

{tag}

Information Security  
Journal  
RTINFOSEC

{/tag}

IJCA Special Issue on Recent Trends in  
© 2014 by IJCA

Year of Publication: 2014

Authors:

Malay B. Pramanik

{bibtex}rtinfosec1411.bib{/bibtex}

## Abstract

Cryptography is an art and science of converting original message into non-readable form. There are two techniques for converting data into non-readable form: 1) Transposition technique 2) Substitution technique. Transposition ciphers use the letters of the plaintext message, but they permute the order of the letters. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. In this Cryptography there is use of three aspects of Columnar Transposition; Single Transposition using ROT-13 applicable to message of the Algorithm, Double Transposition using Caesar Cipher in second round of an Algorithm and Triple Transposition were it combine both the concept and use reverse of the message in second round of the Algorithm.

ences

Refer

- R. I Salawu & S. O Adetona, "The Art and Science of Secured Communication";, Institute of Security of Nigeria, Nigeria 2007
- James Irvine & David Harie, "Data Communications & Network: An Engineering Approach";, John Wiley & Sons Ltd. , 2002
- Brian J. Winkel, Cipher A. Deavours, David Kahn, and Louis Kruh "The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure";, Artech House, August 2005.
- Tyma Paul, "Software Development Secure";, Start Newsletter, Feb 2003.
- Madsen Wayne, "An International Survey of Encryption Policy";, 1998
- S. O Adetona, "Messages Secrecy in Electioneering environment";, proceedings of Institute of Security, Nigeria,2009
- Stamper, David, "Essential of Data Communication";, Saratoga Group
- Eric Maiwald, "Network Security a Beginner's Guide";, Second Edition, McGraw Hill, Osborne, 2003.
- Ed Tittel, "Theory and Problems of Computer Networking";, McGraw Hill, Osborne, 2002

### Index Terms

Computer Science

Security

### Keywords

Cryptography   Substitution   Transposition   Rot-13   Caesar Cipher   Columnar  
Transposition  
Shift Algorithm  
  
Cipher Text  
  
Plaintext  
  
Encryption  
  
Decryption.

