Higher professional and postgraduate training of information security specialists

Nursulu Kapalova†‡, Saule Nyssanbayeva†, Andrey Varennikov†, Dilmukhanbet Dyusenbayev† & Kairat Sakan†‡

Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan†
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan‡

ABSTRACT: The article highlights the issues of training specialists in information security in the system of higher professional and postgraduate education in the Republic of Kazakhstan. Attention is drawn to the need for specialists in the field of information security, and their role in the development and independence of the country. The content of educational programmes of specialties in information security is considered. The authors also presented the developed AL02 block symmetric encryption algorithm, which is well suited for studying the methods of statistical analysis of the quality of ciphertexts. The algorithm scheme provides for five-round encryption of 128-bit blocks. The main transformation is the F transformation, which provides the maximum possible dependence of the bits of the output vector on the bits of the input, and is based on *modulo 2 addition* and a substitution S-box. During the analysis, the cryptographic properties of the developed encryption algorithm and the well-known AES algorithm were tested. The AL02 algorithm was tested for statistical security. For an experimental assessment that ciphertexts are not inferior to a random sequence in their properties, the well-known set of NIST statistical tests was used.

Keywords: Information security, personnel training, encryption algorithm

INTRODUCTION

The concept of information security (IS) of the Republic of Kazakhstan stipulates the need to develop Kazakhstan's own means of ensuring information security, as well as approaches, methods and algorithms for protecting information. In this context the issues of training personnel in information security in higher educational institutions of Kazakhstan, and the development of domestic information security tools require special attention [1]. Kazakhstan is a full member of the Bologna Process, which allows for the implementation of joint educational projects, academic mobility of students and teachers, the convertibility of domestic diplomas in the European region and the right of graduates to employment in any country. The modernisation of the national education system is taking into account the specifics of the political, economic social, and cultural state of the country. This should lead to an increase in the quality of training of specialists and their demand in the labour market without infringing on strategic national interests [2]. The training of specialists in information security should take into account the modern development of ICT and cover the most important areas of information security.

For comparison, one notes that in the US, teaching is concentrated mainly on the training and retraining of specialists in the technical aspects of information security. The training of information security specialists (both mainly technical and humanitarian) is carried out in a developed network of higher educational institutions (more than 150 universities). Also in the US, students have the opportunity to get an education in information security programmes with an MBA degree.

In France, the training of specialists in information security focuses on the study of technical issues related to cryptography, network security and information systems audits.

In Russia, 99 licensed civilian universities train IS specialists on the state order in seven technical specialties of the information security group of specialties (according to the All-Russian Classifier). In 2018, the undergraduate programme included 3,700 places in the specialty *information security* [3].

In the Republic of Kazakhstan in 2016, 60 state grants were allocated for training in the specialty *information security systems*. In 2017, the number increased to 160. By 2022, thanks to an annual increase, the number of grants reached 2,781. At the same time, there is a high demand for information security specialists in the domestic labour market.

The acceleration of the pace of technology development has led to a significant lag in higher education from the increasing market demands in both information technology and information security.

As part of the specialty *information security systems*, new educational programmes were adopted, one of which is *cryptographic information protection systems*. The educational programme of undergraduate and graduate programmes *cryptographic information protection systems* should include areas of cryptography and cryptanalysis.

It is very important to further develop the integration of education and science, carried out by Kazakh research institutes and universities in the framework of joint training in the field of information security.

One of the solutions are the joint educational programmes of Al-Farabi Kazakh National University and research institutes based on the Gylym Ordasy complex, which includes the Institute of Information and Computational Technologies (IICT). The main directions of scientific activity of IICT in the field of information security and information protection are the development and analysis of domestic encryption systems, encrypted data store (EDS) and cryptographic analysis of developed and known encryption systems. The main research results of IICT employees in these areas have already been published in several works [4-10].

