COMPUTER SCIENCE | RESEARCH ARTICLE

A block encryption algorithm based on exponentiation transform

Nursulu Kapalova¹, Ardabek Khompysh²*, Müslüm Arici³ and Kunbolat Algazy²

Abstract: This paper proposes a new block encryption algorithm for cryptographic information protection. It describes a new transformation method EM (Exponentiation Module), which is part of the algorithm, and a method of S-box obtaining. The paper also considers an optimization technique to advance the efficiency of key selection and calculation. We discuss the possibility to obtain good results by applying the peculiar properties of cryptographic primitives in the Galois field. To increase the strength and speed of the encryption algorithm, we used a nonpositional polynomial notation and an indexed view for the Galois field. The paper provides for statistical properties of the ciphertext obtained with the developed algorithm. We also present the results of differential and linear cryptanalysis of the S-box used.

Subjects: Algorithms & Complexity; Computing & IT Security; Computer Engineering; Computer Science; General

Keywords: nonpositional polynomial notations; plaintext; key; ciphertext; index table; S-box; inverse element; cryptography; encryption algorithm

1. Introduction

The widespread use of computer technology in automated information processing and control systems has brought to the fore the problem of protecting information circulating in computer systems from unauthorized access (Biyashev, 1985). Information security in computer systems has a number of specific features related to the fact that information is not rigidly associated with

ABOUT THE AUTHOR

Kapalova Nursulu Leading Research Scientist at the Institute of Information and Computational Technologies, Cond.Tech.Sc.
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 84 works in foreign and domestic publications. Received 9 certificates of state registration of the intellectual property of the Republic of Kazakhstan.
Corresponding author: Ardabek Khompysh - PhD student from KazNU, IICT in specialty: «Information Security Systems». Research interests theme - Development study of information protection algorithm using the non positional number system (scale of notation).

PUBLIC INTEREST STATEMENT

The widespread use of computer technology in automated information processing and control systems has exacerbated the problem of protecting information circulating in computer systems from unauthorized access. One of the main ways of protecting information is cryptographic methods. The article proposes a new encryption algorithm for cryptographic information protection. An optimization method is also considered for implementations of the proposed algorithm, which increases the efficiency of key selection and calculation. The results of the study of the reliability of the proposed algorithm and differential and linear cryptanalysis of the used S-block are presented.
a medium, and can be easily and quickly copied and transmitted over communication channels. There are a plethora of information security threats that can be perpetrated by both external intruders and insiders (Amerbayev et al., 2005).

A comprehensive solution to the problems of protecting electronic information can only be obtained with cryptographic methods that allow solving the most important problems of secure automated processing and data transfer. Cryptographic methods of information protection are special methods of encryption, coding, or other transformation of information that makes the content inaccessible unless a cryptogram key and inverse transformation are presented (Chipiga, 2009). The cryptographic information protection facility has become the main tool to protect data from unauthorized access. Today in the world, in connection with the active growth of digital technologies, the branches of science associated with cryptographic methods of information protection are rapidly developing. Papers (Chengjing et al., 2019; Liu et al., 2018; Ullah et al., 2018; Xiong et al., 2018a) describe these issues in detail, the authors carried out colossal work to review scientific articles on the cryptographic protection of information, including encryption algorithms designed to protect the information in the form of images. In some other works, the authors considered several encryption algorithms and the results of cryptographic attacks against them (Li et al., 2017, 2018; Xiong et al., 2018b).

Cryptographic methods of protection are certainly the most reliable protection techniques, since they secure the information itself, but not access to it. Modern cryptography includes four major sections: symmetric cryptosystems; public-key cryptosystems; digital signature; and key management (Nyssanbayeva et al., 2016). Symmetric cryptosystems use the same key for both encryption and decryption. The whole variety of existing cryptographic methods in symmetric cryptosystems can be reduced to the following four classes of transformations:

- substitution, where the characters of the encrypted text are replaced by characters of the same or another alphabet under a predetermined rule;
- permutation, where characters of the encrypted text are rearranged according to a certain rule within a given block of the transmitted text;
- analytical transformation, where the encrypted text is converted according to a certain analytical rule, for example, additive stream cipher involves modular addition of the source text by a pseudorandom sequence generated on the basis of the key;
- combined transformation represents a sequence of basic transformation techniques applied to a block (part) of the text under encryption.

