2019 International Conference on Computer Communication and Informatics (*ICCCI* -2019), Jan. 23 – 25, 2019, Coimbatore, INDIA

A Complex Polyalphabetic Cipher Technique

Myanmar Polyalphabetic Cipher

Dr. Tun Myat Aung
Faculty of Computer Systems and Technologies
University of Computer Studies, Yangon (UCSY)
Myanmar
tunmyataung@ucsy.edu.mm

Ni Ni Hla
Faculty of Computing and Mathematics
University of Computer Studies, Yangon (UCSY)
Myanmar
ni2hla@ucsy.edu.mm

Abstract—**The rapid development of electronic exchange of digital information increases the importance of information security in storage and transmission of data on public communication network. Cryptography has emerged as a solution that plays a key role in the security of information against malicious attacks. There are various cipher techniques in cryptography, such as monoalphabetic cipher, polyalphabetic cipher, etc. to support data confidentiality as security mechanisms. They are methods of enveloping 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. The Vigenère cipher is one of the most common basic cipher techniques. It is a polyalphabetic cipher technique which uses the Vigenère table for the process of enveloping English alphabets. But Vigenère cipher 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. Then, our proposed technique is extended by designing based on Myanmar alphabet characters for the increase of data security for Myanmar language. This cipher technique transforms the plain text message in Myanmar alphabet characters into the cipher text in Myanmar alphabet characters using the key in Myanmar alphabet characters.**

***Keywords-** Affine cipher; monoalphabetic cipher; polyalphabetic cipher; Vigenère cipher; Myanmar alphabets*

I. INTRODUCTION

Cryptography is the study how to make a secret code. A cipher is a method of concealing that plain text is transformed into cipher text. The procedure of encoding plain text into cipher text is defined as encipherment or encryption; the procedure of decoding cipher text into plain text is defined as decipherment or decryption. Both encipherment and decipherment are controlled by cryptographic keys as shown in Fig. 1.

There are two kinds of basic ciphers: transpositions and substitutions. A transposition cipher changes the location of the elements. An element in the first place of the plain text may come out in the tenth place of the cipher text. An element in the eight place of the plain text may come out in the first place of the cipher text. In other words, a transposition cipher reorders (transposes) the elements. There are two methods for permutation of elements. In the first method, the element is written into a table column by column and then transmitted row by row. In the second method, the element 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.

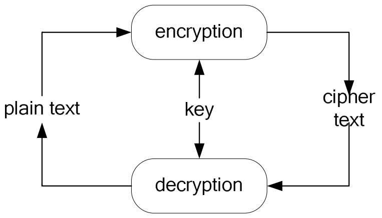


Figure 1. Secret Writing

A cipher Replacement replaces one element with another. If the elements in the plain text are alphabet characters, one character is replaced by another. Chips can be grouped into monoalphabetic chips and polyalphabetic chips. In monoalphabetic replacement, an element (or a symbol) in the plain text is always altered to the same element (or a symbol) in the cipher text without taking into account its position in the text. In monoalphabetic replacement, the mapping between an element in the plain text to an element in the cipher text is always one by one. In polyalphabetic replacement, each occurrence of an element may have a different substitute. The mapping between an element in the plain text to an element 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.

Modern ciphers have two key characteristics: diffusion and confusion. The diffusion concept must hide the correlation between the text of the chip and the plain text. This will

978-1-5386-8260-9/19/$31.00 ©2019 IEEE

frustrate the adversary who uses the cipher text statistics to find the plain text. The confusion concept is to hide the correlation between the cipher text and the key. This will frustrate the opponent who attempts to find the key using the cipher text. Diffusion and confusion can be achieved through Shannon's concept of a complex cipher known as a product cipher [3]. The capability of the cryptographic cipher technique depends upon the fact that how complex it is to be broken down by a cryptanalyst.

The cipher Vigenère is the most popular of the cipher techniques. It is a polyalphabet chip technique which uses the Vigenère table to encrypt and decrypt 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.

The purpose of this paper is to overcome the weaknesses of the Vigenere cipher and to extend our proposed technique by using Myanmar alphabet characters. The structure of this paper is as follows. The section 2 includes general knowledge of ployalphabetic cipher technique and its advantages. In section 3, we discuss Vigenère cipher technique and its weakness. The section 4 includes monoalphabetc ciphers such as additive cipher, multiplicative cipher and Affine cipher used to combine with our proposed technique. In section 5, we discuss our proposed technique. The section 6 extends our proposed technique by using Myanmar alphabet characters. Finally, in the section 7 we conclude our paper.

