МРНТИ 81.93.29
УДК 004.421

https://doi.org/10.51889/2021-3.1728-7901.13

THE ALGORITHM OF BLOCK ENCRYPTION "AL03" AND THE RESULTS OF ITS ANALYSIS

Kapalova N. [1], *Algazy K.* [1,2]*, *Sakan K.* [1, 2], *Dyussenbayev D.* [1]

[1]*Institute of Information and Computational Technologies, Almaty, Kazakhstan*
[2]*Al-Farabi Kazakh National University, Almaty, Kazakhstan*
**email: kunbolat@mail.ru*

Abstract

This paper provides a brief description of the developed block cipher algorithm "AL03" and the results of checking the avalanche effect. This algorithm has the structure of a substitution-permutation network. The check consisted of two stages. At the first stage, the avalanche effect was tested separately for each transformation used in the algorithm. At the second stage, each round of encryption was analyzed. To characterize the degree of the avalanche effect in a transformation, the avalanche parameter is determined and used - the numerical value of the deviation of the probability of changing a bit in the output sequence when a bit in the input sequence changes from the required probability value equal to 0.5. The article presents the results after the 1st, 2nd, 3rd, and 24th rounds in the form of a table. Based on the round results obtained, comparative tests were carried out, as a result of which a positive conclusion was given on further research of this encryption algorithm.

Keywords: encryption algorithm, substitution S-boxes, avalanche effect, cryptographic conversions, encryption key, encryption round.

Аңдатпа

Н. Капалова[1], *К. Алгазы*[1,2]*, *Қ. Сақан*[1,2], *Д. Дюсенбаев*[1]
[1]*Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан*
[2]*әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан*

«AL03» БЛОКТЫ ШИФРЛАУ АЛГОРИТМІ ЖӘНЕ ОНЫ ТАЛДАУ НӘТИЖЕЛЕРІ

Бұл жұмыста құрылымы ауыстыру-ауыстыру желісінің нұсқасы бойынша жасалған «AL03» блоктық шифрлау алгоритмінің қысқаша сипаттамасы мен оның лавиндік әсерін тексерудің нәтижелері келтірілген. Мақалада зерттеу екі кезеңнен тұрады. Бірінші кезеңде алгоритмде қолданылатын әр түрлендіру және ол үшін талдау жеке жүргізілді. Екінші кезеңде талдау шифрлаудың бүтіндей әрбір раунды бойынша жүргізілді. Түрлендіру жүру барысында оның лавиндік әсерінің дәрежесін сипаттау үшін лавиндік параметрі –0,5-ке тең қажетті ықтималдық мәнінен кіріс тізбегіндегі бір ғана бит өзгерген кезде шығу тізбегіндегі барлық өзгеру ықтималдығының ауытқуының сандық мәні – анықталды және зерделенді. Мақалада кесте түрінде 1-ші, 2-ші, 3-ші және 24-ші раундтан кейінгі нәтижелер келтірілген. Алынған раундтық нәтижелер бойынша салыстырмалы тесттер жүргізілді, олардың нәтижелері бойынша осы шифрлау алгоритмін одан әрі зерттеулерді жалғастыру бойынша оң қорытынды берілді.

Түйін сөздер: шифрлау алгоритмдері, S-блок ауыстыру кестелері, лавиндік әсер, криптографиялық түрлендірулер, шифрлау кілті, шифрлау раунды.

Аннотация

Н. Капалова[1], *К. Алгазы*[1,2]*, *К. Сакан*[1,2], *Д. Дюсенбаев*[1]
[1]*Институт информационных и вычислительных технологий, г. Алматы, Казахстан*
[2]*Казахский национальный университет им. аль-Фараби, г. Алматы, Казахстан*

АЛГОРИТМ БЛОЧНОГО ШИФРОВАНИЯ «AL03» И РЕЗУЛЬТАТЫ ЕГО АНАЛИЗА

В данной работе приводятся краткое описание разработанного алгоритма блочного шифрования «AL03» и результаты проверки лавинного эффекта, данный алгоритм имеет структуру подстановочно-перестановочной сети. Исследование состоит из двух этапов. На первом этапе анализ проводился отдельно для каждого преобразования, применяемого в алгоритме. На втором этапе проводился по каждом раундам шифрования. Для характеристики степени лавинного эффекта в преобразовании определен и использован лавинный параметр – численное значение отклонения вероятности изменения бита в выходной последовательности при изменении бита во входной последовательности от требуемого значения вероятности, равной 0,5. В статье представлены результаты после 1-го, 2-го, 3-го и 24-го раунда в виде таблицы. По полученным раундовым результатам проводились сравнительные тесты, по итогам которых, дано положительное заключение по дальнейшему исследованию данного алгоритма шифрования.

