International Journal of Research and Review
Vol. 10; Issue: 2; February 2023
Website: www.ijrrjournal.com
Review Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Data Security Techniques Using Square Block Keys in Text Format

Andysah Putera Utama Siahaan

Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

DOI: https://doi.org/10.52403/ijrr.20230244

ABSTRACT

The text format is a character format that can be read directly with any software. This format is used in sending data to facilitate sending and speed up sending data to message recipients. The text format is the message storage format with he least security because it can be directly read by the person who gets the message. The author wants to build a cryptographic application that can secure text formats using the character transposition technique. Character transposition is used based on the formation of a square matrix which is used as a key in the encryption and decryption process. The size of the matrix used is 4 x 4. The results of the study found that the text format was successfully transformed into ciphertext so as to avoid the possibility of data theft.

Keywords: square, security, block, encryption

INTRODUCTION

Data security is a very important action to take to protect information from being spread to irresponsible people [1]. Data is a collection of information that is owned to be given to the recipient [2]. Data transmission is generally done using a text format. This format is a standard format that has a plaintext form where the text can be directly read using any application. Sending in text format is done to facilitate delivery and not experience problems when the recipient performs the decryption process. But basically, this text format has weaknesses that can result in losses.

Sending messages using text format has weaknesses. The weakness of the text format is that the message can be read directly because it only uses letters, numbers and some punctuation symbol characters so that this message is very easy to be misused by others. The text format also has a moderate number of characters, or about 26 uppercase alphabetic characters, 26 lowercase alphabetical characters, 10 numeric characters and a few punctuation characters. Sending messages in text format requires cryptographic techniques so that messages are not easily disassembled.

The author wants to provide security for sending text formats by using a transposition technique where the characters in the message in the text format will be arranged using a square matrix and each character in the matrix will experience a character exchange with other characters. This matrix is a form of the key that will be used in the process of encrypting and decrypting text messages. The matrix size used in this study is 4 x 4 so that each message block will consist of only 16 characters. If more than a new message block will be created with the same key. The results of the research will get a ciphertext that has undergone character transformation from plaintext.

THEORIES

Encryption

Encryption is changing the original message or plaintext into an unreadable message or ciphertext. This process is carried out using cryptographic techniques that involve certain algorithms in the transformation process [3].

Decryption

Decryption is the conversion of an unreadable message or ciphertext into a readable message or plaintext. This process is also carried out based on the cryptographic technique used during the previous encryption process. The algorithm used must be the same as the algorithm during the encryption process [4].

Transposition

Transposition is a change in the location of a character in a character pattern arrangement. In this technique, the characters in the text block still have the same number and characters but the arrangement of the characters will be randomized or replaced. This technique rearranges the sequence of characters in the text. Another name for this technique is permutation because rearranging each character in the text is the same as permuting characters in the text [5].

METHODS

Research Stages

This study uses several stages consisting of steps used so that the research target is achieved. The stages of the research can be seen in Figure 1.

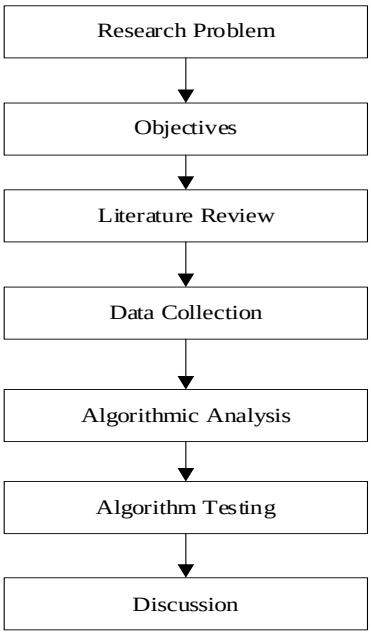

Figure 1. Research Stages

There are several stages carried out in this research which are described as follows:

1. Research Problem
   The formulation of the problem is determined by the author based on the problems that occur in sending messages with text format. The formulation of the problem is how to secure the text format when sending messages.
2. Objectives
   Setting goals is necessary in order to solve problems that occur in sending messages in text format.
3. Literature Review
   Literature review is collecting the information needed for system. The study refers to the science of cryptography, especially transposition techniques.
4. Data Collection
   Data collection originates from messages taken in text format. This message will be used in the character transposition process for encryption and decryption.
5. Algorithm analysis
   Algorithm analysis to see the performance of the transposition process on encryption and decryption. The analysis also aims to see the security of the text format after being encrypted.
6. Algorithm Testing
   Tests were carried out to prove the correctness of the techniques used in this study.
7. Discussion
   The discussion is carried out to see the results of the character transposition process in encryption and decryption using the square matrix block key.

Flowchart

This study has two flowcharts that are used to view the character transposition flow for the encryption and decryption process. The encryption flowchart explains how a text message will be encrypted. The encryption flowchart can be seen in Figure 2.