II. POLYALPHABETIC CIPHER TECHNIQUES

Around 1467, the Florentine architect Alberti innovated polyalphabetic ciphers [4]. He designed a cipher disk with a larger outer and smaller inner wheel, indexed by plaintext and ciphertext elements accordingly. Character arrangements made an easy replacement by rotating the disk. The German monk Trithemius published the first printed book on cryptography in 1518 [4], which contains a 24-elements square table listing all shift substitutions for a fixed arrangement of English alphabets. In 1553, Belaso suggested that the key should be easily varried to design the fixed alphabetic substitutions in a polyalphabetic substitution [4]. Polyalphabetic ciphers can hide the occurrence of the letter in the basic language. However, traditional polyalphabetic ciphers are not much harder to cryptanalyze; the traditional approaches are similar to the simple substitution cipher. Actually, when the block length can be determined, the cipher text elements can be divided into classes (where the class consists of those cipher text elements derived using permutation), and a frequency analysis can be done on each class [4].

A simple replacement cipher has a single mapping of the plaintext element onto cipher text elements. A more complex alternative is to use different substitution mappings (called multiple elements) on various portions of the plaint ext. This leads to so-called polyalphabet replacement. In the simplest case, the different elements are sequentially used and repeated so that the position of each plain text element in the source string determines which mapping is applied. Under different elements, the same plain text element is thus encrypted to different cipher text elements, 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 ciphertext element is made on the basis of the corresponding plaintext element and the position of the plaintext element in the message. This implies that the key ought to be a stream of subkeys, in which each subkey element relies somehow on the position of the character that uses that subkey for encipherment. In other words, a polyalphabetic cipher needs to have a key stream ($k = k_1, k_2, k_3, ...$) in which k_i is used to encipher the i^{th} element in the plain text to create the i^{th} element in the cipher text [3].

III. VIGENÈRE CIPHER

An interesting type of polyalphabetic cipher was designed by Blaise de Vigenère, a French mathematician from the 16th century. It was referred to as Vigenère cipher. It was the most common cipher in the ancient times because of its simplicity and resistance to the frequency analysis test of letters that could crack simple ciphers such as Caesar [4].

A. Encryption and Decryption

In Vigenère cipher a table of English alphabets is used for both encryption and decryption, termed as tabula recta, Vigenère square, or Vigenère table. In the table 26 English alphabets are alphabetically written out in different rows; each alphabet is shifted cyclically to the left row by row.

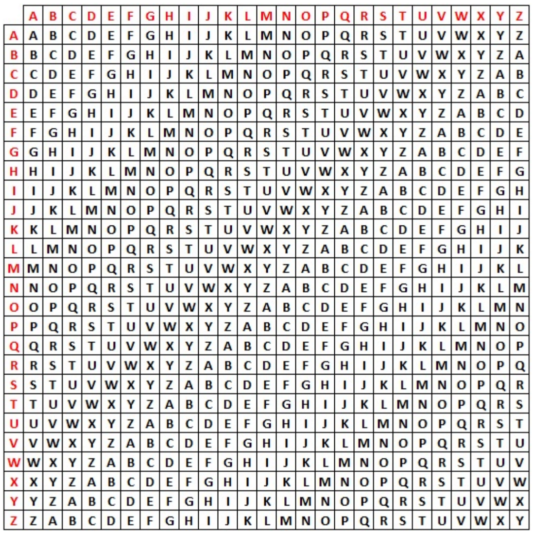
Each cipher element is denoted by a key element, which is the cipher text element that substitutes for the plain text element. Each of the 26 cipher elements is laid out horizontally, with the key element for each cipher element to itself. The Vigenère table is as shown in Fig. 2.

The cipher uses a different element from one of the rows of the Vigenère table at various points in the encryption or decryption processes. The element used depends on a repeating key stream at every point. In order to encrypt a message or plain text, the user should chose a key stream if the key stream length is equal to the plain text length. The cipher text element is at the intersection of the row labeled 'P' and the column labeled 'Q' for a given key element 'P' and the plain text element 'Q'; in which case the cipher text element is 'F'. Decryption is just as simple. The key element identifies the row again. The cipher text element's position in that row determines the column and plaintext element is at the top of the column [3].

The plain text, for example, is: "ATTACKOFFICE". The message sender selects a key stream and repeats it until its length matches with the length of the plaintext, e.g. the key "KING", then the key stream is: "KINGKINGKING".

The first element of the plaintext for encryption is ‘A’, which can be encrypted using the element in row ‘K’, which is the first element of the selected key stream. The cipher element is the intersection of the row ‘K’ and column ‘A’ of the Vigenère square, where the ‘K’ is, and the rest of the plain text elements will continue in this way. The cipher text for the chosen plaintext will be “KBGGMSBLPQPK”.

