International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.372-379
DOI: http://dx.doi.org/10.21172/1.81.048
e-ISSN:2278-621X

AN ENHANCED APPROACH ON VIGENERE CIPHER BY POLYALPHABETICS

V. Subhashini[1], Dr.N.Geethanjali[2]

Abstract: Cryptography is a study of encryption principles and methods.It is an mechanism designed to detect,prevent,and recover the Security attacks.The main objective of this paper is implementation of Caesar Cipher techniques. In this paper we focused only on Polyalphabetic Cipher Techniques.Using Polyalphabetic Cipher technique,Vigenere Cipher is studied. The Vigenère cipher uses a 26×26 table with A to Z as the row heading and column heading. This paper studies the effect of varying the key length on the performance of Vigenère cipher and its frequency analysis attack. In this paper, Vigenere cipher used A to Z alphabets with special characters. Vigenere cipher uses a **32 X 32** table with **A to Z** alphabets and **special characters** with key and without key are explained.

Keywords: Caesar Cipher, Polyalphabetics, Encryption, Decryption, keys

I. INTRODUCTION

Cryptography has become an essential tool in transmission of information. Cryptography is the central part of several fields: information security and related issues, particularly, authentication, and access control. Cryptography encompasses a large number of algorithms which are used in building secure applications. Cryptography is the study of Secret (crypto-)-Writing (-graph). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreement are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures.

The play fair cipher was the first digraph Substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but it was named after Lord Playfair. The technique encrypts pairs if letters instead of single letter as in the simple substitution cipher .The play fair is significally harder to breaks since the frequency analysis used to simple substitution cipher does not work

[1] *Department of Computer Science & Technology Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India.*

[2] *Department of Computer Science & Technology Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India*

with it. Cipher text is used for tactical purposes by British forces in the second Boer War and in World War I and for some purpose by the Australians during the World War II.

II. TRADITIONAL PLAYFAIR CIPHER

The best- known multiple letter encryption cipher is the Playfair, which creates diagrams in the plaintext as single units and translates these units into cipher text diagrams.The playfair algorithm is based on the use of 5 X 5 matrix of letters constructed using a keyword. Playfair is a substitution cipher. Playfair cipher was originally developed by Charles Wheatstone in 1854 but it bears the name of Lord Playfair because he promoted the use of this method.

2.1. EXISTING PLAYFAIR ALGORITHM USING 5 X 5 MATRIX

The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose “DIGITAL LIBRARY” as the secret keyword the matrix is given in Table1.

D	I	G	T	A
L	B	R	Y	C
E	F	H	K	M
N	O	P	Q	S
U	V	W	X	Z

So, the Using the word “DIGITAL LIBRARY”, we get the following code

D I G T A L B R Y C E F H K M N O P Q S V W X Z
A B C D E F G H I K L M N O P Q R S T U V W X Y Z

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message. Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the words COMMUNICATE would be treated as
CO MX MU NI CA TE.

So using the Keyword “DIGITAL LIBRARY” the word “COMMUNICATE” can be decoded as follows

CO MX UN IC AT EX
GK FW SH YG DQ AW

III. VIGENERE CIPHER ALGORITHM

A Simple polyalphabetic cipher in which the cipher text is obtained by modular addition of a repeating keys phrase and an open text, both of same length. The algorithm is based on 26 X 26 matrix. This method is also called as Vigenere cipher algorithm.

3.1 RELATED WORK

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of places down the alphabets. This method is names as Julius Caesar. For the Caesar cipher, the key is the number of characters to shift the cipher alphabets.

3.2 Mathematical Description

Let a=0, b=1, c=2 ……………..z=25 then we can represent the Caesar cipher encryption function,

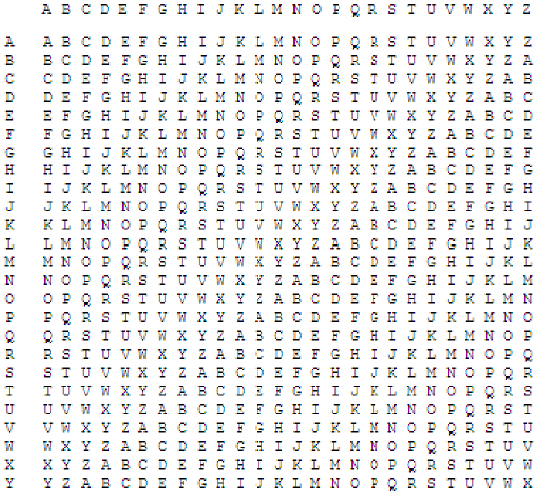
$e(x) = (x+k) \pmod{26}$

and the decryption function,

$d(x) =(x-k) \pmod{26}$

3.3 The Vigenere Cipher

The *Vigenere Cipher*, proposed by Blaise de Vigenere from the court of Henry III of France in the sixteenth century, is a polyalphabetic substitution based on the following 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