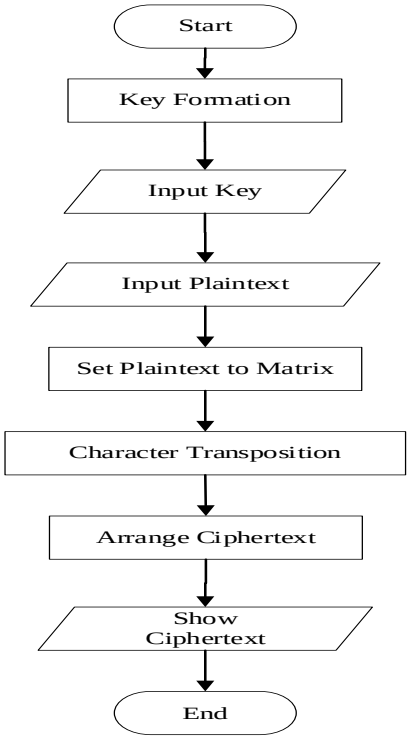

Figure 2. Flowchart of Encryption

Decryption flowchart is a step used to return ciphertext to plaintext. The decryption flowchart can be seen in Figure 3.

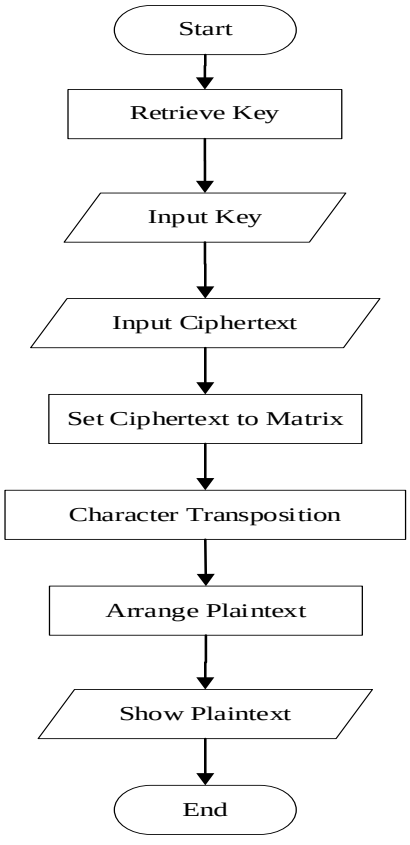

Figure 3. Flowchart of Decryption

System planning

System design was carried out to see how cryptographic techniques were arranged in this study. There are several processes for encrypting and decrypting the system to be built which consist of:

1. Formation of a square matrix block key
2. The process of placing characters in blocks that have been formed
3. Changing the layout of the characters in the message text format according to the key structure pattern formed.

Key Generation Process

The key is the sequence layout used in the character transposition process for encryption and decryption. The key formation process is carried out by forming a matrix with a size of 4 x 4 as follows:

Ordered Index			
a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

Random Index			
b	a	e	f
i	c	j	m
h	o	d	n
l	g	16	k

The ordered index is the ordered character arrangement of the keys in the original message. The key will be exchanged arbitrarily to produce a new random key position. Random index is a text format character arrangement that has undergone a transposition of characters that are exchanged randomly based on the serial number in the initial matrix.

Encryption Process

The process of encrypting or encoding messages is carried out in several stages which are described as follows:

1. Enter the text message to be encrypted.
2. Determine the key matrix.
3. Arrange the messages on the key matrix
4. Transpose the characters in the original message according to the numbering in the key matrix.

Decryption Process

The process of decrypting or returning messages is carried out in several stages which are described as follows:

1. Enter the secret message to be decrypted.
2. Take the key matrix.
3. Arrange the encrypted characters on the key matrix.
4. Transpose the characters in the encrypted message according to the number on the key matrix.

RESULT AND DISCUSSION

In this section, an overall description of the use of the key block for the encryption and decryption of text messages will be explained. The cryptographic process in this study consists of 43 parts, including:

1. Determination of Plaintext
2. Key Generation
3. Encryption
4. Decryption

Plaintext Determination

The plaintext used in this experiment is a sentence of 32 characters which can be converted into 2 blocks. Each block consists of 16 characters, where the number is obtained based on a 4 x 4 calculation. The plaintext used in this experiment is "*A simple fast characters counter*". This plaintext will be formed into a matrix as follows.

Plaintext 1			
A	_	s	i
m	p	l	e
_	f	a	s
t	_	c	h
Plaintext 2			
a	r	a	c
t	e	r	s
_	c	o	u
n	t	e	r

Key Formation

Key generation in this experiment was carried out by randomly arranging key positions to random index so that a key table was obtained as shown below.

Random Index			
6	9	1	4
5	13	11	12
3	7	10	0
2	8	14	15

The key will be used to transform plaintext characters according to the position of the character designated by the key.

