A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher: (Vigenère-Affine Cipher)

Tun Myat Aung, Htet Htet Naing, and Ni Ni Hla

Abstract—**Fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission on public communication networks. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. In cryptography, there are various cipher techniques such as monoalphabetic cipher, polyalphabetic cipher, etc. to support data confidentiality as security mechanisms. They are methods of encrypting plain text message into cipher text protecting it from adversaries. The process of encryption of alphabets is the converting original message into non readable form. One of the most popular cipher techniques is the Vigenère cipher. It is a polyalphabetic cipher technique which uses the Vigenère table for the process of encryption of alphabets. As the Vigenère cipher does not have the properties of diffusion and confusion, it is longer vulnerable to Kasiski and Friedman attacks based on letter frequency analysis. Thus, in this paper we propose a polyalphabetic cipher that is a new encryption and decryption technique with diffusion and confusion properties based on the concept of the complex cipher used by combining of Vigenère cipher with Affine cipher for the increase of data security in data storage and transmission on public communication networks. Our proposed technique can also be considered as a complex transformation technique from Affine cipher known as a monoalphabetic cipher technique to a new polyalphabetic cipher technique that is called Vigenère-Affine cipher.**

Index Terms—**Affine cipher, monoalphabetic cipher, polyalphabetic cipher, Vigenère cipher, complex transformation.**

I. Introduction

Cryptography is the science and studying of secret writing. A cipher is a secret method of writing, plain text is transformed into cipher text. The process of transforming plain text into cipher text is called encipherment or encryption; the reverse process of transforming cipher text into plain text is called decipherment or decryption. Both encipherment and decipherment are controlled by cryptographic key or keys as shown in Fig. 1.

There are two basic types of ciphers: transpositions and substitutions. A transposition cipher changes the location of the symbols. A symbol in the first position of the plain text may appear in the tenth position of the cipher text. A symbol in the eight position of the plain text may appear in the first position of the cipher text. In other words, a transposition cipher reorders (transposes) the symbols. There are two methods for permutation of characters. In the first method, the text is written into a table column by column and then transmitted row by row. In the second method, the text is written into a table row by row and then transmitted column by column. Rail-fence cipher, Route cipher, Columnar cipher, Transposition using Matrix and Double transposition are popular transposition ciphers [1].

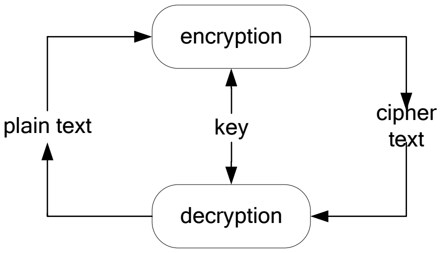


Fig. 1. Secret writing.

A substitution cipher replaces one symbol with another. If the symbols in the plain text are alphabetical characters, we replace one character with another. Substitution ciphers can be categorized as either mono-alphabetic ciphers or poly-alphabetic ciphers. In monoalphabetic substitution, a character (or a symbol) in the plain text is always changed to the same character (or a symbol) in the cipher text regardless of its position in the text. In monoalphabetic substitution, the relationship between a character in the plain text to a character in the cipher text is always one-to-one. In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plain text to a character in the cipher text is one-to-many. Additive cipher, Shift cipher, Caesar cipher, Multiplicative cipher and Affine cipher are popular monoalphabetic ciphers and Vigenère cipher, Autokey cipher, Playfair cipher, Beaufort cipher, Running key cipher, Porta cipher, Hill cipher, One-Time pad and Rotor cipher are popular polyalphabetic ciphers [1].

Modern ciphers possess two important properties: diffusion and confusion. The idea of diffusion is to hide the relationship between the cipher text and the plain text. This will frustrate the adversary who uses the cipher text statistics to find the plain text. The idea of confusion is to hide the relationship between the cipher text and the key. This will frustrate the adversary who tries to use the cipher text to find the key. Diffusion and confusion can be achieved using the concept of complex cipher known as product cipher introduced by Shannon [1]. The success and competence of the cryptographic cipher technique depends upon the fact that how difficult it is to be broken or cracked by a cryptanalyst.

The Vigenère cipher is one of the most popular cipher techniques. It is a polyalphabetic cipher technique which uses

Manuscript received October 20, 2018; revised April 26, 2019.

The authors are with the University of Computer Studies, Yangon, (UCSY), Myanmar (e-mail: tunmyataung@ucsy.edu.mm, htet2naing.h@gmail.com, ni2hla@ucsy.edu.mm).

doi: 10.18178/ijmlc.2019.9.3.801

the Vigenère table for the process of encryption of alphabets. As the Vigenère cipher does not have the properties of diffusion and confusion, it is longer vulnerable to Kasiski and Friedman attacks based on letter frequency analysis. Thus, in this paper we propose a polyalphabetic cipher that is a new encryption and decryption technique with diffusion and confusion properties based on the concept of the complex cipher used by combining of Vigenère cipher with Affine cipher for the increase of data security in data storage and transmission on public communication networks. Our proposed technique can also be considered as a complex transformation technique from Affine cipher known as a monoalphabetic cipher technique to a new polyalphabetic cipher technique that is called Vigenère-Affine cipher.

The purpose of this paper is to overcome the weaknesses of the Vigenere cipher. The structure of this paper is as follows. The Section II includes general knowledge of ployalphabetic cipher technique and its advantages. In Section III, we discuss Vigenère cipher technique and its weakness. The Section IV includes various modified approaches to enhance the security of the Vigenère cipher. The Section V includes monoalphabetc ciphers such as additive cipher, multiplicative cipher and Affine cipher used to combine with our proposed technique. In Section VI, we discuss our proposed technique. Finally, in the Section VII we conclude our paper.

