STATISTICAL CRYPTANALYTICS TECHNIQUES

VasilePREDA, Ph. D,
University of Bucharest

Emil SIMION, Ph. D,
Advanced Technologies Institute
e-mail: simion@pro.math.unibuc.ro

Abstract

This paper presents some useful testing procedures for identification of the language used in plain text version of a cipher text and also the cryptographic system used. The procedures are based only on the knowledge of the cipher text and the tests identifies substitution (monographic and polygraphic) systems, transpositions systems, and polyalphabetic ciphers. The tests functions are universal and can be easy applied to other types of ciphers systems.

Key words: Cryptography,Statistical analysis of cipher tests.
AMS classification: 94A60, 62P99**.**