Login : Jurnal Teknologi Komputer
ISSN : 2302-9692 (print) | 2723-8695 (online)
Vol. 15, No. 1, June 2021, Page 45-50
LOGIN http://login.seaninstitute.org/index.php/Login

Simulation of The Application of Intelligence in Vernam Cipher Cryptography (One Time Pad)

Agustina Simangunsong[1], R. Mahdalena Simanjorang[2]
[1,2]Informatics Engineering Study Program, STMIK Pelita Nusantara Medan.

Article Info

Article history:

Received Apr 27, 2021
Revised Mei 27, 2021
Accepted Jun 28, 2021

Keywords:

Vernam Cipher Algorithm,
Simulation,
Cryptography.

A B S T R A C T

Technological advances in the field of computers allow thousands of people and computers around the world to be connected in one virtual world known as cyberspace or the Internet. But these technological advances are always accompanied by the downside of the technology itself. One of them is the vulnerability of data security, giving rise to challenges and demands for the availability of a data security system that is as sophisticated as the advancement of computer technology itself. In this study, an algorithm that can secure data will be used which the authors discuss is the Vernam Cipher Algorithm. Vernam Cipher Algorithm is one of the key algorithms. Until now, the Vernam Cipher algorithm is still trusted as an encryption method, Vernam Cipher cryptography uses the same key for encryption and decryption.

Corresponding Author:

Agustina Simangunsong,
Informatics Engineering Study Program, STMIK Pelita Nusantara Medan,
Jl. Iskandar Muda, Babura, Kec. Medan Baru, Kota Medan, Sumatera Utara 20152.
Email: agustinasimangunsong93@gmail.com

1. INTRODUCTION

Technological advances in the field of computers allow thousands of people and computers around the world to be connected in one virtual world known as cyberspace or the Internet. Likewise hundreds of organizations such as companies, state institutions, financial institutions, the military and so on. But these technological advances are always accompanied by the downside of the technology itself. One of them is the vulnerability of data security, giving rise to challenges and demands for the availability of a data security system that is as sophisticated as the advances in computer technology itself. This is the background for the development of data security systems to protect data transmitted through a communication network.

Today, 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 systems 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. Data that will be sent and has not been encrypted is known as 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 discusses is the Vernam Cipher Algorithm.

Vernam Cipher Algorithm is one of the key algorithms. Until now, the Vernam Cipher algorithm is still trusted as an encryption method, Vernam Cipher cryptography uses the same key for encryption and decryption. And based on the description above, the author is interested in choosing the title "Simulation of Application of Integers in Vernam Cipher Cryptography (One Time Pad)".

2. RESEARCH METHOD

Research methodology is the steps and procedures that will be carried out in collecting data or information in order to solve problems and test research hypotheses. This section explains how the methodology used to solve research problems through a channel, one of which is cryptography. The research framework can be seen in the diagram below :

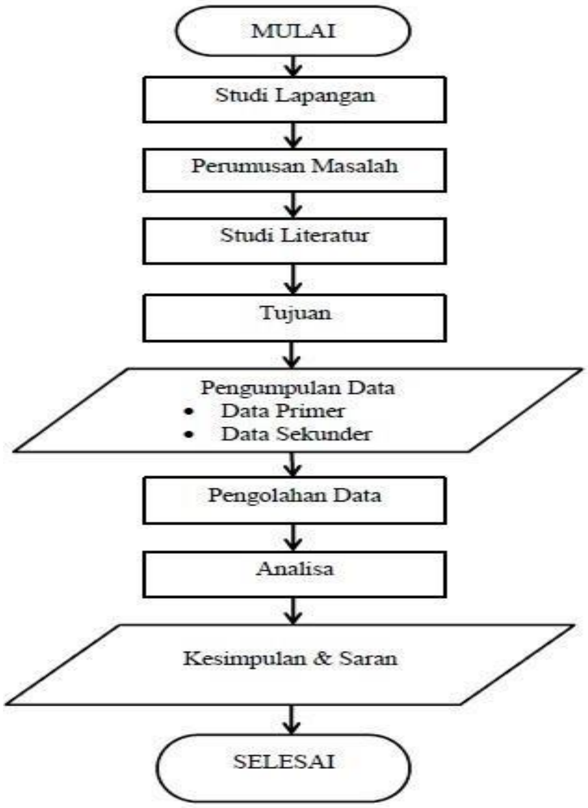

Figure 1. Research Framework

Based on the framework in the picture above, each step can be described as follows:

A. Field Study

The field study is the first step in this research to find out the problems that are often experienced.

B. Formulating the Problem

Based on the literature study, a problem was found which was then modeled and formulated to provide a solution to the problem.

