International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 02, February-2017

Testing the Classic Caesar Cipher Cryptography using of Matlab

Tonni Limbong
Catholic University ST. Thomas SU,
Street. Setiabudi No. 479 F Tanjungsari,
Medan, North Sumatra, Indonesia

Parasian D.P. Silitonga
Catholic University ST. Thomas SU,
Street. Setiabudi No. 479 F Tanjungsari,
Medan, North Sumatra, Indonesia

***Abstract* - Cryptography is a science to disguise / change the form of the original message into a message that can not be known or understood by who is not eligible. Caesar cipher is a method that is classic and very basic in the science of encoding messages. This method has drawbacks such spaces can not encrypt because the formula uses mod 26, and also if after the process of counting the remaining results for her 0 as well, then this result will not have to encrypt results. But the basic technique is very important to learn the techniques of modern cryptography, then it is necessary for a test for the verification process of plaintext into ciphertext (encryption) and also ciphertext into plaintext (decryption) using software testers that Matlab R2010a with the purpose is to make can more easily determine the process logic of cryptography.**

Keywords:* *Cryptography, Caesar Chiper, Matlab

I. INTRODUCTION

Cryptography (cryptography) is derived from the Greek: "cryptos" means "secret" (secret), while the "graphein" means "writing" (writing). So, cryptography means "secret writting" (hieroglyph). There are several definitions of cryptography that has been presented in the literature[4]. Cryptography is the science and art to keep secret the message by way of encoding it into a form that can not be understood more meaning.

Caesar Chipper is an algorithm used by system cryptography symmetry and used long before the public key cryptography system is found, the existing classical cryptography and some forms of classical algorithm has been no trend (considered optimal) because it is easily solved. But in studying the basic cryptography, the classic method is a very good basis to continue into the development of modern cryptography, especially in coaching reasoning logical thinking.

Some of the reasons why it is important to learn classical cryptography algorithms include 1) To give an understanding of the basic concepts of cryptography; 2) The basis for the development of modern cryptographic algorithms; 3) to assess potential system weaknesses cipher.

Science of cryptography lies in the current logic for encryption and decryption process in which the process should be proven not just a theoretical course which will users to develop the basic process of caesarean become a cryptographic cipher modern.untuk test a logic process required a software tester.

In the absence of definite formula in cryptographic methods Caesar Chiper, it can be said that Caesar Chiper difficult to solve. Encryption is important in sending message, especially the message is very secret[1].

The downside of caesar chipper are not able to encrypt or decrypt a message consisting of a few words or sentences, and also with the formula provided that the position of the letters plus numbers round (key) divided by 26 and the rest of him is the position of the letters encoded message (new messages) where can dijelas visible position initial letter is the number 1 (one) while 26 Mod 26, the remainder is 0 (zero) then the message to be encoded will never be found and it should also be understood that the message was never one word so that spaces can not be entered ,

In this paper made an additional rule to address weaknesses in the writing distance from word to word ('spaces') to change the outcome of the mod from 26 to 27, and to cope with index 0 (zero) then made a condition if the results of the mod is 0 then the position encoded message is the position of the letters plus round (key). This process will be tested using Matlab R2010a by example graph visualization using the facilities provided by the figure of the matlab application.

With this study, the researchers are happy to discuss cryptography, especially students and students, this article shows the problem with the caesar chipper and techniques to overcome the problem, thus creating a mindset to find and fix a weakness of methods and algorithms of cryptographic another fine it is for modern cryptography.

II. RESEARCH METHODS

2.1. Substitution Cipher

Substitution cipher is a cryptographic algorithm used by the first Roman emperor, Julius Caesar (so called also caesar cipher), to encrypt a message which he sent to the governors [2].

This is the process of encoding a message by replacing (substituting) each character with another character in alphabetical order (alphabetical).

For example, each letter is substituted with the following third letter of the alphabet arrangement. In this case the key is the number of shifts of letters (ie k = 3).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 02, February-2017

Table substitutions:
pi: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ci: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Information :
Pi = Alphabet alphabet
Ci = Chiper alphabet (Substituted 3)

example:
Message: TONNILIMBONG
be encrypted
Cipher: WRQQLOLPERQJ
The recipient decrypts the message chiperteks using substitution table, so chiperteks.
WRQQLOLPERQJ
can be restored into its original plaintext:
TONNILIMBONG

With encode each letter of the alphabet with integer as follows: A = 0, B = 1, ..., Z = 25, then mathematically caesar ciphers encrypt plaintext into ci pi to the rules:
ci = E (pi) = (pi + 3) mod 26
and decryption chiperteks ci be pi to the rules:
pi = D (ci) = (ci - 3) mod 26

Because there are only 26 letters of the alphabet, the letter shift possible is from 0 to 25. In general, in order to shift the letter as far as k (in this case k is the encryption key and descriptions), the encryption function is
ci = E (pi) = (pi + k) mod 26
and decryption functions are
pi = D (ci) = (ci - k) mod 26

2.2. Cryptanalysis against Caesar Chiper

Caesar cipher is easily solved by the method of exhaustive key search for the key number is very small (there are only 26 keys) [2].
example:
Suppose cryptanalyst find pieces chiperteks (also called a cryptogram) WRQQL. It is assumed that the plaintext prepared cryptanalyst knows is the person's name and a cryptographic algorithm used is caesar cipher. To obtain the plaintext, do the decryption key from the largest, 25, until the key is the smallest, 1. Check if the decryption generates a message that has meaning (see Table 1).

