Abstract

Cryptography is an art and science of converting original message into non-readable form. There are two techniques for converting data into non-readable form: 1) Transposition technique 2) Substitution technique. Transposition ciphers use the letters of the plaintext message, but they permute the order of the letters. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. In this Cryptography there is use of three aspects of Columnar Transposition; Single Transposition using ROT-13 applicable to message of the Algorithm, Double Transposition using Caesar Cipher in second round of an Algorithm and Triple Transposition were it combine both the concept and use reverse of the message in second round of the Algorithm.
Implementation of Cryptography Technique using Columnar Transposition

- Stamper, David, "Essential of Data Communication", Saratoga Group

Index Terms

Computer Science
Security

Keywords

Cryptography Substitution Transposition Rot-13 Caesar Cipher Columnar

Transposition
Shift Algorithm

Cipher Text

Plaintext

Encryption

Decryption.