C. Literature Study

Literature study is the next step in this research in completing the basic knowledge and theories used. To achieve the objectives to be determined, it is necessary to study several literatures/journals that support this research.

D. Purpose

In this stage, the purpose of this research is determined, namely to secure data using cryptographic techniques.

E. Data Processing

In this stage, there are several things that need to be done in data processing including:

1. Determining Variables and Measurements
   The following is the key formation process. This process is carried out by the recipient, in this case B.

a. Choose prime numbers p and q.
b. Calculate n = pq .
c. Calculate j (n) = (p -1)(q -1) .
d. Choose any number b, 1 < b <j (n) , with gcd(b,j (n)) = 1.
e. Calculate the inverse of b, i.e. a = b-1 modj(n) .
f. Public key: (n, b) and secret key: a.

In order to make it easier to understand the password with integers, specifically in this thesis, the plaintext used is only in the form of numbers 0 to 25 which correspond to the letters a to z. However, in actual use, correspondence tables such as ASCII codes are used, as well as very large numbers. In the selection of p and q must meet n = pq more than or equal to the possible plaintext values. In this case n = pq >= 25 .

3. RESULTS AND DISCUSSION

3.1. Cryptographic Analysis of Integers

3.1.1 Modulo Arithmetic

Modulo arithmetic (modular arithmethic) plays an important role in integer computing, especially in cryptographic applications. The operator used in modulo arithmetic is mod. The mod operator, when used for integer division, returns the remainder of the division.

Example :
A = 53
B=5
C = A mod B
= 10 and remainder = 3
Then A=53 MOD B=5 = 3

3.1.2 Key Formation in Round Month Cryptography

The following is the key formation process. This process is carried out by the recipient, in this case B.

(1) Choose prime numbers p and q.
(2) Calculate n = pq .
(3) Calculate j (n) = (p -1)(q -1) .
(4) Choose any number b, 1 < b <j (n) , with gcd(b,j (n)) = 1.
(5) Calculate the inverse of b, i.e. a = b-1 modj(n) .
(6) Public key: (n, b) and secret key: a.

In order to make it easier to understand the password with integers, specifically in this thesis, the plaintext used is only in the form of numbers 0 to 25 which correspond to the letters a to z. However, in actual use, correspondence tables such as ASCII codes are used, as well as very large numbers. In the selection of p and q must meet n = pq more than or equal to the possible plaintext values. In this case n = pq >= 25 .

Table 1. Correspondence of Integers

A	B	C	D	E	F	D	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example :
B choose
- p = 5
- q = 11
- n = p * q = 55

then n = 55
and R= (55) (5 1)(11□1) 4 x 10 40
choose any number (b) = 13
Then GCD = gcd(13,40)
13 = 1.40 - 27
27 = 27.1

gcd = 1
so a = 131 mod 40
= 37
So the public key is (n,b) = (55,13) and the secret key is a = 37

3.1.3 Encryption of Integers

The following is the encryption process on Integers. It is carried out by the sender, in this case A. All calculations for the power of the modulo number are carried out using the fast exponentiation method.
(1) Take the public key (n,b).
(2) Choose plaintext m, with 0 £ m £ n -1 .
(3) Calculate c = mb mod n .
(4) Obtain ciphertext c, and send it to B.
Example :
the plaintext is "crypto", using Table 3.1 above we get m1 = 10, m2 = 17 , m3 = 8 , m4 = 15 , m5 = 19 , and m6 = 14 and then the calculation is carried out to get the crypto value of each character as shown below:
c1 = m1b mod n = 1013 mod 55 = 10
c2 = m1b mod n = 1713 mod 55 = 7
c2 = m1b mod n = 813 mod 55 = 28
c2 = m1b mod n = 1513 mod 55 = 20
c2 = m1b mod n = 1913 mod 55 = 39
c2 = m1b mod n = 1413 mod 55 = 49
So, the ciphertext is 10-7-28-20-39-49.
Example :
B choose
- p = 5
- q = 11
- n = p * q = 55
So n = 55
and R= (55) □□(5 □1)(11□1) □□4 x 10 □□40
choose any number (b) = 13
so GCD= gcd(13,40)
13 = 1.40 - 27
27 = 27.1
gcd = 1
So a = 13^{1} mod 40
= 37
So the public key is (n,b) = (55,13) and the secret key is a = 37

3.1.4 Encryption of Integers

The following is the encryption process on Integers. It is carried out by the sender, in this case A. All calculations for the power of the modulo number are carried out using the fast exponentiation method.
(1) Take the public key (n,b).
(2) Choose plaintext m, with 0 £ m £ n -1 .
(3) Calculate c = mb mod n .
(4) Obtain ciphertext c, and send it to B.
Example :

