International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

A Novel Approach on Encryption and Decryption of 5X5 Playfair Cipher Algorithm

V. Subhashini[1], Dr.N.Geethanjali[2],P.Vidyasagar[3],P.Amrutha[4]
[1]Research Scholar, Department of Computer Science & Technology
Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India.
subhashinivardhan@gmail.com
[2]Professor, Department of Computer Science & Technology
Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India
geethanjali.sku@gmail.com
[3]Associate Professor, Dept. of Information Technology
V.R.Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India.
p.vidyasagar@gmail.com
[4]Research Scholar, Department of Computer Science & Technology
Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India.
p.amruthachowdary@gmail.com

ABSTRACT: Cryptography is the study of Secret (crypto-)-Writing (-graphy). Cryptography is about communication in the presence of an adversary. It is a symbol of art and science to convert the original message into decoded form. It is classified into two types to convert the data. One is Transposition technique and other is Substitution technique. Today's cryptography is more than encryption and decryption not even the large number of keys in a monoalphabetic cipher provides security. This Paper will present a perspective on combination of Playfair techniques. The playfair cipher is to approach for improving security was to encrypt multiple letters. It is based on 5 X 5 matrix of letters and constructed with a keyword. Playfair is a substitution cipher text. Playfair cipher was originally developed by Charles Wheatstone in 1854 but it be named of Lord Playfair because he promoted the use of this method. A modified version MXM of 5X5 playfair cipher is introduced which enable the user to encrypt and decrypt message for any square matrix. A special case of algorithm is discussed where "X" is used for repeating letters. The play fair cipher is introduced as the first digraph cipher. The special rules for encoding are introduced.

Keywords: Cryptography, Keys, Digraphs, Encryption, Decryption, Cryptanalysis

I. INTRODUCTION:

Cryptography has become an essential tool in transmission of information. Cryptography is the central part of several fields: information security and related issues, particularly, authentication, and access control. Cryptography encompasses a large number of algorithms which are used in building secure applications. Cryptography is the study of Secret (crypto-)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances.

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures.

Cryptographic systems are generally classified along three independent dimensions:

a. Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.
b. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.
c. The way in which the plaintext is processed: A block cipher processes the input on block of elements 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.

II. PLAYFAIR CIPHER:

The best- known multiple letter encryption cipher is the Playfair, which creates diagrams in the plaintext as single units and translates these units into cipher text diagrams.

The playfair algorithm is based on the use of 5 X 5 matrix of letters constructed using a keyword. 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.

III. EXISTING PLAYFAIR ALGORITHM USING 5 X 5 MATRIX:

The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose "DIGITAL LIBRARY" as the secret keyword the matrix is given in Table 1.

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

So, the Using the word "DIGITAL LIBRARY", we get the following code

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

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

So using the Keyword "DIGITAL LIBRARY" the word "COMMUNICATE" can be decoded as follows

CO MX UN IC AT EX

GK FW SH YG DQ AW

IV. LIMITATIONS OF PLAYFAIR CIPHER:

The main drawback of the traditional Play fair cipher is that the plain text can consist of 25 uppercase letters only. One letter has to be omitted and cannot be reconstructed after decryption. Also lowercase letters, white space, numbers and other printable characters cannot be handled by the traditional cipher. This means that complete sentences cannot be handled by this cipher. Space between two words in the plaintext is not considered as one character. 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. In a mono alphabetic cipher the attacker has to search in 26 letters only. Play fair cipher being a polyalphabetic cipher the attacker has to search in 26 x 26 = 676 diagrams. Although the frequency analysis is much more difficult than in mono alphabetic cipher still using modern computational techniques the attacker can decipher the cipher text. So performing double substitution and transposition on play fair cipher will considerably increases its security.

V. RULES:

A. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do.

B. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).

C. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

D. If the letters are not on the same row or column, replace them with the letters on

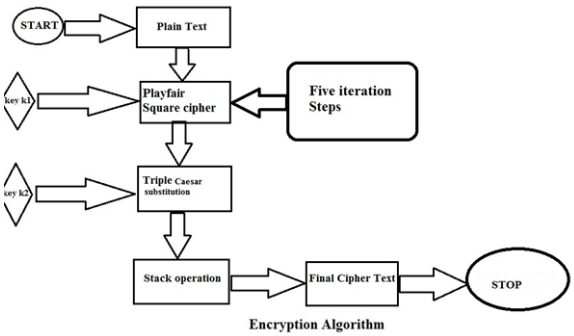
the same row respectively but at the other pair of corners of the rectangle defined

by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s, or "Q"s that do not make sense in the final message when finished).

VI. PROPOSED WORK:

A. Block diagram for Encryption Algorithm



Encryption Algorithm

Plaintext: This is what you want to encrypt

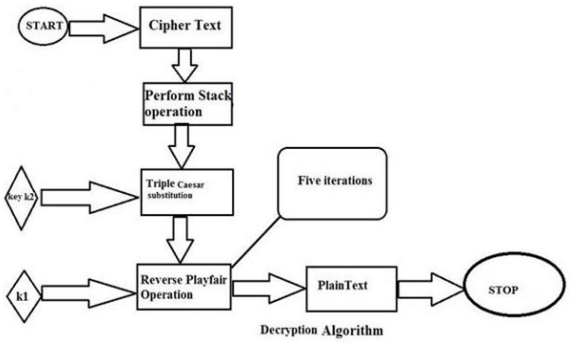
Cipher text: The encrypted output

Enciphering or Encryption: The process by which plaintext is converted into cipher text using five iteration steps. The plaintext can be converted using five iteration steps. The Triple Caesar substitution can be done using stack operations.

Encryption algorithm: The sequence of data processing steps that go into transforming plaintext into cipher text. Various parameters used by an encryption algorithm are derived from a secret key. In cryptography for commercial and other civilian applications, the encryption and decryption algorithms are made public.

Key: A key is used to set some or all of the various parameters used by the encryption algorithm. The important thing to note is that, in classical cryptography, the same secret key is used for encryption and decryption. It is for this reason that classical cryptography is also referred to as symmetric key cryptography.

B.Block diagram for decryption Algorithm



Decryption Algorithm

Deciphering or Decryption: Recovering plaintext from cipher text. Again the cipher text is converted into plain text by using the same five iterations.

Decryption algorithm: The sequence of data processing steps that go into transforming cipher text back into plaintext. In classical cryptography, the various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm.

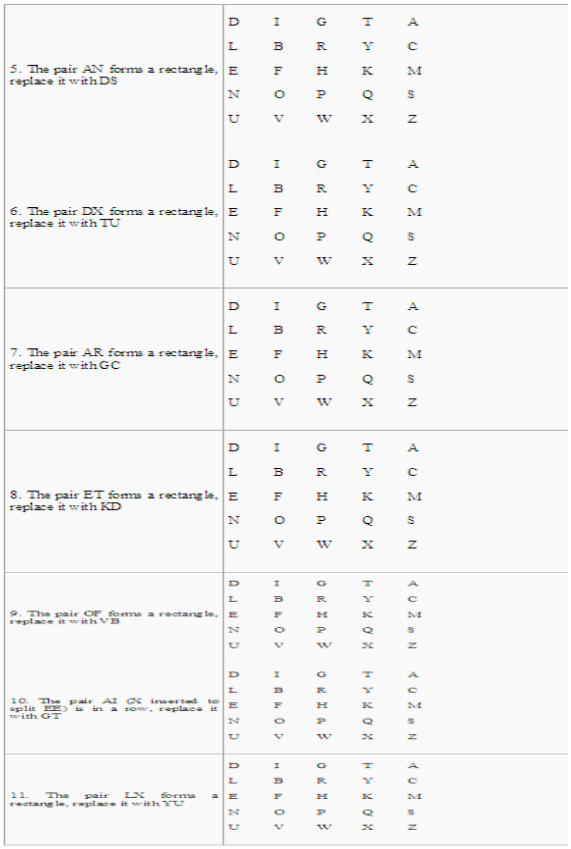
The explanation of proposed play fair algorithm is done in the following example:

Example:

Using "Digital Library" as the key (assuming that I and J are interchangeable), now the sentences are encrypted.
Encrypting the message "DREAM BIG AND DARE TO FAIL" (note the null "X" used to separate the repeated letters

