UDC 004.056.55 **doi: 10.32620/reks.2021.2.04**

V. AVRAMENKO, V. DEMIANENKO

Sumy State University, Sumy, Ukraine

SERIAL ENCRYPTION USING THE FUNCTIONS OF REAL VARIABLE

Context. *Using the functions of a real variable in cryptosystems as keys allow increasing their cryptographic strength since it is more difficult to select such keys. Therefore, the development of such systems is relevant.* ***Objective.*** *Cryptosystems with symmetric keys are proposed for encrypting and decrypting a sequence of characters represented as a one-dimensional numerical array of ASCII codes. These keys are functions of a real variable that satisfies certain restrictions. They can be both continuous and discrete.* ***Method.*** *Two cryptosystem options are proposed. In the first embodiment, the transmitting and receiving sides select two functions, the first transmitted symbol, the area of the function definition, and the step of changing the function argument. Discrete messages are encrypted by calculating the first-order integral disproportion of the encrypted array using a function. The corresponding value of the second function is added to the obtained cipher of each symbol for scrambling to complicate the analysis of the intercepted message. On the receiving side, the second function is subtracted and decryption performed by the inverse transformation of the formula for integral disproportion. In the second version, sequential encryption is performed when the cipher obtained using one of the key functions in the first stage is encrypted again by calculating the disproportion using the second function, the key. Accordingly, in two stages, decryption is performed.* ***Results.*** *Examples of encryption and decryption of a sequence of text characters are presented. It is shown that the same character is encoded differently depending on its position in the message. In the given examples it is presented the difficulty of key functions parameters choosing and the cryptographic strength of the proposed cryptosystem.* ***Conclusions.*** *Variants of the cryptosystem using the first-order integral disproportion function are proposed, in which the functions of a real variable serve as keys. To "crack" such a system, it is necessary not only to select the form of each function but also to find the values of its parameters with high accuracy. The system has high cryptographic strength.*

Keywords: *cryptosystems; disproportion functions; first-order integral disproportion function; real variable functions; key function; encryption; decryption; text messages.*

Abbreviations

AES – Advanced Encryption Standard.

Nomenclature

α is a constant;

β is a constant;

γ is a constant;

ρ is a constant;

$\varphi(t)$ is a function defined parametrically;

$\psi(t)$ is a function defined parametrically;

b is a constant;

c is a constant;

h is a step of changing the argument in the message and in the key functions;

i is a number of the element in the message;

$f_1(i)$ is an element of the array of the key function;

$f_2(i)$ is an array element of the second key function;

$f_1(x)$ is a key function;

$f_2(x)$ is a second key function;

N is a maximum number of characters transmitted;

$P_1(i)$ is an element of the cipher array after the first encryption;

$P_2(i)$ is an element of the cipher array after the second encryption;

t is a parameter;

x is an argument of the function representing the message and the key functions;

y(x) is a transmitted message;

$@d_x^{(n)}y$ is a disproportion over the n-th order derivative of y(x) with respect to x;

$@I_{f(x)}^{(1)}y(x)$ is an integral disproportion over the first-order derivative of y(x) with respect to f(x).

Introduction

The problem of ensuring the quality of information protection in information and communication systems is one of the most urgent one nowadays [1]. One of the possible ways to improve this quality is development of the new approaches in the cryptosystems creation.

Currently, symmetric and asymmetric encryption algorithms are used [2-4]. In symmetric systems, the same key is used for encryption and decryption. Hacking such a system requires listing the possible keys. The complexity of the search depends on the length of the key in bits.

For asymmetric algorithms, there are cryptanalysis methods that work faster than exhaustive search [5]. Therefore, in the case of their use, it becomes necessary to use longer keys compared to keys in symmetric systems.

Both symmetric and asymmetric systems use natural numbers, which makes it possible to develop various methods of breaking such cryptosystems up to the implementation of a simple selection of keys. Therefore, in order to increase the cryptographic strength, it is necessary to increase the length of the keys. However, this should consider constantly growing capabilities of computer technologies that can be used to hack a cryptosystem. In particular, the creation of quantum computers can have a great impact [6]. It is expected that their usage will significantly reduce the cryptographic strength of existing cryptosystems [5]. In particular, Grover's quantum algorithm [7] reduces the complexity of recovering the key of a symmetric encryption algorithm from the message text and cipher text 2 times.

Quantum algorithms also reduce the cryptographic strength of systems with asymmetric encryption [7-9].

All these facts indicate the need to develop cryptosystems based on other principles. In particular, encryption methods based on the use of real numbers may be of interest. It is known [10] that the set of real numbers has greater cardinality compared to the set of natural numbers. It can be expected that such cryptosystems may turn out to be more cryptographically stable in case of an attempt to brute force the key. A variant of this approach using a function of a real variable as a symmetric key is given in [11]. For encryption, the disproportionality function is used [12]. One of the possible options for the development of this approach is presented in this article.

1. Problem statement

It is necessary to develop two algorithms for encrypting and decrypting messages, using two functions of the real variable $f_1(x)$ and $f_2(x)$ as symmetric keys. Both functions can be either continuous or discrete. If the functions are continuous, then they are calculated with the same step for x to obtain N elements of the corresponding arrays $f_1(i)$ and $f_2(i)$.

The transmitted sequence of characters in the form of numerical values of their codes, for example, from the ASCII table, is represented as a one-dimensional array y(i), i = 1, 2, ... N, where N is the maximum possible number of characters in the message.

In the first algorithm, it used a combination of encryption by calculating the disproportionality of the message by the key function $f_1(x)$ and additional scrambling, by adding the function $f_2(x)$ to the result.