II. Polyalphabetic Cipher Techniques

Polyalphabetic ciphers were invented circa 1467 by the Florentine architect Alberti, who created a cipher disk with a larger outer and smaller inner wheel, respectively indexed by plaintext and ciphertext characters. Letter arrangements defined a simple substitution, modified by rotating the disk after enciphering a few words. The first printed book on cryptography, Polygraphia, written in 1508 by the German monk Trithemius and published in 1518, contains the first tableau – a square table on 24 characters listing all shift substitutions for a fixed arrangement of plaintext alphabet characters. Tableau rows were used sequentially to substitute one plaintext character each for 24 letters, where-after the same tableau or one based on a different alphabet arrangement was used. In 1553 Belaso from Lombardy suggested using an easily changed key (and key-phrases as memory aids) to define the fixed alphabetic (shift) substitutions in a polyalphabetic substitution. Polyalphabetic ciphers have the advantage over simple substitution ciphers that symbol frequencies are not preserved. However, polyalphabetic ciphers are not significantly more difficult to cryptanalyze, the approach being similar to the simple substitution cipher. In fact, once the block length is determined, the cipher text letters can be divided into groups (where group consists of those cipher text letters derived using permutation), and a frequency analysis can be done on each group [2].

A simple substitution cipher involves a single mapping of the plaintext alphabet onto cipher text characters. A more complex alternative is to use different substitution mappings (called multiple alphabets) on various portions of the plaint ext. This results in so-called polyalphabetic substitution. In the simplest case, the different alphabets are used sequentially and then repeated, so the position of each plain text character in the source string determines which mapping is applied to it. Under different alphabets, the same plain text character is thus encrypted to different cipher text characters, preventing simple frequency analysis as per monoalphabetic substitution. Therefore, polyalphabetic cipher techniques make the message more secure as compared to various other techniques.

Generally, to create a polyalphabetic cipher, each cipher text character is made dependent on both the corresponding plain text character and the position of plain text character in the message. This implies that the key should be a stream of subkeys, in which each subkey depends somehow on the position of plain text character that uses that subkey for encipherment. In other words, a polyalphabetic cipher needs to have a key stream ($k = k_1, k_2, k_3, \ldots$) in which k_i is used to encipher the i^{th} character in the plain text to create the i^{th} character in the cipher text [1].

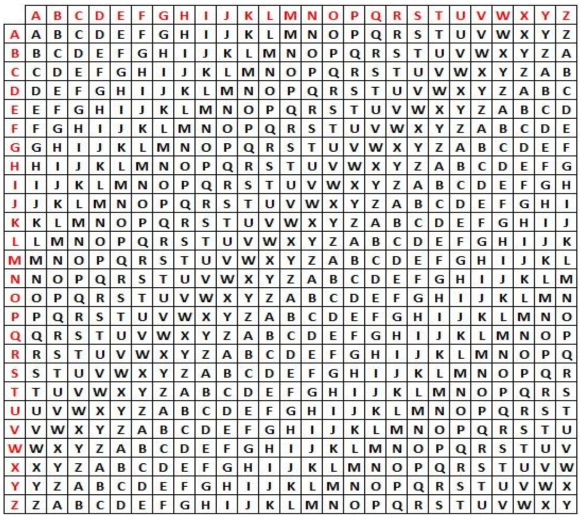
III. Vigenère Cipher

One interesting kind of polyalphabetic cipher was designed by Blaise de Vigenère, sixteenth-century French mathematician. It was known as Vigenère cipher. It was one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher [2].

A. Encryption and Decryption

In Vigenère cipher a table of alphabets can be used for both encryption and decryption, termed as tabula recta, Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers known as additive ciphers.

Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plain text letter. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to itself. The Vigenère table is as shown in Fig. 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

Fig. 2. Vigenère table.

At different points in the encryption or decryption processes, the cipher uses a different alphabet from one of the rows of the Vigenère table. The alphabet used at each point depends on a repeating key stream. For encrypting a message or plain text the user should chose a key stream by satisfying the condition that the length of the key stream should be equal to the length of the plain text. For a given key letter ‘P’ and the plain text letter ‘Q’, the cipher text letter is at the intersection of the row labeled ‘P’ and the column labeled ‘Q’; in this case the cipher text is ‘F’. Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and plaintext letter is at the top of the column [3].

For example the plain text is: “ATTACKOFFICE”. The sender of the message chooses a key stream and repeats it until its length matches with the length of the plaintext, for example, the key “KING”, then the key stream will be: “KINGKINGKING”.

For encryption, the first letter of the plaintext is ‘A’, can be enciphered using the alphabet in row ‘K’, which is the first letter of the key stream chosen. The cipher letter is the intersection of the row ‘K’ and column ‘A’ of the Vigenère square, here it is ‘K’, and the rest of the plain text will continue in this way. The cipher text for the chosen plaintext will be “KBGGMSBLPQPK”.

For decryption select the row based on the key letter, finding the position of the cipher text letter in that row, and use the corresponding column label as the plaintext. In the row ‘K’ identified by the first letter of the key stream, the corresponding cipher letter ‘K’ appears in column ‘A’, which is the first plaintext letter. Next we go to the row ‘I’ from the key stream, locate the cipher text ‘B’ which is found in the column ‘T’, thus ‘T’ is the second plaintext letter. The rest of the cipher text will continue in this way. The plain text for the cipher text “KBGGMSBLPQPK” will be “ATTACKOFFICE”.

B. Algebraic Description

Vigenère cipher can be viewed algebraically. If the letters ‘A’ to ‘Z’ are taken to be the numbers ‘0’ to ‘25’, and addition is performed modulo 26, then Vigenère encryption E using the key K can be written,

$$C_i = E_K(P_i) = (P_i + k_i) \bmod 26 \tag{1}$$

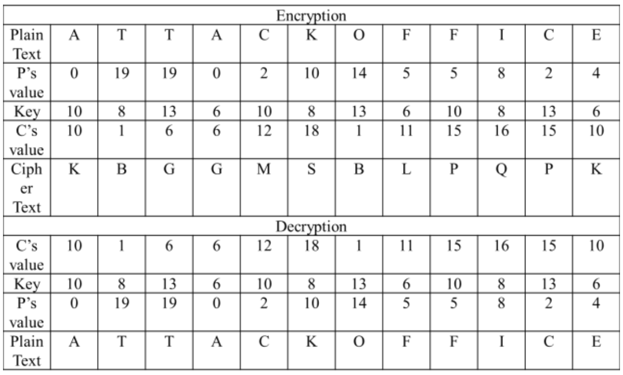
and decryption D using the key K,

$$P_i = D_K(C_i) = (C_i - k_i) \bmod 26 \tag{2}$$

where as $P = P_1, P_2, \ldots, P_n$ is the plain text, $C = C_1, C_2, \ldots, C_n$ is the cipher text and $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots, k_n]$ is the used key. Vigenère cipher can also be seen as combination of n additive ciphers. Thus using the previous example, encryption and decryption processes of Vigenère cipher are algebraically demonstrated using equation (1) and equation (2) in Fig. 3.

