Hybrid Methods of Ciphertext and RSA Cryptographic Algorithm Using Classical Vigenère

Siska Anraeni[a,1], Herdianti[a,2], Mursyid[b,3]

[a] *Moslem University of Indonesia, Urip Sumoharjo Street KM.05, Makassar 90231, Indonesia*
[b]*Sekolah Tinggi Ilmu Komputer Jayapura, Indonesia*
[1] *siska.anraeni@umi.ac.id;* [2] *herdianti.herdianti@umi.ac.id;* [3] *mursidjpr73@gmail.com*

ARTICLE INFO

Article History
Received March 18, 2016
Revised April 22, 2016
Accepted May 3, 2016

Keywords:
Cryptography
Encryption
Decryption
Vigenère Cipher
RSA

ABSTRACT

Maintaining the security of messages is a very important thing both within an organization and the personal especially in the age of information technology today. In order to the sent message does not fall into the one's hands who are not interested, then encryption should be created to maintain the confidentiality of a message remains secure. Classical cryptography method using Vigenère Cipher and RSA (Riverst Shamir Adleman) is one of securing methods which will be used. In this case, the initial process is doing encryption on Vigenère cipher that produces a temporary ciphertext. The temporary ciphertext will be a plaintext on the RSA algorithm and then encrypted again to produce the actual ciphertext. Merging these two methods produces a ciphertext that is more powerful and difficult to solve.

I. Introduction

Communication system security is a requirement that must be had by all parties involved in the system. Exchanging messages or information requires a high level of security, because security protects the messages or information in order not to be read by cryptanalysis and prevents cryptanalysis from modifying the message or information as well. Cryptographic technique is a manage messages or information security problems for a long time [1].

Nowadays, the development of computer technology of multi-user system is available where the data may be shared with other users in a computer network or in a wider network such as internet. Nevertheless, some data need privacy and should be kept confidential. These important data should be protected against irresponsible users, counterfeiting, theft and illegal data conversion [2].

Cryptography is the art and science of keeping messages secure. The word "art" is derived from the historical fact that in the early days of the history of cryptography, each person may have a unique way to conceal the message. The way to conceal the message may depend on each cryptographist and it has its own aesthetic value. The terms used in the field of cryptography including 1) Plaintext (P) is a message to be sent (containing the original data); 2) Ciphertext (C) is an encrypted message which is the result of the encryption; 3) Encryption (E function) is the process of converting plaintext into ciphertext; 4) Decryption (D function) is the opposite of encryption by transforming ciphertext into plaintext, so the preliminary data/original; and 5) The keyword is a secret number that is used in encryption and decryption.

Cryptography itself consists of two main processes namely the encryption and decryption process. As mentioned above, the process of changing plaintext into ciphertext encryption (using a certain keyword) so that the content of the information in the message is hard to understand. An illustration of the cryptographic process can be seen in Figure 1, the cryptographic mechanisms [3].

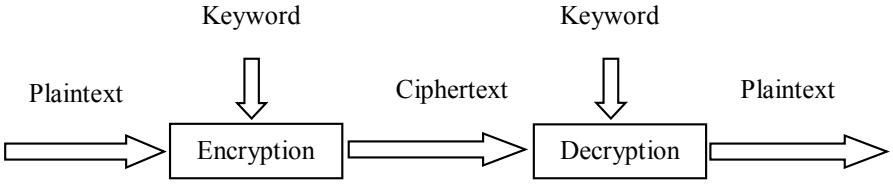

Fig.1. The Cryptographic Mechanism

II. Literature Review

A. Vigenère Cipher

Vigenère cipher method is a part of classical cryptographis. Vigenère name is taken from a man named Blaise de Vigenère. Vigenère cipher is an example of the "manual" cipher compound-alphabet published by a France diplomat (a cryptologist as well), Blaise de Vigenère in the 16th century. Despite of Giovan Battista bellaso have described it first in 1553 as written in his book La Cifra del Sig, but this new algorithm is widely known 200 years later and called Vigenère cipher. This cipher successfully solved by Babbage's and Kasiski in the mid-19th century. Vigenère cipher method is very well known because in addition to using a mathematical formula, using Vigenère square cipher for encryption and decryption. Vigenère square is used to obtain ciphertext by using a keyword that has been determined, Table 1. If the keyword's length is shorter than the length of the plaintext, the keyword is repeated (the periodic system). The encryption with Vigenère cipher use a Vigenère square by dragging a vertical line from the plaintext letter down, then pulling a horizontal line of the letter keywords to the right hand. The intersection of the two lines states the ciphertext letter. Vigenère cipher decryption is done by the opposite way means drawing a horizontal line from letter to the ciphertext letter, and then pull a vertical line to the plaintext letter. Mathematically, suppose the keyword is a series of K_1,K_2,...,K_i, the plaintext is a circuit P_1,P_2,...,P_i, and ciphertext is a circuit of C_1,C_2,...C_i, so that the Vigenère cipher encryption can be expressed:

C_i=(P_i+K_i) mod 26 or C_i=(P_i+K_i)-26, if (P_i+K_i) more than 26 (1)

Decryption mathematically expressed by changing the equation (1), which can be expressed by:

P_i=(C_i-K_i) mod 26 or P_i=(C_i-K_i)+ 26, if (Ci <= Ki) (2)

Information:

C_i = decimal value of ciphertext character to i

P_i = decimal value of plaintext character to i

K_i = decimal value of keyword character to i

Table 1. Table of Longitude Cage Vigenère

		Plaintext																								
		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
K e y	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
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The weakness of the Vigenère cipher algorithm i.e. if the length of the keyword used is less than the length of the plaintext. Less the length of the keyword to the plaintext cause the keywords will be repeated until the keyword length equals to the length of the plaintext. This leads to the possibility of repetition in the ciphertext encrypted string that can be used to find the length of the keyword and further utilized to solve the ciphertext [7]. The first person who managed to find a weakness Vigenère cipher and solve the ciphertext is Friedreich Kasiski in 1863 called Kasiski method [4]. The advantages of Vigenère cipher algorithm is easy to understand how it works. Characteristic of each letter cipher is the ciphertext can have many possibilities for the plaintext letter.

B. RSA (Rivest, Shamir, Adleman)

RSA is an asymmetric cryptographic algorithm discovered in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA name itself is taken from the initials of the inventors of the third front. As a public keyword algorithm, RSA has two keywords, a public keyword and a private keyword. The public keyword may be known by anyone, and is used for the encryption process. While only the private keyword - certain parties who may be informed, and use for the decryption process.

RSA Security password lies in the difficulty of factoring large numbers. Until now RSA is still trusted and widely used on the Internet [4].

Coding scheme of RSA public keyword algorithm consists of three processes, namely generation process of the keywords, encryption, and decryption process. Previously awarded advance some of the concepts of mathematical calculations used RSA [5].

1. Generation process of the keys:
   Generate two random primes p and q and be random and concealed where $p \neq q$. Let $n = p \times q$, where n is known as RSA modulo. Compute $\varphi(n) = (p-1)(q-1)$.
   Determine e random prime, which satisfies: $1 < e < \varphi(n)$. $GCD(e, \varphi(n)) = 1$, called e relatively prime to (n), integer e is called (RSA) enciphering exponent.
   With the extended Euclid algorithm, Count the special number of d by the formula
   $d \equiv e - 1 \; mod \; \varphi(n)$
   $ed \equiv 1(mod \; \varphi(n))$
   $ed \equiv 1 + k.\varphi(n)$ for integer k, which satisfies $1 < d < \varphi(n)$.
   Integer d is called (RSA) deciphering exponent. Note that n, e are public keys and d, p, q are the secret keys.
2. Encryption:
   We encrypt the plaintext by the equation:
   $$C = M^e \; (mod \; n)$$
3. Decryption:
   We decrypt the ciphertext by the equation:
   $$M = C^d \; (mod \; n)$$
   where, M denotes the message/ plaintext and C is ciphertext [6].

III. Method

The encryption process and a description using the Vigenère cipher strengthened by RSA, conducted in four stages as shown in (Figure 2).