Ключевые слова: алгоритм шифрования, таблицы S-блок замены, лавинный эффект, криптографическое преобразование, ключ шифрования, раунд шифрования.

Introduction

Cryptography is divided into theoretical and applied science. To study theoretical issues of cryptography, familiarity with various mathematical disciplines (e.g., probability theory and statistics, algebra, number theory, etc.), the theory of communication and coding is required. Applied cryptography deals with the application of theoretical cryptographic results in practice for solving specific problems.

Encryption algorithms fall into two categories: symmetric and asymmetric algorithms. The fundamental difference between them is that symmetric encryption algorithms use one key, while asymmetric ciphers use two different, but related keys. Symmetric encryption algorithms are faster and require less processing power. Due to its high encryption speed, symmetric algorithms are widely used to protect the information in many modern computer systems. Their main drawback is the key distribution problem, which is successfully solved for key pairs in asymmetric ciphers.

In turn, symmetric algorithms are divided into two types: block and stream ciphers. Block algorithms accept plain text in blocks of several characters, and stream algorithms sequentially convert the plain text character by character or bit by bit. In block ciphers, the source text is divided into blocks of fixed length, and all transformations are performed separately on each block [1-3]. Block ciphers are widely used in practice due to the long-term use of one short key without decreasing the cryptographic strength and high encryption speed, and also have other advantages.

During development, general requirements are imposed on the specified type of ciphers, such as [4-6]:

- Ensuring the required level of cryptographic strength;
- Simplicity, availability, and cost, as well as providing high performance and flexibility in various ways of implementation.

To ensure a high level of information security and data protection, in addition to the above requirements, the algorithms being developed are subject to basic requirements, which are given in [5, 6].

Thus, taking into account the general and basic requirements in the design of block ciphers, we proposed the new symmetric block cipher algorithm AL03, which is one of the modifications of the symmetric block cipher algorithm AL01 [7, 8].

Research results

Brief description of the encryption algorithm

The encryption algorithm AL03, developed by workers of the Institute's Information Security Laboratory, uses blocks and keys with a length of 128 bits. The structure of the cipher is a variant of a substitution-permutation network (SP-network). Encryption is carried out in 24 rounds. The algorithm includes transformations such as key addition using bitwise addition (XOR), substitution boxes (S-boxes), and bitwise shifts.

The encryption process in one round is performed in 5 stages and ends with the addition of the round keys modulo 2 to the results obtained.

At **Stage 1**, the input block of 16 bytes (128 bits) is divided into 4 subblocks of 4 bytes (32 bits) each: $a_0^0, a_1^0, a_2^0, a_3^0, a_0^1, a_1^1, a_2^1, a_3^1, a_0^2, a_1^2, a_2^2, a_3^2, a_0^3, a_1^3, a_2^3, a_3^3$, where the superscript represents the subblock number and the subscript is the byte number in the subblock. The internal transformation for subblocks is performed as follows: 1st and 2nd bytes, 2nd and 3rd bytes, 3rd and 4th bytes are summed modulo 2 and form new 1st, 2nd, and 3rd bytes, respectively. Further, the new 1st byte after the non-linear transformation of the S-box is added modulo 2 to the 4th byte to obtain a new 4th byte.

This transformation is performed for the other three subblocks as well. That is,

$$b_i^j = a_i^j \oplus a_{i+1}^j,\, b_3^j = S_1(b_1^j) \oplus a_3^j, \quad i = 0, 1, 2,\ j = 0, 1, 2, 3.$$

At **Stage 2**, all the results obtained in Stage 1 go through the substitution S-box. The S-box is shown in Table 1.

