ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 13-21 (2017)

www.astesj.com

2nd International Conference of Computer, Environment, Social Science, Health Science, Agriculture & Technology (ICEST) 2017 5-7 May 2017, Medan, Indonesia

ASTESJ

ISSN: 2415-6698

Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma

Elwinus H. A. Mendrofa*[1], Elwin Yunith Purba[1], Boy Yako Siahaan[1], Rahmad W Sembiring[2]

[1]*Department of Informatics Engineering, University of North Sumatera, Medan, 20155, Indonesia*

[2]*Politeknik Negeri Medan, Medan-Indonesia,*

Email: elwin.zeva@gmail.com, elwinpurba.manorsa@gmail.com, rahmadwphd@gmail.com

ARTICLE INFO

Article history:
Received: 14 March, 2017
Accepted: 20 April, 2017
Online: 13 June, 2017

Keywords:
Cryptography
Vigenere Cipher
Rotation of Matrixs

ABSTRACT

Cryptography is still developing today. Classical cryptography is still in great demand for research and development. Some of them are Vigenere Cipher and One Time Pad (OTP) Algorithm. Vigenere Cipher is known as the alphabet table used to encrypt messages. While OTP is often used because it is still difficult to solve. Currently there are many ways to solve the Vigenere Cipher algorithm. OTP itself has constraints with the distribution of keys that are too long. The key length in the OTP algorithm is the same as the plaintext length. Key random creation also increases the intensity of key distribution. This requires a secure network at a high cost. The key repeater also lowers the message security level. EM2B Key algorithm is able to overcome key problem in OTP. EM2B and Increment of Key (L_k) collaborations produce key lengths equal to plaintext. The Rotation of Matrix (ROM) algorithm contributes to manipulating the length of plaintext characters. ROM works with Square Matrix tables that also scramble the contents of plaintext. The addition of Vigenere Cipher further enhances plaintext security. The algorithm was developed with the EnC1 function, Subrange (S_i), and Length of Plaintext (L_p). This research produces a very strong ciphertext. Because plaintext undergoes four stages of encryption to become cipherteks. Then the length of the plaintext changes with the number of cells in the matrix. The value of Si and L_p is added to the plaintext to be a flag for the decryption process.

1. Introduction

In this increasingly sophisticated era almost all the good circles of government, industry, business to personal companies do the work using computer. The capabilities possessed by computer devices is no doubt, this is proved by the level of accuracy to a high speed in completing a job. Besides the bias advantage obtained from the use of computer, the most important thing to be considered is part of its security which if the information/data stored in the computer suffered damage or loss then it could lead to huge losses. The condition of a computer that is not secured properly, will be a great opportunity to the hackers to enter the computer access and steal all the data he wants. Some examples of hacking cases in 2016, among others "Ransomware emerges as a top cyber threat to business, UK second only to US in DDoS attacks, 412 million user accounts exposed in Friend Finder Networks hack, Financial Conduct Authority concerned about cyber security of banks, and other cases caused by the weakness of the security system. For that we need a computer security system. Security of data in a computer is very important to protect the data from other parties that do not have the authority to determine the content of the data [1]. Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security [2].

*Corresponding Author: Elwinus H. A. Mendrofa, Department of Informatics Engineering, University of North Sumatera, Medan, 20155, Indonesia
Email: elwin.zeva@gmail.com

2. Literature Review

The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) [3]. Cryptography is one of the areas of science that studies about information security / data to avoid adverse effects due to misuse of information by irresponsible parties. Cryptography has an important role in maintaining the confidentiality of information both in the computer and at the time of transaction data.

So a more hardheaded goal of cryptography is to make it too work intensive for attacker [11]. The basic terms used in cryptography are discussed bellow:

Plaintext

In crytography, plaintext is a simple readable text before being encrypted into ciphertext [12]. The data can be read and understood without any special measure is called plaintext [13].

Ciphertext

In Cryptography, the transformation of original message into non-readable message before the transmission is known as cipher text [16]. It is amessage obtained by some kind of encryption operation on plain text.

Encryption

Encryption is a process of converting plain text into cipher text. Encryption process requires encryption algorithm and key to convert the plain text into cipher [17]. In cryptography encryption performed at sender end.

Decryption

Decryption is the reverse process of encryption. It converts the cipher text into plain text. In cryptography decryption performed at receiver end [11].

Key

The key is the numeric or alphanumeric text used for the encryption of plain text and decryption of cipher text [16]

Currently the scientists in the field of cryptography has been a lot of research about the science of cryptography by creating a variety of new algorithms developed from previous algorithms. The level of security offered varies, there is a security priority by applying the stages of a very complex algorithm, and by offering the speed of the execution process of the algorithm they created.

Vigenere Cipher is one of the classic cryptographic algorithms that until now is still widely developed by researchers. In the cryptography, it contains different methods among them the cryptography with the Vigenère matrix. Cipher was proposed by BLAISEDE VIGENÈRE in 1583 and has reigned about 03centuries.

