International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25095-25105

http://www.ripublication.com

A Noval Cryptographic Technique Magnified With Shielded Key Contract

[1]M.Janaki, [2]Dr.M.Ganaga Durga
[1]Research Scholar, Bharathiar University,
Assistant Professor, Dr.Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, India.
mjanaki81@gmail.com
[2]Research Supervisor, Bharathiar University,
Assistant Professor, Government Arts College for Women, Sivaganga, Tamilnadu, India. mgdurga@yahoo.com

Abstract

In a public network, the risks to sensitive data are greater than ever before. Network attacks have long been important problem which requires lot of research to be done to design security solutions that truly protects user's data it is essential to transmit private data securely by encapsulating from unauthroised users. The better way to protect data from malicious third party is to scrambled data before transmission. This paper sets out to contribute to area of the cryptography by developing a noval enchipherment technique which will conceal the confidential data sent through the network by obtaining a polyalphameric substitution cipher. The encryption / decryption of data are performed based on the VIJANA Tableau by using the substitution method. The mathematical background of the cryptographic method and key generation is given. This technique becomes more secured when it is works along with the key agreement method which is based on discrete logarithm. Four new algorithms for Key contract, Key generation, Encryption and Decryption are created and implemented. Encrypt / decrypt results got by applying the technique is shown with sample data. The VIJANA enchipherment technique is justified to be a true security solution to ensure privacy of data communication with crypt analysis done.

Keywords: Network security, Data confidentiality, Cryptography, Substitution cipher, Key agreement, Encryption, Decryption.

Introduction

Distributed environment bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between the users. Privacy of communication is essential to ensure that sensitive data cannot be modified or viewed during transmission. Ensuring privacy of confidential data is obtained by cryptography. Cryptography is the art of whispering thoughts secretly. People always had a fascination with keeping information away from others. History is filled with samples where people tried to keep sensitive military information secured from their enemies using basic cryptographic methods[4]. As the world becomes more connected, the demand for information and electronic services is growing and the need for more sophisticated methods of protecting data has also increased. The VIJANA encipherment technique proposed in this paper is a polyalphameric substitution cipher which involves the use of several cipher characters such alphabets, numbers and special symbols. Instead of there being a one - to - one relationship between each character and its substitute, there is a one - to - many relationship between each letter and its substitutes this protects VIJANA cipher from frequency analysis attack and there lies its strength.

Definition of Terms

In this paper, the term *encipher* is used to mean "the process of encoding messages in such a way that only authorized parties can read it", the term *decipher* is used to mean "the process of converting encoded messages back into its original form", the term *antiphon* is used to mean "the piece of information that acts as the secret key which is used to encode and decode messages", the term *communiqué* is used to mean "the discrete unit of communication i.e. message sent by the source for conception of some recipient", the term *dispatcher* is used to mean "the user who is sending a information to someone else", the term *acceptor* is used to mean "the user who is receiving the information from the source", the term *vanilla text* is used to mean "the ordinary readable text before being encoded into cipher text or after being decoded", the term *VIJANA text* is used to mean "the scrambled text which is obtained as the result of encoding performed on normal text using encoding algorithm.

Related Work

Blair demonstrated the cryptographic system on the task of learning to encode with the Caesar or Vigenere Cipher, and have shown how the evolution of one task may fruitfully be cross-pollinated with evolved solutions from other related tasks[1]. Nacira.G and Abdelaziz. A proposed a cipher algorithm of order θ using the Vigenere principle. A cipher method with numerical data is used. The cipher depends on the key that is composed by the triple (K, N, θ) where K is the key, N is a random number. θ is the function degree. The recurrent function and the cryptogram depend on the triple. The cipher of a character depends strongly on the degree of encryption, which is a part of the cipher key and, not only on length of key K. To better secure the transfer of data by Vigenere cipher, it is possible to increase the degree[2]

Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, Manika Sharma have created a Playfair Cipher method, based on polyalphabetic cipher. To add to its security and to make it more usable we are using 6x6 matrix instead of 5x5 which will be able to cover 26 alphabets in English and ten numerals i.e. from 0 to 9. This 6x6 matrix eliminate the case of putting of 2 alphabets (I and J) together in the matrix as it was in the 5x5 matrix. In this approach plaintext as well as key can be numeral, alphabetic or combination of both and a random number will shift the matrix every time[6]. Murali P and Senthilkumar G presented a new approach for secure transmission of message by modified version of Playfair cipher combining with random number generator methods[7].