$$\mathrm{c}_i^j = S_1(b_i^j), \quad i = 0, 1, 2, 3;\ j = 0, 1, 2, 3.$$

Stage 3. In each subblock, a concatenation operation is performed over its 4 bytes at the bit level, followed by a rotate left by a predetermined number of steps L^j (L^j=1, 3, 5, 9) for each subblock, respectively:

$$\mathrm{c}_0^j \parallel \mathrm{c}_1^j \parallel \mathrm{c}_2^j \parallel \mathrm{c}_3^j = (\mathrm{c}_0^j \parallel \mathrm{c}_1^j \parallel \mathrm{c}_2^j \parallel \mathrm{c}_3^j) \lll L^j, \qquad j = 0, 1, 2, 3.$$

At **Stage 4**, the transformation is carried out similarly to Stage 1, but regarding neighboring subblocks. The corresponding values of the 1st and 2nd subblocks, the 2nd and 3rd subblocks, and the 3rd and 4th subblocks are summed modulo 2 and give the new values of the 1st, 2nd, and 3rd subblocks. The new values of the 4th subblock are the sum modulo 2 of the obtained values of the 1st subblock after passing another substitution S-box with the values of the 4th subblock:

$$d_i^j = c_i^j \oplus c_i^{j+1},\ d_i^3 = S_2\left(d_i^0\right) \oplus c_i^3, \quad i = 0,1,2,3;\ j = 0,1,2.$$

At **Stage 5**, all the values of the four sub-blocks obtained in Stage 4 pass through the substitution S-box, according to Table 2.

$$e_i^j = S_2\left(d_i^j\right), \quad i = 0,1,2,3;\ j = 0,1,2,3.$$

One round of encryption is completed by summing modulo 2 the values of e_i^j with the round key.

The above-described six-step encryption process is repeated *k* times depending on the number of rounds.

Analysis results

Multi-round transformations provide the diffusion and confusion properties that strong ciphers should have. Diffusion is the spread of the influence of one plaintext character over a significant number of ciphertext characters. The presence of this property in a cipher allows hiding the statistical dependence between the elements of the original text and does not allow recovering the key in parts. The essence of the confusion is to make the statistical relationship between the ciphertext and the key as complex as possible to resist attempts to determine the key. The cryptanalyst, based on a statistical analysis of the mixed text, should not obtain information about the key [9].

The avalanche effect in the basic transformation is manifested in a significant - "avalanche" - change of bits in the output sequence of the transformation with a small change in the bits in the input sequence. The high degree of the avalanche effect in the encryption algorithm significantly complicates attacks when using the method of differential cryptanalysis because of the impossibility of identifying the underlying differential characteristics of the transformation. If a cryptographic algorithm does not have a sufficient avalanche effect, then an adversary can make certain assumptions about the original test based on the ciphertext. Thus, the achievement of the avalanche effect is an important goal in the development of a cryptographic algorithm. In multi-round block ciphers, the avalanche effect is usually achieved due to the fact that in each round, a change in one input bit leads to changes in several output bits. To check the presence of a good avalanche effect in a particular algorithm, several criteria can be used [10-12].

We will use the notation given in the description of the algorithm. Let $a_0^0, a_1^0, a_2^0, a_3^0, a_0^1, a_1^1, a_2^1, a_3^1, a_0^2, a_1^2, a_2^2, a_3^2, a_0^3, a_1^3, a_2^3, a_3^3$ be the elements of the block for encryption.

In order to find out how each transformation used in the algorithm affects the avalanche effect, two plaintexts are considered that are minimally different from each other. Next, the differences in the values obtained during encryption at each step are investigated. For convenience, key values, encryption results, and their differences are considered in hexadecimal form.

As an example, let's take the following two plaintexts, differing only by one bit in the last byte a_3^3:

1) AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA;
2) AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AB.

Let the master key K_0 be common for both plaintexts: 46 84 1A 41 6E D2 D2 81 79 AA E5 E4 1C 70 72 90. To begin with, according to the algorithm for generating round keys, we derive three round keys required for the first three rounds:

K_1=2A 75 2B C3 8F 13 6F E2 5C 8C 0A 11 C2 81 50 6A

K_2=6F A9 5B AC 8F 55 55 2D 27 BC 0F CA 77 1A 7D 47

K_3=0A F2 61 26 DB A2 C2 34 77 C4 3F 5D 96 78 BD 78

Obviously, modulo two addition (XOR operation) of plaintext with a key does not lead to an avalanche effect, since changes do not affect other bytes.

