**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 15, No. 2, April 2025, pp. 1900~1911
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i2.pp1900-1911

# Development and analysis of symmetric encryption algorithm

**Ardabek Khompysh[1,2], Dilmukhanbet Dyusenbayev[1], Muratkhan Maxmet[2]**
[1]Information Security Laboratory, Institute of Information and Computing Technologies, Almaty, Kazakhstan
[2]Department of University Humanitarian Subjects, Egyptian University of Islamic Culture Nur-Mubarak, Almaty, Kazakhstan

**Article Info**

***Article history:***

Received Apr 12, 2024
Revised Oct 24, 2024
Accepted Nov 20, 2024

***Keywords:***

Algebraic analysis
Exponentiation modulo
Galois field
Nonpositional polynomial notations
S-block
Strict avalanche criterion
Symmetric encryption algorithm

**ABSTRACT**

This paper introduces a new block encryption algorithm designed for the cryptographic protection of data. The paper introduces and explains a newly devised exponentiation modulo (EM) transform method, utilized to obtain the S-block, an essential element within the presented algorithm. A method of optimizing the choice of keys and increasing the efficiency of calculation was also used. It is proposed that incorporating characteristics of cryptographic primitives functioning within the Galois field into the algorithm can lead to favorable outcomes. To increase the encryption algorithm's speed, non-positional polynomial notation systems and a working base index table are used. The paper discusses the implementation of an encryption algorithm in C++ and examines the statistical characteristics of the resulting ciphertexts. For experimental testing of statistical safety, a set of statistical tests by National Institute of Standards and Technology (NIST) and D. Knuth was used. Furthermore, the resulting S-box was examined using linear, differential, and algebraic cryptanalysis techniques. In the future, this proposed S-box will be implemented in the encryption algorithm being developed for the preliminary encryption of confidential data.

***Corresponding Author:***

Ardabek Khompysh
Information Security Laboratory, Institute of Information and Computing Technologies
Almaty, Kazakhstan
Department of University Humanitarian Subjects, Egyptian University of Islamic Culture Nur-Mubarak
Almaty, Kazakhstan
Email: ardabek@mail.ru

## 1. INTRODUCTION

Given that national security is one of the priority areas in any country's development strategy, information security stands out as one of its most crucial components. Consequently, the development of safe and efficient information processing systems is a key priority for every nation [1]. To address the challenge of creating new information security technologies, it is necessary, on the one hand, to provide high-speed processing and handle a large amount of information, while on the other hand, to control access to it and ensure the necessary level of information protection. In Kazakhstan's information security sphere, foreign equipment and software transparent to their developers are primarily used. Therefore, the development of domestic cryptographic information security facilities, including domestic lightweight encryption algorithms [2] based on previously developed encryption algorithms, is currently a critical task.

The Information Security Laboratory at the Institute of Information and Computational Technologies of the Ministry of Science and Higher Education of the Republic of Kazakhstan conducts research and development of new encryption systems, electronic digital signatures, cryptographic key generation, and authentication systems [3], [4]. This includes creating software-based cryptographic information security facilities based on these systems. Conducting research and development in this direction is essential for our country. It aims to advance the development of domestic information security systems and create software and hardware complexes for practical use. According to the project schedule, work has been carried out to develop symmetric block encryption cryptographic algorithms, assess their security, and implement them in software and hardware. So that, creation of the information security tools that meet modern requirements is one of the topical issues. There are many ways to solve these problems, one of the most effective ways to use cryptographic methods, such as cryptographic protection systems. Symmetric block encryption algorithms are currently the main cryptographic means of reliable protection of confidentiality when processing confidential information in information and telecommunication systems [5]. Modern symmetric block ciphers are primarily built on the basis of two approaches: the Feistel network and the substitution-permutation network (SP network). As you know, ciphers are based on reversible transformations of plaintext. When developing them, it is necessary to ensure that each of the operations performed is both cryptographically secure and reversible if the key is known [6]. Modern ciphers are based on Kerkhoff's principle, according to which the secrecy of the cipher is ensured by the secrecy of the key, and not by the secrecy of the encryption algorithm. Block cipher algorithms are an integral part of modern information technology and continue to be relevant and in demand in the ever-evolving field of cybersecurity. Thanks to the efforts of scientists, block cipher algorithms continue to improve, enhancing the level of data security, whose role is constantly increasing in the rapidly changing world of digital technology.

Methods of cryptographic information protection are diverse depending on functional tasks. For example, encryption of large amounts of information at high speeds. Numerous studies have been undertaken to address these challenges, resulting in the development of a new block encryption algorithm [7]. In the developed algorithm, to solve such problems, two different mathematical methods are used. They are: i) polynomial system of residue classes or non-positional polynomial notation systems (NPNs); and ii) calculation of the degree using an index table in the modular exponentiation in extended Galois field $GF(p^v)$.

Non-positional polynomial notations (NPNs). There are numerous works by scientists on number systems, including the residue number system (RNS). In 1955, the Czech engineer M. Valach first introduced the idea of using residual classes in the field of computer technology, and he was actively supported by the Czech mathematician A. Svoboda. In practice, this idea has proven to be the most effective approach, based on the Chinese remainder theorem [8]. Prior to this, the concept was considered a fundamental theorem in abstract algebra, capturing the interest of many groups of scientists, ultimately leading to the emergence of a new scientific discipline known as modular arithmetic. Currently, the residual classes are used in radio engineering, space technology, various scheme techniques, cryptography and many other fields [9].

One of the trends of module arithmetic development, as explored in the works of Kazakhstan's scientist Biyashev and Nyssanbayeva [3], involves investigating the creation, analysis, and application of non-positional polynomial notations. He emphasized that polynomial algebra could encompass any irreducible polynomial module, provided proof of the Chinese remainder theorem for polynomials, and established rules for arithmetic operations within the polynomial system, as well as defining polynomial recovery by residue.