Another classic cryptographic algorithm is *Vernam Cipher*, known as the One *Time Pad* algorithm. In its development *One Time Pad* algorithm is still much in demand by researchers, because the key length generated randomly equal to the length of the message. But the length of the key to be distributed becomes an interesting thing to develop, because when sending a key must require a secure network where the secure network is expensive. The key looping is also a weak point in the algorithm, which means that if the message is encrypted and decrypted then to encrypt the same message must use a new key, it means that network security is a top priority due to frequent distribution of keys.

The key looping is also a weak point in the algorithm, which means that if the message is encrypted and decrypted then to encrypt the same message must use a new key, it means that network security is a top priority due to frequent distribution of keys. This is the case with Vigenere ciphers though considered safe for centuries but then its weaknesses have been identified. Friedrich Kasiki invented a method to identify the period and therefore the key and plaintext [11]

This research provides a solution to the length of keys to be distributed that have lengths to be equal to the message. Doubts over repetition of key biases that result in cryptanalysis can easily know the contents of the message can be overcome by the collaboration with the algorithm *Vigenere Cipher* and *Rotation of Matrix (ROM)*. These three algorithms support each other to ensure the security level of the message and make it difficult for the irresponsible party to guess the contents of the original message.

The message will be sent encryption process four stages where each stage will produce *1st* ciphertext, *2nd* ciphertext, *3rd* ciphertext, and *final ciphertext* [10]. The first stage, the message is encrypted using the *Vigenere Cipher* algorithm by first determining the index of each message character and key. Both indexes are summed and modulated to the specified character length of the index table. The result of this stage is called *1st ciphertext*. . The next step is to determine the value of subrange and Length of plaintext. The subrange value is derived from the sum of each message index and the Length of Plaintext is determined by the number of characters of the message itself. After the subrange and length of plaintext values are obtained then the index value for each key character multiplied by the subrange value and modulated by length of plaintext, this result is called Encryption *1st ciphertext (EnC1)*. *2nd ciphertext* is obtained from multiplication between *1st ciphertext and EnC1* value. The third stage is using the *Rotation of Matrix (ROM)* algorithm where in this stage the message that has been converted into *2nd ciphertext* is inserted into a matrix table. This algorithm aims to scramble messages that have been entered into the matrix table using the rotation method and manipulate the number of characters from the message.

The workings of this algorithm is very easy but requires precision because the rotation value obtained from a key algorithm called *E2mbs Key* Algorithm and the length of the key characters will determine the number of matrix tables to rotate. After all the process at this stage is done then obtained *3rd ciphertext*, and the final stage is using *One Time Pad* algorithm, where as we know this algorithm is run by converting all characters of the message and key into binary numbers which then

operated by exclusive or (XOR) method. The *One Time Pad* algorithm in this research has been modified in the key generation section. Previous research has always used a random machine to generate a key. The need for modifications to the key generation process aims to avoid making such long keys when restoring the original message from ciperthext. The key used to encrypt messages on the *One Time Pad* algorithm is the primary key that has been altered using the *E2mbs* Key algorithm, then to increase the length of the key so that it is the same as the message display, the increment key method is used. The encryption results in this final stage produce *Final Ciphertext* which will be sent to the recipient of the message along with the main key where the length of the character does not have to be the same length of the message. In this classic algorithm has been found a way to find out the contents of the original message without having to know the key, This research is explained that the decryption process will be faster if the recipient of the message to obtain the main key and follow the correct procedure. However, if decrypted by guessing the key then kriptanalis must go through a long route and the weight of the possibility to find out the original message content.

3. Materials and Methods

According to (William, 2010) Cryptography is a technique applied for encryption and decryption. In the field of cryptography there are several techniques available for encryption/decryption. These techniques can be generally classified into two major groups, i.e. Conventional and public key Cryptography [4].

To understand the workings of cryptographic algorithms in this research, the following will be presented a block diagram explaining the flow of the encryption process.

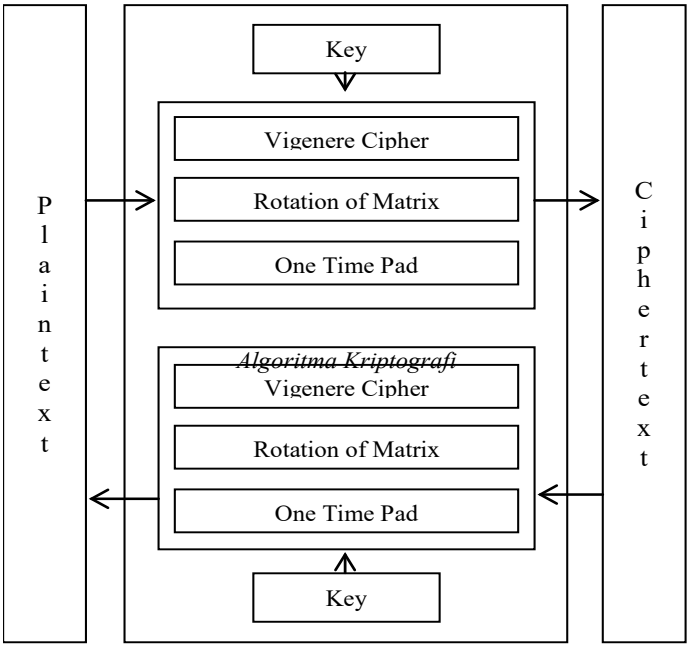


Figure 1. Block Diagram of Cryptography Algorithm Encryption and Decryption.

