ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Enhanced Polyalphabetic Cipher using Extended Vigenere Table

Ravindra Babu Kallam
Professor in CSE,
Vivekananda Institute of Technology and Science SET,
JNTUH, Kareemnagar, AP, India.
rb_kallam@yahoo.com

Dr.S. Udaya Kumar
Deputy Director, SNIST, J N T University,
Hyderabad, AP, India.
uksusarla@rediffmail.com

Dr. A. Vinaya Babu
Director, Admissions, J N T University,
Hyderabad, AP, India.
avb1222@gmail.com

Md Abdul Rasool
HOD CSE, VITS SET,
Kareemnagar, India.
rasool.501@gmail.com

Puskur Pavan
Computer science Engineering, AZCET,
AP, India.
puskurpavan@gmail.com

Abstract: The objective of this investigation is to find the competent and most extensively used cryptographic algorithms form the history, identifying one of its merits and demerits which have not been modified so far. A proposal will be given to overcome the problems in the investigated algorithms to meet the current requirements. Observation of cryptography, its techniques such as transposition & substitution were discussed. Our main focus is on the Poly alphabetic Cipher, its advantages and disadvantages. Finally we have proposed a method to enhance the Poly alphabetic cipher for more secure and efficient cryptography.

Keywords: Security; Algorithm; Cipher;Cryptography;Encryption;Decryption;Substitution;Transposition;Vigenere Table;

I. INTRODUCTION

Cryptography systems are generally classified into types of operations used for transforming plain text to cipher text, the number of keys used, the way in which plain text is processed. All encryption algorithms are based on two general principles: Substitution [5], in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and Transposition, in which element in the plain text are rearranged [1]. Fundamental requirement is that no information will be lost. A block cipher processes the input one block of element at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along [7].

A Poly alphabetic cipher is a method based on different monoalphabetic substitutions as one proceeds through the plain text message. The best known and one of the simplest such algorithm is referred to as Vigenère cipher[8].

In a simple monoalphabetic cipher each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E and so on [6].

The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values. The sender converts plaintext into cipher text using a keyword, the receiver decrypts the cipher text into plain text. Converted plaintext is in sequence of alphabets without any space between them [2].

It may create a problem for receiver to read the message by inserting spaces between words. The converted sentence may or may not form a meaningful one. Even though it is meaning full the sentence, it may not be the exact plain text, because, the receiver needs to guess the exact place to insert space in decrypted plaintext. Hence the user will be under pressure to choose the place for inserting space. To overcome this problem we have proposed an enhanced polyalphabetic cipher with extended vigenere table.

II. EXISTING SYSTEM

Vigenere cipher is one of the simplest and well-known algorithms in polyalphabetic cipher. In this algorithm a table of alphabets can be used for both encryption and decryption, termed as tabula recta, Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.

Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plaintext letter a. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to itself. The Vigenere table is as shown in Figure 1.

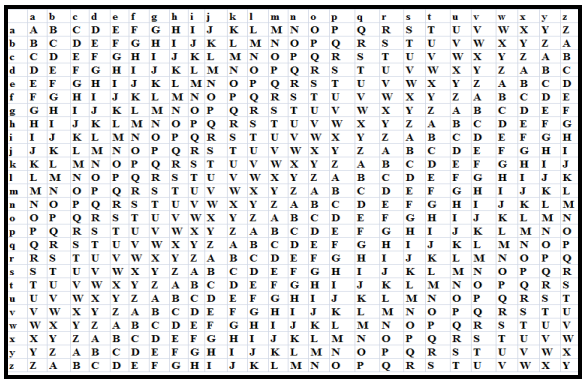

Figure 1: Existing Vigenere Table

At different points in the encryption or decryption processes, the cipher uses a different alphabet from one of the rows of the Vigenere table. The alphabet used at each point depends on a repeating keyword.

For encrypting a message or plaintext the user should chose a key by satisfying the condition that the length of the key should be equal to the length of the plaintext. For a given key letter *x* and the plain text *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.

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 plaintext letter is at the top of the column. For example the plaintext is: *"an ice image"*

The sender of the message chooses a keyword and repeats it until its length matches with the length of the plaintext, for example, the keyword *"lemon",* then the key will be: "lemonlemon"

The first letter of the plaintext is 'a', can be enciphered using the alphabet in row 'l', which is the first letter of the key chosen. The cipher letter is the intersection of the row 'l' and column 'a' of the Vigenère square, here it is 'L', and it will continue as shown below. The cipher text for the chosen plaintext will be 'LRXQRTQMUR'.

