Vigenere Cipher: Trends, Review and Possible Modifications

Al-Amin Mohammed Aliyu
Department of Mathematics,
Ahmadu Bello University Zaria, Nigeria

Abdulrahman Olaniyan
Department of Electrical Engineering,
Ahmadu Bello University Zaria, Nigeria

ABSTRACT

Vigenere cipher is one of the earliest known polyalphabetic cipher which was considered secure for a very long time until 1917 when friedman and kasiski were able to break it by determining repeating segments of the ciphertext and using it to determine the length of the key. Once the length of the key is known, the ciphertext could be grouped in columns and treated as a separate caesar cipher which can be solved. Over the years, a lot of modification has been done to inprove the security of the vigenere cipher. This paper presents a review of the vigenere cipher and also discusses various existing modifications.

General Terms

Cryptography is the art and science of protecting information from unauthorized individuals.

Encryption is a way of converting information (plaintext) into a form that is unreadable to unauthorized individuals (ciphertext).

Keywords

Cipher, Cryptography, Encryption, Substitution, Vigenere.

1. INTRODUCTION

Cryptography is a concept which is defined as the art and science of making information or communications unintelligible to all except the intended recipients, by converting it into a form that is not recognizable by an adversary [4]. Cryptography comprises of two processes – encryption and decryption [11]. Encryption is the process of converting message or plaintext into a form which is unreadable to users with unauthorized access but understandable to an authorized personnel. On the other hand, decryption is the process of converting an encrypted message (ciphertext) into a form that is understandable by an authorized person [8]. The message to be encrypted is known as plaintext, while the encrypted message is known as ciphertext. Through the ages, cryptography was strictly used for military and diplomatic circumstances, where it was used in concealing information communicated over secure and insecure lines [7]. Modern day cryptography, is however said to be defined as the scientific study of techniques for securing digital information, transactions, and distributed computations. There are four basic objectives involved in the process of cryptography. These are: authentication, integrity, privacy/confidentiality and non-repudiation [10].

The concept of cryptography are divided into two basic components of substitution and transposition [15]. In substitution ciphers, letters are replaced by other letters in order to produce the ciphertext, while transposition cipher involves scrambling the letters of a plaintext such that they occupy a different position [18]. There are a number of cryptographic primitives which defines the basic building block of cryptography, such as block ciphers, stream ciphers, and hash functions. A block cipher processes the input; one block of elements at a time, to produce an output block for each input block. A stream cipher on the other hand processes the input elements one bit at a time continuously, to produce the output element. Hash functions are also a type of cryptographic algorithm that takes message of any length as input, and output them into shorter strings, which can be used in a digital signature [6]. Other cryptographic protocols and algorithms are known as symmetric and asymmetric encryption [18]. Symmetric encryption is the type of encryption where a single key is used for both encryption and decryption. It is also known as private key cryptography. Asymmetric Encryption on the other hand is the type of encryption whereby two keys are used in the cryptographic process; one for encryption/encoding (also known as the public key), while the other key used for decoding/decryption process is known as the private key. This kind of encryption is known as public-key cryptography [14].

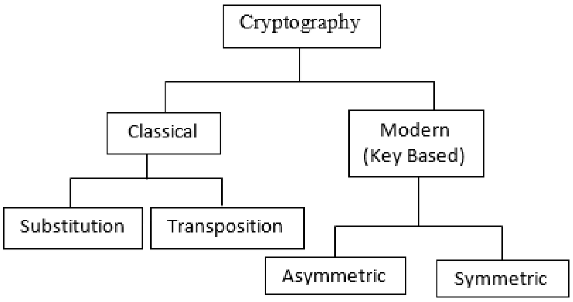


Figure 1: Overview of Cryptography [6]

Cryptanalysis is a technique that is used for forcefully recovering plaintext (encrypted text) from a known ciphertext without prior knowledge of the key that was used for the encryption process [18]. Cryptanalysis is also known as the process of breaking of codes (ciphers) in order to get access to unauthorized information (Morkel, n.d). Both cryptography and cryptanalysis are concepts derived from a general body of knowledge which is the science of concealing, known as cryptology. Information security is a way of protecting information from users with unauthorized access to avoid disruption, modification, alteration, recording or destruction (wikipedia, 2015). The objectives of computer security are integrity, confidentiality, availability, authenticity and accountability. Caesar cipher is one of the earliest known classical encryption technique developed by Julius Caesar to communicate with his army (Vinod, 2012).

