Paper 4

by Universitas Potensi Utama

Submission date: 28-Sep-2020 02:15PM (UTC+0700)
Submission ID: 1399087790
File name: Cipher_Algorithm_in_Securing_Text_Data_With_Md5_Verification.pdf (556.71K)
Word count: 2153
Character count: 10180

Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification

Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification

Edy Victor Haryannto*, Muhammad Zulfadly, Daifiria, Muhammad Barkah Akbar, Ivy Lazuly
Faculty Of Technic And Computer Science, Universitas Potensi Utama

*edyvharyanto55@gmail.com

Abstract. The development of information technology that is increasingly racing today makes it easy for anyone to exchange data or information. On the other hand, there are problems with data security which can be disrupted by irresponsible parties such as wiretapping, destruction, data theft or other misuse. The application of cryptographic techniques is one solution that can be done to overcome these security problems. Cryptography is the science or art of maintaining data security by scrambling data or messages. In cryptography the term*hash*one-wayfunction is widely used to test the integrity of a *file*. In this study, cryptographic algorithms and*hash*functions used are *Nihilist Cipher* and MD5. Messages or *files* textthat will be sent are firstencrypted using thealgorithm *Nihilist Cipher*. Then the MD5 algorithm is used to get the*hash*value from the encrypted message. Furthermore, to get the original message back bydecryption *Nihilist Cipher*, the*file*verification process is first done to ensure that the*file* receivedhas not changed or is still original. The results show that thealgorithms *Nihilist Cipher* and MD5can be implemented properly so that data security can be increased because before decrypting the message, the message has to be verified first.

1. Introduction

1.1 Background

In conveying information, security is very important to be implemented in it. In making a data document, most *users* use an application called Ms. Office, the software has many types of applications that can form a document including Ms. Word, Ms. Excel, Ms. Power Point and so on. Most *users* use application Ms. Word to form a document data. But there are also many Ms. Wordusers that does not care about information security in it. Those who are not responsible in the exchange of information can steal and modify the message in it. Therefore, researchers propose security in *the word file*, the security that can be applied is cryptography and hash functions that have the purpose to test the integrity of a data and prevent third parties from modifying the data.

1.2 Research Contribution

Results of this study can be used to overcome data security problems that can be disrupted by irresponsible parties such as theft and modification of messages. In addition to securing a message, this research can also maintain messages in modifications made by irresponsible parties.

2. Platform Theory

2.1 Cryptography

Cryptography is the science and art of maintaining the confidentiality of messages by encoding them in a form that cannot be understood anymore. In cryptography, there are two processes, namely encryption and decryption. The message to be encrypted is called plaintext.It's called as plaintext because this information can easily be read and understood by anyone. The algorithm used to encrypt and decrypt a plaintext involves using a key form. *Plaintext*messagesthat have been encrypted (or encoded) are known as ciphertext. In cryptography we will often find various terms or terminology.

2.2 Nihilist Cipher

Nihilist cipher was first developed by the Russian *Nihilists*, namely Russians who supported the way of violence to achieve the desired political change, in this case overthrowing the power of Tsar Alexander II in Russia. They used thealgorithm *Nihilist* to communicate and organize terrorists against Tsarist supporters in the 1880s. In addition, this algorithm is also widely used by the *First Chief Directorate*, a division of the KGB (Russian intelligence agency) to communicate their potential spies. Also used to communicate with their allies. By applying this method the theft of the message can be overcome. (Mukhlis, 2013: 2).

This algorithm uses *Polybius Square* (table 1), which is a 5x5 box, referring to the Latin letter by removing the letter J from the alphabet. Each box element is different from each other which is represented by 2 coordinate digits related to the element in question. The placement of each letter can be scrambled, it doesn't have to be regular.

Table 1.Polybius Square

	1	2	3	4	5
1	A	F	L	Q	V
2	B	G	M	R	W
3	C	H	N	S	X
4	D	I	O	T	Y
5	E	K	P	U	Z

In the case of the word MEDAN, the letter M = 23 E = 51 D = 41 A = 11 N = 33 so as to produce a coordinate (23 51 41 11 33).

2.2.1 Nihilist Cipher Encryption

The following steps will explain how to encrypt thealgorithm *Nihilist Cipher* with the assumption that the Latin letters are used.

