Modified 3-D Playfair Stream Cipher

Sagar Gurnani
Computer Dept., VESIT
Mumbai-74, India.

Nitish Mhalgi
Computer Dept., VESIT
Mumbai-74, India.

Samyukta Iyer
Computer Dept., VESIT
Mumbai-74, India.

Deepika Dixit
Computer Dept., VESIT
Mumbai-74,India.

ABSTRACT
The purpose of this algorithm is to offer heightened security for data transmission. The data may include any alphabet, numerals, or special characters. This work proposes an improved version of a 3-D Playfair cipher, by improving the complexity of encryption and decryption. The algorithm uses a 5x5 key matrix for encoding, which not only increases the complexity by providing each character with three-dimensional uniqueness, but also eliminates the idea of dummy characters required in other versions of this cipher. One can consider various types of cryptography attacks and comparisons of the resistance offered by the proposed algorithm with the resistance offered by existing algorithms to judge its practicality.

General Terms
Cipher, Playfair, Security

Keywords
Playfair, Cipher, Security, 3D, Cube

1. INTRODUCTION
William Stallings, in his book 'Cryptography and Network Security', has defined a 'cipher' as "an algorithm for performing encryption or decryption of information—a series of well-defined steps that can be followed as a procedure". The operation of a cipher usually depends on a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be extremely difficult, if not impossible, to decrypt the resulting cipher text into readable plaintext. [1]

2. BLOCK CIPHERS AND STREAM CIPHERS
Block ciphers encrypt a group of plain text symbols as one block. They work on blocks of plain text and produce blocks of cipher text.

Stream ciphers represent a different approach to symmetric encryption from block ciphers. Rob Shaw, in a technical report for RSA Laboratories in 1991, has provided a precise description of how stream ciphers work. Stream ciphers convert one symbol of plaintext immediately into a symbol or group of symbols of cipher text. The algorithms operate on each character. In a stream cipher, each plain text character is encrypted one at a time with the corresponding symbol of the key stream, to give a character of the cipher text stream. [2]

3. TWO-DIMENSIONAL PLAYFAIR CIPHER
3.1 Working of 2D Playfair Cipher
2D Playfair cipher is a key substitution and block cipher. Each block comprises of 2 characters. Using the key, a table is created. This table is a 5x5 matrix- i.e. it can store 25 characters. But we have 26 alphabets that we need to be able to encrypt. So, we write 2 alphabets in one cell (for example: 'i' and 'j' are conventionally placed in one cell of the table) or we skip the letter 'q'. The table is first filled with the letters in the key, without repeating alphabets. The remaining cells are then filled with alphabets not covered in key, starting from a to z and in order. Plain text is divided into blocks of 2 characters, and each pair is then encrypted using the table and following rules:

- If two letters (characters) fall in same row, then they are replaced with their respective next letters circularly following the last.
- If the two letters fall in same column, then they are replaced with their respective next letter (below it) circularly following to the top.
- If the two letters lie neither in same row nor in same column, then find the intersection of row of one and column of other and replace it with letter at intersection.

3.2 An Example
Plain text: balloon

Key: monarchy

	0	1	2	3	4
0	m	o	n	a	r
1	c	h	y	b	d
2	e	f	g	i/j	k
3	l	p	q	s	t
4	u	v	w	x	z

Figure 1: 2D matrix (5x5)

Plaintext is divided into blocks: ba lx lo on

Since the same letter appears twice in a block, 'x' is inserted between the two 'l's: ba lx lo on

Encrypting the first block (ba): replace 'b' with 'i' and replace 'a' with 'b'.

Encrypting the second block (lx): replace 'l' with's' and replace 'x' with 'u'.

Encrypting the third block (lo): replace 'l' with 'p' and replace 'o' with 'm'.

Encrypting the fourth block (on): replace 'o' with 'n' and replace 'n' with 'a'.

Cipher text: ib su pm na

4. 3D PLAYFAIR CIPHER
In the paper titled '3D(4 X 4 X 4) - Playfair Cipher' the authors (Kaur,Verma & Singh) proposed a 3D-Playfair Cipher

(4 X 4 X 4 Playfair cipher) which works on a trigraph rather than using a digraph, as in the 2D Playfair cipher. 3D-Playfair cipher supports all 26 alphabets {A-Z}, 10 digits {0-9} and 28 special characters { ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ | } which eliminate the limitation of classical Playfair where "i" and "j" both character cannot appear at the same time. 3D-Playfair enhances the security by increasing complexity. [3]

4.1 Modification of 3-D Play Fair Cipher

The 3-D Play Fair involves using the 4x4x4 cube introduced above, accommodating the alphabet (26), digits (0-9) and special symbols (28), and making in all 64 unique characters to occupy each cell of the cube.

It also includes using the 5x5 matrix, known for its usage in the 2-D Playfair cipher, for the purpose of encoding the characters in the 4x4x4 cube with the help of a secret key.