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



	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 2. Vigenère table

B. *Algebraic Description*

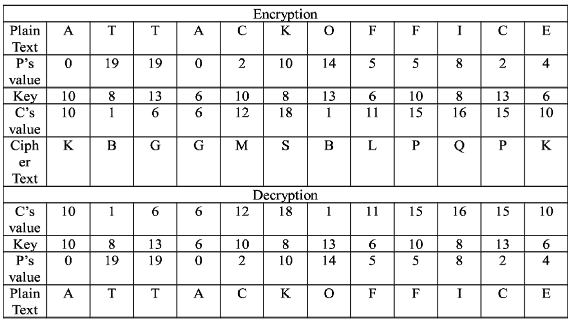
Cipher Vigenère can be viewed algebraically. If the letters ‘A’ to ‘Z’ are taken to be the numbers ‘0’ to ‘25’, and addition is performed modulo 26, then Vigenère encryption E can be written using the key K ,

$$C_i = E_K(P_i) = (P_i + k_i) \bmod 26 \qquad (1)$$

and decryption D using the key K ,

$$P_i = D_K(C_i) = (C_i - k_i) \bmod 26 \qquad (2)$$

Where as $P = P_1, P_2, ..., P_n$ is the plain text, $C = C_1, C_2, ..., C_n$ is the cipher text and $K = [(k_1, k_2, ..., k_m), (k_1, k_2, ..., k_m), ..., k_n]$ 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.



Encryption												
Plain Text	A	T	T	A	C	K	O	F	F	I	C	E
P's value	0	19	19	0	2	10	14	5	5	8	2	4
Key	10	8	13	6	10	8	13	6	10	8	13	6
C's value	10	1	6	6	12	18	1	11	15	16	15	10
Cipher Text	K	B	G	G	M	S	B	L	P	Q	P	K
Decryption												
C's value	10	1	6	6	12	18	1	11	15	16	15	10
Key	10	8	13	6	10	8	13	6	10	8	13	6
P's value	0	19	19	0	2	10	14	5	5	8	2	4
Plain Text	A	T	T	A	C	K	O	F	F	I	C	E

Figure 3. Algebraic Computing of Vigenère cipher

C. *Cryptanalysis*

Like all polyalphabetic ciphers, the design of Vigenère cipher is to conceal plain text letter occurrences which are contained in the basic application of frequency analysis. At different points in the message, the Vigenère cipher can encrypt each plain text element as different cipher text elements, defeating simple frequency analysis.

The key flaw of the Vigenère chip is the reproduction of the key. If a cryptanalyst correctly estimates the key length, the chip text can be broken easily. The Kasiski and Friedman tests can help determine the length of the key.

Kasiski Test began with Riedrich Kasiski in 1863 [4]. The cryptanalyst looks for frequent text pieces of at least three characters in the cipher text in Kasiski test. The distances between successive occurrences of the text chunks are likely to be multiples of the length of the keyword. Finding more frequent text chunks narrows down the possible lengths of the keyword, since we can compute the greatest common divisor of all the distances. The key length is the multiple of the greatest common divisor.

Friedman Test began with William Friedmanis in 1925 [4]. It is a statistical test that can be used to determine whether the chip text comes from a monoalphabetic or polyalphabetic chip. This technique uses the index of coincidence, to measure the inequality of the cipher letter occurrences. 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).

$$l = \frac{K_p - K_r}{K_o - K_r} \qquad (3)$$

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

Researchers suggested various modified approaches to improve the security of the Vigenère cipher as it was not secure over the years.

Kester (2012) proposed a Vigenère-based cryptosystem with a varying key [10]. This method was used to generate consecutive keys based on the initial key value used during the encryption process. The key was changed in the encryption process. The first step key was different from the second step key due to the first step function. The function was used to generate the key for the next encryption stage in subsequent stages. The decryption process was expected to take place abnormally due to the arbitrary generation of encryption keys for encryption, which might not result in the expected result.

Khalid (2012) proposed an alpha-qwerty cipher extending to the cipher Vigenère [6]. This method redesigned the Vigenère table to consist of 92 characters instead of 26 English alphabets. It then became a ninety-two by ninety-two matrix to improve the Vigenère table. It provided a larger set of character that allowed more message variants to be encrypted.

Kester (2013) proposed a Vigenère cipher-based hybrid cryptosystem with columnary transposition cipher [11]. This method used columnary transposition cipher to scramble a plaintext, which was then used as the key to the Vigenère cipher encryption process.

