IRSTI 81.93.29

10.51889/2959-5894.2024.87.3.014

A. Khompysh[1], N.A. Kapalova[1*], D.S. Dyusenbayev[1], V.A. Varennikov[1]

[1]Institute of Information and Computational Technologies, Almaty., Kazakhstan
[*]*e-mail: nkapalova@mail.ru*

STUDY OF THE STATISTICAL SECURITY OF THE AL04 ENCRYPTION ALGORITHM

Abstract

Considering that cryptographic algorithms are among the most reliable methods for protecting information in information systems, assessing their cryptographic strength plays a significant role. For this purpose, comprehensive studies are conducted, and one of the primary characteristics of such an assessment is the statistical security of the obtained ciphertexts. This article investigates the statistical security of the block cipher algorithm AL04, developed in the Information Security Laboratory. The algorithm was implemented in software, and the resulting ciphertexts were analyzed using the test sets of D. Knuth and NIST, as well as checked against the avalanche effect criterion (average number of output bits, degree of completeness, degree of avalanche effect, degree of strict avalanche criterion). The statistical tests used are the main tests in the works of many researchers and determine the properties of sequence randomness with high accuracy. The study found that AL04 does not have deviations in the sequences obtained using the algorithm. Thus, it was established that the algorithm possesses high statistical security.

Keywords: information security, cryptography, algorithm, NIST tests, D. Knuth tests, encryption, key, decryption, S-box.

А. Хомпыш[1*], Н.А. Капалова[1], Д.С. Дюсенбаев[1], В.А. Варенников [1]
[1]Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан

«AL04» ШИФРЛАУ АЛГОРИТМІНІҢ СТАТИСТИКАЛЫҚ ҚАУІПСІЗДІГІН ЗЕРТТЕУ

Аңдатпа

Криптографиялық алгоритмдер ақпараттық жүйелердегі ақпаратты қорғаудың ең сенімді әдістерінің бірі екенін ескере отырып, олардың криптографиялық күшін бағалау маңызды рөл атқарады. Осы мақсатта әр түрлі зерттеулер жүргізіледі, ең бірінші бағаланатын сипаттамалардың бірі алынған шифр мәтіндердің статистикалық қауіпсіздігі. Бұл мақалада ақпаратттық қауіпсіздік зертханасында жасалынған AL04 блокты шифрлау алгоритмінің статистикалық қауіпсіздігі зерттелінді. Алгоритмді зерттеу үшін бағдарламалық жүзеге асырылды. Алынған шифрмәтіндер Д.Кнуттың сынақтар жиынтығы, NIST тесттері арқылы зерттеліп, лавиндік әсерінің критерийі тексерілді (шығыс биттерінің орташа саны, тығыздық дәрежесі, лавиндік әсерінің дәрежесі, қатаң лавиндік критерийінің дәрежесі). Қолданылатын бұл статистикалық сынақтар тізбектердің кездейсоқтық қасиеттерін нақты анықтайтын зерттеушілердің жұмысында кеңінен қолданылатын негізгілері болып табылады. Зерттеу нәтижелері бойынша AL04 алгоритмді қолдану арқылы алынған тізбектерде ауытқулар жоқ екені анықталды. Осылайша, алгоритм жоғары статистикалық қауіпсіздікке ие екендігі анықталды.

Түйін сөздер: ақпараттық қауіпсіздік, криптография, алгоритм, NIST сынақтары, Д.Кнут сынақтары, шифрлау, кілт, керішифрлау, S блок.

А. Хомпыш[1*], Н.А. Капалова[1], Д.С. Дюсенбаев[1], В.А. Варенников [1]
[1]Институт информационных и вычислительных технологий, г.Алматы, Казахстан

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ АЛГОРИТМ ШИФРОВАНИЯ «AL04»

Аннотация

Учитывая, что криптографические алгоритмы являются одним из наиболее надежных методов защиты информации в информационных системах, оценка их криптостойкости играет немаловажную роль. Для этого проводятся разносторонние исследования, один из первых характеристик который оценивается это статистическая безопасность полученных шифртекстов. В данной статье исследован статистическая безопасность алгоритма блочного шифрования AL04, разработанного в лаборатории информационной безопасности. Для проведения исследования алгоритм был программно реализован. Полученные шифртексты были изучены с помощью наборов тестов Д. Кнута, тестов NIST, а также проверены критерий лавинного эффекта (среднее число выходных битов, степень полноты, степень лавинного эффекта, степень строгого лавинного критерия). Эти используемые статистические тесты являются основными, широко используемыми в работах исследователей, которые четко определяют свойства случайности последовательностей. По результатам исследования установлено, что AL04 не имеет отклонений в последовательностях, полученных с помощью алгоритма. Таким образом, было установлено, что алгоритм обладает высокой статистической безопасностью.

