Innovation Security of Beaufort Cipher by Stream Cipher Using Myanmar-Vigenere Table and Unicode Table

Htet Htet Naing[1+], Zin May Aye [2]

[1] University of Computer Studied (Yangon), Myanmar

[2] University of Computer Studied (Yangon), Myanmar

Abstract. Nowadays, securing information and message transformation are going with electronic way, the security becomes very important role on public network. Cryptography is readable message convert to unreadable message using encryption/decryption process. Encryption Process is sender and decryption process are receiver side. Commonly, information can be storing with international language such as English language. At the present time, everyone is trying to be more secure not only English but also own language such as Myanmar, Chinese, Tamil etc. Confidential data are transferred through with regional language by using with more innovative method. To secure such information, encryption/decryption plays an important role in information security. In cryptography, there are several cipher techniques such as, polyalphabetic cipher, Stream cipher, Block cipher etc. This section using Beaufort cipher is an example of substitution cipher, In this paper, we propose an advanced encryption algorithm that improves the security of Beaufort encryption by combining it with a modern encryption method such as Stream cipher for the Myanmar language, Stream cipher is considered relatively as an unbreakable method and uses a binary form (instead of characters) where Plain text, encrypted text and key are bit string.

Keywords: cryptography, encryption, decryption, Beaufort Cipher, Stream Cipher

1. Introduction

Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques we use the same key for both encryption and decryption purpose [1]. Asymmetric-key encryption using public and private keys, the public key is announced to all members while the private key is kept secure by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message. In symmetric method, there are two techniques (substitution and transposition) are used as a classical method [1]. The Beaufort cipher, is a substitution cipher similar to the Vigenère cipher, with a slightly modified enciphering mechanism and tableau [2]. Its most famous application was in a rotor-based cipher machine. Substitution has further two types, Mon oalphabetic and polyalphabetic cipher [3]. In monoalphabetic the character in the Plaintext is changed to the same character in the Ciphertext. In polyalphabetic cipher a single character in the Plaintext is changed to many characters in the Ciphertext .Permutation technique is one in which the Plaintext remains the same, but the order of characters is shuffled around to get the Ciphertext .Also the symmetric ciphers can be divided into Stream ciphers and block ciphers, as a modern ciphers [4]. Stream ciphers encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time. Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size [5].

2. Background Theory

2.1. Vigenere Cipher

The Vigenere cipher is a plain-text form of encoding that uses alphabetical substitution to encode text. The Vigenere cipher, like other contemporary cryptographic ciphers, uses something called a tabula recta .The encryption of the original text is done using the *Vigenère square or Vigenère table.*

- The first row of this table has the 26 Character. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26possible
- The first row of this table has the 26 Character. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26possible.
- The alphabet used at each point depends on a repeating keyword.

Table 1: Vigenere 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	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

2.2. Beaufort Cipher

Beaufort cipher is a polyalphabetic substitution cipher and a variant of Vigenère cipher. Encryption and decryption using Beaufort cipher is achieved though the same algorithm. To encrypt a message, repeat the Keyword above the Cipher. If the plaintext is “S” with key “T”. Find the column with “S” on the top and travel down that column to find key “T”. Travel to the left edge of the tableau to fine the cipher text. To decrypt, the reverse the encryption process. The Beaufort Cipher using the Vigenere Cipher Table.

The Beaufort cipher can be described algebraically. The Beaufort cipher using an encoding of the letters A-Z as the numbers 0-25 and using addition modulo 26, let M=M1……Mn be the characters of the message, C= C1….Cn be the characters of the cipher text and K=K1….Kn be the character of the key, repeated if necessary. Then Beaufort encryption E is written,

$$C=EK(Mi) = (Ki- Mi) \bmod 26$$

Similarly, decryption D using the key K

$$Mi=Dk(Ci) = (Ki -Ci) \bmod 26$$

2.3. Stream Cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as **state cipher**. In practice, a digit is typically a bit and the combining operation is an exclusive-or (XOR) [6].

The Stream cipher is classified as a *synchronous* stream cipher. By contrast, *self-synchronizing* stream ciphers update their state based on previous ciphertext digits [7].