Let us describe the construction of non-positional polynomial notations. If the number of polynomials $p_1(x), p_2(x), \ldots, p_n(x)$ which called working bases are given, then in NPNs any polynomial $F(x)$, can be represented as a sequence of residues of dividing it by the chosen working base numbers [10] respectively:

$$F(x) = \left(a_1(x)a_2(x), a_3(x), \ldots, a_i(x)\right). \tag{1}$$

where $a_i(x),\, i = \overline{1,n}$ is defined by (2):

$$F(x) \equiv a_i(x)\left(mod\, p_i\,(x)\right). \tag{2}$$

Then the working range in NPNs is defined as (3):

$$P(x) = \prod_{i=1}^{n} p_i(x). \tag{3}$$

If the working base numbers degree equal to $m_1, m_2, \ldots, m_i$, then the NPNs' working range degree m will be equal to their sum:

$$m = \sum_{i=1}^{n} m_i. \tag{4}$$

The operation of modular exponentiation in the extended Galois field $GF(p^v)$ [11]. In many scientific papers shown that the $GF$ field has many possibilities in the development of various cryptographic functions, plaintext encryption, and ensuring the confidentiality and integrity of information [12]. One of them is currently operation of modular exponentiation used in the Rivest–Shamir–Adleman (RSA) and El-Gamal, Diffie-Hellman algorithms. The data encryption formula by using the operation of modular exponentiation in the extended field $GF(p^v)$. is defined as (5) [13]:

$$B(x) = A^K(x)\, mod\, P\,(x). \tag{5}$$

where $A(x)$ is plaintext; $K$ is key; and $B(x)$ is ciphertext.

Message decryption formula:

$$A(x) \equiv \sqrt[K]{B(x)}\, mod\, P\,(x). \tag{6}$$

Here we calculate the plaintext by finding the inverse element of K that satisfies the equation:

$$K \cdot (K)^{-1} \equiv 1\, mod(\, 2^{ordP(x)} - 1). \tag{7}$$

where $ord$-the degree to $P(x)$. Then, the decryption formula based on (7) can be expressed as (8):

$$A(x) \equiv B(x)^{K^{-1}}\, mod\, P\,(x). \tag{8}$$

## 2. SYMMETRIC ENCRYPTION ALGORITHM (SEA128)

In the design of the proposed encryption algorithm, the exponentiation modulo (EM) transform method is used. This method functions in a non-positional polynomial notation system, utilizing modular exponentiation in the extended Galois field $GF(p^v)$, and incorporates an S-block substitution table. All methods used are described below. Figures 1 and 2 illustrate the proposed block encryption and decryption algorithm. The main parameter of the algorithm: i) block size 128 bits, ii) key size 128 bits, and iii) number of rounds 8.

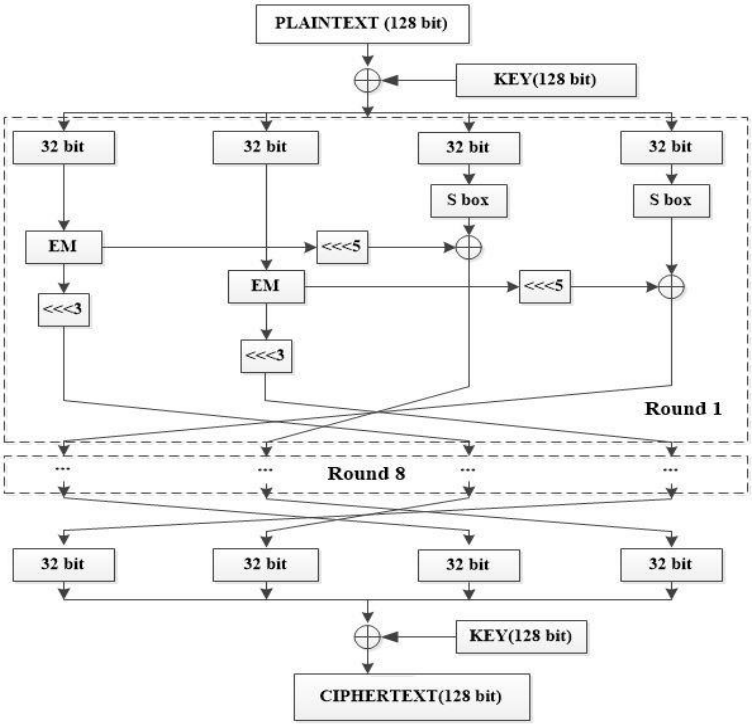


Figure 1. The scheme of block encryption algorithm

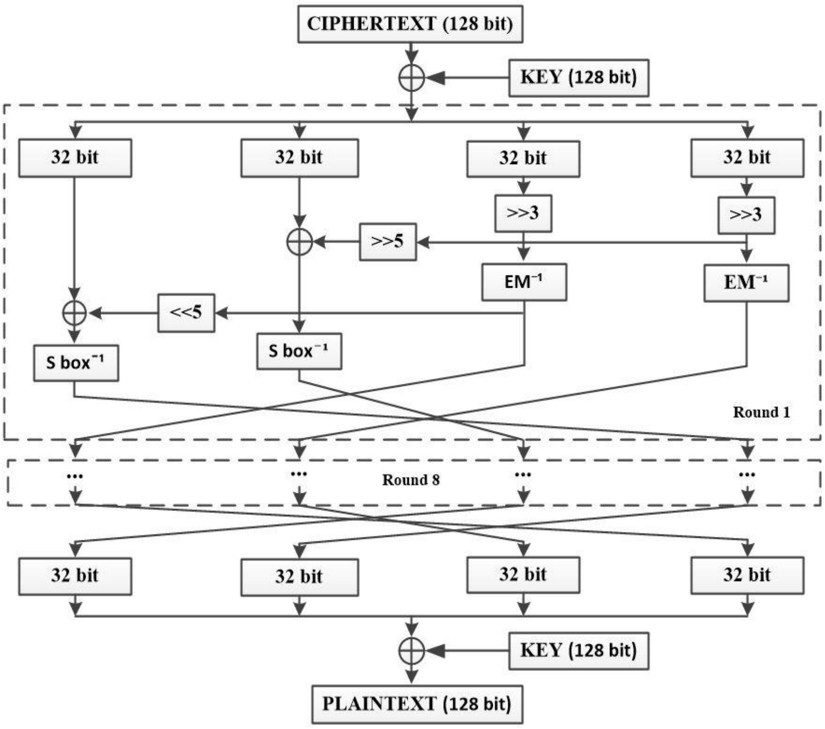


Figure 2. The scheme of block decryption algorithm

The encryption process can be divided into 4 stages:

Stage 1: Incoming data is divided into 128-bit segments. If the final segment is shorter than 128 bits, it is padded with zeros (which are later removed during decryption). Each 128-bit segment is then combined with a 128-bit key using an XOR (⊕) operation. The 128-bit result is split into four 32-bit sub-blocks, which are then processed in the next stages.