C. Cryptanalysis

The idea behind the Vigenère cipher, like all polyalphabetic ciphers, is to disguise plain text letter frequencies, which interferes with a straightforward application of frequency analysis. For instance, if ‘*P*’ is the most frequent letter in a cipher text whose plaintext is in English, one might suspect that ‘*P*’ corresponds to ‘*E*’, because ‘*E*’ is the most frequently used letter in English. However, using the Vigenère cipher, ‘*E*’ can be enciphered as different cipher text letters at different points in the message, thus defeating simple frequency analysis.



<table>
<tr><td colspan="13">Encryption</td></tr>
<tr><td>Plain Text</td><td>A</td><td>T</td><td>T</td><td>A</td><td>C</td><td>K</td><td>O</td><td>F</td><td>F</td><td>I</td><td>C</td><td>E</td></tr>
<tr><td>P’s value</td><td>0</td><td>19</td><td>19</td><td>0</td><td>2</td><td>10</td><td>14</td><td>5</td><td>5</td><td>8</td><td>2</td><td>4</td></tr>
<tr><td>Key</td><td>10</td><td>8</td><td>13</td><td>6</td><td>10</td><td>8</td><td>13</td><td>6</td><td>10</td><td>8</td><td>13</td><td>6</td></tr>
<tr><td>C’s value</td><td>10</td><td>1</td><td>6</td><td>6</td><td>12</td><td>18</td><td>1</td><td>11</td><td>15</td><td>16</td><td>15</td><td>10</td></tr>
<tr><td>Cipher Text</td><td>K</td><td>B</td><td>G</td><td>G</td><td>M</td><td>S</td><td>B</td><td>L</td><td>P</td><td>Q</td><td>P</td><td>K</td></tr>
<tr><td colspan="13">Decryption</td></tr>
<tr><td>C’s value</td><td>10</td><td>1</td><td>6</td><td>6</td><td>12</td><td>18</td><td>1</td><td>11</td><td>15</td><td>16</td><td>15</td><td>10</td></tr>
<tr><td>Key</td><td>10</td><td>8</td><td>13</td><td>6</td><td>10</td><td>8</td><td>13</td><td>6</td><td>10</td><td>8</td><td>13</td><td>6</td></tr>
<tr><td>P’s value</td><td>0</td><td>19</td><td>19</td><td>0</td><td>2</td><td>10</td><td>14</td><td>5</td><td>5</td><td>8</td><td>2</td><td>4</td></tr>
<tr><td>Plain Text</td><td>A</td><td>T</td><td>T</td><td>A</td><td>C</td><td>K</td><td>O</td><td>F</td><td>F</td><td>I</td><td>C</td><td>E</td></tr>
</table>

Fig. 3. Algebraic computing of Vigenère cipher.

The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key’s length, then the cipher text can be treated as interwoven Caesar ciphers, which individually are easily broken. The Kasiski and Friedman tests can help determine the key length.

Kasiski Test was developed in 1863 by Riedrich Kasiski [2]. In Kasiski test, the cryptanalyst searches for repeated text segments, of at least three characters, in the cipher text. Then, the distances between consecutive occurrences of the strings are likely to be multiples of the length of the keyword. Finding more repeated strings narrows down the possible lengths of the keyword, since we can take the greatest common divisor of all the distances. The key length is the multiple of the greatest common divisor.

Friedman Test was developed in 1925 by William Friedmanis [2], a probabilistic test that can be used to determine the likelihood that the cipher text message produced comes from a monoalphabetic or polyalphabetic cipher. This technique uses the index of coincidence, to measure the unevenness of the cipher letter frequencies. By knowing K_p (probability that any two randomly chosen source-language letters are the same, in case of English $K_p = \sum_{i=0}^{25} pi^2 \approx 0.067$, pi is the probability that both the alphabets are i.) and K_r (probability of a coincidence for a uniform random selection from the alphabet, in case of English $K_r = 1/26$), the estimated key length (l) can be solved by equation (3).

$$l = \frac{K_p - K_r}{K_o - K_r} \tag{3}$$

where K_o (observed coincidence rate) is $K_o = \frac{\sum_{i=1}^{c} n_i (n_i - 1)}{N(N-1)}$, where c is the size of the alphabet (26 for English), N is the length of the text, and n_1 to n_c are the observed cipher text letter frequencies.

IV. Modified Approaches

Over the years, when Vigenère cipher was no longer safe, researchers started suggesting various improvements to enhance the security of the Vigenère cipher.

Kester (2012) proposed a cryptosystem based on Vigenère cipher with varying key [3]. This method used successive keys that are dependent on the initial key value during the encryption process. An initial key was used for the encryption process using the Vigenère square. The key then varied as it was used in the encryption process. The first step key was different from the second step key, as a result of a function that operated on the first step. The function is applied to subsequent stages to generate the key for the next encryption stage. The decryption process is likely to behave abnormally because of the random generation of encryption keys for its encryption, which might not give the expected result.

Khalid (2012) proposed an alpha-qwerty cipher which is an extension of the Vigenère cipher [4]. The system expanded and redesigned the Vigenère square table to consist of 92 characters instead of the conventional 26 alphabets. It then becomes a 92 by 92 matrix to enhance the Vigenère square. It provides a greater character set, allowing more characters such as punctuations and numbers to be encrypted, whereas the original Vigenère covers plaintext involving only the 26 characters of the alphabet.