From the picture above can be known in general the process of encryption of a plaintext into ciphertext and the decryption of ciphertext to plaintext.

In this cryptographic algorithm used two tables as parameter to determine character index among others, Plaintext Index Table (0, 1, 2, …, 36) of 37 characters to identify characters (A, B, ..., Z, spaces, 0, 1 , ..., 9) and ASCII tables as character parameters changed into ASCII characters.

Paintext	Index	Paintext	Index	Paintext	Index	Paintext	Index
A	0	K	10	U	20	3	30
B	1	L	11	V	21	4	31
C	2	M	12	W	22	5	32
D	3	N	13	X	23	6	33
E	4	O	14	Y	24	7	34
F	5	P	15	Z	25	8	35
G	6	Q	16	sp	26	9	36
H	7	R	17	0	27		
I	8	S	18	1	28		
J	9	T	19	2	29		

Figure 2. Plaintext Index Table

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

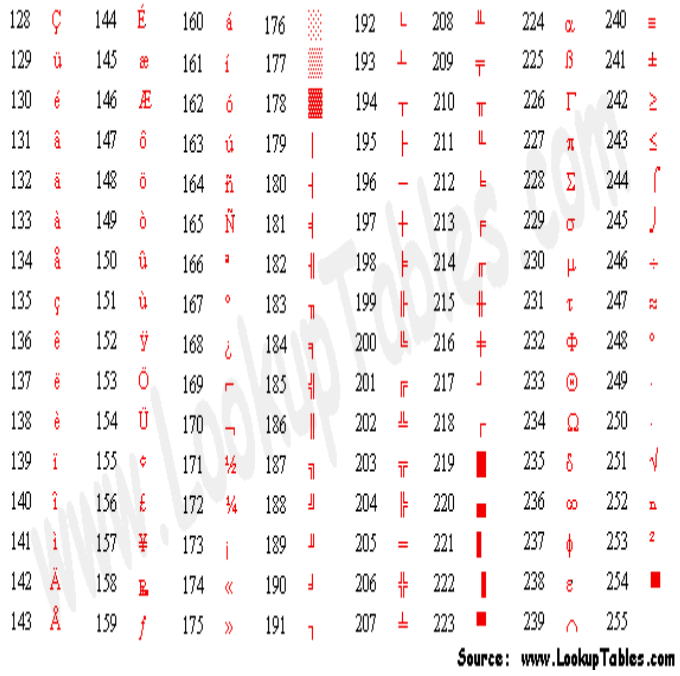


Figure 3. Three-Pass Protocol Process Scheme based on ASCII table
Source: http://www.asciitable.com

The *Vigenere cipher* is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution in which each alphabet can replace with several cipher alphabets [5]. The encoding by the *Vigenère matrix* is the type by substitution. It consists to employ a key composed by a word or by an expression. It utilizes a square composed by the alphabet 25 times in such way it signifies a square matrix where each cell contains a letter of the alphabet (it exists several variants of the matrix) [6]. Message is divided in blocks. Length's block is equal length's key K. Maximal Length of key **is** 208 bits (26*8=208). Key length then could be 128,192,256... for one matrix. To perform the encryption using *Vigenere Cipher* algorithm development required the following functions:

$$C_i = P_i + K_i \ mod\ 37 \qquad (1)$$

This function is then developed by multiplying each index to the value of 1st ciphertext (Ci1) with Encryption 1st ciphertext. Encryption 1st ciphertext (EnC1) is the sum of subrange with length of plaintext.

3.1. Cryptography

The word Cryptography is derived from the Greek, namely from word Cryptos meaning of the word hidden and graphein means writing. Cryptography can be interpreted as an art or a science which researched how the data is converted into a certain shape that is difficult to understand [1]. Cryptography aims to maintain the confidentiality of information or data that can not be known by unauthorized parties (unauthorized person)

Cryptography components

Basically, the cryptographic component consists of several components, such as:

1. Encryption: is very important in cryptography, is a way of securing the transmitted data that are kept confidential. The original message is called plaintext, which is converted into code that is not understood. Encryption can be interpreted with a cypher or code. Similarly, do not understand a word then we will see it in a dictionary or glossary. Unlike the case with encryption, to convert plain text into text-code we use algorithms to encode the data that we want.
2. Decryption: is the opposite of encryption. The encrypted message is returned to the original form (original text), called the message encryption algorithm used for encryption is different from the algorithm used for encryption.
3. Keywords: that means here is the key used for encryption and description.