Ключевые слова: информационная безопасность, криптография, алгоритм, тесты NIST, тесты, Д.Кнут, шифрование, ключ, расшифрование, S блок.

Main provisions

The proposed «AL04» encryption algorithm is used in the military field for protecting information in HF radio communication systems. The proposed algorithm utilizes cryptographic transformations such as S-box, multiplication by an 8×8 matrix, and modular addition. NIST tests are regarded as highly effective for evaluating the characteristics of pseudorandom sequences and their applicability across various platforms. The conducted NIST tests yielded positive results, and D. Knuth's evaluative tests confirmed that the pseudorandom sequences meet all required criteria. The research on the «AL04» encryption algorithm has shown that it is statistically secure.

Introduction

In a world where information security is becoming increasingly important, protecting data confidentiality plays a crucial role. One of the most effective optimal methods for ensuring data security is encryption. Among the most common and reliable methods of data encryption are block cipher algorithms, which work with fixed-size data blocks. These algorithms divide the input data into blocks, each of which is then encrypted. This approach qualitatively ensures a high level of security, as even minor alterations to the original data result in substantial changes in the ciphertext.

This method qualitatively ensures a high level of security, because even small changes in the original data cause significant and unexpected changes in the ciphertext.

Understanding the principles of block cipher algorithms is a key element in ensuring data security and protecting confidentiality in modern conditions [1,2].

Block encryption algorithms are one of the key methods for ensuring reliable information protection in modern information technology. These algorithms provide a high level of data security by processing fixed-size data blocks and applying complex cryptographic operations for their encryption and decryption [3,4].

Research in the field of block cipher algorithms is conducted by scientists worldwide to enhance security and efficiency and develop new encryption methods. One way to determine the cryptographic strength of block cipher algorithms is through their statistical security [5].

The statistical security (or strength) of block cipher algorithms is related to their ability to withstand various types of cryptanalysis based on the statistical security of the ciphertext. This is a critical aspect of security because certain statistical characteristics of the ciphertext can provide an attacker with information about the key or the original message [6,7]. Here are some statistical characteristics that are typically considered when analyzing the statistical security of block cipher algorithms [8,9]:

Uniform bit distribution: The cipher should ensure a uniform bit distribution in the encrypted text. If the ciphertext exhibits any irregularities or frequent repetitions of specific bit sequences, this could indicate vulnerabilities.

Lack of autocorrelation: A robust block cipher algorithm should guarantee that the ciphertext lacks autocorrelation, meaning there should be no statistical dependencies between bits or blocks of the encrypted text.

Resistance to partial knowledge of the key: Even if an adversary has partial knowledge of the key or the original message, the cipher should prevent the disclosure of additional information about the key or the message.

Resistance to statistical attacks: A good block cipher should withstand various statistical attacks, such as differential and linear cryptanalysis, among others.

Complexity of cryptanalysis: The cipher should make cryptanalysis impractical by requiring high computational resources or a large volume of known plaintext.

A statistical hypothesis is used to determine the statistical security of block cipher algorithms. A statistical hypothesis is a predetermined prediction about the type of distribution of a random variable or the parameters of the distribution. The mechanism for testing statistical hypotheses is based on proposing two alternative hypotheses, H_0 and H_1. From the perspective of a specific test, the null hypothesis being tested is whether the pseudo-random sequence (PRS) is truly random, or the alternative decision is that the PRS is not random [10].

A statistical test is used to determine the randomness of any sequence. To evaluate whether a sequence passes the test, the assumption of the null hypothesis's correctness is determined using the normal distribution and Pearson's χ^2 distribution [11].

To determine whether a test has been passed, various statistical criteria must be applied to help accept or reject the null hypothesis. These criteria are used to check whether the test results match theoretical expectations and can vary in terms of reliability. Below are different types of statistical criteria, listed in order of increasing reliability [12,13]:

- Threshold value: In this approach, the computed test statistic is compared to a predefined threshold value. If the statistic exceeds this threshold, the test is considered passed.
- Confidence interval: Using this criterion, the test is considered passed if the test statistic falls within a specified confidence interval, which is determined based on the significance level.
- Probabilistic approach: This method assumes that the set of test statistic values is considered a set of random variable values, distributed according to a given probability distribution.

The last method, the probabilistic approach, has proven to be the most effective and reliable. The significance level α is a measure that reflects the probability that the test will indicate non-randomness in a sequence even if it is actually random. The probability of making the correct decision, meaning the probability that the test correctly does not reject the null hypothesis, is $1 - \alpha$. This means that, at a significance level of α, the probability that the test correctly identifies a random sequence as random is $1 - \alpha$.

