NEWS
OF THENATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X **https://doi.org/10.32014/2020.2518-1726.85**
Volume 5, Number 333 (2020), 76 – 85

UDC 004.056.5
IRSTI 81.96

A.E. Abdrakhmanov[1], G.T. Turdiyeva[2]

[1]Contract production "Delta-IT" LLP, Almaty, Kazakhstan
[2]Academy of the CNS RK, Almaty, Kazakhstan.
E-mail: alzhan17@mail.ru, tguncham@mail.ru

SAFE THRESHOLDS FOR THE PARAMETERS OF CRYPTOGRAPHIC ALGORITHMS AND STANDARD ST RK 1073-2007

Abstract. This article considers the problems of finding modern secure thresholds for the parameters of cryptographic algorithms. We conducted a comparative analysis of the obtained secure thresholds against the thresholds of the state standard of the Republic of Kazakhstan ST RK 1073-2007 "Means of cryptographic protection of information. General technical requirements." Based on the results of the analysis and taking into account the experience of certification tests, we worked out specific proposals for amendments and additions to this Standard.

Key words: information security, cryptography, cryptographic algorithm parameters, state standard, security level.

Introduction. The state standard of the Republic of Kazakhstan ST RK 1073-2007 "Means of cryptographic protection of information. General technical requirements" (hereinafter "the Standard") was adopted 12 years ago and became the main Kazakhstan standard for assessing the quality of Means of Cryptographic Protection of Information (hereinafter – MCPIs) [1, 2].

Over the past time, theoretical cryptography has received new development, as well as the qualifications and computational capabilities of potential adversaries using distributed (network based) and quantum computing have also increased. At the same time, the use of global communication networks has significantly increased, including in banking information and payment systems that need cryptographic protection of information. All of this, makes it relevant, to define modern safe thresholds for parameters of cryptographic algorithms. Moreover, the built models of cryptographic information protection adversaries of also prove that some provisions of the Standard, especially those related to the first and second level of security, are outdated, and the Standard itself needs to be updated[3].

When updating the Standard, it is advisable to be guided by the following conceptual principles that had been substantiated and, to a large extent, verified by previous editions of the Standard [1, 4-6]:

1. Ensuring consistency with the previous editions of the Standard. This, on the one hand, will make it easier for developers and researchers of MCPIs to make a smooth transition to new requirements, and on the other hand, it will allow government bodies and other users of MCPIs to be guided by previously adopted regulatory legal acts in the field of MCPIs, presumably with minor changes.

2. Defining in the Standard all used cryptographic terms will facilitate an unambiguous understanding and application of the Standard, eliminate the need to constantly refer to the scientific and technical literature for the interpretation of terms.

3. Defining in the Standard four security levels of MCPIs associated with possible damage from disclosure, imposition, or uncontrolled changes in the protected information, the budget of a potential adversary, as well as the computational and spatial complexity of the known cryptographic-protection breaking algorithms. This will allow even unskilled users of MCPIs to build adequate protection. Besides, for the sake of consistency, it is advisable not only to maintain the four security levels but if the

requirements for them are tightened, it is highly desirable to do so in such a way that the requirements of each security level of a new version of the Standard do not exceed the requirements of the higher security level of the previous version. This will prevent or limit at one level a decrease in the security level of MCPIs when switching to a new edition of the Standard, which is extremely important for already deployed information and telecommunication systems.

4. Defining in the Standard general requirements, which are elementary in theoretical and applied cryptography and, therefore, are imposed on all MCPIs regardless of the level of security. This will help to counter threats exploiting the lack of deep cryptographic knowledge among individual developers and owners of MCPIs.

5. Defining in the Standard the main parameters of cryptographic algorithms and their secure threshold values, as a rule, with a 20% margin of strength for their absolute values, which provide resistance to known universal algorithms (attacks) for breaking cryptographic protection of the appropriate computational complexity. The need to introduce a margin of strength is confirmed by the history of the development of cryptography, which demonstrates the emergence of cryptographic attacks even on admittedly strong cryptographic algorithms that are more effective than universal attacks. These requirements will help the designers of MCPIs in the development and selection of cryptographic algorithms and protocols of the required strength, as well as, in certification and other tests, effectively identify cryptographic algorithms that are insecure against both universal algorithms for breaking cryptographic protection and most special attacks.

6. Defining in the Standard additional organizational and technical requirements for MCPIs depending on the level of security. This will allow MCPIs to withstand additional threats that substantially depend on the scientific, technical, operational and financial capabilities of the adversary.

7. Quitting in the Standard any definition of specific cryptographic algorithms and protocols. This makes it possible to conduct certification tests of MCPIs of different types and purposes, various domestic and foreign manufacturers.

Analysis of general requirements. In paragraphs 4 "General provisions", 5.1 "General requirements for MCPIs" and 5.2 "Requirements for technical documentation for MCPIs" of the Standard [1] set forth the common requirements for all MCPIs.