Stage 2: The first and second 32-bit sub-blocks undergo an EM conversion method as per a specified scheme. After this conversion, a bit shift operation is performed on these sub-blocks.

Stage 3: The third and fourth 32-bit sub-blocks are processed using an S-box substitution table, according to a predefined scheme. The results from the first and second sub-blocks in Stage 2 are then combined with the processed third and fourth sub-blocks using a modular operation.

Stage 4: Each internal block undergoes specific movements based on a defined scheme in each encryption round. After the final round, an additional key is added to the resulting block using a modular operation, completing the encryption process.

By following these steps, the data is securely encrypted and can later be decrypted by reversing the process.

The decryption scheme of the algorithm is shown in Figure 2. All the methods used are described below. Now let us talk separately about the conversion methods contained in this proposed SEA 128 algorithm. These methods are crucial for ensuring the proper transformation of data during the decryption process. Each method serves a specific purpose, such as bit manipulation, data substitution, and permutation, to ensure that the original encrypted data is accurately restored. The combination of these methods is designed to provide a high level of security while maintaining efficiency in decryption.

### 2.1. Exponentiation modulo transform method

NPNs based on the operation of modular exponentiation in the extended Galois field $GF(p^v)$, consists of three stages: i) creation of working bases system and selection of arrangement order, ii) round keys formation, and iii) input data conversion and inverse conversion. The first stage involves establishing a working base system and determining the order of arrangement, which is critical for the efficiency of subsequent operations. In the second stage, round keys are generated from the initial key, playing a key role in the encryption process by providing the necessary transformation at each round. Finally, the third stage focuses on converting the input data for processing and ensuring its proper inverse conversion, enabling correct decryption and retrieval of the original data. Now, let's look at the structure of these steps.

The first stage. Consider the stage of selection the working bases. Let the number of degrees of the binary sequence of irreducible polynomials accordingly $m_1$equal to $n_1$, $m_2$ equal to $n_2$, $m_S$ equal to $n_S$ [4]. In this case the highest degree of working bases is equal to $H$ and at the stages of selection of working bases with degree $m_i$, up to $i = \overline{1, S}$ we find all the possible solutions of the algebraic equation that satisfy the (5) [5], [10]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_S m_S = H. \tag{9}$$

where $0 \le k_i \le n_i$, $i = \overline{1, S}$: unknown coefficient, $k_i$: the number of irreducible polynomials with selected $m_i$degree, $n_i$: the number of irreducible polynomials with all $m_i$ degree, where $1 \le m_i \le H$, the number of all the working bases is as (10):

$$S = k_1 + k_2 + \cdots + k_S. \tag{10}$$

The second stage. For the implementing the transform method based on the operation of modular exponentiation in the extended Galois field, the values $k_i$ and ${k_i}^{-1}$are obtained by the pseudorandom sequence generator (PSG): i) the construction of sequence, ii) division received binary sequence by selected working bases in accordance with the degree, iii) substitute the binary sequence system to the decimal system, and iv) select the value $k_i$ obtained as GCD ($k_i$,$p^{ord(p_i(x)} - 1$)=1.

The third stage. It is known that the data encryption speed requires a lot of time based on the operation of modular exponentiation according to the formula (15). However, it is advisable to use NPNs to increase speed of the calculation of this procedure. Therefore, let use the NPNs for data encryption procedure, in this case in the proposed algorithm working bases in Galois field $GF(2^v)$ selected in accordance with the formula (9).

In the proposed transform method, input data is provided as length of 128 bits. Then it divided into 32 bits blocks and works with each block. Each 32-bits block is divided into parts according to the working bases degree. The obtained part according to the formula (1) shown as a sequence of remains in NPNs:

$$A(x) = a_1(x), a_2(x), a_3(x), \dots, a_i(x). \tag{11}$$

where $a_i(x)$ - obtained parts, $i = \overline{1, n}$.

For the transformation of the splitted blocks that obtained by formula (11) express as (12) [8]:

$$b_i(x) = a_i^{k_i}(x) \, mod \, p_i \,(x), i = \overline{1, n}. \tag{12}$$

ciphertexts systems obtained by formula (12) express as (13):

$$B(x) = b_1(x), b_2(x), b_3(x), \dots, b_i(x). \tag{13}$$

In this case, the inverse transform corresponds to formula (8) is equal to:

$$a_i(x) = b_i(x)^{k_i^{-1}} \, mod \, p_i \,(x). \tag{14}$$

Obtained plaintexts (11) by formula express as (15):

$$A(x) = a_1(x), a_2(x), a_2(x), \dots, a_i(x). \tag{15}$$

In the proposed algorithm for each block calculate inverse of used key:

$$k_i \cdot (k_i)^{-1} \equiv 1 \, mod(p^{ord(p_i(x)} - 1), i = \overline{1, n}. \tag{16}$$

It is known in the EM transform method calculating the exponentiation process takes a long time. However, in the proposed algorithm calculating the exponentiation by creating an index table, consequently the speed of calculation increases. In the EM transform according to selected working bases $p_i(x)$ the index table are filling in by (17):

$$a(x) = \alpha^j \, mod \, p_i \,(x), \; j = \overline{\infty, \; 2^{ord(p_i(x))} - 1} \tag{17}$$

$\alpha$ - primitive element of a multiplicative group in a field $GF(p^v)$;

For example: Let consider the index table of irreducible polynomial where working bases equal to $p(x) = x^3 + x + 1$ in the field $GF(2^3)$ as shown in Table 1. This polynomial is selected from the finite field $GF(2^3)$, which allows for efficient calculation of the modulo exponentiation operation. And the use of an index table accelerated the encryption and decryption processes. According to the index table of the selected working bases, we introduce the following mathematical equation:

According to the index table of the selected working bases, we introduce the mathematical equation:

$$l = \underset{\alpha}{ind} a_i(x)\, mod(\, p_i(x)). \tag{18}$$

where $l$ - degree of $a(x)$ by $\alpha$ or index $(ind)$. Then we modify the formula (12) as (19):

$$b_i(x) = (\alpha^l)^{k_i}\, mod\, p_i\,(x) = (\alpha^{(lk_i)\, mod(2^{ord(p_i(x))}-1)})\, mod\, p_i\,(x). \tag{19}$$

In the inverse transform instead of $k_i$ inverse element $(k_i)^{-1}$ is used:

$$l = \underset{\alpha}{ind} b_i(x)\, mod(\, p_i(x)) \tag{20}$$

$$a_i(x) = (\alpha^l)^{k_i^{-1}}\, mod\, p_i\,(x) = (\alpha^{(lk_i^{-1})\, mod(2^{ord(p_i(x))}-1)})\, mod\, p_i\,(x) \tag{21}$$

It is shown that the calculation of the index by (12) works faster.