Omolara et al., (2014) proposed a hybrid cryptosystem based on Caesar cipher and Vigenère cipher for secure data communication [9]. A character key and a digit key were used for the encryption process. A Caesar cipher was performed on the character key using the shift of the digit key. Vigenère cipher is then performed on the plaintext using the new key. The binary equivalent of the text generated is then operated exclusively or with the digit key binary to generate the final ciphertext.

Nishith and Kishore (2014) proposed a method to improve the Vigenère cipher security by double columnar transposition [8]. This method used the Vigenère chip on a plaintext before using columnar transposition twice to transform the text further. When competing with the Vigenère chip, the computational complexity was increased.

Ali and Sarhan (2014) suggested an advanced encryption algorithm to improve the Vigenère cipher security [5]. This method combined Vigenère cipher with a current chip like stream cipher. Stream cipher is reasonably considered to be a resistant method and uses binary form instead of characters in which the plaintext, ciphertext and the key are bit streams.

Ashish Shah (2016) proposed an encryption scheme to improve the Vigenère cipher security [1]. This method transformed Vigenère cipher into a product cipher by combining two encryption schemes methodically: RC4 and Vigenère are re-designed.

Mandal and Deepti (2016) proposed a multi-level encryption scheme for Vigenère cipher to improve cryptanalysis security [12]. This method selected the same fixed length of plain text and key and used it in Vigenère table to obtain a new text. The new text was used as a new key. Using the new key the cipher text was transformed more and sends the final cipher text to the receiver. At last the receiver does the decryption in reverse way.

Subandi et al., (2017) developed the three-pass protocol using Vigenère cipher with modification of keystream generator [2]. This method changed the key on Vigenère Cipher. Consequently, if the key length was smaller than the input plaintext length, the key would be generated by a process, so the next key nature would be different from the previous key nature. This method used three-pass protocol, in which message sender does not need to send the key, since each uses its own key for the message encryption and decryption processes, so protecting a message would be more complicated to solved.

V. Monoalphabetic Cipher Techniques

Current ciphers usually use a mixture of substitution with transposition and some other complex transformations to create a cipher text from a plain text. In our paper we stressed the need to propose a new combination method, Vigenère cipher with Affine cipher, because the cipher based on simple Vigenère method is not safe. An Affine chip is a mixture of the additive chip with the multiplicative chip. Additive chips, multiplicative chips and Affine chips 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 [3]. 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	Λ	B	C	D	E

Figure 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 [3]. 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 $C = P \times K(\bmod 26)$. Then, $C = 7 \times 5 = 9(\bmod 26)$. 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	c	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	II	M	R	W	B	G	L	Q	V	A

Figure 5. Multiplicative Cipher Table

C. *Affine Cipher*

The Affine cipher is a monoalphabetic substitution cipher variant, in which each element in an alphabet is mapped to its numerical value; each element is converted into a code using a simple mathematical transformation, and a code is converted back to an element in an alphabet. The applied formula means that each letter turns to one other, and back again. It means the cipher is essentially a typical replacement chip that follows a rule principal which letter goes to which. An Affine chip is created by combining the additive chip with multiplicative chip. It is a combination of both chips with a couple of keys. The first key is used with the cipher multiplier, the second key is used with the cipher additive [3]. The two keys are shared secret keys for both the sender and the message receiver. Fig. 6 shows that the Affine chip is in fact two chips, applied one by one, including only one complex operation for the encryption or decryption such as $C = ((P \times k_1) + k_2) \bmod n$ and $P = ((C - k_2) \times k_1^{-1}) \bmod n$. ‘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 chip 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.

1) *Algebraic Description*

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

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

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 [7]. The decryption function is defined as equation (5).

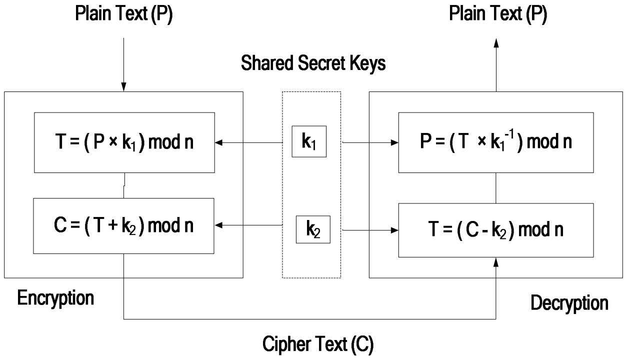


Figure 6. Affine Cipher

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

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

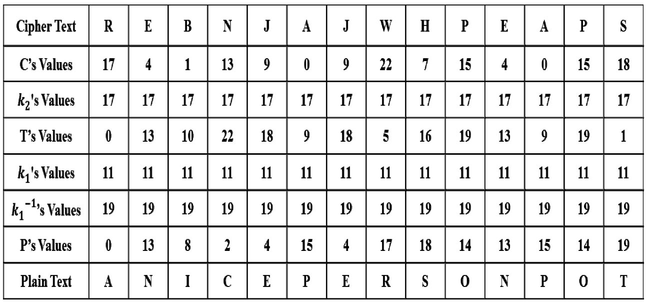
$$1 \equiv k_1 . k_1^{-1} \bmod n \tag{6}$$

The multiplicative inverse of k_1 only exists if k_1 and n are coprime [7].

