MUTUAL CORRELATION OF RANDOMNESS TEST AND ANALYSIS OF TEST OUTPUTS OF TRANSFORMED AND BIASED SEQUENCES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ZİYA AKCENGİZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

AUGUST 2014

Approval of the thesis:

MUTUAL CORRELATION OF RANDOMNESS TEST AND ANALYSIS OF TEST OUTPUTS OF TRANSFORMED AND BIASED SEQUENCES

submitted by **ZİYA AKCENGİZ** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics** _______________

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** _______________

Assoc. Prof. Dr. Ali Doğanaksoy
Supervisor, **Department of Mathematics, METU** _______________

Examining Committee Members:

Dr. Muhiddin Uğuz
Department of Mathematics, METU _______________

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics, METU _______________

Assist. Prof. Dr. Çetin Ürtiş
Department of Mathematics, TOBB ETU _______________

Assist. Prof. Dr. Fatih Sulak
Department of Mathematics, Atılım University _______________

Dr. Cihangir Tezcan
Department of Mathematics, METU _______________

Date: _______________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ZİYA AKCENGİZ

Signature :

ABSTRACT

MUTUAL CORRELATION OF RANDOMNESS TEST AND ANALYSIS OF TEST OUTPUTS OF TRANSFORMED AND BIASED SEQUENCES

Akcengiz, Ziya
M.S., Department of Cryptography
Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy

August 2014, 25 pages

Randomness is one of the most important parts of the cryptography because key generation and key itself depend on random values. In literature, there exist statistical randomness tests and test suites to evaluate randomness of the cryptographic algorithm. Although there exist randomness tests, there is no mathematical evidence to prove that a sequence or a number is random. Therefore, it is vital to choose tests in the test suites due to independency and coverage of the tests used in the suites. Sensitivity of these tests to non-random data is also important.

The tests should be classified to determine that tests are independent and wide. In order to classify, sensitivity of tests to transformations and to nonrandom data should be determined. Therefore, mutual correlations of tests are analyzed.

Keywords : Correlation, randomness tests, transformation, bias

ÖZ

RASTGELELİK TESTLERİNİN İKİ TARAFLI KORELASYONLARI VE
DÖNÜŞMÜŞ VE EĞİLİMLİ DİZİLERİN TEST SONUÇLARININ ANALİZLERİ

Akcengiz, Ziya
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Doç. Dr. Ali Doğanaksoy

Ağustos 2014, 25 sayfa

Rastgelelik kriptografinin en önemli kısımlarından biridir çünkü, anahtar üretimi ve anahtarların kendileri rasgele değerlere bağlıdır. Literatürde bir çok istatiksel rastgelelik testi ve bu testleri içeren test paketleri yer almaktadır. Buna rağmen bir dizinin veya bir sayının rastgele olduğunu gösterecek hiç bir matematiksel kanıt yoktur. Bundan dolayı bir istatiksel test paketi oluştururken bu testlerin seçimi hayati bir önem taşımaktadır. Ayrıca bu testlerin rastgele olmayan verilere karşı duyarlılığıda çok önemlidir.

İstatiksel testlerin birbirinden bağımsız olduğunu ve kapsamının geniş olduğunu belirlemek için sınıflandırılması gerekmektedir. Bu sınıflandırmayı yapabilmek için testlerin dönüşümlere karşı ve rastgele olmayan verilere karşı duyarlılığı belirlenmelidir. Bundan dolayı bu testlerin iki taraflı korelasyonları analiz edildi.

Anahtar Kelimeler : korelasyon, rastgelelik testi, sapma, dönüşüm

To My Family and To My Love

ACKNOWLEDGMENTS

First of all, I would like to gratefully thank to my supervisor Assoc. Prof. Ali Doganaksoy not only for his support, guidance and motivation that make my thesis start and finish but also for being the main factor that makes me choose Cryptography.

I would like to express my deep thanks to Assist. Prof. Dr. Fatih Sulak and Dr. Muhiddin Uguz for their support and contributions to my thesis with their great experiences and knowledge.

I am very grateful to Okan ŞEKER for his endless help, support and most importantly being a good friend.

I greatly appreciate to Ezgi ORBAY for her endless support and help while writing my thesis, but most importantly for her love to me.

I thank to my friends in TUBITAK-UEKAE and Institute of Applied Mathematics for their support and friendships.

I greatly thank to my family for their support to take best education during my life and for their love and encouragement.

At the end I want to express my thanks to all my friends for their friendships.

TABLE OF CONTENTS

CHAPTERS

APPENDICES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Randomness

Random numbers and random sequences have a wide application area such as cryptography, numerical analysis, game history and quantum mechanics. Especially in cryptography, it is very important if the used values are random or not. Some parts of cryptography such as authentication systems, generation of digital signatures and zero knowledge protocols need sequences to be random. But, in all of them, it is the most important feature to use random values in key generation. It is mentioned in the famous principle of Kerkchoffs [6] *that the security of ciphers should depend entirely on the secrecy of keys, not on the details of the encryption/decryption algorithms.* The whole cryptosystem can be broken because if the values are not random enough the system can fail. Therefore, statistical randomness tests are very important for the security evaluation of cryptographic algorithms.

In cryptography, random number generation is a challenging task. True random number generators **(TRNGs)** have ability to produce random number by using a non deterministic source. There are many methods to obtain random numbers. In one of them, the elapsed time between emissions of particles is measured when the radioactive decay time is unpredictable. The other methods use physical quantities like atmospheric noise and thermal noise from a semiconductor diode. TRNGs have some disadvantages like inefficiency and impracticability to store and transmit large number of random bits. Therefore, pseudorandom number generators **(PRNGs)** are more preferable. Compared to TRNGs, they are more efficient and the results of PRNGs are obtained in shorter time. Also, PRNGs are periodic in contrast to TRNGs. These generators use deterministic sources, which means reproducibility of a given sequence of numbers. In PRNGs, a truly random binary sequence (seed) of length k is taken and a periodic “random looking” binary sequence of length $l \gg k$ is produced. The seed is obtained by using TRNGs in most of the applications. The main requirements of PRNGs are sufficiently large length of the seed and unpredictability of the output by adversary.

Making the statistical analysis of PRNGs is very critical because the outputs of PRNGs should not be statistically distinguished from real random sequences. For the statistical analysis, a sample sequence is obtained and evaluated by statistical randomness tests.