In the second algorithm, it is needed to perform sequential encryption, when the disproportionality obtained after encryption using the key $f_1(x)$ is encrypted using the second key - the function $f_2(x)$.

2. Review of the literature

Modern cryptosystems use a block cipher. It works with fixed-length groups of bits - blocks. Their size can be from 64 to 256 bits. The widely used block symmetric ciphers (BSS) are based on the use of several symmetric cryptographic transformations (elementary ciphers) [13]. When building them, three main approaches are used:

- based on Feistel networks; -IDEA-like ciphers;
- SPN (Permutation Replacement Network) structure. One of the common AES systems belongs to the SPN-based BSN [14, 15].

In it, cryptographic transformations are performed in simple substitution mode on 128-bit blocks (16 bytes), the length of which is 128 bits. The key length has several options: 128, 192, 256 bits.

Encryption algorithm GOST 28147-89 [16] also belongs to the category of block ciphers, where the two parts of the selected block of information are of equal size. This is a classic symmetric encryption algorithm based on the Feistel network.

In 1978, the RSA algorithm was proposed [17]. This algorithm was the first full-fledged public key algorithm.

Hash functions are widely used in the implementation of modern cryptosystems [18]. Hashing algorithms are commonly used to digitally fingerprint the contents of a file, often used to ensure that a file has not been altered by an attacker or virus. Hash is one way encryption. Its use prevents finding the original string that created it, despite the fact that many websites claim or suggest otherwise [18].

To enhance the protection of information, a variety of scrambling methods are used [19-21].

In addition to classical crypto systems using natural numbers, algorithms based on functions of real variables have been proposed. So in [12] a function of a real variable is used as a symmetric key. To obtain the cipher, the integral disproportionality of the first order [22] of the encrypted message by the key function is calculated. At the receiving end, decryption is carried out using the same key function. The use of the disproportionality function makes the message invariant with respect to the amplitude of the signal transmitted over the communication channel. This property allows you to use not only digital, but also analog communication channels.

3. Materials and methods

The proposed methods for encrypting and decrypting messages are based on the use of disproportion functions. There are several types of these functions: the disproportion over n-th order derivative, the disproportion over n-th order value, relative and sequential disproportions. All of them are characteristics of numerical functions. Below is a summary of all these functions.

The disproportion over n-th order derivative of the function y (x) with respect to x is described by the expression:

$$@\, d_x^{(n)} y = \frac{y}{x^n} - \frac{1}{n!} \cdot \frac{d^n y}{dx^n}. \qquad (1)$$

Here, the @ symbol is chosen to indicate the operation of calculating disproportion. The symbol “d” means “derivative”. The order is indicated in parentheses. The left side of (1) reads “at d n y with respect to x”.

The disproportion (1) is equal to zero if the function y(x) has the form y = kx^n and it is invariant with respect to the coefficient of proportionality k.

The disproportion over first order derivative (n=1) has the form:

$$@\, d_x^{(1)} y = \frac{y}{x} - \frac{dy}{dx}. \qquad (2)$$

If the functions x = φ (t), y = ψ (t), are defined parametrically (t is parameter), the disproportion (2) has the form:

$$@\, d_{\varphi(t)}^{(1)} \psi(t) = \frac{\psi(t)}{\varphi(t)} - \frac{d\psi / dt}{d\varphi / dt}. \qquad (3)$$

If there is a proportional dependence ψ(t) = kφ(t) between two functions ψ(t) and φ(t), the disproportion (3) is equal to zero in the entire area of their existence, regardless of the value of the proportionality coefficient.

It should be noted that the disproportion functions allow one to calculate unknown coefficients before the known functions that form the sum y(x), using the values obtained for the current value of the argument.

If the function is discrete or constant at some intervals, it is impossible to use the imbalance (3). In this case the first order integral disproportion can be used [22].

This disproportion of the function y(x) with respect to f(x) has the form:

$$@\, I_{f(x)}^{(1)} y(x) = \frac{\int_{x-h}^{x} y(x)dx}{\int_{x-h}^{x} f(x)dx} - \frac{y(x)}{f(x)}, \qquad (4)$$

where h is the preset step for changing x.

For the discrete representation of text symbols sequences this step is equal to one. For discrete function, y(x) and f(x) are represented by one-dimensional arrays. If the approximate values of the integrals in (4) are calculated using the trapezoidal formula, then for the one and the same step h for y(x) and f(x), disproportion (4) takes the form:

$$@\, I_{f_i}^{(1)} y_i = \frac{y_{i-1} + y_i}{f_{i-1} + f_i} - \frac{y_i}{f_i}. \qquad (5)$$

Expression (6) defines the inverse transformation through integral disproportion (5):

$$y_i = \frac{(y_{i-1} - I_i \cdot (f_{i-1} + f_i)) \cdot f_i}{f_{i-1}}. \qquad (6)$$

For encrypting text messages, it is most convenient to use integral disproportion (5). However, in addition to the functions f$_1$(x) and f$_2$(x), it is also necessary to provide for some symbol known to the transmitting and receiving sides, from which the transmission of messages must necessarily begin. This condition provides knowledge of the initial values of the arrays used.

Two cryptosystem options are proposed. The first of them is one of the given functions, for example, f$_1$(x), is used as a key. With its help, the text will be encrypted. For this, the elements of the array P$_1$(i) (i = 1, 2, ..., N) of integral disproportion (5) y(x) with respect to f$_1$(x) are calculated:

$$P_1(i) = @\, I_{f_i(i)}^{(1)} y(i) = \frac{y(i-1) + y(i)}{f_1(i-1) + f_1(i)} - \frac{y_i}{f_1(i)}. \qquad (7)$$

The final cipher P$_2$(i) for the i-th character is formed by scrambling.