Security of cryptographic algorithms depending on how the algorithm works, therefore this kind of algorithm is called finite algorithm. Limited algorithm is an algorithm used a group of people to keep the messages they send.

3.2. Vigenere Chiper

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution. [2]. The characters used in the Cipher Vigenere that is A, B, C, ..., Z and united with the numbers 0, 1, 2, ..., 25. The encryption process is done by writing the key repeatedly. Writing the key repeatedly performed until each character in messages have a couple of key characters. Furthermore, the characters in the message is encrypted using the Caesar Cipher key values that have been paired with numbers. The Confederacy's messages were far from secret and the Union regularly cracked their messages. Throughout the war, the Confederate leadership primarily relied upon three key phrases, "Manchester Bluff", "Complete Victory" and, as the war came to a close, "Come Retribution".[3] The table below show the example of encription using Vigenere Chiper consist of Plaintext, Key and Chipertextin Figure 4.

Plaintext	E	L	W	I	N		P	U	R	B	A		M	A	N	O	R	S	A
Key	M	A	N	O	R	S	A	M	A	N	O	R	S	A	M	A	N	O	R
Chipertext	R	M	K	X	F	S	Q	H	S	P	P	R	F	B	A	P	F	H	S

Figure 4. Examples Using Encryption Vigenere Cipher (Bruen, 2005)

Examples of encryption in Figure 1, the message character "**E**" is encrypted with a key "**M**" and generate cipher text "**R**". The results obtained from the code encrypting the message "**E**" is worth **5** and a key character "**M**" which is worth **13**. Each character value added **5 + 13 = 18**. Because **18** is less than the **26** which is the number of characters used, then **18** divided by **26**. The rest of the division is **18** which is a character "**R**". The encryption process can be calculated by the following equation (Stalling, 2011):

$$Ei=(Pi+Ki)\ mod\ 26 \qquad (2.0)$$

where ***Ei***, ***Pi*** and ***Ki*** an encrypted character, the character of the message and the character key. While the decryption process can use the following equation:

$$Di=(Ci-Ki)\ mod\ 26 \qquad (2.1)$$

with ***Di*** is the result of the decryption code, ***Ci*** is character cipher text or cipher, ***Ki*** is a key character. While other methods to perform the encryption process with Vigenere Cipher method that uses tabula recta (also called Vigenere square; Figure 5).

	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
a	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
b	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	A
c	C	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
d	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	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
j	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
k	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	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	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
t	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
u	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	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	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
y	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
z	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	Y

Figure 5. Tabula recta Vigenere algorithm.

The leftmost column of squares states key letters, while the top line states **plaintext letters**. Each line in the rectangle states the **letters ciphertext** obtained by Caesar Cipher, in which the number of shifts letter plaintext specified numerical values of letters that key (**ie, a = 0, b = 1, c = 2, ..., z = 25**) , Vigenère square is used to obtain the ciphertext by using a key that has been determined. If the key length is shorter than the length of the plaintext, then the key are repeated it's use (the periodic system). When the key length is **m**, then the period is said to be **m**.

3.3. Vernam Chiper

Cryptography for most people is something that is very difficult and we as beginners tend to be lazy to learn it. However there is a cryptographic method that is rather easy to learn and the experts have stated that this method is a cryptographic method that is safe enough to use. The method is commonly known by the name of One Time Pad (OTP) or better known as the Vernam Cipher [4]. Vernam Cipher invented by Major J. Maugborne and G. Vernam in 1917. Algorithms One Time Pad (OTP) is a diversified symetric key algorithm, which means that the key used to encrypt and decrypt the same key. In the process of encryption, algorithm it uses the stream cipher derived from the XOR between bits of plaintext and key bits. In this method, the plain text is converted into ASCII code and then subjected to an **XOR** operation on the key that has been converted into ASCII code.

3.4. One Time Pad

One-time pad (OTP) is a stream cipher to encrypt and decrypt one character each time [5]. This algorithm was found in 1917 by Major Joseph Mauborgne as improvement of Vernam Cipher to produce a perfect security. Mauborgne proposes the use of One-Time Pad containing a row of characters randomly generated key. One pad is used only once (one-time) only to encrypt a message, after the pad has been used demolished so as not be reused for other encrypting messages. Encryption can be expressed as the sum modulo 26 of the plaintext character with one key character one-time pad [6]. This is the equation of one-time pad encryption 26 characters shown in Equation 2.2 below:

$$Ci = (Pi + Ki) \bmod 26 \quad (2.2)$$

If the character that is used is a member of the set of 256 characters (such as characters with ASCII encoding), then the encryption equation shown in equation 2.3 below.