On the basis of IICT, undergraduates and PhD students study the specialty *information security systems* for the training of scientific and pedagogical staff of research institutes. Educational programmes include areas of cryptography and cryptanalysis, as the institute's IS laboratory is engaged in the development and study of cryptographic algorithms. The obtained results are successfully applied in the process of teaching students.

In this article, the authors consider one of the developed block symmetric encryption algorithms, which is well suited for studying cryptanalysis methods.

METHODOLOGY

Cryptographic primitives traditionally used to create symmetric cryptosystems are substitutions, permutations, arithmetic and algebraic operations, and some other auxiliary operations. The main methods for evaluating the strength of cryptographic algorithms include the assessment of their statistical security. Statistical tests are used to experimentally evaluate whether a ciphertext is as good as a random sequence in its properties.

The following test suites are known: NIST, CRYPT-X, DIEHARD, TESTU01, and test sets by Knuth [11] and Doganaksoy [12]. They are used to study the statistical properties of cryptographic primitives and make it possible to obtain a preliminary estimate of cryptographic strength.

RESULTS OF THE DEVELOPMENT OF A NEW CIPHER ALGORITHM

The AL02 Encryption Algorithm

Workers of the Information Security Laboratory have developed the Al02 encryption algorithm, which is new in its architecture and meets modern requirements.

Algorithm parameters: the block length is 128 bits, the number of rounds is five, data size at the input and output of the S-box, which is used in the algorithm as a non-linear function, is eight bits. The main transformations used are *modulo 2 addition* and S-box substitution, as well as the F transformation based on these two transformations. The scheme of this algorithm is shown in Figure 1.

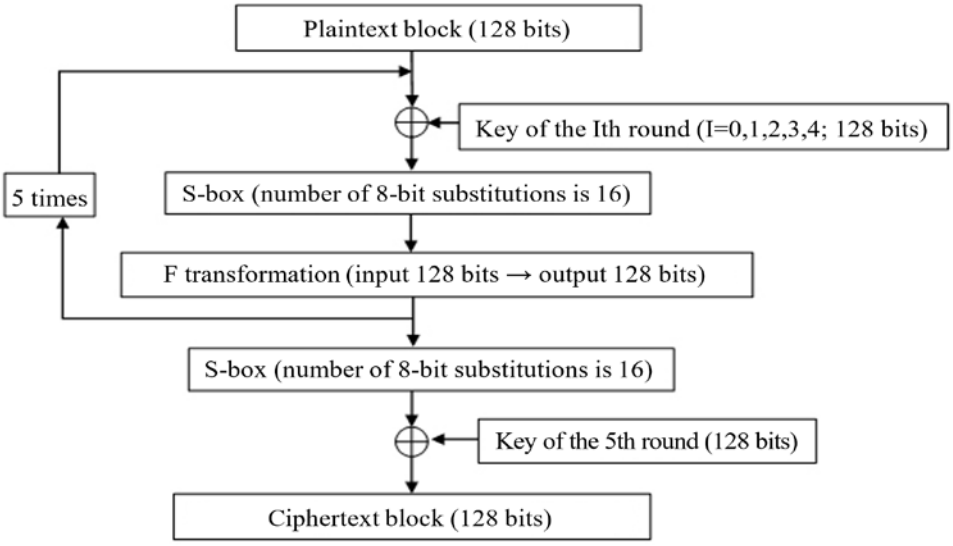

Figure 1: Scheme of the AL02 algorithm.

After the fifth round, the encryption result is passed through the S-box and bitwise addition with the key is performed.

Encryption

Each block is encrypted according to the following scheme:

$$CX\left(K_5, S\left(F\left(S(X(K_4, F(S(X(K_3, F(S(X(K_2, F(S(X(K_1, F(S(X(K_0, A) \dots)))\right)\right).$$

Here *A* is the plain text, *C* is the ciphertext, *X* is the XOR operation, *S* is the S-box transformation, *F* is a non-linear transformation and *I* is an intermediate value.