1.1. Subparagraphs 4.3.1, 4.3.2, 4.3.3, 4.3.4 and paragraph 4.4 of the Standard define four security levels, linked to the cost of the information to be protected with no more than 100, 10,000, 1,000,000 and 100,000,000 MCI for 1, 2, 3 and 4 security levels, as well as with the computational complexity of known algorithms for breaking cryptographic protection at 2^{50}, 2^{80}, 2^{120} and 2^{160}, respectively. The thresholds for the computational complexity of breaking algorithms for levels 1 and 2 are no longer secure [3]. Besides, the development of bank information and payment systems requires the processing of higher-priced information. Therefore, taking into account the models of cryptographic information protection adversaries, it is expedient to amend the wording in subparagraphs 4.3.1, 4.3.2, 4.3.3, 4.3.4 and paragraph 4.4 of the Standard, as follows:

"4.3.* MCPIs of the first (second, third, fourth) security level are designed to protect the information, the damage from disclosure, imposition or unauthorized modification of which in the amount protected using the same key (the same keys) does not exceed 100 (50 thousand, 25 million, 10 billion) monthly calculation indices, from potential adversaries with a budget of no more than 1,000 (1 million, 1 billion and 1 trillion) monthly calculation indices.

4.4 MCPIs cannot be recognized as appropriate to the first, second, third or fourth security levels if an algorithm for breaking cryptographic protection provided by them is known, the computational complexity of which is less than 2^{64}, 2^{96}, 2^{128} and 2^{160} operations, respectively, with due consideration of the inverse multiplicative correction for the probability of its successful application. If an algorithm for breaking cryptographic protection has a space complexity of at least 2^{60}, 2^{80}, 2^{100} and 2^{120} bits, respectively, then this algorithm is considered inapplicable."

1.2. Paragraph 4.2 of the Standard states that MCPIs are considered as technologically complete (workable) means. This wording does not allow us to unambiguously interpret this paragraph as a requirement, although the workability of the MCPIs is of fundamental importance. To correct this, it is advisable to transfer paragraph 4.2 of the Standard from Section 4 "General Provisions" to Section 5 as follows:

"5.1.1 MCPIs shall be technologically complete (workable) hardware, software, or firmware."

1.3. Subparagraphs 5.1.1, 5.3.6, 5.4.6, 5.5.6 and 5.6.6 of the Standard impose requirements on the randomness of generated and formed keys. However, the requirements are largely duplicated, not localized in one paragraph for each level of security, which also complicates the presentation and understanding of the results of certification tests in scientific reports and protocols. To correct this, it is advisable to exclude subparagraph 5.1.1 of the Standard, amend the wording of subparagraphs 5.3.6, 5.4.6, 5.5.6 and 5.6.6, and supplement the list of terms with the notions "random sequence of bits", "pseudo-random sequence of bits" and "non-deterministic pseudo-random sequence of bits".

1.4. Subparagraph 5.2.1 of the Standard requires a complete description of the implemented cryptographic transformation algorithms, and subparagraph 5.2.2 allows replacing the complete description with references to standards defining these algorithms. To correct the formal contradiction between these subparagraphs, it is reasonable to combine them into one subparagraph with the requirement for a complete description of the implemented algorithms or the presence of references to the standards defining these algorithms:

"5.2.1 The technical documentation (design, technological and software documentation, depending on the type of MCPI) for all cryptographic transformation, key generation, formation, distribution, and management algorithms implemented in a MCPI shall contain their full description or references to the defining them state and interstate standards or other regulatory documents on standardization, effective or applicable in the Republic of Kazakhstan in the prescribed manner."

Analysis of the requirements for the parameters of cryptographic algorithms. Paragraphs 5.3 "Requirements for MCPIs of the first security level", 5.4 "Requirements for MCPIs of the second security level", 5.5 "Requirements for MCPIs of the third security level" and 5.6 "Requirements for MCPIs of the fourth security level" of the Standard [1] set forth the requirements for the parameters of cryptographic algorithms that directly depend on the computational complexity of the well-known universal algorithms for breaking cryptographic protection. These requirements only partially comply with the above secure thresholds of 2^{64}, 2^{96}, 2^{128} and 2^{160} operations for security levels 1, 2, 3 and 4, respectively.

2.1. Subparagraphs 5.3.1, 5.4.1, 5.5.1 and 5.6.1 of the Standard specify that the key length of symmetric cryptographic transformation algorithms implemented by MCPIs shall be at least 60, 100, 150 and 200 bits for security levels 1, 2, 3 and 4, respectively. In the case of using these threshold key lengths, the all-key brute-force algorithm, which is universal and the only one applicable to all symmetric algorithms, will be able to break cryptographic protection in 2^{60}, 2^{100}, 2^{150} and 2^{200} encryption operations [7-11]. The value of 2^{60} is below the secure threshold of computational complexity for security level 1, as $2^{60} < 2^{64}$. The values of 2^{100} and 2^{150} correspond to secure thresholds of computational complexity for 2nd and 3rd security levels, but do not provide additional security margins of 20%, since $2^{100*80\%} = 2^{80} < 2^{96}$ and $2^{150*80\%} = 2^{120} < 2^{128}$. Therefore, to ensure the secure key length of symmetric cryptographic transformation algorithms, it is necessary to increase their threshold values in subparagraphs 5.3.1, 5.4.1 and 5.5.1 of the Standard to 80, 120 and 160 bits, respectively, while the requirements of subparagraph 5.6.1 of the Standard can be left unchanged. Then the brute-force algorithm will be able to break cryptographic protection in only 2^{80}, 2^{120}, 2^{160} and 2^{200} encryption operations with an additional security margin of 20%, since $2^{80*80\%} = 2^{64}$, $2^{120*80\%} = 2^{96}$, $2^{160*80\%} = 2^{128}$ and $2^{200*80\%} = 2^{160}$.