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

Figure 7. Encryption of Affine Cipher

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 Fig. 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”.



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

Figure 8. Decryption of Affine Cipher

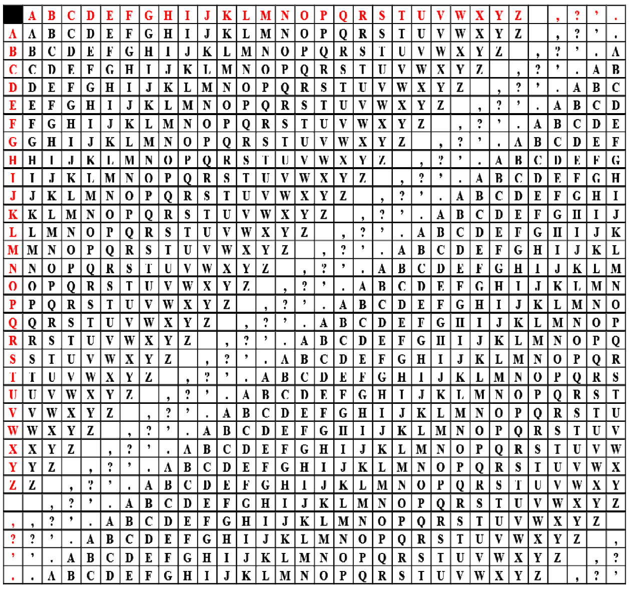
VI. Proposed Technique

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

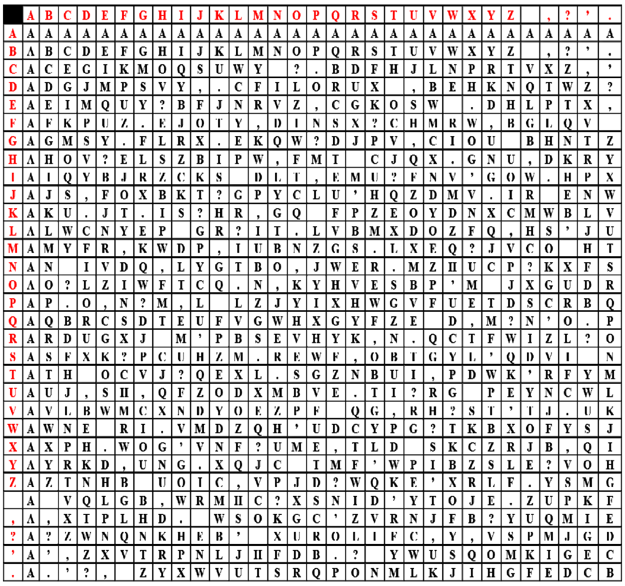
Our proposed technique uses two kinds of tables: addition table and multiplication table. The modified tables are designed by using English alphabet 26 characters and appending another six essential characters such as space, comma, question mark, apostrophe, and full stop to avoid ambiguous meanings 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 [7]. 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.



	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		,	?	’

Figure 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	I	’	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

Figure 10. Multiplication Table

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".

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.

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

Where $P = P_1, P_2, \ldots, P_n$ is denoted as the plain text, $C = C_1, C_2, \ldots, C_n$ is denoted as the cipher text, $FK = [(fk_1, fk_2, \ldots, fk_m), (fk_1, fk_2, \ldots, fk_m), \ldots, fk_n]$ is denoted as the first key stream, $SK = [(sk_1, sk_2, \ldots, sk_m), (sk_1, sk_2, \ldots, sk_m), \ldots, sk_n]$ 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.

