An Extended Version of Four-Square Cipher using 10 X 10 Matrixes

J. Aishwarya
Research Scholar
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India

V. Palanisamy
Professor & Head
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India

K. Kanagaram
Research Scholor
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India

ABSTRACT
Now-a-days web based attacks is an issue in the internet data transmission. Many cryptographic algorithms are developed to secure the data over the communication. The existing algorithm uses alphabets only. In this paper, we proposed an algorithm which uses an innovative Cryptographic Digraph Substitution method to provide a stronger cipher for the network security. The proposed method uses 10x10 matrices that extended to lowercase, symbols and ASCII values. Hence our algorithm is more secure where the intruders could not able to suspect the data.

Keywords
Four-square cipher, Substitution, Digraph, Encryption, Decryption

1. INTRODUCTION
In age of universal electronic connectivity, of viruses and hackers, of electronic fraud, there is indeed no time at which security is not concerned so far. The explosive growth in computer systems and their interconnection via network has increased the dependence of both organizations and individuals. The information stored and communicated using these systems which in turn has led to a sensitive 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 [Jitendra Choudhary].

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable [1]. The key generation for cryptography is divided in to two parts namely, Symmetric Key Encryption and Asymmetric Key Encryption. In symmetric type both sender and receiver shares the same key. In Asymmetric both sender and receiver have pair of key i.e. Public and Private Key [2].

The public key is shared by sender and receiver. Private Key could possible like this and cannot be shared by the sender and receiver. Sender encrypt the message using receiver's public key and receiver decrypt the message with their private key. Basically cryptographic algorithms classified into Monoalphabetic Substitution Ciphers, Transposition Ciphers, Polyalphabetic Substitution Ciphers, Digraph Substitution Ciphers. One of the Digraph Substitution Ciphers classified in to playfair cipher, two square cipher, four square cipher, and hill cipher algorithms [3].

Already lots of researcher have worked on all the methods. But four square ciphers extended very rare so here we are talking extended version of four square ciphers, which remains to implemented very easy and flexible. The four-square cipher is a manual symmetric encryption technique. It was invented by the famous French cryptographer Felix Delastelle [4]. The technique encrypts pairs of letters (digraphs), and thus falls into a category of ciphers known as polygraphic substitution ciphers. The three goals of security – confidentiality, integrity and availability can be threatened by security attacks.

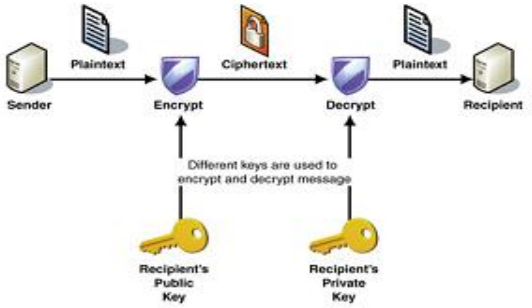

Fig 1. Basic Encryption and Decryption Process

The rest of the paper is constructed as follows. Section 2 brings out the related work on the same research area. Section 3 consists of the basic four square cipher algorithms which are now extended. Section 4 comprises of our proposed 10 X 10 matrixes. Section 5 comes out with the experimental results and conclusion for the proposed area.

2. LITERATURE SURVEY

Ravindra Babu K, S. Uday Kumar, A. Vinay Babu ,I.V.N.S Aditya, P. Komuraiah shows an extension to the traditional playfair cryptographic method. In their discussion they suggests about the existing play fair algorithm, its merits and demerits. The existing play fair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. Their enhanced algorithm, the existing algorithm, uses that a 6 X 6 matrix [8].

Gaurav Shrivastava, Manoj Chouhan, Manoj Dhawan proposes a modified version of extended play fair cipher with 8 X 8 matrixes. The work, made use of a Simple Columnar Transposition Technique with Multiple Rounds in 8X8 Playfair Cipher Substitution Technique and arranged a special symbol by overall Character Frequency Analysis (CFA) [4].

Gulshan Soni, Umesh Gupta,,Nikhil Singh they present some new approach for security enhancement of well known classical substitution cipher (Playfair and Hill cipher). Some drawback inherent the 5x5 Playfair cipher which adversely affect the security of this cipher and also Hill Cipher that succumbs to the known-plaintext attack. Their proposed work focuses on modification that can enhance the security level of these classical encryption techniques so these can resist for different cryptanalysis attacks [5].

Attackers use various methods to discover the encryption key, plaintext to cipher text conversion, cipher identification. According to Tunga& Mukherjee and Schneier frequency analysis have been used to break key encryption initiatives such as Vigenere ciphers. Also, Stallings confirmed an attempt was made on DES and Blowfish by pattern recognition. Neural Networks have uncovered some stream ciphers and enhanced RC6 [11, 13].