Block ciphers in practice are more common than “pure” transformations of one or another class due to their higher cryptographic strength. The Russian and American encryption standards are based on the class of block ciphers (Babenko & Ischukova, 2006; Biyashev & Nyssanbayeva, 2012).

Currently, symmetric block encryption algorithms are the main cryptographic means of ensuring confidentiality when processing information in modern information and telecommunication systems. At the core of present-day ciphers is Kirchhoff’s principle, according to which the security of a cipher is ensured by keeping secret the key, rather than the encryption algorithm (Biyashev et al., 2013). Most block symmetric encryption algorithms use the following types of operations: table substitution, where a group of bits is mapped to another group of bits (S-box); permutation, which is used to rearrange message bits; addition operation modulo 2, denoted by XOR or ⊕; and cyclic shift by a certain number of bits (Babenko & Ischukova, 2006; Moldovyan, 2002). At the same time, modern high-speed methods of cryptographic conversion make it possible to preserve the initial performance of automated systems. Cryptographic data transformations are the most effective means of ensuring data confidentiality, integrity, and authenticity (Chipiga, 2007). Encryption algorithms using systems of residual classes have the following advantages: lack of inter-bit transfers; relatively small numbers used in modular operations; the ability to detect and correct errors; the possibility of developing highly effective means of protecting information in various electronic systems and networks.
In this paper, we propose a new method of the cryptographic transformation EM (Exponentiation Module) and a block encryption algorithm for cryptographic information protection based on the transformation EM and an S-box. The scientific and practical significance of this work lies in the fact that the results obtained will contribute to the development and creation of cryptographic information protection facilities in Kazakhstan. The proposed encryption algorithm at the proper level ensures the security and confidentiality of the information containing images. The developed encryption algorithm was experimentally tested for statistical security of encrypted data and investigated by some cryptanalysis methods.

2. Development of a symmetric block encryption algorithm based on EM
The encryption algorithm includes combining a key with a plaintext using the bitwise addition operation, the developed EM (Exponentiation Module) transformation procedures in a non-positional polynomial notation (NPN) on the basis of modular exponentiation in the extended Galois field GF(2^m), and an S-box substitution table.

2.1. EM transformation
The EM transformation method using non-positional polynomial notations based on exponentiation in the extended Galois field GF(2^m) consists of three stages:

- selection of a system of polynomial bases (formation of an NPN) and the order of their arrangement;
- generation of round keys;
- transformation and inverse transformation of input data.

Stage 1. Let \( p_1(x), p_2(x), \ldots, p_n(x) \) be irreducible binary polynomials used as working bases. A polynomial \( P(x) = p_1(x)p_2(x) \ldots p_n(x) \) of degree \( m = m_1 + m_2 + \ldots + m_n \) is the main working range of the NPN. Here, any polynomial of degree fewer than \( m \) is uniquely representable in the form of its residues modulo the working bases (or the remainders in division by) \( p_1(x), p_2(x), \ldots, p_n(x) \) respectively. Then a data block of length \( N \) bits can be interpreted as a sequence of the remainders \( \alpha_1(x), \alpha_2(x), \ldots, \alpha_5(x) \) of dividing a polynomial \( F(x) \) by the working bases \( p_1(x), p_2(x), \ldots, p_5(x) \) respectively:

\[
F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_5(x)),
\]

where \( F(x) = \alpha_i(x) \pmod{p_i(x)}, i = 1 \ldots 5 \). In Equation (1) the remainders \( \alpha_1(x), \alpha_2(x), \ldots, \alpha_5(x) \) are selected so that the first \( l_1 \) bits of a message assign to binary coefficients of the remainder \( \alpha_1(x) \), the next \( l_2 \) bits assign to binary coefficients of the remainder \( \alpha_2(x) \), etc., and the last \( l_5 \) bits assign to binary coefficients of \( \alpha_5(x) \).

