ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

A CRYPTOSYSTEM BASED ON VIGENÈRE CIPHER WITH ENHANCED KEY MECHANISM FOR DATA SECURITY A CRYPTO SYSTEM BASED ON VIGENERE CIPHER TO ENHANCE DATA SECURITY

Nimai Agarwal[1], Poonam Choudhari[2], Manivannan S S[3]
1 2 3 SITE, VIT University, Vellore, Tamilnadu, India.

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

Cryptography is an art of science which allows one normal public message or information and plaintext to protected private and secure information\message which one cannot read normally this is with the encryption and decryption.This is enables with substitution cipher method called Vigenere. Vigenere cipher is only limited to alphabets which we have extended in this paper to provide and make our communication over internet more secure and reliable. The use of symbols and numbers apart from alphabets brings the more difficult and cannot be predictable plaintext. In this paper we are proposing a reliable advanced method of cryptography for ultimate security.

Keywords: Plaintext, Ciphertext, Key, Cipher, Substitution, Vigenere, encryption and decryption.

Introduction

In today world technology keeps on changing and new development happens every day ,our everything is over internet so we exchange all our information and work through the internet. The amount of information that we exchange has evolved and increased and is till increasing day by day .For communication of information to occur and data should be made secure and a secure transmission path should created to preserve and protect the secret information over non secure or public or non-private channels .The sole and crucial motto of cryptography is to protect information from malicious or middle man individuals, cryptography makes it difficult and intensive for attackers or intruders to have the access to ones private information. The simple meaning of cryptography in Greek is secret writing. Vignere cipher has a limitation to alphabets only and to avoid this limit in this paper we have proposed our extension to numbers and special symbols also. With number and special symbols one can encrypt and decrypt full information with all different ways. Numbers and symbols when added to cipher dictionary the vocabulary of message in increased and enhanced efficiently and largely to a bigger extend.

The basic terms used in cryptography are listed below:

- Plain text

In cryptography, plain content is a basic decipherable content before being encoded into ciphertext. The information that can be perused and comprehended with no extraordinary measure is called plaintext

For example person A send message ―how are you‖ to person B. In this case ―how are you‖ will be our plain text message.

- Cipher text

In Cryptography, the change of unique message into non lucid message before the transmission is known as figure content [5]. It is a message acquired by some sort of encryption operation on plain content.

- Encryption

Encryption is a procedure of changing over plain content into figure content. Encryption handle requires encryption calculation and key to change over the plain content into figure. In cryptography encryption performed at sender end.

- Decryption

Unscrambling is the invert procedure of encryption. It changes over the figure content into plain content. In cryptography unscrambling performed at collector end.

- Key

The key is the numeric or alphanumeric content utilized for the encryption of plain content and unscrambling of figure content.

Objectives of Cryptography

Different objectives of cryptography are introduced in . These objectives include:

- Authentication

Confirmation is check of the personality of the sender at collector end. A client or framework can demonstrate their character to another who does not have individual information of their personality.

- Confidentiality

Privacy is most usually tended to objective. It alludes that transmitted message is just gotten by approved gathering.

- Integrity

Honesty is ensuring that the got message is in same shape as it was sent. Just approved clients have benefits to change the information.

- Access control

Get to control is ensuring that exclusive approved gatherings have benefits to get to the given data.

- Non Repudiation

Non denial is a technique for ensuring message transmission between gatherings by means of computerized mark or encryption. It ensures against the disavowal of confirmation endeavor.

Problem Statement

In existing algorithm we cannot encrypt number and symbols.Only use for encrypt plaintext which contain alphabets only which makes it less secure

Algorithm

Step-1-Take Plain Text (P) as in input. And read that text.

Step 2-If any space come remove that space and make it normal Plain text.

Step 3- Read Keyword for cipher K.

