Abstract

Protecting data from malicious attacks during storage and transmission is the reason for using encryption. Encryption can be achieved by two methods – Transposition and Substitution. Transposition refers to changing the order of characters in a given text. On the other hand, substitution is the process of replacing each character of the plaintext with some other character. Using a combination of transposition and substitution for encryption leads to greater security when compared to using either of them separately. Vigenère Cipher is a poly-alphabetic cipher. It is based on the substitution technique which uses multiple substitution alphabets. In this paper, we introduce double columnar transposition on Vigenère Cipher to enhance its security making cryptanalysis difficult.

References


**Index Terms**

Computer Science

Security

**Keywords**

Transposition, Substitution, Poly-Alphabetic Cipher, Double Columnar Transposition