Steps:

- Construct an arbitrary 4x4x4 cube with 64 characters as mentioned above. Construct a 5x5 Playfair matrix using a secret key.
- Attach one copy of this 5x5 matrix to each/one pair of opposite faces of the cube as shown.
- Locate plain text character in the cube and encode it with 3 characters, one each from the three 5x5 matrices that correspond to the plain text character's co-ordinates. The order to obtain the cipher text characters is assumed to be from the 5x5 matrix affixed to the length face, breadth face and finally, the height face of the cube.

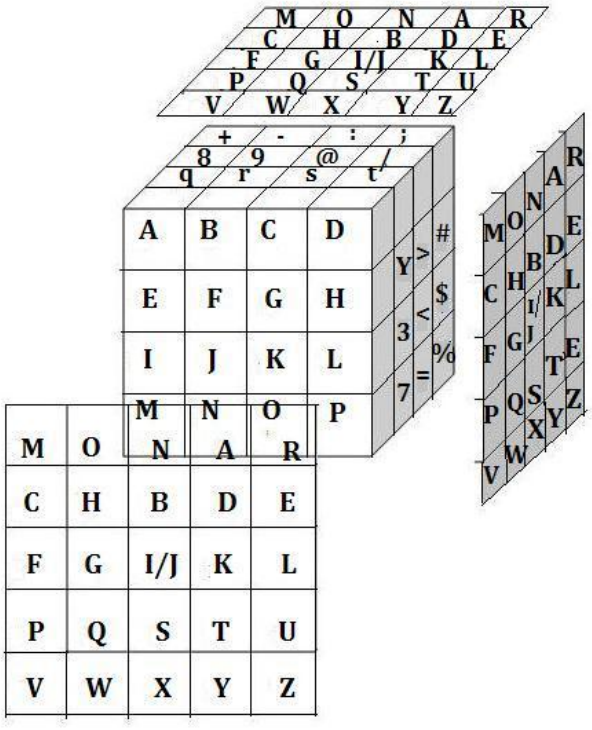

Figure 2: 3D cube with 5x5 matrices on each dimension

5. ENCRYPTION

Thus, this encryption technique discards the block cipher philosophy and follows the stream cipher technique. Each plain-text is independently encoded as and when the input is read. Here, one plain text character is replaced by 3 cipher text characters. This eliminates the use of dummy characters used in block ciphers to complete blocks.

The increased size of cipher text also aims to increase the confusion (making the statistical relation between plaintext and cipher text as complex as possible) and to increase the complexity of decryption by a factor of three. Also, superimposing the 5x5 matrix over a 4x4 face of the cube will render one of its rows and columns as non-usable. Instead of it being a redundancy, it can be used to create uncertainty as to which characters don't appear in the final cipher from that 5x5 matrix.

6. DECRYPTION

The fixed order (length, breadth, height) used to encrypt the plain text is followed as it is for decryption. The intersection of extrapolations of cipher text characters from the 5x5 matrices of all three dimensions will point to a unique character inside the 4x4x4 cube.

Again, the change of philosophy from block to stream ensures that there is no ambiguity in decryption since there are no dummy characters and no additional complexities due to repeating characters.

7. ADVANTAGES AND LIMITATIONS

7.1 Advantages

- No concept of dummy characters and no extra handling for repeating characters.
- Increased complexity by providing each character with three-dimensional uniqueness.
- Technique can be made more robust by initializing the three 5x5 matrices with different secret keys.
- Highly scalable to adopt more characters and improve support from 64 characters to 125 characters.
- Better resistance to brute force attack as each character could possibly be encoded in 64x25x25x25 = 1,000,000 ways (25x25x25= 15625 ways if cube configuration is fixed and not secret).

7.2. Limitations

- Tradeoff between complexity and throughput.
- Three cipher text characters required for one plain text character. But then, encoding techniques have long accepted this limitation. Recurring patterns can indicate higher probability of some characters in a certain language. This technique is called Frequency Analysis. It can be a potential vulnerability.

8. CONCLUSION

Modified 3-D PlayFair Stream Cipher is a three-dimensional encryption technique, which attempts to increase the complexity of encryption significantly, while also doing away with some of the limitations of the existing play-fair ciphers. It uses a 5x5 key matrix to be imposed on a 4x4x4 cube, which ends up increasing the complexity by a factor of three. No separate handling is required for repeating characters, which is not the case with other existing Playfair cipher. This

algorithm is resistant to security attacks as each character can be encoded in 1,000,000 different ways.

9. REFERENCES

[1] William Stallings, Cryptography and Network Security, principles and practices, 4th Edition.

[2] Reference: Matt J. B. Rob Shaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995.

[3] Amandeep Kaur, Harsh Kumar Verma and Ravindra Kumar Singh. Article: 3D(4 X 4 X 4) - Playfair Cipher. *International Journal of Computer Applications* 51(2):36-38, August 2012.