According to the encryption scheme, as a result of the Step-1 transformation, the change is propagated to the last two bytes (a_2^3, a_3^3):

32 3F 9F 17 38 62 3B A2 EF 92 E9 04 D0 10 24 68

32 3F 9F 17 38 62 3B A2 EF 92 E9 04 D0 10 6C ED

After the Step-2 transformation, the last three bytes will change a_1^3, a_2^3, a_3^3 :

64 7F 3E 2E C3 11 DD 11 F2 5D 20 9D 80 81 23 46

64 7F 3E 2E C3 11 DD 11 F2 5D 20 9D 80 83 67 6E

In the next Step-3 transformation, we observe changes in six bytes a_1^3, a_2^3, a_3^3, a_1^2, a_2^2, a_3^2:

AE D1 C8 05 D5 56 04 0C CA 90 6B 67 30 C2 E9 E3

AE D1 C8 05 D5 56 04 0C CA D9 42 F8 30 51 18 C7

As mentioned above, modulo 2 addition of the round key with the result of encryption will not propagate the changes to bytes located elsewhere. Consider propagating changes to byte locations after the second round. As shown in Table 1, after round encryption, changes are observed in the following bytes: $a_0^1, a_1^1, a_2^1, a_3^1, a_0^2, a_1^2, a_2^2, a_3^2, a_0^3, a_1^3, a_2^3, a_3^3$. Likewise, we can compare the values after three rounds (Table 2).

Table 1. Propagation of changes after the second round

Steps	*Code of values after the second round*
Step-1	*A5 89 09 81 F5 21 AF A4 AA 30 E8 03 39 CC B7 23* *A5 89 09 81 F5 21 AF A4 DD 65 04 A1 73 AE 5C 45*
Step-2	*4B 12 13 03 A9 0D 7D 27 46 1D 00 75 CE 65 B9 19* *4B 12 13 03 A9 0D 7D 27 AC A0 94 3B 9D 72 E2 2B*
Step-3	*B5 A1 D1 53 41 3B 97 51 71 3C FD 4B 06 8F 62 D6* *B5 A1 D1 53 63 40 5D 24 D5 96 F2 3B 54 29 23 3C*
Round key addition	*DA 08 8A FF CE 6E C2 7C 56 80 F2 81 71 95 1F 91* *DA 08 8A FF EC 15 08 09 F2 2A FD F1 23 33 5E 7B*

Table 2. Propagation of changes after the third round

Steps	*Code of values after the third round*
Step-1	*47 01 1D 78 11 65 E9 52 88 35 13 B0 4D A3 09 AC* *30 DE CE 06 57 74 9A 2C 1B 04 F8 8B 18 C6 70 20*
Step-2	*8E 02 3A F0 8B 2F 4A 90 06 A2 76 11 6D 18 4D 62* *61 BD 9C 0C BB A4 D1 62 60 9F 11 63 C6 33 81 00*
Step-3	*63 E0 FB D3 F1 F1 4E AD C7 48 F0 4D E6 E8 68 13* *12 98 BB D1 67 F0 CE B0 3A 39 77 A5 3E CD E5 6A*
Round key addition	*69 12 9A F5 2A 53 8C 99 B0 8C CF 10 70 90 D5 6B* *18 6A DA F7 BC 52 0C 84 4D FD 48 F8 A8 B5 58 12*

Thus, when even only one bit in the plaintext changes, the ciphertext undergoes a complete change after Step-1 in the third round. Consequently, the requirement of the avalanche effect on the ciphertext is fulfilled after passing through three rounds of the encryption algorithm. In particular, this example showed the impact of each transformation used in the algorithm.

In the general case, it is necessary to check the avalanche effect for each position of the plaintext. To do this, we select a random plaintext with a length of 128 bits and get 128 plaintexts from this text, which differ only in one position. Further, to study the propagation of the avalanche effect, we encrypt these 128 plaintexts. Now, separately, we compare each of the obtained 128 ciphertexts with the original ciphertext obtained from the selected plaintext, i.e. calculate the probabilities $k_{AVAL}(i, X)$ between the obtained ciphertext and the original ciphertext. $k_{AVAL}(i, X)$ is the probability of changing half of the bits in the output value when changing the ith bit in the input value compared to the output value at the original input value; X is a fixed input value of the transformation, for which the avalanche index is calculated [11].