DecryptionText decryption is performed by the sequential processing of 16-byte blocks using inverse transformation.

To obtain a plaintext block, it is necessary to repeat the inverse transformation $F^{-1}(S^{-1}(X(K_5,C)))$ five times, and then perform the transformation $X(K_0,S^{-1}(I))$ using the compositional method.

Each block is decrypted as per the following scheme:

$$A = X\left(K_0, S^{-1}\left(F^{-1}\left(S^{-1}(X(K_1, \dots, F^{-1}(S^{-1}(X(K_5, C) \dots))\right)\right)\right),$$

where *A* is the plain text, *C* is the ciphertext, *X* is the XOR operation, S^{-1} is the inverse S-box, F^{-1} is the inverse non-linear transformation and *I* is an intermediate value.

The algorithm uses S-boxes given in Table 1 and Table 2.

Table 1: Substitution S-box of the AL02 encryption algorithm.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A5	04	A6	A7	F7	C6	A4	12	5F	C8	C7	D1	F6	D4	7E	7B
1	0B	EF	13	AD	94	5B	4C	8A	0C	FC	CE	1C	9B	76	19	F3
2	21	68	53	96	2D	D0	A1	89	3D	9C	DA	6D	51	AF	E1	E9
3	A2	E3	09	FE	C3	3F	AA	1E	BA	DD	9F	1D	28	54	8E	92
4	E7	D5	43	33	DE	81	3C	97	32	EC	1F	72	74	CD	B3	60
5	3A	95	39	FA	1A	0E	C1	05	DF	CC	A0	8D	87	58	83	D3
6	26	FD	86	7C	20	4B	08	36	45	DC	3B	79	22	BE	AB	14
7	2A	03	99	2C	6B	E5	F9	5C	B0	85	5D	B2	30	80	ED	DB
8	57	8F	9D	A9	D6	B8	EE	24	CB	84	B7	D8	69	A8	6F	50
9	BD	F1	01	38	F8	40	4E	BF	9E	0D	91	C9	7D	F4	47	07
A	B9	63	6E	0F	EB	70	D9	6A	7A	2B	A3	CF	44	65	F5	00
B	98	35	C2	41	27	1B	62	AC	67	23	88	10	B6	8C	4D	C0
C	64	3E	5A	E8	34	D7	9A	16	B4	29	D2	37	73	F2	6C	46
D	06	E6	CA	C4	EA	7F	18	E0	B5	31	FB	FF	71	17	AE	02
E	B1	15	25	78	BB	F0	61	93	11	4F	56	82	8B	42	59	48
F	2F	E2	66	4A	0A	90	2E	75	BC	C5	E4	55	52	77	49	5E

Table 2: Reverse S-box of the AL02 encryption algorithm.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	AF	92	DF	71	01	57	D0	9F	66	32	F4	10	18	99	55	AF
1	BB	E8	07	12	6F	E1	C7	DD	D6	1E	54	B5	1B	3B	37	BB
2	64	20	6C	B9	87	E2	60	B4	3C	C9	70	A9	73	24	F6	64
3	7C	D9	48	43	C4	B1	67	CB	93	52	50	6A	46	28	C1	7C
4	95	B3	ED	42	AC	68	CF	9E	EF	FE	F3	65	16	BE	96	95
5	8F	2C	FC	22	3D	FB	EA	80	5D	EE	C2	15	77	7A	FF	8F
6	4F	E6	B6	A1	C0	AD	F2	B8	21	8C	A7	74	CE	2B	A2	4F
7	A5	DC	4B	CC	4C	F7	1D	FD	E3	6B	A8	0F	63	9C	0E	A5
8	7D	45	EB	5E	89	79	62	5C	BA	27	17	EC	BD	5B	3E	7D
9	F5	9A	3F	E7	14	51	23	47	B0	72	C6	1C	29	82	98	F5
A	5A	26	30	AA	06	00	02	03	8D	83	36	6E	B7	13	DE	5A
B	78	E0	7B	4E	C8	D8	BC	8A	85	A0	38	E4	F8	90	6D	78
C	BF	56	B2	34	D3	F9	05	0A	09	9B	D2	88	59	4D	1A	BF
D	25	0B	CA	5F	0D	41	84	C5	8B	A6	2A	7F	69	39	44	25
E	D7	2E	F1	31	FA	75	D1	40	C3	2F	D4	A4	49	7E	86	D7
F	E5	91	CD	1F	9D	AE	0C	04	94	76	53	DA	19	61	33	E5

