Abstract

Communication is a basic process of exchanging information. Information security is a very important aspect now a day. The introduction of internet and distributed system made the information security issue more challenging and complex. Cryptography plays a crucial role in providing security to data transmitted over the internetwork. Encryption is the most widely used
technique used to scramble the data that is being transmitted over the network from sender to a receiver. The encryption algorithms are available practically and provide the security for user data and information. This paper presents an advanced encryption technique which combines the features of substitution and transposition. Five different key values being used in this algorithms and each key value is used to substitute the corresponding plaintext characters in association with addition operation. Each key value is twice as that of the previous one. The basic key value is a fixed one defined by the user. The transposition technique is employed by left shifting each bit of the data. The shifted data is complemented to alter the each bit of the cipher text that is being generated. The effort of the algorithm is to make the cryptanalysis difficult and to make the algorithm stronger.

Reference

- A block cipher having a key on one side of plaintext Matrix and its Inverse on the other side. Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani .

Index Terms

Computer Science

Security

Key words

Information Security

Plaintext

Ciphertext

Key

Cipher

Substitution
Transposition