2.2. Subparagraphs 5.3.2, 5.4.2, 5.5.2 and 5.6.2 of the Standard indicate that the key length of asymmetric cryptographic transformation algorithms implemented by MCPIs shall be at least 120, 160, 250 and 400 bits for security levels 1, 2, 3 and 4, respectively. In the case of using these threshold key lengths, the all-key brute-force algorithm will be able to break cryptographic protection in 2^{120}, 2^{160}, 2^{250} and 2^{400} encryption operations, respectively. However, in all modern MCPIs, the implemented asymmetric cryptographic transformation algorithms use, as a one-way function, exponentiation in some finite multiplicative group G, usually cyclic and with order $ord(G) \approx 2^k$, where k is the length of the secret and/or public key. Thus the cryptographic strength of these algorithms is based on the computational complexity of the discrete logarithm problem in an arbitrary or cyclic finite multiplicative group. The computational complexity of known effective discrete logarithm algorithms in these groups (the Gelfond-Shanks algorithm, also called the baby-step giant-step algorithm, Pollard's kangaroo (λ) algorithm, Pollard's rho (ρ) algorithm, etc.), which do not impose significant additional restrictions on the group properties, is $O(\sqrt{ord}(G)) \approx \sqrt{ord}(G) \approx \sqrt{2^k} = 2^{k/2}$ and, respectively, 2^{60}, 2^{80}, 2^{125}, and 2^{200} operations for security levels 1, 2, 3 and 4 [7, 8, 12, 13]. The values of 2^{60}, 2^{80}, and 2^{125} do not attain the secure

thresholds of computational complexity for security levels 1, 2, and 3, since, $2^{60} < 2^{64}$, $2^{80} < 2^{96}$ and $2^{125} < 2^{128}$. Therefore, to ensure the secure key length of asymmetric cryptographic transformation algorithms, it is necessary to increase their threshold values in subparagraphs 5.3.2, 5.4.2 and 5.5.2 of the Standard to 160, 240 and 320 bits, respectively, while the requirements of subparagraph 5.6.2 of the Standard can be left unchanged. Then, discrete logarithm algorithms in an arbitrary or cyclic finite multiplicative group will be able to break cryptographic protection in only 2^{80}, 2^{120}, 2^{160} and 2^{200} operations, respectively, with an additional security margin of 20%, since $2^{80*80\%} = 2^{64}$, $2^{120*80\%} = 2^{96}$, $2^{160*80\%} = 2^{128}$ and $2^{200*80\%} = 2^{160}$.

2.3. Subparagraphs 5.3.3, 5.4.3, 5.5.3 and 5.6.3 of the Standard state that the key length of implemented by MCPIs asymmetric cryptographic transformation algorithms, the cryptographic strength of which is based on the computational complexity of the factorization problem or the discrete logarithm problem in a finite field, shall be at least 500, 1500, 4000 and 8000 bits for security levels 1, 2, 3 and 4, respectively. These subparagraphs reflect the fact that in many MCPIs, the implemented asymmetric cryptographic transformation algorithms use, as a mandatory one-way function, exponentiation in a finite field P whose order $ord(P) = n \approx 2^k$, where k is the length of the secret and/or public key. Notice that to provide a "loophole" for such a one-way function, the popular RSA algorithm uses the product of two secret primes: $n = p \times q$ as an element of the public key, and the secret key d falls in the range from 1 to $\varphi(n) = (p-1)(q-1)$, i.e. $n = p \times q \approx (p-1)(q-1) \approx 2^k$, where k is the length of the private key d. Hence, the cryptographic strength of these algorithms is based on the computational complexity of composite factorization or the discrete logarithm problem in a finite field. The computational complexity of the known effective factorization and discrete logarithm algorithms in a finite field (sieve algorithms for a number field) that do not impose additional restrictions on the properties of a composite number and a finite field is subexponential and evaluated as $L_n(1/3, (64/9)^{1/3})$, where $L_n(\alpha, c) = O(exp((c+o(1))(ln\ n)^{\alpha}(ln\ ln\ n)^{1-\alpha}))$ [7, 8, 12, 13]. Special algorithms for solving these problems (for example, special number field sieve algorithms) that impose significant additional restrictions on factorizable numbers and finite fields have a slightly lower computational complexity of $L_n(1/3, (32/9)^{1/3})$. In the case of using the existing threshold key lengths, the above universal algorithms will be able to break cryptographic protection in $2^{63.3}$, $2^{102.3}$, $2^{155.0}$ and $2^{206.5}$ operations, and special algorithms – in $2^{50.2}$, $2^{81.2}$, $2^{123.0}$, and $2^{163.9}$ operations for security levels 1, 2, 3 and 4, respectively. The value $2^{63.3}$ is below the secure threshold of computational complexity for security level 1, since $2^{63.3} < 2^{64}$. The value $2^{102.3}$ exceeds the secure threshold of computational complexity for security level 2, but does not provide an additional security margin even at 7%, since $2^{102.3*93\%} \approx 2^{95.1} < 2^{96}$. Therefore, to ensure the secure key length of asymmetric cryptographic conversion algorithms, the cryptographic strength of which is based on the computational complexity of the problem of composite factorization or the discrete logarithm problem in a finite field, it is necessary to increase their threshold values in subparagraphs 5.3.3 and 5.4.3 of the Standard to 1000 and 2000 bits, respectively, while the requirements of subparagraphs 5.5.3 and 5.6.3 of the Standard can be left unchanged. Then, the above universal algorithms will be able to break cryptographic protection in only $2^{85.9}$, $2^{115.7}$, $2^{155.0}$ and $2^{206.5}$ operations with additional security margins of about 20%, since $2^{85.9*74.5\%} \approx 2^{64}$, $2^{115.7*83.0\%} \approx 2^{96}$, $2^{155.0*82.6\%} \approx 2^{128}$ and $2^{206.5*77.5\%} \approx 2^{160}$.

