A Modified Version of Playfair Cipher Using 7×4 Matrix

A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam

Abstract—This paper deals with the modification of playfair cipher. The original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair cipher in which two symbols "*" and "#" are included. The addition of these two symbols in the matrix creates one-to-one correspondence between the plaintext and the ciphertext, which makes the encryption and decryption easy and unambiguous. The text is more unreadable when these symbols appear in the resulting ciphertext. Also this method can be extended to encrypt and decrypt the messages of any language by taking a proper size matrix.

Index Terms—**Cryptography, ciphertext, plaintext, playfair cipher, substitution cipher, transposition cipher.**

I. Introduction

Cryptography is a Greek word which means secret writing. Today this term refers to the science and art of transforming messages to make them secure and immune to attacks [1]. For the purpose of security and privacy, we need to encrypt the message at the sender side and decrypt it at the receiver side. So cryptography is the study of creating and using encryption and decryption techniques.

Cryptography is divided into two types, Symmetric Key Cryptography and Asymmetric Key Cryptography [1]. In Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message.

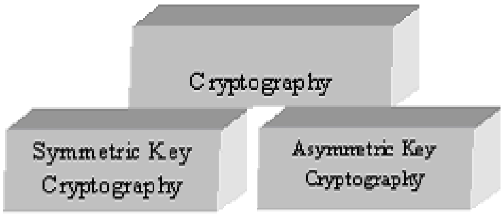

Fig. 1. Types of cryptography.

In Symmetric Key Cryptography two types of ciphers, substitution cipher and transposition cipher are used [1]. In substitution cipher one symbol of the plaintext is replaced by another symbol. Substitution cipher has further two types. Monoalphabetic substitution cipher, in which a character in the plaintext is always changed to the same character in the ciphertext. The well known example of Monoalphabetic substitution cipher is the CAESAR cipher which always change a to d. In polyalphabetic substitution cipher a single character in the plaintext is changed to many characters in the ciphertext. The well known example of polyalphabetic substitution cipher is VIGENERE cipher which changes a single character in the plaintext into many characters in the ciphertext by considering the position of character in the plaintext.

In transposition cipher the characters in the plaintext are swapped to get the ciphertext i.e. the characters retain their plaintext form but their position is changed. The plaintext is organized into two dimensional table and columns are interchanged according to a predefined key.

II. The Playfair Cipher

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].

Playfair is digraph substitution cipher which uses a 5×5 matrix, in which the key word is written first and the remaining cells of the matrix are filled with other letter of alphabets with I and J taken in the same cell. The message is divided into digraphs, in which repeating letters in the same pair are separated by filler letter X. In case of odd number of letters in the message a spare letter X is padded with the word to complete the pair. Then the plaintext is encoded according to the four rules presented in [3].

Any word with no repeating letters can be selected as a key word to fill the matrix. The problem arises when the letter I or J appears in the key word. Suppose we choose the key word "CIPHER" and take the L and M in the same cell as shown in Table I.

TABLE I: Choose the Key Word "CIPHER" and Take the L and M

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

Now we encrypt the message "LOVE ALL PEOPLE" using the rules of the playfair cipher presented in [3].

Plaintext: LOVE ALL PEOPLE
Diagraphs: LO VE AL LP EO PL EX
Ciphertext: GT ZC DJ KH CU HK PZ

The decryption of the above ciphertext generates two valid

Manuscript received November 24, 2012; revised January 26, 2013. This work was supported by university of Malakand K.P.K Pakistan.

The authors are with the Department of Computer Science & IT University of Malakand Chakdara KPK Pakistan (e-mail: alam@uom.edu.pk, shshkhalid@uom.edu.pk, msmdir@gmail.com).

DOI: 10.7763/IJCTE.2013.V5.762

english sentences.

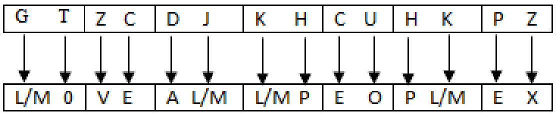

Fig. 2. The decryption of the ciphertext

Considering the first digraph "GT" in the ciphertext it is obvious from the mapping that G can be replaced by L and M. We get the original plaintext "LOVE ALL PEOPLE" if G is replaced by L. But if G is replaced by M , we get the plaintext "MOVE ALL PEOPLE" which is also a valid sentence.

III. Modified Version of Playfair Cipher

The problems in 5×5 matrix playfair cipher arise when either I or J, or both appear in the key word. Also when the plaintext word consist of odd number of characters, a spare letter " X "is padded with the word to complete the pair. In the decryption process this "X" is simply ignored. This creates confusion because X is a valid character and it can be the part of plaintext, so we cannot simply remove it in the decryption process. In this study we proposed 7×4 matrix playfair cipher which efficiently handles these problems.

In 7×4 matrix playfair cipher any word with no repeating letter can be selected as a key word. The remaining spaces are filled in order with the rest of alphabets. The second last cell is filled with the symbol "*" and the last cell is filled with the symbol "# "as shown in the Table II.