1.2 Statistical Randomness Tests

In the literature, there exist multiple test suites such as the suite given in the Knuth's book [7], test suite presented by Rukhin [13], DIEHARD [9], CRYPT-X [3], TestU01 [8], the test suite published by Sulak [16] the test suite published by NIST [2] and various works on statistical tests individually such as Golomb [4] proposed three postulates which are the initiative attempts to investigate the randomness of a periodic binary sequence, a universal statistical test, stated by Maurer [10], a test based on diffusion characteristic of a block cipher, topological binary test defined by Alcover [1] et.al. In spite of that, the study was conducted to tests that in test suite published by NIST, which is the focus of this thesis. However, implementations can be applied to the other test suites in further works and the other published test suites. Test suite published by NIST includes 16 tests (after Fast Fourier Transform Test was discarded). NIST test suite includes Frequency Test, Frequency within a Block Test, Runs Test, Longest Run of Ones in a Block Test, Binary Matrix Rank Test, Discrete Fourier Transform Test, Non-overlapping Template Matching Test, Overlapping Template Matching Test, Maurer's Universal Statistical Test, Lempel-Ziv Compression Test, Linear Complexity Test, Serial Test, Approximate Entropy Test, Cumulative Sums Test, Random Excursions Test, and Random Excursions Variant Test. Brief information about statistical randomness tests that are taken from NIST statistical randomness tests suite [2] and properties of tests are given.

1.2.1 Frequency Test

The distribution of zeroes and ones in the whole sequence is focused in the frequency test. In this test, it is aimed to observe if the number of zeroes and ones in the sequence are approximately the same as in any truly random sequence. In a truly random sequence, the number of ones should be about the same as the number of zeroes. All following tests are conducted after passing the frequency test.

1.2.2 Frequency Test within a Block

Frequency test within a block is about the comparison of the proportion of ones in M bit blocks to the proportion in a truly random sequence. For a truly random sequence, the proportion of ones in M bit block should be approximately $M/2$.

1.2.3 Runs Test

The aim of runs test is to compare the total number of runs in the sequence with the number of runs in a truly random sequence. As defined before, run is an uninterrupted subsequence consisting of only ones or only zeroes. In this test, the situation when the oscillation between zeroes and ones is too fast or too slow is avoided.

1.2.4 Test for the Longest Run of Ones in a Block

The concern of this test is the comparison of the length of the longest run of ones in M bit blocks to that in a truly random sequence. As a remark, the application of another test to longest run of zeroes in the sequence is unnecessary because an irregularity in the longest run of ones causes an irregularity in that of zeroes.

1.2.5 Binary Matrix Rank Test

Binary matrix rank test is about comparison of the rank of disjoint sub-matrices of the whole sequence to the rank of disjoint sub-matrices of a truly random sequence.

1.2.6 Non-overlapping Template Matching Test

The concern of this test is the comparison of the number of non-overlapping predetermined templates in sequences to the number of that in a truly random sequence.

1.2.7 Overlapping Template Matching Test

The concern of this test is the comparison of the number of overlapping predetermined templates in sequences to the number of that in a truly random sequence.

1.2.8 Maurer's "Universal Statistical" Test

If a sequence can be compressed significantly, this sequence is said to be non-random. Maurer's "Universal Statistical" test is about determination of significant compression of a sequence without losing any information.

1.2.9 Linear Complexity Test

Linear complexity test is about the length of a linear feedback shift register (LFSR). In this test, the sequence is determined to have enough complexity to be considered as non-random. The length of LFSRs is directly related to the randomness.

1.2.10 Serial Test

Serial test is aimed to compare the frequency of all possible overlapping m bits in the sequences to that in a truly random sequence. For $m = 1$, this test is identical to the frequency test.

1.2.11 Approximate Entropy Test

Approximate entropy test is very similar to serial test. Despite that, the main purpose of this test is to compare the frequency of all possible overlapping m and $m + 1$ bits and to compare the result to expected result from a truly random sequence.

1.2.12 Cumulative Sums (Cusum) Test

In this test, it is aimed to compare the cumulative sum of the partial sequences in a sequence to the cumulative sum of the partial sequences in the truly random sequence. The cumulative sum of arranged $(-1, +1)$ digits in the sequence describes the random walk. In this test, the maximal excursion of random walk is determined whether it is near zero as expected from a truly random sequence or large as expected from the certain types of non random sequences.

1.2.13 Random Excursions Test

The purpose of this test is to determine whether the number of the cycles making exactly k visits in the tested sequence is the same as in a truly random sequence or not. In order to conduct this test, the sequence is firstly transformed to $-1, +1$ sequence. Cycle is defined as the interval at which the sequence converges to zero when taking partial sum after the transformation of the sequence.

1.2.14 Random Excursions Variant Test

The purpose of this test is to compare the total number of times that a particular state is visited in a cumulative sum random walk of the tested sequence with expected value from a truly random sequence. This test consists of eighteen tests and conclusions. One test and conclusion for each of the states: $-9, -8, \ldots, -1$ and $+1, +2, \ldots, +9$.

In table 1.1 minimum sequence lengths that the statistical tests can be applied are given. In here, statistical tests are divided in two parts that can be applied to short sequences and long sequences. Therefore, frequency test, frequency within a block test, runs test, longest run of ones in a block test, serial test, approximate entropy test, cumulative sums test are tests that can be applied to short sequences. Other tests can be applied to long sequences.

1.3 Motivation

Mutual correlation of used test should be minimized and their contents must be wide for the test suite to achieve successful results. Therefore, selection of tests has a critical

Table 1.1: Minimum Sequence length that the statistical tests can be applied

Tests	Sequence length
Frequency Test	10^2
Frequency Test within a Block	10^2
Runs Test	10^2
Test for the Longest Run of Ones in a Block	10^2
Binary Matrix Rank Test	10^6
Non-overlapping Template Matching Test	10^6
Overlapping Template Matching Test	10^6
Maurer's "Universal Statistical" Test	$387,840$
Linear Complexity Test	10^6
Serial Test	10^2
Approximate Entropy Test	10^2
Cumulative Sums (Cusum) Test	10^2
Random Excursions Test	10^6
Random Excursions Variant Test	10^6

significance in formation of the test suite. Randomness cannot be decided by uncontrollably increasing the number of the criteria as it cannot be decided by applying a few criteria.Studies on classification in the literature remain weak, and therefore deficiencies are causing problems in the test suite. One of the reasons for this deficiency is that a complete method for classification is not found.

The importance of classification of tests is denoted by Soto [15]; in order to obtain reliable results, the tests should be independent. In other words, results of the test must be uncorrelated with each other as possible. Therefore, the tests that appear to be different in spite of having the same results would be avoidable.

In 2003, study by Wegenkittl and Hellekalek [5] showed that 3 tests in the test suites were highly correlated with each other. The rough classification proposed by Turan uses two important features of random sequences emphasized by Robshaw [12]. The first one is the inability to predict and the other one is reproduction of the sequence. However, these two categories are not entirely independent. Also, in the comparison by Turan [14], some tests which are commonly used in test suites were found to be correlated with each other, and important results are obtained. In a study conducted by Sulak [16] in 2011, a base for the classification of the statistical randomness tests was prepared. Therefore, how some transformations defined on the data affect the tests is observed and a new classification has been proposed according to the results of this observation.