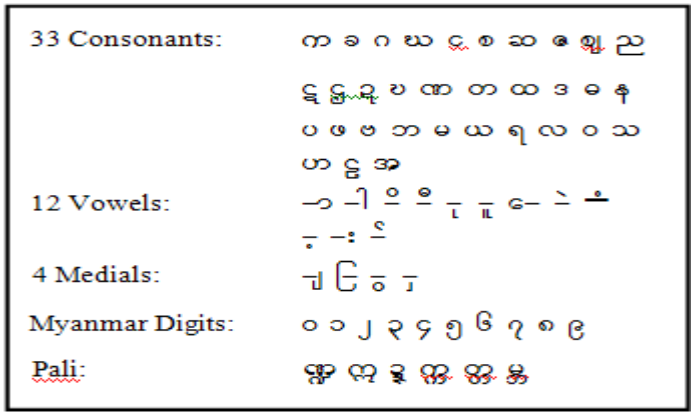

Fig. 1: Sample a set of Myanmar Alphabet

3. Proposed System

In normal Vigenere table uses a 26×26 table with A to Z as the row heading and column heading. Traditionally Myanmar Fonts have been pretending to be English fonts. This means that they are using the numbers allocated for the Latin alphabet to represent Myanmar characters. Our paper propose method uses a 31×31 table in Myanmar Language Vigenere table. These 31 characters is the mostly used of Myanmar character. This table is usually referred to as the Original Vigenère Table. The first row of this table has the 31 Myanmar Character. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. The table consists of the alphabets written out 31 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 31 possible. Modern cipher is normally use combination of substitution with transposition. In this paper, we proposed a new combination method Beaufort cipher by using Myanmar Vigenere Table. In this paper, Myanmar Character □-□ as the number 0-31 after getting the cipher text. In Stream Cipher, half of work, for example the user enters the message in Myanmar language and this is divided into each work. And then half of work the message length. For example, the message length is 20, the first 10 Myanmar character are encrypted with Beaufort Cipher and last 10 Myanmar character are encrypted with Stream Cipher. The stream cipher process using binary code, so Myanmar Character Unicode are converted to Binary code [7-8].

Table 2: Propose Myanmar Vigenere Table

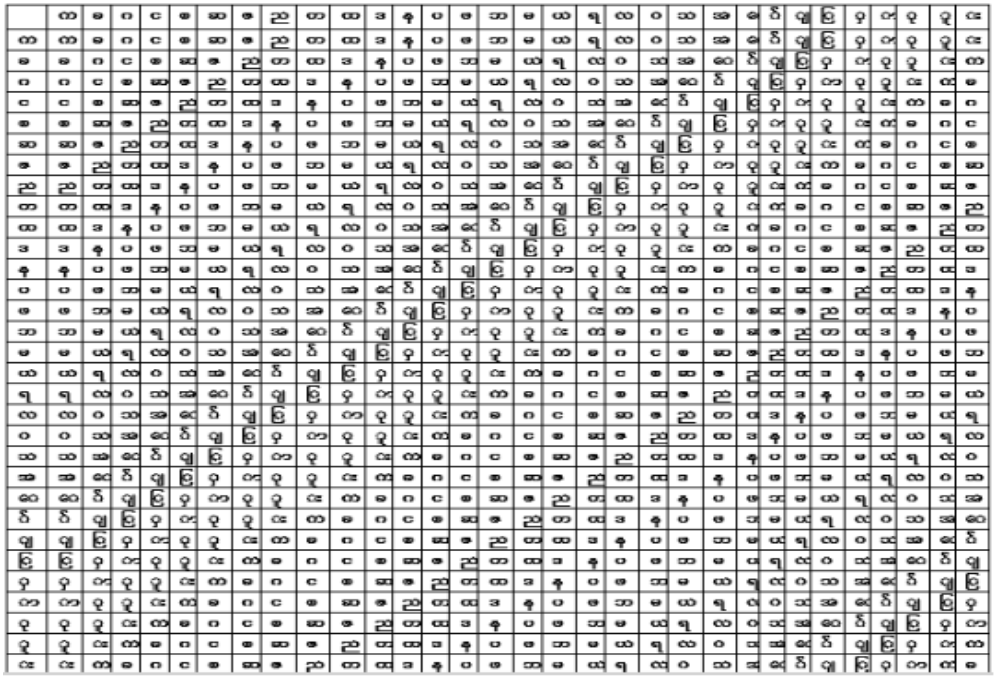

Table 3: Sample of Myanmar Unicode And Binary Code Table

က 10000000	ခ 10000001	ဂ 10000010	ဃ 10000100	စ 10000101	ဆ 10000110
ဇ 10000111	ည 10001010	တ 10010000	ထ 10010001	ဒ 10010010	န 10010100
ပ 10010101	ဖ 10010110	ဘ 10011000	မ 10011001	ယ 10011010	ရ 10011011
လ 10011100	ဝ 10011101	သ 10011110	အ 10100001	ဧ 10110001	ဵ 10110101
ျ 10111011	ြ 10111100	ွ 10111101	ာ 10101100	ု 10101111	ူ 10110000
း 10111000					

3.1. Step by Step of Proposed System Process

1. Start
2. Read Plaintext P
3. Read Key K
4. Using Beaufort equation C =K-M or Beaufort cipher by using Vigenere Table the characters in First half locations of Plaintext.
5. Apply stream cipher to encipher each character in the second half location as follows:
   - Converting the characters to Unicode value then to equivalent binary form.
   - Enciphering these characters using stream cipher equation C = P $\oplus K_{bin}$.
   - Converting the resulted binary numbers to equivalent Unicode value then to characters to obtain the Cipher characters.

