Abstract

This work proposes an improved scheme to encrypt the plain text message for its security. All the conventional encryption techniques are very weak and brute force attack and traditional cryptanalysis can be used to easily determine the plain text from encrypted text. In this work of encryption technique, a new concept of conventional ceaser cipher algorithm with hill cipher algorithm is used to make encryption technique more secure and stronger than the earlier concept. The plain text is encrypted in such a way that it becomes difficult to decrypt it. The proposed system is divided into two phases. In first phase, the plain text message is converted to first encrypted text using a new substitution approach which uses poly-alphabetic cipher technique. The encryption is done using variable length key which depends on the string length. In the second phase, the hill cipher technique is applied on the first encrypted text to produce new encrypted text or cipher text. At the receiver end, if the receiver has appropriate decryption key, he can generate the text message similar to the original message. This paper is organized into following sections. Section 1 contains a general introduction to the cryptography, types of cryptography and hill cipher. Section 2 contains literature review on some classical and modern text encryption techniques. Section 3 contains description of the
An Improved Cryptographic Technique to Encrypt Text using Double Encryption

proposed system. Finally paper is concluded in the Section 4.

References

- Amogh Mahapatra, Rajballav Dash "Data Encryption and Decryption by Using Hill Cipher Technique and Self Repetitive Matrix", in 2007.

Index Terms

Computer Science Security

Keywords

Cryptography Plaintext Ciphertext Hill Cipher