Another attempt that was made to improve the security of the Vigenère cipher was made by Kester (2013) where he proposed a hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher [5]. He suggested the use of transposition cipher to scramble a plaintext, which is then used as the key for the Vigenère cipher encryption process.

Omolara *et al*., (2014) proposed a modified hybrid Caesar cipher and Vigenère cipher for secure data communication [6]. A lettered key and a numbered key were used for the encryption process. A Caesar cipher was performed on the lettered key using the shift of the numbered key. Vigenère cipher is then performed on the plaintext using the new key. The binary equivalent of the text generated is then XORed with the binary of the numbered key to generate the final ciphertext.

Nishith and Kishore (2014) proposed improving security of Vigenère cipher by double columnar transposition [7]. This involves applying the Vigenère cipher on a plaintext, before subsequently applying columnar transposition twice to further scramble the text. An increase in the computational complexity was noticed when compared with the Vigenère cipher.

Ali and Sarhan (2014) proposed an advanced encryption algorithm which improves the security of Vigenère method by combining it with modern cipher method like Stream cipher [8]. Stream cipher relatively regards as unbreakable method, and it uses binary form (instead of characters) where the Plaintext, Ciphertext and the Key are strings of bits.

Ashish Shah (2016) proposed an enhancement to the Vigenère cipher by converting it into a product cipher as an encryption combining the 2 encryption techniques, Modified RC4 and Vigenère in a systematic manner [9].

Mandal and Deepti (2016) proposed a multi-level encryption scheme by using Vigenère cipher to improve better security against cryptanalysis [10]. In this method an equivalent fixed length of plain text and a key is selected and applied in Vigenère table to get a new cipher text. This cipher text is act as a new key. With this new key the cipher text is encrypted once again and sends the final cipher text to the receiver. Finally the receiver does the decryption in reverse way.

Subandi *et al.*, (2017) developed the three-pass protocol using Vigenère cipher with keystream generator modification [11]. In this study, they modify the key on Vigenère Cipher, so when the key length smaller than the length of plaintext entered, the key will be generated by a process, so the next key character will be different from the previous key character. In this study also applied the technique of Three-pass protocol, a technique which message sender does not need to send the key, because each using its own key for the message encryption and decryption process, so the security of a message would be more difficult to solved.

V. Monoalphabetic Cipher Techniques

Modern ciphers normally use a combination of substitution with transposition and some other complex transformations to create a cipher text from a plain text. In our paper we put emphasis on proposing a new combination method, Vigenère cipher with Affine cipher, because the cipher based on simple Vigenère method is not secure. An Affine cipher is a combination of the additive cipher and multiplicative cipher. Additive cipher, multiplicative cipher and Affine cipher are monoalphabetic cipher techniques.

A. Additive Cipher

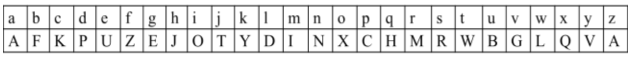
Additive cipher is one method of deriving a permutation of the letters of the alphabet. In it, every letter in the alphabet is cyclically shifted by the same amount and the relative order of the letters is kept the same [1]. The number of position the letter has been shifted is called the key. For example if we use a key value of 5, ‘a’ is shifted 5 positions right in the alphabet to ‘F’, ‘b’ to ‘G’ and so on. The letter ‘u’ is shifted to ‘Z’ and then we wrap around to the beginning of the alphabet. The letter ‘v’ is mapped to ‘A’ and so on. (Here note: lowercase is used for plain text and uppercase is used for cipher text.) In other words, additive cipher can also be done by using the position numbers of the letters of the alphabet. In this way, the English letters ‘A’ to ‘Z’ are firstly mapped to be the position numbers ‘0’ to ‘25’. For example, since plain text letter (P) is ‘a’ and the key (K) is 5, the cipher text letter is computed by modular arithmetic addition operation such as $C = P + K(\bmod 26)$. Then, $C = 0 + 5(\bmod 26) = 5$. The position number ‘5’ is mapped to the letter ‘F’. Thus the cipher text letter is ‘F’. The complete cipher table is shown in Fig. 4.

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
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

Fig. 4. Additive cipher table.

B. *Multiplicative Cipher*

Multiplicative cipher is another method for generating a permutation of the letters of the alphabet. In it, taking a key value and each letter's position number is multiplied by 5 and then the product is reduced by modulo 26 [1]. For example, since plain text letter (P) is ‘h’ and the key (K) is 5, the cipher text letter is computed by modular arithmetic multiplication operation such as $C = P \times K (\text{mod} 26)$. Then, $C = 7 \times 5 = 9 (\text{mod} 26)$. The position number ‘9’ is mapped to the letter ‘J’. Thus the cipher text letter is ‘J’. The complete cipher table is shown in Fig. 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	F	K	P	U	Z	E	J	O	T	Y	D	I	N	X	C	H	M	R	W	B	G	L	Q	V	A

Fig. 5. Multiplicative cipher table.

C. *Affine Cipher*

The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. An Affine cipher is created by combining the additive cipher and multiplicative cipher. It is a combination of both ciphers with a pair of keys. The first key is used with the multiplicative cipher, the second key is used with the additive cipher [1]. The pair of keys is shared secret keys for both the sender and the receiver of the message. Fig. 6 shows that the Affine cipher is actually two ciphers, applied one after another, including only one complex operation for the encryption or decryption such as $C = ((P \times k_1) + k_2) \text{mod} n$ and $P = ((C - k_2) \times k_1^{-1}) \text{mod} n$. ‘T’ is used as a temporary result and indicates two separate operations: multiplication and addition for encryption; subtraction and division for decryption. As a result of a combination of ciphers, Affine cipher has reverse transformations in each process, encryption or decryption. If addition is the last operation in encryption, then subtraction should be the first in decryption. If multiplication is the first operation in encryption, then division should be the last in decryption. According to modular arithmetic concept, division operation can be transformed to multiplication using its corresponding modular multiplicative inverse operation.