The values of the avalanche index ε_A in the "input value - output value" pair are determined by the formula:

$$\varepsilon_A(i, X) = |2k_{AVAL}(i, X) - 1|$$

It can be seen from the formula that the extremality ε can take values from 0 to 1 inclusive. The closer the value of ε is to zero, the "better" the algorithm is. Conversely, the closer the value of ε is to 1, the "worse" the algorithm is. Tables 3-6 show the specific ε values relative to the first, second, third, and twenty-fourth rounds with an indication of their average value of 0.561, 0.142, 0.061, and 0.062, respectively. Based on these values, it can be seen that the avalanche effect of the algorithm reaches a good indicator after the third round. Comparative data of the avalanche effect of the encryption algorithm for the first three rounds are shown in Figure 1, where the abscissa axis contains *i* – ordinal numbers of the changed bits in the input text, and the ordinate axis contains the values of $\varepsilon_A(i, X)$.

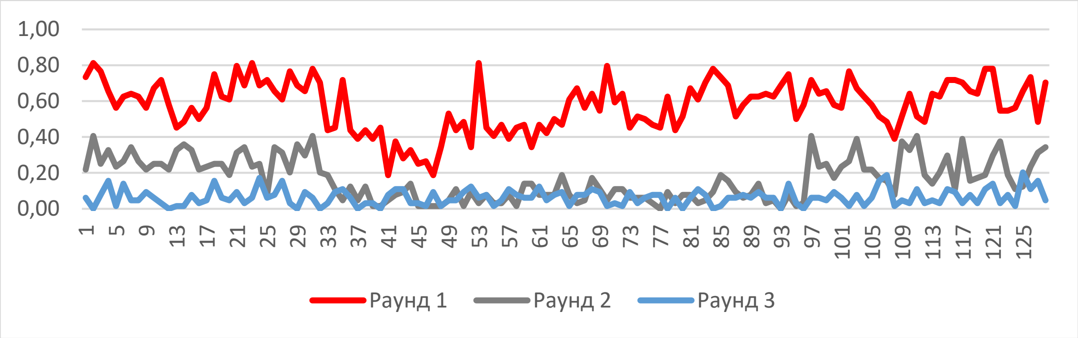

Figure 1. Comparative data of the avalanche effect from 1 to 3 rounds

Table 3. Analysis of the avalanche effect of the AL03 algorithm after the first round

i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i
1	0,73	17	0,56	33	0,44	49	0,53	65	0,61	81	0,67	97	0,72	113	0,64
2	0,81	18	0,75	34	0,45	50	0,44	66	0,67	82	0,61	98	0,64	114	0,63
3	0,77	19	0,63	35	0,72	51	0,48	67	0,56	83	0,70	99	0,66	115	0,72
4	0,66	20	0,61	36	0,44	52	0,34	68	0,64	84	0,78	100	0,58	116	0,72
5	0,56	21	0,80	37	0,39	53	0,81	69	0,55	85	0,73	101	0,56	117	0,70
6	0,63	22	0,69	38	0,44	54	0,45	70	0,80	86	0,69	102	0,77	118	0,66
7	0,64	23	0,81	39	0,39	55	0,41	71	0,59	87	0,52	103	0,67	119	0,64
8	0,63	24	0,69	40	0,45	56	0,47	72	0,64	88	0,58	104	0,63	120	0,78
9	0,56	25	0,72	41	0,19	57	0,39	73	0,45	89	0,63	105	0,58	121	0,78
10	0,67	26	0,66	42	0,38	58	0,45	74	0,52	90	0,63	106	0,52	122	0,55
11	0,72	27	0,61	43	0,28	59	0,47	75	0,50	91	0,64	107	0,48	123	0,55
12	0,58	28	0,77	44	0,33	60	0,34	76	0,47	92	0,63	108	0,39	124	0,56
13	0,45	29	0,69	45	0,25	61	0,47	77	0,45	93	0,69	109	0,52	125	0,66
14	0,48	30	0,66	46	0,27	62	0,42	78	0,63	94	0,75	110	0,64	126	0,73
15	0,56	31	0,78	47	0,19	63	0,50	79	0,44	95	0,50	111	0,52	127	0,48
16	0,50	32	0,70	48	0,34	64	0,47	80	0,52	96	0,58	112	0,48	128	0,70