The relations between tests in NIST test suite are clearly revealed by the correlation results in which sensitivity to transformations and weaknesses of tests are determined. In the light of this study, the tests in the test suites and the tests that are not included in any test suites can be correlated after passing through these stages, and success can be achieved with the minimum number of test when creating new test suites. !!!After determining if the tests are correlated or not correlated, similarly sensitive to transformations or not and reaction to bias sequences are same or not, the criteria of classification can be created.

1.4 Brief Information of Chapters

- In chapter two, mutual correlation of statistical randomness tests are given
- In chapter three, the transformations are identified and the original and the generated sequences are inserted in the test suite of NIST and correlation analysis of p-values are conducted.
- In chapter four, brief definition of bias is given and sensitivities of statistical randomness tests are investigated.
- According to the obtained results, the conclusion is made in chapter five.

CHAPTER 2

MUTUAL CORRELATION OF RANDOMNESS TESTS

Correlation determines direction and power of the direct relation between two random variables at probability theorem and statistics. In this study, the relation between $p-values$ generated by two different tests is investigated. In the general statistical application, the correlation shows how getting away from independence. If the obtained value converges to 1 then the results are positively dependent, if it converges to 0 then the results are independent, and if it converges to -1 than the results are negatively dependent. Here, positively dependent means that if one value increases then the other one does too and negatively dependent means that one value decreases while the other one increases.

For different situations, different correlation coefficients are developed. The best known one of them is Pearson correlation coefficient [11]. It is obtained by dividing covariance of two variables by the product of standard deviation of these variables. In this study, Pearson correlation coefficient is used to obtain the results.

This chapter is examined in two parts, randomness tests that can be applied to short sequences and randomness tests that can be applied to long sequences. Distinct results are given for both of the parts. In order to get the results, IBM SPSS Statistic is used. In this study, we call tests correlated if the correlation coefficient is higher than 0.5.

2.1 Randomness Tests That can be Applied Short Sequences

For the tests in this chapter, approximately 200000 sequences each of length of 1024 bits are used. The same results can be obtained by using different length sequences. In the table 2.1, the correlation analysis values of p_values are given. In this table 2.1, diagonal results give the correlation within test's itself and, naturally, the result equals to 1. Therefore, the results should be investigated without considering the diagonal. According to these results, relatively high correlation values are considered between the tests

- Frequency and cumulative sum type1 (coefficient 0.767) see Table 2.2.
- Frequency and cumulative sum type2 (coefficient 0.768) see Table 2.2.

Table 2.1: Mutual Correlation of Randomness Tests that can be Applied Short Sequences

TESTS	Frequency	Block Frequency	Runs	Longest Run of Ones	Serial 1	Serial 2	Appr. Entropy	CUSUM1	CUSUM2
Frequency	1.000	0.281	0.006	**0.280**	0.002	0.000	**0.198**	**0.767**	**0.768**
Block Frequency	**0.281**	1.000	0.001	0.107	0.005	0.001	0.082	**0.465**	**0.466**
Runs	0.006	0.001	1.000	0.079	0.004	-0.001	0.191	0.006	0.007
Longest Run of Ones	**0.280**	0.107	0.079	1.000	0.005	0.001	**0.231**	**0.244**	**0.247**
Serial 1	0.002	0.005	0.004	0.005	1.000	**0.681**	0.020	0.005	0.001
Serial 2	0.000	0.001	-0.001	0.001	**0.681**	1.000	0.002	0.000	-0.001
Appr. Entropy	**0.198**	0.082	0.191	**0.231**	0.020	0.002	1.000	0.176	0.177
CUSUM1	**0.767**	**0.465**	0.006	**0.244**	0.005	0.000	0.176	1.000	**0.723**
CUSUM2	**0.768**	**0.466**	0.007	**0.247**	0.001	-0.001	0.177	**0.723**	1.000

- Cumulative sum type1 and type2 (coefficient 0.723) see Table 2.2.
- Serial type1 and type 2 (coefficent 0.681) see Table 2.3.

Among the other tests, some considerable correlation are observed. However, the correlations are not as high as the correlations of these tests and they are not put in the class of ”correlated tests”.

According to the obtained results, it is thought that only one of frequency tests, CUSUM1 and CUSUM2 is appropriate to be used in the test suites since there are high correlation between them.Similarly, serial 1 and serial 2 are highly correlated. Therefore, the use of only one of these tests in the test suites is thought not to cause any loss.

2.2 Randomness Tests that can be Applied Long Sequences

In this section, the correlations between the tests that can be applied to long sequences. In the conducted study, 200 sequences that are length of 2^{20} bits are inserted to the tests and distinct p-values are obtained for every sequence. As a result of the studies, it is understood that many tests are not correlated with each other. However, the correlation between random excursion test and random excursion variant test is very high. Also, the relation between only serial1 and serial2 is found when applied to short sequences; however, the relation between approximate entropy test and serial tests is found when applied to long sequences. Templates of 9 bits are used in non-overlapping and overlapping template matching test.

Table 2.2: Observed Correlation 1

	frequency	cusum1	cusum2
frequency	1	0.767	0.768
cusum1	0.767	1	0.723
cusum2	0.768	0.723	1