Let us consider the process of selecting the working bases. Let \( n_i \) be the number of irreducible binary polynomials of degree \( m_i \). The residues modulo these polynomials are all binary polynomials of degree no higher than \( m_i - 1 \). To represent each of these residues, it needs \( m_i \) bits (similarly for the residues modulo other bases). Let respectively \( n_i \) be the number of irreducible binary polynomials of degree \( m_i \), etc., and finally \( n_5 \) be the number of irreducible polynomials of degree \( m_5 \). Then the procedure for selecting all systems of working bases of degree \( m_i \) reduces to determining all possible solutions of the polynomial equation (Babenko & Ischukova, 2006; Biyashev & Nyssanbayeva, 2012; Biyashev et al., 2013; Nyssanbayeva et al., 2016):

\[
r_1m_1 + r_2m_2 + \ldots + r_5m_5 = N,
\]

where \( 0 \leq r_i \leq n_i, i = 1 \ldots 5 \) are unknown coefficients, \( r_i \) is the number of selected irreducible polynomials of degree \( m_i \). One solution of the Equation (2) is one particular set of coefficients \( r_i \).
determining one system of working bases with all possible permutations thereof. Since \( n \) is the number of all irreducible polynomials of degree \( m_i \), \( 0 \leq m_i \leq N \), the number of all selected bases is:

\[
S = r_1 + r_2 + \ldots + r_s
\]  

Equation (3) specifies the number of bases \( S \) with residues covering a block of length \( N \) of the given message. These \( S \) bases are chosen out of the total number of all irreducible polynomials of different degrees. All chosen bases must be different from each other even though they are irreducible polynomials of the same degree, as the theory of residue systems relies on the Chinese remainder theorem (Amerbayev et al., 2005).

Stage 2. To implement the EM transformation method using modular exponential operations in the extended Galois field \( GF(2^r) \), we obtain the value of \( k_i \) utilizing a pseudorandom sequence generator (PSG):

1. generation of a key (pseudorandom) sequence;
2. interpretation of the obtained sequence in the working bases;
3. decimalization of the interpreted sequence;
4. checking for \( \text{GCD}(k_i, 2^{\nu(r_i)} - 1) = 1 \), \( i \in \overline{1, S} \). If this condition is true, then we proceed to Stage 3, otherwise, we return to Stage 1.

Stage 3. As is known, a modular exponential operation takes a good deal of time. To reduce the execution time of the procedure, it is expedient to use an NPN.

Let us consider a procedure of stream cipher using an NPN. In this case, for the proposed algorithm, we select working bases as per (1) in the Galois field \( GF(2^r) \). Most scientists believe that the Galois fields \( GF(2^r) \) allow much room for the implementation of various cryptographic functions to ensure information confidentiality and integrity (Moldovyan, 2002). The proposed transformation method divides input data into 128-bit blocks. Prior to encryption, each block is divided into 4 32-bit sub-blocks. Each sub-block is interpreted as a sequence of remainders in the selected working bases, i.e., in our case, \( N = 32 \):

\[
A(x) = a_1(x), a_2(x), \ldots , a_S(x).
\]  

Where \( a_i(x) = \overline{1, S} \) are the blocks obtained.

