International Journal of Artificial Intelligence & Robotics (IJAIR) E- ISSN: 2686-6269
Vol.1 No.1, 2019, pp.26-32

Modified Vegenere Cipher to Enhance Data Security Using Monoalphabetic Cipher

Siti Agustini[1]*, Weny Mistarika Rahmawati[2], Muchamad Kurniawan[3]
[a,b]Institut Teknologi Adhi Tama Surabaya, Jl.Arief Rahman Hakim No.100, Indonesia
[a]sitiagustini@itats.ac.id*; [2]wenymistarika@gmail.com; [3]muchamad.kurniawan@itats.ac.id
*corresponding author

ABSTRACT

The rapid progression of exchange data by public networks is important, especially in information security. We need to keep our information safe from attackers or intruders. Furthermore, information security becomes needed for us. Many kind cipher methods of cryptography are improved to secure information such as monoalphabetic cipher and polyalphabetic cipher. Cryptography makes readable messages becoming non-readable messages. One of the popular algorithms of a polyalphabetic cipher is Vigenere cipher. Vigenere cipher has been used for a long time, but this algorithm has weaknesses. The calculation of the encryption process is only involving additive cipher, it makes this algorithm vulnerability to attacker based on frequency analysis of the letter. The proposed method of this research is making Vigenere cipher more complex by combining monoalphabetic cipher and Vigenere cipher. One of the monoalphabetic ciphers is Affine cipher. Affine cipher has two steps in the encryption process that are an additive cipher and a multiplicative cipher. Our proposed method has been simulated with Matlab. We also tested the vulnerability of the result of encryption by Vigenere Analyzer and Analysis Monoalphabetic Substitution. It shows that our method overcomes the weakness of Vigenere Cipher. Vigenere cipher and Affine cipher are classical cryptography that has a simple algorithm of cryptography. By combining Vigenere cipher and Affine cipher will make a new method that more complex algorithm.

Keywords: Monoalphabet cipher; Polyalphabet cipher; Vigenere cipher, Matlab

I. INTRODUCTION

Problems related to data or information security are issues that have existed since ancient times until now. Confidential information must be kept secure in the contents of the data so it cannot be accessed by parties who are not entitled to the information. There have been many examples of cases such as tapping into conversations or leaking company information. These cases give the message that securing data or information is very important to implement and has become a major requirement for many parties.

Data or information security is closely related to cryptography. According to Schneier, cryptography is the art and science of keeping messages secure [1]. Meanwhile, according to Menez, the definition of cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, authentication, and data integrity [2]. Cryptography techniques have been developed since ancient times (classical cryptography) until now (modern cryptography). Cryptography has been widely implemented in several fields such as e-commerce, telecommunications, commerce, and even government.

Classical Cryptography has two basic ciphers namely substitutions and transpositions. Substitution ciphers work by replacing each plaintext unit with another. Plaintext consisting of an alphabet can be replaced with another alphabet. Cipher substitution can be classified into 2 groups, namely monoalphabetic substitution, and polyalphabetic substitution. Monoalphabetic substitution places each alphabet in the plaintext having exactly 1 other alphabet (one-to-one). Caesar cipher, multiplicative cipher, the shift cipher, and Affine cipher are monoalphabetic ciphers. Polyalphabetic substitution places 1 plaintext alphabet in several alphabets to become a ciphertext. Polyalphabetic substitution algorithms include Vigenere cipher, Playfair cipher, Beaufort cipher, hill cipher [3].

Vigenere cipher is an alphabet encryption method. Vigenere cipher uses encryption based on the Vigenere cipher table which reflects the polyalphabetic nature. Vigenere cipher encrypts where the first character in the plaintext is encrypted with the first character on the key and so on. However, if the key length of the alphabet is shorter than the plaintext, the key will be repeated until the length is the same as the plaintext. This key loop can also be a weakness of this method. Cryptanalysis using the alphabetical frequency will be able to solve the ciphertext results from the vigenere cipher. In addition, the encryption process is fairly simple. In 1863, Riedrich Kasiski was developed cryptanalyst research of repeated text segments in the ciphertext of at least 3 characters [4]. Searching the repeated character can know the length of key. Then take the gcd (great common divisor) to all distance between characters. So, the length of the key is the multiple of great common divisor.

