Bulletin of the *Transilvania* University of Braşov • Vol 4(53) No. 2 - 2011
Series III: Mathematics, Informatics, Physics, 129-140

STATISTICAL TOOLS USED IN CRYPTOGRAPHIC EVALUATION

Adela GEORGESCU [1] **Ruxandra Florentina OLIMID** [2] **Emil SIMION**[3]

Communicated to:
The Seventh Congress of Romanian Mathematicians, June 29 - July 5, 2011, Braşov, Romania

Abstract

This paper gives an overview of some statistical tools used in cryptography from ancient times to nowadays. Statistical tests are very useful in the cryptanalysis of pen and paper ciphers, offering a good tool for identification of the enciphering system used in a cryptogram and of the statistical structure of the text, leading to finding the plaintext. NIST statistical tests were used in the evaluation of the AES candidates. Also, linear and differential cryptanalysis for block ciphers are based on a statistical approach.

2000 *Mathematics Subject Classification:* 62A01, 62G10, 94A60, 94A15.
Key words: cryptography, cryptanalysis, statistical test, decision rule, ciphers.

1 Introduction

The use of statistical testing in cryptography seems to date back to the first millennium after Christ, due to Abu Yusuf Yaqub ibn Ishaq al-Sabah Al-Kindi (801-873) who was a pioneer in cryptanalysis and cryptology (S. Singh [21]). He is credited with developing a method where variations in the frequency of the occurrence of letters could be analyzed and exploited to break ciphers (i.e. cryptanalysis by frequency analysis).

Much later, in 1863, Friedrich Kasiski published a 95-page book on cryptography "Secret writing and the Art of Deciphering". This was the first published account of a procedure for attacking polyalphabetic substitution ciphers, especially the Vigenere cipher. The method relied on the analysis of gaps between repeated fragments in the ciphertext; such analysis can give hints as to the length of the key used (D. Khan [7]).

Later on, during World War II, we refer to code talkers who transmitted secret tactical messages over radio communications nets using formal or informally developed codes built upon their native languages. The name code talkers is strongly associated with bilingual Navajo speakers specially recruited during WW II by the Marines to serve in their standard communications units in the Pacific Theater (N. Aaseng [1]).

[1]Faculty of Mathematics and Computer Science, University of Bucharest, Romania
[2]Faculty of Mathematics and Computer Science, University of Bucharest, Romania
[3]University Politehnica of Bucharest, Romania

The examples mentioned before show the usage of statistics in early cryptography. The rest of the paper presents in more details some of the utilization of statistical tools in the field. Section 2 introduces the basics of statistical testing, giving the example of the frequency test and indicating some of the used statistical tools. Applications of statistics to pen and pencil ciphers, as solving a substitution cipher or different specific test functions are highlighted in Section 3. In a similar way, Section 4 deals with the statistical usage in evaluating and cryptanalysis the block ciphers. Finally, in Section 5 we conclude.

2 Statistical testing

2.1 The basics of statistical testing

A statistical test provides a mechanism for making decisions, using data, about a binary sequence $\mathbf{x} \in \{0, 1\}$ which usually represents the output of a source. The aim is to decide whether there is enough evidence to "reject" a conjecture or hypothesis about the sequence. The hypothesis to be tested represents an assumption that may or may not be true and it is called a statistical hypothesis.

A statistical test requires a pair of hypotheses regarding the sequence to be tested:

- the null hypothesis H_0 - the sequence $\mathbf{x}$ is produced by a binary memory less source: $Pr(X = 1) = p_0$ and thus $Pr(X = 0) = 1 - p_0$ (in this case we say that the sequence does not present any predictable component);
- the alternative hypothesis H_1 - the sequence $\mathbf{x}$ is produced by a binary memory less source: $Pr(X = 1) = p_1$ and $Pr(X = 0) = 1 - p_1$ with $p_0 \neq p_1$, (in this case we say that the sequence presents a predictable component regarding the probability p).