In most practical applications, the significance level α is usually set at 0.05. For cryptographic tasks, where security is critically important, stricter significance levels are used, typically within the range of [0.001, 0.01] [9].

Let's list several well-known tools for statistical testing of pseudorandom sequences [14-16]:

– Knuth's tests;

– DIEHARD tests (G. Marsaglia);

– NIST test suite (A. Rukhin et al.);

– TestU01 suite (P. L'Ecuyer);

Research methodology

The developed encryption algorithm 'AL04' is architecturally new and meets modern requirements (Figure 1).

Algorithm parameters: block length – 128 bits, number of rounds – 8, size of the S-box, which acts as a nonlinear function in the algorithm – 8 bits. Key length – 128 bits. Transformations used – bitwise XOR, substitution S-box, and multiplication by a square matrix. A detailed description of the algorithm is provided in reference [17].

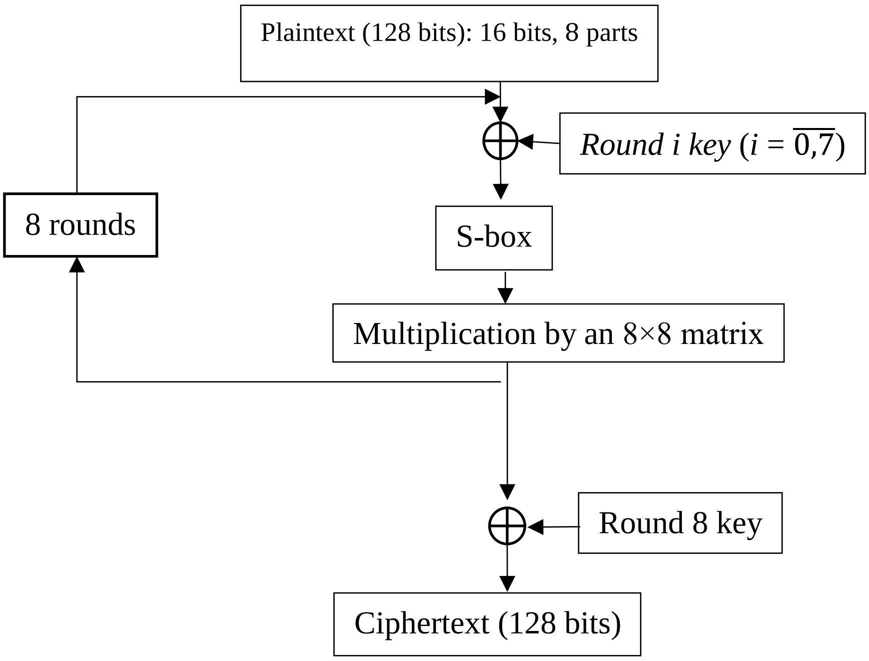

Plaintext (128 bits): 16 bits, 8 parts
Round i key ($i = \overline{0,7}$)
8 rounds
S-box
Multiplication by an 8×8 matrix
Round 8 key
Ciphertext (128 bits)

Figure 1. Block diagram of algorithm AL04

Encryption function:

$$\bar{C} = M\otimes\bar{S}(\dots\bar{S}(M\otimes\bar{S}(\bar{A}\oplus\overline{K_0})\oplus\overline{K_1})\dots\oplus\overline{K_7})\oplus\overline{K_8} \qquad (1)$$

Decryption function:

$$\bar{A} = \overline{M^{-1}\otimes S^{-1}}(\dots\overline{S^{-1}}\big(M^{-1}\otimes\overline{S^{-1}}(\bar{C}\oplus\overline{K_8})\oplus\overline{K_7}\big)\dots\oplus\overline{K_1})\oplus\overline{K_0}, \qquad (2)$$

where the square matrix is selected relative to the size of the matrix during encryption or decryption. The size of the vectors $\bar{A}, \bar{C}, \overline{K_\iota}$ is equal to $\frac{128}{2^k}$, $\bar{S}$ and $\overline{S^{-1}}$ are operations respectively transforming vector elements through S-boxes. $\bar{A}$ represents plaintext, $\bar{C}$ – ciphertext, and $\overline{K_\iota}$ – round keys.

Results of the study

Results of the statistical analysis of the AL04 algorithm

In Donald Knuth's book "The Art of Computer Programming," systematic approaches to testing random sequences were first introduced. These early tests laid the foundation for further developments and remain relevant in contemporary research in cryptography and randomness statistics [18].

Seven of Knuth's statistical tests are used to evaluate the randomness of sequences. These tests are described in more detail in [17]. They are assessed using the χ^2 statistical criterion. By comparing the value obtained from the χ^2 statistic with specifically tabulated results and depending on the probability of the statistical value, conclusions are drawn about its significance or quality.

