A Modified Version of Vigenere Cipher using 95×95 Table

Khairun Nahar, Partha Chakraborty

***Abstract**: Cryptography is a current field of research at the moment as it can be crucial to offer protection to extremely delicate and confidential records from criminal wrongdoings throughout transmission over the network. The vigenere cipher is one of the standard cryptographic algorithms that prevent attackers from understanding the raw data throughout the transmission. The traditional vigenere cipher encrypts only the alphabetic plaintext with a 26×26 vigenere table because it includes only 26 English alphabets A to Z. The researcher extended the original vigenere table into 95×95 which introduces all possible characters, mathematical symbols, digits, and punctuations that are available on an ordinary QWERTY keyboard layout that can be encrypted easily by this technique and conjointly introduced case sensitivity. The objective of this modification makes the cryptanalysis procedure more difficult and increases the information security.*

Keywords: Cryptography, Poly-Alphabetic cipher, Vigenere cipher, Substitution cipher, Cipher techniques.

I. INTRODUCTION

With the increasing trend of digital communications and internet technologies, many of us exchange our secrets and private information in cyber space. Whatever we exchange in cyberspace is unprotected and open to cyber criminals for manipulation and misuse. In recent days, protecting confidential and sensitive data from undesirable individuals and maintaining privacy and security for illegal issues is a big concern. In these situations, cryptography plays an important role in providing security in cyberspace. Cryptography is a way of attaining safety where original message rearranges to a non-understandable presentation so that only the intended recipient can understand and use it [1]. Cryptography requires a key and an algorithm to transform the meaning into an undesirable presentation so that only authorized participants can realize it. The related terms of cryptography are described below:

Cryptanalysis and Cryptanalyst: The strategy of interpreting a non-recognizable layout into its original layout without any hints how they are initially before is referred as cryptanalysis and the person who does this job is known as cryptanalyst [1].

- **Plain text and Cipher text:** A message which uses normal language for communication is referred to as the plaintext while the codified message produces the cipher text [1].
- **Encryption and Decryption:** Encryption rearranges the original message into a non-recognizable format whereas the alternate way of getting back the previous message is termed as decryption [1].
- **Caeser Cipher:** The world's first encryption algorithm is Caeser cipher which replaces each character of the plain text with a character that is three places down the line [1].

The achievement and functionality of the encrypted process rely on how tough it is to be damaged or torn apart and extract the precise meaning.

Revised Manuscript Received on June 25, 2020.

* Correspondence Author
Khairun Nahar*, Department of CSE, Comilla University, Cumilla, Bangladesh. E-mail: knahareva@gmail.com
Partha Chakraborty, Department of CSE, Comilla University, Cumilla, Bangladesh. E-mail: partha.chak@cou.ac.bd