Table 4. Analysis of the avalanche effect of the AL03 algorithm after the second round

i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i	i	ε_i
1	0,22	17	0,23	33	0,19	49	0,05	65	0,08	81	0,08	97	0,41	113	0,14
2	0,41	18	0,25	34	0,11	50	0,11	66	0,03	82	0,03	98	0,23	114	0,20
3	0,25	19	0,25	35	0,05	51	0,02	67	0,05	83	0,05	99	0,25	115	0,30
4	0,33	20	0,19	36	0,13	52	0,09	68	0,17	84	0,09	100	0,17	116	0,11
5	0,23	21	0,31	37	0,05	53	0,03	69	0,11	85	0,19	101	0,23	117	0,39
6	0,27	22	0,34	38	0,13	54	0,08	70	0,05	86	0,16	102	0,27	118	0,16
7	0,34	23	0,23	39	0,02	55	0,03	71	0,11	87	0,09	103	0,39	119	0,17
8	0,27	24	0,25	40	0,02	56	0,03	72	0,11	88	0,06	104	0,22	120	0,19

9	*0,22*	*25*	*0,08*	*41*	*0,05*	*57*	*0,08*	*73*	*0,06*	*89*	*0,08*	*105*	*0,22*	*121*	*0,30*
10	*0,25*	*26*	*0,34*	*42*	*0,08*	*58*	*0,02*	*74*	*0,06*	*90*	*0,14*	*106*	*0,17*	*122*	*0,38*
11	*0,25*	*27*	*0,31*	*43*	*0,09*	*59*	*0,14*	*75*	*0,06*	*91*	*0,03*	*107*	*0,16*	*123*	*0,19*
12	*0,22*	*28*	*0,20*	*44*	*0,14*	*60*	*0,14*	*76*	*0,03*	*92*	*0,05*	*108*	*0,08*	*124*	*0,11*
13	*0,33*	*29*	*0,36*	*45*	*0,02*	*61*	*0,08*	*77*	*0,00*	*93*	*0,00*	*109*	*0,38*	*125*	*0,13*
14	*0,36*	*30*	*0,30*	*46*	*0,02*	*62*	*0,08*	*78*	*0,09*	*94*	*0,08*	*110*	*0,33*	*126*	*0,23*
15	*0,33*	*31*	*0,41*	*47*	*0,02*	*63*	*0,08*	*79*	*0,03*	*95*	*0,02*	*111*	*0,41*	*127*	*0,31*
16	*0,22*	*32*	*0,20*	*48*	*0,02*	*64*	*0,19*	*80*	*0,08*	*96*	*0,03*	*112*	*0,19*	*128*	*0,34*

Table 5. Analysis of the avalanche effect of the AL03 algorithm after the third round

i	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i
1	*0,06*	*17*	*0,05*	*33*	*0,03*	*49*	*0,05*	*65*	*0,02*	*81*	*0,06*	*97*	*0,06*	*113*	*0,05*
2	*0,00*	*18*	*0,16*	*34*	*0,09*	*50*	*0,05*	*66*	*0,08*	*82*	*0,11*	*98*	*0,06*	*114*	*0,03*
3	*0,08*	*19*	*0,06*	*35*	*0,11*	*51*	*0,09*	*67*	*0,08*	*83*	*0,08*	*99*	*0,05*	*115*	*0,11*
4	*0,16*	*20*	*0,05*	*36*	*0,06*	*52*	*0,13*	*68*	*0,11*	*84*	*0,00*	*100*	*0,09*	*116*	*0,09*
5	*0,02*	*21*	*0,09*	*37*	*0,00*	*53*	*0,06*	*69*	*0,09*	*85*	*0,02*	*101*	*0,06*	*117*	*0,03*
6	*0,14*	*22*	*0,03*	*38*	*0,03*	*54*	*0,08*	*70*	*0,02*	*86*	*0,06*	*102*	*0,02*	*118*	*0,08*
7	*0,05*	*23*	*0,06*	*39*	*0,03*	*55*	*0,02*	*71*	*0,03*	*87*	*0,06*	*103*	*0,08*	*119*	*0,03*
8	*0,05*	*24*	*0,17*	*40*	*0,00*	*56*	*0,05*	*72*	*0,02*	*88*	*0,08*	*104*	*0,02*	*120*	*0,11*
9	*0,09*	*25*	*0,06*	*41*	*0,08*	*57*	*0,11*	*73*	*0,09*	*89*	*0,06*	*105*	*0,06*	*121*	*0,14*
10	*0,06*	*26*	*0,08*	*42*	*0,11*	*58*	*0,08*	*74*	*0,03*	*90*	*0,09*	*106*	*0,16*	*122*	*0,03*
11	*0,03*	*27*	*0,16*	*43*	*0,11*	*59*	*0,06*	*75*	*0,06*	*91*	*0,06*	*107*	*0,19*	*123*	*0,08*
12	*0,00*	*28*	*0,03*	*44*	*0,03*	*60*	*0,06*	*76*	*0,08*	*92*	*0,06*	*108*	*0,02*	*124*	*0,02*
13	*0,02*	*29*	*0,00*	*45*	*0,03*	*61*	*0,13*	*77*	*0,08*	*93*	*0,00*	*109*	*0,05*	*125*	*0,20*
14	*0,02*	*30*	*0,09*	*46*	*0,02*	*62*	*0,05*	*78*	*0,00*	*94*	*0,14*	*110*	*0,03*	*126*	*0,11*
15	*0,08*	*31*	*0,06*	*47*	*0,09*	*63*	*0,08*	*79*	*0,06*	*95*	*0,03*	*111*	*0,11*	*127*	*0,16*
16	*0,03*	*32*	*0,00*	*48*	*0,02*	*64*	*0,09*	*80*	*0,00*	*96*	*0,00*	*112*	*0,03*	*128*	*0,05*