For the study of statistical security of encryption algorithms using Knuth's tests, 120 original files were used. These files were encrypted using the AL04 algorithm, resulting in 120 encrypted texts. The number of successful Donald Knuth tests for each encrypted text is shown in Figure 2.

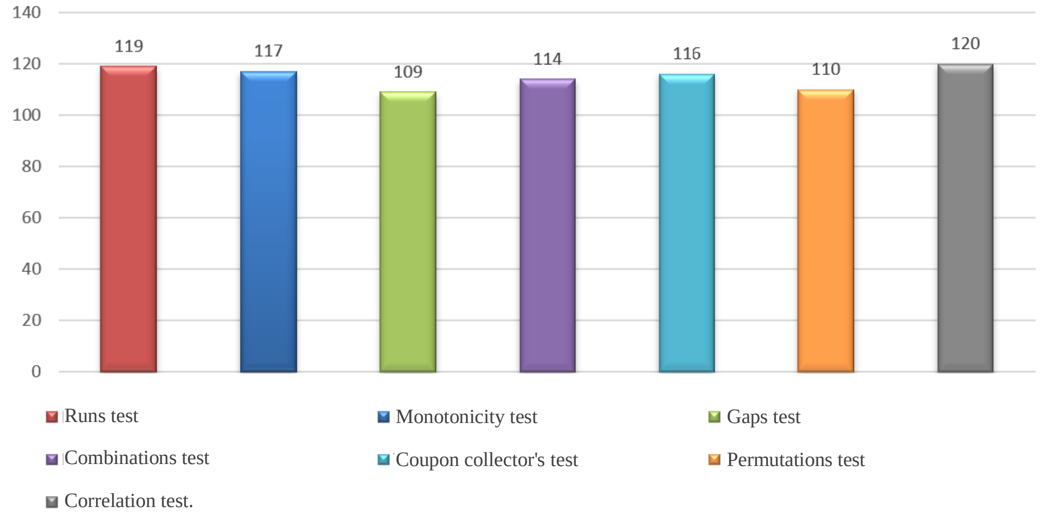


Figure 2. Number of successful Donald Knuth tests passed

NIST statistical tests

NIST (the National Institute of Standards and Technology) was one of the first organizations to develop a set of statistical tests for assessing the randomness and quality of random sequence generators. These tests are part of the NIST Statistical Test Suite and are designed to evaluate the randomness in random sequence generators and data streams [19].

Each test in the NIST Statistical Test Suite compares the statistic computed for the tested sequence with the corresponding theoretical value, which is calculated for the chosen reference distribution of the random variable. The following reference distributions are used in each test [20]:

- Chi-square (χ^2) distribution: This distribution is used to assess how well the observed data match the expected data when they are categorized.
- Normal distribution: This distribution describes a situation where the values of a random variable are symmetrically distributed around the mean. In tests, it is used to check whether statistics, such as the sum or difference of bits, conform to a normal distribution.

To find the statistics of the considered pseudo-random sequence (PRS), the processes of centering and normalization are often used to bring the data into a standard form. Centering and normalizing a pseudo-random sequence is done using the formula $z = \frac{x-\mu}{\sigma}$. The calculation of the *p-value* is performed using an additional error function:

$$erfc(z) = \frac{2}{\sqrt{\pi}}\int_{z}^{\infty} e^{-u^2}\,du$$

The χ^2 distribution involves comparing the observed frequencies F_i with the expected frequencies f_i of a presumed distribution. The statistic used in this case is:

$$\chi^2 = \sum_{i=1}^{k} \frac{(F_i - f_i)^2}{f_i}$$

In this case, the calculation of the *p-value* is conducted using the incomplete gamma function, defined by the formula below:

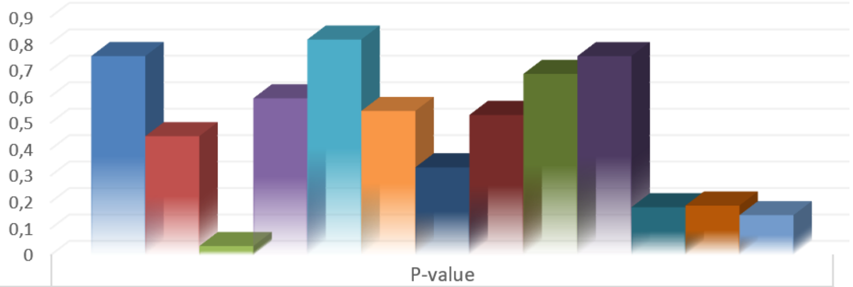
$$Q(a,x) \equiv \frac{\Gamma(a,x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)}\int_{x}^{\infty} e^{-t}\, t^{a-1}dt, \Gamma(z) = \int_{0}^{\infty} e^{-t}\, t^{z-1}dt$$

All tests belonging to the NIST STS suite are parametric, so it is crucial to make correct choices for the necessary parameter values when using them.