Table 2.3: Observed Correlation 2

	serial1	serial2
serial1	1.000	0.681
serial2	0.681	1.000

Table 2.4: Mutual Correlation of Randomness Tests can be Applied Long Sequences

	frequency	block frequency	run	long run	serial1	serial2	app.entropy	cusum1	cusum2	lin.complexity	non-overlapp.	overlapping	bin matrix	universal	r.excursion	r.e.variant
frequency	1.000	-0.012	0.022	0.010	0.050	-0.099	0.096	0.796	0.769	-0.020	-0.049	0.164	-0.042	0.075	0.169	0.247
block frequency	-0.012	1.000	0.127	-0.146	0.021	-0.005	-0.005	0.015	0.033	0.103	0.029	0.094	-0.104	0.012	-0.032	-0.145
run	0.022	0.127	1.000	-0.025	0.044	0.019	0.017	0.022	-0.028	-0.044	-0.015	0.049	0.031	0.006	-0.012	0.006
long run	0.010	-0.146	-0.025	1.000	0.001	-0.008	-0.022	-0.011	-0.014	-0.094	0.007	-0.045	0.112	-0.044	-0.037	-0.016
serial1	0.050	0.021	0.044	0.001	1.000	0.648	0.676	0.064	0.057	0.054	-0.103	0.074	0.054	0.079	0.110	0.024
serial2	-0.099	-0.005	0.019	-0.008	0.648	1.000	0.001	-0.038	-0.072	0.015	-0.062	0.042	0.118	0.039	-0.016	-0.037
app.entropy	0.096	-0.005	0.017	-0.022	0.676	0.001	1.000	0.089	0.065	0.054	-0.032	0.035	-0.052	-0.018	0.089	0.026
cusum1	0.796	0.015	0.022	-0.011	0.064	-0.038	0.089	1.000	0.752	0.025	0.013	0.154	-0.052	0.092	0.300	0.427
cusum2	0.769	0.033	-0.028	-0.014	0.057	-0.072	0.065	0.752	1.000	0.038	-0.040	0.092	-0.065	0.090	0.079	0.200
lin.complexity	-0.020	0.103	-0.044	-0.094	0.054	0.015	0.054	0.025	0.038	1.000	0.031	-0.081	0.053	-0.033	-0.084	0.019
non-overlap	-0.049	0.029	-0.015	0.007	-0.103	-0.062	-0.032	0.013	-0.040	0.031	1.000	-0.111	0.022	-0.038	-0.011	-0.043
overlapping	0.164	0.094	0.049	-0.045	0.074	0.042	0.035	0.154	0.092	-0.081	-0.111	1.000	-0.051	-0.033	-0.012	0.003
bin matrix	-0.042	-0.104	0.031	0.112	0.054	0.118	-0.052	-0.052	-0.065	0.053	0.022	-0.051	1.000	0.087	-0.030	-0.101
universal	0.075	0.012	0.006	-0.044	0.079	0.039	-0.018	0.092	0.090	-0.033	-0.038	-0.033	0.087	1.000	0.147	0.015
random excursion	0.169	-0.032	-0.012	-0.037	0.110	-0.016	0.089	0.300	0.079	-0.084	-0.011	-0.012	-0.030	0.147	1.000	0.690
r.e.variant	0.247	-0.145	0.006	-0.016	0.024	-0.037	0.026	0.427	0.200	0.019	-0.043	0.003	-0.101	0.015	0.690	1.000

Table 2.5: Observed Correlation 3

	serial1	serial2	app. Entropy
serial1	1.000	0.648	0.676
serial2	0.648	1.000	0.001
app. Entropy	0.676	0.001	1.000

Table 2.6: Observed Correlated 4

	random excursion	random excursion variant
random excursion	1.000	0.681
random excursion variant	0.681	1.000

CHAPTER 3

TRANSFORMATIONS

Given a sequence $s \in S$ and a transformation $\varphi : S \longrightarrow s$. We apply a statistical test T to s and $\varphi(s)$. By comparing the $p - values$ $P_T = T(s)$ and $P_{T\varphi} = T(\varphi(s))$ to examine how the test respects the transform φ. This behaviors of tests with respect to the considered transform may give a clue for the similarity of tests.

3.1 Transformation Methods

In this section, the transformation methods are stated. The transformation methods we consider;

- Reversing,
- Binary derivative,
- t-rotation,
- Masking,
- Swapping,
- Flipping.

If complex transformations are applied, the relations between the tests can be found. However, this causes to get away from the intended results. Therefore, the simplest level of transformations is used to observe how the tests react to transformations. After this point of the section, there are explanations of the described transformations and simple examples for each transformation.

3.1.1 Reversing

In this transformation, sequences are reversed. In other words reverse of the sequence $a_1a_2a_3a_4 \ldots a_n$ is the sequence $b_1b_2b_3b_4 \ldots b_n$ where $b_1b_2b_3b_4 \ldots b_n = a_na_{n-1}a_{n-2} \ldots a_1$

Example 3.1. $a_n = 1001011010011110$ then the reverse of a_n is,

$b_n = 0111100101101001$

3.1.2 Binary Derivative

In this transformation, sequences are generated by the XOR of two consecutive bits. In other words, binary derivative of $a_1a_2a_3a_4 \ldots a_n$ is $b_1b_2b_3b_4 \ldots b_n$ where $b_1, b_2, b_3, b_4, \ldots, b_n = a_1 \oplus a_2, a_2 \oplus a_3 \ldots, a_i \oplus a_{i+1}, \ldots, a_{n-1} \oplus a_n, a_1$

Example 3.2. $a_n = 1001011010011110$ then the binary derivative of a_n is

$b_n = 1011101110100011$

Remark 3.1. The generation of last bit can change. For example , in some usages, last bits are fixed with 1, but this can lead lost of information for higher order derivative.

3.1.3 t-Rotation

In this transformation, the place of first t bits of the sequences are changed. They are extracted from the beginning and added at the end. In other words, t-rotation of $a_1, a_2, a_3, a_4, \ldots, a_n$ is $b_1, b_2, b_3, b_4, \ldots, b_n$ where $b_1, b_2, b_3, b_4, \ldots, b_{t+i}, \ldots, b_{n-t}, b_{n-t+1}, \ldots, b_n = a_{t+1}, a_{t+2}, \ldots, a_{t+i}, \ldots, a_n, a_1, \ldots, a_t$

Example 3.3. $a_n =$ **1001**011010011110 then 4-rotation of a_n is,

$b_n =$ 011010011110**1001**

3.1.4 Masking Bits

To mask a sequence S means to add a mask M bitwisely to S. That is masking $S = a_1, a_2, \ldots, a_n$ with $M = m_1, m_2, \ldots, m_n$ produces to $b_1, b_2, \ldots, b_n$ where $b_1, b_2, \ldots, b_n = a_1 \oplus m_1, a_2 \oplus m_2, \ldots, a_n \oplus m_n$ where M is equal to;

- $Mask0 = 111 \ldots$. (This transformation is also called complementation.)
- $Mask1 = 101010 \ldots$,
- $Mask2 = 110011001100 \ldots$,
- $Mask4 = 111100001111000011110000 \ldots$,
- $Mask8 = 11111111000000001111111100000000 \ldots$.

Example 3.4. $a_n = 1001011010011110$ then Mask4 of a_n is

$b_n = 1001011010011110 \oplus 1111000011110000 = 0110011001101110$

3.1.5 Swapping

In this transformation, initially, sequence is divided $2k$ equal length subsequences. First bites of subsequences $2i$, where $i = 0, 1, 2 \ldots, k - 1$,is changed with the first bites of the subsequences $2i + 1$. In this study, k is choosen $\sqrt{n}$.

Example 3.5. $a_n = 1000100111010010$ length of $a_n = 16$ so 4 is the square root of the sequence length so $2k = 8$ then subsequences are

$b_0 = 10$, $b_1 = 00$, $b_2 = 10$, $b_3 = 01$, $b_4 = 11$, $b_5 = 01$, $b_6 = 00$, $b_7 = 10$ then the transformed sequence is

$b_n = 0010001101111000$

3.1.6 Flipping

In this transformation, i^{th} bit of the sequence is flipped. In other words, if i^{th} bit is 0 it is changed by 1 and vice versa. That is, sequences are masked with M where

$$M = 00\ldots \underbrace{1}_{i^{th}\ bite} 00\ldots.$$

3.2 Sensitivities of Randomness Tests

As a result of the conducted studies, the sensitivity of tests against to transformations is measured. Thus, tests that react to transformations in the same way can be considered together, and so a classification can be formed. The reactions of the tests against to transformations are given in the table 3.1. Also, the tables that show the correlations between the tests are given. The tests that are thought to be correlated with each other are grouped as follows:

- Frequency ,block frequency, Cusum1,Cusum2, random excursion and random excursion see table 3.2
- Runs, serial1, serial2, approximate entropy see table 3.3
- There is no correlation between other tests.