Table 1. $p(x) = x^3 + x + 1$ the index table of working bases

| In the form of index $(ind)$ | In the form of polynomial $a(x)$ |
|---|---|
| $\alpha^{\infty}$ | $0$ |
| $\alpha^0$ | $1$ |
| $\alpha^1$ | $x$ |
| $\alpha^2$ | $x^2$ |
| $\alpha^3$ | $x+1$ |
| $\alpha^4$ | $x^2+x$ |
| $\alpha^5$ | $x^2+x+1$ |
| $\alpha^6$ | $1$ |

## 2.2. S-block substitution table

The used S-block is used as a substitution operation in symmetric encryption algorithms. The table contains n-bit input data and randomly generated output data from m-bit in Figure 3. S-blocks are usually part of the conversion method and are of great importance for the cryptobility of the block encryption algorithm. When changing the input values included in the S-block, the bits in the output values should be selected as any.

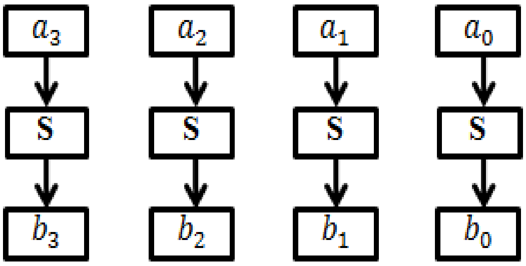


Figure 3. S-block substitution table

The way of chosen the S-block may be different. But its reliability is determined by its cryptographic strength. It is known that the S-block is currently used in many symmetric block encryption algorithms, such as BelT, advanced encryption standard (AES), ShangMi 4 (SM4), GOST28147-89, data encryption standard (DES), and TWOFISH [14].

In the block encryption algorithm using the EM transform method, the selection of the S-block is determined by a mathematical transformation. An irreducible polynomial of the multiplicative group in the Galois field $GF(2^v)$ is chosen, along with any polynomial referred to as bases. The chosen polynomial is then exponentiated by the elements of the multiplicative group, as shown in formula (22).

$$S_i = A(x)^{p_i(x)}(x)\, mod\, P\,(x),\ i = \overline{0, 2^{ord(P(x))} - 1}.) \tag{22}$$

Where $S_i$ is S-block, $A(x)$ is polynomial called base, $p_i(x)$ is multiplicative group elements, $P(x)$ is module irreducible polynomial. The S-box permutations obtained by the proposed method are shown in Table 2.

Table 2. S-box used in the proposed encryption algorithm SEA128

| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 1B | 34 | 5E | D4 | 65 | 13 | EC | 8F | C6 | 92 | A8 | 74 | C9 | B | F5 |
| 8D | F0 | FA | 14 | AD | 03 | 2D | 5C | E2 | D | AF | 35 | 45 | E0 | 3B | C7 |
| 89 | 9C | 2A | 1D | 6E | E6 | 61 | 7F | 3C | 86 | 05 | 77 | E4 | 57 | 17 | 80 |
| 5F | CF | 51 | 4D | 38 | EA | D5 | 7E | 27 | B2 | 5B | A3 | 81 | 44 | FB | F |
| 99 | 5D | F9 | 39 | F1 | E1 | 20 | F3 | D7 | 48 | 4F | E | 82 | 69 | A7 | ED |
| 94 | F2 | CC | 7C | 11 | DA | E7 | 7A | 4B | 62 | 52 | 60 | 64 | 08 | D8 | D1 |
| 12 | F7 | BB | 98 | 46 | CD | 67 | 25 | 84 | 33 | 1F | 58 | 8E | DD | A6 | F6 |
| A0 | AC | 18 | 19 | 02 | 36 | 68 | BC | D9 | CA | 26 | A9 | 6F | FD | 55 | 21 |
| E8 | E3 | 16 | 9B | 6B | 91 | 85 | 28 | 2B | 06 | 5A | B8 | B5 | 1A | 2F | 6A |
| 8A | B1 | 76 | FF | 63 | 49 | 54 | 3A | DC | BD | C2 | FE | 78 | 7D | A | EE |
| B9 | AE | 2E | 71 | BE | EF | A2 | 9A | 70 | A5 | DB | FC | 4E | 15 | B6 | 37 |
| 73 | 88 | 87 | 1E | 43 | BA | 83 | 72 | 93 | B3 | 40 | 97 | DF | 90 | 9E | 1C |
| 75 | D2 | 3F | AB | 59 | 95 | E9 | F8 | 22 | C5 | BF | F4 | 96 | C4 | A4 | C0 |
| C8 | 10 | C1 | D3 | 24 | 9F | 07 | 41 | 8C | EB | CE | 4A | 79 | 66 | 3E | B0 |
| 6D | CB | 3D | 9D | 31 | 29 | 30 | 32 | 04 | 6C | D0 | 09 | C3 | E5 | 4C | 23 |
| DE | 8B | AA | 42 | A1 | B7 | 2C | 47 | D6 | 53 | 7B | 50 | 56 | C | B4 | 00 |

## 3. ENCRYPTION ALGORITHMS ANALYSIS

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. Statistical security (or strength) of block cipher algorithms is related to their ability to withstand various types of cryptanalyses based on the statistical properties 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.

The encryption algorithm model was implemented in C++. An analysis and evaluation of tests were conducted to assess the statistical safety of the proposed algorithm. For testing the proposed algorithm: i) 15 files of different sizes and ii) 10 full-key and different working bases were used. 150 ciphertext obtained by proposed algorithm were tested to statistical safety tests. One of the primary aspects in evaluating the strength of cryptographic algorithms involves assessing their statistical security. If the sequence of ciphertexts generated by an encryption algorithm provides properties of randomness, then the algorithm is considered statistically secure [15]. Hence, the statistical properties of the proposed encryption algorithm were examined using D. Knuth and NIST tests [16], [17].