Ravindra et.al made survey on types of ciphers in which, Block ciphers and stream ciphers are the two types of symmetric algorithms that are used for encryption. The block ciphers are excelling in their performance in hardware as well as software environment where as the stream cipher is used in secure communication for high throughput. That is used for encryption [9].

Encryption is the process of transforming the information to ensure the security. With the huge growth of networks and advantages in the communication technology, huge amount of data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [10].

Vidyasagar Potdar, Elizabeth Chang in their paper proposed the technique to encrypt the text and made it hidden and evaluated the various security issues that are raised [12]. In the paper Cryptographic Algorithms for Secure Data Communication, by Zirra Peter Buba and Gregory Maksha Wajiga the asymmetric keys and its performance efficiency, key scheduling is discussed [14].

3. BASIC FOUR SQUARE CIPHER

The four-square cipher is a manual symmetric encryption technique. It was invented by the famous French cryptographer Felix Delastelle. The four-square cipher uses four 5 by 5 (5x5) matrices arranged in a square. Each of the 5 by 5 matrices contains the letters of the alphabet (usually omitting "Q" or putting both "I" and "J" in the same location to reduce the alphabet to fit).

In general, the upper-left and lower-right matrices are the "plaintext squares" and each contain a standard alphabet. The upper-right and lower-left squares are the "cipher text squares" and contain a mixed alphabetic sequence. To generate the cipher text squares, one would first fill in the spaces in the matrix with the letters of a keyword or phrase (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (again omitting "Q" to reduce the alphabet to fit).

The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitutes the cipher key. The four-square algorithm allows for two separate keys, one for each of the two cipher text matrices [5].

3.1 Procedure for Encryption and Decryption

Break up the plaintext into bigrams i.e. ATTACK AT DAWN → AT TA CK AT DA WN. An 'X' (or some other character) may have to be appended to ensure the plaintext is an even length.

Using the four 'squares', two plain alphabet squares and two cipher alphabet squares, locate the bigram to encrypt in the plain alphabet squares. The example below enciphers the bigram 'AT'. The first letter is located from the top left square, the second letter is located in the bottom right square.

```
a b c d e    Z G P T F
f g h i k    O I H M U
l m n o p    W D R C N
q r s t u    Y K E Q A
v w x y z    X V S B L

M F N B D    a b c d e
C R H S A    f g h i k
X Y O G V    l m n o p
I T U E W    q r s t u
L Q Z K P    v w x y z
```

1. Locate the characters in the cipher text at the corners of the rectangle that the letters 'AT' make:

```
a b c d e   Z G P T F
f g h i k   O I H M U
l m n o p   W D R C N
q r s t u   Y K E Q A
v w x y z   X V S B L

M F N B D   a b c d e
C R H S A   f g h i k
X Y O G V   l m n o p
I T U E W   q r s t u
L Q Z K P   v w x y z
```

2. Using the above keys, the bigram 'AT' is encrypted to 'TI'. The text 'attack at dawn', with the keys, becomes as

zgptfoihmuwdrcnykeqaxysbl and 'mfnbdcrhsaxyogvituewlqzkp', as

ATTACKATDAWN
TIYBFHTIZBSY

4. PROPOSED WORK

In the extended version of Four Square Cipher method we use 10 x 10 matrixes to generate cipher text. This algorithm can accept the Plaintext containing Alphabets (capital letters and small letters), Numbers and Special characters. So the user can easily encrypt combination of alphabets, numbers and characters efficiently. And we are not omitting "q" in our proposed work because 10 x 10 matrixes can adopt up to 64 characters. In proposed work cipher text contain mixture of alpha numeric characters and some special characters. For Ex: UNIVERSITY is spliced as UN IV ER SI TY.

4.1 Encryption algorithm

The encryption of the text involves the following steps split the user given payload message into digraphs. For Ex: UNIVERSITY is spliced as UN IV ER SI TY.

Step 1: Find out the first letter of the message in the provided plaintext, at Upper-left 10 X 10 matrixes as follows:

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é â
```

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

Step 2: Find the associated second letter in the digraph placed at lower – right plain text matrix.

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

Step 3: The first letter of the encrypted digraph is in the same row as the first plaintext letter and the same column as the second plaintext letter. It is therefore in the upper-right cipher text matrix.

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ `space = @ Ç ü é ä
```

Step 4: The first letter of the encrypted digraph is in the same row as the first plaintext letter and the same column as the second plaintext letter. It is therefore in the upper-right cipher text matrix.