As a result of the conducted studies, it is observed that the tests are not generally affected by swapping or flipping only one bit. Also, reversing is not a very distinctive transformation.

In the studies, the connection between run test and frequency test is revealed. Meaning that, the binary derivative transformation results of frequency test is same as the result of run test. Also, in the tables, the reason of having 2 different t-rotation is to obtain different results for the different t values.

Table 3.1: Correlation results of transformed sequences

	original	reversing	bin.der.	t-rotation	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8	swapping	flipping
frequency	1.000	1.000	0.007	1.000	1.000	1.000	0.002	0.003	-0.005	-0.001	1.000	0.991
block frequency	1.000	1.000	0.013	0.965	0.758	1.000	-0.007	-0.009	-0.008	-0.006	1.000	0.996
runs	1.000	1.000	0.001	0.996	1.000	0.961	0.961	0.001	0.166	0.427	0.973	0.992
long run	1.000	1.000	0.038	0.299	1.000	0.058	0.032	0.035	0.014	0.183	0.984	0.993
binary matrix	1.000	1.000	0.112	-0.130	-0.035	0.153	0.129	0.036	0.156	0.089	0.998	0.998
non-overlapping	1.000	1.000	0.377	1.000	1.000	0.016	-0.084	-0.013	0.367	0.115	1.000	1.000
non-overlapping	1.000	0.321	0.071	1.000	1.000	-0.086	0.028	0.119	0.335	-0.022	1.000	1.000
overlapping	1.000	0.789	-0.015	0.984	0.977	0.059	0.034	-0.074	-0.053	-0.010	1.000	1.000
universal	1.000	-0.004	0.229	0.277	-0.125	1.000	0.125	0.048	0.076	-0.045	1.000	0.749
linear compl.	1.000	-0.060	0.364	0.024	-0.151	0.327	0.103	0.128	0.028	-0.106	0.998	0.999
serial1	1.000	1.000	0.459	1.000	1.000	1.000	0.484	0.239	0.114	0.055	0.932	0.965
serial2	1.000	1.000	-0.012	1.000	1.000	1.000	0.480	0.236	0.121	0.059	0.927	0.962
app.entr	1.000	1.000	0.472	1.000	1.000	1.000	0.471	0.232	0.111	0.079	0.983	0.987
cusum1	1.000	1.000	0.009	0.816	0.817	0.907	-0.002	-0.001	-0.003	-0.002	0.815	0.811
cusum2	1.000	1.000	0.010	0.813	0.805	0.907	-0.002	-0.001	0.003	-0.002	0.815	0.811
random excursion	1.000	-0.055	-0.141	0.805	0.610	0.499	0.093	0.084	-0.066	0.002	0.987	0.553
r.excur.variant	1.000	1.000	-0.025	0.867	0.851	0.528	0.011	-0.072	0.060	-0.012	0.995	0.752

Table 3.2: Frequency, Block Frequency,Cusum1, Cusum2, Random Excursion and Random Excursion Variant

	original	reversing	binary derivative	t-rotation	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8	swapping	flipping
frequency	1.000	1.000	0.007	1.000	1.000	1.000	0.002	0.003	-0.005	-0.001	1.000	0.991
block frequency	1.000	1.000	0.013	0.965	0.758	1.000	-0.007	-0.009	-0.008	-0.006	1.000	0.996
cusum1	1.000	1.000	0.009	0.816	0.817	0.907	-0.002	-0.001	-0.003	-0.002	0.815	0.811
cusum2	1.000	1.000	0.010	0.813	0.805	0.907	-0.002	-0.001	0.003	-0.002	0.815	0.811
random excursion	1.000	-0.055	-0.141	0.805	0.610	0.499	0.093	0.084	-0.066	0.002	0.987	0.553
r.excur. variant	1.000	1.000	-0.025	0.867	0.851	0.528	0.011	-0.072	0.060	-0.012	0.995	0.752

Table 3.3: Runs, Serial1, Serial2, Approximate Entropy

	original	reversing	binary derivative	t-rotation	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8	swapping	flipping
runs	1.000	1.000	0.001	0.996	1.000	0.961	0.961	0.001	0.166	0.427	0.973	0.992
serial1	1.000	1.000	0.459	1.000	1.000	1.000	0.484	0.239	0.114	0.055	0.932	0.965
serial2	1.000	1.000	-0.012	1.000	1.000	1.000	0.480	0.236	0.121	0.059	0.927	0.962
app entr	1.000	1.000	0.472	1.000	1.000	1.000	0.471	0.232	0.111	0.079	0.983	0.987

CHAPTER 4

SENSITIVITIES OF TESTS TO BIASED SEQUENCES

A sequence has a bias if the probability of ones or zeros differs from $1/2$. In other words, if a number generator produces 1 with probability $1/2 \mp q$ then sequences has bias q.

When conducting this study, random number generator produces numbers in the range of 0 and $2^{16}-1$ and these are divided into $2^{16}-1$. If the result is between 0.5 and 1, then 0 is assigned. Hence, 1 is generated with the probability of $1/2$ and 0 is generated with the probability of $1/2$. After that, the generated sequences are given bias beginning from 0.001, and so 0 is assigned if the number is between 0.501 and 1. This process continues until bias is 0.3. While some sequences generates 0 $p-value$ even at small biases, binary matrix test does not react biases until 0.25 and linear complexity test does not react any of the biases. In this preliminary work we have assumed that all $p-values$ equally distributed and thus 10 equal box values are created. Therefore, the expected value for each box values is $1/10$. When generating final $p-value$, the number of $p-value$ are counted for each box and then $chi-square$ is applied. Due to the used method, the generated sequence fails serial test, random excursion test and random excursion variant test.

According to the results, the sequence passes frequency test and CUSUM test until the bias is 0.005. Frequency test within a block, test of longest run of ones in a block, approximate entropy test and Maurer's ”universal statistical” test accept the sequence as random until 0.01 bias. On the other hand, the sequence passes run test until 0.03 bias.

According to the results, the most sensitive tests to the biases are non-overlapping and overlapping template matching tests. While overlapping template matching test generates 0 $p-value$ at 0.003 bias, non-overlapping template matching test generates 0 $p-value$ at 0.002 bias.

The probability of random number generator to produce 1 is increased when giving the biases. Therefore, the uniformity characteristics which is mentioned at the beginning is ruined. Based on these results, the reactions of the tests are observed if ones and zeroes are not uniformly distributed.