$$Pi = (Ci - Ki) \bmod 26 \quad (2.3)$$

After the sender encrypts the message with the key, he destroyed the key. Recipient of the message using the same pad to decrypt the ciphertext characters into characters plaintext with equation 2.4 below.

$$Pi = (Ci - Ki) \bmod 26 \quad (2.4)$$

for the 26-letter alphabet, or for the 256-character alphabet with equation 2.5 below.

$$Pi = (Ci - Ki) \bmod 256 \quad (2.5)$$

The ways of working one time pad method:

$$C = P \text{ XOR } K \quad (2.6)$$
$$P = C \text{ XOR } K \quad (2.7)$$

Note that the key length should be equal to the length of the plaintext, so there is no need to repeat the use of the key during the encryption process (as in vernam cipher).

3.5. Rotation Matrix

Rotation matrix is shifting ciphertext character that has been incorporated into the matrix column clockwise, along the defined distance of the key. How to determine the length of shifts and the number of shifts can be seen in the following Table 1 below:

Table 1. Calculation of Long Shifts in Matrix

Plaintext	E	L	W	I	N		P	U	R	B	A		M	A	N	O	R	S	A
Key	M	A	N	O	R	S	A	M	A	N	O	R	S	A	M	A	N	O	R
Chipertext	R	M	K	X	F	S	Q	H	S	P	P	R	F	B	A	P	F	H	S

Ki	M	A	N	O	R	S	A	
A = Dec(Ki)	77	65	78	79	82	83	65	(2.8)
B = A+C_{n-1}	76	90	91	79	83	87	70	(2.9)
C = A mod 26	25	13	0	1	4	5	13	(2.10)
D = B+C mod 26	23	25	13	2	9	14	5	(2.11)
Char	W	Y	M	B	I	N	E	
G = Dec(Char)	87	89	77	66	73	78	69	(2.12)
Rg = G mod 26	9	11	25	14	21	0	17	(2.13)

Explanation:
Ki : Key
A : Decimal ASCII value of the key characters
B : Results Summation with a decimal value key with the previous result (C).
C : The decimal value of a key character mod 26
D : Number of B + C mod 26

Char : The result of the shift in the index table alphabetic characters as much as the value of D
G : Decimal ASCII value of the key characters
Rg : Long shifts in the character matrix table

Whereas for the amount of shift is determined by the character key.

Forms of research conducted by the authors in this paper is a review of literature. The literature review is a framework, concepts, or orientation to perform the analysis and classification of facts collected in a study. Referral sources from books and journals, which are referred to in this paper are directly related to the object under researched, that is the plaintext encryption. The method of research that used in this paper is a flowchart. This method includes determining a model of encryption, the completion of the encryption algorithm, encryption simulation manufacture and analysis of simulation results encryption. Flowchart design simulations on complete this research can be seen in Figure 6.

Plain Text	E	L	W	I	N		P	U	R	B	A		M	A	N	O	R	S	A
Index Plaintext	5	12	23	9	14	0	16	21	18	2	1	0	13	1	14	15	18	19	1
Index Key	13	1	14	15	18	19	1	13	1	14	15	18	19	1	13	1	14	15	18
P + K mod 26	18	13	11	24	6	19	17	8	19	16	16	18	6	2	1	16	6	8	19
Cipertext_1	R	M	K	X	F	S	Q	H	S	P	P	R	F	B	A	P	F	H	S

Figure 6. Table Testing of Encryption Vigenere Cipher

Rotation Key Algorithm

Rotation key generation algorithm aims to improve the security of the plaintext by changing the keys into a new character. Furthermore, the new character is converted to decimal and then look for the value of the modulation to determine the length of a shift towards the characters in the matrix table. Consider the following Figure 7.

Key	M	A	N	O	R	S	A
A = ASCII Code	77	65	78	79	82	83	65
B = A + C(n-1)	76	90	91	79	83	87	70
C = Mod(ASCII Code)	25	13	0	1	4	5	13
D = Mod (B + C)	23	25	13	2	9	14	5
Chiper_Key	W	Y	M	B	I	N	E
X = ASCII Code	87	89	77	66	73	78	69
Y = Mod(X)	9	11	25	14	21	0	17
	RT 9	RT11	RT25	RT14	RT21	RT0	RT17

Figure 7. Process Key Algorithm determining Long Shifts on Matrix rotation

Rotation algorithm

In this process, all the characters ciphertext that has been generated on Vigenere Cipher algorithm written into the matrix table where condition matrix which must consist of a matrix of squares, where the number of rows equals the number of columns (Figure 8). To run this algorithm, first consider the following steps.

1. Write down all of the ciphertext into the matrix
2. The matrix will be formed must consist of the same number of rows and columns.
3. To define a matrix of rows and columns calculate the amount of n ciphertext; n = length of ciphertext.
4. If **0 < n <= 9**, it will form a **3 x 3** matrix.

