A Simple Algebraic Model based Polyalphabetic Substitution Cipher

Abstract

Cryptography is considered to be a disciple of science of achieving security by converting sensitive information to an un-interpretable form such that it cannot be interpreted by anyone except the transmitter and intended recipient. An innumerable set of cryptographic schemes persist in which each of it has its own affirmative and feeble characteristics. In this paper we have developed a traditional or character oriented Polyalphabetic cipher by using a simple algebraic equation. In this we made use of iteration process and introduced a key K0 obtained by permuting the elements of a given key seed value. This key strengthens the cipher and it does not allow the cipher to be broken by the known plain text attack. The cryptanalysis performed clearly indicates that the cipher is a strong one.

References

- Ayushi, (2010), A Symmetric Key Cryptographic Algorithm, International Journal of
Computer Applications (0975 - 8887) Volume 1. No. 15.

**Index Terms**

Computer Science  
Security

**Keywords**

Polyalphabetic substitution  variable length key stream  bit-ratio test  frequency test