II. RELATED WORK

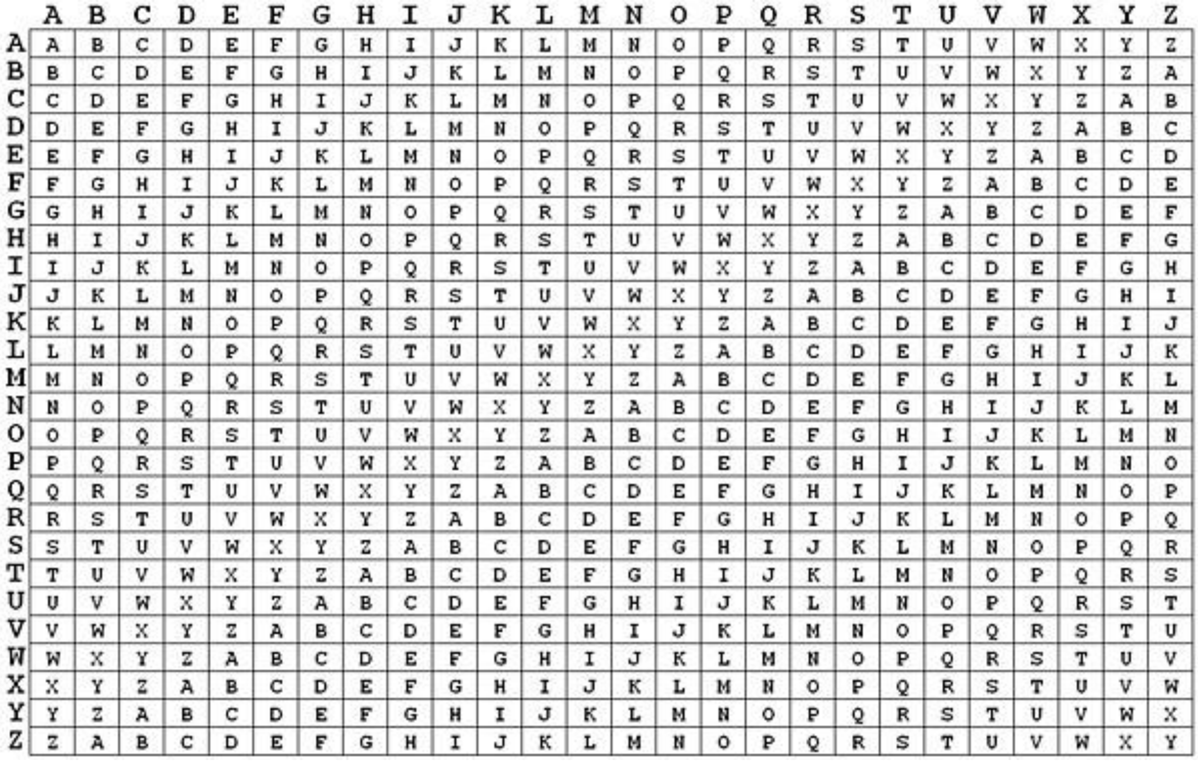
C.R.S Bhardwaj (2012) proposed two modifications to the traditional Vigenere cipher. First, the encryption key must be any type of character for example: mathematical symbols (+,-,*,/,%), numbers (0,1…9), punctuations instead of characters. Second, an arbitrary number is introduced for the key to spread the spectrum so that only experts can understand the message [2]. Khalid et al., (2012) extended the original vigenere table to the 92 characters. It includes 66 additional characters to the original table and redesigned the mapping structure for characters. Though it includes a large character set and introduces case sensitivity to the encryption process, it still suffers from encrypting the space, single quote, backslash because they are not part of the table [3]. Kester (2013) proposed algorithm, first applies the columnar transposition technique to re-arrange the plain text along with the keyword and then applies Vigener cipher to produce output cipher text [4]. Senthil et al., (2013) presented an algorithm that uses the prime number, its primitive roots, and their generator to bring some addition to the Vigenere cipher and Julies Caesar cipher techniques. Shift and substitution method produces the cipher text [5]. Fairouz et al., (2014) proposed algorithm applies some complex transformation to generate the cipher text. It applies the substitution technique on even location characters and transposition techniques to the odd position characters. The summation of the numeric value of even location characters and keys produces the cipher characters for even location where odd location character treats as separately. For odd locations, they generate a random number for the key and convert both numeric values to the ASCII equivalent. Both ASCII equivalent is transformed into the binary equivalent and performs exclusive or operation on them. The resultant binary number converts to the equivalent ASCII, then back to the character to generate the odd position cipher characters [6].

Omolara et al., (2014) presented method applies two methods: Caesar and Vigenere cipher and use two keys: Numbered key and lettered key.