Caesar cipher is one of the first encryption scheme employed for the sake of securing a message. It is carried out by shifting each letter three places down the alphabet in the message [5]. Another classical cipher that was used is the atbash cipher which is a monoalphabetic substitution cipher created in the middle east and used by the Hebrew. It relies on transposing the letters of the alphabet by substituting the first alphabet for the last, the second for the letter before the last, and so on.

Saeed and Rashid, (2010) proposed an encryption algorithm which involved blending the playfair cipher and vigenere cipher with the structural aspects of DES and 3DES. Srikantaswamy & Phaneendra, (2012) proposed an encryption algorithm of an extended Caesar cipher technique and the columnar transposition cipher, with random number generation technique used for key generation operations. Kester, (2012) proposed a new method of implementing vigenere cipher by generating successive keys that will be dependent on an initial key created for the encryption process. Kashish & Supriya, (2013) proposed a modified Caesar cipher algorithm by fixing the key as one. Here, the alphabet index is checked such that if the index is even, then the value is increased by one, else if the alphabet index is odd, then the value is decreased by one. Kester, (2013) proposed a hybrid of a vigenere cipher and columnar transposition cipher, where he used the columnar transposition as the key generator for the vigenere cipher, in order to complement its weakness. Omolara *et al.*, (2014) proposed a hybrid system which combines the vigenere cipher and a modified Caesar cipher algorithm for data security. Malay, (2014) proposed a system of cryptography which involves multiple application of columnar transposition method of encryption on plaintext, alongside other forms of caesar cipher. This was suggested as a means to further strengthen the columnar transposition cipher. Nishith and Kishore, (2014) proposed a method of improving vigenere cipher by double columnar transposition.

This paper aims at contributing to the general body of knowledge in the area of application of cryptography by reviewing the vigenere cipher and all the existing modifications to improve on it.

2. VIGENERE CIPHER

Vigenere cipher is a polyalphabetic substitution cipher which constitutes a matrix of 26 by 26 Caesar cipher shifts. It consists of a set of monoalphabetic substitution rules of Caesar ciphers with shifts of 0 through 25 [18]. The technique was named after its inventor, Blaise de Vigenere from the court of Henry III of France in the sixteenth century, and was considered unbreakable until 1917 [8]. Vigenere encryption is carried out by adding each of the index of the plaintext character to the index of the password character, based on the vigenere square (also known as the vigenere tableau) represented by figure 2.

The encryption and decryption process of the vigenere cipher can also be represented mathematically as:

$$Ci \equiv E\left(Pi + Ki\right) \bmod 26 \tag{1}$$

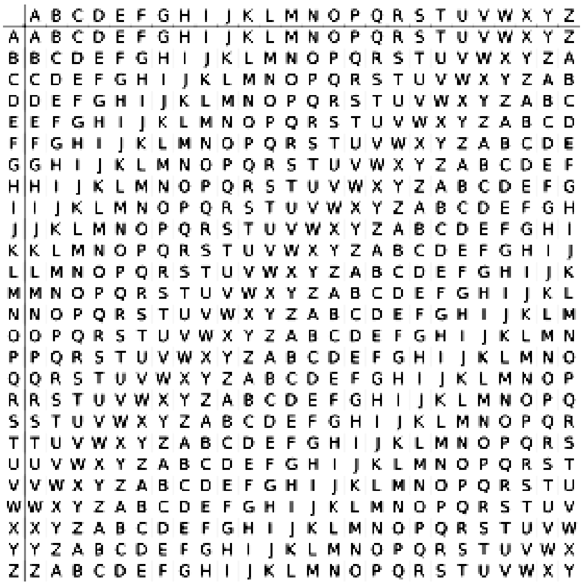
$$Pi = D(Ci - Ki) \bmod 26 \tag{2}$$

Where C represents the ciphertext,

P represents the plaintext character,

K represents the key

E is the encryption function, while D is the decryption function.