2.4. Subparagraphs 5.3.4, 5.4.4, 5.5.4, and 5.6.4 of the Standard specify that the length of the hash code calculated by MCPIs shall be at least 120, 160, 250 and 400 bits for security levels 1, 2, 3 and 4, respectively. If these threshold hash code lengths are used, the universal pre-image search algorithm by exhaustive search of pre-images will be able to break cryptographic protection in 2^{120}, 2^{160}, 2^{250} and 2^{400} hash operations, but Yuval's algorithm (attack) for collision search, based on the birthday paradox and having computational complexity of $\approx 2^{m/2}$, where m is the length of the hash code, will be able to break cryptographic protection in2^{60}, 2^{80}, 2^{125} and 2^{200} hashing operations, respectively [7, 8, 14]. The values 2^{60}, 2^{80} and 2^{125} are below the corresponding secure thresholds of computational complexity for security levels 1, 2, and 3, since $2^{60} < 2^{64}$, $2^{80} < 2^{96}$ and $2^{125} < 2^{128}$. Therefore, to ensure secure hash code lengths, it is necessary to increase their threshold values to 160, 240 and 320 bits, respectively, in subparagraphs 5.3.4, 5.4.4 and 5.5.4 of the Standard, while the requirements of subparagraph 5.6.4 of the Standard can be left unchanged. Then Yuval's algorithm will be able to break cryptographic protection in only 2^{80}, 2^{120}, 2^{160}

and 2^{200} hashing operations with an additional security margin of 20%, since $2^{80*80\%} = 2^{64}$, $2^{120*80\%} = 2^{96}$, $2^{160*80\%} = 2^{128}$ and $2^{200*80\%} = 2^{160}$.

2.5. The Standard does not impose any requirements on the length of Message Authentication Code (MAC) computed by MCPIs. However, the complexity of breaking cryptographic protection provided by a MAC substantially depends on its length *m*. Since message authentication codes are designed to control data integrity and provide protection against falsified data entry and unauthorized modification of messages, then in addition to the all-key brute-force algorithm accounted for in subparagraphs 5.3.1, 5.4.1, 5.5.1 and 5.6.1 of the Standard, for breaking cryptographic protection, universal search algorithms for MACs (guessing attempts) can be used. The exhaustive algorithm for MACs has a computational complexity of 2^m operations for checking MACs [7, 8]. However, its characteristic feature is that the algorithm is not executed on the computing tools of an adversary, but by MCPIs, whose performance is significantly lower. Besides, MCPIs can limit the number of attempts to receive data with incorrect MACs. For these reasons, adversaries usually use for MACs a partial enumeration algorithm with the computational complexity *r* of operations for checking MACs or, taking into account the correction for the probability of its successful application, $r / (r/2^m) = 2^m$, where *r* is the number of attempts $1 \le r << 2^m$. Therefore, to ensure a secure length of MACs, it is necessary to supplement paragraphs 5.3, 5.4, 5.5, and 5.6 of the Standard with the following subparagraphs:

"5.*.5 The length of a MAC calculated by a MCPI shall be at least 80 (120, 160, 200) bits. For the sole purpose of protecting a MCPI against unauthorized modification, identifying corrupted keys, and garbled encrypted data, it is allowed to use shorter MACs, but not less than 15 (20, 30, 40) bits."

In the general case, search algorithms for MACs will be able to break cryptographic protection in only 2^{80}, 2^{120}, 2^{160} and 2^{200} operations for checking MACs with an additional security margin of 20%, since $2^{80*80\%} = 2^{64}$, $2^{120*80\%} = 2^{96}$, $2^{160*80\%} = 2^{128}$ and $2^{200*80\%} = 2^{160}$. In the above-mentioned exceptional cases, the algorithms will be able to break the cryptographic protection provided by a MAC, in just 2^{15}, 2^{20}, 2^{30} and 2^{40} operations, as corrected. However, in these cases, a MAC is an additional line of defense and breaking by an adversary of the entire cryptographic protection of a MCPI will be complicated by the expected organizational and physical protection of the MCPI against unauthorized access and modifications, the complexity of the directed and secretive change of the MCPI operation; organizational, cryptographic (encryption) and other technical protection of keys at the stage of their distribution and loading, identification of mismatch of downloaded keys by synchronization protocols of several MCPIs; cryptographic (encryption) protection of encrypted data, as well as the execution of a search algorithm for MACs by a MCPI itself, and not on the high-performance computing facilities of an adversary. The need for introducing exceptions is dictated by the principles of maintaining consistency with the previous edition of the Standard and ensuring that the requirements of each security level of the new version of the Standard do not exceed the requirements of the higher security level of the previous edition and, in particular, the requirements of subparagraphs 5.4.7, 5.4.8, 5.5.7, 5.5.8, 5.6.7 and 5.6.8 of the current Standard.