Cryptography

The technique that protects sensitive information travels in the network is called as cryptography. Actually the subject has three names cryptography, cryptology, and cryptanalysis which are often used interchangeably. Cryptology is the all-inclusive term for the study of communication over non-secure channels. The process of designing systems to do this is called cryptography[6]. Cryptanalysis deals with breaking such systems. Modern cryptography is a field that draws heavily upon mathematics, computer science and cleverness. Cryptography can be either symmetric or asymmetric in nature based on the keys used for encipher and decipher. In symmetric key cryptography same (secret) key is used for both encipher and decipher. In asymmetric key cryptography public key is used for encipher and private key is used for decipher[8]. In cryptography a cipher is an algorithm for performing encipher or decipher, a series of well – defined steps can be followed as a procedure. There are many different types of ciphers available today. Some common ciphers are alphabet ciphers, math based ciphers and transposing or substitution ciphers.

Polyalphabetic cipher was first used by Leon Battista Alberti[5]. He used the substitution method of shifting multiple alphabets for a single alphabets later Johannes Trithemius have invented the tabula recta and Trithemius cipher in his work polygraphia. Using of a separate key was introduced by Glovan Batlista Bellaso. He have added a repeated “Counter Sign Key” known as a key for more security. Blasie de vigenere have created a methods called viginer cipher which is auto key cipher along with the table generated with 26 alphabets. The table contains 26 X 26 rows and columns with shifted alphabets from A to Z[10]. Francis Beaufort has found reciprocal cipher with a small modification of vigenere cipher. Along with the alphabets the 10 numerals from 0 to 9 are added in the table by Gronsfeld and its known as Gronsfeld cipher.

Key Exchange

One of the most important assumptions in modern cryptography is Kerckhoff’s Principle. In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used. This principle was enunciated by Auguste Kerckchoffs in 1883 in his classic teatise “La Cryptographic Militaire”[3]. The enemy can obtain this information in many ways such as encipher/decipher machines can be captured and analyzed. The security of the system should therefore be based on the key and not on the obscurity of the algorithm used.

Claude shannon’s 1948 paper “A Mathematical Theory of Communication” gave birth to the twin disciplines of information theory and coding theory. Information theory is the study of achievable bounds for communication and is largely probabilistic and analytic in nature. Coding theory attempts to realize the promise of these bounds by models which are constructed through mainly algebraic means[9]. Information passes from a source to a sink via a channel. The structure of information at source and sink is chosen by the user, but the behavior of the channel is not under user control. Cryptography is certainly concerned with communication; however the emphasis is not on efficiency but instead upon security. Nevertheless modern cryptography shares certain attributes and techniques with coding theory. Hence the key exchange between the users can be done efficiently by applying coding theory.

Communication Scenario

In the basic communication scenario there are two parties, we'll call them Adhira and Adharsh, who want to communicate with each other. A third party, Robin, is a potential eavesdropper. When Adhira wants to dispatch a communique, called the Vanilla text, to Adharsh, She enciphers it using a method prearranged i.e. VIJANA Encipherment with Adharsh. Usually the encipherment method is assumed to be known to Robin; what keeps the communique secret is an antiphon. When Adharsh accepts the enciphered communiqué called the VIJANA text, he changes it back to the Vanilla text using a decipher key.

Robin could have one of the following goals:

Case 1: Read the communiqué.

Case 2: Find the Antiphon and thus read all communiques enciphered with that Antiphon.

Case 3: Corrupt Adhira's communiqué into another communiqué in such a way that Adharsh will think Adhira dispatched the altered communique.

Case 4: Masquerade as Adhira and thus communicates with Adharsh eventhough Adharsh believes he is communicating with Adhira.

This communication scenario is shown in the following figure Figure 1.