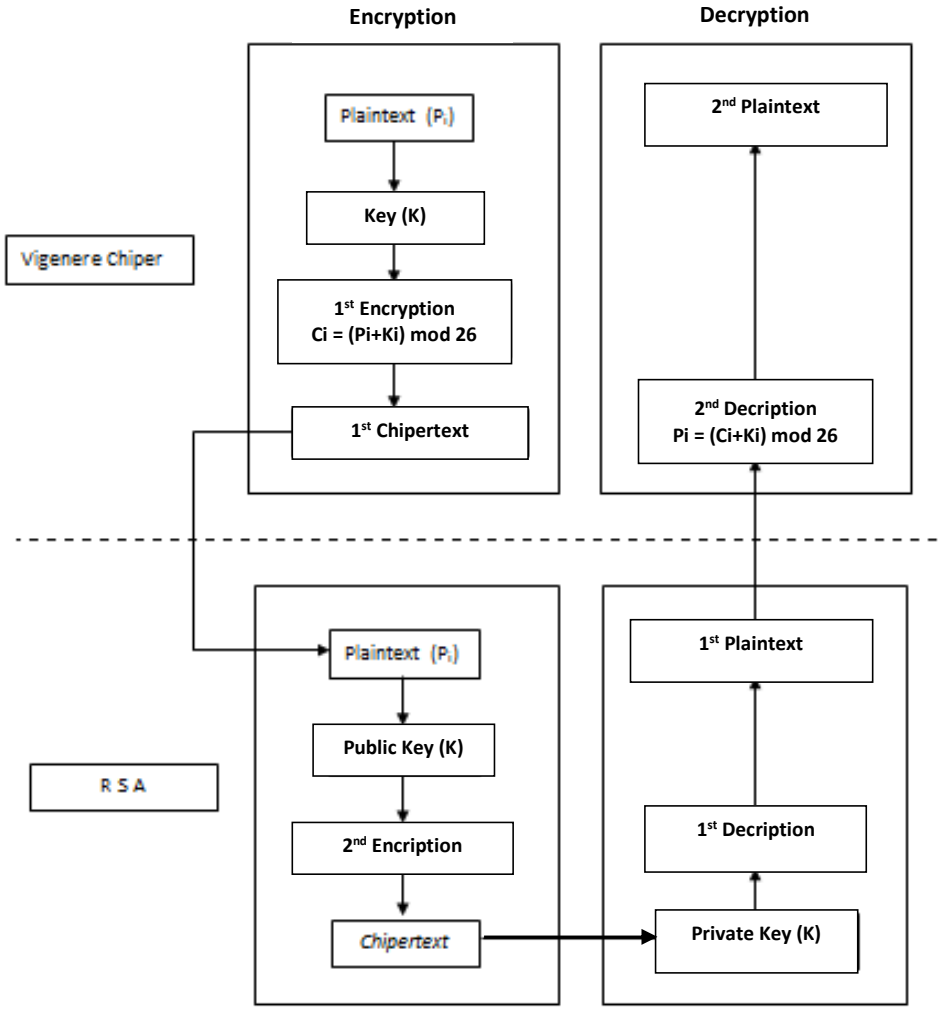

Fig.2. Flow of Vigenère Encryption and Decryption Using Cipher and RSA processes

IV. Results

A. First Encryption Process Using Vigenère Cipher

Plaintext: KEAMANAN KOMPUTER

Keyword: pasca

The plaintexts with the keyword above were obtained:

Table 2. The Plaintext and Keyword

Plaintext	K	E	A	M	A	N	A	N	K	O	M	P	U	T	E	R
Keyword	p	a	S	C	a	p	A	s	c	a	p	a	s	c	a	p
Ciphertext 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
Value	25	4	18	14	0	25	0	5	11	14	1	15	12	21	4	6

1st Solution:

In the example above keyword "PASCA" is repeated periodically until the keyword length equals the length of the plaintext. If calculated by the formula Vigenère encryption, plaintext first letter K (which has a value of P_i = 10) will be shifting with the letter P (which had a $K\_i = 15$), then proceed as follows:

$$\boldsymbol{C_i = (P_i + K_i)\ mod\ 26}$$
$$\boldsymbol{= (10 + 15)\ mod\ 26}$$

$= \mathbf{25}\ \boldsymbol{mod}\ \mathbf{26}$

$= \mathbf{25}$

$\boldsymbol{C_i} = \mathbf{25}$, then the ciphertext letter with a value of 25 is Z. And so on is done in accordance with the shift keyword on any letter to all encrypted plaintext into ciphertext. Once all the letters encrypted, then the decryption process can be calculated as follows:

$\boldsymbol{P_i} = (\boldsymbol{C_i} - \boldsymbol{K_i})\ \boldsymbol{mod}\ \mathbf{26}$

$= (\mathbf{25} - \mathbf{15})\ \boldsymbol{mod}\ \mathbf{26}$

$= \mathbf{10}\ \boldsymbol{mod}\ \mathbf{26}$

$= \mathbf{10}$

$\boldsymbol{P_i} = \mathbf{10}$, then the plaintext letter with a value of 10 is K. And so on is done in accordance with the shift keyword on any letter to all ciphertext has been decrypted into plaintext.