2.6. Subparagraphs 5.3.5, 5.4.5, 5.5.5 and 5.6.5 of the Standard state that the length of an electronic digital signature (DS) generated by a MCPI shall be at least 120, 200, 300 and 400 bits for security levels 1, 2, 3 and 4, respectively. In the case of using these threshold lengths of DS, the universal exhaustive algorithm for signatures will be able to break cryptographic protection in 2^{120}, 2^{200}, 2^{300} and 2^{400} operations for DS checking. However, in many modern MCPIs, the implemented DS generation and verification algorithms use the El-Gamal scheme, in which the signature is a pair (*r*, *s*) of length *m* bits with the elements *r* and *s*, as a rule, of the same length *m*/2 bits, and the signature verification reduces to comparing the value of an expression with the element *s*. Consequently, the exhaustive algorithm for elements *s* has the computational complexity of $2^{m/2}$ public key signature verification operations and, if threshold DS lengths are used, it can break cryptographic protection in 2^{60}, 2^{100}, 2^{150}, and 2^{200} operations for security levels 1, 2, 3 and 4, respectively [7, 8, 12, 13]. The value of 2^{60} does not attain the safe threshold of computational complexity for security level 1, since $2^{60} < 2^{64}$. The values of 2^{100} and 2^{150} are above the secure thresholds of computational complexity for 2nd and 3rd security levels, but do not provide an additional security margin of 20%, since $2^{100*80\%} = 2^{80} < 2^{96}$ and $2^{150*80\%} = 2^{120} < 2^{128}$. Therefore, to ensure a secure DS length, it is necessary, in subparagraphs 5.3.5, 5.4.5 and 5.5.5 of the Standard, to increase their threshold values to 160, 240 and 320 bits, respectively, while the requirements of subparagraph 5.6.5

of the Standard can be left unchanged. Then the exhaustive algorithm of the signature element will be able to break cryptographic protection in, respectively, only 2^{80}, 2^{120}, 2^{160} and 2^{200} operations of signature verification with an additional security margin of 20%, since $2^{80*80\%} = 2^{64}$, $2^{120*80\%} = 2^{96}$, $2^{160*80\%} = 2^{128}$ and $2^{200*80\%} = 2^{160}$.

2.7. Subparagraphs 5.3.6, 5.4.6, 5.5.6 and 5.6.6 of the Standard specify that the principle of generating and forming keys implemented by a MCPI shall ensure that each bit of the key takes on the value of one with a probability from the interval (0.5 ± 0.03), (0.5 ± 0.01), (0.5 ± 0.003) and (0.500 ± 0.001) for security levels 1, 2, 3 and 4, respectively, and, additionally, for security levels 3 and 4, keys shall be random-number sequences and generated using random-noise generators based on physical processes. These requirements, even with the increased specification for the computational complexity of cryptographic protection breaking algorithms, provide the necessary level of security [15]. So, a partial enumeration algorithm for the most probable keys of the same weight will have the computational complexity of C_n^w encryption operations or, subject to the correction for the probability of its successful application, $C_n^w / (C_n^w (0,5+d)^w (0,5-d)^{n-w}) = (0,5+d)^{-w} (0,5-d)^{w-n} \geq (0,5+d)^{-w} (0,5+d)^{w-n} = (0,5+d)^{-n}$, where n is the key length, w is the key weight (the number of 1-bits), $0,5+d$ is the probability that a bit of the key takes on a value of one. In the case of threshold values of the specified intervals, that is, for d = 0.03, 0.01, 0.003 and 0.001, the partial enumeration algorithm for the most probable keys with the lengths of 80, 120, 160 and 200 bits of cryptographic transformation algorithms will be able to break cryptographic protection in only more than $2^{73.2}$, $2^{116.5}$, $2^{158.6}$ and $2^{199.4}$ operations, as corrected, and with a security margin of more than 12%, since $2^{73.2*87.4\%} \approx 2^{64}$, $2^{116.5*82.4\%} \approx 2^{96}$, $2^{158.6*80.7\%} \approx 2^{128}$ and $2^{199.4*80.2\%} \approx 2^{160}$. Consequently, to ensure a secure interval of the probability that each bit of the key takes on the value of one, the threshold values in subparagraphs 5.3.6, 5.4.6, 5.5.6 and 5.6.6 of the Standard can be left unchanged, but the requirements themselves can be reworded as follows:

"5.3.6 The keys generated and formed by a MCPI shall be a random or non-deterministic pseudo-random sequence of bits, where each bit takes the value of one with a probability within the interval (0.500 ± 0.03).

5.4.6 The keys generated and formed by a MCPI shall be a random or non-deterministic pseudo-random sequence of bits, where each bit takes the value of one with a probability within the interval (0.500 ± 0.01).

5.5.6 The keys generated and formed by a MCPI shall be a random sequence of bits, where each bit takes the value of one with a probability within the interval (0.500 ± 0.003).

5.6.6 The keys generated and formed by a MCPI shall be a random sequence of bits, where each bit takes the value of one with a probability within the interval (0.500 ± 0.001)."

Analysis of additional requirements. In paragraphs 5.4 "Requirements for MCPIs of the second security level", 5.5 "Requirements for MCPIs of the third security level" and 5.6 "Requirements for MCPIs of the fourth security level" of the Standard [1] set forth additional security requirements.

3.1. Subparagraphs 5.4.7, 5.5.7 and 5.6.7 of the Standard state that MCPIs shall implement procedures for calculating and verifying key checking information to prevent the use of keys corrupted at the stage of distribution and loading with a probability of at least 0.9999, 0.999999 and 0.999999999 for levels 2, 3 and 4, respectively. In order to achieve compliance with the aforementioned lengths of MACs of 20, 30 and 40 bits, it is necessary to increase the threshold probability values to $1–10^{-6}$, $1–10^{-9}$ and $1–10^{-12}$, respectively.