	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: Vigenere Square table [8]

If for example, we have a plaintext: “***SECURITY IS ESSENTIAL***”, and a keyword: “***TRUE”.*** The Vigenere cipher encryption is done by aligning the keyword below the plaintext.

Plaintext: SECURITY IS ESSENTIAL

Keyword: TRUETRUETRUETRUETRU

The resultant ciphertext from the above text becomes: “***LVWYKZNCBJYWLVHXBRF***”.

Calculating the index of coincidence of the ciphertext using the formula:

$$I.C = \frac{\sum_{i=A}^{i=Z} fi(fi-1)}{N(N-1)} \tag{3}$$

Where N is the total number of characters and f is the frequency of character i present.

The index of coincidence and entropy of the ciphertext based on the conventional vigenere cipher method were calculated and compared with other methods.

The index of coincidence is 0.02925 and entropy is 3.7216 bits.

The ciphertext distribution is represented in figure 3.

Note that the entropy of the English language text is approximately 4.7bits [2]. This is because all characters are not equally likely to occur and due to the existence of digrams and trigrams in an English text.

The vigenere cipher was later broken by Friedman and Kasiski [11]. This was done by exploiting the repeating nature of the key to break it. Once the length of the key to a vigenere encryption is known, the ciphertext could be grouped and treated as multiple Caesar ciphers which can easily be broken [11].

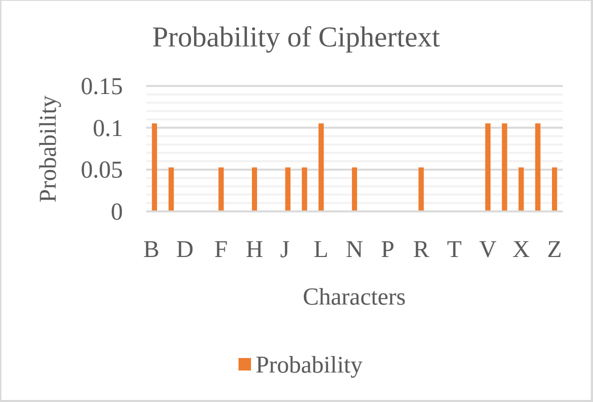


Figure 3: Ciphertext Representation based on Vigenere

The main weakness of the vigenere cipher was however identified to be the repeating nature of its key, which makes it vulnerable to frequency analysis by kasiski attack and calculating the index of coincidence [18].

3. TRENDS AND MODIFICATIONS OF THE VIGENERE CIPHER

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

Kester (2012) proposed a cryptosystem based on vigenere cipher with varying key. 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 vigenere 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 vigenere cipher. The system expanded and redesigned the vigenere square table to consist of 92 characters instead of the conventional 26 alphabets as shown in figure 4.

It then becomes a 92 by 92 matrix to enhance the vigenere square. It provides a greater character set, allowing more characters such as punctuations and numbers to be encrypted, whereas the original vigenere covers plaintext involving only the 26 characters of the alphabet.

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

Consider an example plaintext “SECURITY IS ESSENTIAL” with Key “TRUE”.

A different key is generated using transposition based on the given key.

New key = UYSTEISEASRISICTENL

When this is used for the vigenere encryption, the ciphertext generated is: “***MCUNVQLCIKVAKMPMMNW***”.

The index of coincidence is calculated as 0.05849, while the entropy is 3.4058 bits.

This increased the security of the vigenere cipher but could still be vulnerable to frequency analysis, due to its low entropy level, as illustrated in the given example.

Omolara *et al.,* (2014) proposed a modified hybrid Caesar cipher and vigenere cipher for secure data communication. 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. Vigenere 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.

The encryption was only based on the 26 characters of the English language alphabet. It doesn’t make provision for special characters that might need to be encrypted. Consider an example plaintext “SECURITY IS ESSENTIAL” with Key (K1) “3”, and Key (K2) “TRUE”

The first step involves changing the key using Caesar cipher to become: WUXH.