Two types of errors can result from a statistical test:

- the first order error α - the risk of rejecting the null hypothesis when it is in fact true, also called the level of significance

  α = Pr(reject H_0 | H_0 is true) = 1 - Pr (accept H_0 | H_0 is true);
- the second order error β - the risk of failing to reject (accepting) the null hypothesis when it is in fact false

  β = Pr(accept H_0 | H_0 is false) = 1 - Pr (reject H_0 | H_0 is false).

These two errors can't be minimized simultaneously since the risk β increases as the risk α decreases and vice versa (Neymann-Pearson tests minimize the value of β for a given α). The analysis plan of the statistical test includes decision rules for rejecting the null hypothesis. These rules are described in two ways:

- **Decision based on confidence intervals** An example of decision rule is the following: for a fixed value of α we find the confidence region for the test statistic and check if the test statistic value is in the confidence region. The confidence region is

computed using the quantiles of order $\frac{\alpha}{2}$ and $1-\frac{\alpha}{2}$(for example the quantile u_α of order α is defined by $Pr(X < u_\alpha) = \alpha$;

- **Decision based on P-value** Let us denote f_{test} the value of test function. Another equivalent method is to compare the $P - value = Pr(X < f_{test})$ with α and decide the randomness if $P - value \geq \alpha$.

2.2 An example of statistical test: Frequency test

Let us show an example of a well-known statistical test, called the *frequency test*. This is used to test the randomness of a sequence of zeroes and ones. In fact, it tests the closeness of the proportion of ones to 0.5.

Input: binary sequence $s^N = s_1, ..., s_N$ Denote by $p_0 = Pr(S = 1)$ the probability of occurrences of symbol 1, and $q_0 = 1 - p_0 = Pr(S = 0)$ the probability of occurrences of symbol 0.

Output: Accept or reject the randomness of the sequence, meaning that the sequence s^N is the output of a symmetric binary source with $Pr(S = 1) = p_0$, the alternative hypothesis being $Pr(S = 1) = p_1 \neq p_0$.

STEP 0. Read the sequence s^N and the rejection rate α.

STEP 1. Compute the test function:

$$f(s^N) = \frac{1}{\sqrt{np_0q_0}} \left(\sum_{i=1}^{N} s_i - Np_0 \right).$$

STEP 2. If $f(s^N) \in [u_{\frac{\alpha}{2}}, u_{1-\frac{\alpha}{2}}]$ then accept the hypothesis of randomness, otherwise reject it (remember that $u_{\frac{\alpha}{2}}$ and $u_{1-\frac{\alpha}{2}}$ are the quantiles of order $\frac{\alpha}{2}$ and $1-\frac{\alpha}{2}$ of the normal distribution).

STEP 3. Compute the second error probability (probability of acceptance or a false hypothesis):

$$\beta = 1 + \Phi\left(\left(u_{\frac{\alpha}{2}} - \frac{N(p_1 - p_0)}{\sqrt{Np_0q_0}} \right) \sqrt{\frac{p_0q_0}{p_1q_1}} \right) - \Phi\left(\left(u_{1-\frac{\alpha}{2}} - \frac{N(p_1 - p_0)}{\sqrt{Np_0q_0}} \right) \sqrt{\frac{p_0q_0}{p_1q_1}} \right).$$

2.3 Some statistical tools

We present in the following some existing tools (in the area of cryptography) which have the possibility to perform statistical tests:

- NIST Statistical Test Suite (STS);
- Donald Knuth describes in his book [10] several empirical tests;
- The Crypt-XS suite of statistical tests developed by researchers at the Information Security Research Centre at Queensland University of Technology in Australia;

- The DIEHARD suite of statistical tests developed by George Marsaglia;
- CrypTool developed by the universities of Siegen and Darmstadt.

The NIST Statistical Test Suite (STS) 800-22 is a statistical testing package developed by the National Institute for Standards and Technology published in NIST SP 800-22 and it consists of 16 statistical tests based on confidence intervals. The tests detect a general class of defects of (pseudo)random generators. We must remark the fact that NIST 800-22 was one of the cryptographic tools which were involved in the evaluation of the candidates for Advanced Encryption Standard (FIPS PUB 197) (see Section 4.2). The NIST evaluation procedure is the following:

1. Compute the *test statistic*;
2. Compute its $p-value$;
3. Compare the $p-value$ to *const* (where *const* is chosen in the $(0.001, 0.01]$ interval): **success** whenever $p-value > const$ and **failure** whenever $p-value < const$.