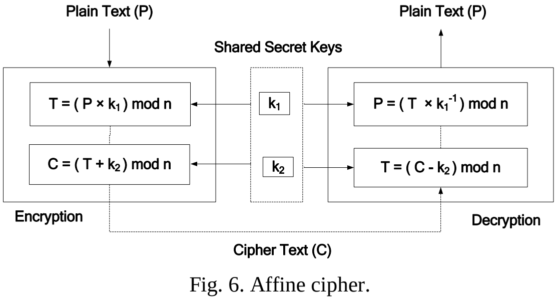


Fig. 6. Affine cipher.

1) *Algebraic description*

In the Affine cipher the letters of an alphabet of size n are first mapped to the integers in the range: $0, \ldots, n-1$. It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that corresponds to a cipher text letter. The encryption function for a single letter is defined as equation (4).

$$C = ((P \times k_1) + k_2) \text{mod } n \tag{4}$$

where modulus n is the size of the alphabet and k_1 and k_2 are the keys of the cipher. The value k_1 must be chosen such that k_1 and n are coprime [12]. The decryption function is defined as equation (5).

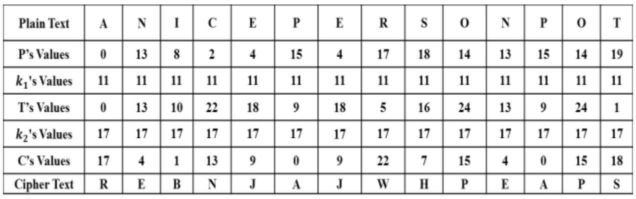
$$P = ((C - k_2) \times k_1^{-1}) \text{mod } n \tag{5}$$

where k_1^{-1} is the modular multiplicative inverse of k_1 modulo n i.e., it satisfies the equation (6).

$$1 \equiv k_1 . k_1^{-1} \text{mod } n \tag{6}$$

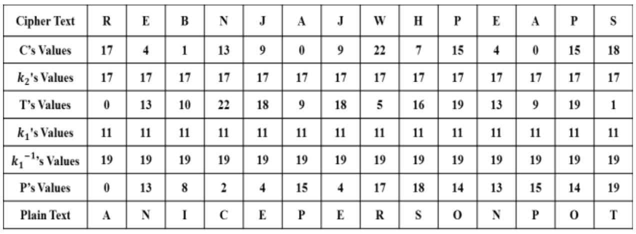
The multiplicative inverse of k_1 only exists if k_1 and n are coprime [12].

For example the plain text is: “A NICE PERSON’S POT”. If space and apostrophe characters are not considered, the plain text is arranged as “ANICEPERSONSPOT”. The English letters ‘A’ to ‘Z’ are taken to be the numbers ‘0’ to ‘25’. When the plain text is enciphered with $k_1 = 11$ and $k_2 = 17$ as shown in Fig. 7, the plain text is “REBNJAJWHPEAPS”. When the cipher text is deciphered with $k_2 = 17$ and $k_1 = 11$ as shown in Figure (8), the plain text is “ANICEPERSONSPOT”. The receiver of the message can define the plain text as ambiguous meanings such as “A NICE PERSON SPOT”, “AN ICE PERSON SPOT”, “AN ICE PERSONS POT” or “A NICE PERSONS POT”.



Plain Text	A	N	I	C	E	P	E	R	S	O	N	P	O	T
P’s Values	0	13	8	2	4	15	4	17	18	14	13	15	14	19
k_1's Values	11	11	11	11	11	11	11	11	11	11	11	11	11	11
T’s Values	0	13	10	22	18	9	18	5	16	24	13	9	24	1
k_2's Values	17	17	17	17	17	17	17	17	17	17	17	17	17	17
C’s Values	17	4	1	13	9	0	9	22	7	15	4	0	15	18
Cipher Text	R	E	B	N	J	A	J	W	H	P	E	A	P	S

Fig. 7. Encryption of affine cipher.



Cipher Text	R	E	B	N	J	A	J	W	H	P	E	A	P	S
C’s Values	17	4	1	13	9	0	9	22	7	15	4	0	15	18
k_2's Values	17	17	17	17	17	17	17	17	17	17	17	17	17	17
T’s Values	0	13	10	22	18	9	18	5	16	19	13	9	19	1
k_1's Values	11	11	11	11	11	11	11	11	11	11	11	11	11	11
k_1^{-1}'s Values	19	19	19	19	19	19	19	19	19	19	19	19	19	19
P’s Values	0	13	8	2	4	15	4	17	18	14	13	15	14	19
Plain Text	A	N	I	C	E	P	E	R	S	O	N	P	O	T

Fig. 8. Decryption of affine cipher.

VI. PROPOSED TECHNIQUE

Our proposed technique is that the original Vigenère cipher is developed by combining Vigenère cipher with Affine cipher. Our proposed technique is also considered as a complex transformation technique from Affine cipher known as a monoalphabetic cipher technique to polyalphabetic cipher technique that is called Vigenère -Affine cipher which based on the combination of Vigenère cipher with Affine cipher.

