Abstract

Information theoretic approach for decipherment problems is the recent trend in cryptanalysis. The behavioral transformation of message units is addressed upto certain extent in the encryption process. However the amount of confusion and diffusion in terms of statistical distribution parameters between message and cipher text is a point of interest for cryptanalyst. In the present work we addressed this issue with the help of enhanced probability distribution function. The basic units of any message text are observed to be heuristic in nature depending on the sample. Averaging function is adopted while evaluating the enhanced probabilities of message units. The retrieved efficiency of cipher text only attack on samples of English, Hindi Telugu, Kannada is presented in this paper.

Reference
Decipherment of Substitution Cipher using Enhanced Probability Distribution

- Sujith Ravi, Kevin Knight.: Attacking Letter Substitution Ciphers with Integer
Decipherment of Substitution Cipher using Enhanced Probability Distribution

- C. E. Shannon.: Prediction and Entropy of Printed English. In the Bell System Technical Journal pp. 53-64 (1951)

Index Terms

Computer Science
Information Security

Key words

Cryptanalysis
probability distribution
Conditional probability distribution
Enhanced probability distribution