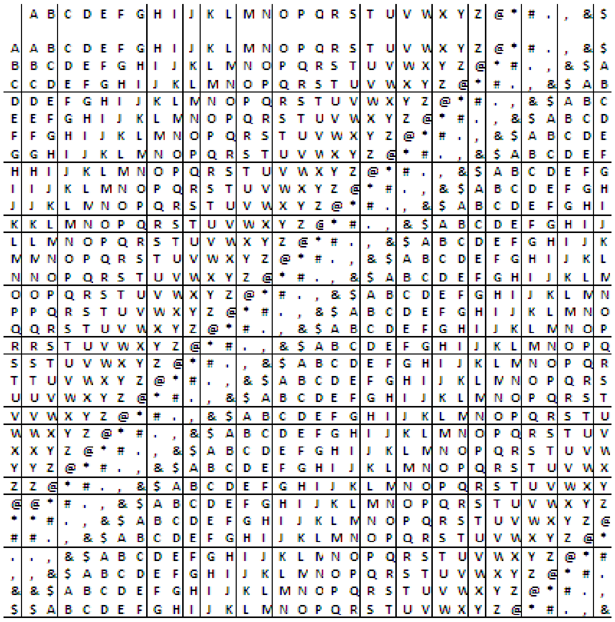
Fig1: Vigenere Table

IV. PROPOSED APPROACH

4.1 METHODOLOGY

The new method employs the Vigenère square and key in its encryption process. In this method the special case of 32 X 32 matrix in introduced. The plain text can be encrypted to any sentence. The special case of special characters is introduced. “@” “#” “.” “&” “$” .The encryption and decryption method with key and without key are discussed. A software program was written to demonstrate the effectiveness of the algorithm using java programming language and cryptanalysis performed on the cipher text. The algorithm ultimately makes it possible for encryption and decryption of the plain text.

So, after introducing the special characters the Vigenere Cipher Table changes as follows:



	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
@	@	*	#	.	,	&	$	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	@	*
.	.	,	&	$	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	@	*	#	.	,
$	$	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	@	*	#	.	,	&

Fig2: Vigenere Table

Note: The first row is a shift of 0; the second is a shift of 1; and the last is a shift of 32. So, the max value of m is 32.

4.2 Encryption Algorithm

The encryption can be described by the following formula

$C_i = T_i + K_i \pmod{m}$

C_i is the ith character of the Cipher text

T_i is the ith character of the Plain text

K_i is the character of the key phrase

m is the length of the Alphabets

4.3 Decryption Algorithm

The process of decryption is analogous. The key phrase is modularly subtracted from the Cipher text.

$T_i = Ci - K_i \pmod{m}$

C_i is the ith character of the Cipher text

T_i is the ith character of the Plain text

K_i is the character of the key phrase m is the length of the Alphabets

4.4 Mathematical Description

Let a=0, b=1, c=2 ……………...z=25 then we can represent the Caesar cipher encryption function,

e(x) = (x+k) (mod 32)

and the decryption function,

d(x) =(x-k) (mod 32)

Mathematically, the encryption of the message at letter i, is equal to the alphabetic value of i, in the plain text plus the alphabetic value of the corresponding I in the key.

$E_k (M_i) = (M_i + K_i) \bmod 32$

Decryption is the same process reversed, subtracting the key instead of adding to arrive back at the original, and plain text value.

$D_k (C_i) = (C_i - K_i) \bmod 32$

The Vigenere Cipher was an improvement upon previous historical encryption techniques, but is still vulnerable brute attacks force attacks and frequency analysis, though to lesser degree than the Caesar Cipher.

4.4 Example

A .Encryption with Key

Suppose the plain text is

CIPHER@GMAIL.COM

Keyword is "SKU"

C I P H E R @ G M A I L . C O M

S K U S K U S K U S K U S K U S

Each letter is encoded by finding the intersection in the grid (fig: 2) between the plaintext and keyword so,

The first letter C is encrypted with S is U

The second letter I is Encrypted with K is S and so on.