Encryption

Encryption is done by transposing each plaintext block with a random key. Each character in plaintext has an index number starting from 0 to 15. This index indicates that there are 16 characters for each plaintext block. The encryption process can be seen in the following section.

Plaintext 1			
A^0	$\_^1$	s^2	i^3
m^4	p^5	l^6	e^7
$\_^8$	f^9	a^{10}	s^{11}
t^{12}	$\_^{13}$	c^{14}	h^{15}
Random Index			
6	9	1	4
5	13	11	12
3	7	10	0
2	8	14	15
Ciphertext 1			
l^6	f^9	$\_^1$	m^4
p^5	$\_^{13}$	s^{11}	t^{12}
i^3	e^7	a^{10}	A^0
s^2	$\_^8$	c^{14}	h^{15}

The ciphertext results are obtained from the characters taken from the plaintext based on the index number in the random key. The second block of plaintext also experiences the same thing. The plaintext will be randomized using the specified key.

Plaintext 2			
a^0	r^1	a^2	c^3
t^4	e^5	r^6	s^7
$\_^8$	c^9	o^{10}	u^{11}
n^{12}	t^{13}	e^{14}	r^{15}
Random Index			
6	9	1	4
5	13	11	12
3	7	10	0
2	8	14	15
Ciphertext 2			
r^6	c^9	r^1	t^4
e^5	t^{13}	u^{11}	n^{12}
c^3	s^7	o^{10}	a^0
a^2	$\_^8$	e^{14}	r^{15}

After both plaintext blocks have been worked on, the ciphertext result is "*lf mp*

stieaAs chrcrtetuncsoaa er".

Decryption

Decryption is done by returning characters that have occupied new positions in the ciphertext using random keys so that the character positions return to their original position as in the plaintext. The following is a complete description of the decryption process.

Ciphertext 1			
l^{0}	f^{1}	$\_^{2}$	m^{3}
p^{4}	$\_^{5}$	s^{6}	t^{7}
i^{8}	e^{9}	a^{10}	A^{11}
s^{12}	$\_^{13}$	c^{14}	h^{15}
Random Index			
6	9	1	4
5	13	11	12
3	7	10	0
2	8	14	15
Ciphertext 1			
A^{6}	$\_^{9}$	s^{1}	i^{4}
m^{5}	p^{13}	l^{11}	e^{12}
$\_^{3}$	f^{7}	a^{10}	s^{0}
t^{2}	$\_^{8}$	c^{14}	h^{15}

This process is carried out as many blocks as specified during the encryption process. The next process is decryption for the next ciphertext as in the following section.

Ciphertext 2			
r^{0}	c^{1}	r^{2}	t^{3}
e^{4}	t^{5}	u^{6}	n^{7}
c^{8}	s^{9}	o^{10}	a^{11}
a^{12}	$\_^{13}$	e^{14}	r^{15}
Random Index			
6	9	1	4
5	13	11	12
3	7	10	0
2	8	14	15
Plaintext 2			
a^{6}	r^{9}	a^{1}	c^{4}
t^{5}	e^{13}	r^{11}	s^{12}
$\_^{3}$	c^{7}	o^{10}	u^{0}
n^{2}	t^{8}	e^{14}	r^{15}

After doing the decryption process twice, the previous ciphertext managed to return to plaintext.

CONCLUSION

After the entire research is completed, the writer can present some conclusions. Text message security techniques using a square matrix block key can secure messages in text format. The use of keys with a size of 4 x 4 provides the ability to transpose characters properly. The decrypted message has the same result as the original message.

Declaration by Authors

Acknowledgement: None

Source of Funding: None

Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

1. M. Abror, "Pengertian dan Aspek-Aspek Keamanan Komputer," 2018. [Online]. Available: https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/. [Accessed: 01-Oct-2018].
2. K. Davis, "What Are Information Systems?," *GitHub*, 2020. [Online]. Available: https://saylordotorg.github.io/text_business-information-systems-design-an-app-for-that/s05-01-what-are-information-systems.html. [Accessed: 04-Feb-2021].
3. M. Iqbal, M. A. S. Pane, and A. P. U. Siahaan, "SMS Encryption Using One-Time Pad Cipher," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 54–58, 2016, doi: 10.9790/0661-18060205458.
4. A. A. Abdullah, R. Khalaf, and M. Riza, "A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm," *Math. Probl. Eng.*, vol. 2015, pp. 1–6, 2015, doi: 10.1155/2015/481824.
5. A. Subandi, R. Meiyanti, C. L. M. Sandy, and R. W. Sembiring, "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 2, no. 5, pp. 1–5, Jun. 2017, doi: 10.25046/aj020501.

How to cite this article: Andysah Putera Utama Siahaan. Data security techniques using square block keys in text format. *International Journal of Research and Review*. 2023; 10(2): 354-358. DOI: *https://doi.org/10.52403/ijrr.20230244*

******