Round Key Algorithm

The 128-bit seed key is set randomly. Based on this key, round keys are formed for each iteration of this transformation. Figure 2 shows the scheme for generating round keys, where *G* is a non-linear transformation.

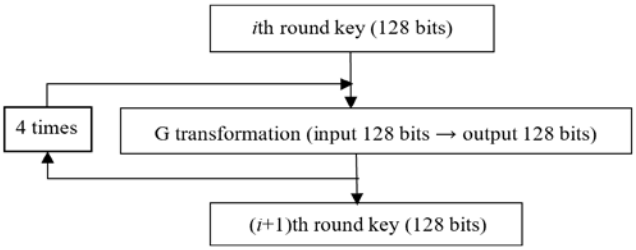

Figure 2: Scheme of the round key algorithm.

ANALYSIS OF CRYPTOGRAPHIC SECURITY BY STATISTICAL RESEARCH METHODS

Statistical Analysis

Now some key points of the testing methodology need to be highlighted. As mentioned above, different test suites are used for evaluation. For testing, two options for selecting open texts were considered: randomly selected files with different extensions and specially selected files with a different number of blocks. For encryption, the well-known AES encryption algorithm and the developed new algorithm AL02 were used.

First Option

For the statistical study, the authors selected 20 files with different extensions: 1.docx, 2.xls, 3.pptx, 4.pdf, 5.rar, 6.zip, 7.jpg, 8.png, 9.txt, 10.html, 11.html, 12.cat, 13.mp4, 14.wmz, 15.dll, 16.log, 17.lex, 18.djvu, 19.xml and 20.mp3. Encrypting these files with different keys, 100 ciphertexts were obtained. Below are the results of the analysis of files encrypted using the AES (Figure 3) and AL02 (Figure 4) algorithms.