Caesar cipher applies a key: Lettered key which uses a shift of the numbered key. Then, plain text applies Vigenere cipher with a new key. The binary value of cipher is Exclusive-ORed with the key: Numbered key. Resultant Exclusive-ORed value converted back to its ASCII value and then back to the character to produce the final output cipher text [7]. Nishith and Kishore (2014) proposed algorithm requires two keys and uses substitution and transposition techniques. First, it applies a vigenere cipher using the first key. Then columnar transposition technique applies twice on the plain text which is the resultant cipher text of the previous step [8]. Aized et al. (2016) proposed technique employs multiple tables and each alphabet has more than one numeric value. The proposed algorithm developed for 27 characters. The extra character is a space and denoted by the character "&" [9]. Aditi et al., (2016) presented an algorithm is a mixture of Vigenere and Caeser cipher. Keywords and message letters are represented by the initial rows and columns of the table. First, pick a keyword character and its corresponding plain text character as a row and column-wise and getting the intersection entry of row (key) and column (plain text) index. Add 3 to the entry value to produce the cipher text. The size of the character set is 36. The additional characters are numeric value (0-9) [10]. Deepanshu et al., (2018) proposed algorithm is a mixture of the Vigenere cipher and Modified Ceasar cipher technique and based on 36 characters. They include numbers (0-9) to the original tables. The initial row and column represent the keyword and plain text characters respectively. The intersection entry of the key (row) and plain text (column) characters is added to the key-value (called Ukey) to produce the cipher character [11]. From this study, it is seen that various method has proposed but still suffers from some lacks. This paper extends the original vigenere table to cover all characters and also increase the difficulty level of crack the algorithm.

ORIGINAL VIGENERE CIPHER

Vigenere cipher translates the alphabetic content on the message through the use of the various Caesar cipher based on some key letters. This cipher applies a transferring mechanism that shifts every character on message with a different amount and a table called "Vigenere Table" is used for achieving this purpose which is a matrix of 26 rows and 26 columns. The table comprises 26 language alphabets that are written out 26 times in numerous rows where every letter is shifted to the one position left cyclically compared to the previous one [12].



	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.1. The Original 26 × 26 Vigenere table [13].

The encryption equation (E) for a Vigenere cipher:

Cipher text, C = E (K, P) = (Pi + Ki) mod 26.

The decryption equation (D) for Plain text:

Plain text P = D(C, K) = (Ci - Ki) mod 26.

Here Ci, Pi, and Ki denote the offset of the ith character of cipher text, plain text, and key.

First we assign the alphabet, A to Z by the number 0-25, so that A=0, B=1….Z=25. For encrypting a message using the vigenere cipher, the encryption key length must be equal to the plain text. Usually, the key repeats itself until all the plain text letters are processed. According to the vigenere table, a plain text **COMILLAUNIVERSITY** with a key KOTBARI is encrypted and produces the cipher text **MCFJLCIEBBWEIASHR.**

Vigenere cipher suffers from certain flaws. Firstly, the vigenere table does not include mathematical symbols, punctuation and digits and does not mention their encryption technique. Secondly, the repeating nature of its key is its primary weakness. The cryptanalysis uses the Kasiski examination and Friedman test to predict the key length. As soon as the key length is resolved, the cipher textual content may be handled as interwoven Caesar ciphers, which can effortlessly be broken individually [12].

III. PROPOSED METHOD

A. Extended Vigenere Cipher

Vigenere Cipher encodes only the alphabets (A-Z). A plain text message that contains the upper case alphabets and lower case alphabets must be converted to the uppercase alphabet before encryption. There is no place of case sensitivity in the previous algorithm. Besides this, the algorithm does not provide the facility to encode numbers, blank spaces, special characters or symbols that we use in the English language. The researchers have proposed an extended version of the vigenere Cipher using a 95 × 95 vigenere table which provides the facility for encrypting the lower case letters (a-z), numbers (0-9) and 33 specials characters including with space that is used in keyboard and English Language. The proposed algorithm is kind of equivalent to the unique algorithm because it makes the use of modulo 95 in its place of utilizing modulo 26. The extended 95 × 95 Vigenere table is shown below:

	A	B	…	Z	a	b	…	z	0	1	…	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,	.	?	/
A	A	B	…	Z	a	b	…	z	0	1	…	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,	.	?	/
B	B	C	…	a	b	c	…	0	1	2	…	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,	.	?	/	A
⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Z	Z	a	…	y	z	0	…	+	=	{	…	"	'		<	>	,	.	?	/	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	a	b	…	z	0	1	…	=	{	}	…	'		<	>	,	.	?	/	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	…	0	1	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
⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
z	z	0	…	+	=	{	…	H	I	J	…	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
0	0	1	…	=	{	}	…	I	J	K	…	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
1	1	2	…	{	}	[	…	J	K	L	…	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	0
⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
9	9	~	…	"	'		…	R	S	T	…	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8
~	~	`	…	'		<	…	S	T	U	…	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9
`	`	!	…		<	>	…	T	U	V	…	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~
!	!	@	…	<	>	,	…	U	V	W	…	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`
@	@	#	…	>	,	.	…	V	W	X	…	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!
#	#	$	…	,	.	?	…	W	X	Y	…	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@
$	$	%	…	.	?	/	…	X	Y	Z	…	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#
%	%	^	…	?	/	A	…	Y	Z	a	…	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$
^	^	&	…	/	A	B	…	Z	a	b	…	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%
&	&	*	…	A	B	C	…	a	b	c	…	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^
*	*	(	…	B	C	D	…	b	c	d	…	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&
(	(	)	…	C	D	E	…	c	d	e	…	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*
)	)	-	…	D	E	F	…	d	e	f	…	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(
-	-	_	…	E	F	G	…	e	f	g	…	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)
_	_	+	…	F	G	H	…	f	g	h	…	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-
+	+	=	…	G	H	I	…	g	h	i	…	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_
=	=	{	…	H	I	J	…	h	i	j	…	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+
{	{	}	…	I	J	K	…	i	j	k	…	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=
}	}	[	…	J	K	L	…	j	k	l	…	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{
[	[	]	…	K	L	M	…	k	l	m	…	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}
]	]	|	…	L	M	N	…	l	m	n	…	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[
|	|	\	…	M	N	O	…	m	n	o	…	w	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]
\	\	:	…	N	O	P	…	n	o	p	…	x	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|
:	:	;	…	O	P	Q	…	o	p	q	…	y	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\
;	;	"	…	P	Q	R	…	p	q	r	…	z	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:
"	"	'	…	Q	R	S	…	q	r	s	…	0	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;
'	'		…	R	S	T	…	r	s	t	…	1	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"
		<	…	S	T	U	…	s	t	u	…	2	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'
<	<	>	…	T	U	V	…	t	u	v	…	3	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'	
>	>	,	…	U	V	W	…	u	v	w	…	4	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<
,	,	.	…	V	W	X	…	v	w	x	…	5	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>
.	.	?	…	W	X	Y	…	w	x	y	…	6	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,
?	?	/	…	X	Y	Z	…	x	y	z	…	7	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,	.
/	/	A	…	Y	Z	a	…	y	z	0	…	8	9	~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[	]	|	\	:	;	"	'		<	>	,	.	?

Fig.2. Extended 95 × 95 Vigenere table

B. Structure of the Encryption Algorithm

Step 1: First assign a numeric equivalent to each letter. The numeric equivalent for uppercase alphabets (A-Z), lower case alphabets (a-z), numeric values (0-9), and special characters including the space is shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fig.3. Numeric Equivalent for Uppercase alphabets (A-Z)

Retrieval Number: E9941069520/2020©BEIESP
DOI: 10.35940/ijeat.E9941.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

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
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

Fig.4. Numeric Equivalent for Lowercase alphabets (a-z)

0	1	2	3	4	5	6	7	8	9
52	53	54	55	56	57	58	59	60	61

Fig.5. Numeric Equivalent for Numeric Values (0-9)

~	`	!	@	#	$	%	^	&	*	(	)	-	_	+	=	{	}	[
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80

]	|	\	:	;	"	'		<	>	,	.	?	/
81	82	83	84	85	86	87	88	89	90	91	92	93	94

Fig. 6. Numeric Equivalent for Special Characters

Step 2: Read the plain text message (P) and convert each letter to its numeric equivalent.

Step 3: Read the keyword (K) for encryption. If the keyword length does not match the length of plain text (P), then it repeats itself.

Step 4: Convert every letter of the keyword (K) to its numeric equivalent.

Step 5: Add the numeric equivalent of the plain text (P) alphabet to the corresponding numeric equivalent of the key (K) alphabet.

Step 6: Takes modulo 95 on the sum which is derived from the previous step and translates each numeric equivalent back to the corresponding alphabet which is the output cipher text(C).

Step 7: End.

C. Structure of the Decryption Algorithm

Step 1: Read the cipher message (C). Then convert each letter to its numeric equivalent.

