Abstract

The most important issue for every organization is nothing but security. This paper deals with the confidentiality of electronic data which is transmitted over the internet. To ensure security we are cryptography. “Cryptography” is the process of converting readable format of text to unreadable format of text. This is mainly used for secured communication. Many ciphers have been developed to provide security. Out of these techniques we considered five cipher techniques those are “Caesar Cipher, Mono alphabetic Cipher, Poly alphabetic Cipher, Row Transposition Technique, and Rail fence Techniques”. The main objective of this proposed system is to combine the functionality of these five techniques to overcome the disadvantages of these techniques and to form a new hybrid technique named as “Classical Hybrid Encryption Substitution and Transposition Techniques” which can provide a good security when compared to techniques.

This method uses two stages of encryption. In the first stage Substitution techniques – Mono alphabetic, Caesar cipher, poly alphabetic cipher are used to generate partial cipher text. The
key for Caesar cipher and poly alphabetic technique is generated randomly by using Multiplicative linear congruential generator (Random number generation technique). In the second stage of Encryption Technique Transposition methods – Row Transposition and Rail fence Techniques are used to generate final cipher text.

This algorithm provides $91!$ of key space and in addition of that this encryption technique is multistage with each stage uses different key. Through this technique we will achieve good security against Brute-Force Attack and Cryptanalysis.

References

5. Prof.K.Govinda, Dr.E. satihamoorth – “Multileve I Cryptography Technique using Graceful codes” –JGRCS, Volume 2, No.7, July 2011
8. Packirisamy Murali and Gandhi doss Senthil Kumar-“Modified Version of Playfair cipher using Linear feedback Shift Register “-IJCNS, vol.8, No.12, December 2008

Index Terms

Computer Science Security

Keywords
Cryptography, C, Decryption, Ciphers, Multiplicative linear Congruential Generator, Key space, Brute-Force Attack, Cryptanalysis