In 1969, Knuth [18] presented the first set of statistical tests in his classic work “The Art of Programming.” D. Knut's tests are based on a statistical criterion: check for uncoupled runs, check for intervals, check for combinations, test for coupon collector, check for permutations, check for monotony and check for correlation. The tests are based on a statistical $\chi^2$ criterion. The calculated value of statistics is $\chi^2$ with tabular results and, depending on the probability of the appearance of such statistics, a conclusion is made about its quality [19]. D. Knut's tests use graphical and evaluation tests to study the statistical properties of ciphertext. Graphic tests results may not be exact, as the graphic viewer can not have any actual results, so there may be various deviations. The number of successfully passed tests by D. Knuth shown in Figure 4.

Graphic tests results: Histogram of the distribution of elements, distribution on the plane, checking the series, checking for monotony, byte autocorrelation function (ACF), bit autocorrelation function (ACF), graphic spectral test, complexity profile was tested accordingly 147, 148, 149, 143, 144, 147, 149, and 150 ciphertexts. Assessment test results show which results are passed or and which are not as shown in Figure 5.

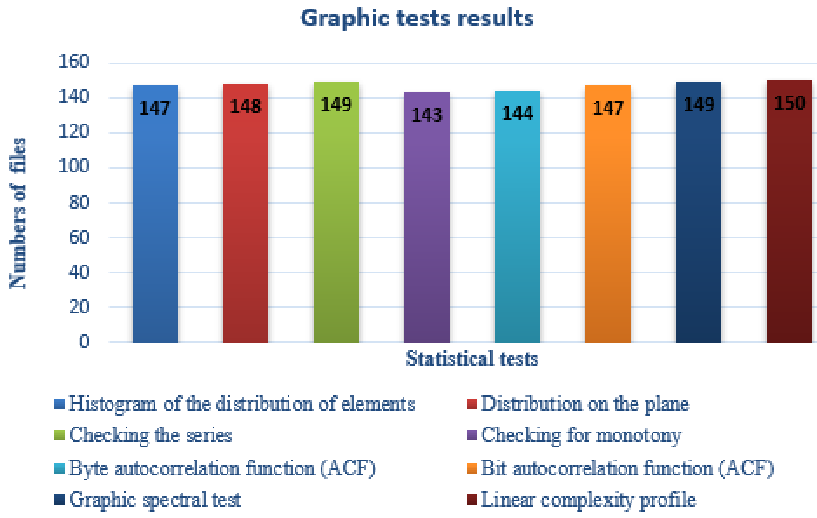


Figure 4. Graphic tests results

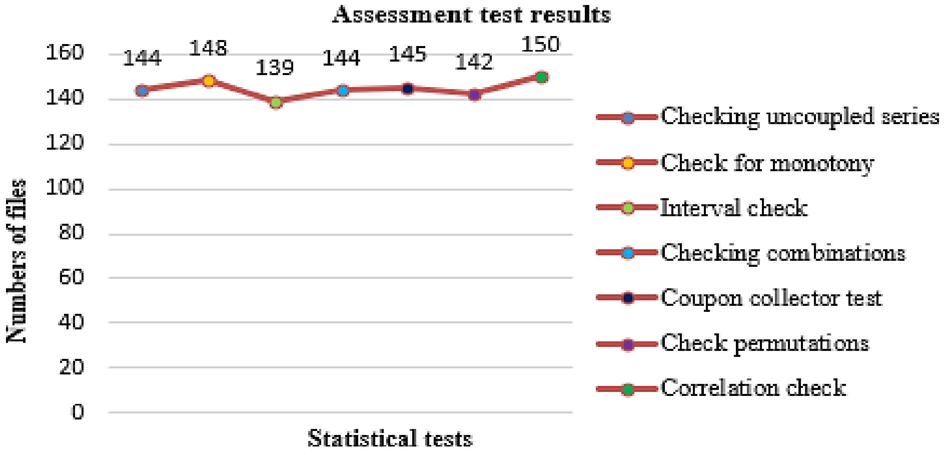


Figure 5. Assessment test results

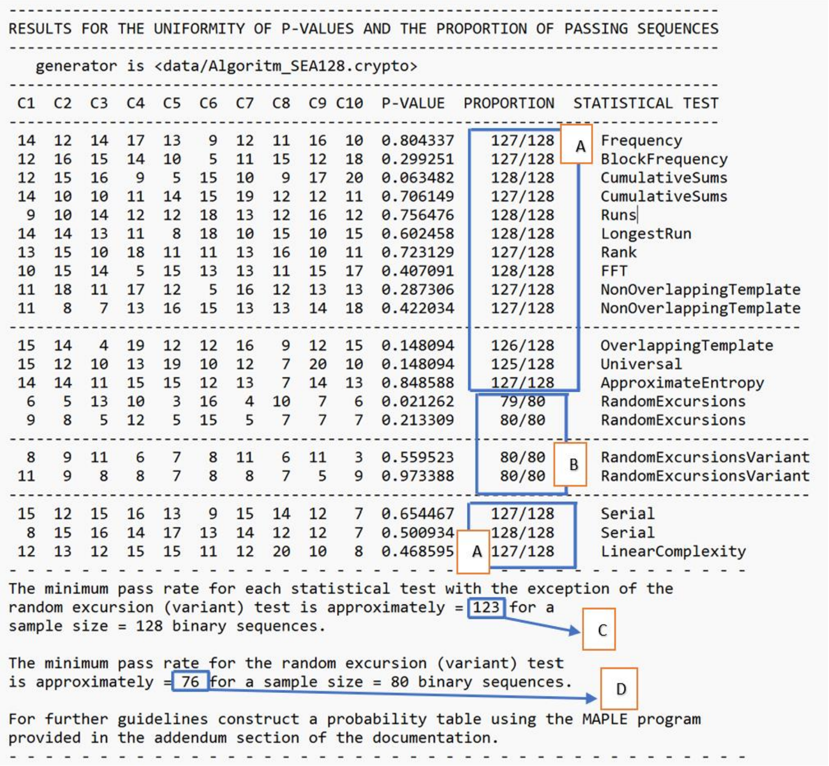
Assessment test results: checking uncoupled series, checking for monotony, interval check, checking combinations, coupon collector test, check permutations, the correlation check was test passed, respectively, 144, 148, 139, 144, 114, 145, 142, and 150 ciphertexts. NIST has created several statistical tests [20], that involve calculating a statistic representing a particular property of a sequence and comparing it to a reference statistic. These reference statistics are derived mathematically, a topic extensively covered in various theorems and scientific papers in the fields of cryptography, probability theory, and number theory.