The ciphertext after the first encryption is: “***OYZBNCQFEMBZOYKAEUI***”

The final ciphertext then becomes:

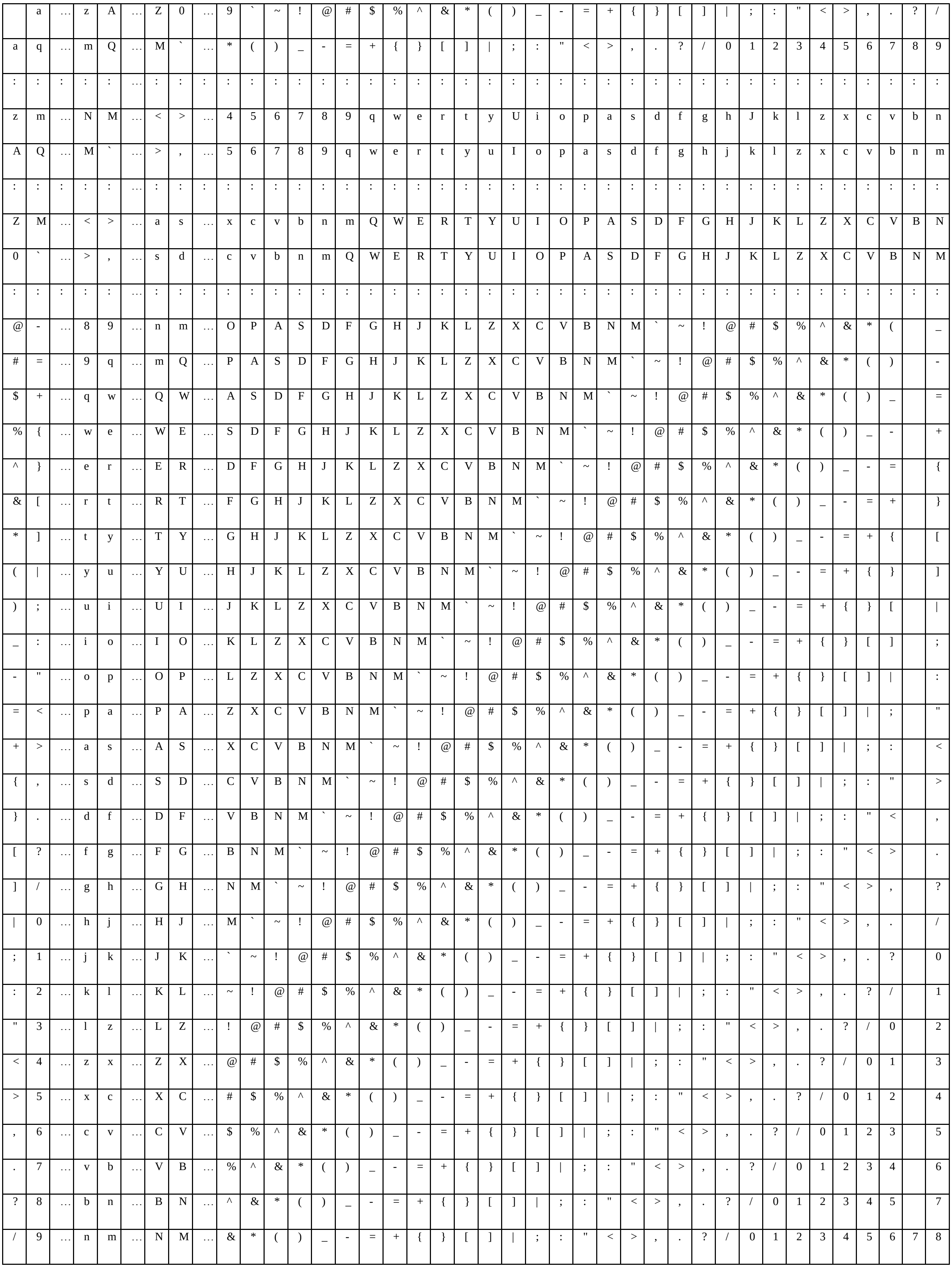
“|***% =s0a’b/m7x!j+n;r***”

The index of coincidence cannot be determined, and the entropy level is 4.2479 bits, which is 14.14% increase compared to the conventional vigenere cipher.