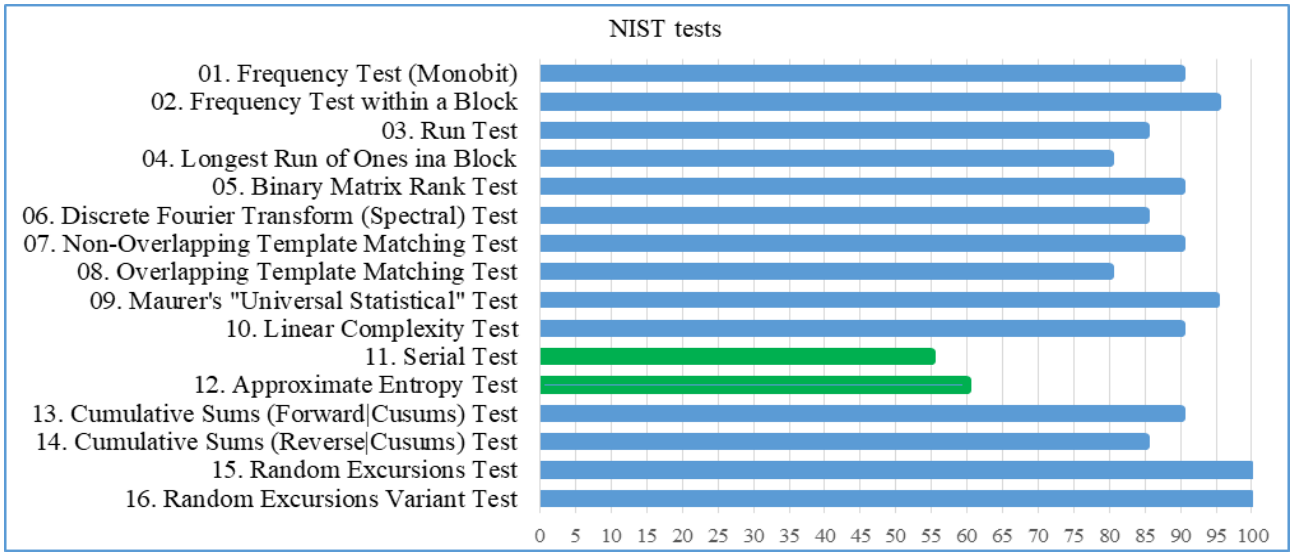

Figure 3: NIST test results in graphical form for the AES algorithm.

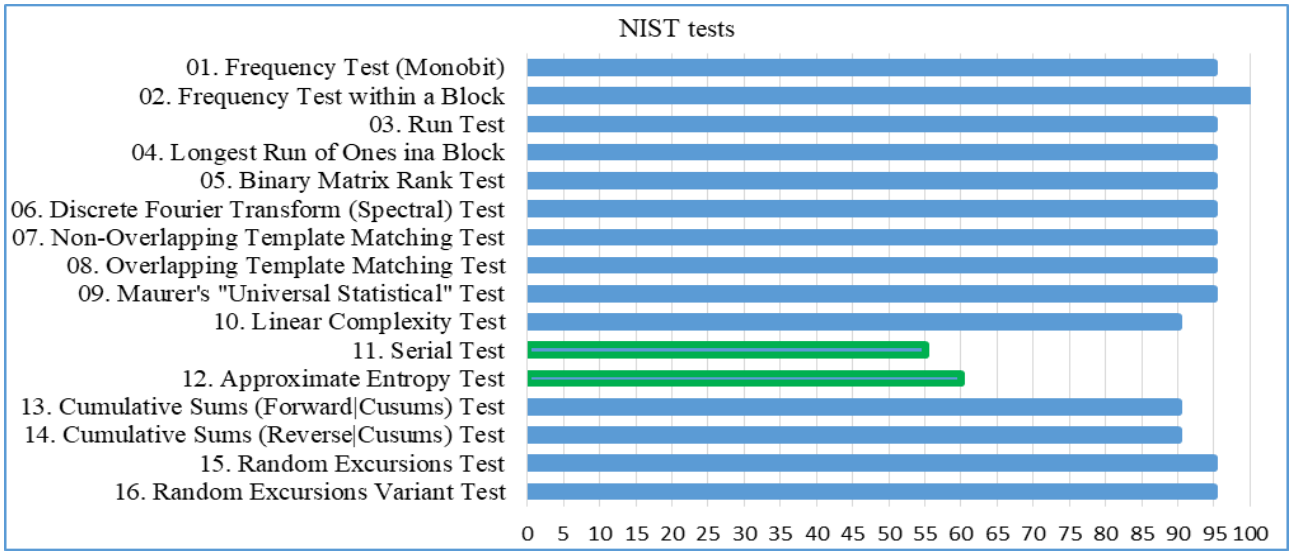

Figure 4: NIST test results in graphical form for the AL02 algorithm.

Figure 3 and Figure 4 show that the results of the serial test and the approximate entropy test do not meet the criteria for data randomness. The reason for this is a large number of repeating blocks in the 2.xls, 3.pptx, 11.html, 12.cat, 14.wmz, 15.dll, 16.log, 19.xml and 20.mp3 source files, resulting in a large number of repeating blocks in the corresponding encrypted files. Table 3 presents data on the number of block repetitions in the specified files. A closer look at the 2.xls file of 163968 bits clarifies the situation. After removing the repeating blocks, its size was 90624 bits. Table 3 shows the characteristics of the original file compared to the characteristics of the processed file.