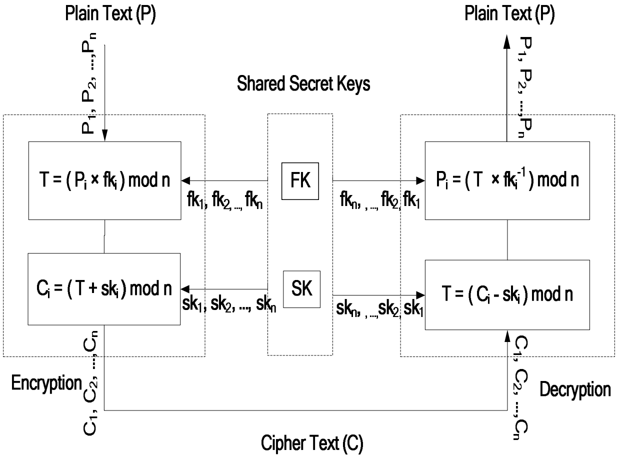

Plain Text (P)
$P_1, P_2, \ldots, P_n$
Shared Secret Keys
Plain Text (P)
$P_1, P_2, \ldots, P_n$
$T = (P_i \times fk_i) \bmod n$
$fk_1, fk_2, \ldots, fk_n$
FK
$fk_n, \ldots, fk_2, fk_1$
$P_i = (T \times fk_i^{-1}) \bmod n$
$C_i = (T + sk_i) \bmod n$
$sk_1, sk_2, \ldots, sk_n$
SK
$sk_n, \ldots, sk_2, sk_1$
$T = (C_i - sk_i) \bmod n$
$C_1, C_2, \ldots, C_n$
Encryption
$C_1, C_2, \ldots, C_n$
Decryption
Cipher Text (C)

Figure 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

Figure 12. Algebraic Computing of Encryption Process

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

Figure 13. Algebraic Computing of Decryption Process

VII. MYANMAR POLYALPHABETIC CIPHER

Our proposed technique can also be extended by any language. In this section, our proposed technique is extended by Myanmar language for the increase of data security for Myanmar language. This cipher technique transforms the plain text message in Myanmar alphabet characters into the cipher text in Myanmar alphabet characters using the key in Myanmar alphabet characters.

A. Encryption and Decryption

Myanmar Unicode Character Map includes 160 characters [13]. To extend our proposed technique by Myanmar language we must first really design the modified tables, addition table and multiplication table, using 160 characters of Myanmar alphabet. Thus, the size of these tables is 160×160. But, these tables' designs are too large to fit the size of the paper. Thus, the modified tables are designed, for example, by the limitation of the characters of Myanmar alphabet, based on characters that include in the message and the keys. The following example includes a total of 17 different characters of Myanmar alphabet as shown in Fig. 14. Thus, the size of these tables is 17×17. The additive table with Myanmar alphabet characters is shown in Fig. 15 and the multiplication table with them is shown in Fig. 16. These tables are created by using character position numbers of Myanmar alphabet and our implementation system of finite field arithmetic operations [7] and used for encryption and decryption processes like Vigenère-Affine cipher.

For example,

The plain text: ပန်းကလေးများ ဖူးပွင့်နေသည်
The first key: ညနေ
The second key: ကောင်းကင်

The plain text consists of 25 characters. The sender of the message chooses two keys and repeats it until its length matches with the length of the plain text. These two keys are shared secret keys for both the sender and the receiver of the message. The Fig. 17 shows the encipherment and the decipherment of the Myanmar polyalphabetic cipher using the Myanmar addition table and Myanmar multiplication table. In the figure the symbol 'P' is denoted as plain text, 'C' as cipher text, 'K' as keys and 'T' as temporary storage.

For the first step transformation of encryption process, the first letter of the plain text can be enciphered using the alphabet in the row 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 and the column of the Myanmar multiplication table. For the second step transformation using additive cipher, the letter that got from multiplicative cipher can be again enciphered using the alphabet in the row which is the first letter of the second key stream. In additive cipher, the cipher letter is the intersection of the row and the column of the Myanmar addition table. The rest of the plain text will continue in these procedures.

For the first step transformation of decryption process, using Myanmar addition table, in the row identified by the first letter of the second key stream, the corresponding cipher letter appears in the column which is the first letter got from the additive cipher. For the second step transformation using Myanmar multiplication table, in the row identified by the first letter of the first key stream, the corresponding letter got from the additive cipher appears in the column which is the first plaintext letter got from the multiplicative cipher. The rest of the cipher text will continue in these procedures.