3.2. Subparagraphs 5.4.8, 5.5.8 and 5.6.8 of the Standard specify that MCPIs shall implement procedures for calculating and verifying checking information about encrypted data to identify corrupted encrypted data with a probability of at least 0.9999, 0.999999 and 0.999999999 for security levels 2, 3 and 4, respectively, but for security levels 2 and 3 the requirement applies only to pre-encryption. This exception for online encryption was introduced for the possibility to certify for security levels 2 and 3 cryptographically strong encryptors for analog telephones and radio stations operating on a very narrowband voice data transfer channel and, therefore, excluding its use for transmitting additional checking information. However, the known definitions of preliminary encryption are more theoretical than practical, which leads to a subjective interpretation and circumvention of the requirements of the Standard when a MCPI is under development and certification tests. On the other hand, modern telecommunication

facilities and their data transfer protocols have built-in tools for detecting and/or correcting errors, which often makes it unnecessary for a MCPI to detect corrupted encrypted data. Given this and intending to comply with the aforementioned lengths of MACs of 20, 30 and 40 bits, it is necessary to increase the threshold probability values to $1–10^{-6}$, $1–10^{-9}$ and $1–10^{-12}$, respectively, and extend this requirement in the above subparagraphs to all types of encryption as follows:

"5.4.8 MCPIs shall implement procedures for calculating and verifying checking information about encrypting data to identify random errors in encrypted data with a probability of at least $1–10^{-6}$ or the MCPI documentation shall contain organizational and technical measures to ensure protection against this threat.

5.5.8 MCPIs shall implement procedures for generating and verifying MACs or DS for encrypting data to identify randomly or deliberately corrupted encrypted data with a probability of at least $1–10^{-9}$ or the MCPI documentation shall contain organizational and technical measures to ensure protection against this threat.

5.6.8 MCPIs shall implement procedures for generating and verifying MACs or DS for encrypting data for encrypted data to identify randomly or deliberately corrupted encrypted data with a probability of at least $1–10^{-12}$."

3.3. Subparagraph 5.4.9 of the Standard states that MCPIs shall inform the operator of the establishment, reset, and also the impossibility of establishing an encryption mode. Subparagraph 5.5.9 of the Standard, additionally, requires reporting other irregularities in operation. Moreover, subparagraph 5.6.9 of the Standard adds the requirement to prevent the transfer of open data to the storage, distribution, and subsequent processing of encrypted data. That is, the current version of these subparagraphs is oriented towards encryption and takes little account of authentication and key generation issues. The requirement to prevent transfer is poorly combined with the requirements of reporting and is also more theoretical than practical, which leads to a subjective interpretation of data areas and circumvention of the requirements of the Standard when a MCPI is under development and certification tests. At the same time, the Standard does consider issues of logging, which in recent years have been given a significant place in the integrated security system. Based on the foregoing, it is proposed to amend subparagraphs 5.4.9, 5.5.9, and 5.6.9 of the Standard as follows:

"5.4.9 MCPIs shall inform the operator about the current mode of operation.

5.5.9 MCPIs shall inform the operator about the current mode of operation and irregularities in operation.

5.6.9 MCPIs shall inform the operator about the current mode of operation and irregularities in operation, and to automatically log these events."

3.4. Subparagraph 5.5.11 of the Standard states that the routine procedures for deletion (destruction) of keys by a MCPI shall ensure that they cannot be recovered. In addition to this, subparagraph 5.6.11 of the Standard requires the delivery of technical means completed with the MCPI that implement the specified procedures, if the MCPI itself does not implement them. However, the issues of recovering information deleted in the RAM or external memory of a computer on various electronic and optical media are often very knowledge-based and ambiguous, which leads to a subjective interpretation of the impossibility of recovering deleted keys when a MCPI is under development and certification tests. The inclusion of a paper shredder or an incinerator for burning paper and other key carriers in each set of MCPI is excessive, especially in the presence of several MCPIs of the same type in an enterprise. Hence, it is advisable to amend subparagraphs 5.5.11 and 5.6.11 of the Standard as follows:

"5.*.11 MCPIs shall delete (destruct) keys on completing their distribution, management, and use, or the MCPI operational documentation shall contain organizational and technical measures for the deletion (destruction) of keys."

Conclusion. The secure thresholds for the parameters of cryptographic algorithms defined in the paper make it necessary to quickly revise the standard ST RK 1073-2007 to bring it into line with the current level of development of theoretical cryptography and the capabilities of potential adversaries. The developed proposals are specific and consistent with the current version of the Standard.

А.Е. Абдрахманов[1], Г.Т. Турдиева[2]

[1]«Delta-IT» келісімшарттық өндіріс» ЖШС, Алматы, Қазақстан;
[2]ҚР ҰҚК Академиясы, Алматы, Қазақстан

КРИПТОГРАФИЯЛЫҚ АЛГОРИТМ ПАРАМЕТРЛЕРІНЕ АРНАЛҒАН ҚАУІПСІЗ ШЕГІ ЖӘНЕ СТ РК 1073-2007 СТАНДАРТЫ

Аннотация. Қазақстан Республикасының ҚР СТ 1073-2007 «Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар» мемлекеттік стандарты 12 жыл бұрын қабылданды және ақпаратты криптографиялық қорғау құралдарының (АККҚ) сапасын бағалауда негізгі қазақстандық стандарт болып саналады. Осы күнге дейін теориялық криптография жаңаша дамуда, сондай-ақ әлуетті бұзушылардың біліктілігі мен есептеу мүмкіншіліктері де артты. Ақпараттың криптографиялық қорғанысын бұзушылардың құрастырған моделі, осы стандарттың бірнеше ережелерінің, әсіресе, бірінші және екінші деңгейдегі қауіпсіздікке қатыстылары ескірген, ал стандарттың өзін жаңалау қажеттілігін дәлелдейді.