3 Applications of statistics to pen and paper ciphers

3.1 Types of encryption systems

We start this section with the presentation of statistical tests applied to pen and paper ciphers. We will consider the following classes of ciphers:

- *monoalphabetic unilateral substitution systems using standard cipher alphabets* - each plaintext letter is replaced by one ciphertext letter using two equivalent alphabets in cyclic or reverse order;
- *monoalphabetic unilateral substitutions systems using mixed cipher alphabets* - each plaintext letter is replaced by one ciphertext letter using two equivalent alphabets in pseudorandom or random order;
- *monoalphabetic multilateral substitutions systems* - each plaintext letter is replaced by one or two cipher letters or numbers using a equivalence of the alphabets;
- *polygraphic substitution systems* - each plaintext digram (or trigram) is replaced, via a table of equivalence, with a ciphertext digram (or trigram);
- *polyalphabetic substitution systems* - is a generalization of the monoalphabetic systems;
- *transpositions systems* - in these systems we permute the letters or words of the plaintext.

3.2 Solving a substitution cipher

William Friedman (born in Kishinev, 1981) formulated some fundamental operations in order to obtain the solution to cryptograms belonging to the above ciphers: find the language employed in the plaintext, find the general cryptographic system used, reconstruct the specific key in the case of a cipher system, or the reconstruction of, partial or complete, code book, in the case of a code system or both in the case of an enciphered code system and finally, reconstruct the plaintext.

According to the Navy Department OP-20-G Course in Cryptanalysis, in order to find the solution of a substitution cipher one must go through the following stages:

- **analysis of the cryptogram(s)**: preparation of a frequency table, search for repetitions, determination of the type of system used, preparation of a work sheet, preparation of individual alphabets (if more than one), tabulation of long repetitions and peculiar letter distributions;
- **classification of vowels and consonants** by a study of: frequencies, spacing, letter combinations, repetitions;
- **identification of letters**: breaking in or wedge process, verification of assumptions, filling in good values throughout messages, recovery of new values to complete the solution;
- **reconstruction of the system**: rebuilding the enciphering table, recovery of the key(s) used in the operation of the system, recovery of the key or keyword(s) used to construct the alphabet sequences.

3.3 Test functions as statistical tools

In the following, we address the problem of identification of the enciphering system used in a cryptogram. The cryptanalysis method is based on computing statistical estimators for some test functions. The resulting estimators are then compared with the values for each language. It is important to note that the plaintext must be homogeneous (only one language involved). Otherwise, by a suitable procedure, the text can be split in homogeneous parts and apply the procedure for each part. This test allows identifying the ciphering model and the statistical structure of the plaintext, which will lead to finding the solution.

Let us denote by $T = (t_1, ..., t_M)$ and $T^{'} = (t_1^{'}, ..., t_M^{'})$ two sequences of length M over the same vocabulary Z_N (of size N). Denote by m_i and $m_i^{'}$ the frequencies of occurrences of the i^{th} letter from the source alphabet in the sequence T respectively $T^{'}$. Thus we have:

$$\sum_{i=1}^{N} m_i = M$$

and

$$\sum_{i=1}^{N} m_i^{'} = M.$$

The decision functions *Kappa, Chi, Psi* and *Phi* are described in the following.

The Kappa function

Coincidence counting (Kappa function) is the technique (invented by William F. Friedman) of putting two texts side-by-side and counting the number of times that identical letters appear in the same position in both texts. Thus

$$Kappa(T, T^{'}) = \frac{\sum_{i=1}^{M} \delta(t_i, t_i^{'})}{M}.$$

where δ is *Kronecker's symbol.* We have two theorems regarding invariance of the Kappa function.