Next, we will conduct a statistical evaluation of the AL04 encryption algorithm and test the encrypted text using a program implemented in Visual C# with the NIST tests. In each test, the P-value is calculated, and conclusions are drawn based on this value. If $\alpha = 0{,}01$ is chosen for the tests, the following decision is made [9,18]:

- If $P \geq 0{,}01$, we consider that the obtained encrypted text is random with a probability of 99%;
- If $P < 0{,}01$, we consider that the obtained encrypted text is non-random with a probability of 99%.

Based on the results presented in Figures 3, 4, and 5, it was established that the AL04 encryption algorithm fully passes the NIST tests, meaning that the obtained encrypted text is classified as random.



	P-value
■ Frequency (Monobit) Test	0,7520025
■ Frequency Test within a Block	0,4490719
■ Runs Test	0,0338461
■ Test for the Longest Run of Ones in a Block	0,5923904
■ Binary Matrix Rank Test	0,8146149
■ Discrete Fourier Transform (Spectral) Test	0,5447421
■ Non-overlapping Template Matching Test	0,3314899
■ Overlapping Template Matching Test	0,5295287
■ Maurer's Universal Statistical Test	0,6846561
■ Linear Complexity Test	0,7518722
■ Approximate Entropy Test	0,1805995
■ Serial Test	0,1869391
■ Cumulative Sums (Cusum) Test	0,1506537

Figure 3. AL04 algorithm values according to NIST tests

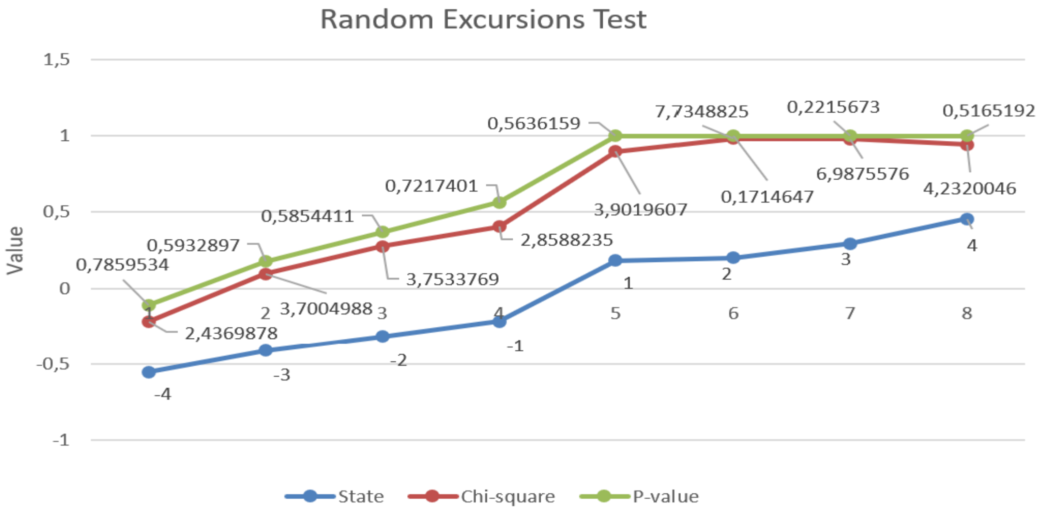
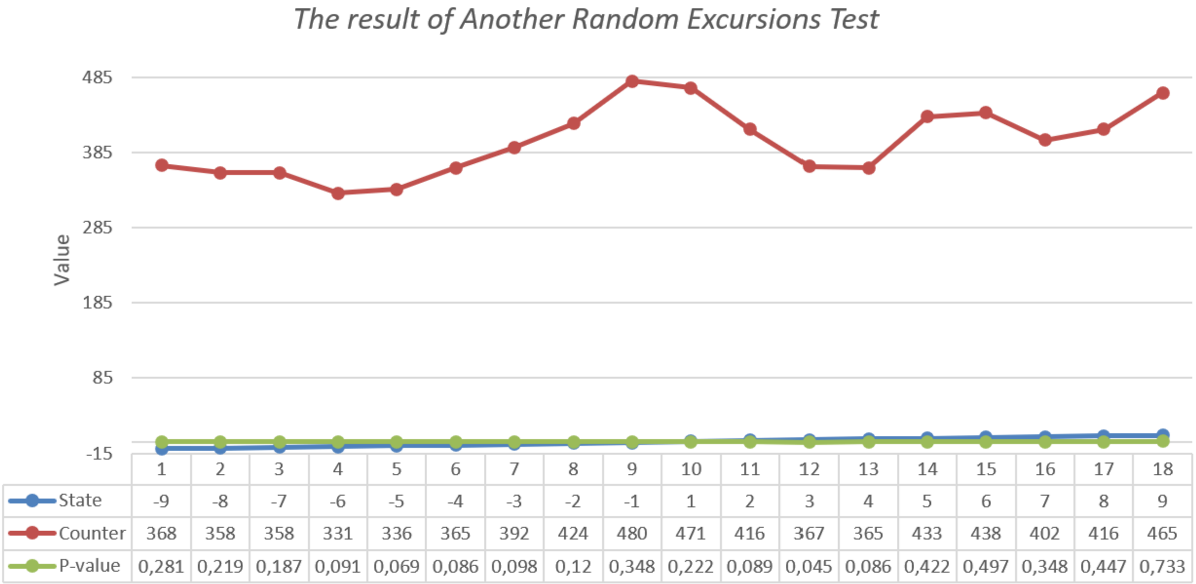