Step 2: Read the keyword (K) for decryption. If the keyword length does not match the length of cipher text (C), then it repeats itself.

Step 3: Convert every letter of the keyword (K) to its numeric equivalent.

Step 4: Subtract the numeric equivalent of cipher text (C) alphabet to the corresponding numeric equivalent of the key (K) alphabet.

Step 5: Takes modulo 95 on the subtraction which is derived from the previous step and translates each numeric equivalent back to the corresponding alphabet which is the plain text message.

Step 6: End.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

To examine the proposed encryption and decryption algorithm, we consider the Plain text message: Comilla University and the keyword: Kotbari. The generation of output cipher text and plain text is given in below:

Table- I: Encryption process to generate cipher text

Plain Text (P):	C	o	m	i	l	l	a		U	n	i	v	e	r	s	i	t	y
Numeric Equivalent:	2	40	38	34	37	37	26	88	20	39	34	47	30	43	44	34	45	50
Keyword(K):	K	o	t	b	a	r	i	K	o	t	b	a	r	t	K	o	t	b
Numeric Equivalent:	10	40	45	27	26	43	34	10	40	45	27	26	43	34	10	40	45	27
Sum= (Pi+Ki)	12	80	83	61	63	80	60	98	60	84	61	73	73	77	54	74	90	77
Perform ((Pi+Ki) mod 95)	12	80	83	61	63	80	60	3	60	84	61	73	73	77	54	74	90	77
Cipher Text (C):	**M**	**[**	\	**9**	`	**[**	**8**	**D**	**8**	**:**	**9**	**)**	**)**	**=**	**2**	**-**	**>**	**=**

Table- II: Decryption process to generate the plain text

Cipher Text (C):	M	[	\	9	`	[	8	D	8	:	9	)	)	=	2	-	>	=
Numeric Equivalent:	12	80	83	61	63	80	60	3	60	84	61	73	73	77	54	74	90	77
Keyword(K):	K	o	t	b	a	r	i	K	o	t	b	a	r	t	K	o	t	b
Numeric Equivalent:	10	40	45	27	26	43	34	10	40	45	27	26	43	34	10	40	45	27
Subtract= (Ci-Ki)	2	40	38	34	37	37	26	-7	20	39	34	47	30	43	44	34	45	50
Perform ((Ci-Ki) mod 95)	2	40	38	34	37	37	26	88	20	39	34	47	30	43	44	34	45	50
Plain Text(P):	**C**	**o**	**m**	**i**	**l**	**l**	**a**		**U**	**n**	**i**	**v**	**e**	**r**	**s**	**i**	**t**	**y**

Now, we generate some cipher text that uses same plain text with different keys and different plain text with same keys based on our proposed algorithm which is shown below:

Table- III: Generation of cipher text with different keys and different plain text

	Plain Text (P)	**Keyword (K)**	**Cipher text (C)**
Different keys on the same plain text	COMILLA UNIVERSITY	KOTBARI	mcfJLcIebbWEiaShr
		kotbari	m25jI2i411we80s7^
		KOTbari	Mcfjl2iebbwe80Shr
	"March 15,	ENCRYPT	>Zc80wM5&?K{$)4E

Retrieval Number: E9941069520/2020©BEIESP
DOI: 10.35940/ijeat.E9941.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

	2020"	Encrypt	Vz2"{-m\BYkJ?E|e
Different plain text on the same key	Comilla University	Kotbari	M[\9`[8d8:9))=2->=
	ComiLLa university		M[\9l28D":9))=2->=
	Dhaka University		N)*`0k[x-.5^'%3>

In the above table, we generate three cipher text **mcfJLcIebbWEiaShr**, **m25jI2i411we80s7^**, **Mcfjl2iebbwe80Shr** using the same plain text **COMILLAUNIVERSITY** with three different keywords **KOTBARI**, **kotbari**, **KOTbari**. The three keywords that are used in this example have the same meaning, but we make it different by using lower and uppercase alphabets. These simple changes generate three cipher texts that are different from each other.