The purpose of this study is to resolve the weaknesses of the algorithm. This study combines vigenere cipher and monoalphabetic cipher, affine cipher. The combination of these two techniques makes the encryption technique with complex transformations to convert plaintext to ciphertext. The combination of vigenere cipher and affine cipher is expected to increase data security in public communication networks.

 DOI: 10.25139/ijair.v1i1.2029

II. METHOD

A. Vigenere Cipher

Vigenere cipher is one of the best in the polyalphabetic cipher group which uses a matrix of 26 by 26 Caesar cipher shift [5]. This algorithm is also very popular because it is easy to understand and to be applied. Vigenere cipher uses a table as a guide to simplify the encryption process. The Vigenere cipher table contains the alphabet where the first line is the alphabet of the plaintext while the first column is the alphabet of the key. To find out the results of encryption only need to draw lines in the rows from the plaintext and columns from the key. The intersection of the two lines represents the ciphertext letter. For example, as in Figure 1, which is the process of encrypting plaintext with the alphabet T and key I. When a line is drawn from the two alphabets, the intersection is in alphabet B so that B can be expressed as ciphertext.

For example, plain text "indonesia adalah negara" with keyword 'mobil'". If the key length is shorter than plaintext so the key must be repeated at encryption. So, it becomes like this:

Plain text: `indonesiaadalahnegara`

Key: `mobilmobilmobilmobilm`

The same way that is to draw a line between the plaintext and the key so that the intersection is obtained. The results of all the encryption are:

Plaintext : `indonesiaadalahnegara`

Key: `mobilmobilmobilmobilm`

Ciphertext: `UBEWYQGJILPOMISZSHICM`

The encryption and decryption process of Vigenere Cipher in formulated in mathematical equations. Suppose the key is used along m then $k_1, k_2, k_3, \ldots, k_m$, plain text is the sequence of alphabets $p_1, p_2, p_3, \ldots, p_m$, and ciphertext is sequence of $c_1, c_2, \ldots, c_m$. Key, plaintext, and ciphertext are satisfied by equation below [6]:

$$C = e_k(c_1, c_2, \ldots, c_m) = (p_1+k_1, p_2+k_2, \ldots, p_m+k_m) \bmod 26 \quad (1)$$

$$P = d_k(p_1, p_2, \ldots, p_m) = (c_1-k_1, c_2-k_2, \ldots, c_m-p_k) \bmod 26 \quad (2)$$

	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 1. Encryption of plaintext "T" and key "I"

Another way to perform Vigenere cipher is by mapping all of the alphabets into an index [7] as seen in Table 1. For the encryption process, change the key and plaintext as Table 1. Use additive operation for index key and plaintext. If plaintext is longer than key, the repeat the key for the additive process. Last, convert the result of the additive process into alphabet as seen in Table 1. For example:

Table 1. Transformation of the alphabet into index

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
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

DOI: 10.25139/ijair.v1i1.2029

Plaintext : indonesiaadalahnegara
Kunci : mobilmobilmobilmobilm
Index of plaintext : 8 13 3 14 13 4 18 0 0 3 0 0 11 0 7 13 3 6 0 17 0
Index of key : 12 14 1 8 11 12 14 1 8 11 12 14 1 8 11 12 14 1 8 11 12

mod 26 : 20 27 4 22 24 16 32 1 8 14 12 14 12 8 18 25 17 7 8 28 12
Ciphertext: UBEWYQGJILPOMISZSHICM

B. Affine Cipher

Affine Cipher is an algorithm of the monoalphabetic cipher. This algorithm maps each alphabet with one other alphabet and vice versa for the decryption process. Affine cipher combines multiplicative and additive cipher with a pair of keys. The first key is used for multiplicative cipher while the second key is used for additive cipher [8]. The first key and the second key are numbers. The two keys are distributed between the sender and receiver. Mathematic model of the encryption process can be formulated as follows:

$$C = ((P \times k_1)+k_2) \bmod n \quad (3)$$

Equation (3) shows that there are two processes in encryption namely the alphabet plaintext multiplied by the first key. The results are then added to the second key. The modular process with mod n where n is the number of the alphabet, which is 26. So that equation (3) can be rewritten as equation (4).

$$C = ((P \times k_1)+k_2) \bmod 26 \quad (4)$$

The decryption process is the reverse process of encryption so that it can be defined mathematically like equation (5).

$$P = ((C - k_2) \times k_1^{-1}) \bmod n \quad (5)$$

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26 \quad (6)$$

In the decryption process there is a modular multiplicative inverse of k_1^{-1} mod 26 in Figure 2. Modular multiplicative inverse can be formulated as:

$$1 \equiv k_1.k_1^{-1} \bmod 26 \quad (7)$$

$$k_1.x = 1 \bmod 26 \quad (8)$$

$$k_1.x = 1 + 26.y \quad (9)$$

$$x = \frac{1+26.y}{k_1} \quad (10)$$

Equation (7) can be fulfilled if k_1 and n are coprime [6].

