International Journal of Mathematical Archive-2(10), 2011, Page: 2078-2083
Available online through www.ijma.info ISSN 2229 – 5046

AN ENHANCED CRYPTOGRAPHIC SUBSTITUTION METHOD FOR INFORMATION SECURITY

***Kallam Ravindra Babu[1], Dr. S. Udaya Kumar[2], Dr. A. Vinaya Babu[3] and Dr. M. Thirupathi Reddy[4]**

[1]Research Scholar (JNTUH), HOD CSE&IT, AZCET, Mancherail, A.P, India
[2]Principal, M. V. S. R. Engineering College, Hyderabad, Andhra Pradesh, India
[3]Director, Admissions, JNTUH, Hyderabad, A.P, India,
[4]Principal, AZCET, Mancherial, A.P, India

rb_kallam@yahoo.com, uksusarla@rediffmail.com, avb1222@gmail.com, mtreddy3@gmail.com

(Received on: 14-10-11; Accepted on: 01-11-11)

ABSTRACT

In this paper, we brief the importance of cryptography and its two variants transposition and substitution methods, difference between mono alphabetic and poly alphabetic substitution ciphers, mentioned the recent modifications on play fair cipher, then we describe the most popular Vigenere cipher algorithm, the variations in Vigenere cipher and its merits, de merits and finally we explain the ***Enhanced Vigenere cipher****, suitable for encryption and decryption of all characters, numbers and symbols on the key board.*

Keywords: *Cipher, Steganography, Cryptography, Substitution, Transposition, Poly Alphabetic, Play fair, PCC.*

---

1. INTRODUCTION:

The widespread use of computerized data storage, processing and transmission makes, sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission. Due to rapid growth in communications and eavesdropping technologies, business organizations and private individuals are beginning to protect their information in computer systems and networks by using security algorithms [1]. New computer applications are being found every day, and the cost of computer hardware continues to decline.

As a result, more computer systems are taking a distributed form in which an increasing use of computer data communications is being made. This provides more readily available access to the authorized users of the computers and data, but also creates more opportunities for unauthorized individuals to gain similar access.

Increased intimidation and opponent activities in recent times and a doubt about existing security algorithms have created a need for either updating the existing security algorithms or for inventing stronger secure algorithms. In the recent past Dr Vinay et al, have updated the Playfair cipher [3][4], Poly alphabetic cipher [5] and also invented a new cryptographic algorithm[7][8] by name it is play color cipher.

Most of the security algorithms were implemented by using either Steganography or Cryptography. Steganography is a form of covert communication in which a secret message is camouflaged with in a carrier message. Cryptography deals with all the means and methods for converting an intelligible message into an unintelligible or secret form, and for reconverting the secret form in to the intelligible message by a direct reversal of the steps used in the original process. In the coming sections we brief some of the cryptographic techniques and explain the proposed Vigenere cipher algorithm.

2. CRYPTOGRAPHIC TECHNIQUES:

Cryptographic systems are characterized along three independent dimensions: The type operations used for transforming plaintext to cipher text, the number of keys used and the way in which the plaintext is processed [2]. For converting plain text in to cipher text we have two techniques, transposition and substitution. In transposition the elements in the plain text are rearranged example: rail fence technique. In substitution each element in the plain text is mapped into another element example: Caesar cipher, mono alphabetic cipher, play fair cipher, hill cipher, poly

---

***Corresponding author:** *Kallam Ravindra Babu[1], ***E-mail:** rb_kallam@yahoo.com*

alphabetic cipher etc. If both sender and receiver use same key, the system is referred to as symmetric, single key, secret key or conventional encryption. If sender and receiver use different keys, the system is referred to as asymmetric, two key or public key encryption. A block cipher processes the input one block at a time, producing an out put block for each input block. A stream cipher processes the input elements continuously, producing out put one element at a time. In substitution technique we have two basic classes, mono alphabetic and poly alphabetic [6].

2.1 Mono Alphabetic Substitution Cipher:

A simple substitution cipher, called a mono alphabetical substitution cipher (MSC), there is a one-to-one correspondence between the symbols and their substitutes [9]. To construct the cipher alphabet, the first letter could be any of the 26 letters. The second letter could be any of the remaining 25 letters. The third letter could be any of the remaining 24 letters, and so on. The total number of permutations is 26 x 25 x 24 x ... ...x 1 (otherwise written as 26!) The ciphers in this substitution section replace each letter with another letter according to the cipher alphabet. Ciphers in which the cipher alphabet remains unchanged throughout the message are called Mono alphabetic Substitution Ciphers.

2.2 Poly Alphabetic Substitution Cipher:

A given letter of the alphabet will not always encipher by the same cipher text letter and as a consequence, cannot be described by a single set of cipher text alphabet corresponding to a single set of plaintext alphabet [2].

The simplest way to produce a poly alphabetic cipher is to combine different mono alphabetic ciphers. On such simple and most popular technique is Vigenere cipher [6].

2.2.1 Vigenere Cipher:

This cipher was invented in the 16th century, and first written down by a French diplomat, Blaise de Vigenère. For almost 300 years it was thought to be unbreakable, and it was popular for encoding sensitive data for transmission over the telegram system during the 19th century. It was first cracked by Kasiski in 1863[6].

In this scheme, the set of related mono alphabetic substitution rules consists of the 26 Caesar ciphers, with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plain text letter a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value d [2].

To aid in understanding the scheme and to aid in its use, a matrix known as the Vigenere tableau is constructed. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plain text runs across the top. The process of encryption is simple: Given a key letter x and a plain text letter y, the cipher text letter is at the intersection of the row labeled x and the column labeled y; in this case the cipher text is V. To encrypt a message a key is needed that is as long as the message. Usually, the key is a repeating keyword. Decryption is equally simple. The key letter again identifies the row, the position of the cipher text letter in that row determines the column, and the plain text letter is at the top of that column. The strength of this cipher is that there are multiple cipher text letters for each plain text letter, one for each unique letter of the key board.

2.2.2 Variations in Vigenere Cipher:

For increasing the security **auto key system** is used, in which a key word is concatenated with the plain text itself to provide a running key it was proposed by AT & T engineer named Gilbert Vernam in 1918. An army signal crop officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. He suggested using random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then discarded. Each new message requires a new key of the same length as the new message. Such a scheme is known as **One- time pad**, is unbreakable [9].

As we discussed earlier, the Vigenere table invented in 16th century was of 26X26 matrix, considers only 26 English alphabets, and can convert the messages only in English alphabets. It was one of the limitation in the basic Vigenere table and the other is, it do not consider the space between the words. In the English literature meaning of the message can change based on the space between the words. Consider an sentence ‘ an ice image’, it can also spell as a ‘a nice image’. To solve this problem, in his paper Dr Udaya et al, have given a solution[5] by introducing a new character for the indication of the space, while encrypting the message the space character should be inserted in the text wherever it is mandatory. After decryption it has to be removed again.

With all this, we can encrypt the message which is in the form of only English alphabets(26), but it do not consider the message in the form of alphabets, numbers and key board symbols. In the next section we explain the enhanced vigenere cipher.

3. ENHENCED VIGENERE CIPHER:

To extend the range and the scope of the vigenere cipher, we have considered alphabets (1 to 26), numbers (0 to 9) and all the symbols available on the Key board (32). For this a new Vigenere table has built with 68X68 matrix as shown in Table 1,2,3and 4.

Because the table length is more, it is difficult to show the table as a hole and hence we have divided the table in to four parts as shown below.

Enhanced Vigenere Table 1
Enhanced Vigenere Table 2
Enhanced Vigenere Table 3
Enhanced Vigenere Table 4

To aid in understanding the scheme and to aid its use, a matrix known as the Enhanced Vigenere table is constructed. Each of the 26 ciphers is laid out horizontally, with the key letter (alphanumeric) for each cipher to its left. Consider the symbols in the key board; continue placing them horizontally from left to right, bottom symbol on the key first and upper next, as shown in the table. Similarly a normal alphabet, symbols and the numbers in the same sequence for the plain text runs across the top. For encryption we have to simply follow three steps, locate the plain text letter on the top row, locate the key letter on the side column and encrypt using the letter where your row and column meet in the table

For example:

Key: t e mpe r a t ure1
Plain text (alphanumeric): c= 5 /9* (f -32)
Cipher text (alphanumeric): V#$ L~/ (Y | &6I

In the above example it is noticeable that the plain text is the combination of alphabets, numbers and symbols, it is an equation **"c =5/9*(f -32)"** for converting the fahrenheit into centigrade. The key considered in this example is "temperature1" and the generated cipher text is**" V #$L~/ (Y| & 6 I "**. It is even difficult to read and very difficult for the cryptanalyst to analyze and decrepit the cipher text. The length of the key can be any permutation of sixty eight alphanumeric characters, and can be applied to the message in the form of alphabets, numbers and all symbols on the keyboard.

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

Table: 1 Enhanced Vigenere table-1

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

Table: 2 Enhanced Vigenere table-2

Key \ Plaintext	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	2	3	4	5	6	7
8	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?
9	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A
0	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B
-	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C
=	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D
~	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E
!	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F
@	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G
#	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H
$	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I
%	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J
^	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K
&	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L
*	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M
(	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N
)	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
_	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
+	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
[	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
]	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
\	\	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
{	{	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
}	}	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
|	|	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
;	;	'	:	"	,	.	/	<	>	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
'	'	:	"	,	.	/	<	>	?	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	`	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	`	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	`	1	2	3
<	<	>	?	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	2	3	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	`	1	2	3	4	5
?	?	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6

Table: 3 Enhanced Vigenere table-3

Key \ Plaintext	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>	?
8	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	2	3	4	5	6	7
9	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	2	3	4	5	6	7	8
0	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	2	3	4	5	6	7	8	9
-	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0
=	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-
~	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=
!	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~
@	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!
#	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@
$	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#
%	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$
^	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%
&	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^
*	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&
(	O	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*
)	P	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(
_	Q	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)
+	R	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_
[	S	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+
]	T	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[
\	U	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]
{	V	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\
}	W	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{
|	X	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}
;	Y	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|
'	Z	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;
:	`	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'
"	1	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:
,	2	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"
.	3	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,
/	4	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.
<	5	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/
>	6	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<
?	7	8	9	0	-	=	~	!	@	#	$	%	^	&	*	(	)	_	+	[	]	\	{	}	|	;	'	:	"	,	.	/	<	>

Table: 4 Enhanced Vigenere table-4

4 CONCLUSION:

In this paper we have explained the importance of information security, the role of cryptography and Steganography in providing network and information security, difference between mono alphabetic and poly alphabetic substitution techniques, Vigenere cipher and its drawbacks in the basic model, modern Vigenere cipher, its merits and de merits.

We have mainly focused and discussed about the "Enhanced Vigenere Cipher" algorithm suitable for all keys on the keyboard.

5. ACKNOWLEDGMENTS:

The first author like to thank the management of AZCET for providing all the resources.

6. REFERENCES:

[1] Dennie van tassel, Cryptographic Techniques for Computers: Substitution Methods, Vol. 6, 241-249.

[2] Williem stallings, Cryptography and Network Security,2005, Person education, Vol. 5, 29-47.

[3] Ravindra babu, Udaya Kumar, Vinaya babu, An Improved Play Fair Cipher Cryptographic Substitution Algorithm, IJARCS,0976-5697, Vol 2, No 1, Feb 2011

[4] Ravindra babu, Udaya Kumar, Vinaya babu, An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method, IJCA,0975-8887, Vol. 17, No 5, March 2011.

[5] Ravindra babu, Udaya kumar, Vinaya babu, An Enhanced Poly Alphabetic Cipher using Extended Vigenere Table, IJARCS, 0976-5697, Vol 2, No 2, April 2011.

[6] Ravindra babu, Udaya kumar, Vinaya babu, A Survey on Cryptography and Steganography Methods for Information Security, IJCA, 0977-8887, Vol. 12, No 2, Nov 2010.

[7] Ravindra babu, Udaya kumar, Vinaya babu, A Block Cipher Generation using Color Substituition, IJCA, 0975-8887, Vol. 1, No 28, 2010.

[8] Ravindra babu, Udaya kumar, Vinaya babu, A Variable Length Block Cipher Generation Using Modern Play Color Cipher Algorithm with Alphanumeric key and Iterative Functions, ICNICT11, ISBN 978-93-81126-21-1,288-293.

[9] F Ayoub, Cryptographic Techniques and Network Security, IEEE Procedings, Vol. 131, Dec 1984, 684-694.

****