Table 3: Results of analysis of repeating blocks of file 2.xls.

File characteristics	Original file	File after removing repeated blocks
Number of bits	163,968	90,624
Theoretical frequency of "0" and "1"	81,984	45,312
Number of blocks	1,281	708
"0" frequency	83,330	45,087
"1" frequency	80,638	45,537
Chi-squared value for the frequency of "0" and "1"	44,197	2,235

The results of the statistical tests show that repeated blocks have an impact on the characteristics of the ciphertext.

Second Option

When testing, a *selected* text was used based on 100 blocks of 16 bytes each, obtained using a pseudo-random sequence generator. The *selected* text uses each original block and its 128 variations, differing by one bit. The resulting file is 206,400 bytes in size. Figure 5 and Figure 6 show data for 100 texts that passed the NIST tests. The source texts were selected according to the second option and encrypted using the AES and AL02 algorithms.

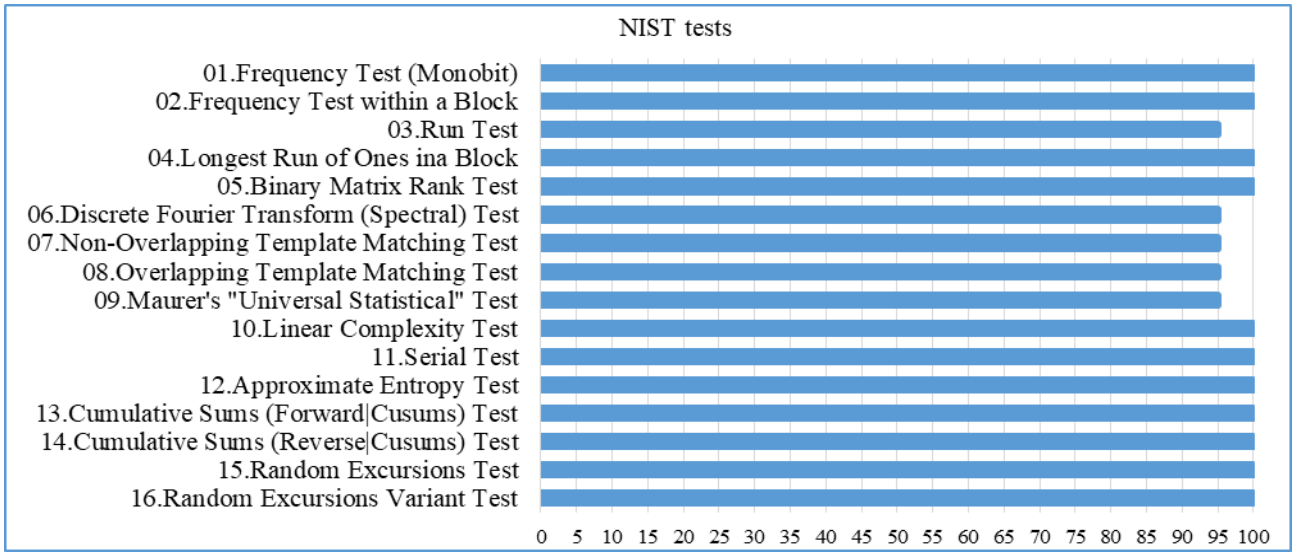

Figure 5: Results of statistical tests of the AES algorithm for the second option.

