International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-4, April 2013

A Survey of Existing Playfair Ciphers

Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh

Abstract— ***The role of cryptography in today's world is increasing day by day. Information is flowing from one place to another on the network. One most common cryptography technique is substitution cipher. Play fair is most common substitution cipher. In this paper, we present an overview of existing playfair ciphers. Encryption/decryption is a very popular task. We also explain the fundamentals of sequential cryptography. We describe today's approaches for play fair cipher. Their strengths and weaknesses are also investigated. It turns out that the behavior of the algorithms is much more similar as to be expected.***

Index Terms*— *Cryptography, Network Security, Symmetric Key, Playfair cipher and substitution

I. INTRODUCTION

In this age of universal electronic connectivity, of viruses and hackers, of electronic fraud, there is indeed no time at which security does not matter. The explosive growth in computer systems and their interconnection via network has increased the dependence of both organizations and individuals on the information stored and communicated using these systems which intern has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks.

Also the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security. Cryptography is the design of certain techniques for ensuring the secrecy and/or authenticity of information. Earlier the requirement of information security within an organization was primarily provided by physical and administrative means [1]. But the concept of network security became quite evident with the introduction of computers and later with introduction of distributed systems. The need of cryptographic algorithm is to avoid threat to integrity confidentiality and availability.

Symmetric Cipher Technique is also known as Conventional, Single key, Secret Key, One – key and classical encryption techniques. This technique is based on the encryption of plain-text to cipher-text which is safe to transmit and from unauthorized access, by using a secret key in a specific encryption algorithm. It uses the following ingredients:

Manuscript published on 30 April 2013.
***** Correspondence Author (s)
Jitendra Choudhary, Computer Science Department, SSSIST, Sehore, India.
Prof. Ravindra Kumar Gupta, Computer Science Department, SSSIST, Sehore, India.
Dr. Shailendra Singh, Computer Science Department, NITTTR, Bhopal, India.

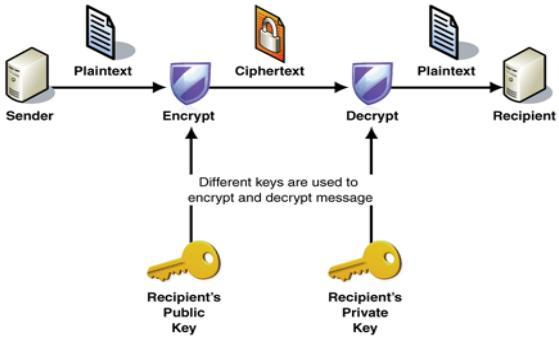

Fig.1- Process of encryption and decryption

A. Plain Text

This in an intelligible piece of information i.e. original text that needs to transferred safely to the receiver. It is the main input to the encryption algorithm.

B. Secret Key

This is another input to the encryption and decryption algorithm, which is the main component used for converting the plain-text to cipher-text i.e. an unintelligible form which has the useful content hidden in a way.

C. Encryption Algorithm

This is the actual process by which we are converting the plain-text into cipher text.

D. Cipher Text

This is the output of encryption process in which we are taking plain-text and secret key as input and processed by encryption algorithm. The cipher-text can be understood as a scrambled piece of text which has useful information in secret form.

E. Decruption Algorithm

This algorithm is the reverse of the encryption algorithm which takes in cipher-text and secret key as inputs and produces plain-text as the output.

II. PLAYFAIR CIPHER

Playfair cipher that is a substitution cipher was first developed by Charles Wheatstone in 1854. Later it was promoted by Lord Playfair. Now it is called playfair cipher [2, 6].

A. Existing Playfair Algorithm using 5x5 Matrix

The existing playfair cipher working on 5x5 matrix is constructed with a keyword "CRYPTO". The Table 1 below shows the construction of 5x5 matrix using the keyword "CRYPTO" plus the uppercase alphabets satisfying the rules of preparing the table. The matrix is first filled by the keyword from left to right and the remaining cells are filled by the uppercase alphabets ignoring the letters of keyword.

TABLE-I-Playfair 5x5 matrix

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

2.1.1 Rules

a) Plaintext letters that fall in the same row of the matrix are replaced / substituted by the letter to the right, with the first element of the row circularly following the last. For example pt is encrypted as TC.

b) Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following in the last. For example, cu is encrypted as OC.

c) Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, oh becomes BF, and fd becomes IO (or JO, as the enciphered wishes) [2].

Limitations of 5x5 Matrix

- It considers the letters I and J as one character.
- 26 letters alone can take as keyword without duplicates.
- Space between two words in the plaintext is not considered as one character.
- It cannot use special characters and numbers.
- It only uppercases alphabets.
- A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored. X is a valid character and creates confusion because it could be a part of plaintext, so we cannot simply remove X in decryption process.
- X is used a filler letter while repeating letter falls in the same pair are separated.

B. Existing Palyfair Algorithm using 7x4 matrix

A keyword is used to construct 7x4 matrix using letters and symbols „*" and „#" which is the base for this Playfair Algorithm. The 7x4 matrix is constructed by filling keyword with no repeating letters. Here the keyword "CRYPTO" is used. The remaining spaces are filled with the rest of alphabets. As shown in the table 2, the last cell is filled by the symbol "#" and the remaining cell that is before the last cell is filled by the symbol "*" [3].

TABLE-II-Playfair 7x4 matrix

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

The same rules of playfair 5x5 matrix are used here to encrypt the plaintext with the following modification.

- When same letters fall in a pair it adds "*" so that the message BALLS become BAL*LS.
- If a word consists of odd number of letters, it will add symbol "#" to complete the pair. So BIT becomes BI T#. The symbol # is simply ignored when the ciphertext is decrypted.

Limitations of 7x4 Matrix

- 26 characters only can take as a keyword without any repetition.
- The space between two words in the plaintext is not considered as one character.
- It cannot use numbers and special characters except „*" and „#".
- It is not case sensitive.
- It ignores the symbols „*" and „#" at the time of decipherment.

III. CONCLUSION

In this paper, we surveyed the existing variants of play fair cipher. There strength and weaknesses are also observed. In a forthcoming paper we will propose a new variant of playfair cipher.

REFERENCES

[1] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.

[2] William Stallings, "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall, 2006.

[3] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, "Universal Playfair Cipher Using MXN Matrix". International Journal of Advanced Computer Science, Vol.1, No.3, Pp.113-117, Sep.2011.

[4] Ravindra Babu K, S.Uday Kumar, A. Vinay Babu, I.V.N.S. Aditya, P.Komuraiah, "An Extension to Traditional Playfair Cryptographic Method". International Journal of Computer Applications (0975 – 8887), Volume 17- No.5, March 2011.

[5] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)". World Academy of Science, Engineering and Technology 73 2011.

[6] Dhenakaran, Ilyaraja, "Extension of play fair cipher" IJCA, pg no 37-41, June 2012.