Encryption

P	ပ	န	်	း	က	ေ	လ	း	မ	ျ	ာ	း	ဖ	ူ	း	ပ	ွ	င	်	့	ေ	န	သ	ည	်
K	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည
T	ပ	ေ	်	ေ	း	ေ	ူ	သ	မ	ာ	ူ	း	မ	က	း	ပ	ာ	င	သ	်	ေ	ည	မ	ည	သ
K	ေ	က	ာ	င	်	း	က	င	်	ေ	က	ာ	င	်	း	က	င	်	ေ	က	ာ	င	်	း	က
C	ေ	ာ	ူ	ဖ	ေ	ျ	သ	ူ	ာ	့	သ	ွ	း	လ	လ	က	ေ	သ	း	လ	့	ွ	ာ	်	်

Decryption

C	ေ	ာ	ူ	ဖ	ေ	ျ	သ	ူ	ာ	့	သ	ွ	း	လ	လ	က	ေ	သ	း	လ	့	ွ	ာ	်	်
K	ေ	က	ာ	င	်	း	က	င	်	ေ	က	ာ	င	်	း	က	င	်	ေ	က	ာ	င	်	း	က
T	ပ	ေ	်	့	း	ေ	ူ	သ	မ	ာ	ူ	း	မ	က	း	ပ	ာ	င	သ	်	ေ	ည	မ	ည	သ
K	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည	ေ	န	ည
P	ပ	န	်	း	က	ေ	လ	း	မ	ျ	ာ	း	ဖ	ူ	း	ပ	ွ	င	်	့	ေ	န	သ	ည	်

Figure 14. Encipherment and Decipherment Using Myanmar Tables

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည

Figure 15. Character Map

	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည
ပ	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည
န	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ
်	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န
း	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်
က	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း
ေ	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က
လ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ
မ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ
ျ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ
ာ	ာ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ
ဖ	ဖ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ
ူ	ူ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ
ွ	ွ	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ
င	င	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ
့	့	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င
သ	သ	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့
ည	ည	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ

Figure 16. Myanmar Addition Table

	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည
ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ	ပ
န	ပ	န	်	း	က	ေ	လ	မ	ျ	ာ	ဖ	ူ	ွ	င	့	သ	ည
်	ပ	်	က	လ	ျ	ဖ	ွ	့	ည	န	း	ေ	မ	ာ	ူ	င	သ
း	ပ	း	လ	ာ	ွ	သ	န	က	မ	ဖ	င	ည	်	ေ	ျ	ူ	့
က	ပ	က	ျ	ွ	ည	း	မ	ူ	သ	်	လ	ဖ	့	န	ေ	ာ	င
ေ	ပ	ေ	ဖ	သ	း	ျ	င	န	လ	ူ	ည	က	ာ	့	်	မ	ွ
လ	ပ	လ	ွ	န	မ	င	်	ျ	့	း	ာ	သ	က	ဖ	ည	ေ	ူ
မ	ပ	မ	့	က	ူ	န	ျ	သ	ေ	ွ	်	ာ	ည	လ	င	း	ဖ
ျ	ပ	ျ	ည	မ	သ	လ	့	ေ	င	က	ွ	း	ူ	်	ဖ	န	ာ
ာ	ပ	ာ	န	ဖ	်	ူ	း	ွ	က	င	ေ	့	လ	သ	မ	ည	ျ
ဖ	ပ	ဖ	း	င	လ	ည	ာ	်	ွ	ေ	သ	ျ	န	ူ	က	့	မ
ူ	ပ	ူ	ေ	ည	ဖ	က	သ	ာ	း	့	ျ	်	င	မ	န	ွ	လ
ွ	ပ	ွ	မ	်	့	ာ	က	ည	ူ	လ	န	င	ျ	း	သ	ဖ	ေ
င	ပ	င	ာ	ေ	န	့	ဖ	လ	်	သ	ူ	မ	း	ည	ွ	ျ	က
့	ပ	့	ူ	ျ	ေ	်	ည	င	ဖ	မ	က	န	သ	ွ	ာ	လ	း
သ	ပ	သ	င	ူ	ာ	မ	ေ	း	န	ည	့	ွ	ဖ	ျ	လ	က	်
ည	ပ	ည	သ	့	င	ွ	ူ	ဖ	ာ	ျ	မ	လ	ေ	က	း	်	န

Figure 17. Myanmar Multiplication Table

The followings show the algebraic computing of Myanmar polyalphabetic cipher. It uses the equation (7) for the encryption process shown in Fig. 18 and the equations (8) and (9) for the decryption process shown in Fig. 19, using the algebraic computing that is described in the section (6.2).