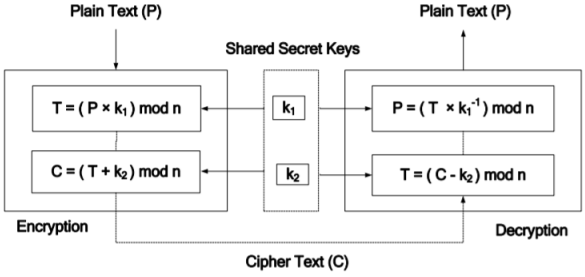

Fig. 2. Affine Cipher

C. Proposed Method

This research focuses on the application of encryption using Vigenere cipher an Affine cipher. In addition, the encryption and decryption process are simulated with MATLAB. With the Affine cipher implemented, the encryption and decryption process is more complex. The relationship between plaintext and ciphertext will be hiding. It makes it difficult to find the text by ciphertext statistical analysis. In addition, it will be very difficult to determine the key because it is difficult to find the relationship between the key and the ciphertext. Materially, the proposed method can be written as follows for the encryption process:

$$C_i = ((p_i \times fk_i)+sk_i) \bmod n \quad (11)$$

$$C = ((p_1 \times fk_1)+sk_2, (p_1 \times fk_1)+sk_2, \ldots\ldots, (p_m \times fk_m)+sk_m) \bmod n \quad (12)$$

The decryption process follows the following equation:

$$P_i = ((C_i - sk_i) \times fk_i^{-1}) \bmod n \quad (13)$$

$$fk_i^{-1} \bmod n \quad (14)$$

$$1 \equiv fk_1.fk_1^{-1} \bmod n \quad (15)$$

DOI: 10.25139/ijair.v1i1.2029

where :
$C_i = C_1, C_2 \ldots C_m$ (Ciphertext)
$p_i = p_1, p_2 \ldots p_m$ (Plaintext)
$fk_i = = fk_1, fk_2 \ldots fk_m$ (First key stream)
$sk_i = = sk_1, sk_2 \ldots sk_m$ (second key stream)
$fk_i^{-1} mod\ n$ = *modular multiplicative inverse*

the workflow of the combination of the two algorithms can be seen in the pseudo-code below:

%%Encryption%%

```
1. find index of plaintext P, key1 K1, key2 K2.
2. compute encryption C, where i start from 1,
   x = P(i)*K1(i)+K2(i)
   C = x mod 26
3. loop process number 2, while i <= length plaintext
4. change format of C to String -> cipher text
```

%%Decryption%%

```
1. find index of Ciphertext C, key1 K1, key2 K2.
2. compute value Decryption D, where i start from 1
   x = C(i)-K2(i)*InversMod(K2(i))
   D = x mod 26
3. loop process number 2, while i <= length C
4. change format C to String -> plaintext
```

III. RESULT AND DISCUSSION

We have simulated the combination of Vigenere cipher and Affine cipher with Matlab. The result can be shown in figure 3. In the first simulation, the plaintext is "aan", first keystream is "one" and second keystream is "dua". This algorithm will begin encryption start from first character (plaintext, first key, and second key) then second character (plaintext, first key, and second key) and so on. Encryption process begins with multiplicative cipher between first character of plaintext "a" and first key "s". We did the multiplicative by changing the character into index as seen in Table 2 and Table 3. Then, the result of multiplicative process is enciphered into additive cipher with second key. Finally, we get the encrypted character of "a", that is character "d". The decryption process is following equation (14). For example, decryption process of character "d" which is first key = "s" and second key="d". In decryption process, we also have to change the character into index for easy calculation. The first step in solving the modular implicative inverse of second key's index. The second step is subtraction between index ciphertext character "d" and first key index.