Plaintext: ကျောင်းသားများ စာဖတ်နေသည်

(English : the students are learning)

Key: စာအုပ်

(English : Book)

Plaintext: ကေ ကျ တာ c ်ိ း သ တာ း မ ျ တာ း စ တာ ဖ တ ်ိ ေ န သ ည ်ိ

Key: စ တာ အ ု ပ ်ိ စ တာ အ ု ပ ်ိ စ တာ အ ု ပ ်ိ စ တာ အ ု

	0	1	2	3	4	5	6	7	8	9	10	11
Plain text	ေ	က	ျ	တ	c	်ိ	း	သ	တ	း	မ	ျ
Key	စ	တ	အ	ု	ပ	်ိ	စ	တ	အ	ု	ပ	်ိ
Cipher Text	ဖ	တ	ု	ခ	ထ	က	ဆ	ည	ြ	ူ	ု	း

Table 4: Encryption Beaufort Cipher of First Half Location by Using Myanmar-Vigenere Table

	13	14	15	16	17	18
Plain text	တ	း	စ	တ	ဖ	တ
Unicode equivalent	4140	4152	4101	4140	4118	4112
Key	စ	တ	အ	ု	ပ	်ိ
P_{bin} $\ominus$ K_{Bin}	10101100 10000101	10111000 10101100	10000101 10100001	10101100 10101111	10010110 10010101	10010000 10110101
C_{Bin}	00101001	00010100	00100100	00000011	00000011	00100101
CipherText	ဩ	န	ဤ	ဃ	ဃ	ဥ

Table 5: Encryption of Stream Cipher for Second Half Location by Using Myanmar Unicode Table

$C=P_{bin} \oplus K_{bin}$

	19	20	21	22	23	24
Plain text	ိ	ေ	ာ	သ	ည	ိ
Unicode equivalent	4149	4145	4116	4126	4106	4149
Key	ဓ	ဝ	ဆ	ဍ	ဂ	ဒ
P_{bin} ⊕ K_{Bin}	10110101 10000101	10110001 10101100	10010100 10100001	10011110 10101111	10001010 10010101	10110101 10110101
C_{Bin}	00110000	00011101	00110101	00110001	00011111	00000000
CipherText	ွ	ံ	ိ	ေ	ဟ	ဝ

4. Scope and Limitation of Proposed System

Proposed System aimed to the security of Myanmar Language. Security in cryptography is based on how secure the algorithm is against various attacks for Myanmar Language. Myanmar Language contain consonants, vowels, Medial, virama, Myanmar digits and Pali. Some Limitation of our proposed system. In our system can use only Myanmar Characters on the above table (Table 2). I didn't think about Pali (ပါဠိ) for Myanmar Language.

5. Conclusion

Beaufort cipher regard as simplest and weakest method, that mean it is very easy to attack. To overcome the limitations of this method, we propose a new algorithm which includes combining Beaufort substitution cipher with Stream cipher. We notice that repeated portions of plaintext always encrypted with the different portion of the keyword or binary key, because we encipher the letters in first location with Beaufort cipher and the letters in second locations with Stream cipher, result in different ciphertext segments, that mean proposed algorithm hides the relationship between Ciphertext and Plaintext, and makes the cryptanalysis more difficult. Furthermore, the proposed combination method enhances the security of Vigenere method and make the detection process not easy, because the Stream cipher relatively regards as unbreakable. This paper attempts to enhance the encryption / decryption of the regional language.

6. References

[1] Paar C. and Pelzl J. 2010, Understanding Cryptography, Springer-Verlag Berlin Heidelberg.

[2] https://en.wikipedia.org/wiki/Beaufort_cipher

[3] Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan "Enhancing Security of Vigenere Cipher by Stream Cipher". International Journal of Computer Applications (0975 –8887). Volume 100–No.1, August2014

[4] T.M. Aung, H.H. Naing"AComplexTransformationofMonoalphabeticCiphertoPolyalphabeticCipher:(Vigenère-AffineCipher)". International Journal of Machine Learning and Computing, Vol. 9, No. 3, June 2019

[5] https://en.wikipedia.org/wiki/Block_cipher

[6] https://www.Utf8-chartable.de/Unicode-utf8-table.pl?start=4096&number=128&utf8=string-literal

[7] https://en.wikipedia.org/wiki/Stream_cipher

[8] "https://www.unicode.org/notes/tn11/UTN11_3.pdf