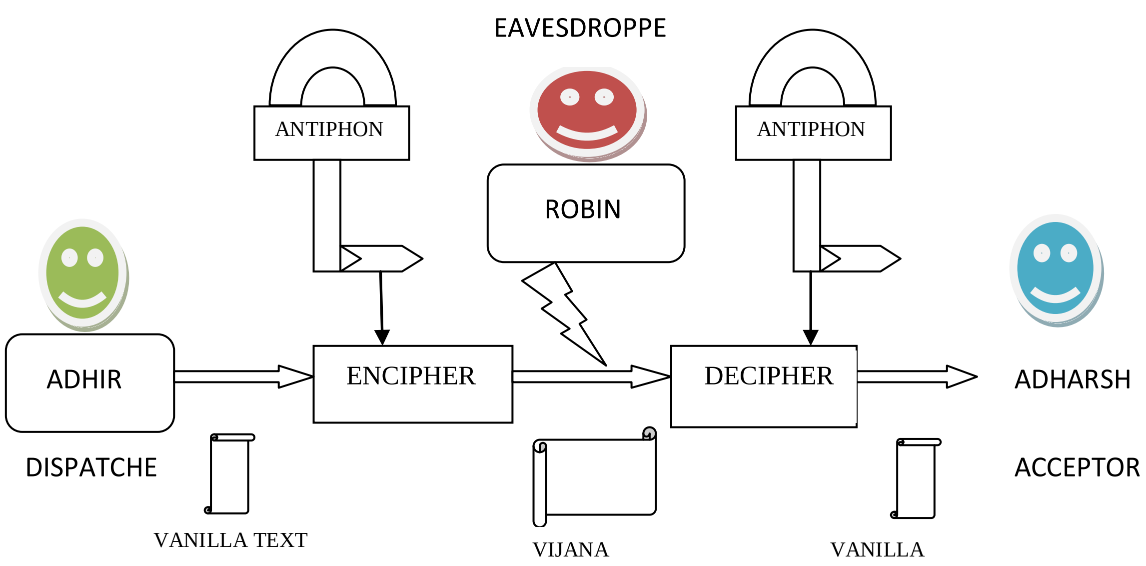

Figure 1: The Basic Communication Scenario for Cryptography

Proposed System

We propose a new technique called VIJANA Encipherment which is capable of enciphering the data by the dispatcher before transmission and deciphering the disguised data by the acceptor after transmission. This technique makes use of a key contract method based on discrete logarithm which allows this technique to enjoy with the secured key agreement as its advantage.

Vijana Encipherment Technique

The technology behind VIJANA Encipherment includes the polyalphameric substitution cipher based on VIJANA Tableau. A polyalphameric substitution cipher involves the use of several cipher characters such as alphabets, numbers and special symbols. Instead of there being a one-two-one relationship between each character and it substitute; there is a one-two-many relationship between each character and its substitutes. The VIJANA character set has 95 characters which includes 26 uppercase alphabets, 26 lowercase alphabets, 10 numerals, 6 braces, 7 operators, 19 special characters and a space. During encipherment or decipherment the ASCII code of the characters are taken into account.

The character set of the VIJANA Tableau is shown in the following table Table 1.

Table 1: VIJANA Character Set

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
SP	**!**	**“**	**#**	**$**	**%**	**&**	**‘**	**(**	**)**	*****	+	**,**	**-**	**.**	/	**0**	**1**	**2**
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
3	**4**	**5**	**6**	**7**	**8**	**9**	**:**	**;**	<	=	>	**?**	**@**	**A**	**B**	**C**	**D**	**E**
39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
F	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**
58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
Y	**Z**	**[**	\	**]**	^	**_**	**`**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**K**
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
l	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**{**	|	**}**	**~**

Using this character set VIJANA Tableau is generated with 95 rows and 95 columns. Each row of the table contains 95 characters shifted in a circular fashion. The first row is a shift of 0; the second row is a shift of 1; the third row is a shift of 2 and the last of row is a shift of 94. The VIJANA chipper uses this table together with a key word to encipher a message. If suppose the plain text message need to be enciphered using a keyword, The characters in the keyword have to be repeated as many times as necessary i.e. number of characters equivalent to the plain text message to derive the cipher text using the VIJANA tableau, for each character in the plain text there intersection of the row is given by the corresponding keyword character is found and the column given by the plain text itself to pick out the cipher text letter. Decipherment of an enciphered message is equally to straight forward. Here keyword letter is used to pick a row of the VIJANA tableau and then colum is traced across the row to get the corresponding cipher text letter the index of that colum is the plain text letter.

