Abstract

The main purpose of our research is to provide security for the data that contains alphabets and integer values during the transmission, when data is transmitted from sender to receiver. As we know that playfair technique is best for multiple letter encryption, which treats the plain text as single units and translates these units into cipher text. It is highly difficult to the attacker to understand or to decrypt the cipher text. The existing playfair technique 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. But many algorithms have been proposed that allow text which contains alphabets, integers as well as special symbols using 6 * 6 matrix and 10 * 9 matrix etc. In playfair technique a group of 2 letters in the plain text is converted to cipher text during encryption using a key. Similarly on other hand during decryption cipher text are converted to
Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Caesar Cipher

plain text using the same key. Some time it may be possible for the attacker to understand the plaintext. To overcome this problem we proposed an algorithm that extends the security of playfair technique using excess 3 code and caesar cipher technique where first each alphabets and integer is converted into binary number and then its equivalent excess 3 code and after that with the help of key encryption process will be apply. In our proposed technique we are using 6 * 6 matrix which contain alphabets and integers only.

References

- Wikipedia (http://en.wikipedia.org/wiki/Playfair_cipher)
- C Nisarga Chand, Subhajit Bhattacharyya "A Novel Approach for Encryption of Text Messages Using PLAY -FAIR Cipher 6 by 6 Matrix with Four Iteration Steps";
- 10-16.

Index Terms

Computer Science
Security
Keywords

Playfair cipher  excess 3 code  ceasar cipher  Plaintext  cipher text  rectangular matrix  key
encryption
decryption
binary number.