   If **9 < n <= 16**, it will form a matrix of **4 x 4**

   If **16 < n <= 25**, it will form a matrix of **5 x 5,** etc.
5. If the matrix column empty, fill it with the alphabet from A until the empty column full of character.
6. Copy the first column then make a new ending column
7. After that copy the first line and then make a new ending line.
8. Make the first shift in which the shift length is determined by the rotation of key algorithms. Rotation matrix will end after reaching n MAX of keys.

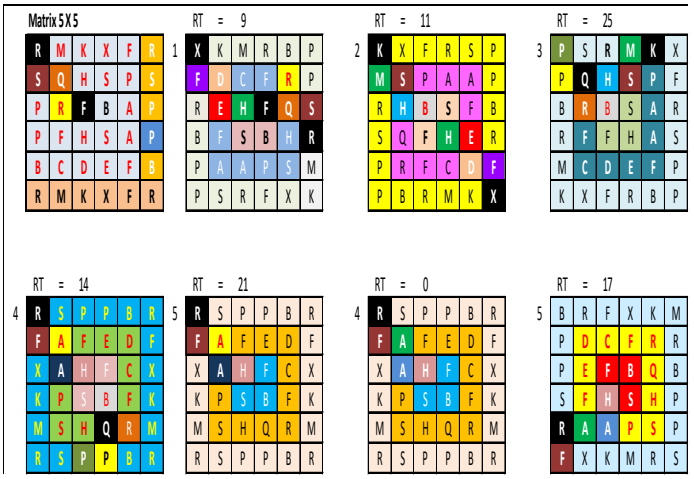


Figure 8. Process of Rotation Matrix

Retrieved end Cipertext:
BRFXKMPDCFRRPEFBQBSFHSHPRAAPSPFXKMS

Vernam Cipher

Encryption can be expressed as the result of the Exclusive OR (XOR) of the plaintext character with an OTP key characters. This algorithm acts to encrypt the plaintext where the key is generated randomly. This key is valid only disposable where if you want to decrypt the same message then the generated key will be changed.

One Time Pad

In this method, there are two things that need to be encrypted is the key and the ciphertext obtained from vigenere chipper. This method works in advance is change the main key with One Time Pad methode to produce the Ciphertext of the key then this key will be the **second key** or a **new key** (Figure 9).

Ei : Pi XOR Ki
The main key : MANORSA
Random key :
Key Ciphertext : "€ +« "n%

Plaintext	Binary Bit	Random Bit	XOR	Key
M	01001101	11100101	10101000	“
A	01000001	11000001	10000000	€
N	01001110	01100101	00101011	+
O	01001111	11100100	10101011	«
R	01010010	11111010	10101000	“
S	01010011	00111101	01101110	n
A	01000001	01100100	00100101	%

Figure 9. Encryption Results of Main Key

The next new key that has been generated is used to encrypt the ciphertext that has been obtained from vigenere cipher.

From the results of the main key encryption in the previous process we obtain a new key and then the key is repeated until the key length equal to the length of the plaintext. The result of the encryption of the plaintext and the key will be the end of the process to produce a strong ciphertext.

Plaintext : BRFXKMPDCFRRPEFBQBSFHSHPRAAPSPFXKMRS
Key :
“€+«“n%“€+«“n%“€+«“n%“€+«“n%“€+«“n%“

Ciphertext :
ÛÊm¾Ò#uý ├m¨·>`¯┬zÚ¹(m¹╚{¨Ú/u¹ðm¾Ò#w¹

The encryption process is represented in binary form :

Pi : 01000010 01010010 01000110
01011000 01001011
01001101
Ki : 10101000 10000000 00101011
10101011 10101000
01101110
Ci : 11101010 11010010 01101101
11110011 11100011
00100011

Pi : 01010000 01000100 01000011
01000110 01010010
01010010
Ki : 00100101 10101000 10000000
00101011 10101011
10101000
Ci : 01110101 11101100 11000011
01101101 11111001
11111010

Pi : 01010000 01000101 01000110
01000010 01010001
01000010
Ki : 01101110 00100101 10101000
10000000 00101011
10101011
Ci : 00111110 01100000 11101110
11000010 01111010
11101001

Pi : 01010011 01000110 01001000
01010011 01001000
01010000
Ki : 10101000 01101110 00100101
10101000 10000000
00101011
Ci : 11111011 00101000 01101101
11111011 11001000
01111011

Pi : 01010010 01000001 01000001
01010000 01010011
01010000
Ki : 10101011 10101000 01101110
00100101 10101000
10000000
Ci : 11111001 11101001 00101111
01110101 11111011
11010000

Pi : 01000110 01011000 01001011
01001101 01010010
01010011
Ki : 00101011 10101011 10101000
01101110 00100101
10101000
Ci : 01101101 11110011 11100011
00100011 01110111
11111011

Fig. 8 The encryption process with the one-time pad method

4. Results and Discussions

The results of encryption on this method obtain ciphertext to be sent to the recipient where there are two keys that are sent, among others, the key to decrypt the plaintext and the key to decrypt the key.