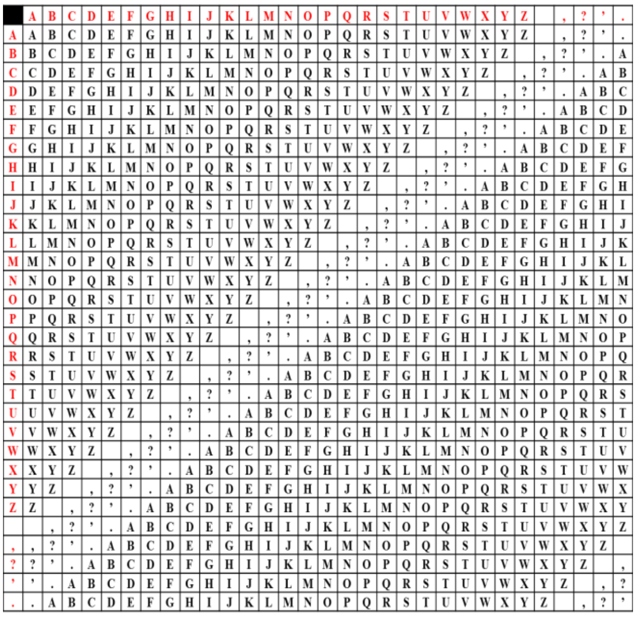
A. Encryption and Decryption

Our proposed technique uses two kinds of tables: addition table and multiplication table. The modified tables are designed by using English alphabet 26 characters and appending another six essential characters such as space, comma, question mark, apostrophe, and full stop to avoid ambiguous meanings and to solve meaningful sentence. We must first design the modified tables, addition table and multiplication table, using 31 characters of English alphabet. Thus, the size of these tables is 31×31. These tables are created by using character position numbers of English alphabet and our implementation system of finite field arithmetic operations [12]. Addition table shown in Fig. 9 is used for encryption and decryption processes of additive cipher. Multiplication table shown in Fig. 10 is used for encryption and decryption processes of multiplicative cipher. The encryption and decryption processes of Vigenère-Affine cipher are two steps-transformation processes shown in Fig. 11. A pair of key streams, the first key stream and the second key stream, is used in each process, encryption or decryption. In encryption process, the first key stream is used with multiplicative ciphers at the first step transformation and the second key stream is used with additive ciphers at the second step. In decryption process, the second key stream is used with additive ciphers at the first step transformation and the first key stream is used with multiplicative ciphers at the second step. For each transformation process the user should chose a key stream by satisfying the condition that the length of the key stream should be equal to the length of the plain text or the cipher text.

For example the plain text is: “A NICE PERSON’S POT”. The plain text consists of 19 characters including space and apostrophe characters. The sender of the message chooses two keys and repeats it until its length matches with the length of the plain text, for example, the first key is “KING”, then the first key stream will be: “KINGKINGKINGKINGKIN”. If the second key is “TREE”, then the second key stream will be: “TREETREETREETREETRE”. These two keys are shared secret keys for both the sender and the receiver of the message.

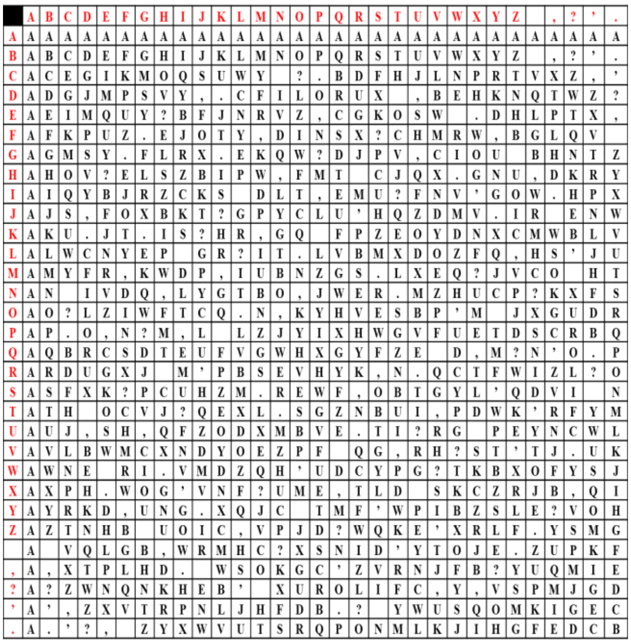
For the first step transformation of encryption process, the first letter of the plain text is ‘A’ and it can be enciphered using the alphabet in row ‘K’, which is the first letter of the first key stream. At the first step using multiplicative cipher, the cipher letter is the intersection of the row ‘K’ and column ‘A’ of the multiplication table; here it is ‘A’. For the second step transformation using additive cipher, the letter ‘A’ that got from multiplicative cipher can be again enciphered using the alphabet in row ‘T’, which is the first letter of the second key stream. In additive cipher, the cipher letter is the intersection of the row ‘T’ and column ‘A’ of the addition table; here it is ‘T’. The rest of the plain text will continue in these procedures. The cipher text for the chosen plaintext will be “TISVISBB?’V ZVBFOFD”.

For the first step transformation of decryption process, using addition table, in the row ‘T’ identified by the first letter of the second key stream, the corresponding cipher letter ‘T’ appears in column ‘A’, which is the first letter got from the additive cipher. For the second step transformation using multiplication table, in the row ‘K’ identified by the first letter of the first key stream, the corresponding letter ‘A’ got from the additive cipher appears in the column ‘A’, which is the first plaintext letter got from the multiplicative cipher. The rest of the cipher text will continue in these procedures. The plain text for the given cipher text will be “A NICE PERSON’S POT”. If we did not consider space and apostrophe characters, the plain text may be ambiguous meaning like “AN ICE PERSON SPOT”.



	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
		,	?	’	.	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	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	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	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	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		,	?	’

Fig. 9. Addition table.