Algebric Description

VIJANA can be viewed algebraically, if the uppercase letters A-Z, lowercase letters a-z, numerals 0-9 and special symbols are to be numbered from 0-94 and addition is performed modulo 95.

VIJANA encipher E using the antiphon (Key K)

$C_i = E_K(M_i) = (M_i + K_i) \mod 95$

VIJANA decipher using the antiphon (Key K)

$M_i = D_K(C_i) = (C_i - K_i) \mod 95$

Whereas $M=M_0,M_1,\ldots.M_n$ *is the message*

$C=C_0,C_1,\ldots..C_n$ *is the cipher text*

$K=K_0,K_i\ldots.K_m$ *is used key*

Key Contract

The key exchange methodology based on discrete log problem will provide a better way to share the keys between the users. The dispatcher and the acceptor will get a common key without sharing it through the network. Automatically the common key is generated by sharing only a prime number and a primal root of the number.

The key contract method of agreeing with a common sealed key is shown in the following figure Figure 2.

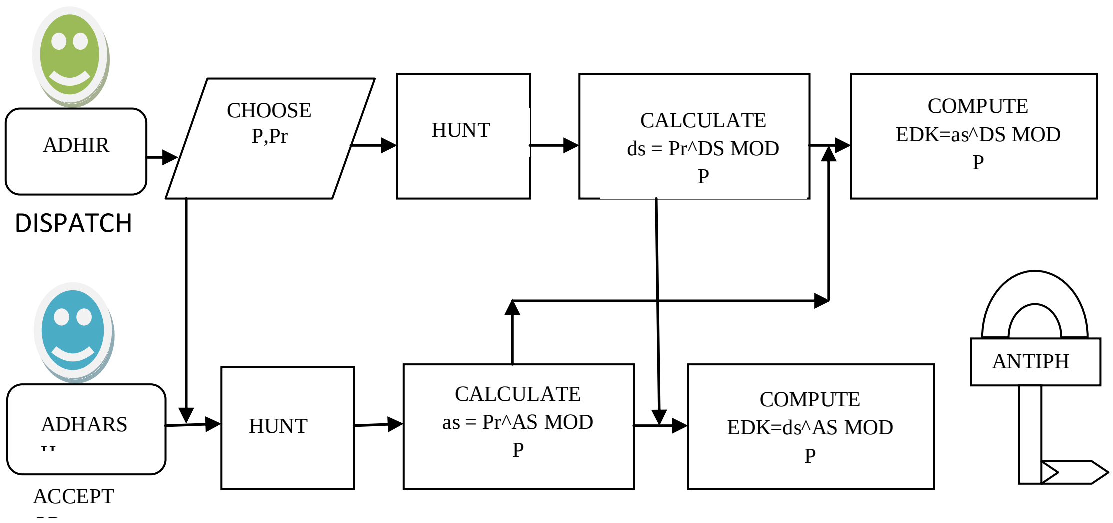

Figure 2: Key Agreement Method

The above figure Figure 2. Shows how the dispatcher computes her encipher key by finding the shared secret from the choosen prime number and primal root and how the acceptor computes the decipher key by finding the common shared secret form the prime number, primal root and his own sealed secret.

Formulation of Algorithms

There are four algorithms in VIJANA encipherment. The first algorithm is for key contract between the acceptor and the dispatcher. The second algorithm is for generating the antiphon key which will be used for encryption and decryption. The third algorithm is for enciphering the Vanila text into the VIJANA text using generated antiphon. The fourth algorithm is for deciphering the VIJANA text bact into the Vanila text.

The following table Table 2. Shows the notations used in the four algorithms of VIJANA Encipherment technique.