Стандартты жаңалауда төмендегі тұжырымдымалық қағидаларға негізделген жөн:

1. Стандарттың алдыңғы редакциясымен сабақтастығын сақтау.

2. Стандартта қолданылатын барлық криптографиялық терминдерді анықтау.

3. Жариялаудан, мәжбүрлі немесе қорғаныстағы ақпаратты басқара алмайтындай етіп бұрмалаудан, әлеуетті бұзушы бюджетінен, сондай-ақ криптографиялық қорғаныстың белгілі алгоритмдерін есептеудегі және кеңістігіндегі қиыншылықтан келетін зақымды ескеріп, стандарттағы АККҚ қауіпсіз төрт деңгейін анықтау.

- Бірінші, екінші, үшінші және төртінші деңгейдегі АККҚ бюджеті 1000, 1 млн., 1 млрд, және 1 трлн АЕК болған әлеуеттік бұзушылардан бағасы сәйкес 100, 50 мың, 25 млн. және 10 млрд АЕК артпайтын ақпаратты қорғауға арналған;

- егер қолдану ықтималдылығы сәтті деп кері мультипликативті түзетуді ескере отырып алынған алгоритм күрделілігі 2^{64}, 2^{96}, 2^{128} және 2^{160} операциядан кем болса және криптографиялық қорғаныс алгоритмі белгілі болса, АККҚ қауіпсіздіктің сәйкес бірінші, екінші, үшінші және төртінші дейгейі бола алмайды. Егер криптографиялық қорғанысты ашу алгоритмінің күрделілігі 2^{60}, 2^{80}, 2^{100} және 2^{120} биттен аз болса, мұндай алгоритм қолдануға болмайды деп болжам жасаймыз.

4. Стандарттың жалпы талаптарында қорғаныс деңгейіне қарамастан барлық АККҚ қолданылатын теориялық және қолданбалы криптографияда белгілі нәрсені анықтап алу.

5. Стандартта криптографиялық алгоритмдердің негізгі параметрлерін және олардың есептеу күрделілігіне сәйкес криптографиялық қорғаныстарды ашудың (шабуыл) универсал алгоритмдерге төзімділігін қамтамасыз етететін, беріктігін ескере отырып қауіпсіздік шегінің шамасын анықтау. Нақты айтқанда:

- АККҚ криптографиялық түрлендірудегі симметриялық алгоритмде іске асырылатын кілт ұзындығы 1, 2, 3 және 4 қауіпсіздік деңгейі үшін сәйкес 80, 120, 160 және 200 биттен аз болмауы тиіс;

- АККҚ криптографиялық түрлендірудегі асимметриялық алгоритмде іске асырылатын кілт ұзындығы сәйкес 160, 240, 320 және 400 биттен аз болмауы тиіс;

- АККҚ криптографиялық түрлендірудегі асимметриялық алгоритмде іске асырылатын кілт ұзындығы криптографиялық төзімділігі құрама санның көбейткішке жіктеуге немесе ақырғы өрісте дискретті логорифмдеу мәселесіне негізделе отырып, есептің есептеу күрделілігіне сәйкес 1000, 2000, 4000 және 8000 биттен аз болмауы тиіс.

6. АККҚ қауіпсіздік деңгейіне сәйкес, стандарттағы ұйымдастырушы және техникалық қосымша талаптарды анықтау.

7. Стандарттағы нақты криптографиялық алгоритмдер мен протоколдарды анықтаудан бас тарту.

Түйін сөздер: ақпаратты қорғау, криптография, криптографиялық алгоритмдер параметрі, мемлекеттік стандарт, қорғаныс деңгейі.

А.Е. Абдрахманов[1], Г.Т. Турдиева[2]

[1]ТОО "Контрактное производство "Delta-IT", Алматы, Казахстан;
[2]Академия КНБ РК, Алматы, Казахстан

БЕЗОПАСНЫЕ ПОРОГИ ДЛЯ ПАРАМЕТРОВ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ И СТАНДАРТ СТ РК 1073-2007

Аннотация. Государственный стандарт Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" был принят 12 лет назад и стал

основным казахстанским стандартом для оценки качества средств криптографической защиты информации (СКЗИ). За прошедшее время теоретическая криптография получила новое развитие, а также выросли квалификация и вычислительные возможности потенциальных нарушителей. Построенные модели нарушителей криптографической защиты информации доказывают то, что ряд положений этого Стандарта, особенно касающиеся первого и второго уровня безопасности, устарели, а сам Стандарт необходимо обновить.

При обновлении Стандарта целесообразно руководствоваться следующими концептуальными принципами:

1. Сохранение преемственности с предыдущими редакциями Стандарта.

2. Определение в Стандарте всех используемых в нем криптографических терминов.