Table 4.1: Bias Results of Statistical Randomness Tests

	0	.001	.002	.003	.004	.005	.006	.007	.008	.009	.01	.02	.03	.04
frequency	0.111	0.000	0.035	0.023	0.040	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
block frequency	0.940	0.112	0.071	0.108	0.825	0.080	0.259	0.836	0.071	0.533	0.001	0.000	0.000	0.000
run	0.135	0.350	0.031	0.053	0.949	0.113	0.648	0.160	0.460	0.849	0.926	0.426	0.053	0.000
longest run	0.352	0.549	0.245	0.563	0.479	0.361	0.513	0.903	0.096	0.664	0.001	0.000	0.000	0.000
app. Entropy	0.555	0.089	0.767	0.214	0.952	0.746	0.680	0.299	0.014	0.849	0.181	0.000	0.000	0.000
CUSUM	0.076	0.002	0.002	0.080	0.023	0.000	0.009	0.000	0.000	0.000	0.000	0.000	0.000	0.000
non-overlapping	0.682	0.165	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
overlapping	0.328	0.358	0.169	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
universal	0.862	0.085	0.095	0.047	0.399	0.075	0.160	0.701	0.573	0.374	0.004	0.000	0.000	0.000

Table 4.2: Bias Results of Linear Complexity and Binary Matrix Rank Test

	0	.002	.005	.008	.01	.04	.07	.10	.15	.20	.25	.30	.35
linear comp.	0.279	0.721	0.940	0.768	0.082	0.078	0.292	0.122	0.203	0.442	0.593	0.786	0,487
binary matrix	0.622	0.593	0.870	0.602	0.515	0.069	0.862	0.416	0.573	0.451	0.945	0.000	0.000

CHAPTER 5

CONCLUSION

In cryptography, random numbers and random sequences are of crucial importance. Therefore, generation of them should be carefully made. Although it is not possible to mathematically define if a finite sequence or a number is random or not, statistical randomness tests are defined and used for this purpose.

In the literature, there are many statistical tests and test suites. However, the relations between these tests and the reactions which they give to transformations are not investigated. Moreover, the kinds of tests which are sensitive against to biased sequences are not known.

In this study, tests are evaluated by divided into two groups: the tests which can be applied to long sequences and the tests which can be applied to short sequences. Progress is conducted by adhering to these two groups. First part of the study, it is observed that some tests are correlated, some of them are partly correlated or not correlated. The clearest ones of them are the relations between frequency test and CUSUM test; serial1, serial2 and approximate entropy test; and random excursion and random excursion variant tests. Being correlated or not correlated with each other may shed light on generation of new test suites.

Also, sensitivity of tests to transformed sequences is analyzed in this study. Many tests are observed to be insensitive to reversing, flipping and Mask0; however, they are observed to be sensitive of partly sensitive to other transformations. Due to obtained results, some tests are observed to react transformations in same way. Frequency test and CUSUM test which have high correlation give the same reaction to transformations. Also, frequency test within a block, random excursion and random excursion variant test with these two tests react the same transformations. Moreover, run test, serial1, serial2 and approximate entropy test give the same reactions to the same transformations.

According to the results, elimination of some tests is thought not to cause losses in the obtained results when creating the test suites. Therefore, CUSUM test can be removed because it is same as frequency test in terms of the results that it gives. Similarly, run test, one of the serial test and approximate entropy test can be removed. The reason why run test can be removed is that the results of run test are obtained by the results of frequency test after transformations.

Also, based on the conducted studies, it is observed that the some tests are not affected by ruining the uniformity of the sequences and some of them are too late to be affected. Linear complexity test and binary rank test are not affected by the biased sequences. Run test responds to biases later than most tests. Due to the used method, serial test, random excursion test and random excursion variant test are not investigated in this regard.

As a result of the conducted studies, investigating the relation between the tests, the reactions of them against to transformations and the sensitivity of them against to biased sequences are important when classifying the tests. Also, it is concluded that the same results can be obtained due to transformations by decreasing the number of the tests and the number of the produced $p - value$.

In formation of new tests and test suites, classification of tests are great of significance. With new transformations being described later and the transformations in this study, the classification can be made by examining not only correlation between these tests but also correlation between several tests. One of the most important studies which is not included in this thesis but should be investigated later is to determine if the templates are important to non-overlapping and overlapping tests.

REFERENCES

[1] P. M. Alcover, A. Guillamon, and M. d. C. Ruiz, New randomness test for bit sequences., Informatica, 24(3), pp. 339–356, 2013.

[2] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical report, NIST, Gaithersburg, MD, United States, 2010.

[3] W. Caelli, Crypt x package documentation, Technical report, Information Security Research, 1992.

[4] S. W. Golomb, *Shift Register Sequences*, Aegean Park Press, Laguna Hills, CA, USA, 1982, ISBN 978-0894120480.

[5] P. Hellekalek and S. Wegenkittl, Empirical evidence concerning aes, ACM Trans. Model. Comput. Simul., 13(4), pp. 322–333, October 2003, ISSN 1049-3301.

[6] A. Kerckhoffs, La cryptographie militaire, Journal des Sciences Militaires, pp. 161–191, 1883.

[7] D. E. Knuth, *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997, ISBN 0-201-89684-2.

[8] P. L'Ecuyer and R. Simard, Testu01: A Clibrary for empirical testing of random number generators, ACM Trans. Math. Softw., 33(4), August 2007, ISSN 0098-3500.

[9] G. Marsaglia, The marsaglia random number CDROM including the DIEHARD battery of tests of randomness, http://www.stat.fsu.edu/pub/diehard/, 1995.

[10] U. Maurer, A universal statistical test for random bit generators, Journal of cryptology, 5, pp. 89–105, 1992.

[11] K. Pearson, *Notes on regression and inheritance in the case of two parents*, Proceedings of the Royal Society of London, 1895.

[12] M. Robshaw, Stream ciphers, Technical Report TR - 701, RSA Laboratories, July 1994.

[13] A. Ruhkin, Testing randomness: A suite of statistical procedures, Theory of Probability & Its Applications, 45(1), pp. 111–132, 2001.

[14] M. Sönmez Turan, *On statistical analysis of synchronous stream ciphers, Supervisor Assoc. Prof. Dr. Ali Doğanaksoy*, PhD Thesis,Ankara : METU, 2008.

[15] J. Soto and L. Bassham, Randomness testing of the advanced encryption standard finalist candidates, in *NIST IR 6483, National Institute of Standards and Technology*, 1999.

[16] F. Sulak, *Statistical analysis of block ciphers and hash functions, Supervisor Assoc. Prof. Dr. Ali Doğanaksoy*, PhD Thesis,Ankara : METU, 2011.

