Identification of Encryption Method for Block Ciphers using Histogram Method *

Sreenivasulu Nagireddy
Hema A. Murthy
Department of Computer Science and Engineering
Indian Institute of Technology Madras
Chennai, India

Shri Kant †
Coordinator, Joint Cipher Bureau
Department of Defence R & D
M. G. Road, Metcalfe House
Delhi 110 054, India

Abstract

In this paper, we propose a histogram based method for identification of encryption method from a cipher text obtained using a block cipher. Frequency of occurrence of symbols formed by groups of bits in the cipher text, is obtained to build a histogram. The proposed method is seen to be efficient for ECB mode. We also show that the entropy based on the probabilities of symbols in the cipher texts can be used to distinguish between the ECB and CBC modes. Finally, we propose a multiple histogram based method for identifying the starting position of a block in a cipher text for the ECB mode of encryption.

Keywords : *Block ciphers, mode of encryption, histogram based classifications.*

1. Introduction

A block cipher is a symmetric cipher that divides a plain text into blocks of symbols and uses a specially constructed function which mixes a block of the plain text with a secret key to produce a block of the cipher text. A block cipher that uses a block length k is designed in such a way that it can take one of the 2^k possible blocks of plain text and produce 2^k

*This paper was presented at '*Pre-ICM International Convention on Mathematical Sciences*' held at Department of Mathematics, University of Delhi, 18-20 December, 2008.

†*E-mail*: shrikant.ojha@gmail.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 4, pp. 319–328