

NESSIE

Project Number IST-1999-12324
Project Title NESSIE
Deliverable Type Report
Security Class Public
Deliverable Number D03
Title of Deliverable List of General NESSIE Test Tools

Nature of the Deliverable

Document reference NES/DOC/SAG/WP2/D03/1
Contributing WPs WP2 - Toolbox Development
Contractual Date of Delivery Y1M06
Actual Date of Delivery Y1M12
Editor Markus Dichtl, Siemens AG

Abstract Outline description of general analytic tools for use in the evaluation of NESSIE submissions

Keywords cryptanalysis, RIPE, tools

Disclaimer The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Document Control

Document History

This is the first issued version of this document.

Changes Forecast

This document will not be maintained as it will be superseded by D09.

Table of Contents

1. Introduction.....	3
2. Descriptions of the General Tools	3
2.1 New Tools.....	3
2.2 The RIPE Test Suite.....	4
2.3 The NIST Test Suite	6
3. Status of the Tools	6

List of General NESSIE Test Tools

1. Introduction

The purpose of Workpackage 2, “Toolbox Development” of NESSIE is to provide tools for the analysis of the NESSIE submissions. The group of tools outlined here consists of those general tools which have not been specifically developed for the analysis of any individual submission.

This is an interim report proving a snapshot of the tools.

The subsequent deliverable D09 will provide both the toolbox itself, confidential to the project, and a public status report.

2. Descriptions of the General Tools

2.1 New Tools

Tools for Linear and Differential Cryptanalysis

Linear ([4]) and differential ([1]) cryptanalysis are the most important methods for the analysis of block ciphers. It is clear how to analyse the S-boxes of a block cipher for linear and differential properties, but it is not clear, in which generality the propagation of those properties can be evaluated by a software tool. In order to achieve a very general tool, a formal description of the architecture of the block cipher is needed. There is also a trade off between the generality of the tool and the effort to specify and implement it.

Related Keys Tool

The idea of this tool is to check whether the related key attacks introduced in [2] are possible. The key of the block cipher is expanded, and the expanded key is compared with a rotated copy of itself. If, for any shift, the two copies have significantly too many or too few equal bits, a message is printed out.

Percolation Test

The percolation test is a newly introduced test for the randomness of a sequence of bits. The random bits are used to determine whether a tree is standing at a position in the simulation of a forest. Then the propagation of a simulated forest fire is evaluated statistically.

Correlation Test

The correlation test is part of the RIPE test suite, which will be distributed for the NESSIE partners. By using the FFT, this test determines the number of coincidences of a bit sequence with its shifted copy simultaneously for various shifts. However, the problem is the correct statistical evaluation of these numbers of coincidences, which are not independent. If no theoretical solution can be found, the test will be calibrated by reference values generated by a good pseudo random number generator.

Neyman-Pearson Test Tool

This test turns up in the proof of the Neyman Person theorem. It is the optimal test to distinguish between two different probability distributions.

Constant Runs Test

This test determines the numbers and the lengths of contiguous subsequences of zeros or ones in a sequence of bits. The numbers of these “runs” of various lengths are evaluated statistically. This statistical evaluation is non-trivial, and some publications about this topic are definitely wrong. The runs tests is also part of the NIST test suite described below, but the statistical approach followed there seems to be questionable.

***p*-adic Span Tool**

The *p*-adic span is an analogue to the linear complexity of a bit sequence. The linear complexity is based on linear feedback shift registers; the linear span is based on feedback shift registers with carry. The theory of the *p*-adic span is described in [3].

2.2 The RIPE Test Suite

This test suite was developed in the project RIPE (RACE Integrity Primitives Evaluation). The tools will be distributed among the NESSIE partner for the statistical evaluation of NESSIE submissions.

RIPE-Tests for Block Ciphers

The Dependence Test

The dependence test computes the dependence matrix and the distance matrix of a block cipher. The degree of completeness, the degree of the avalanche effect, and the degree of the strict avalanche criterion are also computed.

The Linear Equation, Linear Approximation, and Correlation Immunity Test

This test is based on the Fast Walsh Transform. It can not be used for block ciphers of a practical block size, but for S-boxes.

The Linear Factors Test

The linear factors test determines linear equations which hold between plaintext bits, key bits, ciphertext bits, and ciphertext bits obtained when one key or plaintext bit is toggled.

The Cycle Test

This tool can be used to detect cycles when a block cipher is applied repeatedly.

RIPE-Tests for Stream Ciphers

The Frequency Test

The frequency test splits up the bit sequence into subsequent, disjoint *m*-tuples of bits. *m* is called the blocksize of the test. The frequencies of the occurrences of those *m*-tuples are counted and evaluated statistically.

The Overlapping *m*-tuple Test

The overlapping *m*-tuple test splits up the bit sequence into *m*-tuples of words. Each word contains a fixed number of bits. In the overlapping *m*-tuple test, the *m*-tuples are not disjoint; to take the next *m*-tuple, an *m*-word-window over the original sequence is shifted by one word. So the next *m*-tuple consists of *m*-1 shifted words of the previous *m*-tuple and one new word with bits from the sequence. Since subsequent *m*-tuples are not independent, the statistical evaluation is more involved than in the case of the frequency test, but this is handled by the test program. This test is applied to cyclic shifts of the original sequence as well.