2nd Solution:

The first plaintext letter *N* (which has a value of $P_i = 13$) will be shifting with the letter S (which has $K_i = 18$), then proceed as follows :

$\boldsymbol{C_i} = (\boldsymbol{P_i} + \boldsymbol{K_i})\ \boldsymbol{mod}\ \mathbf{26}$

$= (\mathbf{13} + \mathbf{18})\ \boldsymbol{mod}\ \mathbf{26}$

$= \mathbf{31}\ \boldsymbol{mod}\ \mathbf{26}$

$= \mathbf{5}$

$\boldsymbol{C_i} = \mathbf{5}$, then the ciphertext letter with value of 5 is F. And so on is done in accordance with the shift keyword on any letter to all encrypted plaintext into ciphertext. Once all the letters encrypted, then the decryption process can be calculated as follows:

$\boldsymbol{Pi} = (\boldsymbol{Ci} - \boldsymbol{Ki})\ \boldsymbol{mod}\ \mathbf{26}$

$= (\mathbf{5} - \mathbf{18} + \mathbf{26}$

$= -\mathbf{13} + \mathbf{26}$ // summed with 26 for $C_i \leq K_i$

$= \mathbf{13}$

$\boldsymbol{P_i} = \mathbf{13}$, then the plaintext letter with a value of 13 is N. And so on is done in accordance with the shift keyword on any letter to all ciphertext has been decrypted into plaintext.

B. Second Encription Process Using RSA Method

First seek public keyword and private keyword by taking any two primes.

For Example: $p = 31;\ q = 37$

1. $N = p.q = (31)(37) = 1147$

   $\varphi(N) = (p - 1)(q - 1) = (31 - 1)(37 - 1) = (30)(36) = 1080$

2. Menentukan Public keyword : $e < 1080, e > 1$

   - $e = 13$
   - $ed = 1\ (mod\ \phi(N))$

     $13d = 1\ mod\ 1080$

Use the extended Euclid algorithm to get d:

Table 3. The Extended Euclid Algorithm

k	0	1	2	3
r_k	1080	13	1	0
q_k		83	13	
s_k	1	0	1	
t_k	0	1	−83	

According to theorem"$If\ 0 \leq k \leq n + 1$, then$r_k = s_k a + t_k b$":

$(1)(1080) + (-83)(13) = 1\ mod\ 1080$

$(-83)(13) = 1\ mod\ 1080$

$d = -83\ or\ 997$

- So, Public Keyword = $(e, N) = (13, 1147)$

  Private Keyword = $(d, N) = (997, 1147)$

3. 1st Ciphertext of Vigenère encryption results (m) = ZESOACAFMOBPMVAG

Table 4. The ASCII Code of 1st Chipertext

Ciphertext 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
ASCII Code	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71

m broken down into eleven blocks measuring 3 digits:

$m_1 = 906$ $m_2 = 983$ $m_3 = 796$ $m_4 = 567$ $m_5 = 657$ $m_6 = 077$

$m_7 = 796$ $m_8 = 680$ $m_9 = 778$ $m_{10} = 665$ $m_{11} = 71$

Encryption process using the Public Keyword (e,N) = (13 , 1147)

$c = m^e \, mod \, N$

$c1 = m_1^e \, mod \, N = 90613 \, mod \, 1147 = 143$

$c2 = m_2^e \, mod \, N = 98313 \, mod \, 1147 = 509$

$c3 = m_3^e \, mod \, N = 79613 \, mod \, 1147 = 301$

$c4 = m_4^e \, mod \, N = 56713 \, mod \, 1147 = 793$

$c5 = m_5^e \, mod \, N = 65713 \, mod \, 1147 = 99$

$c6 = m_6^e \, mod \, N = 07713 \, mod \, 1147 = 585$

$c7 = m_7^e \, mod \, N = 79613 \, mod \, 1147 = 301$

$c8 = m_8^e \, mod \, N = 68013 \, mod \, 1147 = 643$

$c9 = m_9^e \, mod \, N = 77813 \, mod \, 1147 = 334$

$c10 = m_{10}^e \, mod \, N = 66513 \, mod \, 1147 = 369$

$c11 = m8e \, mod \, N = 7113 \, mod \, 1147 = 266$

Then, ciphertext end produced are:

c = 143 509 301 793 99 585 301 643 334 369 266

Table 5. The 2nd Chipertext

Ascii Code	**14**	**35**	**09**	**30**	**17**	**93**	**99**	**58**	**53**	**01**	**64**	**33**	**34**	**36**	**92**	**66**
Ciphertext 2	**<SO>**	**#**	**<TAB>**	**<RS>**	**<DC1>**	**]**	**c**	**:**	**5**	**<SOH>**	**@**	**!**	**“**	**$**	****	**B**