The corresponding element f$_2$(i) is added to the disproportion (7)

$$P_2(i) = P_1(i) + f_2(i). \qquad (8)$$

This cipher is transmitted over the communication channel.

At the receiving end, f$_2$(i) is subtracted from the received cipher first. The obtained result P$_1$(i) is used for decryption in accordance with expression (6):

$$y(i) = (y(i-1) - P_1(i)(f_1(i-1) + \\ + f_1(i)))\frac{f_1(i)}{f_1(i-1)}. \qquad (9)$$

The second option is a sequential (cascade) encryption/decryption of the message using two functions - keys. The initial message y(i), i = 1, 2, ..., N is encrypted by calculating its integral disproportion (7) using the first key function $f_1(i)$. For the code $P_1(i)$ obtained during the first encryption, the integral disproportion of $P_2(i)$ is calculated using the second key-function $f_2(i)$:

$$P_2(i) = @I^{(1)}_{f_2(i)}P_1(i) = \frac{P_1(i-1)+P_1(i)}{f_2(i-1)+f_2(i)} - \frac{P_2(i)}{f_2(i)}. \qquad (10)$$

This disproportion is the final cipher of the i-th character and is transmitted over the communication channel. At the receiving point, the code is first decrypted using the second key function $f_2(i)$:

$$P_1(i) = (P_1(i-1) - P_2(i)(f_2(i-1) + \\ + f_2(i)))\frac{f_2(i)}{f_2(i-1)}. \qquad (11)$$

Then this code is decrypted again using the first key- function $f_1(i)$:

$$y(i) = (y(i-1) - P_1(i)(f_1(i-1) + \\ + f_1(i)))\frac{f_1(i)}{f_1(i-1)}. \qquad (12)$$

As a result, the transmitted message is completely decrypted.

4. Experiments

For each version of the cryptosystem the results of messages encryption and decryption are investigated using computer simulation. In addition, the results of attempts to crack these systems by selecting functions parameters are presented.

Functions used:

$$f_1(x) = e^{\alpha\cos(\beta x)} + \gamma^{\sin(\rho x)} + \rho(0.1 + bx)^{\sin(cx)}, \qquad (13)$$

$$f_2(x) = \gamma e^{\cos(\rho x)}. \qquad (14)$$

Here, x=ih is an argument,

i is a sequence number of the character in the encrypted message,

h = 1 is a step of changing the argument,

α = 0.1, β = 0.25, b = 0.65, c = 0.15, γ=0.14, ρ=1.25 are constants.

The symbol 'G', whose ASCII code is 71, is taken as a required first character.

5. Results

First, the results of the study of the first version of the cryptosystem are shown, in which encryption is performed using the key function $f_1(x)$. Second function $f_2(x)$ serves to hide the resulting cipher. Encrypted and decrypted texts are shown in the Table 1.

To crack the cryptosystem, you need not only to find expressions for $f_1(x)$ and $f_2(x)$, but also to select their parameters with high accuracy, as it can be seen from Table 2.

This table shows the results of incorrect selection of only one parameter of the key function. When decrypting, instead of b = 0.65, an incorrect value of 0.648 was selected.

Obviously, even such a slight discrepancy makes it impossible to decrypt the text.

The effect of incorrect parameter selection for the function $f_2(x)$ is also separately shown.

When decoding, instead of ρ = 1.25, an incorrect value of 1.248 was selected. From Table 3 it is seen that in this case, the source text is not restored.

Table 4 represents codes for some repeating characters. It is shown that these codes are not repeated. This property greatly complicates the hacking of system.

Below the experimental results for the second variant of the cryptosystem are shown, in which the message is encrypted / decrypted sequentially. Obviously, sequential encryption increases computational complexity. Accordingly, minor errors can lead to distortion of the transmitted message. Therefore, as in the previous case, below are the results of the normal operation of the system, as well as for unsuccessful attempts to select the parameters of the key functions.

Table 5 shows the results of sequential encryption and decryption of the text during normal operation of the cryptosystem.

Table 6 shows the message of repeating characters.

It can be seen that the ciphers of consecutive identical characters differ significantly.

Table 7 shows the results of an attempt to select the value of at least one of the parameters of the key functions. When trying to break in, instead of α = 0.1, α = 0.098 was used. The values of the remaining parameters of the functions $f_1(x)$ and $f_2(x)$ remained correct.

Obviously, even such a minor change in the decryption system did not allow the recovery of encrypted characters. For many characters, even incorrect decryption failed. The cell of result is empty.

Table 1

Results of the study of the first version
of the cryptosystem

Character number	Source character	Character code	Decrypted character
1		4.736651	
2	T	9.827081	T
3	h	0.755083	h
4	i	5.261803	i
5	s	1.152270	s
6		3.755743	
7	i	9.116020	i
8	n	0.786342	n
9	f	2.269933	f
10	o	1.826009	o
11	r	1.472602	r
12	m	1.002936	m
13	a	0.201286	a
14	t	0.809798	t
15	I	0.709713	i
16	o	0.305642	o
17	n	1.089021	n
18		2.385154	
19	I	5.722505	i
20	s	2.220175	s
21		5.790948	
22	v	7.284821	v
23	e	3.446238	e
24	r	0.744297	r
25	y	11.901334	y
26		10.441133	
27	s	21.930138	s
28	e	4.811599	e
29	c	7.407188	c
30	r	2.014043	r
31	e	10.269830	e
32	t	29.005365	t
33		25.716858	
34	1	3.933851	1
35		6.844367	
36	2	0.908304	2
37		0.476755	
38	3	17.774094	3
39		2.668039	
40	&	1.690020	&
41		5.701226	
42	%	2.056424	%
43		0.008956	
44	+	12.513533	+
45		2.917707	
46	$	1.573350	$
47		4.929141	
48	@	1.444875	@