4.1. Description

One Time Pad

To know the plaintext from the ciphertext received by the rightful recipient of the message, that is by first using the one-time pad method. The message recipients require a new key as a reference to recover the plaintext.

Ciphertext :
ÛÊm¾Ò#uý ├m¨·>`¯┬zÚ¹(m¹╚{¨Ú/u¹ðm¾Ò#w¹
New Key : “€+«“n%

Ciphertext and the key then is XOR ed using the formula:

Di : Ci XOR Ki

The process of the message recipient to get a new message that is still in the form of Ciphertext are:

BRFXKMPDCFRRPEFBQBSFHSHPRAAPSPFXKMRS.

After successful decryption of the message recipient to decrypt back to find out the main key is still the one-time pad method.

Ciperteks key : “€+«“n%

Key : åÁeäú=d

Main Key = Ci XOR Ki

“ : 10101000	XOR	å : 11100101	=	01001101 : M
€ : 10000000	XOR	Á : 11000001		=01000001 : A
+ : 00101011	XOR	e : 01100101		=01001110 : N
« : 10101011	XOR	ä : 11100100		=01001111 : O
“ : 10101000	XOR	ú : 11111010		=01010010 : R
N : 01101110	XOR	=: 00111101		=01010011 : S
% : 00100101	XOR	d : 01100100		=01000001 : A

Main Key : MANORSA

Rotation algorithm

The next decryption algorithm is an algorithm in which the rotation that has been encrypted ciphertext of the previous methods to be put into a matrix table. See the Figure 10 below.

Ciphertext:
BRFXKMPDCFRRPEFBQBSFHSHPRAAPSPFXKMRS

B	R	F	X	K	M
P	D	C	F	R	R
P	E	F	B	Q	B
S	F	H	S	H	P
R	A	A	P	S	P
F	X	K	M	R	S

Figure 10. Matrix Ciphertext

In the previous encryption process, ciphertext character that is in the column of the matrix are moved forward along key value, but on the decryption algorithm ciphertext character that is in the matrix table is sliding backwards or revers along key value and repeated as much as the key length. The key value is obtained from the following process in the Figure 11 and Figure 12.

Key	M	A	N	O	R	S	A
A = ASCII Code	77	65	78	79	82	83	65
B = A + C(n-1)	76	90	91	79	83	87	70
C = Mod(ASCII Code)	25	13	0	1	4	5	13
D = Mod (B + C)	23	25	13	2	9	14	5
Chiper_Key	W	Y	M	B	I	N	E
X = ASCII Code	87	89	77	66	73	78	69
Y = Mod(X)	9	11	25	14	21	0	17
	RT 9	RT11	RT25	RT14	RT21	RT0	RT17

Figure 11. The process of determining the value of the key.

After a successful key value is determined next process is to do a rotation matrix algorithm.

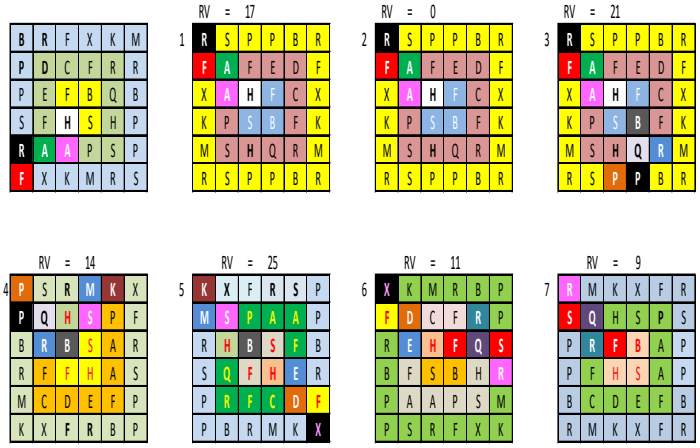


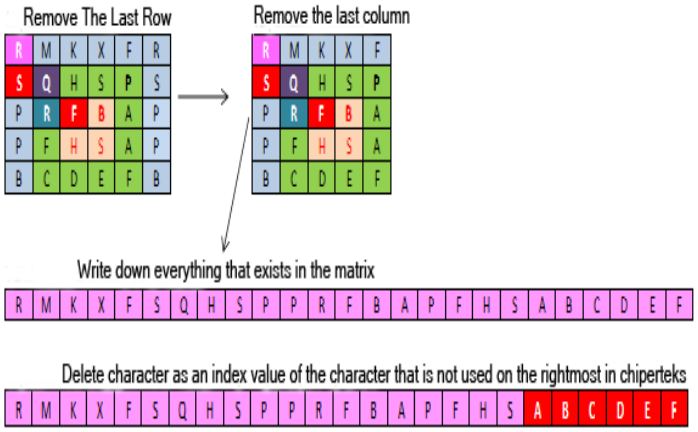
Figure 12. Process Description ciphertext with Matrix Ciphertext Algorithm