Nishith and Kishore, (2014) proposed improving security of vigenere cipher by double columnar transposition. This involves applying the vigenere 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 vigenere cipher.

Consider an example plaintext “SECURITY IS ESSENTIAL” with Key (K1) “TRUE”, and Key (K2) “41325”

The first step of the encryption involves the vigenere process using key (K1) to give the first ciphertext (C1) as: “***LVWYKZNCBJYWLVHXBRF”***.



	a	…	z	A	…	Z	0	…	9	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/
a	q	…	m	Q	…	M	`	…	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2	3	4	5	6	7	8	9
:	:	:	:	:	…	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
z	m	…	N	M	…	<	>	…	4	5	6	7	8	9	q	w	e	r	t	y	U	i	o	p	a	s	d	f	g	h	J	k	l	z	x	c	v	b	n
A	Q	…	M	`	…	>	,	…	5	6	7	8	9	q	w	e	r	t	y	u	I	o	p	a	s	d	f	g	h	j	k	l	z	x	c	v	b	n	m
:	:	:	:	:	…	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Z	M	…	<	>	…	a	s	…	x	c	v	b	n	m	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N
0	`	…	>	,	…	s	d	…	c	v	b	n	m	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M
:	:	:	:	:	…	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
@	-	…	8	9	…	n	m	…	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(		_
#	=	…	9	q	…	m	Q	…	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)		-
$	+	…	q	w	…	Q	W	…	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_		=
%	{	…	w	e	…	W	E	…	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-		+
^	}	…	e	r	…	E	R	…	D	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=		{
&	[	…	r	t	…	R	T	…	F	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+		}
*	]	…	t	y	…	T	Y	…	G	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{		[
(	|	…	y	u	…	Y	U	…	H	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}		]
)	;	…	u	i	…	U	I	…	J	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[		|
_	:	…	i	o	…	I	O	…	K	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]		;
-	"	…	o	p	…	O	P	…	L	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|		:
=	<	…	p	a	…	P	A	…	Z	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;		"
+	>	…	a	s	…	A	S	…	X	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:		<
{	,	…	s	d	…	S	D	…	C	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"		>
}	.	…	d	f	…	D	F	…	V	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<		,
[	?	…	f	g	…	F	G	…	B	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>		.
]	/	…	g	h	…	G	H	…	N	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,		?
|	0	…	h	j	…	H	J	…	M	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.		/
;	1	…	j	k	…	J	K	…	`	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?		0
:	2	…	k	l	…	K	L	…	~	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/		1
"	3	…	l	z	…	L	Z	…	!	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0		2
<	4	…	z	x	…	Z	X	…	@	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1		3
>	5	…	x	c	…	X	C	…	#	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2		4
,	6	…	c	v	…	C	V	…	$	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2	3		5
.	7	…	v	b	…	V	B	…	%	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2	3	4		6
?	8	…	b	n	…	B	N	…	^	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2	3	4	5		7
/	9	…	n	m	…	N	M	…	&	*	(	)	_	-	=	+	{	}	[	]	|	;	:	"	<	>	,	.	?	/	0	1	2	3	4	5	6	7	8

Figure 4: Figure 4: The Alpha-Qwerty Cipher Description [10]

The second step involves applying transposition using key (K2) to give "***VNWBYBVFWCLRLZYXKJH***" as second ciphertext (C2). The final step involves another transposition using the key (K2) to give the final ciphertext (C3) as "***NVRKBWZHWFLJVBLXYCY"***.

The index of coincidence is calculated to be 0.02925 and entropy is 3.7216 bits. This is the similar to the vigenere cipher value, because the same characters exist in transposition cipher, only the arrangement is different.

The ciphertext graphical representation is the same as figure 3. This method only changes the arrangement of the characters but does not increase the entropy.