The process:
Pi = WRQQL
K = 24 (Y) 1 + 24
pi: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ci: Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
results: YTSSN

K = 19 (T) → 1 + 19
pi: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ci: T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
results: DYXXM

K = 9 (J) → 1 + 9
pi: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ci: J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
results: NIHHC

K = 3 (D)
pi: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
ci: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
results: Tonni

and so on, and then stacking each of the above processes into the table as shown below

Table 1. Examples of exhaustive key search against chiperteks WRQQL

Key (k) Chiperin g	'Message' of the descriptio n	Key (k) Chiperin g	'Message' of the descriptio n	Key (k) Chiperin g	'Message' of the descriptio n
0	WRQQL	17		8	
25	*YTSSN*	16		7	
24		15		6	
23		14		5	
22		13		4	
21		12		3	*TONNI*
20	*DYXXM*	11		2	
19		10	*NIHHC*	1	
18		9			

From Table 1, said in Behalf of potential into plaintext is Tonni using k = 3. This key is used to decrypt the other chiperteks.

II. RESULTS AND DISCUSSION

In an ongoing process, to be more easily and optimally in the proof needed to be resolved by using available tools or software. Testing and verification is necessary so that the reader can more easily understand and comprehend how a method is implemented and working to solve the problem.

Likewise with classical cryptography is that the Caesar system, the logic steps as follows:

1. The shift 0 is equal to a shift of 27 (arrangement of letters does not change)
2. Another shift for k> 25 can also be carried out but the results will be congruent with the integers modulo 27. For example, k = 37 congruent with 11 in the modulo 26, or 37 → 11 (mod 27).
3. Because there is the addition operation in the equation, then the caesar cipher sometimes also called additive cipher.

So for the purposes of the above problems, it can be concluded:

1. The number of indexes that exist in the alphabet (26) should be added one (1) character "blank spaces" in the beginning or middle of the alphabet arrangement,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 02, February-2017

because the logic of a sentence made up of several words, each word separated by whitespace.

2. The formula for the plaintext can be changed from Ci = E (pi) = (pi + 3) mod 26 becomes ci = E (pi) = (pi + 3) mod 27
3. The formula for the ciphertext can be changed from Pi = D (pi) = (pi - 3) mod 26 becomes Pi = D (pi) = (pi - 3) mod 27

3.1. Testing Ekripsi with Matlab R2010a

To test this caesar encryption that need to be considered are [3]:

a. Number of Constanta to index the actual letter that has been added to the "space"

b. The number of iteration loops that arises is as long text message fed.

c. Encryption is determined by the results: Ci = E (pi) = (pi + 3) mod 27

The shape of the source code for encryption are as follows:

```
data = [ 'ABCDEF GHIJKLMNOPQRSTUVWXYZ'];
word = upper (input ( 'Enter the text:', 's'));
round= input ( 'Lock:');
ce = [];
m = [];
de = [];

pj = size (word, 2);
x = 0;
for i = 1: pj;
  m = [m word (i)];
  ce = [ce find (data (:,:) == word (i))];
  de = [ce find (data (:,:) == word (i))];
x = mod ((ce + round), 27);
s = ce;
st = data(:, x);
end
initial = s
chiper = x
ciphertext = st
plot (x)
grid on
```

3.2. Testing Decryption with Matlab R2010a

To test this caesar encryption that need to be considered are:

a. Specify Constanta to index the actual letter that has been added to the "space"

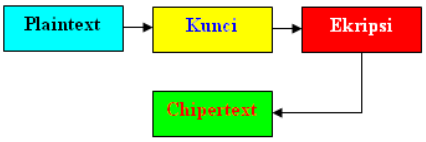
b. The number of iteration loops that arises is as long text message fed.

c. Results Decryption is determined by: Pi = D (pi) = (pi - 3) mod 27

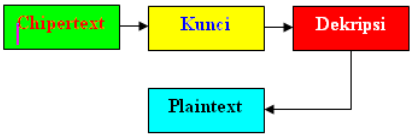
The shape of the source code for decryption is as follows:

```
data = ['ABCDEF GHIJKLMNOPQRSTUVWXYZ'];
word = upper (input ('Enter the text:', 's'));
round = input ( 'Lock:');
ce = [];
m = [];
de = [];
pj = size (word, 2);
x = 0;
for i = 1: pj;
  m = [m word (i)];
  ce = [ce find (data (:,:) == word (i))];
  de = [ce find (data (:,:) == word (i))];
x = mod ((ce-round), 27);
s = ce;
st = data (:, x);
end
initial = s
chiper = x
Plaintext = st
plot (x)
grid on
save the name CaesarD in the form of M-Files.
```

The shape of the testing process can be seen in pigure 1 below.