1. Referring to thetable *Polybius Square* a plaintext is obtained with the word KASKUS so it can be represented as a coordinate (52 11 34 52 54 34). The coordinates are obtained based on the rows and columns in thetable *Polybius square* as follows:
   a. The letter K is in row 5 and column 2, the coordinate of the letter K is 52
   b. The letter A is in row 1 and column 1 the coordinate of the letter A is 11
   c. The letter S is in row 3 and column 4 then the coordinates of the letter S is 34
   d. The letter K is in line 5 and column 2 then the coordinates of the letter K are 52
   e. The letter U is in row 5 and column 4 then the coordinates of the letter U are 54
   f. Letter S is in row 3 and column 4 is the coordinate the letter S is 34
2. Then specify the *key* to be used is CENDOL, the coordinates are obtained (31 51 33 41 43 13). For the *key* does not have to have the same character length in plaintext, if thelength *key* is shorter than plaintext, the *key* will be repeated periodically. The coordinates on the *key are* obtained based on the rows and columns in thetable *Polybius Square* following:
   a. The letter C is in row 3 and column 1 then the coordinates on the letter C are 31
   b. The letter E is in row 5 and column 1 then the coordinates on letter E are 51
   c. Letter N is in row 3 and column 3 then the coordinates on letter N are 33

d. The letter D is on row 4 and column 1 then the coordinates on letter D are 41
e. Letter O is in row 4 and column 3 then the coordinates on letter O are 43
f. letters L line on line 1 and column 3 then the coordinates of the letter L are 13

3. Do the addition operations on the plaintext and coordinates*key* kfor the *key* pto plaintext c for ciphertext. Then obtained:

p = 52 11 34 52 54 34
k = 31 51 33 41 43 13 +
c = 83 62 67 93 97 47

From the above operation, the ciphertext obtained from the word KASKUS with *key* CENDOL is a coordinate 83 62 67 93 97 47

Table 2.Encryption Results Nihilist Cipher

p	**52**	**11**	**34**	**52**	**54**	**34**
k	**31**	**51**	**33**	**41**	**43**	**13**
Ct	**83**	**62**	**67**	**93**	**97**	**47**

2.2.2 TheNihilist Cipher Decryption

The following will explain the steps in decrypting with thealgorithm *Nihilist Cipher* as follows:

1. To do a decryption it must know the key and the ciphertext. *The key to* be used is CENDOL and 83 62 67 93 97 47 as ciphertext.
2. Referring to thetable the *Polybius Square* word CENDOL can be represented by coordinates 31 51 33 41 43 13. The coordinates are obtained based on rows and columns in thetable *Polybius Square*as follows:
   a. Letter C is in row 3 and column 1 then the coordinates on the letter C are 31
   b. The letter E is in row 5 and column 1 then the coordinates on the letter E are 51
   c. The letter N is in row 3 and column 3 then the coordinates on the letter N are 33
   d. Letter D is on the line 4 and column 1 the coordinates in letter D are 41
   e. Letter O is in row 4 and column 3 then the coordinates on letter O are 43
   f. Letter L is in line 1 and column 3 then the coordinates in letter L are 13

Table 3.Polybius Square

	1	**2**	**3**	**4**	**5**
1	**A**	**F**	**L**	**Q**	**V**
2	**B**	**G**	**M**	**R**	**W**
3	**C**	**H**	**N**	**S**	**X**
4	**D**	**I**	**O**	**T**	**Y**
5	**E**	**K**	**P**	**U**	**Z**

3. Then do the subtraction operation between the coordinates on the ciphertext and *key*.It is knownc is for the ciphertext and k is for the *key* and obtained:

c = 83 62 67 93 97 47
k = 31 51 33 41 43 -
p = 52 11 34 52 54 34

Table 4.Decryption Results of Nihilist Cipher

c	**83**	**62**	**67**	**93**	**97**	**47**
k	**31**	**51**	**33**	**41**	**43**	**13**
p	**52**	**11**	**34**	**52**	**54**	**34**

4. The final step is to find the equivalent characters for each coordinate obtained above with the *Polybius Square* table as in table II.3, obtained the word plaintext KASKUS.

2.3 Hash Function

The*hash*function is a function that acceptsinput *string* any length and converts it into a *string,* fixed-length outputis generally much smaller than the size of the original*string*. The*hash*function can accept any input of *string*. If the *string* declares a*message*, thenanymessage of *M* with any size is compressed by the*H hash*function through the equation.

$$h = H(M) \ldots\ldots\ldots\ldots\ldots (1)$$

The output of the*hash*function is also called the*hash*value (*hash-value*) or*message digest*. In equation (2.1), *h* is the*hash*value or *digest message* of the*H*function for input *M*. In other words, the*hash*function compresses any message of any size into a *messagedigest* whose size is always fixed (and shorter than the original message length. The hash function *is* usually used to store passwords, as testing the integrity of data, and as*fingerprint*messages.

In this study the author uses the*hash*function used to test integrity and integrity of a data. In practice, the data to be sent in advance will be encrypted, and the encryption result will be hashing process. by using hashing data, the received data can be tested in advance whether intact or have been modified by parties who are not responsible.