Table 6. Analysis of the avalanche effect of the AL03 algorithm after the 24th round

i	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i	*i*	ε_i
1	*0,11*	*17*	*0,05*	*33*	*0,02*	*49*	*0,05*	*65*	*0,02*	*81*	*0,16*	*97*	*0,09*	*113*	*0,06*
2	*0,13*	*18*	*0,14*	*34*	*0,06*	*50*	*0,03*	*66*	*0,05*	*82*	*0,09*	*98*	*0,03*	*114*	*0,09*
3	*0,02*	*19*	*0,17*	*35*	*0,03*	*51*	*0,08*	*67*	*0,03*	*83*	*0,02*	*99*	*0,16*	*115*	*0,09*
4	*0,02*	*20*	*0,11*	*36*	*0,17*	*52*	*0,03*	*68*	*0,03*	*84*	*0,13*	*100*	*0,08*	*116*	*0,03*
5	*0,14*	*21*	*0,05*	*37*	*0,09*	*53*	*0,06*	*69*	*0,02*	*85*	*0,05*	*101*	*0,03*	*117*	*0,05*
6	*0,03*	*22*	*0,08*	*38*	*0,03*	*54*	*0,03*	*70*	*0,06*	*86*	*0,08*	*102*	*0,20*	*118*	*0,03*
7	*0,08*	*23*	*0,02*	*39*	*0,13*	*55*	*0,09*	*71*	*0,09*	*87*	*0,05*	*103*	*0,13*	*119*	*0,20*
8	*0,05*	*24*	*0,03*	*40*	*0,02*	*56*	*0,05*	*72*	*0,03*	*88*	*0,08*	*104*	*0,09*	*120*	*0,02*
9	*0,02*	*25*	*0,06*	*41*	*0,00*	*57*	*0,06*	*73*	*0,02*	*89*	*0,02*	*105*	*0,13*	*121*	*0,11*
10	*0,03*	*26*	*0,14*	*42*	*0,06*	*58*	*0,06*	*74*	*0,13*	*90*	*0,05*	*106*	*0,13*	*122*	*0,03*
11	*0,02*	*27*	*0,02*	*43*	*0,03*	*59*	*0,03*	*75*	*0,03*	*91*	*0,13*	*107*	*0,11*	*123*	*0,14*
12	*0,00*	*28*	*0,00*	*44*	*0,09*	*60*	*0,05*	*76*	*0,06*	*92*	*0,08*	*108*	*0,00*	*124*	*0,11*
13	*0,06*	*29*	*0,03*	*45*	*0,09*	*61*	*0,03*	*77*	*0,14*	*93*	*0,02*	*109*	*0,08*	*125*	*0,11*
14	*0,05*	*30*	*0,05*	*46*	*0,11*	*62*	*0,16*	*78*	*0,08*	*94*	*0,08*	*110*	*0,08*	*126*	*0,00*
15	*0,02*	*31*	*0,08*	*47*	*0,06*	*63*	*0,08*	*79*	*0,19*	*95*	*0,09*	*111*	*0,03*	*127*	*0,08*
16	*0,02*	*32*	*0,08*	*48*	*0,02*	*64*	*0,11*	*80*	*0,00*	*96*	*0,00*	*112*	*0,11*	*128*	*0,00*

Conclusion

The structure of the algorithm uses the *XOR* operation and a substitution S-box. In one round of encryption, only 56 elementary operations are performed, therefore, for the entire algorithm with the number of rounds of 24, 1344 operations are performed. By the number of elementary operations, when compared with other well-known encryption algorithms, this is considered as an acceptable level of performance for a computer.