The formula to transform the blocks in the expression (4) is:

\[
b_i(x) = a_i^k(x) \mod p_i(x), i = \overline{1, S}.
\]  

Equation (5) is the resulting ciphertext takes the form:

\[
B(x) = (b_1(x), b_2(x), \ldots , b_S(x)).
\]  

In this case, the inverse (5) is given by:

\[
a_i(x) = b_i^{k^{-1}}(x) \mod p_i(x), i = \overline{1, S}.
\]  

Equation (7) We can rewrite the plaintext obtained in (7):

\[
A(x) = (a_1(x), a_2(x), \ldots , a_S(x)).
\]  

Equation (8)
The proposed algorithm calculates the inverse keys for each block:

\[ k_i \cdot (k_i)^{-1} \equiv 1 \mod \left(2^{\deg(p(x))} - 1\right) \text{, } i = 1, \ldots, 3. \]  \hfill (9)

However, as noted above, a modular exponential operation is regarded as a low-speed one. To increase the performance of a cryptographic system, it is advantageous to use an indexed view of finite field elements (Chipiga, 2009). We complete an index table for the EM transformation in the selected working bases \( p_i(x) \):

\[ a(x) = \alpha^i \mod p_i(x), \quad j = 0, 2^{\deg(p_i(x))} - 2, \]  \hfill (10)

where \( \alpha \) is the generator of the multiplicative group of \( GF(p^r) \).

As an example, Table 1 shows the indexed view of the elements of the extended Galois field \( GF(2^3) \) generated by the polynomial \( p(x) = x^3 + x + 1 \).

Let us introduce the following mathematical equation as per the table of indices in the selected working bases:

\[ l = \text{ind}_a a_i(x) \mod p_i(x). \]  \hfill (11)

Here \( l \) is the power or indexed representation of \( a_i(x) \). Then we modify the formula (5) as:

\[ b_i(x) = \left(\alpha^i\right)^{-1} \mod p_i(x) = \left(\alpha^{(l_i \mod 2^{\deg(p_i(x))}) - 1}\right) \mod p_i(x). \]  \hfill (12)

In the process of the inverse transform, we replace \( k_i \) with the inverse element \( (k_i)^{-1} \), i.e. \( l = \text{ind}_a b_i(x) \mod p_i(x) \) and \( a_i(x) = \left(\alpha^i\right)^{-1} \mod p_i(x) = \left(\alpha^{(l_i \mod 2^{\deg(p_i(x))}) - 1}\right) \mod p_i(x) \).

### 2.2. S-box selection

The selection of good S-boxes is a challenging task. There are many competing approaches to solving the task, with four main methods among them.

#### 2.2.1. Random sampling

It is amply that small random S-boxes are insecure, while large random S-boxes may prove to be reasonably good. Random S-boxes having eight and more inputs can be sufficiently secure. The strength of S-boxes will increase, if they are simultaneously both random and depend on the key.

| Power representation \( a(x) \) | Polynomial representation \( p(x) = x^3 + x + 1 \) |
|---------------------------------|------------------------------------------|
| \( \alpha^0 \) | 1 |
| \( \alpha^1 \) | \( x \) |
| \( \alpha^2 \) | \( x^2 \) |
| \( \alpha^3 \) | \( x + 1 \) |
| \( \alpha^4 \) | \( x^2 + x \) |
| \( \alpha^5 \) | \( x^2 + x + 1 \) |
| \( \alpha^6 \) | \( x^2 + 1 \) |
Sampling followed by testing. In some ciphers, random S-boxes are generated first, and then their properties are testing against a set of requirements.

2.2.2. Manual development
Here, mathematical tools are hardly used, as S-boxes are created by using intuitive techniques. Bart Preneel has stated that “... theoretically interesting criteria are not sufficient (for selection of Boolean functions of S-boxes) ...” and “... special design criteria are necessary” (Preneel, 1993).

2.2.3. Mathematical development
S-boxes are generated under mathematical laws, hence they are guaranteed secure against differential and linear cryptanalysis and good diffusion properties (Kapalova & Dyuysenbayev, 2016). It was suggested to combine the “mathematical” and “manual” approaches, but in real practice, randomly chosen S-boxes compete with the ones having certain properties. Among the advantages of the last approach is its optimization against the known cryptanalytical attacks—differential and linear cryptanalysis.