Table 2. Transformation of character into index

Plaintext	a	a	n	
Index	0	0	13	
First key	s	a	t	u
Index	18	0	19	20
Second key	d	u	a	
Index	3	20	0	

Table 3. Algebraic Encryption and Decryption

Character	First key	Second key	Encryption	Decryption
a	s	d	$C(a) = \big((0 \times 18) + 3\big) mod\ 26$ $C(a) = 3\ mod\ 26$ $C(a) = 3$ $C(a) = d$	$P(d) = ((3-3) \times 18^{-1}) mod\ 26$ $P(d) = 0$ $P(d) = a$
a	a	u	$C(a) = \big((0 \times 0) + 20\big) mod\ 26$ $C(a) = 20\ mod\ 26$ $C(a) = 20$ $C(a) = u$	$P(u) = ((20-20) \times 0^{-1}) mod\ 26$ $P(u) = 0$ $P(u) = a$
n	t	a	$C(n) = \big((13 \times 19) + 0\big) mod\ 26$ $C(a) = 247\ mod\ 26$ $C(a) = 13$ $C(a) = n$	$P(n) = ((13-0) \times 19^{-1}) mod\ 26$ $P(u) = (13 \times 11) mod\ 26$ $P(u) = 13$ $P(u) = n$

DOI: 10.25139/ijair.v1i1.2029

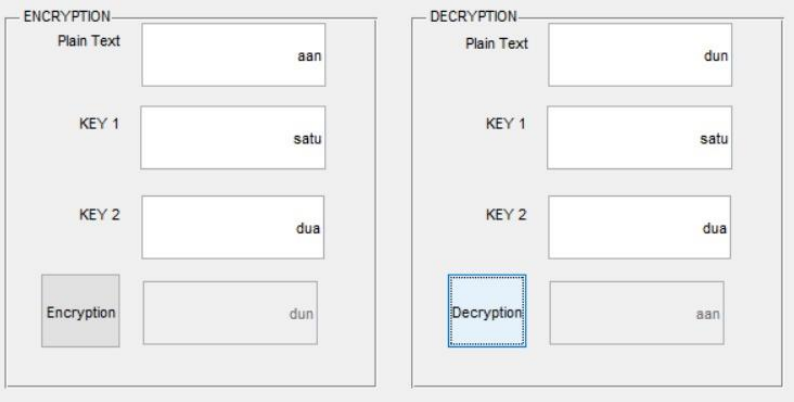

Fig. 3. First simulation: Cryptography by combination of Vigenere Cipher and Affine Cipher

In the second simulation, we used the plaintext “cryptography”. The first keystream is southwest Asia and the second keystream is Indonesia Jaya. With these keys, we get ciphertext "srpnqaqcajwi". In this simulation not just encrypt the plaintext, we also simulate the decryption process. The input of the decryption process is the ciphertext "srpnqaqcajwi" with the same pair of keys as an encryption process. Figures 4 and 5 show that the simulation works well. This paper also uses cryptanalysis to find how to secure this method. Cryptanalysis is a process to break a cipher in illegal decryption [9]. The cryptanalysis process uses Cryptool 2.1. With that tool, we can input the ciphertext and the tool will analyze the plaintext. In this case, Vigenere Analyzer is implemented. Figure 4 shows that with Vigenere Analyzer could not break the ciphertext. When we input the ciphertext, the output is not plaintext. Another cryptanalysis that we use is Analysis Monoalphabetic Substitution. This analysis coud not break the ciphertext in Figure 6.

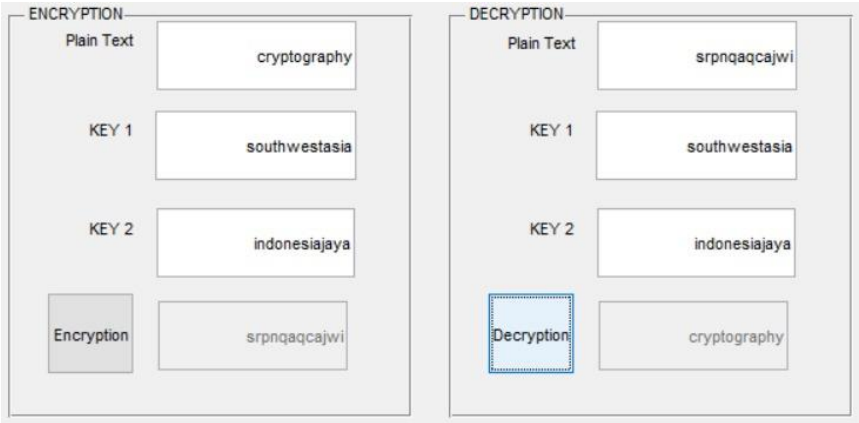

Fig. 4. Second simulation: Cryptography by a combination of Vigenere Cipher and Affine Cipher

