**Playfair Cipher**

***Abstract*- Playfair cipher is the most popular polyalphabetic cipher. It is a form of block cipher which has no limit on the number of characters in a message it can do, but it operates on block of characters encrypting two characters at a time cipher. In this, the plain text digrams are converted to cipher text digrams(pairs of letters) and vice versa using a pre-shared key. This is achieved by performing several operations column wise row wise and by creating rectangular form. The traditional 5 x 5 Playfair cipher supports twenty- five uppercase alphabets.**

**History:**

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher. It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment. A typical scenario for Playfair use would be to protect important but non-critical secrets during actual combat. By the time the enemy cryptanalysts could break the message the information was useless to them.

**Description:**

In traditional Playfair the position of I=J are incorporated into one square since English alphabets consist of 26 letters but in Playfair a matrix of 5X5 grid(also known as key-square) is made that is twenty five letters can only be embedded including keyword. For instance, if we select **puzzle** as the confidential keyword the matrix is as shown

P U Z L E

A B C D F

G H I K M

N O Q R S

T V W X Y

Then the message is wrecked up into digraphs or groups of two letters.If there is an odd number of letters, a Z is added to the last letter. Each letter can only be used once so further use of a letter is ignored leftover spaces are filled with the rest of the letters of the alphabet.The substitution occurs depending on the following three principles.

1. Just in case both the letters are in the same row, replace them with the letter on the right of the letter. If the letter is at the start, go to the next letter.
2. Just in case both the letters are in the same column, replace them with the letter below them. If the letter is at the top, go to the bottom of the column and use the letter to replace with top letter.
3. If neither of the alphabets lies in the same column nor same row, imagine creating a rectangle form and write the corners alphabets.

As an example, consider **puzzle** as the keyword and **ballon** as the plain text. Since ballon has repeating characters the letter X is inserted between the two repeated letters. So, the final digraphs are **BA LX LO NX.**

* For the primary digraph B and A square measures **within the same row**. According to rule one it is encrypted to BC.
* Next LX lies within the **same column** and hence gives DL on applying rule two.
* Consequent digraph is LO and that is **neither within the same row or column**. Applying rule 3 gives UR
* Now the last diagram is NX and it **neither lies in the identical row** nor in the same column and is encrypted to RT.

So the cipher text is **BCDLURRT**.

**Cryptoanalysis:**

The playfair cipher is more complicated than a substitution cipher.It is significantly harder to break since the frequency analysis technique used to break simple substitution ciphers is difficult but still can be used on (25\*25) = 625 digraphs rather than 25 monographs which is difficult. Frequency analysis thus requires more cipher text to crack the encryption.

An interesting weakness is the fact that a digraph in the ciphertext (AB) and it’s reverse (BA) will have corresponding plaintexts like UR and RU (and also ciphertext UR and RU will correspond to plaintext AB and BA, i.e. the substitution is self-inverse). That can easily be exploited with the aid of frequency analysis, if the language of the plaintext is known.