To investigate the statistical security of the proposed SEA128 encryption algorithm, the following NIST statistical tests [21] were used: frequency (Monobit) test, frequency test within a block, runs test, test for the longest run of ones in a block, binary matrix rank test, discrete Fourier transform (spectral) test, non-overlapping template matching test, overlapping template matching test, Maurer’s Universal statistical test, linear complexity test, serial test, approximate entropy test, Cumulative Sums (Cusum) test, random excursions test, random excursions variant test.

In each test, a P-value is calculated to indicate the level of randomness. A P-value of 1 signifies an ideally random sequence, while a P-value of 0 indicates a completely predictable sequence. The P-value is then compared to a threshold level of α (randomness), typically set at 0.01. If the P-value exceeds α, the null hypothesis is accepted, and the sequence is considered random; otherwise, it is deemed non-random. This process leads to the following conclusions [22]: i) if the $p\ value \geq 0.01$ satisfies the condition, then the ciphertext is considered random with a trust level of 99%; and ii) if the $p\ value \leq 0.01$ satisfies the condition, then the ciphertext is considered non-random with a trust level of 99%.

The test tool assesses randomness by analyzing the proportion of sequences that pass statistical tests for homogeneity and examining the distribution of P-values, as detailed in the article [23]. This tool can perform all statistical tests simultaneously. In this case, parameters common to all tests are sequence length and sample size, both of which are required.