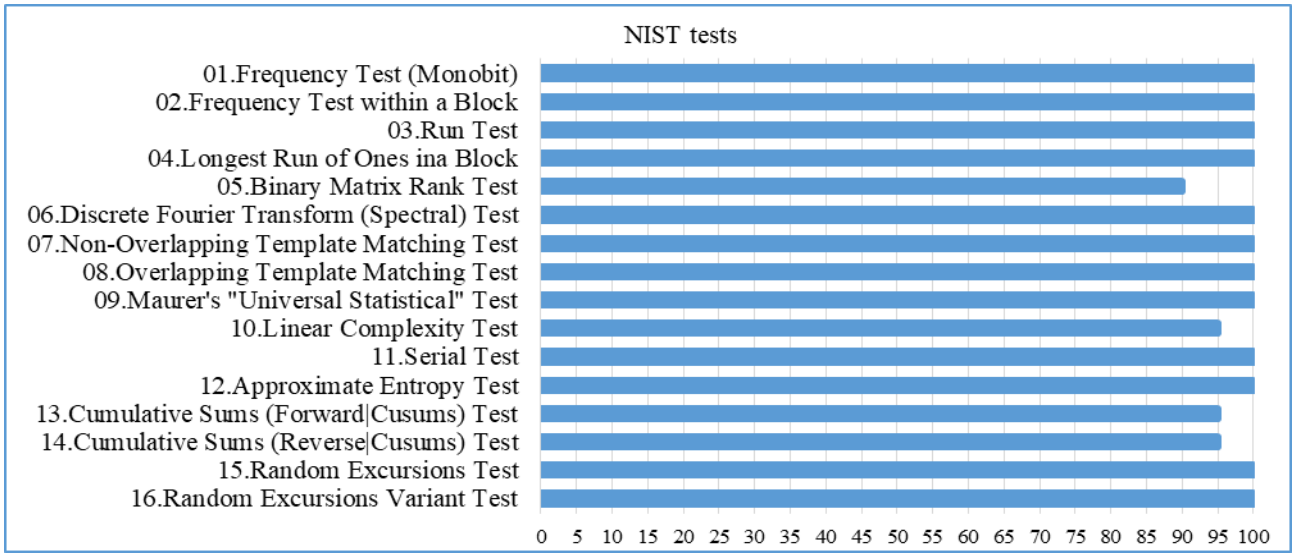

Figure 6: Results of statistical tests of the AL02 algorithm for the second option.

The comparison confirmed the hypothesis that when testing cryptographic algorithms for statistical security, it is necessary to use the second option, since repeating blocks can distort the test results.

CONCLUSIONS

The foundation for further development of the process of training personnel in the field of information security should be the actualisation of the methodology for teaching IS, taking into account the requirements of the modern market.

In this article, the methodology of testing for statistical security of cryptographic algorithms is considered, as well as results of statistical tests presented.

Sets of various tests were used for evaluation. For testing, two variants of the selection of open texts were considered: randomly selected files with different extensions and specially selected files with a different number of blocks. The well-known AES encryption algorithm and the developed new AL02 algorithm were used for encryption.

ACKNOWLEDGMENTS

The research work was carried out within the framework of the project AP08856426 *Development and study of an encryption algorithm and creation of a software and hardware complex for its implementation* at the Institute of Information and Computational Technologies, Almaty, Kazakhstan.