An S-box is an ordinary substitution, i.e. a mapping of m-bit inputs onto n-bit outputs. S-boxes usually form a part of a transformation function and are essential to the strength of an encryption algorithm. Any changes in the input data of an S-box must lead to similar-to-random changes in the output data. The relationship between input and output values should not be linear or easily approximated by linear functions (this particular property is used in the linear cryptanalysis) (Kapalova & Haumen, 2018). It is known that S-boxes are used now in many symmetric encryption algorithms, such as AES, GOST R34.13–2015, DES, Twofish, etc. (Babenko & Ischukova, 2006).

Let us consider a method for producing an S-box in the block encryption algorithm based on the EM transformation. We first select an irreducible polynomial generating a multiplicative group in the Galois field GF(p^n) and any polynomial designated as the base. Then we complete a modular exponential operation over the chosen polynomial:

\[ S_i(x) = A^p(x) mod P(x), \quad i = 0, 2^{deg P(x)} - 1. \]  

(13)

Here, \( S_i(x) \) are the elements of the S-box, \( A(x) \) is the polynomial designated as the base, \( p_i(x) \) are the elements of the multiplicative group, \( P(x) \) is the module (an irreducible polynomial). The substitution table obtained is shown in Table 2.

2.3. Encryption algorithm
The flow chart of the developed encryption algorithm is shown in Figures 1 and 2. The algorithm supports the lengths of the block and key of 128 bits. The number of encryption rounds is 16. Before encryption, the input data are split into 16-byte or 128-bit blocks. The last block, as may be required, is filled according to specified conventions (e.g., with zeroes). Next, the following transformations are performed.

Procedure 1 provides for the addition of the key and a plaintext block modulo 2 (XOR operation). The input block is further split into 4 parts (sub-blocks) of 32 bits, which serve as inputs for subsequent procedures.

Procedure 2. The first and the second input sub-blocks undergo the EM transformation as per the flow chart.

Procedure 3. The third and the fourth input sub-blocks, according to the flow chart, undergo S-box transformation, and then the XOR operation with the results of Procedure 1 is performed.

The last round is completed with the modulo 2 addition of the result to the key.
Table 2. S-box substitution table

|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 01| 1B| 34| 5E| D4| 65| 13| EC| 8F| C6| 92| A8| 74| C9| B |
| 1 | 8D| F0| FA| 14| AD| 03| 2D| 5C| E2| D | AF| 35| 45| E0| 3B| C7|
| 2 | 89| 9C| 2A| 1D| 6E| E6| 61| 7F| 3C| 86| D5| 77| E4| 57| 17| 80|
| 3 | 5F| CF| 51| 4D| 38| EA| D5| 7E| 27| B2| 5B| A3| 81| 44| FB| F |
| 4 | 99| 5D| F9| 39| F1| E1| 20| F3| D7| 48| 4F| E | 82| 69| A7| ED|
| 5 | 94| F2| CC| 7C| 11| DA| E7| 7A| 4B| 62| 52| 60| 64| 08| D8| D1|
| 6 | 12| F7| BB| 98| 46| CD| 67| 25| 84| 33| 1F| 58| 8E| DD| A6| F6|
| 7 | A0| AC| 18| 19| 02| 36| 68| BC| D9| CA| 26| A9| 6F| FD| 55| 21|
| 8 | E8| E3| 16| 9B| 6B| 91| 85| 28| 2B| 06| 5A| B8| B5| 1A| 2F| 6A|
| 9 | 8A| B1| 76| FF| 63| 49| 54| 3A| DC| BD| C2| FE| 78| 7D| A | EE|
| A | B9| AE| 2E| 71| BE| EF| A2| 9A| 70| A5| DB| FC| 4E| 15| B6| 37|
| B | 73| 88| 87| 1E| 43| BA| 83| 72| 93| B3| 40| 97| DF| 90| 9E| 1C|
| C | 75| D2| 3F| AB| 59| 95| E9| F8| 22| C5| BF| F4| 96| C4| A4| C0|
| D | C8| 1D| C1| D3| 24| 9F| 07| 41| 8C| EB| CE| 4A| 79| 66| 3E| B0|
| E | 6D| CB| 3D| 9D| 31| 29| 30| 32| 04| 6C| D0| 09| C3| E5| 4C| 23|
| F | DE| 8B| AA| 42| A1| B7| 2C| 47| D6| 53| 7B| 50| 56| C | B4| 00|