(a) Diagram Encryption



(b) Diagram Decryption

Figure 1. Diagram Cryptography

Form view the test results are as follows:

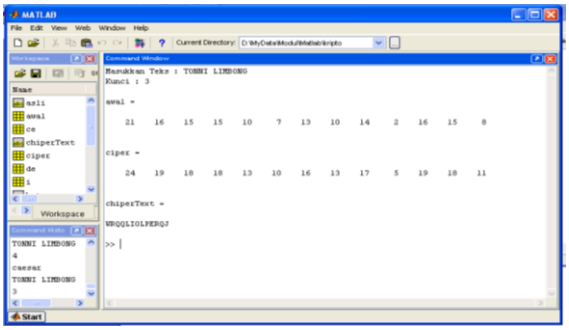


Figure 2. Display Encryption Test Results

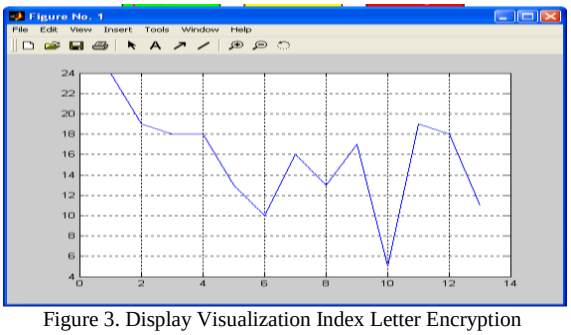


Figure 3. Display Visualization Index Letter Encryption

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 02, February-2017

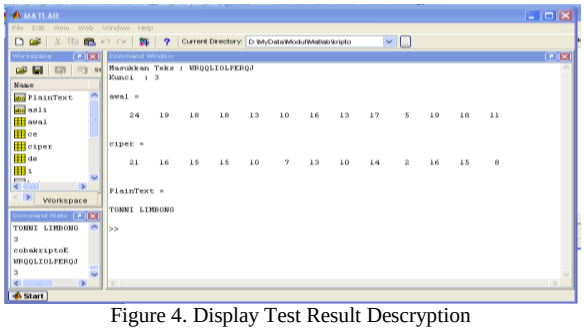


Figure 4. Display Test Result Descryption

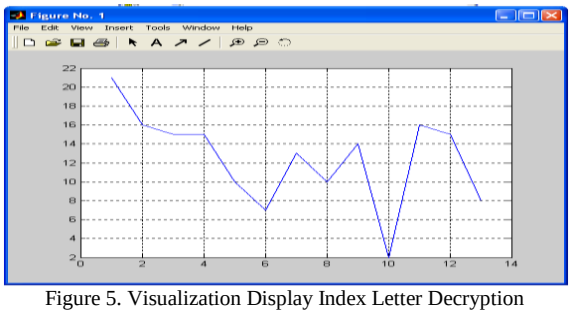


Figure 5. Visualization Display Index Letter Decryption

Figure 6. Display Form Cryptography Caesar Chiper

IV. CONCLUSION

Of writing and testing it can be concluded that:

1. Caesar was not so optimal Cryptography is used to protect the message because it has a key bit counter which is only 26 keys.
2. In order to accommodate the sentences in which there are "empty spaces" should be added in the index so that the number of character is no longer 26 but to 27, so that the process also turns into MOD modulo 27.
3. Classical Cryptography is still very important to know for basic study and create a modern cryptography.

REFERENCES

[1] Anjar Pradipta, Implementation Methods Caesar Cipher Alphabet Compound In Cryptography For Information Security, Indonesian Journal on Networking and Security - Volume 5 No 3 – Agustus 2016, page 16-19.

[2] Dony Ariyus. 2008. "Introduction to Cryptography Theory, Analysis, and Implementation", Andi OFFSET, Yogyakarta

[3] Gunaidi, A. 2006. "Matlab Programing". Informatics.

[4] Rinaldi Munir. 2006. "Cryptography". Bandung: Informatics Bandung.

[5] Sasongko, J., 2005, Data Security Information Using Classical Cryptography, DINAMIK Vol 10 No 3, ISSN 0854-9524, pp 160-167.

[6] Yusuf Triyuswoyo ST. et.all, Algorithm Implementation Caesar, Cipher Disk And Application Scytale Encryption And Decryption Short Message, Lumasms, Proceedings of the National Scientific Seminar on Computer and Intelligence Systems (KOMMIT 2014) Vol. October 8, 2014 Gunadarma University - Depok - 14 - October 15, 2014 ISSN: 2302-3740