3. Определение в Стандарте четырех уровней безопасности СКЗИ, увязанных с возможным ущербом от разглашения, навязывания или неконтролируемого изменения защищаемой информации, с бюджетом потенциального нарушителя, а также с вычислительной и пространственной сложностью известных алгоритмов вскрытия криптографической защиты:

- СКЗИ первого, второго, третьего и четвертого уровней безопасности предназначены для защиты информации стоимостью не более 100, 50 тыс., 25 млн. и 10 млрд. МРП от потенциальных нарушителей с бюджетом не более 1000, 1 млн., 1 млрд. и 1 трлн. МРП соответственно;

- СКЗИ не могут быть признаны соответствующими первому, второму, третьему или четвертому уровню безопасности, если известен алгоритм вскрытия криптографической защиты, обеспечиваемой ими, вычислительная сложность которого составляет менее 2^{64}, 2^{96}, 2^{128} и 2^{160} операций соответственно, с учетом обратной мультипликативной поправки на вероятность его успешного применения. Если алгоритм вскрытия криптографической защиты имеет пространственную сложность не менее 2^{60}, 2^{80}, 2^{100} и 2^{120} бит соответственно, то этот алгоритм полагается неприменимым.

4. Определение в Стандарте общих требований, являющихся азбучными в теоретической и прикладной криптографии и, потому, предъявляемых ко всем СКЗИ независимо от уровня безопасности.

5. Определение в Стандарте основных параметров криптографических алгоритмов и их безопасных пороговых значений с запасом прочности, обеспечивающих стойкость к известным универсальным алгоритмам (атакам) вскрытия криптографической защиты соответствующей вычислительной сложности. В частности:

- длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 80, 120, 160 и 200 бит для 1, 2, 3 и 4 уровней безопасности соответственно;

- длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 160, 240, 320 и 400 бит соответственно;

- длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 1000, 2000, 4000 и 8000 бит соответственно.

6. Определение в Стандарте дополнительных организационных и технических требований, предъявляемых к СКЗИ в зависимости от уровня безопасности.

7. Отказ от определения в Стандарте конкретных криптографических алгоритмов и протоколов.

Ключевые слова: защита информации, криптография, параметры криптографических алгоритмов, государственный стандарт, уровень безопасности.

Information about the authors:

Alzhan Abdrakhmanov, Candidate of Physical and Mathematical Sciences, Advisor to Director General for cryptographic protection of information of Contract Production "Delta-IT" LLP, Almaty, Kazakhstan; alzhan17@mail.ru; https://orcid.org/0000-0003-2257-397X;

Guncham Turdiyeva, Docent of Academy of the Committee for the National Security, Almaty, Kazakhstan; tguncham@mail.ru; https://orcid.org/0000-0001-7566-7852

REFERENCES

[1] ST RK 1073-2007. Means of cryptographic protection of information. General technical requirements. Astana: Gosstandart, **2008**. 30 p. (in Russ.).

[2] On the approval of unified requirements in the field of information and communication technologies and information security: Decree of the Government of the Republic of Kazakhstan of 20.12.2016 № 832. *SAPP RK*. **2016**. № 65. P.428. (in Russ.).

[3] Abdrakhmanov A.E. Models of violators of cryptographic protection and standard ST RK 1073-2007. *Reports of the National Academy of Science of the Republic of Kazakhstan.* Almaty: NAS RK, **2017**. Volume 6, Number 316. P.62-71. (in Russ.)

[4] ST RK 1073-2002. Means of cryptographic protection of information. General technical requirements. Astana: Gosstandart, **2002**. 32 p. (in Russ.).

[5] Abdrakhmanov A.E., Baibatchayeva D.A. Cryptographic grounds for the development of standard ST RK 1073-2007. *VII International Scientific and Practical Conference "Information Security in Information and Telecommunication Systems"*. K.: EKMO, TEZIS, KPI, **2004**. P.59-60. (in Russ.).

[6] Abdrakhmanov A.E., Baibatchayeva D.A. Cryptographic grounds for the development of standard ST RK 1073-2007. *XI International Scientific and Practical Conference "Information Security in Information and Telecommunication Systems"*. K.: EKMO, TEZIS, KPI, **2008**. P.20-21. (in Russ.).

[7] A.Menezes, P.Oorschot, S.Vanstone. Handbook of Applied Cryptography. Boca Raton, New York, London, Tokyo: CRC Press, **1997**. 780 p. (in Eng.).

[8] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Cryptography basics. Study guide. M.: Gelios ARV, **2001**. 480 p. (in Russ.).

[9] J.Daemen, V.Rijmen. The Design of Rijndael. AES – The Advanced Encryption Standard. Berlin: Springer-Verlag, **2002**. 247 p. (in Eng.).

[10] Panasenko S.P. Encryption algorithms. Special handbook. St.Pb.: BHV-Petersburg, **2009**. 576 p. (in Russ.).

[11] Tokareva N.N. Symmetric cryptography. Short course: study guide. Novosibirsk: NSU, **2012**. 234 p. (in Eng.).

[12] N.Koblitz. A Course in Number Theory and Cryptography. 2nd ed. New York, Berlin, Heidelberg: Springer-Verlag, **1994**. 245 p. (in Eng.).

[13] A.Salomaa. Public-Key Cryptography. 2nd ed. Berlin, Heidelberg, New York: Springer-Verlag, **1996**. 285 p. (in Eng.)

[14] T.Bartkewitz. Building Hash Functions from Block Ciphers, Their Security and Implementation Properties. Bochum: Ruhr-University, **2009**. 20 p. (in Eng.).

[15] Abdrakhmanov A.E., Baibatchayeva D.A. On the question of the use of non-uniformity of the key generator when breaking ciphers using the brute force method. *Mathematical Journal.* Almaty: Institute of Mathematics MES RK, **2006**. Volume 6, Number 3(21). P.14-17. (in Russ.).