Figure 4. AL04 algorithm values according to the Random Excursions Test



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
State	-9	-8	-7	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6	7	8	9
Counter	368	358	358	331	336	365	392	424	480	471	416	367	365	433	438	402	416	465
P-value	0,281	0,219	0,187	0,091	0,069	0,086	0,098	0,12	0,348	0,222	0,089	0,045	0,086	0,422	0,497	0,348	0,447	0,733

Figure 5. AL04 algorithm values according to the Another Random Excursions Test

Results of the analysis of statistical security metrics of the algorithm

In statistical security studies, we use the following metrics [26]:

- Avalanche effect: This measures how strongly a change in a single bit of the plaintext affects the ciphertext.
- Degree of avalanche effect (d_a): This key metric describes how a change in one bit of the plaintext affects the ciphertext generated by the cryptographic algorithm. Ideally, changing a single bit in the plaintext sequence should result in a change in half of the bits in the ciphertext sequence, which ensures a high level of algorithm security.
- Degree of completeness ($\boldsymbol{d_c}$): This characteristic of a cryptographic function describes the extent to which the algorithm meets specific security and functionality requirements. Completeness includes both the algorithm's ability to perform its claimed functions and its satisfaction with critical security requirements.
- Degree of strict avalanche criterion ($\boldsymbol{d_{sa}}$): This is a more detailed and stringent metric that measures how precisely the cryptographic algorithm adheres to the avalanche effect principle.

The objective of this research is to calculate the values for each round of the AL04 encryption algorithm based on the aforementioned metrics and to evaluate the results. The analysis was conducted on ciphertexts of lengths 100, 1000, and 10,000 blocks, generated by the AL04 algorithm. Table 1 presents the results of the statistical assessment of the AL04 encryption algorithm.

Table 1. Results of the statistical assessment of the AL04 encryption algorithm

Round No.	D_{min}	D_{max}	d_w	M_{min}	M_{max}	m_w	d_c	d_a	d_{sa}
AL04(100 blocks)									
1.	*9.00202*	*10.86369*	*9.932860*	*3.07485*	*5.70765*	*4.39125*	*0.125*	*0.137226*	*0.086708*
2.	*50.69342*	*52.555096*	*51.624261*	*11.3026625*	*13.9354625*	*12.6190625*	*0.468261*	*0.394345*	*0.331406*
3.	*64.68940*	*66.551071*	*65.620235*	*20.81735*	*23.45015*	*22.13375*	*1*	*0.691679*	*0.634501*
4.	*43.96099*	*45.822668*	*44.891833*	*27.319537*	*29.952337*	*28.635937*	*1*	*0.893993*	*0.835097*
5.	*20.96599*	*22.827668*	*21.896833*	*30.147662*	*32.780462*	*31.464062*	*1*	*0.977666*	*0.911474*
6.	*15.54508*	*17.406757*	*16.475922*	*30.579693*	*33.212493*	*31.896093*	*1*	*0.989868*	*0.919458*
7.	*14.86085*	*16.722529*	*15.791693*	*30.7411*	*33.3739*	*32.0575*	*1*	*0.98875*	*0.921914*