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~`space = @ Ç ü éä
```

Step 5: Here is the four-square cipher written out again but blanking all of the values that aren't used for encrypting the first digraph "UN" into "y-"

```
! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ `space = @ Ç ü é ää
```

```
  ! " # $ % & ' ( ) *    A B C D E F G H I J
+ , - . / 0 1 2 3 4    K L M N O P Q R S T
5 6 7 8 9 : ; < = >    U V W X Y Z a b c d
? @ A B C D E F G H    e f g h I j k l m n
I J K L M N O P Q R    o p q r s t u v w x
S T U V W X Y Z [ \    y w x y z 0 1 2 3 4
] ^ _ ` a b c d e f    5 6 7 8 9 , . < ? >
g h I j k l m n o p    / " : ; ' { } + ) [
q r s t u v w x y z    ( & ] | \ ^ ! # $ %
{ | } ~ Ç ü é â ä Space ~ ` space = @ Ç ü é ä
```

The given plain text is “UNIVERSITY”; the encrypted cipher text is “yN'X} _.N4Y”.

As can be seen clearly, the method of encryption simply involves finding the other two corners of a rectangle defined by the two letters in the plaintext digraph. The encrypted digraph is simply the letters at the other two corners, with the upper-right letter coming first.

4.2 Decryption algorithm

Decryption works the same way, but in reverse. The cipher text digraph is split with the first character going into the upper-right matrix and the second character going into the lower-left matrix. The other corners of the rectangle are then located. These represent the plaintext digraph with the upper-left matrix component coming first.

Examples

Plain Text : Department of Computer Science

Engg, Alagappa University, karaikudi”

Cipher text : gH1B0XäQ

U, e"UE$) U1V5F, cyC+E) J|jfS#MJ

cdO'C, V|f4Q(Y~`/O5ZON~ [ÇQ'[ÇT

5. CONCLUSION

The Proposed Algorithm works better than existing 8 x 8 matrices. It improves the security, by means of increasing complexity to hack the original text. This algorithm uses different types of keys for the Four-square encryption process. The Keys are used to alter the plaintext when symmetric key cryptosystem, it enhances the 5x5 matrix into augmented format of 10x10 matrixes. In future, the 10x10 matrix is implemented into 16x16 matrixes to improve their security in more secured way.

6. REFERENCES

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

[2] Behrouz A. Forouzan, “Data Communications and Networking”, 4th ed., McGraw-Hills, 2006. Tunga1, H., Mukherjee, S. (2012),

[3] “*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.

[4] Gaurav Shrivastava, Manoj Chauhan, Manoj Dhawan, *“A Modified Version Of Extended Plafair Cipher (8x8)*”, in International Journal of Engineering and Computer Science, Vol2, Issue 4, April 2013, pp: 956-961.

[5] Gulshan Soni, Umesh Gupta, Nikhil Singh, “Analysis *of Modified Substitution Encryption Techniques*”, PP: 643-647.

[6] Hans Delfs and Helmut Knebl, “Introduction to Cryptography: Principles and Applications”, Springer International Edition.

[7] Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh, “A Survey of Existing Playfair Ciphers”, International Journal of Engineering and Advanced Technology”, Vol 2, issue 4.

[8] Ravindra Babu Kallam, Dr. S.Udaya Kumar, Dr. A.Vinaya Babuushi, “A New Framework for Scalable Secure Block Cipher Generation using Color Substitution and Permutation on Characters, Numbers, Images and Diagrams”. International Journal of Computer Applications (0975 – 8887) vol. 20, no. 5, April 2011

[9] Ravindra, K., Kumar, S. , Vinay A.,Aditya V.S., Komuraiah P. (2011),An Extension to Traditional Playfair Cryptographic Method, International Journal of Computer Applications Ravindra, K., Kumar, S. , Vinay A.,Aditya V.S., Komuraiah P. (2011),An Extension to Traditional Playfair Cryptographic Method, International Journal of Computer Applications (0975 –8887),Vol.17 No.5,March 2011.

[10] M. Sonka, V. Hlavac. And R. Boyle, "*Digital image processing," in: image Processing, Analysis, and Machine Vision*, 1998, 2nd Ed.

[11] Tunga1, H., Mukherjee, S. (2012)," *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 .

[12] V.Potdar and E.chang, "*Disguising text cryptography using Image cryptography*", International Network Conference in plumouth, UK, 6-9, July, 2004.

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

[14] Zirra Peter Buba & Gregory Maksha Wajiga "*Cryptographic Algorithms for Secure Data Communication",* International "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.