	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	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
B	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		,	?	’	.
C	A	C	E	G	I	K	M	O	Q	S	U	W	Y		?	.	B	D	F	H	J	L	N	P	R	T	V	X	Z	,	’
D	A	D	G	J	M	P	S	V	Y	,	.	C	F	I	L	O	R	U	X		,	B	E	H	K	N	Q	T	W	Z	?
E	A	E	I	M	Q	U	Y	?	B	F	J	N	R	V	Z	,	C	G	K	O	S	W		.	D	H	L	P	T	X	,
F	A	F	K	P	U	Z	.	E	J	O	T	Y	,	D	I	N	S	X	?	C	H	M	R	W	,	B	G	L	Q	V	
G	A	G	M	S	Y	.	F	L	R	X	.	E	K	Q	W	?	D	J	P	V	,	C	I	O	U		B	H	N	T	Z
H	A	H	O	V	?	E	L	S	Z	B	I	P	W	,	F	M	T		C	J	Q	X	.	G	N	U	,	D	K	R	Y
I	A	I	Q	Y	B	J	R	Z	C	K	S		D	L	T	,	E	M	U	?	F	N	V	’	G	O	W	.	H	P	X
J	A	J	S	,	F	O	X	B	K	T	?	G	P	Y	C	L	U	’	H	Q	Z	D	M	V	.	I	R		E	N	W
K	A	K	U	.	J	T	.	I	S	?	H	R	,	G	Q		F	P	Z	E	O	Y	D	N	X	C	M	W	B	L	V
L	A	L	W	C	N	Y	E	P		G	R	?	I	T	.	L	V	B	M	X	D	O	Z	F	Q	,	H	S	’	J	U
M	A	M	Y	F	R	,	K	W	D	P	,	I	U	B	N	Z	G	S	.	L	X	E	Q	?	J	V	C	O		H	T
N	A	N		I	V	D	Q	,	L	Y	G	T	B	O	,	J	W	E	R	.	M	Z	H	U	C	P	?	K	X	F	S
O	A	O	?	L	Z	I	W	F	T	C	Q	.	N	,	K	Y	H	V	E	S	B	P	’	M		J	X	G	U	D	R
P	A	P	.	O	,	N	?	M	,	L		L	Z	J	Y	I	X	H	W	G	V	F	U	E	T	D	S	C	R	B	Q
Q	A	Q	B	R	C	S	D	T	E	U	F	V	G	W	H	X	G	Y	F	Z	E		D	,	M	?	N	’	O	.	P
R	A	R	D	U	G	X	J		M	’	P	B	S	E	V	H	Y	K	,	N	.	Q	C	T	F	W	I	Z	L	?	O
S	A	S	F	X	K	?	P	C	U	H	Z	M	.	R	E	W	F	,	O	B	T	G	Y	L	’	Q	D	V	I		N
T	A	T	H		O	C	V	J	?	Q	E	X	L	.	S	G	Z	N	B	U	I	,	P	D	W	K	’	R	F	Y	M
U	A	U	J	,	S	H	,	Q	F	Z	O	D	X	M	B	V	E	.	T	I	?	R	G		P	E	Y	N	C	W	L
V	A	V	L	B	W	M	C	X	N	D	Y	O	E	Z	P	F		Q	G	,	R	H	?	S	T	’	T	J	.	U	K
W	A	W	N	E		R	I	.	V	M	D	Z	Q	H	’	U	D	C	Y	P	G	?	T	K	B	X	O	F	Y	S	J
X	A	X	P	H	.	W	O	G	’	V	N	F	?	U	M	E	,	T	L	D		S	K	C	Z	R	J	B	,	Q	I
Y	A	Y	R	K	D	,	U	N	G	.	X	Q	J	C		T	M	F	’	W	P	I	B	Z	S	L	E	?	V	O	H
Z	A	Z	T	N	H	B		U	O	I	C	,	V	P	J	D	?	W	Q	K	E	’	X	R	L	F	.	Y	S	M	G
	A		V	Q	L	G	B	,	W	R	M	H	C	?	X	S	N	I	D	’	Y	T	O	J	E	.	Z	U	P	K	F
,	A	,	X	T	P	L	H	D	.		W	S	O	K	G	C	’	Z	V	R	N	J	F	B	?	Y	U	Q	M	I	E
?	A	?	Z	W	N	Q	N	K	H	E	B	’		X	U	R	O	L	I	F	C	,	Y	,	V	S	P	M	J	G	D
’	A	’	,	Z	X	V	T	R	P	N	L	J	H	F	D	B	.	?		Y	W	U	S	Q	O	M	K	I	G	E	C
.	A	.	’	?	,		Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B

Fig. 10. Multiplication table.

B. Algebraic Description

In the Vigenère-Affine cipher the letters of an alphabet of size n are first mapped to the integers in the range: $0,\ldots,n-1$. The English letters ‘A’ to ‘Z’ are taken to be the numbers ‘0’ to ‘25’ and then map space character to ‘26’, comma to ‘27’, question mark to ‘28’, apostrophe to ‘29’ and full stop to ‘30’. It includes a total of 31 characters. It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that corresponds to a cipher text letter. The encryption function for a single letter is defined as equation (7). The algebraic computing for encryption process of the Vigenère-Affine cipher is demonstrated in Fig. 12.

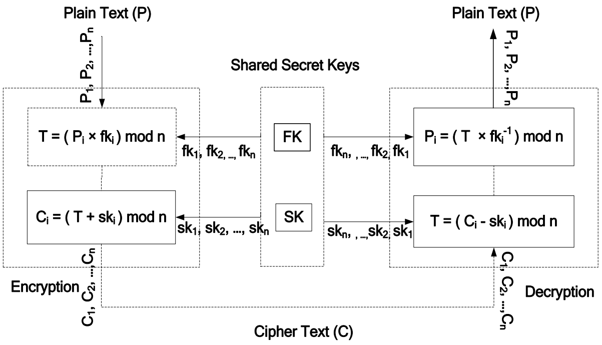


Fig. 11. Vigenère-affine cipher.

Plain Text	A		N	I	C	E		P	E	R	S	O	N	’	S		P	O	T
P’s Values	0	26	13	8	2	4	26	15	4	17	18	14	13	29	18	26	15	14	19
Key (FK)	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N
FK’s Values	10	8	13	6	10	8	13	6	10	8	13	6	10	8	13	6	10	8	13
T’s Values	0	22	14	17	20	1	28	28	9	12	17	22	6	15	17	1	26	19	30
Key (SK)	T	R	E	E	T	R	E	E	T	R	E	E	T	R	E	E	T	R	E
SK’s Values	19	17	4	4	19	17	4	4	19	17	4	4	19	17	4	4	19	17	4
C’s Values	19	8	18	21	8	18	1	1	26	29	21	26	25	1	21	5	14	5	3
Cipher Text	T	I	S	V	I	S	B	B	?	’	V		Z	B	V	F	O	F	D

Fig. 12. Algebraic computing of encryption process.

$$C_i = ((P_i \times fk_i) + sk_i) \bmod n \tag{7}$$

where $P = P_1, P_2, ..., P_n$ is denoted as the plain text, $C = C_1, C_2, ..., C_n$ is denoted as the cipher text, $FK = [(fk_1, fk_2, ..., fk_m), (fk_1, fk_2, ..., fk_m), ..., fk_n]$ is denoted as the first key stream, $SK = [(sk_1, sk_2, ..., sk_m), (sk_1, sk_2, ..., sk_m), ..., sk_n]$ is denoted as the second key stream and the modulus n is the size of the alphabets. The decryption function is defined as equation (8). The algebraic computing for decryption process of the Vigenère-Affine cipher is demonstrated in Fig. 13.

$$P_i = ((C_i - sk_i) \times fk_i^{-1}) \bmod n \tag{8}$$

where fk_i^{-1} is the modular multiplicative inverse of fk_i modulo n .i.e., it satisfies the equation (9).

$$1 = fk_i \times fk_i^{-1} \bmod n \tag{9}$$

The modulus n should be prime such that every letter of an alphabet of size n possesses the corresponding modular multiplicative inverse i.e. the size of the alphabets should be prime.