3. Testing System

Testing system is carried out to ensure that the system that has been built can run well in accordance with the functions previously determined at the stage of analysis and planning system. The results from the system can be seen in the following figure:

3.1 System Encryption Testing

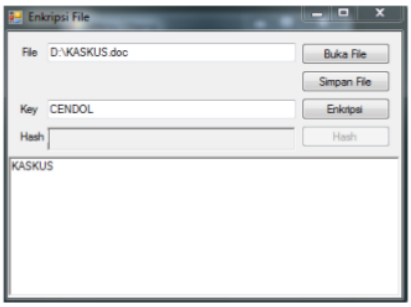

Figure 1.Plaintext

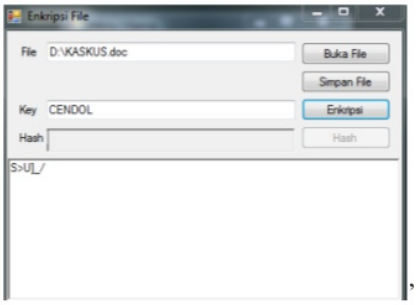

Figure 2. Ciphertext

3.2 Generate Hash MD5

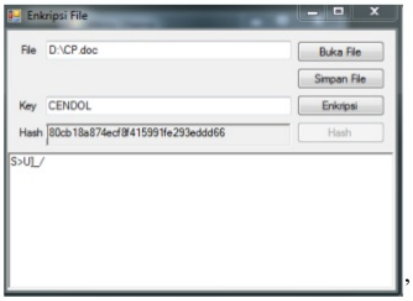

Figure 3.Hash Value MD5

3.3 Testing System Decryption

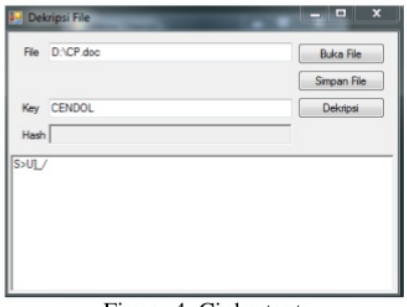

Figure 4. Ciphertext

3.4 Message Verification Process in the System

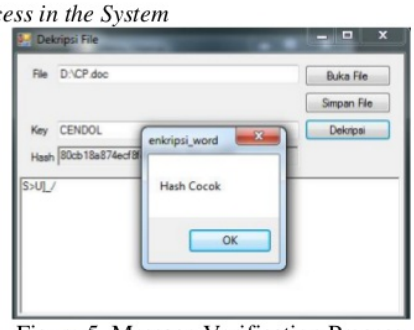

Figure 5. Message Verification Process

3.5 Decryption Results

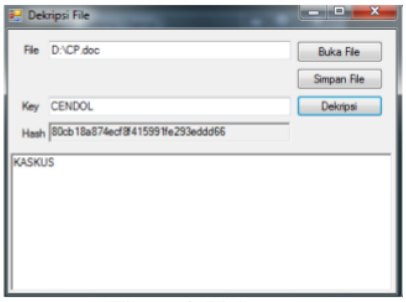

Figure 6. Plaintext

4. Conclusions

The conclusion of this research are as follows:

1. Thealgorithm *Nihilist Cipher* can be applied to the system to properly and correctly encrypt and decrypt.
2. MD5 algorithm is able to perform data integrity testing so as to ensure that the message received is genuine and does not experience modification.

References

[1]. Mukhlish, 2013. "***Modification of Nihilist Cipher***". School of Electrical and Informatics Engineering Bandung Institute of Technology. Bandung

[2]. Pobokory. Dkk, 2015, "***Cryptographic Implementation of Data Security in Text Messages, Fill Document Files, and Document Files Using Advanced Encryption Standard Algorithms***". **Vol.10 No.1**. Computer Science Study Program, FMIPA, Mulawarman University.

[3]. Rendi et al, "***Data Integrity Testing Using the MD5 Algorithm***".**Vol.3 No.1** Informatics Engineering Study Program PPKIA STMIK PradnyaParamita.

Paper 4

ORIGINALITY REPORT

15%	12%	12%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Marliana Sari, Gunawan, Nanang Sadikin. "Server Temperature Monitoring System Using Web Based Censor And SMS Gateway", Journal of Physics: Conference Series, 2019 Publication	5%
2	Submitted to Universitas Sultan Ageng Tirtayasa Student Paper	2%
3	mafiadoc.com Internet Source	2%
4	www.semanticscholar.org Internet Source	2%
5	doi.org Internet Source	2%
6	Tonni Limbong, Janner Simarmata, ARS Tambunan, Parulian Siagian et al. "The implementation of computer based instruction model on Gost Algorithm Cryptography Learning", IOP Conference Series: Materials Science and Engineering, 2018	1%

Publication

7	D Tri Octafian. "Design of The Web-Based Tracer Study Application of STMIK PalComTech", Journal of Physics: Conference Series, 2019 Publication	1%
8	ieeexplore.ieee.org Internet Source	1%

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	Off		