Then the encrypted message is

U S D Z O F M Q A S S $ P M C &

This can be done using algorithm as follows

C + S = 20 + 18 = U

I + K =8 + 10 = S

and so on…

Then the encrypted message is

U S D Z O F M Q A S S $ P M C &

B. **Encryption without Key**

Suppose the plain text is

CIPHER@GMAIL.COM

Here the plain text itself becomes a keyword so,

C I P H E R @ G M A I L . C O M

C I P H E R @ G M A I L . C O M

Each letter is encoded by finding the intersection in the grid (fig: 2) between the plaintext and keyword so,

The first letter C is encrypted with C is E

The second letter I is Encrypted with I is Q and so on.

Then the encrypted message is

E Q & O I C U M Y A Q W @ E * Y

This can be done using algorithm as follows

C + C = 2 + 2 =E

I + I = 8 + 8 =Q

and so on…

E Q & O I C U M Y A Q W @ E * Y

C. Decryption with key

Now the cipher text is

U S D Z O F M Q A S S $ P M C &

Keyword is SKU

U S D Z O F M Q A S S $ P M C &

S K U S K U S K U S K U S K U S

Each letter is encoded by finding the intersection in the grid (fig: 2) between the plaintext and keyword so,

The first letter U is encrypted with S is C

The second letter S is Encrypted with K is I and so on.

Then the decrypted message is

C I P H E R @ G M A I L . C O M

This can be done using algorithm as follows

U – S=20-18 = C

S-K = 18-10= I and so on..

Then the decrypted message is

C I P H E R @ G M A I L . C O M

D. Decryption without key

E – C = 4 – 2 = C

Q - I = 16 – 8 = I and so on…

Then the decrypted message is

C I P H E R @ G M A I L . C O M

V. CONCLUSIONS

1. A generalized model of Vigenere cipher is proposed in which any matrix whose rows or columns are unique can be used in place of Vigenere square.

2. Using random matrices in place of Vigenere square will increase the difficulty level of cracking the cipher.

3. An improved random key stream generation method is also suggested to enhance the security level of the Vigenere cipher.

REFERENCES

[1] Stalling W. “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.

[2] Menezes A. J., Oorschot P. C. and Vanstone S. A. handbook of applied cryptography, CRC Press, 1996.

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

[4] Phaneendra H. D. and Srikantaswamy S.G. "A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques", International Journal of Computer Applications,2011, Vol. 29, No.8, pp 34-36.

[5]. International Journal of Computer Applications (0975 – 8887) Volume 100– No.1, August 2014 1 Enhancing Security of Vigenere Cipher by Stream Cipher Fairouz Mushtaq Sher Ali Department of Computer Science/ College of Education for Girls/ University of Kufa Najaf/ Iraq Falah Hassan Sarhan Department of Mathematics/ College of Education for Girls/ University of Kufa Najaf/ Iraq

[6] F. W. Kasiski. Die Geheimschriften und die Dechiffrirkunst. Mittler und Sohn, 1863. [7] D. Salomon. Data Privacy and Security. Springer, 2003.

[8] D. Schweitzer and L. Baird. The Design and Use of Interactive Visualization Applets for Teaching Ciphers. In Proceedings of IEEE Information Assurance Workshop, pages 69–75, 2006.

[9] VIGvisual: A Visualization Tool for the Vigenère Cipher Can Li, Jun Ma, Jun Tao, Jean Mayo, Ching-Kuang Shene Department of Computer Science Michigan Technological University Houghton, MI {canli,junm,junt,jmayo,shene}@mtu.edu Melissa Keranen Department of Mathematical Sciences Michigan Technological University Houghton, MI msjukuri@mtu.edu Chaoli Wang Department of Computer Science & Engineering University of Notre Dame Notre Dame, IN chaoli.wang@nd.edu

[10] A. Razzaq, et al., "Strong Key Machanism Generated by LFSR based Vigenère Cipher," presented at the 13 International Arab Conference on Information Technology, 2013.

[11] O. Omolara, et al., "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," Computer Engineering and Intelligent Systems, vol. 5, pp. 34-46, 2014.

[12] F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications, vol. 100, pp. 1-4, 2014