Figure 1. Flow chart of the symmetric block data encryption algorithm based on EM.
3. Results from the statistical analysis of ciphertexts

One of the main constituents to assess the strength of cryptographic algorithms is the assessment of their statistical security. It is believed that an algorithm will be statistically secure if the sequence (ciphertexts) that it generates is as good in its properties as a random one. For experimental sequence assessment, statistical tests are used (Ivanov & Chugunkov, 2003; Knuth, 2004).

The study of the statistical properties of encrypted texts obtained using the encryption algorithm under consideration includes the following successive procedures:

- encryption of plaintexts as per the proposed models;
- execution of a set of statistical tests for the obtained ciphertexts;
- study of the results of the statistical ciphertext testing;
- making decisions on the properties of the obtained ciphertexts for the proposed models.

To test the statistical properties of the ciphertexts obtained using the proposed encryption algorithm, we conducted computer-aided experiments with the use of:

- 10 plaintexts of different sizes and extensions (Table 3);
- 12 keys K1, K2, ..., K12, differing in the number of working bases.

We obtained 120 ciphertexts and tested them for statistical security. For the testing, we used a developed software package implementing a system for evaluating the quality of the ciphertexts based on graphical and assessment tests.
### 3.1. Graphical testing analysis

The results of graphical tests are presented in the form of a histogram (Figure 3). Out of 120 obtained ciphertexts, 116, 119, 118, 109, 114, 117, and 120 ones passed, respectively, the following graphical tests: distribution of elements, plane distribution, checking the series, checking for monotony, byte autocorrelation function (ACF), bit autocorrelation function (ACF), graphical spectral test, and linear complexity profile. Graphical tests showed good results for the texts encrypted with the proposed algorithm.

### 3.2. Assessment testing analysis

The results of graphical tests are interpreted by users, so a disparate treatment thereof is possible. In contrast, assessment tests give a specific numerical characteristic that allows the user to unambiguously determine whether a test is passed or not.

The histogram of the assessment tests is shown in Figure 4.

Out of 120 obtained ciphertexts, 114, 119, 118, 109, 114, 117, 98, and 120 ones passed, respectively, the following assessment tests: checking 0 and 1, checking uncoupled series, symbol test, interval check, checking combinations, coupon collector’s test, permutation test, and correlation check.

#### Table 3. Plaintext files used in testing the encryption algorithm

| File No. | File ext. | Description                                      | Size    |
|----------|-----------|--------------------------------------------------|---------|
| 1        | docx      | Microsoft Word Document                         | 231 KB  |
| 2        | xls       | Microsoft Excel 97–2003 Spreadsheet              | 20.0 KB |
| 3        | pptx      | Microsoft PowerPoint Presentation                | 2.95 MB |
| 4        | pdf       | PDF document                                     | 7.3 MB  |
| 5        | rar       | RAR archive                                      | 2.23 MB |
| 6        | zip       | Zip file                                         | 339 KB  |
| 7        | jpg       | Joint Photographic Experts Group                 | 856 KB  |
| 8        | png       | Corel PaintShop Photo Pro Browser Directory      | 1.1 MB  |
| 9        | txt       | Text file                                        | 78.1 KB |
| 10       | gif       | Graphics Interchange Format                      | 548 KB  |
It follows from the graphical and evaluation tests that the encrypted files are statistically secure. It was also revealed that the encryption algorithm under consideration shows different results for different tests depending on the type of file.

