Abstract

This paper deals with the tidings of cryptography in history, how it has played a vital role in World War -1, World War-2. It also deals with the Substitution, Transposition Cryptographic techniques and Steganography principles which can be used to maintain the confidentiality of computerized and none computerized information files.

A number of well known techniques have been adapted for computer usage including the Ceaser cipher, Mono alphabetic cipher, Homophonic substitution, Bale cipher, Play fair cipher, Poly alphabetic cipher, Vigenere Cipher, One- time pad cipher, Vernam ciphers, Play Color Cipher and usage of rotor machine in Substitutions, Rail fence technique, more complex
permutations for more secure transposition and some Steganography principle were briefly discussed with merits and demerits.

Finally it gives the broad knowledge on almost all the cryptographic and Steganography principles where a reader or scholar have lot of scope for updating or invention of more secure algorithms to fulfill the global needs in information security.

Reference

- Deavours.C.A “The black chamber: a column, how the British broke Enigma”, Cryptoloyia, 1980, 4, pp. 129 132
- The Beale Cipher Association,“The Beale ciphers”, Ned field, MA, 1978
- Vernam. G. J, "Cipher printing telegraph systems for secret wire and radio telegraphic communications”, AIEE, 1926, 45, pp. 109 115
Index Terms

Computer Science

Information Security

Key words

Block Cipher

Play Color

Cryptography

Encryption

Decryption

Decillions

Homophonic

Steganography

HSC

PSC

PCC

SIS

Substitution

Transposition