Abstract

Cryptographic plays a significant role in the internet world. Cryptography comes from the Greek words "secret communication" in the presence of third parties. Cryptographic techniques are used to protect information like substitution and transposition. Caesar cipher is one of the simplest and most extensively known substitution techniques. In Caesar cipher each letter in the plaintext is replaced by a letter in some fixed number of positions down the alphabet. Zigzag cipher is a form of transposition cipher. It derives its name from the way in which it is encoded. In a Disrupted transposition cipher certain positions in a grid are blanked out, and not used when filling in the plaintext. This breaks up regular patterns and makes the cryptanalyst's job more difficult. Caesar Substitution Cipher, Zigzag Cipher and Disrupted Transposition Cipher Techniques are used independently then cipher text acquired is easy to break. To reduce the drawback of substitution and transposition techniques, in this paper we proposed combination of substitution and transposition techniques in order to provide to secure cipher text.
An Overview on Disrupted Transposition Cipher for Security Enhancement

1. William Stallings 2009 cryptography and network security
2. https://books.google.co.in/books?isbn=0486320316

Index Terms

Computer Science
Security

Keywords

Cryptography, Substitution, Transposition, Caesar Cipher, Zigzag Cipher, Disrupted Transposition Cipher, Cipher Text.