4. Cryptanalysis of the S-box in use

It is known that the cryptostrength of block encryption algorithms depends on the cryptostrength of the S-boxes used in the algorithms. In this context, the linear and differential analyses were performed for the S-boxes used in the proposed algorithm, and the results obtained were compared with the same for the S-boxes of other algorithms (Table 4) (Kapalova & Haumen, 2018).

5. Conclusion

As far as the proposed algorithm is performed based on the modular exponentiation, a long number in a positional number system can be considered in a residue class as a set of smaller numbers, and one can work with an index table in the selected working bases. This, in turn, enables quickly finding and correcting errors and cutting the time taken by the algorithm. It was also established that the S-box used in the block encryption algorithm based on the EM transform

Table 4. Linear and differential cryptanalysis results

| Algorithm                                      | Minimum | Maximum | Chi-square | Degree of freedom |
|------------------------------------------------|---------|---------|------------|-------------------|
| DES                                            | Linear  | 12      | 48         | 480               | 944               |
|                                                |         | 0       | 16         | 20,514            | 1,007             |
| Magma (GOST R34.13–2015)                       | Linear  | 4       | 12         | 120               | 224               |
|                                                |         | 0       | 4          | 384               | 239               |
| Kuznyechik (GOST R34.13–2015)                  | Linear  | 100     | 156        | 32,640            | 65,024            |
|                                                |         | 0       | 8          | 111,297           | 65,279            |
| AES-128                                        | Linear  | 111     | 145        | 32,639            | 65,024            |
|                                                |         | 0       | 5          | 67,123            | 65,279            |
| Block encryption algorithm developed from EM transformation | Linear  | 100     | 156        | 32,640            | 65,024            |
|                                                |         | 0       | 8          | 111,960           | 65,279            |
method showed good results against the linear and differential cryptanalysis. The proposed algorithm was implemented in software, while the ciphertexts obtained were tested for statistical security through the use of assessment and graphical tests. The experimental tests for statistical security demonstrated positive results.

The next stages of the work will be a further study of the strength of the proposed encryption algorithm using other cryptanalysis methods.

Acknowledgements
The research work was carried out within the framework of the project BR05236757 “Development of software and firmware means for cryptographic protection of information during its transfer and storage in information and communications systems and general-purpose networks” at the Institute of Information and Computational Technologies.

Funding
This work was supported by the Ministry of Education and Science of the Republic of Kazakhstan, Institute of Information and Computational Technologies (BR05236757).

Author details
Nursulu Kapalova¹
E-mail: nkapalova@mail.ru
ORCID ID: http://orcid.org/0000-0001-9743-9981
Ardabek Khompis³
E-mail: ardbek@mail.ru
Muslum Arici³
E-mail: muslumarici@gmail.com
ORCID ID: http://orcid.org/0000-0002-3397-2215
Kunbolat Algayz²
E-mail: kunbolat@mail.ru
¹ Institute of Information and Computational Technologies of the RK MES CS, Kazakhstan.
² Al-Farabi Kazakh National University, Almaty, Kazakhstan.
³ Mechanical Engineering Department, Kaceli University, Izmir, Turkey.

Citation information
Cite this article as: A block encryption algorithm based on exponentiation transform, Nursulu Kapalova, Ardabek Khompis, Muslum Arici & Kunbolat Algayz, Cogent Engineering (2020), 7: 1788292.

References
Amerbayev, V. M., Biyashev, R. G., & Nyssanbayeva, S. E. (2005). Use of nonpositional notations in cryptographic protection. Izv National Academy of Sciences Resp Kazakhstan, Series Physical Materials, (3), 84–89.
Babenko, L. K., & Ishchukova, E. A. (2006). Modern block encryption algorithms and methods of their analysis. Helios, ARV.

Biyashev, R., Nyssanbayeva, S., & Kapalova, N. (2013). The key exchange algorithm on basis of modular arithmetic. Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013) (pp. 16–21), Hong Kong-Lancaster, USA: DEStech Publications.