TABLE II: 7 ×4 Matrix Playfair Cipher

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

To encrypt the plaintext, the same rules presented in [3] are followed with the following modification.

- If both letter are same in a digraph, add a "*" after the first letter, so a BALLOON will be treated as BA L* LO ON.
- If a word consists of odd number of letters, add the symbol "#" to complete the pairs. So ALL become AL L#. The "#" is simply ignored when the ciphertext is decrypted.

Now we encrypt the message "LOVE ALL PEOPLE" using modified playfair cipher.

Plaintext: LOVE ALL PEOPLE
Diagraphs: LO VE AL LP EO PL E#
Ciphertext: KQ UR RM MI DU IM BY

By decrypting the above ciphertext and ignoring the "#" symbol, we get a single sentence "LOVE ALL PEOPLE" which is the original plaintext message. The mapping of the ciphertext into plaintext is shown in Fig. 3. There correspondence between ciphertext and plaintext is one-to-one. So there is no confusion in the decryption process.

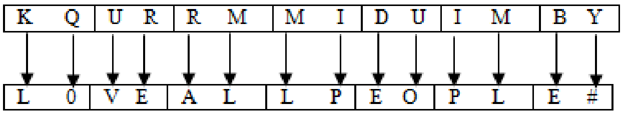

Fig. 3. Decrypting the ciphertext

IV. Cryptanalysis

In cryptography, confusion and diffusion play an important role in the development of a cipher [4]-[6]. Confusion refers to making the relationship between the key and ciphertext as complex as possible and can be achieved by transposition. Diffusion refers to making the relation between the plaintext and ciphertext as complex as possible. Strong confusion and diffusion make it difficult for the attacker to find the key or plaintext if the attacker has large number of plaintext and ciphertext pairs.

Like the original playfair cipher, the algorithm proposed in this study can also be easily cracked if someone has enough ciphertext and plaintext pairs. The addition of the " * " and " # " symbols have greatly increased the diffusion but still the proposed algorithm can be cracked by the same methods as the original 5×5 matrix playfair.

V. Conclusion

In this paper the original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair cipher. The symbols "*"and "#" are included in the matrix which create one-to-one correspondence between the plaintext and the ciphertext. So the encryption and decryption process is unambiguous and easy. The beauty of the proposed method is that it can be applied to any language by just taking a proper size matrix, which can accommodate all alphabets of that language.

Acknowledgement

The we are very thankful to Almighty Allah; whose grace and blessed mercy enabled us to complete this work with full devotion and legitimacy. We are grateful to Mr. Fakhruddin and Mr. Nasir Rashid (Department of Computer Science and IT, University of Malakand) for their invaluable support and guidance throughout this research work.

We also want to thank our friends and family for their encouragement; without whose support we could not have lived through this dream of ours.

References

[1] A. Forouzan and G. Hill, *Data Communications and Networking*, 4th Edition by Behrouz, Feb 9, 2006.

[2] Playfair Cipher. (2010). [Online]. Available: http://en.wikipedia.org/wiki/Playfair_cipher.

[3] *Cryptography and Network Security: Principles and Practice*, 4th Edition by William Stallings, Prentice Hall, Nov 26, 2005.

[4] H. A. A. Hassan, M. Saeb, and H. D. Hamed, "The PYRAMIDS block cipher," *International Journal of Network Security*, vol. 1, no. 1, pp. 52-60, 2005.

[5] Y. Kurniawan, M. S. Mardiyanto, and S. Sutikno, "The new block cipher: BC2," in *Ternational Journal of Network Security*, vol. 8, no.1, pp. 16-24, 2009.

[6] P. Lin, W. L. Wu, and C. K. Wu, "Security analysis of double length compression function based on block cipher," *International Journal of Network Security*, vol. 4, no. 2, pp. 121-127, 2007.

A. Aftab Alam was born in Chakdara, Pakistan, in 1982. He received his BS-IT (Hons) degree from University Of Malakand, Pakistan in 2007 and MS (CS) degree from FSAT-NU, Pakistan in 2010, with specialization in Networking. Currently he is perusing his Ph.D from University of Malakand, Pakistan. His current research interests include information security, next generation networks, 3D Graphics and Bioinformatics.

B. Shah Khalid was born in Tekni Payeen,Pakistan in 1981. He received his M.Sc degree in Computer Science from University of Peshawar,Pakistan in 2004 and now perusing his M.S. degree in Computer Science from Abaseen University, Pakistan. Currently he is working as Lecturer in the department of computer science, University of Malakand Pakistan. His current research interests include wireless and mobile communications, network security and virtual reality environments.

C. Muhammad Salam was born in Dir Pakistan, in 1981. He received his M.Sc degree in Computer Science from University of Peshawar,Pakistan in 2004. Currently he is perusing his Ph.D from University of Malakand Pakistan and also works as Assistant Professor in the Deptt: of Computer Science in the same Institute. His current research interests include Software Outsourcing and network security.