APPENDIX A

SOME IMPORTANT TABLES

Table A.1: Frequency Test Transformation Result

	original	bin.der.	mask1	mask2	mask4	mask8	flipping
original	1,000	0,007	0,002	0,003	-0,005	-0,001	0,991
bin.der.	0,007	1,000	-0,003	-0,003	-0,002	0,004	0,007
mask1	0,002	-0,003	1,000	-0,004	0,001	-0,001	0,002
mask2	0,003	-0,003	-0,004	1,000	0,000	-0,004	0,003
mask4	-0,005	-0,002	0,001	0,000	1,000	0,000	-0,004
mask8	-0,001	0,004	-0,001	-0,004	0,000	1,000	-0,002
flipping	0,991	0,007	0,002	0,003	-0,004	-0,002	1,000

Table A.2: Frequency Test Within a Block Correlation Results

	original	bin. der.	t-rotation	t-rotation	Mask1	Mask2	Mask4	Mask8	flipping
original	1,000	0,013	0,965	0,758	-0,007	-0,009	-0,008	-0,006	0,996
bin. der.	0,013	1,000	0,012	0,013	0,007	-0,013	0,001	0,003	0,013
t-rotation	0,965	0,012	1,000	0,783	-0,006	-0,009	-0,007	-0,006	0,965
t-rotation	0,758	0,013	0,783	1,000	-0,007	-0,008	-0,006	-0,008	0,757
mask1	-0,007	0,007	-0,006	-0,007	1,000	-0,007	-0,002	-0,008	-0,007
mask2	-0,009	-0,013	-0,009	-0,008	-0,007	1,000	-0,008	-0,008	-0,010
mas4	-0,008	0,001	-0,007	-0,006	-0,002	-0,008	1,000	-0,009	-0,008
mask8	-0,006	0,003	-0,006	-0,008	-0,008	-0,008	-0,009	1,000	-0,006
flipping	0,996	0,013	0,965	0,757	-0,007	-0,010	-0,008	-0,006	1,000

Table A.3: Runs Test Tranformation Results

	original	bin. der.	Mask1	Mask2	Mask4	Mask8	flipping
original	1,000	0,001	0,961	0,001	0,166	0,427	0,992
bin. der.	0,001	1,000	0,001	0,001	-0,001	0,002	0,001
Mask1	0,961	0,001	1,000	0,001	0,160	0,418	0,954
Mask2	0,001	0,001	0,001	1,000	0,162	0,038	0,002
Mask4	0,166	-0,001	0,160	0,162	1,000	0,425	0,165
Mask8	0,427	0,002	0,418	0,038	0,425	1,000	0,425
flipping	0,992	0,001	0,954	0,002	0,165	0,425	1,000

Table A.4: Test for the Longest Run of Ones in a Block Transformation Results

	original	bin. der.	t-rotation	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8
original	1,000	0,038	0,299	1,000	0,058	0,032	0,035	0,014	0,183
bin. der.	0,038	1,000	0,033	0,038	0,039	0,160	0,059	0,014	0,035
t-rotation	0,299	0,033	1,000	0,299	0,052	0,016	0,022	0,025	0,043
t-rotation	1,000	0,038	0,299	1,000	0,058	0,032	0,035	0,014	0,183
Mask0	0,058	0,039	0,052	0,058	1,000	0,035	0,033	0,013	0,186
Mask1	0,032	0,160	0,016	0,032	0,035	1,000	0,021	0,050	0,029
Mask2	0,035	0,059	0,022	0,035	0,033	0,021	1,000	0,037	0,035
Mask4	0,014	0,014	0,025	0,014	0,013	0,050	0,037	1,000	0,017
Mask8	0,183	0,035	0,043	0,183	0,186	0,029	0,035	0,017	1,000
flipping	0,993	0,038	0,299	0,993	0,058	0,032	0,035	0,014	0,182

Table A.5: Binary Matrix Rank Test Transformation Results

	original	bin. der.	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8
original	1,000	0,112	-0,130	0,153	0,129	0,036	0,156	0,089
bin. der.	0,112	1,000	0,151	0,021	0,133	-0,008	0,042	0,017
t-rotation	-0,130	0,151	1,000	0,058	-0,038	-0,023	-0,094	-0,051
Mask0	0,153	0,021	0,058	1,000	0,076	0,133	0,120	0,123
Mask1	0,129	0,133	-0,038	0,076	1,000	0,009	0,231	-0,001
Mask2	0,036	-0,008	-0,023	0,133	0,009	1,000	0,078	0,055
Mask4	0,156	0,042	-0,094	0,120	0,231	0,078	1,000	0,214
Mask8	0,089	0,017	-0,051	0,123	-0,001	0,055	0,214	1,000

Table A.6: Non-overlapping Template Matching Test Transformation Results

	original	bin.der.	mask0	mask1	mask2	mask4	mask8	flipping
normal	1,000	0,377	0,016	-0,084	-0,013	0,367	0,115	1,000
bin.der.	0,377	1,000	0,196	-0,032	0,013	0,200	0,090	0,377
mask0	0,016	0,196	1,000	0,213	0,061	0,012	0,055	0,016
mask1	-0,084	-0,032	0,213	1,000	0,230	-0,127	-0,193	-0,084
mask2	-0,013	0,013	0,061	0,230	1,000	-0,101	-0,093	-0,013
mas4	0,367	0,200	0,012	-0,127	-0,101	1,000	0,042	0,367
mask8	0,115	0,090	0,055	-0,193	-0,093	0,042	1,000	0,115
flipping	1,000	0,377	0,016	-0,084	-0,013	0,367	0,115	1,000

Table A.7: Overlapping Template Matching Test Transformation Results

	original	reversing	bin.dev.	t-rotation	Mask0	Mask1	Mask2	Mask4	Mask8
original	1,000	0,789	-0,015	0,917	0,059	0,034	-0,074	-0,053	-0,010
reversing	0,789	1,000	-0,015	0,836	0,077	0,056	0,016	-0,123	-0,027
bin.dev.	-0,015	-0,015	1,000	-0,003	0,049	0,107	-0,094	0,063	0,014
t-rotation	0,917	0,836	-0,003	1,000	0,091	0,034	-0,040	-0,073	-0,030
Mask0	0,059	0,077	0,049	0,091	1,000	-0,060	0,046	-0,069	0,040
Mask1	0,034	0,056	0,107	0,034	-0,060	1,000	0,028	-0,020	0,033
Mask2	-0,074	0,016	-0,094	-0,040	0,046	0,028	1,000	0,035	0,121
Mask4	-0,053	-0,123	0,063	-0,073	-0,069	-0,020	0,035	1,000	-0,130
Mask8	-0,010	-0,027	0,014	-0,030	0,040	0,033	0,121	-0,130	1,000