Biyashev, R. G. (1985). Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs [Doctoral Dissertation in Technical Sciences]. (in Russian)

Biyashev, R. G., & Nyssanbayeva, S. E. (2012). Algorithm for creation a digital signature with error detection and correction. Cybernetics and Systems Analysis, 48 (4), 489–497. https://doi.org/10.1007/s10559-012-9428-5

Chengqing, L., Zhang, Y., & Xie, E. Y. (2019). When an attacker meets a cipher-image in 2018: A year in review. Journal of Information Security and Applications, 48, 102361. https://doi.org/http://dx.doi.org/10.1016/jjis.2019.102361

Chigipa, A. A. (2007). Application of extended Galois fields to increase information secrecy of data transfer [Text]. A.A. Chigipa, I.A. Kalmykov, A.B. Khaivatov, Sagdeev A.K. Advances in Modern Science, (5), 103–105. http://ecorf.roseu/article/3633

Chigipa, A. A. (2009). Cryptographic data protection in information technologies based on nonpositional polynomial notations [Text]/A.A. Chigipa, I.A. Kalmykov, A.V. Barilskaya, O.A. Kikhtenko. SFU News, Technical science (pp. 210–220).

Chigipa, A. A. (2009, November 1520). Implementation of the inverse nonlinear encryption procedure using the index representation for the Galois field. In A. A. Chigipa, I. A. Kalmykov, A. V. Barilskaya, O. A. Kikhtenko, & V. R. Gakhov (Eds.), Proceedings of the electronic correspondence conference of the Russian Academy of Natural Sciences "Applied research and development in priority areas of science and technology.

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

Kapalova, N., & Dyusenbayev, D. (2016). Security analysis of an encryption scheme based on nonpositional polynomial notations. Open Engineering, 6(1), 250–258. https://doi.org/10.1515/eng-2016-0034

Kapalova, N., & Haumen, A. (2018). The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. Open Engineering, 8(1), 140–146. https://doi.org/10.1515/eng-2018-0013

Knuth, D. E. (2004). The art of computer programming. Transl. from English, 3rd ed., vol. 2. Seminumerical Algorithms. Publishing house Williams.

Li, C., Lin, D., & Lu, J. (2017). Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE Multimedia, 25(4), 64–71. https://doi.org/10.1109/MMUL.2017.3051512

Li, C., Lin, D., Lu, J., & Hao, F. (2018). Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimedia, 25(4), 46–56. https://doi.org/10.1109/MMUL.2018.2873472

Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., & Mao, S. (2013). Image block encryption algorithm based on chaotic maps. JET Signal Processing, 12(1), 22–30. https://doi.org/10.1049/jet-spr.2016.0584

Moldovan, A. A. (2002). Cryptography: Fast ciphers, SPb. BHV-Petersburg. (in Russian).

Nyssanbayeva, B. S., Kapalova, N., & Haumen, A. (2016). Modified symmetric block encryption-decryption algorithm based on modular arithmetic. Proceedings
of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016) (pp. 263–265).

Preneel, B. (1993, January). Analysis and design of cryptographic hash functions [Ph.D. dissertation]. Katholieke Universiteit Leuven.

Ullah, A., Jamal, S. S., & Shah, T. (2018). A novel scheme for image encryption using substitution box and chaotic system. Nonlinear Dynamics, 91(1), 359–370. https://doi.org/10.1007/s11071-017-3874-6

Xiong, Y., He, A., & Quan, C. (2018a). Security analysis of a double-image encryption technique based on an asymmetric algorithm. Journal of the Optical Society of America. A, Optics and Image Science, 35(2), 320–326. https://doi.org/10.1364/JOSAA.35.000320

Xiong, Y., He, A., & Quan, C. (2018b). Cryptanalysis of an optical cryptosystem based on phase-truncated Fourier transform and nonlinear operations. Optics Communications, 428, 120–130. https://doi.org/10.1016/j.optcom.2018.07.058.R