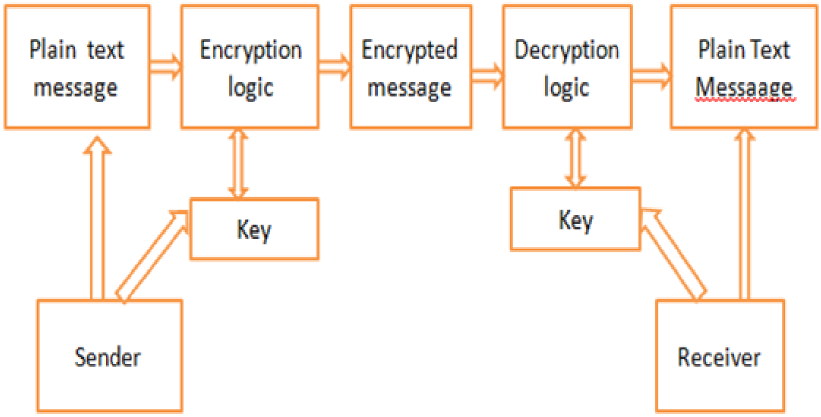
Step 4- Apply Equation C=P+K. We will get Cipher text from 1st Iteration.

Step 5- After Iteration 1st we will get the cipher text and to make it more secure again read the new Keyword (K) and repeat the Step 4.

Step 6- After every iteration we are getting new cipher text and perform the step 5 method until the iteration you want.

Step 7- Finally your message is encrypted, do same process in reverse for decryption.