Table A.8: Maurer's "Universal Statistical" Test Transformation Results

	original	reversing	bin.dev.	t-rotation	mask0	mask1	mask2	mask4	mask8	flipping
original	1,000	-0,004	0,229	-0,125	1,000	0,125	0,048	0,076	-0,045	0,749
reversing	-0,004	1,000	-0,067	0,038	-0,004	-0,035	-0,164	-0,064	0,033	-0,036
bin.dev.	0,229	-0,067	1,000	0,021	0,229	0,291	0,004	0,057	-0,136	0,150
t-rotation	-0,125	0,038	0,021	1,000	-0,125	-0,023	-0,151	0,118	-0,071	-0,117
mask1	0,125	-0,035	0,291	-0,023	0,125	1,000	0,006	0,050	-0,032	0,021
mask2	0,048	-0,164	0,004	-0,151	0,048	0,006	1,000	0,064	0,027	0,087
mask4	0,076	-0,064	0,057	0,118	0,076	0,050	0,064	1,000	-0,011	0,075
mask8	-0,045	0,033	-0,136	-0,071	-0,045	-0,032	0,027	-0,011	1,000	0,016
flipping	0,749	-0,036	0,150	-0,117	0,749	0,021	0,087	0,075	0,016	1,000

Table A.9: Linear Complexity Test Transfomation Results

	original	reversing	bin.dev.	t-rotation	mask0	mask1	mask2	mask4	mask8	swapping	flipping
original	1,000	-0,060	0,364	0,024	0,327	0,103	0,128	0,028	-0,106	0,998	0,999
reversing	-0,060	1,000	0,054	0,197	0,080	0,044	-0,044	0,049	0,053	-0,062	-0,063
bin.dev.	0,364	0,054	1,000	0,089	0,321	0,018	-0,049	0,048	-0,139	0,370	0,359
t-rotation	0,024	0,197	0,089	1,000	0,035	-0,003	-0,062	0,036	0,056	0,027	0,024
mask0	0,327	0,080	0,321	0,035	1,000	0,158	0,088	0,005	-0,096	0,321	0,329
mask1	0,103	0,044	0,018	-0,003	0,158	1,000	-0,009	-0,081	-0,083	0,105	0,103
mask2	0,128	-0,044	-0,049	-0,062	0,088	-0,009	1,000	0,052	-0,038	0,121	0,126
mask4	0,028	0,049	0,048	0,036	0,005	-0,081	0,052	1,000	0,052	0,029	0,026
mask8	-0,106	0,053	-0,139	0,056	-0,096	-0,083	-0,038	0,052	1,000	-0,110	-0,106
swapping	0,998	-0,062	0,370	0,027	0,321	0,105	0,121	0,029	-0,110	1,000	0,998
flipping	0,999	-0,063	0,359	0,024	0,329	0,103	0,126	0,026	-0,106	0,998	1,000

Table A.10: Approximate Entropy Test Transformation Results

	original	bin. dev	Mask1	Mask2	Mask4	Mask8	flipping
original	1,000	0,472	0,471	0,232	0,111	0,079	0,987
bin. dev	1,000	0,472	0,471	0,232	0,111	0,079	0,987
derivative	0,472	1,000	0,473	0,229	0,110	0,080	0,470
mask1	0,471	0,473	1,000	0,232	0,113	0,081	0,465
Mask2	0,232	0,229	0,232	1,000	0,112	0,061	0,229
Mask4	0,111	0,110	0,113	0,112	1,000	0,089	0,111
Mask8	0,079	0,080	0,081	0,061	0,089	1,000	0,079
flipping	0,987	0,470	0,465	0,229	0,111	0,079	1,000

Table A.11: Random Excursion Test Transofmation Results

	original	reversing	bin.dev.	t-rotation	mask0	mask1	mask2	mask4	mask8	swapping	flipping
original	1,000	-0,055	-0,141	0,610	0,499	0,093	0,084	-0,066	0,002	0,987	0,553
reversing	-0,055	1,000	-0,064	-0,076	0,002	0,034	0,055	0,042	0,161	-0,039	-0,058
bin.dev.	-0,141	-0,064	1,000	-0,043	-0,149	0,012	-0,052	-0,153	-0,021	-0,133	0,047
t-rotation	0,610	-0,076	-0,043	1,000	0,542	0,144	0,002	0,028	0,010	0,613	0,568
mask0	0,499	0,002	-0,149	0,542	1,000	0,024	-0,039	0,026	0,051	0,490	0,453
mask1	0,093	0,034	0,012	0,144	0,024	1,000	-0,138	-0,025	0,014	0,096	0,126
mask2	0,084	0,055	-0,052	0,002	-0,039	-0,138	1,000	-0,001	0,043	0,073	0,032
mask4	-0,066	0,042	-0,153	0,028	0,026	-0,025	-0,001	1,000	-0,073	-0,071	-0,061
mask8	0,002	0,161	-0,021	0,010	0,051	0,014	0,043	-0,073	1,000	-0,020	0,006
swapping	0,987	-0,039	-0,133	0,613	0,490	0,096	0,073	-0,071	-0,020	1,000	0,566
flipping	0,553	-0,058	0,047	0,568	0,453	0,126	0,032	-0,061	0,006	0,566	1,000

Table A.12: Random Excursion Variant Test Transformation Results

	original	reversing	bin.dev.	t-rotation	mask0	mask1	mask2	mask4	mask8	swapping	flipping
original	1,000	-0,013	-0,118	0,574	0,566	0,190	0,000	0,131	-0,083	0,949	0,450
reversing	-0,013	1,000	-0,023	0,018	0,015	-0,043	0,096	-0,020	-0,045	0,009	-0,069
bin.dev.	-0,118	-0,023	1,000	-0,085	-0,011	-0,031	-0,078	-0,075	-0,058	-0,082	-0,123
t-rotation	0,574	0,018	-0,085	1,000	0,526	0,156	0,025	0,122	0,012	0,589	0,644
mask0	0,566	0,015	-0,011	0,526	1,000	0,082	-0,001	0,103	-0,116	0,515	0,537
mask1	0,190	-0,043	-0,031	0,156	0,082	1,000	-0,030	0,016	0,016	0,200	0,144
mask2	0,000	0,096	-0,078	0,025	-0,001	-0,030	1,000	-0,017	-0,020	0,001	-0,002
mask4	0,131	-0,020	-0,075	0,122	0,103	0,016	-0,017	1,000	-0,096	0,132	0,044
mask8	-0,083	-0,045	-0,058	0,012	-0,116	0,016	-0,020	-0,096	1,000	-0,092	-0,015
swapping	0,949	0,009	-0,082	0,589	0,515	0,200	0,001	0,132	-0,092	1,000	0,425
flipping	0,450	-0,069	-0,123	0,644	0,537	0,144	-0,002	0,044	-0,015	0,425	1,000

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Akcengiz, Ziya
Nationality: Turkish
Date and Place of Birth: 1989, Ankara
Marital Status: Single
Phone: +905064240038

EDUCATION

Degree	**Institution**	**Year of Graduation**
B.S.	Mathematics	2012
High School	Kalaba Anadolu Lisesi	2007

PROFESSIONAL EXPERIENCE

Year	**Place**	**Enrollment**
2013-	Middle East Technical University	Project Assistant