Cipher Text	T	I	S	V	I	S	B	B	?	’	V		Z	B	V	F	O	F	D
C’s Values	19	8	18	21	8	18	1	1	26	29	21	26	25	1	21	5	14	5	3
Key (SK)	T	R	E	E	T	R	E	E	T	R	E	E	T	R	E	E	T	R	E
SK’s Values	19	17	4	4	19	17	4	4	19	17	4	4	19	17	4	4	19	17	4
T’s Values	0	22	14	17	20	1	28	28	7	12	17	22	6	15	17	1	26	19	30
Key (FK)	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N
FK’s Values	10	8	13	6	10	8	13	6	10	8	13	6	10	8	13	6	10	8	13
Inverse (FK)	28	4	12	26	28	4	12	26	28	4	12	26	28	4	12	26	28	4	12
P’s Values	0	26	13	8	2	4	26	15	4	17	18	14	13	29	18	26	15	14	19
Plain Text	A		N	I	C	E		P	E	R	S	O	N	’	S		P	O	T

Fig. 13. Algebraic computing of decryption process.

VII. Conclusion

The Vigenere cipher regards as the simplest and weakest technique, which means it is very easy to detect by intruders or attackers. To overcome the weaknesses of the Vigenere cipher, we propose the Vigenère-Affine cipher that is a new polyalphabetic cipher with diffusion and confusion properties based on the concept of the complex cipher used by combining of Vigenère cipher with Affine cipher. As our proposed encryption technique is a complex transformation technique using two modified tables with a pair of key streams, it possesses high level diffusion and confusion properties. Thus, it hides the relationship between the cipher text and the plain text, and makes the cryptanalysis more difficult. On the other side, the modified tables of the proposed technique are designed not to make the meaningful sentences ambiguous for the receiver of the message. Furthermore, the concept of introducing the more characters in modified tables can be added so as to make the process of cryptanalysis more complex. Our proposed technique can also be extended by any language.

References

[1] B. A. Forouzan, “Traditional symmetric-key ciphers,” *Cryptography and Network Security*,” International Edition, Singapore, McGraw-Hill Press, pp. 55-90, 2008.

[2] D. E. Denning, “Encryption algorithms,” *Cryptography and Data Security*,” Addison Wesley Publishing Company Inc., U.S.A., pp. 59-125, 1982.

[3] Q. A. Kester, “A cryptosystem based on Vigenère cipher with varying key,” *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 1, no. 10, pp. 108-113, Dec. 2012.

[4] M. Khalid, N. Wadhwa, and V. Malhotra, “Alpha-qwerty cipher,” *International Journal of Advanced Computing*, vol. 3, no 3, pp 107-118, May 2012.

[5] Q. A. Kester, “A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher,” *International Journal of Advanced Technology and Engineering Research*, vol. 3, no. 1, pp. 141-147, Jan. 2013.

[6] O. E. Omolara, A. I. Oludare, and S. E. Abdulahi, “Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication,” *International Journal of Computer Engineering and Intelligent Systems*, vol. 5, no 5, pp. 34-46, 2014.

[7] N. Sinha and K. Bhamidipati, “Improving security of vigenère cipher by double columnar transposition,” *International Journal of Computer Applications*, vol. 100, no. 14, pp. 6-10, Aug. 2014.

[8] F. M. S. Ali, and F. H. Sarhan, “Enhancing security of vigenere cipher by stream cipher,” *International Journal of Computer Applications*, vol. 100, no. 1, pp. 1-4, Aug. 2014.

[9] A. Shah, “Enhancing security of vigenere cipher using modified RC4,” *International Journal of Computer Applications*, vol. 136, no 5, pp. 38-41, Feb. 2016.

[10] S. K. Mandal and A. R. Deepti, “A cryptosystem based on vigenere cipher by using mulitlevel encryption scheme,” *International Journal of Computer Science and Information Technologies*, vol. 7, no. 4, pp. 2096-2099, 2016.

[11] A. Subandi, R. Mieyanti, C. L. M. Sandy, and R. W. Sembiring, “Three-pass protocol implementation in vigenere cipher classic cryptography algorithm with keystream generator modification,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 5, pp. 1-5, 2017.

[12] 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.

Tun Myat Aung was born in Yangon, Myanmar. He passed matriculation exam with 3 subject distinctions in 1986. He got the B.Econ from Yangon University of Economics, M.I.Sc. from University of Computer Studies, Yangon (UCSY), M. Engnn & Tech (I.T) and Ph.D (I.T) from National Research Nuclear University MEPhI (Moscow Engineering Physics Institute). He is a professor from University of Computer Studies, Yangon (UCSY). He is interested in cryptography, stenography and network security, communication technology, software computing technology, database technology, business and economic information technology, mathematics and mobile computing.

Ni Ni Hla was born in Laputta, Myanmar. She is a lecturer from University of Computer Studies, Yangon (UCSY). She got M.Sc. (Maths) from Yangon University and M.I.Sc. from University of Computer Studies, Yangon. She is interested in mathematics, software computing, cryptography, coding theory, network and data security and stenography.

Htet Htet Naing was born in Taunggyi, Myanmar. She is an assistant lecturer from University of Computer Studies, Pinlon. She got M.C.Sc. from University of Computer Studies (Mandalay). Now she is a Ph.D candidate from University of Computer Studies, Yangon. She is interested in mathematics, software computing, cryptography, stenography, network and data security, embedding system and digital forensic.