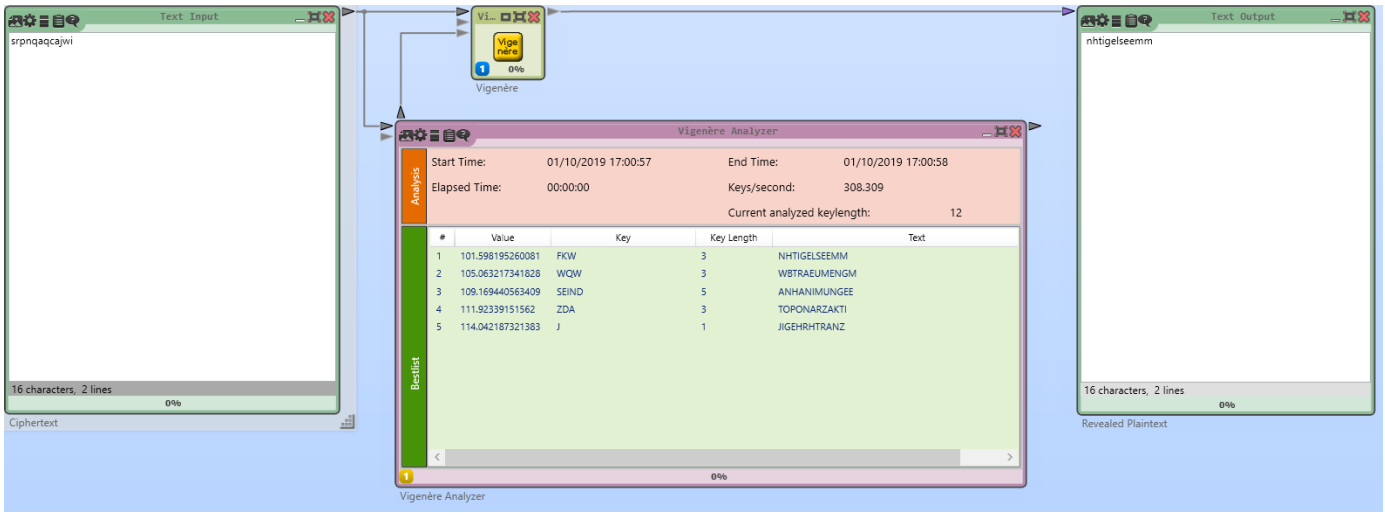

Fig. 5. Cryptanalysis with Vigenere Analyzer

 DOI: 10.25139/ijair.v1i1.2029

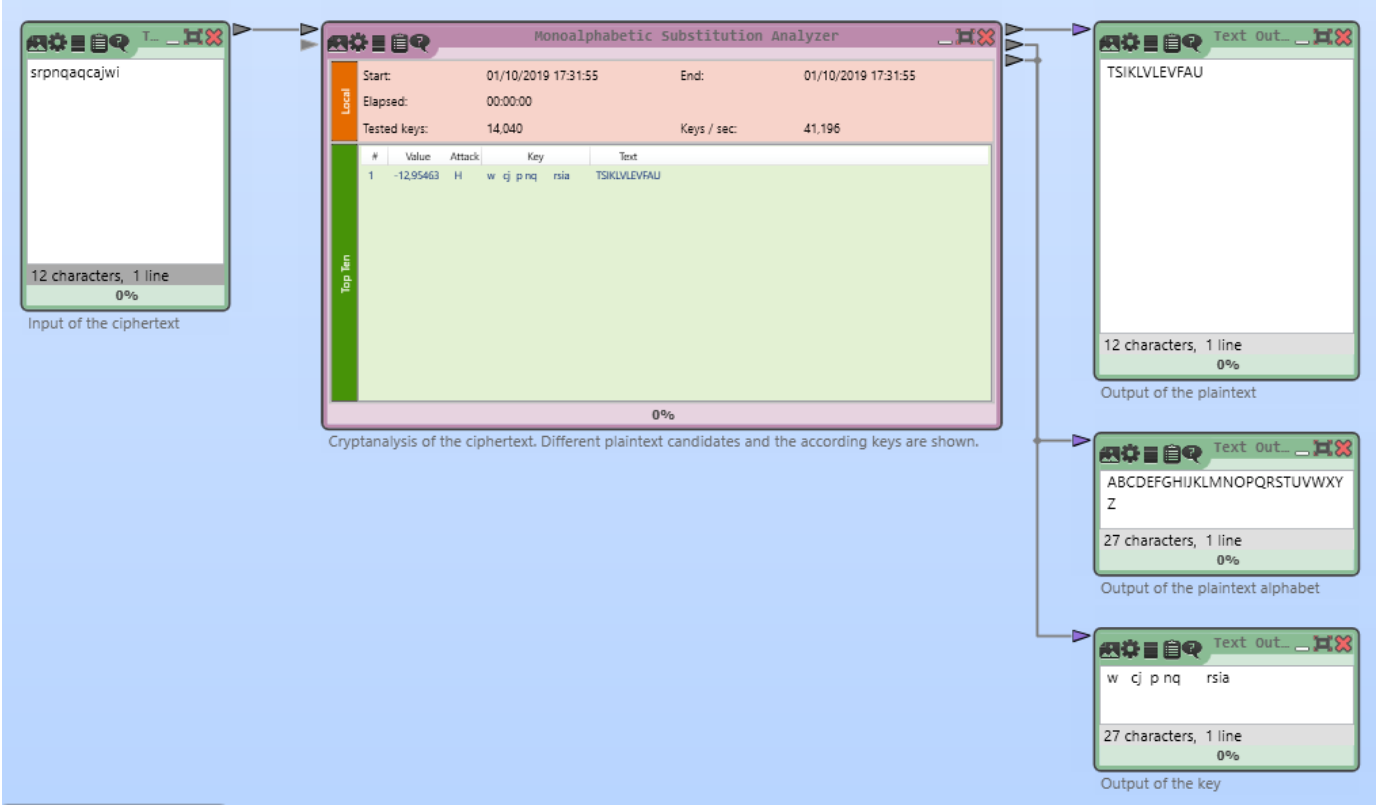

Fig. 6. Cryptanalysis with Analysis Monoalphabetic Substitution

IV. CONCLUSION

Vigenere cipher is a famous algorithm of polyalphabetic cipher with simple calculations. This algorithm has weaknesses that can be detected easily by intruders because the algorithm is simple and needs improvement for complex algorithms. This paper proposes combining Affine cipher and Vigenere cipher to produce more complex algorithms. By result and cryptanalysis, this method is more secure than before. It was proofed by the cryptanalysis process with Vigenere analyzer and Monoalphabetic Substitution, and the cryptanalysis could not break the plaintext.

REFERENCES

[1] Schneier, B., (1996), Applied Cryptography 2nd, John Wiley&Sons.
[2] Menez, A, J., Oorschot, P. C., Vanstone, S.A. (1996), Handbook of Applied Cryptography, CRC Press.
[3] B. A. Forouzan, “Traditional symmetric-key ciphers,” Cryptography and Network Security,” International Edition, Singapore, McGraw-Hill Press, pp. 55-90, 2008.