Plain Text	ပ	န	◌်	◌း	က	◌ေ	လ	◌း	မ	◌ျ	◌ာ	◌း	ဖ	◌ူ	◌း	ပ	◌ွ	င	◌်	◌့	◌ေ	န	သ	ည	◌်
P's Values	0	1	2	3	4	5	6	3	7	8	9	3	10	11	3	0	12	13	2	14	5	1	15	16	2
Key (FK)	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည
Key's Values	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16
T's Values	0	5	2	14	3	5	11	15	7	9	11	3	7	4	3	0	9	13	15	2	5	16	7	16	15
Key (SK)	◌ေ	က	◌ာ	င	◌်	◌း	က	င	◌်	◌ေ	က	◌ာ	င	◌်	◌း	က	င	◌်	◌ေ	က	◌ာ	င	◌်	◌း	က
Key's Values	5	4	9	13	2	3	4	13	2	5	4	9	13	2	3	4	13	2	5	4	9	13	2	3	4
C's Values	5	9	11	10	5	8	15	11	9	14	15	12	3	6	6	4	5	15	3	6	14	12	9	2	2
Cipher Text	◌ေ	◌ာ	◌ူ	ဖ	◌ေ	◌ျ	သ	◌ူ	◌ာ	◌့	သ	◌ွ	◌း	လ	လ	က	◌ေ	သ	◌း	လ	◌့	◌ွ	◌ာ	◌်	◌်

Figure 18. Algebraic Computing for Myanmar Encryption Process

Cipher Text	◌ေ	◌ာ	◌ူ	ဖ	◌ေ	◌ျ	သ	◌ူ	◌ာ	◌့	သ	◌ွ	◌း	လ	လ	က	◌ေ	သ	◌း	လ	◌့	◌ွ	◌ာ	◌်	◌်
C' s Values	5	9	11	10	5	8	15	11	9	14	15	12	3	6	6	4	5	15	3	6	14	12	9	2	2
Key (SK)	◌ေ	က	◌ာ	င	◌်	◌း	က	င	◌်	◌ေ	က	◌ာ	င	◌်	◌း	က	င	◌်	◌ေ	က	◌ာ	င	◌်	◌း	က
K's Values	5	4	9	13	2	3	4	13	2	5	4	9	13	2	3	4	13	2	5	4	9	13	2	3	4
T's Values	0	5	2	14	3	5	11	15	7	9	11	3	7	4	3	0	9	13	15	2	5	16	7	16	15
Key (FK)	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည	◌ေ	န	ည
Key's Values	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16	5	1	16
Key's Inverse	16	7	1	16	7	1	16	7	1	16	7	1	16	7	1	16	7	1	16	7	1	16	7	1	16
P's Values	0	1	2	3	4	5	6	3	7	8	9	3	10	11	3	0	12	13	2	14	5	1	15	16	2
Plain Text	ပ	န	◌်	◌း	က	◌ေ	လ	◌း	မ	◌ျ	◌ာ	◌း	ဖ	◌ူ	◌း	ပ	◌ွ	င	◌်	◌့	◌ေ	န	သ	ည	◌်

Figure 19. Algebraic Computing for Myanmar Decryption Process

VIII. CONCLUSION

The Vigenere cipher sees it as the simplest and weakest technique, making it easy for intruders or attackers to detect it. 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 complex cipher concept used to combine Vigenère cipher with Affine cipher. Since our proposed encryption technique is a complex process of transformation using two modified tables with a pair of key streams, it has high level diffusion and confusion properties. It hides the correlation between the cipher text and the plain text, and makes the cryptanalysis more difficult. On the other hand, the modified tables of the proposed technique are designed for the message recipient not to be ambiguous in a sentence. In addition, the idea of introducing the more characters in modified tables can be added so that the cryptanalysis process is more complex. Our proposed technique can also be extended by any language and it has now been done by using characters of Myanmar alphabet. Myanmar polyalphabetic cipher can also be extended for military purpose and e-government system of Myanmar.

REFERENCES

[1] A. Shah, "Enhancing Security of Vigenere Cipher using modified RC4", International Journal of Computer Applications, vol. 136, no 5, pp 38-41, Feb. 2016.

[2] A. Subandi, R. Mieyanti, C. L. M. Sandy, 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, pp1-5, 2017.

[3] B. A. Forouzan, "Traditional Symmetric-Key Ciphers", in "Cryptography and Network Security", International Edition, Singapore, McGraw-Hill press, 2008, pp 55-90.

[4] Dorothy E. Denning, "Encryption Algorithms", in Cryptography and Data Security", Addison Wesley Publishing Company Inc., U.S.A., 1982, pp 59-125.

[5] F. M. S. Ali, 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.

[6] M. Khalid, N. Wadhwa, V. Malhotra, "Alpha-Qwerty Cipher", International Journal of Advanced Compting, vol. 3, no 3, pp 107-118, May 2012.

[7] N. N. Hla, 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 (IJERT), Volume 6, Issue 08, pp 450-453, August – 2017, DOI: 10.17577/IJERTV6IS080209.

[8] N. Sinha, 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.

[9] O. E. Omolara, A. I. Oludare, 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.

[10] 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.

[11] 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.

[12] S. K. Mandal, 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.

[13] https:/unicode.org/charts/PDF/U1000.pdf