For the numerical study of the developed algorithm, software was compiled in the Delphi 7 programming language. With the help of this software, studies were carried out to assess the propagation of the avalanche effect. The paper presents in more detail the results of verification to satisfy the avalanche effect criterion. It was found that good results in diffusion and confusion are observed after the third round of encryption. However, to achieve the maximum degree of nonlinearity and taking into account the optimal distribution of the balance between security and performance of the algorithm, the number of rounds is set to 24.

As is well known, one of the main requirements for an algorithm under development is its cryptographic strength. At the moment, there are preliminary positive research results in this area. The method for obtaining the used S-box in the considered algorithm and the results of other more in-depth analyzes will be published in subsequent articles.

Acknowledgment

The research work was carried out within the framework of the grant funding project AP08856426 "Development and study of an encryption algorithm and the creation of a software-hardware complex for its implementation" of the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan.

References

1 Varfolomeyev A.A. Sovremennaya prikladnaya kriptografiya [Modern Applied Cryptography], Moscow: PFUR, 2008. – 188 p., [in Russian].

2 Keith Martin, Everyday Cryptography: Fundamental Principles and Applications. - Oxford University Press, 2012. – 560 p.

3 Jonathan Katz and Yehuda Lindell Introduction to Modern Cryptography: Third Edition Chapman & Hall/CRC Cryptography and Network Security Series, 2020. – 648 p.

4 Gorbenko I. D., Dolgov V., Oleynikov R. V., Ruzhentsev V. I., Mikhaylenko, M. S., Gorbenko, Y. I., "Razrabotka trebovaniy i printsip proektirovaniya perspektivnogo simmetrichnogo blochnogo algoritma shifrovaniya [Development of requirements and design principle perspective symmetrical block encryption algorithm]", Izvestiya YUFU. Tekhnicheskie nauki. no. 1. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (2007), (3.11.2020), [in Russian].

5 Apparatnoe shifrovanie dlya PK [Hardware encryption for PC]. Press center Company Active, 2013. URL: https://www.aktiv-company.ru/press-center/publication/2003-04-10.html (23.11.2020), [in Russian].

6 Znaenko N.S., Kapitanchuk V.V., Petrishchev I.O., Shubovich V.G., "Nekotorye kriterii ocenki kachestva algoritmov shifrovaniya [Some criteria for evaluating the quality of encryption algorithms]", NovaInfo.Ru. Tekhnicheskie nauki no. 59 (2017) URL: https://novainfo.ru/article/11211 (23.11.2020), [in Russian].

7 Report on the research work "Development of software and hardware for cryptographic protection of information during its transmission and storage in info communication systems and general-purpose networks" // Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan, Institute of Information and Computing Technologies, State Registration No. 0118RK01064, 2020.

8 Dyusenbaev D.S., Algazy K.T., Sakan K.S. Issledovaniye algoritmov shifrovanii "Al01" i "Qamal" na osnove algebraicheskogo kriptoanaliza [Research of encryption algorithms "Al01" and "Qamal" on the basis of algebraic cryptanalysis], Bulletin of KazNRTU, – 2020. - №5. - 620-629p. [in Russian].

9 Bruce Shnier Applied Cryptography: Protocols, Algorithms, and Source Code in C. – 1996. - John Wiley & Sons. – 784 p.

10 Rejane Forre, «The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition», Proceedings on Advances in cryptology, Springer-Verlag New York, Inc, 1990, – 450 p.

11 Sidorenko A. V., Mulyarchik K. S. Lavinnii effekt v algoritmah shifrovaniya na osnove dinamicheskogo haosa [in Russian: Avalanche effect in dynamic chaos-based encryption algorithms] https://elib.bsu.by/bitstream/123456789/52134/1/105-109.pdf [in Russian].

12 Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. Turk J Elec Engin. – 2001. – T. 9, № 2. – 137-145p.