Table 2

Results of incorrect selection of only
one parameter b of the function

Character number	Source character	Character code	Decrypted character
1		4.736145	
2	T	9.827502	T
3	h	0.755026	h
4	i	5.262350	h
5	s	1.154490	t
6		3.757312	
7	i	9.119426	h
8	n	0.783920	m
9	f	2.269396	e
10	o	1.826811	m
11	r	1.476416	q
12	m	0.997617	m
13	a	0.205887	`
14	t	0.815445	s
15	i	0.708061	h
16	o	0.306217	m
17	n	1.093251	l
18		2.394330	
19	i	5.724770	i
20	s	2.229892	s
21		5.787251	
22	v	7.284874	s
23	e	3.450069	a
24	r	0.732833	u
25	y	11.897505	•
26		10.427940	!
27	s	21.937176	t
28	e	4.810447	c
29	c	7.410173	a
30	r	2.025765	y
31	e	10.258139	r
32	t	29.018993	x
33		25.704985	!
34	1	3.936796	1
35		6.846261	#
36	2	0.918751	=
37		0.458459	,
38	3	17.782860	9
39		2.650315	"
40	&	1.695828	'
41		5.701799	"
42	%	2.064831	0
43		0.030493	1
44	+	12.511976	5
45		2.940573	#
46	$	1.583545	&
47		4.928022	"
48	@	1.451049	F

Table 3

Results of incorrect selection of only one parameter ρ of the function $f_2(x)$

Character number	Source character	Character code	Decrypted character
1		4.736328	
2	T	9.827351	T
3	h	0.755047	h
4	i	5.262154	i
5	s	1.153693	t
6		3.756739	
7	i	9.118203	i
8	n	0.784798	n
9	f	2.269593	f
10	o	1.826527	n
11	r	1.475055	r
12	m	0.999550	n
13	a	0.204263	a
14	t	0.813394	t
15	i	0.708669	i
16	o	0.306020	n
17	n	1.091755	m
18		2.391024	
19	i	5.724051	i
20	s	2.226370	r
21		5.788615	
22	v	7.284837	t
23	e	3.448728	b
24	r	0.736921	t
25	y	11.899046	|
26		10.432673	
27	s	21.934574	s
28	e	4.810894	c
29	c	7.409145	a
30	r	2.021633	v
31	e	10.262514	m
32	t	29.014231	v
33		25.709368	!
34	1	3.935677	1
35		6.845631	!
36	2	0.915115	9
37		0.465123	'
38	3	17.780052	6
39		2.656818	!
40	&	1.693630	&
41		5.701655	!
42	%	2.061946	,
43		0.022813	*
44	+	12.513064	1
45		2.932309	"
46	$	1.579694	%
47		4.928509	!
48	@	1.448968	D

Table 4

Codes results for repeating characters

Character number	Source character	Character code	Decrypted character
1		4.736651	
2	a	12.332898	a
3	a	3.870525	a
4	a	4.947813	a
5	a	1.464428	a
6	a	5.052976	a
7	a	1.745526	a
8	a	1.140239	a
9		6.086579	
10	A	0.644718	A
11	A	0.908728	A
12	A	0.710290	A
13	A	0.508348	A
14	A	0.075961	A
15	A	0.110512	A
16	A	0.335408	A
17		1.473863	
18	0	0.895035	0
19	0	1.114129	0
20	0	0.666694	0
21	0	0.588647	0
22	0	0.105267	0
23	0	1.115444	0
24	0	0.021846	0
25		1.822263	
26	1	6.832296	1
27	1	1.938426	1
28	1	0.840899	1
29	1	1.335157	1
30	1	5.506334	1
31	1	11.042415	1
32		3.697263	
33	%	0.325424	%
34	%	4.033030	%
35	%	1.813313	%
36	%	2.172785	%
37	%	10.710403	%
38	%	4.579929	%
39	%	0.696619	%
40		5.428902	
41	*	1.877837	*
42	*	0.484670	*
43	*	10.899045	*
44	*	8.360439	*
45	*	0.088501	*
46	*	4.769559	*
47	*	3.726852	*
48		1.383015	
49	^	18.771311	^

Continuation of the Table 4

Character number	Source character	Character code	Decrypted character
50	^	11.266954	^
51	^	2.538162	^
52	^	5.122117	^
53	^	5.237040	^
54	^	2.362503	^
55	^	1.346288	^

Table 5

Results of sequential encryption and decryption of the text during normal operation of the cryptosystem

Character number	Source character	Character code	Decrypted character
1		4.690454	
2	T	8.047946	T
3	h	4.010225	h
4	e	2.791579	e
5		2.530756	
6	r	8.546450	r
7	e	2.965447	e
8	s	1.918389	s
9	u	1.524762	u
10	l	1.526856	l
11	t	0.502380	t
12	s	0.291666	s
13		3.795387	
14	s	2.034440	s
15	u	3.246364	u
16	c	0.828073	c
17	c	1.495243	c
18	e	1.082021	e
19	s	1.262968	s
20	s	12.145824	s
21	i	9.436130	i
22	v	6.408713	v
23	e	10.422213	e
24		6.812392	
25	e	24.949280	e
26	n	25.262545	n
27	c	3.958015	c
28	r	10.328294	r
29	y	5.330626	y
30	p	21.770363	p
31	t	33.014248	t
32	i	5.095774	i
33	o	13.558111	o
34	n	5.956150	n
35		0.900549	
36	a	46.172897	a
37	n	2.926001	n
38	d	15.682445	d
39		7.617536	
40	d	20.759953	d
41	e	12.218971	e
42	c	5.407150	c
43	r	5.710254	r
44	y	3.656684	y
45	p	1.611940	p
46	t	0.797022	t
47	i	1.737167	i
48	o	0.847489	o
49	n	0.706682	n
50	@	0.698381	@
51		0.125770	=