The Collision Test

The collision test splits up the bit sequence into *m*-tuples of words and evaluates, how often such *m*-tuples occur more than once.

The Gap Test

The gap test splits up the bit sequence into subsequent, disjoint *m*-tuples of bits. *m* is called the word length of the test. These *m*-tuples are interpreted as binary representations of numbers, and the lengths of gaps, where the numbers are not within a numerical range given as a parameter of the test, are registered and evaluated statistically. The gap test is applied to

cyclic shifts of the original sequence as well. For each shift the percentage level of acceptance is given.

The Run Test

The run test splits up the bit sequence into subsequent, disjoint m -tuples of bits. m is called the block size of the test. These m -tuples are interpreted as binary representations of numbers. The lengths of runs of these numbers, that is strictly increasing sequences of subsequent numbers, are evaluated statistically.

The Coupon Collector's Test

The coupon collector's test splits up the bit sequence into subsequent, disjoint m -tuples of bits. m is called the word length of the test. In the test the number of subsequent m -tuples it takes until all possible 2^m m -tuples have appeared is evaluated statistically.

The Universal Maurer Test

The universal Maurer test splits up the bit sequence into subsequent, disjoint m -tuples of bits.

m is called the block size of the test. The test evaluates statistically how many m -tuples later an m -tuple re-appears in the sequence. The test result of the Maurer test is closely related to the entropy of the bit sequence.

The Poker Test

The poker test splits up the bit sequence into subsequent, disjoint m -tuples of bits; m is called the word-length of the test. This sequence of m -tuples is split up into subsequent, disjoint k -tuples of m -tuples.

The poker test evaluates statistically how many of the m -tuples in the k -tuple are equal.

The Correlation Test

The correlation test determines in how many places the original sequence and the sequence shifted by n bits have the same value. This is done for all shifts up to the length of the original sequence. To support the interpretation of the results, for each shift the probability for a sequence of random, independent, and uniformly distributed bits to have this number or less coincidences with its shifted copy is determined. Only values where these probabilities are close to 0 or 1 are printed. The print level is the maximal deviation from 0 or 1 for the probability in order to get printed.

The Spectral Test

The spectral test applies the Fast Walsh Transform to the given sequence. It uses two values derived from the transform to assess the randomness of the sequence.

The Rank Test

In the rank test the bits of the sequence to test are used to fill square matrices. The bits are treated as elements of the field GF(2), and the ranks of the matrices are evaluated statistically.

The Linear Complexity Test

The linear complexity test uses the Berlekamp-Massey algorithm to determine the length of the shortest linear feedback shift register which can produce the given bit sequence. For the linear complexity profile, this is done for the first 1, 2, 3, ... bits of the original sequence. The increase in the linear complexity is studied.

The Nonlinear Complexity Test

The nonlinear complexity test determines the minimal length of a shift register with arbitrary feedback function which generates the given sequence.

The Ziv Lempel Complexity Test

The Ziv Lempel complexity test measures how well a bit sequence can be reconstructed from earlier parts of the bit sequence.

2.3 The NIST Test Suite

The US-NIST has recently published a statistical test suite for the evaluation of the randomness of sequences of bits. It is available for download at [5].

3. Status of the Tools

Note that this is a snapshot status as of Quarter 3, Year 1 (August 2000).

Name of the Tool	Status
Tools for Linear and Differential Cryptanalysis	Ongoing development at Haifa
Related Keys Test	Under development at UCL
Percolation Test	Finished at Siemens, ready for distribution
Correlation Test	Available as part of the RIPE Tools, needs additional theory for the evaluation. Looking for a theoretical solution at Siemens. Otherwise calibration with a good PRNG.
Neyman-Pearson Test Tool	At a very early stage at Siemens. Currently put on hold, since it is not clear to which distributions it should be applied. Can be implemented at short notice if needed.
Constant Runs Test	Theoretical work and implementation done at Siemens, ongoing
p -adic Span Tool	Running software at Siemens. Must be documented
RIPE Test Suite	Accuracy checked at Siemens, results available on the NESSIE internal webpages. The tools will be distributed to the NESSIE partners for use within NESSIE.
NIST Test Suite	Available, should be checked carefully

References

- [1] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology - Eurocrypt '90, Springer-Verlag, 1991, pp 2-21
- [2] E. Biham, New Types of Cryptanalytic Attacks Using Related Keys, Advances in Cryptology - Eurocrypt '93, Springer-Verlag, 1994, pp 398-409.
- [3] A. Klapper, M. Goresky, Feedback Shift Registers, 2-Adic-Span, and Combiners with Memory, Journal of Cryptology, Vol. 10,.n. 2, Spring 1997, pp 111-147
- [4] M. Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology - Eurocrypt '93, Springer-Verlag, 1994, pp 386-397
- [5] The NIST Test Suite: <http://csrc.nist.gov/rng>