Round No.	D_{min}	D_{max}	d_w	M_{min}	M_{max}	m_w	d_c	d_a	d_{sa}
8.	*14.40422*	*16.265894*	*15.335058*	*30.625475*	*33.258275*	*31.941875*	*1*	*0.989462*	*0.920371*
AL04(1000 blocks)									
1.	*9.002025*	*10.863696*	*9.932860*	*3.07485*	*5.70765*	*4.39125*	*0.125*	*0.137226*	*0.086708*
2.	*50.693426*	*52.555096*	*51.624261*	*11.3026625*	*13.9354625*	*12.6190625*	*0.468261*	*0.394345*	*0.331406*
3.	*64.689400*	*66.551071*	*65.620235*	*20.81735*	*23.45015*	*22.13375*	*1*	*0.691679*	*0.634501*
4.	*43.960998*	*45.822668*	*44.891833*	*27.319537*	*29.952337*	*28.635937*	*1*	*0.893993*	*0.835097*
5.	*20.965998*	*22.827668*	*21.896833*	*30.147662*	*32.780462*	*31.464062*	*1*	*0.977666*	*0.911474*
6.	*15.545086*	*17.406757*	*16.475922*	*30.579693*	*33.212493*	*31.896093*	*1*	*0.989868*	*0.919458*
7.	*14.860858*	*16.722529*	*15.791693*	*30.7411*	*33.3739*	*32.0575*	*1*	*0.98875*	*0.921914*
8.	*14.404223*	*16.265894*	*15.335058*	*30.625475*	*33.258275*	*31.941875*	*1*	*0.989462*	*0.920371*
AL04(10000 blocks)									
1.	*9.002025*	*10.863696*	*9.932860*	*3.07485*	*5.70765*	*4.39125*	*0.125*	*0.137226*	*0.086708*
2.	*50.693426*	*52.555096*	*51.624261*	*11.3026625*	*13.9354625*	*12.6190625*	*0.468261*	*0.394345*	*0.331406*
3.	*64.689400*	*66.551071*	*65.620235*	*20.81735*	*23.45015*	*22.13375*	*1*	*0.893993*	*0.834501*
4.	*43.960998*	*45.822668*	*44.891833*	*27.319537*	*29.952337*	*28.635937*	*1*	*0.893993*	*0.835097*
5.	*20.965998*	*22.827668*	*21.896833*	*30.147662*	*32.780462*	*31.464062*	*1*	*0.977666*	*0.911474*
6.	*15.545086*	*17.406757*	*16.475922*	*30.579693*	*33.212493*	*31.896093*	*1*	*0.989868*	*0.919458*
7.	*14.860858*	*16.722529*	*15.791693*	*30.7411*	*33.3739*	*32.0575*	*1*	*0.98875*	*0.921914*
8.	*14.404223*	*16.265894*	*15.335058*	*30.625475*	*33.258275*	*31.941875*	*1*	*0.989462*	*0.920371*

As the results of the study show, it was established that complete mixing of the input sequence occurs at the 2nd round of encryption using the AL04 algorithm.

Discussion

The main method of statistical testing for block ciphers involves creating various pseudo-random sequence generators based on the tested block cipher. These sequences are then subjected to statistical testing. It is important how these generators are constructed and which tests are used for testing the sequences. Currently, there are many test suites for checking sequence statistics. Among them, we use the test suites by Donald Knuth and NIST. These sets of tests were chosen for several key reasons. Each statistical test proposed by D. Knuth is designed to test the hypothesis of randomness of the input sequence, which helps identify potential weaknesses in random number generators and cryptographic algorithms.

In turn, the NIST test suite was developed by the National Institute of Standards and Technology (NIST), a prominent government organization supported by a team of highly qualified experts in mathematical statistics.

This test suite is used for assessing the randomness of sequences and has been employed for testing cryptographic algorithms at the national level, including block ciphers that participated in the AES standardization competition. During the investigation of the AL04 encryption algorithm, it was established that the AL04 encryption algorithm fully meets the criteria of statistical security based on the numerical indicators of the NIST and Donald Knuth tests.

Conclusion

Evaluating the statistical security of block cipher algorithms is one of the primary criteria for determining the reliability of these algorithms. Therefore, this article examines and presents the results of the statistical security assessment of the algorithm. This aspect of security is crucial in evaluating the reliability of block cipher algorithms under real operational conditions. The proposed algorithm AL04 was implemented programmatically to investigate the statistical security of files encrypted with this algorithm. According to the research findings, all P-values from the NIST tests fall within the interval [0, 1], indicating that 99% of the encrypted text characteristics correspond to a random sequence. It was also found that according to the tests by Donald Knuth, the output sequence is pseudo-random. Furthermore, it has been demonstrated that the statistical indicators meet security requirements starting from the second round, i.e., with $d_c = 1$.

Thus, based on these results, the AL04 algorithm can be considered statistically secure. Further research into other properties of the algorithm is planned for future work.

Acknowledgment

Research works were carried out on the basis of the grant project AP14870419 "Development of a cryptographic information protection facility for securing communications in HF radio communication.

References

[1] Biyashev R.G., Smolarz A., Algazy K. T., Khompysh A. Encryption algorithm "Qamal NPNS" based on a nonpositional polynomial notation // KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 2020, 105(1), pp.198–207.