Table 6

Message of repeating characters

Character number	Source character	Character code	Decrypted character
1		4.690454	
2	a	10.239541	a
3	a	5.899044	a
4	a	2.497451	a
5	a	6.476577	a
6	a	0.164803	a
7	a	1.700911	a
8	a	2.365286	a
9		3.086447	
10	A	2.453165	A
11	A	0.061252	A
12	A	0.137451	A
13	A	0.497965	A
14	A	0.465165	A
15	A	1.760381	A
16	A	1.248392	A
17		2.009082	
18	0	0.626486	0
19	0	0.858078	0
20	0	5.069551	0
21	0	5.009539	0
22	0	1.455607	0
23	0	3.659701	0
24	0	1.969203	0
25		4.520895	
26	1	14.347497	1
27	1	0.095464	1
28	1	5.738425	1
29	1	2.401474	1
30	1	9.890567	1
31	1	13.504825	1
32	1	0.350023	1

Continuation of the Table 6

Character number	Source character	Character code	Decrypted character
33		8.080703	
34	%	1.531735	%
35	%	7.400918	%
36	%	11.073833	%
37	%	0.775017	%
38	%	4.971673	%
39	%	1.988361	%
40	%	5.483652	%
41		2.815113	
42	*	0.158020	*
43	*	2.833350	*
44	*	1.414040	*
45	*	0.771326	*
46	*	0.365959	*
47	*	0.518192	*
48	*	0.382304	*
49		0.377935	
50	^	0.824084	^
51	^	0.128106	^
52	^	0.090439	^
53	^	0.042821	^
54	^	0.051633	^
55	^	0.320289	^
56	^	0.445522	^

Table 7

Results of an attempt to select the value of at least one of the parameters of the key functions for the message of repeating characters

Character number	Source character	Character code	Decrypted character
1		4.748097	
2	a	10.167147	`
3	a	5.949846	_
4	a	2.563663	[
5	a	6.391641	]
6	a	0.093599	]
7	a	1.760433	[
8	a	2.423949	V
9		3.154067	
10	A	2.370525	2
11	A	0.012345	1
12	A	0.201686	/
13	A	0.561330	)
14	A	0.537713	
15	A	1.676859	,
16	A	1.171159	0
17		2.071810	
18	0	0.560162	
19	0	0.931029	
20	0	4.980809	$
21	0	4.925797	)
22	0	1.386247	)
23	0	3.719603	"
24	0	2.040457	
25		4.432795	
26	1	14.249585	+
27	1	0.162092	+
28	1	5.794245	#
29	1	2.470923	
30	1	9.796751	%
31	1	13.409384	+
32	1	0.415038	+
33		8.130970	
34	%	1.600165	
35	%	7.312530	
36	%	10.983509	
37	%	0.837987	
38	%	5.025629	
39	%	2.054488	
40	%	5.399350	
41		2.738085	
42	*	0.093902	
43	*	2.890316	
44	*	1.480261	
45	*	0.693815	
46	*	0.438466	
47	*	0.581506	
48	*	0.443650	
49		0.445842	
50	^	0.746201	L
51	^	0.201591	&
52	^	0.155069	
53	^	0.105113	
54	^	0.120200	
55	^	0.242766	)
56	^	0.370484	n

6. Discussion

The proposed cryptosystems are sensitive to computational errors. It should also be noted that in these systems there is an effect similar to the “avalanche effect” in the AES cryptosystem. It consists of the fact that behind an incorrectly decrypted character the remaining message is decrypted incorrectly.

Therefore, key functions must satisfy the following requirements:

1) the functions should not be constant and not take zero values;

2) when using the key-function, a situation should not arise when the number is divided by a number close to zero, which leads to the appearance of an unacceptable calculation error. To this end, it is recommended to test the cryptosystem for the entire alphabet of characters that will be used in messages.

Conclusions

New methods are proposed for encrypting and decrypting text messages based on two functions of a real variable. In this case, first-order integral disproportions are used. To create such a system, it is necessary to define two functions of a truly variable that satisfy certain requirements. Also, a character is set that must be transmitted at the very beginning of the message. The simulation results of these systems confirm their performance. To crack these systems, you need to know the form of both key functions, as well as the values of their parameters. Given examples confirm the high cryptographic strength of the systems. However, such cryptosystems are sensitive to computational errors. Therefore, it is recommended to check decrypted message before sending an encrypted one.

Usage of the disproportionality function makes the message invariant with respect to the amplitude of the signal transmitted over the communication channel. This property allows you to use not only digital, but also analog communication channels.

In the future, it is expected to do more detailed study of the requirements for Key Functions and their coefficients. In addition, it will be considered to study proposed cryptosystem resistance to cracking.

References (GOST 7.1:2006)

1. Shelechov, I. V. A Hierarchical Fuzzy Quality Assessment of Complex Security Information Systems [Text] / I. V. Shelechov, N. L. Barchenko, V. V. Kalchenko, V. K. Obodiak // Radioelectronic and computer systems. - 2020. - Vol. 4. – P. 106-115. DOI: 10.32620/reks.2020.4.10.

2. Smart, N. Cryptography: An Introduction [Electronic resource] / N. Smart ; 3rd ed. – University of Bristol, 2014. – 424 p. – Access mode: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf. – 12.02.2021.