Table 2: Notations

S. No	Symbol	Description
1	P	Prime Number
2	Pr	Primal Root
3	DS	Dispatcher Sealed Secret
4	AS	Acceptor Sealed Secret
5	ds	Dispatcher Shared Secret
6	as	Acceptor Shared Secret
7	EDK	Encipher/Decipher Key
8	K	Antiphon
9	Vt	Vanilla Text
10	VT	VIJANA Text

The fist algorithm for key agreement between the dispatcher and the acceptor based on the discrete logarithm is as follows,

---

Algorithm 1 : KEY CONTRACT

Data : Prime P, Primal root Pr
Result : Encipher/Decipher Key EDK
Begin
Step 1 : Dispatcher and Acceptor agrees with the initial inputs P and Pr.
Step 2 : Dispatcher hunts his Sealed Secret DS.
Step 3 : Acceptor hunts his Sealed Secret AS.
Step 4 : Dispatcher calculates ds = (Pr ^ DS) mod P.
Step 5 : Acceptor calculates as = (Pr ^ AS) mod P.
Step 6 : Dispatcher sends dispatcher shared secret ds to the

Acceptor.
Step 6 : Acceptor sends acceptor shared secret as to the Dispatcher.
Step 7 : Dispatcher computes EDK = (as ^ DS) mod P
Step 8 : Acceptor computes EDK = (ds ^ AS) mod P.
End

The second algorithm for generating the Antiphon key from the exchanged key is as follows,

---

Algorithm 2 : ANTIPHON GENERATION

Data : Encipher/Decipher Key EDK
Result : Antiphon K
Begin
Step 1 : Find S = EDK * EDK.
Step 2 : Split S in to two – two digits such that $S_i = S_1, S_2, S_3 \ldots\ldots\ldots S_m$, where m = n/2 [n is the number of digits in S].
Step 3 : Check if S_i >95 then
Find V_i = Si mod 95
end if.
Step 4 : Take the corresponding V_i^{th} character from the VIJANA character Set.
Step 5 : Repeat steps 3 and 4 for all Si where i = 1,2,3……….m.
Step 6 : Obtain the Antiphon K by concatenating the VIJANA character got from each V_i.
End

The above algorithm is capable of splitting the exchanged key as two-two digits and equivalent key from the VIJANA chacter set is taken as the Antiphon Key.

The third algorithm is for disguising the plain Vanila text into cipher VIJANA text using the polyalphameric substitution cipher is as follows,

---

Algorithm 3 : JKG ENCIPHER

Data : Vanilla Text Vt, Antiphon K
Result : VIJANA Text VT
Begin
Step 1 : Write the Antiphon repeated as many times as necessary (i.e.) equal to the number of characters in Vanilla Text.
Step 2 : Find the index of each character in Vt_i and K_i from the VIJANA character set, where i = 1,2,3,……..n
[n is the length of Vanilla Text].
Step 3 : Compute $VT_i = (Vt_i + K_i)$ mod 95.
Step 4 : Find the characters of the index VT_i from VIJANA character set.

Step 5 : Repeat Steps 2, 3 and 4 for all characters in the Vanilla
Text Vt to obtain the VIJANA Text VT.
End

The above algorithm will encipher the Vanila text by using the VIJANA Tableau along with the generated Antiphon key.

The fourth algorithm is for obtaining the Vanila text from the VIJANA text using the polyalphameric substitution cipher is as follows,

---

Algorithm 4 : JKG DECIPHER

Data : VIJANA Text VT, Antiphon K
Result : Vanilla Text Vt
Begin
Step 1 : Write the Antiphon repeated as many times as necessary
(i.e.) equal to the number of characters in VIJANA Text.
Step 2 : Find the index of each character in VT_i and K_i from the
VIJANA character set, where i = 1,2,3,……..n
[n is the length of VIJANA Text].
Step 3 : Compute $Vt_i = (VT_i - K_i) \bmod 95$.
Step 4 : Find the characters of the index Vt_i from VIJANA
character set.
Step 5 : Repeat Steps 2, 3 and 4 for all characters in the VIJANA
Text VT to obtain the Vanilla Text Vt.
End

The above algorithm will obtain the original Vanila Text form the VIJANA Tableau by using the Antiphon key.