A sequence length of 1,000,000 bits and a sample size of 128 were selected as parameters to test the ciphertext obtained from the proposed encryption algorithm for randomness. If all the A and B values are greater or equal than C and D respectively, the test result is PASS. The results obtained are presented in Figure 6. To investigate the statistical security of the output sequences of the SEA 128 encryption algorithm using the NIST tests, the same 150 files were used as for the Knuth statistical tests. The number of successful tests obtained as a result of the study of the SEA128 encryption algorithm is shown in Figure 7.



```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <data/Algoritm_SEA128.crypto>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 14  12  14  17  13   9  12  11  16  10  0.804337    127/128     Frequency
 12  16  15  14  10   5  11  15  12  18  0.299251    127/128     BlockFrequency
 12  15  16   9   5  15  10   9  17  20  0.063482    128/128     CumulativeSums
 14  10  10  11  14  15  19  12  12  11  0.706149    127/128     CumulativeSums
  9  10  14  12  12  18  13  12  16  12  0.756476    128/128     Runs
 14  14  13  11   8  18  10  15  10  15  0.602458    128/128     LongestRun
 13  15  10  18  11  11  13  16  10  11  0.723129    127/128     Rank
 10  15  14   5  15  13  13  11  15  17  0.407091    128/128     FFT
 11  18  11  17  12   5  16  12  13  13  0.287306    127/128     NonOverlappingTemplate
 11   8   7  13  16  15  13  13  14  18  0.422034    127/128     NonOverlappingTemplate
-----------------------------------------------------------------------------------------
 15  14   4  19  12  12  16   9  12  15  0.148094    126/128     OverlappingTemplate
 15  12  10  13  19  10  12   7  20  10  0.148094    125/128     Universal
 14  14  11  15  15  12  13   7  14  13  0.848588    127/128     ApproximateEntropy
  6   5  13  10   3  16   4  10   7   6  0.021262     79/80      RandomExcursions
  9   8   5  12   5  15   5   7   7   7  0.213309     80/80      RandomExcursions
------------------------------------------------------------------------------------------
  8   9  11   6   7   8  11   6  11   3  0.559523     80/80      RandomExcursionsVariant
 11   9   8   8   7   8   8   7   5   9  0.973388     80/80      RandomExcursionsVariant
------------------------------------------------------------------------------------------
 15  12  15  16  13   9  15  14  12   7  0.654467    127/128     Serial
  8  15  16  14  17  13  14  12  12   7  0.500934    128/128     Serial
 12  13  12  15  15  11  12  20  10   8  0.468595    127/128     LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 123 for a
sample size = 128 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately = 76 for a sample size = 80 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 6. Descriptions in final analysis report

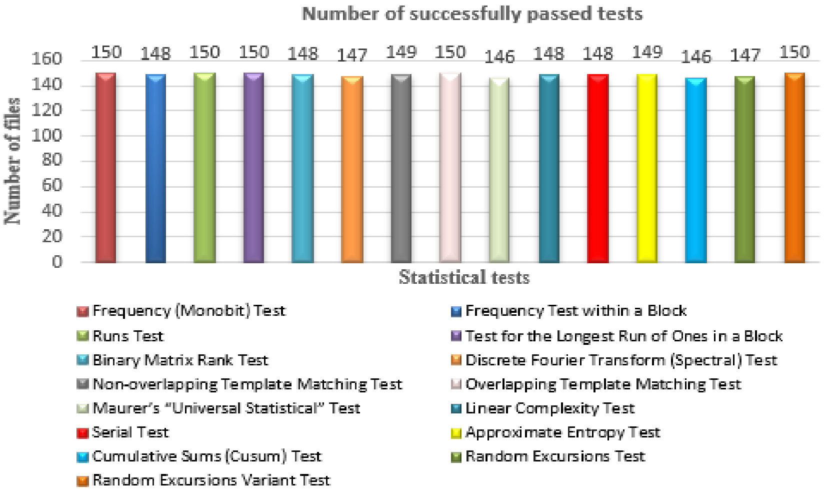


Figure 7. NIST tests results

It is known that the determination of the cryptographic strength of block encryption algorithms is directly related to the strength of the S-block applied to these algorithms. Therefore, a linear, differential and algebraic analysis was performed on the S-block applied to the proposed algorithm and compared with other algorithms [24], [25]. The results of linear and differential analysis are shown in Table 3, and the results of algebraic analysis are shown in Table 4 and Figure 8.

We used standard algebraic analysis to evaluate the quality of the S-box applied to the NBC encryption algorithm. This analysis includes bit independence, nonlinearity, strict avalanche criterion, and probabilities of both differential and linear approximations [26]. At least two examples of the results of executing this encryption algorithm under minimal conditions, that is to say, with minimal disturbances on its inputs (one different bit per execution).

Table 3. Linear and differential cryptanalysis results

| Name | Analysis | Minimum value | Maximum value | Chi-square value | Degree of freedom |
|---|---|---|---|---|---|
| DES | Linear | 12 | 48 | 480 | 944 |
| | Differential | 0 | 16 | 20514 | 1007 |
| GOST 28147-89 | Linear | 2 | 14 | 120 | 224 |
| | Differential | 0 | 8 | 480 | 239 |
| GOST R 34.13-2015 | Linear | 100 | 156 | 32640 | 65024 |
| | Differential | 0 | 8 | 111297 | 65279 |
| AES | Linear | 111 | 145 | 32639 | 65024 |
| | Differential | 0 | 5 | 67123 | 65279 |
| Proposed block encryption | Linear | 100 | 156 | 32640 | 65024 |
| algorithm SEA128 | Differential | 0 | 8 | 111960 | 65279 |

Table 4. SAC analysis of S-box (SEA128)

| | Bit 0 | Bit 1 | Bit 2 | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 |
|---|---|---|---|---|---|---|---|---|
| $f_0$ | 136 | 128 | 116 | 132 | 140 | 132 | 120 | 140 |
| $f_1$ | 132 | 120 | 132 | 120 | 124 | 128 | 120 | 112 |
| $f_2$ | 124 | 120 | 128 | 136 | 121 | 112 | 132 | 136 |
| $f_3$ | 124 | 128 | 120 | 144 | 136 | 124 | 140 | 120 |
| $f_4$ | 128 | 132 | 120 | 144 | 136 | 132 | 120 | 116 |
| $f_5$ | 124 | 128 | 136 | 120 | 144 | 120 | 132 | 124 |
| $f_6$ | 120 | 132 | 120 | 124 | 128 | 120 | 112 | 132 |
| $f_7$ | 128 | 120 | 144 | 136 | 124 | 140 | 120 | 124 |

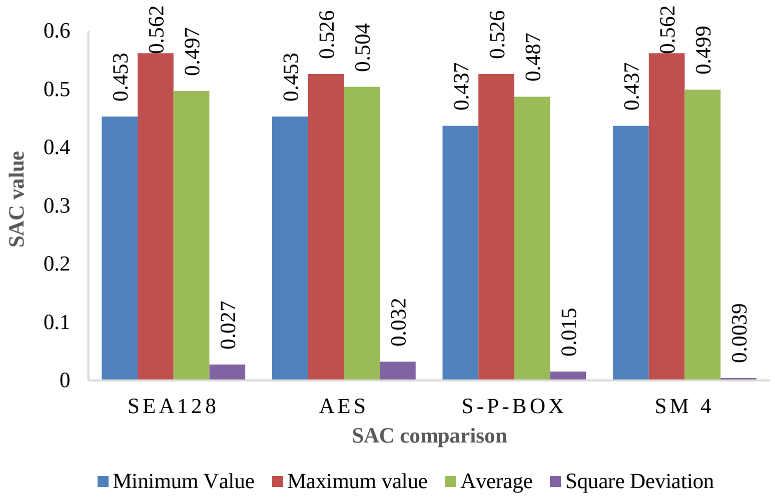


Figure 8. Graphical representation of SAC

## 4. CONCLUSION

The proposed algorithm relies on exponentiation modulo, treating large-digit numbers in residue classes within a positional number system as several sets of smaller digits. This enables operations using an index table based on the selected working bases. Here's a paraphrased version of the text: This feature enables quicker error detection, correction, and implementation. The S-box used in the block encryption algorithm based on the EM transform method shows good results in linear and differential analysis. The program implementation of the proposed algorithm has been developed and the statistical security of ciphertexts encrypted by this algorithm was tested through assessment and graphic tests. The research of other algorithm properties is planned for the future.

## ACKNOWLEDGEMENTS

Research work was carried out within the framework of the project BR24993052 “Development and study of cryptographic algorithms for information protection in resource-constrained systems and evaluation of their strength”, which is being implemented at the Institute of Information and Computer Technologies.

## REFERENCES

[1] R. G. Biyashev, A. Smolarz, K. T. Algazy, and A. Khompysh, “Encryption algorithm ‘QAMAL NPNS’ based on a nonpositional polynomial notation,” *Journal of Mathematics, Mechanics and Computer Science*, vol. 105, no. 1, pp. 198–207, Apr. 2020, doi: 10.26577/JMMCS.2020.v105.i1.17.

[2] A. Khompysh, N. Kapalova, O. Lizunov, D. Dilmukhanbet, and S. Kairat, “Development of a new lightweight encryption algorithm,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, pp. 452–459, 2023, doi: 10.14569/IJACSA.2023.0140548.

[3] R. G. Biyashev and S. E. Nyssanbayeva, “Algorithm for creating a digital signature with error detection and correction,” *Cybernetics and Systems Analysis*, vol. 48, no. 4, pp. 489–497, Jul. 2012, doi: 10.1007/s10559-012-9428-5.

[4] A. Khompysh, N. A. Kapalova, D. S. Dyusenbayev, and V. A. Varennikov, “Study of the statistical security of the AL04 encryption algorithm,” *Series of Physical and mathematical sciences*, vol. 87, no. 3, pp. 154–163, 2024, doi: https://doi.org/10.51889/2959-5894.2024.87.3.014.