Table 1: Comparison of Some methods

	Index of Coincidence	Entropy (bits)
Vigenere Cipher	0.02925	3.7216
Double columnar	0.02925	3.7216
Modified Caesar Cipher and Vigenere	-	4.2479
Alpha-Qwerty cipher	-	-
Columnar and Vigenere cipher	0.05849	3.4058

4. CONCLUSION

From the analysis of the vigenere cipher modifications, it shows that various methods have been proposed to further enhance the cipher. The double columnar transposition scrambled the text so many times, but the ciphertext still contains all the characters of the text. Both the I.C and entropy are low, which means that cryptanalysis is still possible. The summary on table 1 shows that as the vigenere cipher is being modified, it tends to be stronger. A different modification could be carried out based on a different method of transposition to generate the key for the vigenere encryption, and a different combination of substitution and permutation methods to increase the entropy of the system, and thus further strengthen the vigenere cipher.

5. ACKNOWLEDGMENT

We give glory to God Almighty who has made it possible to ensure the success of this paper in order to contribute to knowledge in the area of cryptography.

6. REFERENCES

[1] Abdullah, J. M., & Azman , S. (2010). A New Public-Key Encryption Scheme Based on Non-Expansion. *International Journal of Computer Science Issues IJCSI.*

[2] Forouzan, B.A. (2007). *Cryptography and Network Security.* (Special Indian Edition). McGraw Hills Company Inc. New York

[3] Hamdan, A., Zaidan, B. B., & Zaidan , A. A. (2010). New Comparative Study Between DES, 3DES and AES within nine factors. *Journal of computing, Vol 2* (Issue 3), 152-157.

[4] Information Security (2015), Retrieved from https://en.m.wikipedia.org/wiki/information_security on 8/8/2015

[5] *Interactive Maths*. (n.d.). Retrieved on February 2, 2015, from www.interactive-maths.com/Encryption/Atbash Cipher - Crypto Corner.htm

[6] Kashish, G., & Supriya, K. (2013). Modified Caesar Cipher for better Security Enhancement. *International Journal of Computer Applications*, 26-30

[7] Katz, J. and Lindell Y. (2008). *Introduction to modern cryptography*. Chapman and Hall, Taylor & Francis Group6000 Broken Sound Parkway NW.

[8] Kester, Q.-A. (2013). A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher. *International Journal of Advaced Technology and Engineering Research*, 141-147

[9] Kester, Q-A. (2012). A Cryptosystem based on Vigenere cipher with varying key. *International Journal of Advanced Research in Computer Engineering and Technology*, 108-112.

[10] Md. Khalid, I. R., Neeta, W., & Vaibhav, M. (2012). Alpaha-Qwerty Cipher: An Extended Vigenere Cipher. *Advanced Computing: An International Journal*, 107-117.

[11] Nishith, S., and Kishore, B. (2014). Improving Security of Vigenere Cipher by Double Columnar Transposition. *International Journal of Computer Applications,* Vol 100 (No. 14). Pp 6-10

[12] Omolara, O. E., Oludare, A. I., & Abdullahi, S. E. (2014). Developing a modified Hybrid Caesar cipher and Vigenere cipher for secure Data Communication. *IISTE*, 34-46.

[13] Saeed, F., & Rashid, M. (2010). Integrating Classical Encryption with Modern Technique. *International Journal of Computer Science and Network Security*, 280-285.

[14] Sangapu, V.A. and Gomatam V.S.A (2014), Recent Advancements on Symmetric Cryptography Techniques - A Comprehensive Case Study, Global Journal of Computer Science and Technology, Vol 14, Issue 2, pp 19-30

[15] Serge, V. (2006). *A Classical Introduction to Cryptography Applications for Communications Security*. Springer Science Business Media, Inc.

[16] Shannon, C. and Warren, W. (2009). *The Mathematical Theory of Communication*. University of Illinois Press, U.S.A., pp. 12-29.

[17] Srikantaswamy, S. G., & Phaneendra, H. D. (2012). Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption. *International Journal on Cryptography and Information Security*, 39-49.

[18] Stallings, W. (2011). *Cryptography and Network Security - Principles and Practice. (*Fifth edition), Pearson Education, Inc.