Theorem 1. *For all polyalphabetic ciphers, the Kappa of two texts of equal length, encrypted with the same key, is invariant.*

Theorem 2. *For all transpositions, the Kappa of two texts of equal length, encrypted with the same key, is invariant*

The Chi function

The *Chi function* is defined by:

$$Chi(T, T^{'}) = \frac{\sum_{j=1}^{N} m_i m_i^{'}}{M^2}.$$

Theorem 3. *For all monoalphabetic ciphers the Chi of two texts of equal length, encrypted with the same key, is invariant.*

Theorem 4. *For all transpositions, the Chi of two texts of equal length, encrypted with the same key, is invariant.*

The Psi function

The *Psi function* is related to the *Chi* function and is defined by:

$$Psi(T) = Chi(T, T).$$

We also have similar invariance theorems:

Theorem 5. *For all monoalphabetic ciphers the Psi of texts is invariant.*

Theorem 6. *For all transpositions, the Psi of texts is invariant.*

We have the *Kappa − Chi theorem*:

Theorem 7. *For two texts T and T' over the same vocabulary and the same length the value $Chi(T,T')$ is the arithmetic mean of all $Kappa(T^{(i)},T')$ ($T^{(i)}$ is the text T shifted cyclically by i positions to the right and the connection formula is $t_j^* = t_{(j-i-1) \bmod M+1}$ for $j = 1,...,M$):*

$$Chi(T,T') = \frac{1}{M}\sum_{i=0}^{M-1} Kappa(T^{(i)},T').$$

In the situation when $T \equiv T'$ we obtain the *Kappa − Psi theorem.*

The Phi function

The *Phi* functions are defined by:

$$Phi(T) = \frac{\sum_{j=1}^{N} m_i(m_i-1)}{M(M-1)}.$$

Theorem 8. *For all monoalphabetic ciphers the Phi of text is invariant.*

Theorem 9. *For all transpositions ciphers the Phi of text is invariant.*

We have the *Kappa − Phi theorem*:

Theorem 10. *For a text T of length M over a vocabulary Z_N the value of $Phi(T)$ is the average of all $Kappa(T^{(i)},T)$ ($T^{(i)}$ is the text T shifted cyclically by i positions to the right):*

$$Phi(T) = \frac{1}{M-1}\sum_{i=1}^{M-1} Kappa(T^{(i)},T).$$

The test functions presented above are invariant under a large class of cipher systems like transpositions and substitutions and can be used in the identification of the plain text language, cipher system used for encryption, key recovery and plain text recovery. The Kappa function is used in cipher system identification and in language identification (this function is a reference test for language identification). The procedure of language identification is also based on the comparison of the values of Psi and Phi of the cipher text with the values of Psi and Phi of each language (this functions are confirmatory tests at this time). Phi is useful because rare letters have no contribution to the decision procedure. The function Chi is used in *isolog* attacks (different texts encrypted with the same key). Kappa, Chi, Psi and Phi tests can be also applied on digrams and trigrams etc.

4 Application of statistics to block ciphers

4.1 Preliminary notions

A block cipher is a symmetric key cipher (with no memory and time-invariant) that operates on fixed-length groups of bits, called *blocks*. In general, block ciphers are constructed by repeating the same function. Each iteration is called a *round* and the applied function is named the *round function*.

For a r-rounds cipher, consider the following notations: N the block length, K the key length, X the plaintext, Y the ciphertext, $X^{(i)}$ the input in the round i, $Y^{(i)}$ the output in round i, $Z^{(i)}$ the key in round i, $1 \leq i \leq r$.

4.2 Application to AES standardization process

The output of an encryption system should be computationally undistinguished from a random source. Statistical tests are used in order to evaluate the randomness of the output.

This represented one of the criteria used for the selection of the AES (Advanced Encryption Standard) algorithm. Papers [19], [20] describe how the output of the candidate algorithms were tested for randomness.