[4] D. E. Denning, “Encryption algorithms,” Cryptography and Data Security,” Addison Wesley Publishing Company Inc., U.S.A., pp. 59-125, 1982.
[5] A. M. Aliyu and A. Olaniyan, “Vigenere Cipher : Trends, Review, and Possible Modifications”, International Journal of Computer Application, Vol 135, No. 11, 2016.
[6] T. M. Aung, H.H. Naing, and N. N. Hla, “A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher: (Vigenere-Affine Cipher)”, International Journal of Machine Learning and Computing,Vol.9, No.3, June, 2019.
[7] Emy Setyaningsih, (2015), “Kriptografi dan Implementasinya menggunakan Matlab”, Penerbit Andi, 2015.
[8] N. N. Hla and T. M. Aung. “Implementation of finite field arithmetic operations for large prime and binary fields using Java BigInteger class,” International Journal of Engineering Research and Technology, vol. 6, issue 08, pp. 450-453, August 2017.
[9] R. Marwati and K. Yuliawati, “Cryptanalysis on Classical Cipher based on Indonesian Language”, International Seminar of Mathematics, Science, and Computer Science Education, 2018.
[10] Stallings, W. (2011). Cryptography and Network Security - Principles and Practice. (Fifth edition), Pearson Education, Inc.

 DOI: 10.25139/ijair.v1i1.2029