[5] H. Najm, H. K. Hoomod, and R. Hassan, “A proposed hybrid cryptography algorithm based on GOST and salsa (20),” *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 3, pp. 1829–1835, 2020, doi: 10.21533/pen.v8i3.1619.

[6] T. U. Haq, T. Shah, G. F. Siddiqui, M. Z. Iqbal, I. A. Hameed, and H. Jamil, “Improved twofish algorithm: a digital image enciphering application,” *IEEE Access*, vol. 9, pp. 76518–76530, 2021, doi: 10.1109/ACCESS.2021.3081792.

[7] K. T. Algazy *et al.*, “Differential cryptanalysis of new qamal encryption algorithm,” *International Journal of Electronics and Telecommunications*, vol. 66, no. 4, pp. 647–653, 2020, doi: 10.24425-ijet.2020.134023/745.

[8] N. I. Chervyakov, P. Lyakhov, M. Babenko, I. N. Lavrinenko, and A. V Lavrinenko, *Computer calculations based on modular algebra*, (In Russian) Stavropol: Publishing and information center "Fabula", 2015. doi: 10.13140/RG.2.1.3749.1283.

[9] R. G. Biyashev, N. A. Kapalova, D. S. Dyusenbayev, K. T. Algazy, W. Wojcik, and A. Smolarz, “Development and analysis of symmetric encryption algorithm qamal based on a substitution-permutation network,” *International Journal of Electronics and Telecommunications*, vol. 67, no. 1, pp. 127–132, 2021, doi: 10.24425/ijet.2021.135954.

[10] S. M. Kareem and D. A. M. S. Rahma, “A modified on twofish algorithm based on cyclic group and irreducible polynomial in GF (28),” *Al-Qadisiyah Journal of Pure Science*, vol. 25, no. 1, pp. 1–9, 2020, doi: 10.29350/2411-3514.1220.

[11] M. M. Hazzazi, S. Attuluri, Z. Bassfar, and K. Joshi, “A novel cipher-based data encryption with Galois field theory,” *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063287.

[12] L. G. Nardo, E. G. Nepomuceno, G. T. Bastos, T. A. Santos, D. N. Butusov, and J. Arias-Garcia, “A reliable chaos-based cryptography using Galois field,” *Chaos*, vol. 31, no. 9, 2021, doi: 10.1063/5.0061639.

[13] A. R. Omondi, “Modular exponentiation, inversion, and division,” *Advances in Information Security*, vol. 77, pp. 183–201, 2020, doi: 10.1007/978-3-030-34142-8_6.

[14] A. Khompysh, N. Kapalova, K. Algazy, D. Dyusenbayev, and K. Sakan, “Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information,” *Cogent Engineering*, vol. 9, no. 1, 2022, doi: 10.1080/23311916.2022.2080623.

[15] S. Popereshnyak, “Technique of the testing of pseudorandom sequences,” *International Journal of Computing*, pp. 387–398, Sep. 2020, doi: 10.47839/ijc.19.3.1888.

[16] O. Kocak, F. Sulak, A. Doganaksoy, and M. Uguz, “Modifications of Knuth randomness tests for integer and binary sequences,” *Communications Faculty of Science University of Ankara Series A1Mathematics and Statistics*, vol. 67, no. 2, pp. 64–81, 2018, doi: 10.1501/commua1_0000000862.

[17] M. P. Savelov, “The limit joint distributions of statistics of three tests of the NIST package,” *Discrete Mathematics and Applications*, vol. 33, no. 4, pp. 247–257, 2023, doi: 10.1515/dma-2023-0022.

[18] D. E. Knuth, “Art of computer programming, the: semi numerical algorithms,” 3rd Edition, Addison Wesley Longman, 2011.

[19] O. Kuznetsov, N. Poluyanenko, E. Frontoni, and S. Kandiy, “Enhancing smart communication security: a novel cost function for efficient S-box generation in symmetric key cryptography,” *Cryptography*, vol. 8, no. 2, 2024, doi: 10.3390/cryptography8020017.

[20] A. Perov, “Using NIST statistical tests for the analysis of the output sequences of block ciphers,” *Science Bulletin of the Novosibirsk State Technical University*, no. 3, pp. 87–96, 2019, doi: 10.17212/1814-1196-2019-3-87-96.

[21] M. O. Pikuza and S. Y. Mikhnevich, “Testing a hardware random number generator using NIST statistical test suite,” *Doklady BGUIR*, vol. 19, no. 4, pp. 37–42, 2021, doi: 10.35596/1729-7648-2021-19-4-37-42.

[22] A. Spanos, “How the post-data severity converts testing results into evidence for or against pertinent inferential claims,” *Entropy*, vol. 26, no. 1, 2024, doi: 10.3390/e26010095.

[23] A. Rukhin, J. Soto, and J. Nechvatal, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Gaithersburg, MD, 2010, doi: 10.6028/NIST.SP.800-22r1a.

[24] M. Liu, X. Lu, and D. Lin, “Differential-linear cryptanalysis from an algebraic perspective,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12827 LNCS, pp. 247–277, 2021, doi: 10.1007/978-3-030-84252-9_9.

[25] E. Ishchukova, E. Maro, and P. Pristalov, “Algebraic analysis of a simplified encryption algorithm GOST R 34.12-2015,” *Computation*, vol. 8, no. 2, p. 51, 2020, doi: 10.3390/COMPUTATION8020051.

[26] Y. Naseer, T. Shah, D. Shah, and S. Hussain, “A novel algorithm of constructing highly nonlinear s-p-boxes,” *Cryptography*, vol. 3, no. 1, pp. 1–13, 2019, doi: 10.3390/cryptography3010006.

## BIOGRAPHIES OF AUTHORS

**Ardabek Khompysh** graduated from the Faculty of Information Technology of the Satbayev University, Almaty, Kazakhstan, with the specialty informatics in 2008. Research scientist at the Institute of Information and Computational Technologies, PhD in specialty information security systems. Theme of scientific research development and research of reliable algorithms for generating pseudorandom sequences used to generate key sequences for symmetric block and stream encryption, as well as the development of cryptographic information protection algorithms using modular arithmetic. Published 20 works in foreign and domestic publications. Received two certificates of state registration of the intellectual property of the Republic of Kazakhstan. He can be contacted at email: ardabek@mail.ru.

**Dilmukhanbet Dyusenbayev** graduated from the Faculty of Mechanics and Mathematics of Al-Farabi Kazakh National University (KazNU), Almaty, Kazakhstan, with the specialty mathematics in 1994. Between 1994 and 1998, he worked as a researcher at the Research Institute of Informatics and Management, Almaty, Kazakhstan. Later, he taught mathematics at the Republican School of Physics and Mathematics. In 2007-2009, he studied computer science and computer engineering at Bauman Moscow State Technical University (MVTU, Moscow, Russia). For several years, he worked in the field of information in the state structure. Since 2015, he has been working as a researcher at the Scientific Institute of Information and Computing Technologies in Almaty, Kazakhstan. In addition, since 2019, he has been working as a senior lecturer at the Faculty of Mechanics and Mathematics at KazNU. His field of scientific research is information protection in the public and private sectors. He can be contacted at email: dimash_dds@mail.ru.

**Muratkhan Maxmet** graduated from the Faculty of Information Technology of the Satbayev University, Almaty, Kazakhstan, with the specialty informatics in 2008. In 2008-2013, he studied religious studies at Egyptian University of Islamic Culture Nur-Mubarak. Director of the Academic Affairs Department of Nur-Mubarak Egyptian University of Islamic Culture. His research interests include current issues in the field of Islamic studies, information security in information systems. Published 10 works in foreign and domestic publications. He can be contacted at email: murat1215@mail.ru.