Different sets of data were used as input in order to examine the sensitivity of the algorithms in different conditions: *128-Bit Key Avalanche and Plaintext Avalanche* (to examine the randomness of the output to changes in the key, respectively plaintext while maintaining the plaintext, respectively the key to all-zero), *Plaintext/Ciphertext Correlation*, (to examine the correlation of plaintext/ciphertext pairs), *Cipher Block Chaining Mode* (to examine the sensitivity in CBC mode for all-zero initialization vector IV, all-zero plaintext and random key value), *Low Density Plaintext, Low Density 128-Bit Keys, High Density Plaintext and High Density 128-Bit Keys* (to test the randomness in extreme weight difference between the appearance of 0's and 1's). A *Random Plaintext/Random 128-Bit Keys* set of data was also applied for the candidates.

Multiple NIST statistical tests were applied to each algorithm using the sets of data previously mentioned, on different platforms and implementations. The decision rule was based on confidence interval with the level of significance $\alpha = 0.01$. 6 out of 15 candidates did not pass all the tests, displaying deviation from randomness.

4.3 Differential cryptanalysis

Differential cryptanalysis is a chosen-plaintext attack based on statistical approach that was introduced by E. Biham and A. Shamir at Crypto '90 [3]. It analyses the effect of particular differences in plaintext pairs according to the difference of the resultant ciphertext pairs. It can be applied to a iterated cipher with a weak round function, assuming that the subkeys used in the r-rounds of the encryption are chosen independently and uniformly at random (i.u.r.). An independent key is a list of subkeys which is not necessarily derived from the key scheduling algorithm [3].

Definition 1. *[12] An i-round differential is defined as a couple (α, β), where α is the difference of a pair of distinct plaintexts X and X^*, and β is the possible difference for the resulting i-th round outputs $Y(i)$ and $Y^*(i)$. The probability of a i-round differential (α, β) is the difference $\Delta Y(i)$ given the plaintext pair (X, X^*) with $\Delta X = \alpha$ when the plaintext X and the round subkeys $Z^{(1)}$... $Z^{(i)}$ are i.u.r. and is denoted by: $P(\Delta Y(i) = \beta | \Delta X = \alpha)$.*

Differentials are then used to determine the most probable key (in the last round). The basic procedure of performing a differential cryptanalysis attack is [12]:

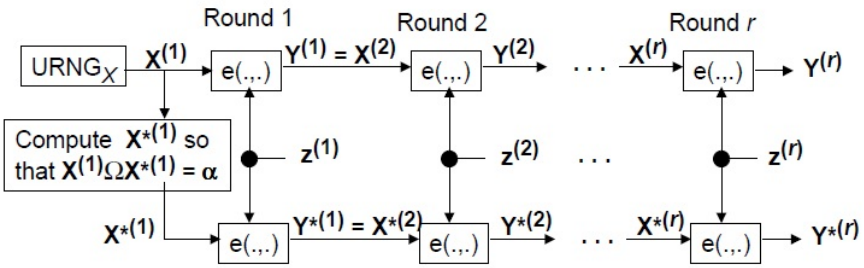

Figure 1: Differential cryptanalysis (URNG = Uniformly Random Number Generator; Ω = the appropriate notion of difference) [13].

STEP 1. Choose plaintext X uniformly at random and compute X^* so that $\Delta X = \alpha$. Then, submit them both for encryption with the key Z;

STEP 2. From the resultant ciphertext $Y(r)$ and $Y^*(r)$, find all values $Z^{(r)}$ of the last round subkey corresponding to the anticipated difference $\Delta Y(r-1) = \beta$. Add 1 to the count of the number of appearances of each such value $Z^{(r)}$;

STEP 3. Repeat previous steps until one key $Z^{(r)}$ is counted significantly more often than the others. This is considered the last round subkey.

The required number of plaintext/ciphertext pairs represents the measure of security of the cipher against the differential attack.

In order to evaluate the vulnerability of this kind of attack, the probabilities are computed for different independently random subkeys. Note that in the differential attack, the key (and therefore the subkeys) are fixed and only the plaintext can be chosen. As was pointed out by Lai, Massey and Murphy, the theory of differential cryptanalysis rests on the *Hypothesis of Stochastic Equivalence*: For a (r-1) differential (α, β): $P(\Delta Y(r-1) = \beta | \Delta X = \alpha) \approx P(\Delta Y(r-1) = \beta | \Delta X = \alpha, Z^{(1)} = \omega_1, ..., Z^{(r-1)} = \omega_{r-1})$ for almost all subkey values $(\omega_1, ..., \omega_{r-1})$ [12].