Results

After implementing the VIJANA encipherment with the shielded key contract the following results are obtained. The size of the original file is 512 bytes, the key generated is 32 bits. The Vanilla text before encipherment and VIJANA text after encipherment using the Antiphon key generated are,

Vanila Text :

Patiend–id:PUC1051,Disease:Kidney-Stone, Specification:8mm-Stone-in-left-Kidney Requirement:opinion.

Antiphon Key : Jx1*yaNZ?3+trA#5

VIJANA Text:

Y15q+rMG35;iDEF#"~ARflnpz/*235xyPN,:58Mne2;'4
@cCA4h5ra239-%rql opmK6005y?FeJanaki6253xy*2onx

Cryptanalysis

The brute-force attack by a hacker would start at one-digit passwords before moving to two-digit passwords and so on, trying all possible combinations until one works.

While using VIJANA cipher technique it is not possible for hacker to use brute-force attack because keyword is generated based on the discrete logarithm. Encrypted text is sometimes achieved by replacing one letter by another. To start deciphering the encryption it is useful to get a frequency count of all the letters. The most frequent letter may represent the most common letter in English E followed by T, A, O and I whereas the least frequent are Q, Z and X. Hackers would use this frequency analysis for tracing the password. This can be prevented by VIJANA encipherment since multiple characters are substituted for a single character, every time a different character is substituted for the same character since we have several shifts. The index of coincidence is a measure of how similar a frequency distribution is to the uniform distribution. Measures the probability that two random elements of the n-letters string x are identical. VIJANA encipher masks the character coincidence because it replaces multiple characters for a single character.

Conclusion

In order to provide better security in the network during the transmission of data, polyalphameric substitutions ciphers can be used. Thee proposed methodology in this paper used this substitutions cipher effectively along with the key generation based on discrete log problem. The VIJANA encipherment is successfully implemented and proved to the efficient by the crypt analysis done. This encipher technique will resist to many of the possible attacks made by the hackers in the network. Thus the confidential data can be protected by disguising it using the VIJANA encipherment.

References

[1] Blair, A. “Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination” Evolutionary Computation (CEC), 2013 IEEE Congress.

[2] Nacira.G, Abdelaziz. A ,”The &thetas;-vigenere cipher extended to numerical data” Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004.

[3] Omran, S.S. ; Al-Khalid, A.S. ; Al-Saady, D.M. “A cryptanalytic attack on Vigenère cipher using genetic algorithm” Open Systems (ICOS), 2011 IEEE.

[4] Mehmet E. Dalkilic, Cengiz Gungor, “An Interactive Cryptanalysis Algorithm for the Vigenere Cipher”, Advances in Information Systems Lecture Notes in Computer Science Volume 1909, 2000, pp 341-351.

[5] William J. Spezeski, “A Keyless Polyalphabetic Cipher”, Technological Developments in Networking, Education and Automation 2010, pp 529-532.

[6] Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, Manika Sharma, “Enhanced Block Playfair Cipher”, Quality, Reliability, Security and Robustness in Heterogeneous Networks, Lecture Notes of the Institute for

Computer Sciences, Social Informatics and Telecommunications Engineering Volume 115, 2013, pp 689-695.

[7] Murali, P, Senthil kumar, G. "Modified Version of Playfair Cipher Using Linear Feedback Shift Register", Information Management and Engineering, 2009. ICIME '09.

[8] Ranju s kartha, Varghese Paul, "Survey : recent modifications in vigenere Cipher ", IOSR Journal of computer Engineering, Volume 16 Issue 2, Mar-Apr 2014.

[9] Kallam Ravinda Babu, Dr.S. Valaya Kumar, Dr.A. Vinaya Babu, Dr.M. Thirupathi Reddy, "An Enhanced cryptographic substitution method for information security", International Journal of Mathematical Archive -2 (10) 2011.

[10] Quist – Aphetsi Kester , " A Crypto System based on vigenere cipher with varying key, International Journal of advanced research in Computer Engineering and Technology, Volume 1, Issue 10, December 2012.