[2] Biyashev R.G., Kalimoldayev M.N., Nyssanbayeva S.E., Kapalova N.A., Dyusenbayev D.S., Algazy K.T. Development and analysis of the encryption algorithm in nonpositional polynomial notations // Eurasian Journal of Mathematical and Computer Applications, 2018, 6(2), pp. 19-33.

[3] Kapalova N., Khompysh A., Arici M., Algazy K., A block encryption algorithm based on exponentiation transform // Cogent Engineering, 2020. 7(1). https://doi.org/10.1080/23311916. 2020.1788292

[4] Leander G., Moos T., Moradi A., & Rasoolzadeh S. The SPEEDY Family of Block Ciphers: Engineering an Ultra Low-Latency Cipher from Gate Level for Secure Processor Architectures // IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(4), pp. 510–545. https://doi.org/10.46586/tches.v2021.i4.510-54

[5] Lu Y., Zhang W., and Cao L. Data Security Encryption Method Based on Improved AES Algorithm //" 2022 Global Reliability and Prognostics and Health Management (PHM-Yantai), Yantai, China, 2022, pp. 1-6, https://doi:10.1109/PHM-Yantai55411.2022.9942058.

[6] Hłobaż A. Statistical Analysis of Enhanced SDEx Encryption Method Based on SHA-256 Hash Function // 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 2019, pp. 238-241, https://doi:10.1109/LCN44214.2019.8990714.

[7] Cardona-López M.A., Chimal-Eguía J.C., Silva-García V.M., Flores-Carapia R. Statistical Analysis of the Negative–Positive Transformation in Image Encryption // Mathematics, 2024, 12(908), https://doi.org/10.3390/math12060908

[8] Puchala D., Stokfiszewski K., Yatsymirskyy M. Image Statistics Preserving Encrypt-then-Compress Scheme Dedicated for JPEG Compression Standard // Entropy, 2021, 23(421), https://doi.org/10.3390/e23040421

[9] Khompysh A., Kapalova N., Lizunov O., Dilmukhanbe, D., Kairat S. Development of a new lightweight encryption algorithm // International Journal of Advanced Computer Science and Applications, 2023, 14(5), 452-459, https://doi.org/10.14569/IJACSA.2023.0140548

[10] Pikuza M. O., & Mikhnevich S. Yu. Testing of hardware random number generator using a set of NIST statistical tests // Reports of BSUIR, 2012, 19(4), pp. 37-42, https://doi.org/10.35596/1729-7648-2021-19-4-37-42

[11] Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001,10 p.

[12] Al-Hazaimeh O. M., Al-Shannaq M. A., Bawaneh M.J., & Naha K. M. Analytical Approach for Data Encryption Standard Algorithm // International Journal of Interactive Mobile Technologies (iJIM), 2023, 17(14), pp. 126–143. https://doi.org/10.3991/ijim.v17i14.38641

[13] Alvarez R., Martinez F., Zamora A. Improving the Statistical Qualities of Pseudo Random Number Generators // Symmetry, 2022, 14(269). https://doi.org/10.3390/sym14020269

[14] Knuth D. E. The art of computer programming. Transl. from English, 3rd ed., V. 2., 2004, Seminumerical Algorithms. Publishing house Williams.

[15 Pierre L'Ecuyer., Richard Simard. TestU01: A C library for empirical testing of random number generators // ACM Transactions on Mathematical Software, 2007, 33(4):22-39. https://doi: 10.1145/1268776.1268777

[16] Perov A. A. Using NIST statistical tests for the analysis of the output sequences of block ciphers // Sci. Bull. of NSTU, 2019, 3(76), pp. 87-96, 2019. https://doi:10.17212/1814-1196-2019-3-87-96.

[17] Khompysh A., Nysanbayeva S.E., Ostapenko V.V. Statistical Security Assessment of the AL04 Encryption Algorithm // Proceedings of the VIII International Scientific and Practical Conference 'Informatics and Applied Mathematics'. Almaty, 2023. pp. 327–333.

[18] Ivanov, M. A., & Chugunkov, I. V. The theory, application, and evaluation of the quality of pseudorandom sequence generators // CUDYC-OBRAZ, 2003, pp. 240. Moscow.

[19] Sulak F., Uğuz M., Koçak O., and Doğanaksoy A. On the independence of statistical randomness tests included in the NIST test suite // Turk. Jour. of Elec. Engin. & Comp. Scien., 2017, vol. 25, no.5, pp. 3673-3683, https://doi:10.3906/elk-1605-212.

[20] Pikuza M. O., Yu S. Testing a hardware random number generator using NIST statistical test suite // BSUIR Reports, 2021, vol. 19, no. 4, pp. 37-42, https://doi.org/10.35596/1729-7648-2021-194-37-42.