The introduced hypothesis states that the probabilities in the attack model and in the analyzed model are approximately the same. Under this assumption, keeping in mind that there are 2^N possible values for $\Delta Y(r-1)$, a r-round round cipher with independent subkeys is vulnerable to the differential attack iff the round function is weak and there exists a $(r-1)$-round differential (α, β) such that $P(\Delta Y(r-1) = \beta | \Delta X = \alpha) \gg 2^{-N}$. The first condition assures that the second step from the basic attack procedure can be done, while the second condition assures the succes of the third step.

Different methods have been developed starting from the idea of the differential attack. For example, L.Knudsen introduced 2 variants of differential cryptanalysis: *impossible differential cryptanalysis* that tracks the differences that are impossible to appear (the possibility equals 0) [8] and *Truncate differential cryptanalysis* that considers differences that are only partially determined, predicting only some bits and not the full block [9].

Examples of partial or total differential attacks (or variants) include DES (Data En-

cryption Standard) [4], PES (Proposed Encryption Standard) [12], IDEA (International Data Encryption Algorithm) [8], [2], FEAL (Fast Data Encipherment Algorithm) [5].

4.4 Linear cryptanalysis

Linear cryptanalysis is a known-plaintext attack based on a statistical approach that was introduced by Matsui at Eurocrypt '92 [16]. It finds a linear relation that holds in probability between some bits of the plaintext X, ciphertext Y and key Z. The technique allows the attacker to determine some bits of the key and to compute the remaining bits by other means (for example brute force). It can be applied to an iterated cipher with a weak round function, assuming that the plaintexts and the subkeys had been chosen independently and uniformly at random.

C. Harpes, G. Kramer and J. Massey generalized Matsui's linear cryptanalysis [6] by replacing linear expression with I/O sums, defined based on the notion of imbalance:

Definition 2. *Let S be a binary random variable. Then, S is balanced if $P(S = 0) = P(S = 1) = 0.5$. The imbalance of S is defined as $I(S) = 2|P(S = 0) - 0.5|$. The conditionally imbalanced of S given by $Z = z$ is $P(S|Z = z) = 2|P(S = 0|Z = z) - 0.5|$. The average conditioned imbalance of S given by Z is: $I(S|Z) = \sum_Z I(S|Z = z)P(Z = z)$.*

Definition 3. *An i multi-round I/O sum is $S_{1...i} = f_1(X^{(1)}) \oplus g_i(Y^{(i)})$, where f_i is a balanced binary-valued function on the input, g_i is a balanced binary-valued function on the output and h_i is a balanced binary-valued function on the key.*

The basic procedure of performing a linear cryptanalysis attack is [6]:

STEP 1. Find a $(r-1)$ multi-round I/O sum $S_{1...(r-1)} = f_1(X^{(1)} \oplus g_{r-1}(Y^{(r-1)}))$ with large imbalance;

STEP 2. For each possible sets of bits in subkey $Z^{(r)}$ that affect the value of $g_{r-1}(Y^*)$:

- for each plaintext X, decrypt the corresponding ciphertext Y for only one round of encryption to obtain Y^*;
- compute $S = f_1(X) \oplus g_{r-1}(Y^*)$, which represents the value of $S_{1..(r-1)}$ assuming that the key was guessed correctly;
- compute the empirical imbalance of these values;

STEP 3. Decide on the key $Z^{(r)}$ that has the greatest empirical imbalance.

Linear cryptanalysis is more effective than differential analysis on block ciphers such as DES [14], [15] and FEAL [16], where the key is inserted into the round through bit-by-bit modulo addition.

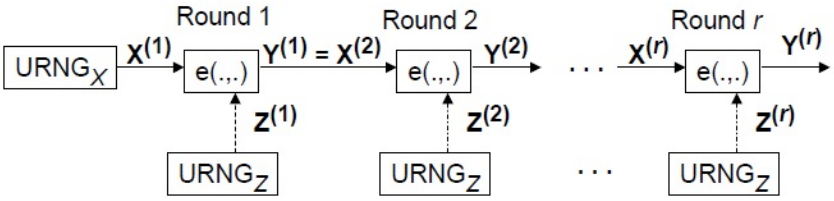

Figure 2: Linear cryptanalysis (URNG = Uniformly Random Number Generator)[13].