3. Ferguson, N. Cryptography Engineering: Design Principles and Practical Applications [Text] / N. Ferguson, B. Schneier, T. Kohno. – New York : John Wiley & Sons, 2010. – 353 p. DOI: 10.1002/9781118722367.

4. Boneh, D. A Graduate Course in Applied Cryptography. Version 0.5. [Electronic resource] / D. Boneh, V. Shoup. – Access mode: https://toc.cryptobook.us/book.pdf. – 12.02.2021.

5. Ключарев, П. Г. Квантовый компьютер и криптографическая стойкость современных систем шифрования [Текст] / П. Г. Ключарев // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия «Естественные науки». – 2007. – № 2. – С. 113-120.

6. Quantum Computing [Text] / T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'Brien // Nature. – 2010. – Vol. 464. – P. 45-53. DOI: 10.1038/nature08812.

7. Grover, L. K. Quantum Mechanics Help in Searching for a Needle in a Haystack [Text] / L. K. Grover // Phys. Rev. Lett. – 1997. – Vol. 79. – P. 325-328. DOI: 10.1103/PhysRevLett.79.325.

8. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P. W. Shor // SIAM Journal on Computing. – 1997. – Vol. 26, Iss. 5. – P. 1484-1509. DOI: 10.1137/S0097539795293172.

9. Proos J. Shor's discrete logarithm quantum algorithm for elliptic curves [Electronic resource] / J. Proos, C. Zalka. – University of Waterloo, 2004. – 34 p. – Access mode: https://arxiv.org/pdf/quant-ph/0301141v2.pdf. – 12.02.2021.

10. Kolmogorov, A. N. Elements of the Theory of Functions and Functional Analysis Kindle Edition [Electronic resource] / A. N. Kolmogorov, S. V. Fomin. – 2020. – 128 p. – Access mode: https://www.amazon.com/Elements-Theory-Functions-Functional-Analysis-ebook/dp/B08CDF9FTM. – 12.02.2021.

11. Avramenko, V. V. Cryptosystem based on a key function of a real variable [Electronic resource] / V. V. Avramenko, V. M. Demianenko // CEUR Workshop Proceedings (CMIS 2020). – Access mode: http://ceur-ws.org/Vol-2608/paper51.pdf. – 12.02.2021.

12. Авраменко, В. В. Характерные непропорциональности числовых функций и их применение при решении задач диагностики [Електронний ресурс] / В. В. Авраменко // Вісник Сумського державного університету. Серія : Технічні науки. – 2000. – № 16. – С. 12-20. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/1824/1/5201C993d01.pdf. – 12.04.20211.

13. Carlet, Claude. Boolean Functions for Cryptography and Error Correcting Codes [Electronic resource] / Claude Carlet. – Access mode: https://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf. – 12.02.2021.

14. Advanced encryption standard (AES) : Federal Information Processing Standards Publication 197 [Text]. – Effective from 2002-05-26. – Gaithersburg : FIPS PUBS, 2001. – 47 p. DOI: 10.6028/NIST.FIPS.197.

15. Hankerson, D. R. Guide to elliptic curve cryptography [Text] / D. R. Hankerson, A. J. Menezes, S. A. Vanstone. – New York : Springer, 2003. – 311 p. ISBN 978-0-387-21846-5.

16. ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм *криптографічного перетворення (ГОСТ 28147-89). – Введ. 2009-02-01. – К. : Державний Стандарт України, 2009. – 28 р.*

17. *Rivest, R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21, Issue 2. – P. 120-126. DOI:10.1145/359340.359342.*

18. *Kessler, Gary C. An Overview of Cryptography [Electronic resource] / Gary C. Kessler. – Access mode: https://www.garykessler.net/library/crypto.html. – 02.04.2021.*

19. *Bagwe, G. R. Voice encryption and decryption in telecommunication [Text] / G. R. Bagwe, D. S. Apsingekar, S. Gandhare, S. Pawar // 2016 International Conference on Communication and Signal Processing (ICCSP), 2016. – P. 1790-1793, DOI: 10.1109/ICCSP.2016.7754475.*

20. *Lee, B. Gi. Fundamentals of Scrambling Techniques [Text] / B. Gi Lee, S. C. Kim // Scrambling Techniques for Digital Transmission / Telecommunication Networks and Computer Systems. – London : Springer, 1994. – P. 13-24. DOI: 10.1007/978-1-4471-3231-8_2*

21. *Vedantam, Sh. Sh. Enhanced Scrambled Prime Key Encryption Using Chaos Theory and Steganography [Text] / Shanmukha Shreyas Vedantam, Kushalnath Devaruppala, Ravi Shankar Nanduri // Intelligent Data Communication Technologies and Internet of Things. – January 2020. DOI: 10.1007/978-3-030-34080-3_12.*

22. *Карпенко А. П. Интегральные характеристики непропорциональности числовых функций и их применение в диагностике [Електронний ресурс] / А. П. Карпенко // Вісник Сумського державного університету. Серія : Технічні науки. – 2000. – № 16. – С. 20-25. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/10931/1/4_Karpenko.pdf. – 12.04.2021.*

References (BSI)

1. Shelechov, I. V., Barchenko, N. L., Kalchenko, V. V., Obodiak, V. K. A Hierarchical Fuzzy Quality Assessment of Complex Security Information Systems. *Radioelectronic and computer systems*, 2020, vol. 4, pp. 106-115. DOI: 10.32620/reks.2020.4.10.

2. Smart, N. *Cryptography: An Introduction*, 3rd ed., University of Bristol, 2014. 424 p. Available at: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf. (accessed 12.02.2021).