REFERENCES

1. Decree of the Government of the Republic of Kazakhstan Dated June 30, 2017, No.407 On Approval of the Cybersecurity Concept *Cybershield Kazakhstan*.
2. Decree of the Government of the Republic of Kazakhstan Dated December 12, 2017 No.827 On Approval of the State Program *Digital Kazakhstan*.
3. Karpov, D.S., Mikryukov, A.A. and Kozyrev, P.A., Improving the quality of learning of specialists in the field of learning *information security*. *Open Educ.*, 23, **6**, 22-29 (2019) (in Russian).
4. Kapalova, N., Dyusenbayev, D. and Sakan, K., A new hashing algorithm - HAS01: development, cryptographic properties and inclusion in graduate studies. *Global J. of Engng. Educ.*, 24, **2**, 155-164 (2022).
5. Sakan, K., Nyssanbayeva, S., Kapalova, N., Algazy, K., Khompysh, A. and Dyusenbayev, D., Development and analysis of the new hashing algorithm based on block cipher. *Eastern-European J. of Enterprise Technologies*, 116, **2/9**, 60-73 (2022).
6. Khompysh, A., Kapalova, N., Algazy, K., Dyusenbayev, D. and Sakan, K., Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. *Cogent Engng.*, 9, **1**, 1-14 (2022).
7. Algazy, K., Babenko, L., Biyashev, R., Ishchukova, E., Romaniuk, R., Kapalova, N., Smolarz, A. and Nysynbaeva, S., Differential cryptanalysis of new Qamal encryption algorithm. *Inter. J. of Electronics and Telecommunic.*, 66, **4**, 647-653 (2020).
8. Kapalova, N. and Haumen, A., The model of encryption algorithm based on non-positional polynomial notations and constructed on an SP-network. *Open Engng.*, 8, **1**, 140-146 (2018).
9. Biyashev, R.G., Kalimoldayev, M.N., Nyssanbayeva, S.E., Kapalova, N.A., Dyusenbayev, D.S. and Algazy K.T., Development and analysis of the encryption algorithm in nonpositional polynomial notations. *Eurasian J. of Mathematical and Computer Applications*, 6, **2**, 19-33 (2018).
10. Kapalova, N. and Dyusenbayev, D., Security analysis of an encryption scheme based on nonpositional polynomial notations. *Open Engng*., 6, **1**, 250-258 (2016).
11. Иванов, М.А. и Чугунков, И.В., Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: *КУДИЦ-ОБРАЗ*, 240, (2003) (in Russian).
12. Шнайер, Б., Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. - М.: ТРИУМФ, 816 (2003) (in Russian).

BIOGRAPHIES

Nursulu Kapalova received her Master's degree in mathematics from Al-Farabi Kazakh National University (KazNU), Almaty, Kazakhstan in 2002, and her Candidate of Technical Sciences degree (Almaty, Kazakhstan) in 2009. Currently, she is a leading researcher in the Information Security Laboratory at the Institute of Information and Computing Technology, Almaty, Kazakhstan, and an associate professor in the Department of Information Systems at KazNU. Her area of scientific work is development and research in the field of information protection.

Saule Nyssanbayeva graduated from the Faculty of Mechanics and Mathematics of Al-Farabi Kazakh National University (KazNU), Almaty, Kazakhstan, majoring in mathematics in 1971. She received her Master's degree in mathematics, and her doctorate in technical sciences (Almaty, Kazakhstan) in 2009. Currently she is an associate professor in the Department of Information Systems at KazNU and conducts research to protect information - ensuring its confidentiality, accessibility and integrity, as well as avoiding any compromise in a critical situation. Her research is carried out on the basis of scientific research and practical experience of a company producing information security systems.

Andrey Varennikov has been working with software engineering for more than 40 years, specialising in the development of cryptographic protection software, high-capacity multiuser distributed databases, workflow applications, artificial intelligence, system programming. He currently works in the Institute of Information and Computational Technologies of the Ministry of Science and Higher Education of the Republic of Kazakhstan. His *alma mater* is Kazakh National University, form which he received his Master of Science (MS) degree in computer science and applied mathematics.

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.

Kairat Sakan graduated from the Faculty of Mechanics and Mathematics of Al-Farabi Kazakh National University (KazNU), Almaty, Kazakhstan, majoring in mathematics and applied mathematics in 2001. In 2001-2002, he worked as a teacher in the Department of Applied Mathematics and Mathematical Modelling at KazNU. Between 2003 and 2005, he worked as a junior researcher at the Research Institute of Mathematics and Mechanics (IMM) of KazNU. After that, he worked in the field of information protection in the state structure for several years. Since 2018, he has been working as a mathematician in the Information Protection Laboratory at the Scientific Institute of Information and Computing Technologies, Almaty, Kazakhstan. Currently, he is a doctoral student at KazNU, majoring in information security systems. The field of scientific research is information protection in the public and private sectors.