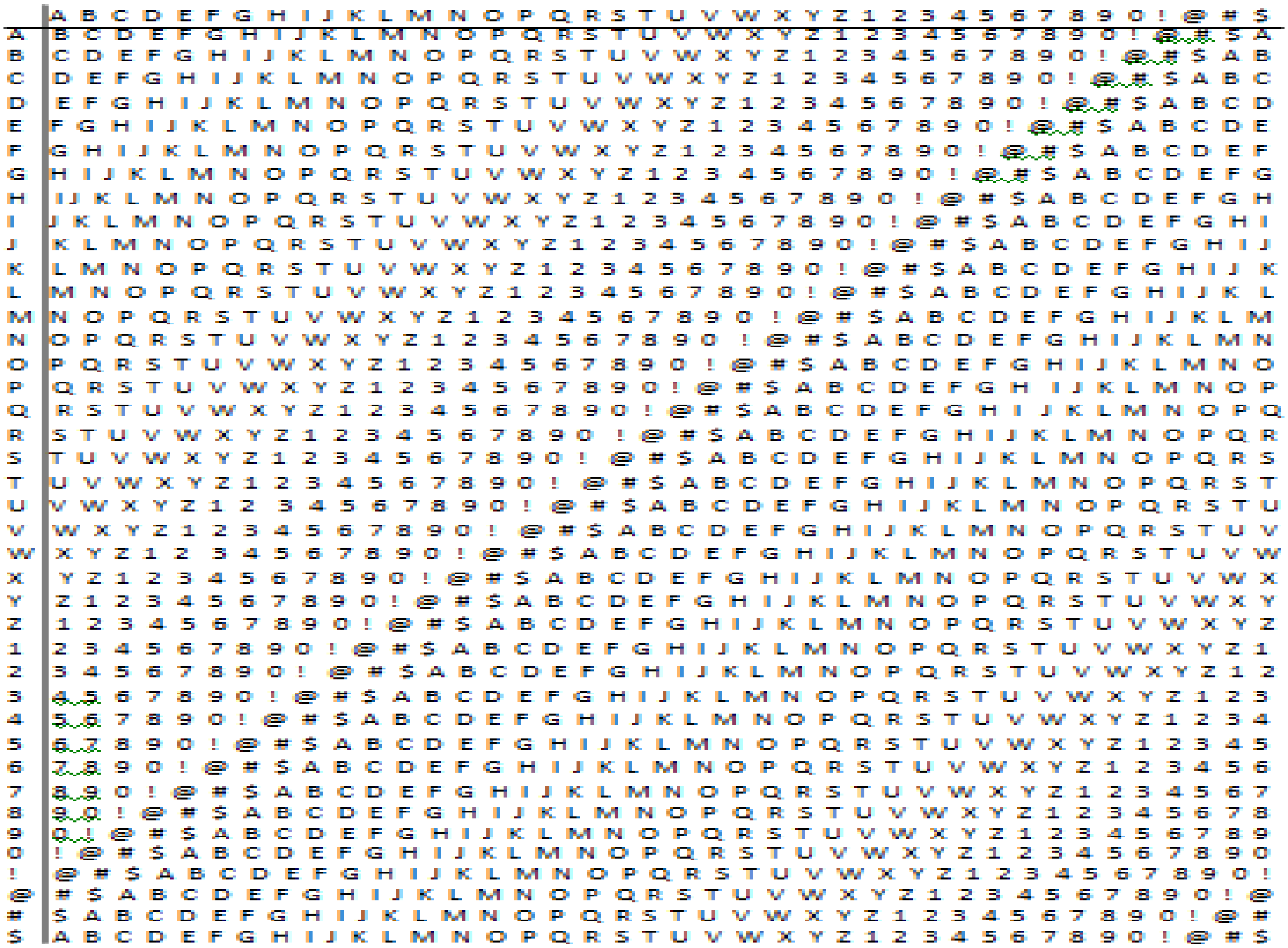
Architecture



Example:

Symmetric and Asymmetric are the two sorts of encryption. In symmetric encryption methods we utilize a similar key for both encryption and unscrambling purpose. Unbalanced key encryption utilizing open and private keys, people in general key is declared to all individuals while the private key is kept secure by the client. The sender utilizes people in general key of the beneficiary to encode the message. The collector utilizes his own particular private key to decode the message. In symmetric strategy, there are two procedures (substitution andtransposition) are utilized as a traditional techniques. Substitution procedure maps the Plaintext components into figurecontent components. Substitution has promote two sorts, Monoalphabetic andpolyalphabetic figure. In monoalphabetic the character in the Plaintext is changed to a similar character in the Ciphertext. In polyalphabetic figure a solitary character in the Plaintext is changed to numerous characters in the Ciphertext. Stage system is one in which the Plaintext continues as before, yet the request of characters is rearranged around to get the Ciphertext. Likewise the symmetric figures can be separated into Stream figures and piece figures, as an advanced ciphers.

Table- Vigenère cipher Square (43x43)



	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	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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
Z	1	2	3	4	5	6	7	8	9	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	Z
1	2	3	4	5	6	7	8	9	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	Z	1
2	3	4	5	6	7	8	9	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	Z	1	2
3	4	5	6	7	8	9	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	Z	1	2	3
4	5	6	7	8	9	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	Z	1	2	3	4
5	6	7	8	9	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	Z	1	2	3	4	5
6	7	8	9	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	Z	1	2	3	4	5	6
7	8	9	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	Z	1	2	3	4	5	6	7
8	9	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	Z	1	2	3	4	5	6	7	8
9	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	Z	1	2	3	4	5	6	7	8	9
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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	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	Z	1	2	3	4	5	6	7	8	9	0	!	@	#	$

1. Encryption

Iteration 1:

Plain text- SECURITY@123

Key 1-DOGDOGDOGDOG

Cipher Text- WTJY7PX$E5C0

Iteration 2:

Text(From Iteration 1)- - WTJY7PX$E5C0

Key 2- CATCATCATCAT

Cipher text- ZU42801AY8D9

Iteration 3:

Text(From Iteration 2)- ZU42801AY8D9

Key 3-RATRATRATRAT

Cipher Text- DVJF9PEBELE0

2. Decryption

Iteration 3:

Cipher Text- DVJF9PEBELE0

Key 3- RATRATRATRAT

Text- ZU42801AY8D9

Iteration 2:

Cipher Text- ZU42801AY8D9

Key 2- CATCATCATCAT

Text- WTJY7PX$E5C0

Iteration 1:

Cipher Text- WTJY7PX$E5C0

Key 1- DOGDOGDOGDOG

Plain Text- SECURITY@123

Conclusion

From the analysis and past work development the performance of Vigenere cipher was only limited to alphabets thus providing a small key length which is increased in this paper by including numbers and special symbols thus a higher key length.This make the performance of Vigenere cipher more secure and less predictable, performance of application is not compromised in this paper

The future work can include the cryptography of Vigenere cipher text with various other key length and performing the encryption and decryption of the plaintext two or more time to make the process perfect secure and 0% predictable.

References:

1. International Journal of Advanced Technology & Engineering Research(IJATER) www.ijater.com
2. A.Menezes, P.Van Oorschot and S.Vanstone, "Hndbook of Applied Cryptography". CRC Press, 1996.
3. D.Khan, " The Code breakers, the story of secret writing". New York: Mcmillan, 1967.
4. Advanced Computing: An International Journal(ACIJ), Vol 3, No.3, May 2012.