3. Ferguson, N., Schneier, B., Kohno, T. *Cryptography Engineering: Design Principles and Practical Applications*. New York, John Wiley & Sons Publ., 2010. 353 p. DOI: 10.1002/9781118722367.

4. Boneh, D., Shoup, V. A *Graduate Course in Applied Cryptography. Version 0.5*. Available at: https://toc.cryptobook.us/book.pdf. (accessed 12.02.2021).

5. Klyucharev, P. G. Kvantovyi komp'yuter i kriptograficheskaya stoikost' sovremennykh sistem shifrovaniya [Quantum computer and cryptographic strength of modern encryption systems]. *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N. E. Baumana. Seriya «Estestvennye nauki» – Bulletin of the Moscow State Technical University. N. E. Bauman. Series "Natural Sciences"*, 2007, no. 2, pp. 113-120.

6. Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O'Brien, J. L. *Quantum Computing*. Nature, 2010, vol. 464, pp. 45-53. DOI: 10.1038/nature08812.

7. Grover, L. K. Quantum Mechanics Help in Searching for a Needle in a Haystack. *Phys. Rev. Lett.*, 1997, vol. 79, pp. 325-328. DOI: 10.1103/PhysRevLett.79.325.

8. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 1997, vol. 26, iss. 5, pp. 1484-1509. DOI: 10.1137/S0097539795293172.

9. Proos, J. A., Zalka, C. *Shor's discrete logarithm quantum algorithm for elliptic curves.* University of Waterloo, 2004. 34 p. Available at: https://arxiv.org/pdf/quant-ph/0301141v2.pdf. (accessed 12.02.2021).

10. Kolmogorov, A. N., Fomin, S. V. *Elements of the Theory of Functions and Functional Analysis Kindle Edition*. 2020. 128 p. Available at: https://www.amazon.com/Elements-Theory-Functions-Functional-Analysis-ebook/dp/B08CDF9FTM. (accessed 12.02.2021).

11. Avramenko, V. V., Demianenko, V. M. Cryptosystem based on a key function of a real variable. *CEUR Workshop Proceedings (CMIS 2020).* Available at: http://ceur-ws.org/Vol-2608/paper51.pdf. (accessed 12.02.2021).

12. Avramenko, V. V. Kharakternye neproportsional'nosti chislovykh funktsii i ikh primenenie pri reshenii zadach diagnostiki [Characteristic disproportions of numerical functions and their application in solving diagnostic problems]. *Visnyk Sums'koho derzhavnoho universytetu. Seriya : Tekhnichni nauky – Visnik of the Sumy State University. Series: Technical Sciences*, 2000, vol. 16, pp. 12-20. Available at: https://essuir.sumdu.edu.ua/bitstream-download/123456789/1824/1/5201C993d01.pdf. (accessed 12.02.2021).

13. Carlet, Claude. *Boolean Functions for Cryptography and Error Correcting Codes*. Available at: https://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf. (accessed 12.02.2021).

14. *Advanced encryption standard (AES) : Federal Information Processing Standards Publication 197*. Effective from 2002-05-26, Gaithersburg, FIPS PUBS, 2001. 47 p. DOI: 10.6028/NIST.FIPS.197.

15. Hankerson, D. R. Menezes, A. J., Vanstone, S. A. *Guide to elliptic curve cryptography*. New York, Springer Publ., 2003. 311 p. ISBN 978-0-387-21846-5.

16. *DSTU HOST 28147:2009 Systema obrobky informatsiyi. Zakhyst kryptohrafichnyy. Alhorytm kryp-*

tohrafichnoho peretvorennya (HOST 28147-89) [DSTU GOST 28147: 2009 Information processing system. Cryptographic protection. Cryptographic transformation algorithm (GOST 28147-89)]. Enter. 2009-02-01, Kyiv, State Standard of Ukraine, 2009. 28 p.

17. Rivest, R. L. Shamir, A., Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, issue 2, pp. 120-126. DOI:10.1145/359340.359342.

18. Kessler, Gary C. *An Overview of Cryptography*. Available at: https://www.garykessler.net/library/crypto.html. (accessed 2.04.2021).

19. Bagwe, G. R., Apsingekar, D. S., Gandhare, S., Pawar, S. Voice encryption and decryption in telecommunication. *2016 International Conference on Communication and Signal Processing (ICCSP)*, 2016, pp. 1790-1793. DOI: 10.1109/ICCSP.2016.7754475.

20. Lee, B. Gi., Kim, S. C. Fundamentals of Scrambling Techniques. *Scrambling Techniques for Digital Transmission. Telecommunication Networks and Computer Systems*. London, Springer Publ., 1994, pp. 13-24. DOI: 10.1007/978-1-4471-3231-8_2.

21. Vedantam, Shanmukha Shreyas., Devaruppala, Kushalnath., Nanduri, Ravi Shankar. Enhanced Scrambled Prime Key Encryption Using Chaos Theory and Steganography. *In book: Intelligent Data Communication Technologies and Internet of Things*. January 2020, DOI: 10.1007/978-3-030-34080-3_12.

22. Karpenko, A. P. Integral'nye kharakteristiki neproportsional'nosti chislovykh funktsii i ikh primenenie v diagnostike [Integral characteristics of the disproportionality of numerical functions and their application in diagnostics]. *Visnyk Sums'koho derzhavnoho universytetu. Seriya : Tekhnichni nauky – Visnik of the Sumy State University. Series: Technical Sciences*, 2000, no. 16, pp. 20-25. Available at: https://essuir.sumdu.edu.ua/bitstream-download/123456789/10931/1/4_Karpenko.pdf. (accessed 12.04.2021).