Plaintext:	aniceimage
Key:	lemonlemon
Cipher text:	LRXQRTQMUR

For decryption select the row based on the key letter, finding the position of the cipher text letter in that row, and use the corresponding column label as the plaintext.

It is to be noticed that the existing algorithm do not consider the space in the sentence while converting. Hence the receiver will be under ambiguity where to insert the space in the available text, because there is a possibility of forming two different sentences with different meaning with the same decrypted text. It can be observed from the above example that the plain text can be any of the following.

A. a nice image
B. an ice image

In security a service, each communication is very critical and has a lot of hazard involves, in such a case the receiver should not have a choice to select the sentence, they should obey their superior order, otherwise that may leads to lot of problems.

The technology [4] is changing a lot with rapid speed, many surveys saying that, the usage of computer is massively increasing. Hence stronger security algorithms need to be invented or the existing algorithms should be updated for providing more security to the information either in the PC or in the transmission [3].

To meet the current requirements, we have enhanced the Play fair algorithm.

III. PROPOSED SYSTEM

In order to conquer this difficulty we have anticipated an enhanced polyalphabetic cipher with extended vigenere table.

For this we have added a new symbol into the row and column of the Vigenere Tableau, which is not in use worldwide. The new symbol can be used to represent or to locate the blank space in the plaintext. Hence the user can easily encrypt or decrypt the message or plaintext with out any ambiguity. Our proposed Vigenere Table is as shown in the Figure 2.

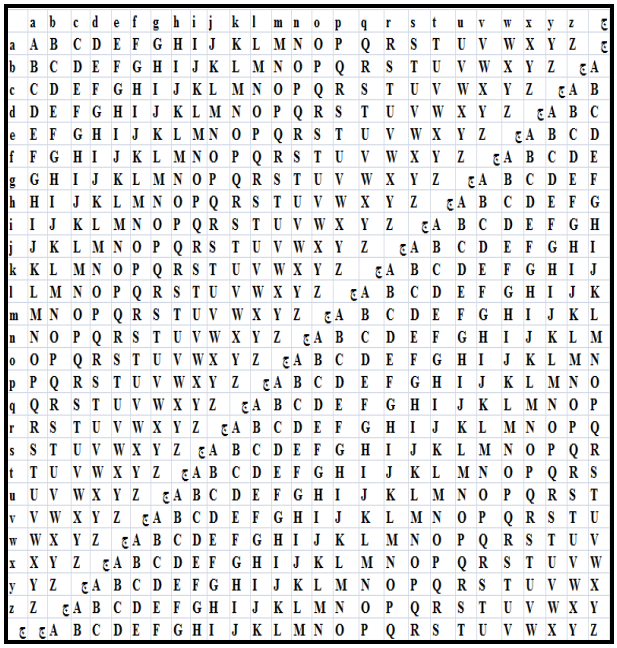

Figure 2: Enhanced Vigenere table

With this, it is mandatory for the sender to use the special invented symbol in the plaintext where ever the space is needed and then it can be encrypted as usual.

The plain text in the previous example"an ice image" should be first written as "anᓭiceᓭimage" and can follow the same procedure as before. If the keyword is same then the plaintext, key and cipher text are as follows:

Plaintext:	anᓭiceᓭimage
Key:	Lemonlemonle
Cipher text:	LRLWPPDUBNRI

ᓭ= this symbol indicates space between the words.

After decryption at the receiving end the receiver must remove the space characters in the text and hence, he will get the actual plain text.

IV. RESULTS

With this enhanced poly alphabetic cipher with extended vigenere table the user can encrypt and decrypt the message with out any ambiguity and with minor changes in the existing system.

V. CONCLUSION

Concept of cryptography was discussed in brief. Impotence of poly alphabetic cipher was highlighted; its merits and demerits were presented with example. Focused on extended vigenare table to solve the existing problems in present algorithms and its need were discussed.

VI. ACKNOWLEDGMENT

We like to thank the Principal and Management of Vivekananda Institute of Technology and Science, Kareemnagar, AP, India for providing all the facilities to complete the task.

VII. REFERENCES

[1] Diffi and Hellman, " Privacy and authentication: an introduction to cryptography",Proceedings of the IEEE,67(1979), PP, 379-427.

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

[3] Linda S Rutledge, "A Survey of Issues in Computer Network Security", Elsevier Science Publishers B.V North Holland, Computers and Security 5 (1986) 296-308.

[4] Rivest.R,"The impact of technology on cryptography", Proc. IEEE International Communications Conference, Toronto, Canada, June 1978.

[5] 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.

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

[7] William Stallings, "Cryptography and Network Security", Fifth Impression,2008, p age no: 35 – 54.

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