DR EA MB IG AN DX AR ET OF AI LX

1. The pair DR forms a rectangle, replace it with GL	D	I	G	T	A
	L	B	R	Y	C
	E	F	H	K	M
	N	O	P	Q	S
	U	V	W	X	Z
2. The pair EA is in a column, replace it with MD	D	I	G	T	A
	L	B	R	Y	C
	E	F	H	K	M
	N	O	P	Q	S
	U	V	W	X	Z
3. The pair MB forms a rectangle, replace it with FC	D	I	G	T	A
	L	B	R	Y	C
	E	F	H	K	M
	N	O	P	Q	S
	U	V	W	X	Z
4. The pair IG forms a rectangle, replace it with DT	D	I	G	T	A
	L	B	R	Y	C
	E	F	H	K	M
	N	O	P	Q	S
	U	V	W	X	Z



IL MD FC DT DS TU GC KD VB GT YU

Thus the message "DREAM BIG AND DARE TO FAIL "becomes "ILMDFCDTDSTUGCKDVBGTYU". (Breaks included for ease of reading the cipher text.)

VII. CONCLUSION:

A. In this paper we have analyzed the merits and demerits of the original Playfair cipher. We then looked at the variations that have been proposed. Then we discussed the modified Playfair cipher which we proposed. By doing cryptanalysis we showed that this modified cipher is stronger than the original Playfair cipher.

B. If we take small letters, capital letters, numerical and other printable characters as four different groups. The sequence of the groups can change to any matrix with the same keyword. This should make cryptanalysis more difficult. This can be tried out and the results can be analyzed.

REFERENCES:

[1] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition 2007, Tata McGraw- Hill Publishing Company Limited, New Delhi.

[2] Wikipedia (http://en.wikipedia.org/wiki/Playfair_cipher)

[3] William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Pearson Education.

[4] Atul Kahate, Cryptography and Network Security, 2nd Ed., Tata McGraw-Hill Publishing Company Limited, New Delhi.

[5] 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.

[6] Shiv Shakti Srivastava, Nitin Gupta "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011

[7] Gaurav Agrawal, Saurabh Singh, Manu Agarwal "An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text", Journal of Current Computer Science and Technology Vol. 1 Issue 3 [2011]10-16

[8] Packirisamy Murali and Gandhidoss Senthilkumar "Modified Version of Playfair Cipher using Linear Feedback Shift Register", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[9] Harinandan Tunga, Soumen Mukherjee "A New Modified Playfair Algorithm Based On Frequency Analysis", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

[10] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani "A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009 1793-8201

[11]William Stalling"Network Security Essentials (Applications and Standards)", Pearson Education, 2004

[12] practicalcryptography.com/ciphers/rail-fence-cipher/ [6] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education.

[13].T. Bass, "Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness", Communications of the ACM, vol. 43, no. 4, (2002), pp. 99-105

[14] B. D'Ambrosio, M. Takikawa, D. Upper, et al., "Security situation assessment and response evaluation (SSARE)", In: Proceedings of the DARPA Information Survivability Conference & Exposition II, Los Alamitos, America: IEEE Computer Society, (2001), pp. 387-394.

[15] X. Chen, Q. Zheng and X. Guan, "Evaluation method of quantitative hierarchical network security threat situation", Journal of software, vol. 17, no. 4, (2006), pp. 885-897.

[16]] Y. Liang, H. Wang and J. Lai, "A method of network security situation awareness based on Rough Set Theory", Computer science, vol. 34, no. 8, (2007), pp. 95-97.

[17] H. Xiao, "Analysis and Research on the network security situation assessment and the trend of perception: [PhD thesis]", Shanghai: Shanghai Jiao Tong University School of Electronic Engineering, (2007), pp. 89- 98.

[18] Y. Wei, Y. Lian and D. Feng, "Network security situation assessment model based on information fusion", Research and development of computer, vol. 46, no. 3, (2009), pp. 353-362.

[19]. Cryptography and network Security byBehrouz A. Forouzon, Tata McGrawHill.

[20].Information Security Intelligence: Cryptographic Principles and Applications by Calabrese, Thomson India Edition