
Pesan XOR Kunci	**8**	**8**	**2**	**9**	**9**
Karakter	**BS**	**BS**	**STX**	**HT**	**HT**

Then it will produce an encryption character : **US – DLE – TAB – NULL–ACK**
To describe, the reverse process is carried out, namely.\

Table 4
Decryption Process

Plain Teks/Char	**Desimal**
BS	8
BS	8
STX	2
HT	9
HT	9

Table 5
Key Ascii

Teks Kunci	Desimal
B	66
I	73
N	78
J	74
E	69

Table 6
Descriptions Calculation Results

Message	**8**	**8**	**2**	**9**	**9**
Key	**66**	**73**	**78**	**74**	**69**
Key XOR message	**74**	**65**	**76**	**65**	**78**
Character	**J**	**A**	**L**	**A**	**N**

From the table above, it can be concluded as follows:
XOR Key Encryption Message : **74 - 65 – 76 – 65 – 78**
Then the decimal number is converted back to liquid form, so the result is as below:
= **J - A - L - A - N**

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

4. Conclusion

Based on the results of the discussion above, the researchers took several conclusions as follows :

a. Applications designed using the Eclipse program and using the One Time Pad algorithm
b. This application only performs encryption and decryption of files.
c. From the results of the encryption in the form of a file (ciphertext) will be decrypted using the application designed.

6. References

[1] G. Leander et al., "New Lightweight DES Variants," Proc. Fast Software Encryption (FSE 07), LNCS 4593, Springer-Verlag, 2007, pp. 196-210

[2] 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

[3] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES Implementation on a Grain of Sand," IEE Proc, vol. 152, no. 1, Oct. 2005, pp. 13-20.

[4] Novelan, M. S., Husein, A. M., Harahap, M., &Aisyah, S. (2018). SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. Journal of Physics: Conference Series, 1007(1), 12037. Retrieved from http://stacks.iop.org/1742- 6596/1007/i=1/a=012037

[5] 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

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