SECTION 6

BLOCK CIPHERS
COMPARISON OF BLOCK CIPHERS

Helen Gustafson* Ed Dawson* Bill Caelli**

* School of Mathematics
Queensland University of Technology
GPO Box 2434
Brisbane Q 4001

** Information Security Research Centre
Queensland University of Technology
GPO Box 2434
Brisbane Q 4001

ABSTRACT

Several DES replacement block ciphers have been published. In this paper a report will be given on the development of a package for analysis and comparison of block ciphers. Experimental results are presented on applying this package to DES, FEAL-N, and Madryga ciphers.

1. INTRODUCTION

There are several properties that a block cipher should satisfy in order to be secure from cryptanalytic attack including plaintext - ciphertext independence, completeness, nonaffine system and the strict avalanche effect. In this paper a report is given on the development of a package for analysis and comparison of block ciphers in terms of the above properties. This package is being designed in such a manner that block ciphers of the same block length can be compared.

Several DES replacement block ciphers with block length 64 have been published including FEAL-N (N = 4, 8, 16, 32) (see [1] and [2]), and Madryga (see [3]). FEAL-N is a Feistel type cipher with N rounds of an F-function. The cipher is faster in encryption and decryption speed than DES in both software and hardware implementation. In [4] Den Boer has a chosen plaintext cryptanalysis of FEAL 4. The Madryga algorithm was designed as a DES replacement block cipher by the Canadian Imperial Bank of Commerce. It is not a Feistel type cipher. In Sections 3 and 4 each of the above block ciphers will be used in a comparison with DES.

In Section 2 several measures of randomness for finite sequences will be discussed consisting of statistical tests, sequence complexity and the binary derivative. In Section 3 it will be shown how these measures of randomness can be used to examine plaintext - ciphertext independence.

In Section 4 it will be shown how to examine the strict avalanche effect by applying the Kolmogrov-Smirnov test to the entries of a dependence matrix defined by avalanche vectors. In addition the dependence matrix defined by plaintext - ciphertext avalanche vectors allows one to determine whether or not the block is complete and nonaffine (for a particular choice of key).