Надійшла до редакції 30.04.2021, розглянута на редколегії 20.05.2021

ПОСЛІДОВНЕ ШИФРУВАННЯ З ВИКОРИСТАННЯМ ФУНКЦІЙ ДІЙСНОЇ ЗМІННОЇ

В. В. Авраменко, В. М. Дем’яненко

Актуальність. Використання функцій дійсної змінної в криптосистемах як ключів дозволяє збільшити їх криптографічну силу, оскільки вибір таких ключів складніший. Тому розробка таких систем є актуальною. Криптосистеми з симетричними ключами пропонуються для шифрування та дешифрування послідовності символів, представлених у вигляді одновимірного масиву числових значень ASCII кодів. Ці ключі є функціями дійсної змінної, що задовольняє певним обмеженням. Вони можуть бути як безперервними, так і дискретними. **Метод.** Пропонуються два варіанти криптосистеми. У першому варіанті передавальна і приймаюча сторони вибирають дві функції, перший переданий символ, область визначення функції, а також етап зміни аргументу функції. Дискретні повідомлення шифруються шляхом обчислення інтегральної непропорційності першого порядку зашифровуваного масиву за допомогою однієї з функцій. Відповідне значення другої функції для скремблювання додається до отриманого шифру кожного із символів, щоб ускладнити аналіз перехопленого повідомлення. На приймаючій стороні віднімається друга функція і розшифрування виконується шляхом зворотного перетворення формули інтегральної диспропорції. У другій версії послідовне шифрування виконується, коли шифр, отриманий з використанням однієї з ключових функцій на першому етапі, знову зашифровується шляхом обчислення диспропорції за допомогою другої функції, ключа. Відповідно, на двох етапах відбувається дешифрування. **Результати.** Представлені приклади шифрування та дешифрування послідовності текстових символів. Показано, що один і той же символ кодується по-різному залежно від його позиції в повідомленні. Наведені приклади, які показують складність вибору параметрів ключових функцій та криптографічну силу запропонованої криптосистеми. **Висновки.** Запропоновано варіанти криптосистеми, що використовують інтегральну функцію непропорційності першого порядку, в якій функції дійсної змінної служать ключами. Для того, щоб “зламати” таку систему, необхідно вибрати вид кожної функції, а також знайти значення її параметрів з дуже високою точністю. Система має високу криптографічну міцність.

Ключові слова: криптосистеми; функції непропорційності; інтегральна функція непропорційності першого порядку; функції дійсних змінних; ключова функція; шифрування; дешифрування; текстові повідомлення; скремблірування.

ПОСЛЕДОВАТЕЛЬНОЕ ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИЙ ДЕЙСТВИТЕЛЬНОЙ ПЕРЕМЕННОЙ

В. В. Авраменко, В. Н. Демьяненко

Актуальность. Использование функций действительной переменной в криптосистемах в качестве ключей позволяет повысить их криптографическую стойкость, поскольку такие ключи труднее выбрать. Поэтому разработка таких систем актуальна. Предлагаются криптосистемы с симметричными ключами для шифрования и дешифрования последовательности символов, представленных в виде одномерного массива числовых значений ASCII кодов. Эти ключи являются функциями действительной переменной, которые удовлетворяют определенным ограничениям. Они могут быть как непрерывными, так и дискретными. **Метод.** Предлагаются два варианта криптосистемы. В первом варианте передающая и принимающая стороны выбирают две функции, первый передаваемый символ, область определения функции, а также шаг изменения аргумента функции. Дискретные сообщения шифруются путем вычисления интегральной непропорциональности первого порядка шифруемого массива с помощью одной из функций. Соответствующее значение второй функции для скремблирования добавляется к полученному шифру каждого из символов, чтобы усложнить анализ перехваченного сообщения. На приемной стороне вторая функция вычитается, и расшифровка производится путем обратного преобразования формулы интегральной непропорциональности. Во второй версии последовательное шифрование выполняется, когда шифр, полученный с использованием одной из ключевых функций на первом этапе, снова зашифровывается путем вычисления диспропорции с использованием второй функции, ключа. Соответственно, расшифровка выполняется в два этапа. **Результаты.** Приведены примеры шифрования и дешифрования последовательности текстовых символов. Показано, что один и тот же символ кодируется по-разному в зависимости от его положения в сообщении. Приведены примеры, показывающие сложность выбора параметров ключевых функций и криптостойкость предлагаемой криптосистемы. **Выводы.** Предложены варианты криптосистемы с использованием функции интегральной непропорциональности первого порядка, в которых функции действительных переменной служат ключами. Чтобы «взломать» такую систему, необходимо выбрать вид каждой функции, а также найти значения ее параметров с очень высокой точностью. Система обладает высокой криптографической стойкостью.

Ключевые слова: криптосистемы; функции непропорциональности; интегральная функция непропорциональности первого порядка; функции действительных переменных; ключевая функция; шифрование; дешифрование; текстовые сообщения; скремблирование.

Авраменко Віктор Васильович – канд. техн. наук, доцент, доцент кафедри комп’ютерних наук, Сумський державний університет, Суми, Україна.

Дем’яненко Володимир Миколайович – аспірант кафедри комп’ютерних наук, Сумський державний університет, Суми, Україна.

Viktor Avramenko – PhD, Associate Professor, Associate Professor of Computer Science Department, Sumy State University, Sumy, Ukraine,
e-mail: avramenko1938@gmail.com, ORCID: 0000-0002-6317-6711.

Volodymyr Demianenko – PhD student of Computer Science Department, Sumy State University, Sumy, Ukraine,
e-mail: vldemyan@gmail.com, ORCID: 0000-0002-1512-970X.