The plaintext is "crypto", using Table 1 above we get m1 = 10, m2 = 17, m3 = 8, m4 = 15, m5 = 19, and m6 = 14 and then the calculation is carried out to get the crypto value of each character as shown below :
c1 = m1b mod n = 1013 mod 55 = 10
c2 = m1b mod n = 1713 mod 55 = 7
c2 = m1b mod n = 813 mod 55 = 28

c2 = m1b mod n = 1513 mod 55 = 20
c2 = m1b mod n = 1913 mod 55 = 39
c2 = m1b mod n = 1413 mod 55 = 49
So, the ciphertext is 10-7-28-20-39-49.

3.1.4 Decryption of Integers

The following is the process of decrypting the integer algorithm. Performed by the recipient of the ciphertext, namely B.
(1) Take public key (n,b) and secret key a.
(2) Calculate m = ca mod n .
Cipher text = 10-7-28-20-39-49 then take the secret key a = 37 , and do the following calculations.
m1 = c1a mod n = 1037 mod 55 = 10
m2 = c2a mod n = 737 mod 55 = 17
m3 = c3a mod n = 2837 mod 55 = 8
m4 = c4a mod n = 2037 mod 55 = 15
m5 = c5a mod n = 3937 mod 55 = 19
m6 = c6a mod n = 4937 mod 55 = 14
Obtained plaintext 10-17-8-15-19-14, if corresponded according to Table 5.1, obtained the original message sent by A, namely "crypto".

3.1.5 One Time Pad

In this study, the analysis of the One Time Pad algorithm will be discussed. For example, when sending a message to someone, the message must be confidential. In this discussion, One Time Pad will encrypt messages so that they are safe. Below will be explained an example of using the one time pad algorithm in a message.

For example: A message "HELLO" will be encrypted with the key "XMCKL" with the following calculation, it will get the following results:

Table 2. Message ascii

Plain Teks	**Ascii**
H	7
E	4
L	11
L	11
O	14

Table 3. Key ascii

Key text	Ascii
X	23
M	12
C	2
K	10
L	11

From the table above it can be concluded as follows:

Message (plaintext)	: 7(H)	4(E)	11(L)	11(L)	14(O)
Key	: 23(X)	12(M)	2(C)	10(K)	11(L)
Key message	: 30	16	13	21	25
Pesan di enkripsi dengan mod 26					
Message + key mod 26	: 4(E)	16(Q	13(N)	21(V)	25(Z)

Then it will generate encryption : **E Q N V Z**
To describe it, the reverse process is carried out, namely.

Ciphertext	: 4(E)	16(Q	13(N)	21(V)	25(Z
Key	: 23(X)	12(M)	2(C)	10(K)	11(L)
Ciphertext - key	: -19	4	11	11	14
Ciphertext - key mod 26	: 7(H)	4(E)	11(L)	11(L)	14(O)

Then the encryption message will return to its original state: H E L L O

4. CONCLUSION

The software designed functions to encrypt and decrypt information by using the Vernam Ciper (One Time Pad) algorithm, This software can only encrypt plain text.

REFERENCES

[1] Agustanti, Sri Primaini, Pengamanan Kunci Enkripsi One Time Pad menggunakan Enkripsi RSA, Jurnal Media Teknik, 2010
[2] Blum, L., Blum, M., Shub, M., A Simple Unpredictable Pseudo-Random Number Generator, Society For Industrial and Applied Mathematics, 1986.
[3] Blum, Manuel., Micali, Silvio, How to Generate Cryptographically Strong Sequence of Pseudo Random Bits.
[4] Junod, Pascal, Cryptographic Secure Pseudo-Random Bits Generation: The Blum Blum Shub Generator, 1999
[5] Leung, Debbie W., Quantum One Time Pad Cipher, Quantum Information and Computation, 2001
[6] Menezes, A., Oorschot, van P., Vanstone, S., Handbook of Applied Cryptography, CRC Press, 1996
[7] Munir, Rinaldi, Algoritma Enkripsi Citra dengan pseudo One-Time Pad yang menggunakan sistem chaos, Konferensi Nasional Informatika, 2011
[8] Munir, Rinaldi, Kriptografi, Penerbit Informatika, Bandung, 2005
[9] Sholeh, M., Hamokwarong, J.V., Aplikasi Kriptografi dengan metode One Time Pad Cipher dan Metode Permutasi, Momentum, 2011
[10] Stalling, William, Cryptography and Network Security, Principle and Practice, Pearson Education, 2003