5 Conclusions

The paper highlights the applicability of statistics in cryptography. Different techniques of evaluation, testing and cracking cryptographic systems from ancient times until present are possible due to statistical tests and implementing statistical tools.

We give the basics of statistical testing, exemplify through the frequency test and also present some of the existing statistical tools.

We merely emphasize the applicability of statistics to cracking pen and pencil ciphers by the use of statistical tests. Finally, we present the AES candidates' evaluation by applying randomness tests and the development of new techniques based on a statistical approach, such as differential and linear cryptanalysis.

References

[1] Aaseng, N., *Navajo Code Talkers: Americas Secret Weapon in World War II*, New York: Walker & Company, 1992.

[2] Biham, E., Dunkelman, O. and Kellner, N., *A New Attack on 6-round IDEA*, Proceedings of FSE, 2007, pp. 211-224.

[3] Biham E. and Shamir, A., *Differential Cryptanalysis of DES-like Cryptosystems*, Advances in Cryptology, CRYPTO'90, 1990.

[4] Biham E. and Shamir, A., *Differential Cryptanalysis of the Data Encryption Standard*, Springer Verlag, 1993.

[5] Biham E. and Shamir, A., *Differential Cryptanalysis of Feal and N-Hash*, Advances in Cryptology, EUROCRYPT '91, 1991.

[6] Harpes, C., Kramer G.C. and Massey, J.L., *A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma*, Advances in Cryptology, EUROCRYPT '95, 1995.

[7] Kahn, D., *The Codebreakers - The Story of Secret Writing*, revised ed, Scribner, 1996.

[8] Knudsen, L., *DEAL - A 128-bit Block Cipher*, NIST AES Proposal, 1998.

[9] Knudsen, L., *Truncated and Higher Order Differentials*, 2nd International Workshop on Fast Software Encryption (FSE), Leuven, LNCS, Springer 1008, Springer-Verlag, 1994, 196-211.

[10] Knuth, D. E., *The art of computer programming, vol 2: Seminumerical algorithms*, 3rd edition, Addison Wesley, Reading, Massachusetts, 1998.

[11] Lai, X., *On the Design and Security of Block Ciphers*, ETH Series in Information Processing (Ed. J. L. Massey), **1**, 1992.

[12] Lai, X. Massey J.L. and Murphy, S., *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology, CRYPTO '91, 1991.

[13] Massey, J.L., *Design and Analysis of Block Ciphers - Course material*, *http://www.win.tue.nl/wsk/eidma/courses/minicourses/massey/MC-CIC-7-sheets.html*

[14] Matsui, M., *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, EUROCRYPT '93, 1993.

[15] Matsui, M., *The First Experimental Cryptanalysis of the Data Encryption Standard*, Advances in Cryptology, CRYPTO '94, 1994.

[16] Matsui, M. and Yamagishi, A., *A New Method for Known Plaintext Attack of FEAL Cipher*, Advances in Cryptology, EUROCRYPT '92, 1992.

[17] Oprina, A., Popescu, A. Simion E. and Simion, Gh., *Walsh-Hadamard randomness test and new methods of test results integration*, Bulletin of Transilvania University of Braov, **2(51)** Series III, 2009.

[18] Popescu, A., Preda V. and Simion, E., *Cryptanalysis. Techniques and mathematical methods*, University of Buchrarest, Bucharest, 2004,ISBN 973575975-6.

[19] Soto, J., *Randomness Testing of the Advanced Encryption Standard Candidate Algorithms*, National Institute of Standards and Technology.

[20] Soto, J. and Bassham, L., *Randomness Testing of the Advanced Encryption Standard Finalist Candidates*, National Institute of Standards and Technology.

[21] Singh, S., *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*,Anchor Books, 1999, ISBN 978-0385495325.