Abstract

It is unlikely any system can completely prevent unauthorized interception to transmission signal hence a more practical method that is traditionally employed for achieving privacy is to alter the message so only an authorized receiver can understand it. The method used to do this is termed encryption and decryption of information. By encrypting the massage before it is transmitted the message is unintelligible to everyone that receives it except the rightful recipient. The encryption/decryption methods process a message using an algorithm and a key. Transposition Cipher which shuffles characters around instead of substituting them with other characters is one way achieving privacy of data thereby assuring data owners of their data confidentiality. In this paper the Rubik’s cube a modified Rubik’s cube puzzle is employed at levels higher than 3×3×3 as a transposition cipher to encrypt data. Although no system is hundred percent secured the proposed algorithm sufficiently encrypt data with sufficient rotations of the cube.
A Proposed Enhanced Transposition Cipher Algorithm based on Rubik’s Cube Transformations

References

   https://www.tandfonline.com/doi/abs/10.1080/0161-119291866928
   ISBN: 0072822945

Index Terms

Computer Science       Security

Keywords

Encryption, Decryption, Transposition Cipher, Algorithm, Rubik’s Cube, Character Level Encryption.