The results of the first rotation indicated at number one in the previous figure 10 wherein **R** is on the line five-column one. If we look at previous matrix characters that are in row one column one is **B**, then calculated spin clockwise as key values obtained from the previous process. The key value is taken values that are at the end of the index is **17**, the next process is the value at the previous index up until the beginning of the index, this is certainly the opposite of encryption algorithms. Having calculated the characters are on the order of **17** is **R** then **R** is placed on row one column one on the following matrix and is followed by the next character, then repeated continuously until the last process (Figure 13). In the process of this algorithm obtained the final matrix below:

R	M	K	X	F	R
S	Q	H	S	P	S
P	R	F	B	A	P
P	F	H	S	A	P
B	C	D	E	F	B
R	M	K	X	F	R

Figure 13. The Results of Algorithm Rotation Matrix

The next stage removes the last row and the last column of the matrix.



The Ciphertext become:

R	M	K	X	F	S	Q	H	S	P	P	R	F	B	A	P	F	H	S

Algoritma Vigenere

Last decryption algorithm using the algorithm vigenere cipher by using the key with formula:

$$Di = (Ci - Ki) \bmod 26$$

So the result we can see below:

Ciphertext : RMKXFSQHSPPRFBAPFHS
Key : MANORSAMANORSAMANOR
Plaintext : ELWIN PURBA MANORSA

R	M	K	X	F	S	Q	H	S	P	P	R	F	B	A	P	F	H	S
18	13	11	24	6	19	17	8	19	16	16	18	6	2	1	16	6	8	19
M	A	N	O	R	S	A	M	A	N	O	R	S	A	M	A	N	O	R
13	1	14	15	18	19	1	13	1	14	15	18	19	1	13	1	14	15	18
5	12	23	9	14	0	16	21	18	2	1	0	13	1	14	15	18	19	1
E	L	W	I	N		P	U	R	B	A		M	A	N	O	R	S	A

5. Conclusions

The encryption mechanism used in the present research is still modest or simple, but is expected to be useful as a first step to enter into the world of cryptography, particularly in the implementation of message security algorithms using other combinations. To the future, this research is expected to be developed, used and applied in the areas of life that is more complex.

References

[1] Zaeniah, Bambang Eka Purnama, "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm", *(IJACSA)* International Journal of Advanced Computer Science and Applications, 6(9), 2015.

[2] K Hashizume , "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open Journal: 1-13, 2013.

[3] Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri, "An Introduction to Information Security", National Institute of Standards and Technology Special Publication 800-12 Revision 1, 2017.

[4] William Stallings, "Cryptography and Network Security: Principles & Practices", Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.

[5] C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols," Journal of Computer Engineering (IOSRJCE) ISSN No: 2278-0661, 2012.

[6] Anuja Priyam, "Extended Vigenère using double Transposition Cipher with One Time Pad Cipher", Intl J Engg Sci Adv Research; 1(2):62-65, ISSN No: 2395-0730, 2015.

[7] Sundram Prabhadevi, Rahul De, Pratik Shah, "Cost Effective Poly Vernam Cipher With Cache Optimization", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, 2013.

[8] Shukla, R. and Prakash, H.O., "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem", *IEEE Conference:* International Conference on Machine Intelligence and Research Advancement 174-178, DOI: 10.1109/ICMIRA.2013.40, 2013.

[9] Borowski, M., Lesniewicz, M.,"Modern usage of old one-time pad", IEEE Conference :Communications and Information Systems: 1-5, ISBN:978-***1***-4673-1422-0, 2012

[10] Elwinus Mendrofa, Elwin Yunith Purba, Boy Yako Siahaan, Rahmad W Sembiring, "Manipulation Vigenere Cipher Algorithm With Vernam Cipher Trough Matrix Table Rotation", 2nd International Conference of Computer, Environment, Social Science, Health Science, Agriculture & Technology (ICEST), ISBN: 979-458-964-0, 2017.

[11] Aized Amin Soofi, Irfan Riaz, Umair Rasheed, "An Enhanced Vigenere Cipher For Data Security", International Journal Of Scientific & Technology Research 5(03), March 2016, ISSN:22778616.

[12] M. Rouse. (2007, Plain text. Available: http://searchsecurity.techtarget.com/definition/plaintext, 2017.

[13] T. Gunasundari and K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms," International Journal of Computer Science and Mobile Applications, ISSN no.2321-8363, 2014.

[14] Digital Economy Promotion Agency, under the Administrative Supervision of the Minister of Digital Economy and Society, 2016.

[15] Avialable at: —http://www.sipa.or.th", 2017.

[16] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4, pp. 877-882, 2012.

[17] V. Beal. (2009, Encryption. Available: http://www.webopedia.com/TERM/E/encryption.html, 2017.