V. CONCLUSION

Many researchers have worked on this topic but the scope of their work was insufficient because of using small character sets. The researchers on this paper are trying to further enlarge this character sets by working with more characters, so that the proposed 95 × 95 Vigenere table includes the maximum number of characters. Original algorithm suffers from frequency attacks but this problem does not work on the proposed algorithm, because there is a vast character set. It is difficult to produce a specific frequency of incidence of the proposed character set. The proposed algorithm applies a simple algorithmic technique and does not want deep technical knowledge and also maintains the similarity of the original algorithm.

Recently, people use various platforms such as Messenger, Twitter, and Facebook to send messages to the receiver. They use different emoticons (emoji), stickers, and animated gifs as a part of the plain text. In future work, emoticons, stickers, and animated gifs that are used in social media platforms are added in the extended Vigenere table to make the cryptanalysis more complex.

REFERENCES

1. Atul Kahate, *Cryptography and Network Security*, 3rd ed. New Delhi: Tata McGraw-Hill Education, 2013.
2. C. R. S. Bhardwaj, "*Modification of Vigenère Cipher by Random Numbers,Punctuations & Mathematical Symbols*," IOSR Journal of Computer Engineering (IOSRJCE), vol. IV, no. 2, pp. 35-38, Sep.-Oct 2012.
3. Neeta Wadhwa and Vaibhav Malhotra Md. Khalid Imam Rahmani, "*ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER*," Advanced Computing: An International Journal (ACIJ), vol. 3, no. 3, May 2012.
4. Quist-Aphetsi Kester, "*A HYBRID CRYPTOSYSTEM BASED ON VIGENÈRE CIPHER AND COLUMNAR TRANSPOSITION CIPHER*," International Journal of Advanced Technology & Engineering Research (IJATER), vol. 3, no. 1, January 2013.
5. K.Prasanthi and R.Rajaram K.Senthil, "*A Modern Avatar of Julius Ceasar and Vigenere Cipher*," in IEEE International Conference on Computational Intelligence and Computing Research, 2013.
6. Fairouz Mushtaq Sher Ali and Falah Hassan Sarhan, "*Enhancing Security of Vigenere Cipher by Stream Cipher*," International Journal of Computer Applications (0975 – 8887), vol. 100, no. 1, August 2014.
7. A.I. Oludare and S.E. Abdulahi O.E. Omolara, "*Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication*," Computer Engineering and Intelligent Systems, vol. 5, no. 5, 2014.
8. Nishith Sinha and Kishore Bhamidipati, "*Improving Security of Vigenère Cipher by Double Columnar Transposition*," International Journal of Computer Applications (0975 – 8887), vol. 100, no. 14, August 2014.
9. Irfan Riaz and Umair Rasheed Aized Amin Soofi, "*An Enhanced Vigenere Cipher For Data Security*," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 5, no. 3, March 2016.
10. Chahat Khatria, Sudhakara, Prateek Thakrala and Prantik Biswasa Aditi Saraswata, "*An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication*," in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), Bhubaneswar, Odisha, India., 2016, pp. 355-360.
11. Chandan Agrawal, Parth Sharma, Munish Mehta and Poonam Saini Deepanshu Gauta, "*An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher*," in 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018.
12. *Vigenère cipher* - Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher [Accessed June 7, 2020]
13. The Vigenère Cipher Encryption and Decryption. [Online]. https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html [Accesed June 7,2020]

AUTHORS PROFILE

Khairun Nahar, is at the moment working as a lecturer in CSE Dept. at Comilla University. She has accomplished her B.Sc (Engg.) and M.Sc (Engg.) degree from CSE at Comilla University, Bangladesh.

Partha Chakraborty received his BSc and MSc degree in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka, Bangladesh. He began his teaching career as a Lecturer, Department of CSE in Comilla University and now he is an Assistant Professor in this department. He is actively engaged in various research activities and educational activities. He published a good number of research articles as well as attends various conferences. His research area includes Machine Learning, Artificial Intellegence, Computer Vision, Robotics, Image Processing and Human Robot Interaction.

Retrieval Number: E9941069520/2020©BEIESP
DOI: 10.35940/ijeat.E9941.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication