World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 4,167-171, 2011

A Contemporary Polyalphabetic Cipher using Comprehensive Vigenere Table

Prof.Ravindra Babu Kallam[1], Dr.S.Udaya Kumar[2], Dr. A.Vinaya babu[3] and V.Shravan kumar[4].
[1]Professor in Computer Science, Vivekananda Institute of Technology and Science SET, Karimnagar, A.P, India
[2] Principal MVSR Engineering College, Hyderabad, Andhra Pradesh, India
[3]Director, Admissions, JNTUH, Hyderabad,A.P, India, [4]Aizza college of Engineering and Technology,Mancherial,A.P, India
rb_kallam@yahoo.com, uksusarla@rediffmail.com, avb1222@gmail.com, vemula.vsk@gmail.com

Abstract— in this paper we describe the importance of cryptography with its substitution techniques. Our main focus is on poly alphabetic cipher, discuss about its merits and demerits. We have proposed and implemented a comprehensive Vigenare square appropriate for encryption and decryption of all the alphanumeric characters, symbols on the keyboard and e.t.c. We have explained the algorithm with suitable example and have proven that it can encrypt or decrypt any kind of text. Finally we have concluded that it is cryptographically stronger as comparing with previous poly alphabetic cipher.

Keywords- Algorithm; Security; Cipher; Modern Vigenere Cipher; Substitution; Cryptography; Polyalphabetic.

I. INTRODUCTION

Historically, cryptography referred exclusively to *encryption*, which is the process of converting ordinary information into unintelligible gibberish. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This is a secret parameter known only to sender and receiver for a specific message exchange context.

A "cryptosystem" is the structured list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Traditionally, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations. Some use the terms cryptography and cryptology interchangeably in English, while others use cryptography to refer specifically to the use and practice of cryptographic techniques and cryptology to refer to the combined study of cryptography and cryptanalysis.

Cryptography [1-3] systems are basically classified into types of operations used for transforming plain text to cipher text, the number of keys used, the way in which the plain text is processed. A substitution [4][9][10] technique is the one in which each letter of the plain text is replaced by another character, number, symbol or any color. Fundamental requirement is the no information will be lost. A stream cipher is the one which encrypts a digital data stream one bit or byte at a time. A block cipher is the one in which a block of plain text is treated as a whole to produce a cipher text of same length [7-8].

A poly alphabetic cipher is the method depends on different mono alphabetic substitutions as one proceeds through the plain text message. The best known and simplest such algorithm is referred to as Vigenere cipher [4-6]. The Vigenere ciphers consist of several Caesar ciphers in sequence with different shift values. The sender encrypts the plain text to cipher text using a keyword, the receiver decrypts the cipher text into plain text using the same keyword used for encryption.

II. EXISTING SYSTEM

From the history, Vigenere cipher is a well known algorithm used in polyalphabetic cipher. This algorithm consists of a Vigenere table used for encryption and decryption of the data or message. This Vigenere table is known as Vigenere square or tabula recta. This table comprises of alphabets written out 26 times in different rows, each alphabet is cyclically left shifted compared to the previous alphabet, resulting 26 possible combinations of Caesar ciphers. Each cipher is a key letter, which is the cipher text letter that is replaced for the plain text letter[11].

Later it was enhanced [1] by Dennie Van Tassel in his paper and was constructed by using 36X36 matrix comprising of 26 alphabets and numbers from 0 to 9. It was named as modern Vigenere cipher. The curb in this was, it be able to encrypt only alphabets (26) and numeric values (0-9).

Recently, Dr. Udaya et al has enhanced the Modern Vigenere table by constructing 68X68 matrix[4-5], consisting of alphabets (1 to 26), numbers (0 to 9) and all the symbols present on the keyboard (32). He could able to encrypt and decrypt the combination of all kinds of text and the symbols on key board.

From the analysis we did on this algorithm, it has a limitation that it can not consider all ASCII (128 ASCII+ 128 Extended ASCII) characters. In many situations we used to have the messages or the information in the form of ASCII and Extended ASCII characters as shown in table 1&2, especially in the case of mathematical equations and messages communicated in the defense services. To congregate the current requirements and to overcome the drawback in the previous method it is essential to enhance the existing system. Hence, we have enhanced the existing algorithm.

III. PROPOSED SYSTEM

To fulfill the need in the field of secrecy we have implemented a new Vigenere table of 256X256 matrix and named it as a comprehensive Vigenere table with 128 ASCII and 128 Extended ASCII characters.

Algorithm for implementing 256X256 matrix:

```
int alg[][]=new int[256][256];
for (int i=0;i<256;i++)
{
  int k1=i,k2=0;
  for(int j=0;j<256;j++)
   {
     if(i!=0)
      {
       if(k1==256)
          {
           alg[i][j]=k2; k2=k2+1;
           }
        else
          {
           alg[i][j]=k1;  k1++;
           }
      }  else
     {
      alg[i][j]=j;
     }
  }
}
```

Algorithm for receiving plain text:

```
int ptext[]=new int[t.length()];
for(int i=0;i<t.length();i++)
{
  char c = t.charAt(i);  int j = (int) c; ptext[i]=j;
}
```

Algorithm for receiving Key:

```
int pkey1[]=new int[ks1.length];
   for ( int i = 0; i < ks1.length; ++i )
      {
        char c = ks1[i];
        int j1 = (int) c;
        pkey1[i]=j1;
       }
```

The process of encryption is explained below with the flow chart:

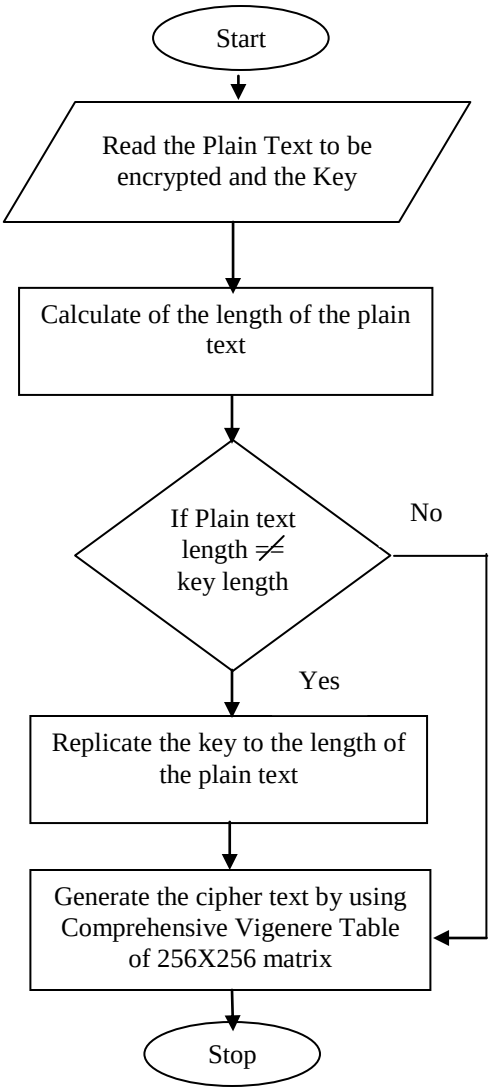

Figure 1. Flowchart for encryption

To understand the process of encryption and decryption two examples were given below:

Keyword-1 : Hello321
Plain text-1 : We!come To New 321@World.!
Cipher text-1: ŸÊ • ÏÞ —QœÔŒºÔªRdz–¬ÃÞ¥□ •v†
Keyword-2: Democr@tic_INDIA31
Plain text-2: Inform@tion_H!dden
Cipher text-2: • ÓÓÞÕß€ èÒÒÍ¨–e-¥˜Ÿ

In the above example it is clearly perceptible that the plain text and the key is the combination of the alphabets, numbers, and special symbols. Each of the 256 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal 256 plain text characters run across the top. For encryption, if the key character H and the plaintext character W is given then the intersection of the row labeled H and the column labeled W is the cipher text character, in this case it is Y. For decryption the key character identifies the row and the position of the cipher letter in that row determines the column, and the plain text character is at the top of that column. In this example as shown in the fig 1, we have used a key and its length is less then the length of the plaintext and hence it recommended that to replicate it to desired length of the plaintext and then perform the encryption and decryption process. The past experience tells us that, it can be easily broken [1] by the cryptanalyst by knowing relative frequency of English letters in English text [6]. Hence it is strongly recommended that to use **One-time pad** in our algorithm, in which the length of the key is truly as long as the message, with no reputations as shown in fig 2.

Be cause the key can be any combination of 256!, **brute force approach** is not possible, our cipher is very strong and hence it is un breakable by the crypt analyst.

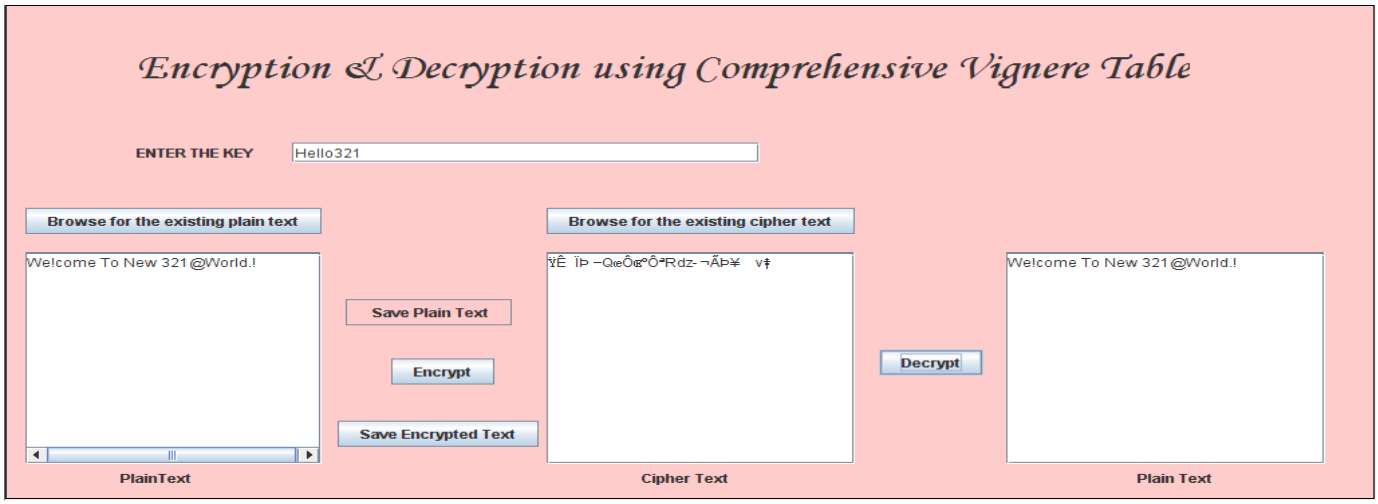

Figure 2. Encryption and Decryption using Comprehensive Vigenere table

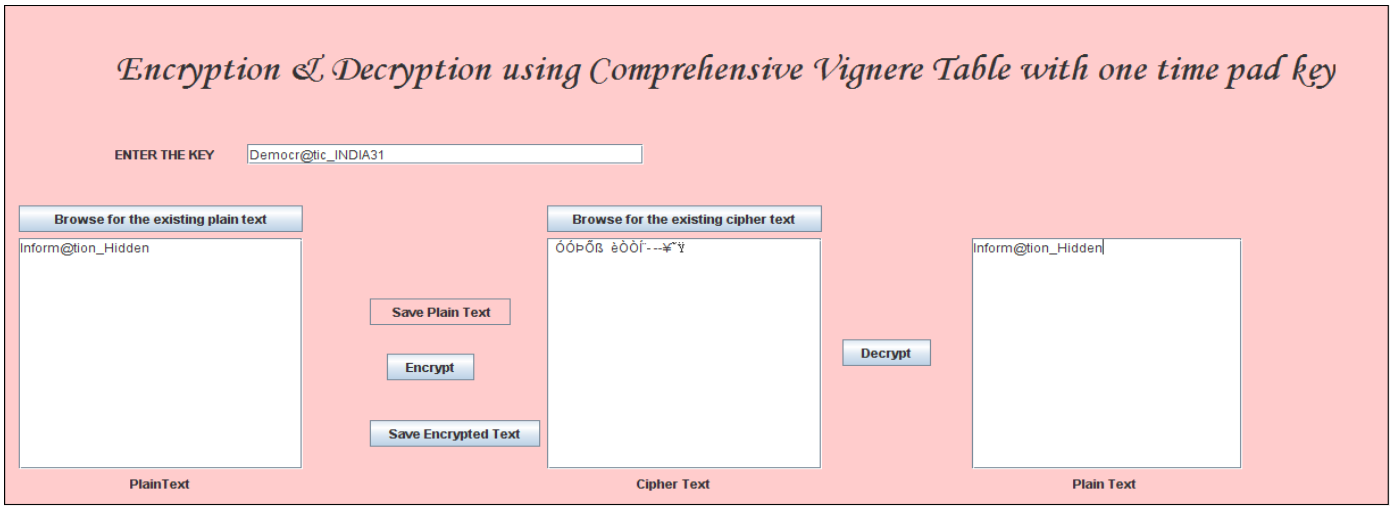

Figure 3. Encryption and Decryption using Comprehensive Vigenare table and with one time pad key

TABLE I. ASCII CHARACTERS AND ITS CORRESPONDING NUMBERS

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

TABLE II. EXTENDED ASCII CHARACTERS AND THEIR CORRESPONDING NUMBERS

128	Ç	144	É	160	á	176	▒	192	└	208	╨	224	α	240	≡
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	241	±
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
131	â	147	ô	163	ú	179	│	195	├	211	╙	227	π	243	≤
132	ä	148	ö	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
139	ï	155	¢	171	½	187	╗	203	╦	219	█	235	δ	251	√
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	

IV. RESULT AND CONCLUSION

In this paper we have explained the concept of cryptography, cryptanalysis, and the importance of cryptosystem. Merits and demerits of the existing poly alphabetic cipher were discussed and to over come the problems in the existing system the process of constructing comprehensive Vigenere table were explained with example. In this we have used a 256X256 matrix. If we assume that the length of the key is 256 characters and with out repetition of any characters, then there will be 256 permutations, is 256!. With this, if we can perform 1decryption per micro second it takes approximately **$253X\ 10^{19}$ years** for trying all possible keys [11]. Hence brute force attack is not possible. With this we can conclude that the cipher is very strong.

ACKNOWLEDGMENT

The first author likes to thank Dr. S.Udaya kumar and Dr.A.Vinaya Babu for their over whelming support all along

to complete the task successfully. He also likes to thank his parents and family members for their continence encouragement. Special thanks to WCSIT for allowing us to use its template.

REFERENCES

[1] Dennie Van Tassel, "Cryptographic Techniques for Computers: Substitution methods", Vol-6, Page: 241-249,Pergamon Press 1970,Britan.

[2] F Ayoub, Cryptographic techniques and network security", IEEE Proceedings, Vol. 131, Dec 1984, 684-694.

[3] Micheal Willet, "Cryptography Old and New", Computers and Security, North-Holland, 0167-4048 /82/ 0000/ 177-186, 1982.

[4] Ravindra babu Kallam, Dr. Udayakumar,"An enhanced and efficient cryptographic substitution method for Informaation Security",is submitted to IJNS, Taiwan. (in press)

[5] Ravindra babu kallam, Dr. Udayakumar,"An enhanced poly alphabetic cipher using extended vigenere table", IJARSC, Volume-2, No.2, Mar-April 2011.

[6] Ravindra babu kallam, Dr.Udayakumar,"A survey on cryptography and steganography methods for information security", International Journal for Computer Applications, (0975-8887), Vol-12, No-2, November 2010.

[7] Ravindra babu kallam, Dr. A.Vinaya Babui," A more secure block cipher generation involving multiple transposition and substitution with a large key", IJARCS, Vol 2, No 2, March-April 2011.

[8] Ravindra babu kallam, Dr.Udayakumar, Dr.A.Vinaya babu," A new frame work for scalable secure block cipher generation using color substitution and permutation on characters, numbers, images and diagrams", IJCA, Vol 20, No 5, April 2011.

[9] Ravindra babu kallam, Dr. A.Vinaya Babui, " A modern play color cipher involving dynamic permuted key with iterative and modular arithmetic functions", IJARCS, Vol 2, No 3, May- June 2011.

[10] Simmons, "Cryptography", Encyclopedia Britannica, Fifteenth Edition, 1993.

[11] Williams Stallings, "Cryptography and Network Security", Fifth Impression, 2008, page no: 35-54.

AUTHORS PROFILE

The first author**,** Lt Ravindra Babu Kallam, received B.E in Computer Science from Nagpur University in 1999, M. Tech in Computer Science from J.N.T.U, Kakinada in 2005, Completed Pre PhD in 2009 in Computer Science from JNTU Hyderabad in the field of Cryptography and Network security and working towards his PhD. He has gone through the Army Training to become associate NCC Officer, Secured state first in PRCN-133 batch., also received prestigious Best NCC Officer award in 2010 from 32 Andhra battalion NCC, Adilabad, AP, India. He is having 12 years of teaching experience and received many best lecturer awards. So far, he has published 13 research papers and many more are under review process in International Journals in the fields of Cryptography Network Security. He is a Review board Member of IJCA, IJNS, WCSIT and also a Member of International Association of Engineers. Presently working as a Professor in Computer Science in VITS SET, Kareemnagar, AP, India.