C. The First Decription Process Using RSA Method

The second ciphertext messages in ASCII code = 143 509 301 793 99 585 301 643 334 369 266

Private Keyword = (d,N) = (997 , 1147)

$m = c^d \bmod N$

$m_1 = c_1^d \bmod N = 143^{997} \bmod 1147 = 906$

$m_2 = c_2^d \bmod N = 509^{997} \bmod 1147 = 983$

$m_3 = c_3^d \bmod N = 301^{997} \bmod 1147 = 796$

$m_4 = c_4^d \bmod N = 793^{997} \bmod 1147 = 567$

$m_5 = c_5^d \bmod N = 99^{997} \bmod 1147 = 657$

$m_6 = c_6^d \bmod N = 585^{997} \bmod 1147 = 077$

$m_7 = c_7^d \bmod N = 301^{997} \bmod 1147 = 796$

$m_8 = c_8^d \bmod N = 643^{997} \bmod 1147 = 680$

$m_9 = c_9^d \bmod N = 334^{997} \bmod 1147 = 778$

$m_{10} = c_{10}^d \bmod N = 369^{997} \bmod 1147 = 665$

$m_{11} = c_{11}^d \bmod N = 266^{997} \bmod 1147 = 71$

The obtained message (plaintext) or decryption first in what will be in the decrypted again with Vigenère Cipher to get the actual plaintext:

m = 906 983 796 567 657 077 796 680 778 665

Table 6. The 1st Plaintext

ASCII code	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71
Plaintext 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G

D. The Second Decription Process Using Vigenère Cipher Method

The description of the RSA method, here in after be described again using Vigenère Cipher.

Table 7. The Second Decription Process Using Vigenère Cipher Method

ASCII code	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71
Ciphertext 2	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
Keyword	P	A	S	C	A	P	A	S	C	A	P	A	S	C	A	P
Value	10	4	0	12	0	13	0	13	10	14	12	15	20	19	4	17
Plaintext	K	E	A	M	A	N	A	N	K	O	M	P	U	T	E	R

Solution of searching **K** letter:

$\mathbf{P_i = (C_i - K_i) \bmod 26}$

$\mathbf{= (25 - 15) \bmod 26}$

$\mathbf{= 10 \bmod 26}$

= 10, is the K (See Table 1)

Solution of searching **N** letter:

$\mathbf{P_i = (C_i - K_i) \bmod 26}$

$\mathbf{= (2 - 15) + 26}$

$\mathbf{= -13 + 26}$

= 13, is the N (See Table 1)

V. Conclusion and Recommendation

The conclusions of this study are as follows:

1. Vigenère cipher with a shorter keyword than the plaintext provided greater risk to be solved. The method used to solve ciphertext of Vigenère is known as Kasiski method.
2. RSA with two keywords of public keyword and private keyword are able to provide security messages more.
3. Combination of Vigenère Cipher and RSA method produces stronger ciphertext i.e. with twice the process of encoding (encryption) and twice the process of decryption then it could provide the level of security messages that are more secure and difficult to solve.

Recommendation in this study is to work on further development with several things to consider:

1. This method could be aplly on massages security system.
2. This method could be combining with the other algorithm.

References

[1] Juliadi, Bayu Prihandono, Nilamsari Kusumastuti. Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat dengan Vigenère Cipher. Volume 02, No. 2 (2013), hal 87– 92. 2013.

[2] Erna Kumalasari Nurnawati. Analisis Kriptografi Menggunakan Algoritma Vigenère Cipher Dengan Mode Operasi Cipher Block Chaining (CBC). Seminar Nasional Aplikasi Sains Dan Teknologi. 2008.

[3] Putu H. Arjana1, Tri Puji Rahayu , Yakub, Hariyanto. Implementasi Enkripsi Data Dengan Algoritma Vigenère Cipher. Yogyakarta, 10 Maret 2012.

[4] Riyanto, M. Zaki., & Ardhi Ardian. Kriptografi Kunci Publik: Sandi RSA. 2008. http://sandi.math.web.id, accessed on February 13,2016.

[5] Mollin, Richard A. RSA and Public-Keyword Cryptography. Florida, BocaRaton: CRC Press LLC. 2002.

[6] Takagi, Tsuyoshi. "Fast RSA-type cryptosystem modulo p k q", Advances in Cryptology — CRYPTO '98, pp (318-325). 1998.

[7] Jawahir, Ahmad and Haviluddin. An audio encryption using transposition method. International Journal of Advances in Intelligent Informatics, Vol 1, No 2, July 2015, pp. 98-106. ISSN: 2442-6571