AN ANALOGUE OF THE EL GAMAL SCHEME BASED ON THE MARKOVSKI ALGORITHM

CZU: 004.421.056.55

Nadeghda MALYUTINA

Doctoral School of Physical, Mathematical, Information and Engineering Sciences, Moldova State University

Today, different points of view on the same mathematical idea lead to different generalizations. We considered in our work an analogue of the El Gamal encryption system based on the Markovski algorithm [1; 2].

Keywords: *quasigroup, El Gamal's scheme, Markovski algorithm, encryption, decryption.*

Usually the classical Taher El Gamal encryption system is formulated in the language of number theory using multiplication modulo of a prime number [3]. The scheme was proposed by Taher El Gamal in 1985 [4, 5].

The sender of messages and their recipient can be individuals, organizations, or technical systems. These may be subscribers of a network, users of a computer system, or abstract "parties" involved in information interaction. But more often participants are identified with people and replaced with the formal designations *A* and *B* by Alice and Bob.

It is assumed that messages are transmitted through the so-called "open" communication channel, available for listening to some other persons. In cryptography, it is usually assumed that a person sending messages or receiving them has some opponent *E* and this opponent can intercept messages transmitted over an open channel. The adversary is considered as a certain person named Eve, who has at her disposal powerful computing equipment and owns cryptanalysis methods. Naturally, Alice and Bob want their messages to be incomprehensible to Eve, and use special ciphers for this.

Before sending a message over an open communication channel from *A* to *B, A* encrypts the message, and *B,* having received the encrypted message, decrypts it, restoring the original text. In cryptography, it is generally accepted that the adversary can know the encryption algorithm used, the nature of the transmitted messages and the intercepted ciphertext, but does not know the secret key.

Developers of modern cryptosystems strive to make attacks on known and selected text invulnerable. Significant successes have been achieved along this path.

El Gamal's scheme

Suppose there are subscribers *A* and *B* want to transmit encrypted messages to each other without having any secure communication channels. We will consider the code proposed by El-Gamal, which solves this problem, using only one message forwarding.

Keys are generated first:

1) A random prime number p is chosen.

2) An integer g is chosen - the antiderivative root p.

3) Then each subscriber selects his secret number c_i, $1 < c_i < p-1$, where the numbers c_i and $p-1$ are coprime.

4) Each subscriber computes the corresponding public key d_i:

$$d_i = g^{c_i} (mod\ p) \quad (1)$$

The public keys are d_i, and the private keys are the numbers c_i.

We show now how A sends message m to the subscriber B. We will assume, that the message is presented as a number $m < p$.

Encryption. *A* forms a random number k (session key), $1 \le k \le p-2$, moreover, k and $(p-1)$ are coprime. The numbers are calculated:

$$r = g^k (mod\ p) \quad (2)$$

$$e = m \cdot d_B^k (mod\ p) \quad (3)$$

and a pair of numbers (r, e) is transmitted to the subscriber B.

Decryption. B, receiving (r, e) and knowing the private key c_B calculates:

$$m' = e \cdot r^{p-1-c_B} (mod\ p) \quad (4)$$

Statement 1 (properties of the El Gamal cipher).

1) The subscriber B received a message, i.e. $m' = m$;

2) The adversary, knowing p, g, d_B, r and e, cannot calculate m.

Example 1. Consider the transmission of message $m = 218$ from A to B.

Take a random prime number $p = 293$.

Choose an integer number $g = 2$ − is the smallest primitive root of number 293.

Subscribers then select their secret keys. Let subscriber A chooses a secret number $c_A = 15$ and subscriber B chooses for himself a secret number $c_B = 21$.

Each subscriber computes the corresponding public key using (1):

$$d_A \equiv 2^{15} (mod\ 293) = 245,\ d_B \equiv 2^{21} (mod\ 293) = 151.$$

Encryption. Subscriber *A* randomly chooses the number $k = 49$ and calculates using (2) and (3):

$$r \equiv 2^{49} (mod\ 293) = 248,\ e \equiv 218 \cdot 151^{49} (mod\ 293) = 224.$$

Now □ sends an encrypted message as a pair of numbers $(248, 224)$.

Decryption. □ gets the pair $(248,224)$ and calculates:

$$m' \equiv 224 \cdot 248^{293-1-21} (mod\ 293) \equiv 224 \cdot 103 (mod\ 293) = 218.$$

So B was able to decrypt the transmitted message $218.$

By a similar scheme, all subscribers in the network can send messages. Moreover, any subscriber who knows the public key of subscriber B can send him messages encrypted using the public key d_B. But only subscriber B, and no one else, can decrypt these messages using the secret key c_B.

An analogue of the El Gamal scheme based on the Markovski algorithm

We give an analogue of the El Gamal encryption system based on the Markovski algorithm [4; 5].

Let (Q, f) be a binary quasigroup and $T = (\alpha, \beta, \gamma)$ be its isotopy. Alice's keys are as follows:

The public key: $(Q, f), T, T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k),\ m, n, k \in \mathbb{N}$, and the Markovski algorithm.

The private key m, n, k.

Encryption. To send a message $b \in (Q, f)$, Bob is calculates $T^{(r,s,t)}, T^{(mr,ns,kt)}$ for the random $r, s, t \in \mathbb{N}$ and $(T^{(mr,ns,kt)}(Q, f))$. The ciphertext: $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$. To obtain $(T^{(mr,ns,kt)}(Q, f)b)$, Bob uses the Markovski algorithm which is known to Alice.

Decryption. Alice knows m, n, k, so if she gets the ciphertext $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$, she will calculate $(T^{(mr,ns,kt)}(Q, f))^{-1}$ using $T^{(r,s,t)}$ and finally she will calculate b.

Example 2. Let (Q, f) be a binary quasigroup defined by the following Cayley table:

Table 1

·	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	5	2	6	4	0	3	1
1	1	6	5	3	4	2	0
2	0	5	4	6	3	1	2
3	4	1	3	0	2	6	5
4	2	4	0	1	6	5	3
5	6	3	1	2	5	0	4
6	3	0	2	5	1	4	6

and $T = (\alpha, \beta, \gamma)$ its isotopy, where:

$\alpha = (2\,3\,4)\,(0\,5\,1\,6)$; $\beta = (0\,3\,2\,1)\,(5\,6)$;

$\gamma = (1\,2\,3\,6\,0\,5\,4)$.

And for γ we have the inverse γ^{-1} the following kind: $\gamma^{-1} = (6\,4\,1\,2\,5\,0\,3)$.

As a result, we get the following Cayley tables:

Table 2

α $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	6	3	1	2	5	0	4
1	3	0	2	5	1	4	6
2	4	1	3	0	2	6	5
3	2	4	0	1	6	5	3
4	0	5	4	6	3	1	2
5	1	6	5	3	4	2	0
6	5	2	6	4	0	3	1

Table 3

β $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	2	6	3	1	5	4	0
1	5	3	0	2	1	6	4
2	0	4	1	3	2	5	6
3	1	2	4	0	6	3	5
4	6	0	5	4	3	2	1
5	3	1	6	5	4	0	2
6	4	5	2	6	0	1	3

Table 4

γ^{-1} $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	5	0	6	3	2	1	4
1	2	5	4	6	0	3	1
2	6	3	1	2	5	4	0
3	3	2	5	1	4	0	6
4	1	4	3	0	6	2	5
5	4	1	0	5	3	6	2
6	0	6	2	4	1	5	3

Then Alice's keys are as follows:

The private key: $m = 3$, $n = 6, k = 5$.

The public key is $(Q, f), T, T^{(3,6,5)} = (\alpha^3, \beta^6, \gamma^5)$ and the Markovski algorithm, where:

$\alpha^3 = (0\,6\,1\,5)$; $\beta^6 = (0\,2)\,(1\,3)$; $\gamma^5 = (0\,3\,1\,5\,6\,2\,4)$, $(\gamma^5)^{-1} = (0\,4\,2\,6\,5\,1\,3)$.

As a result, we get the following Cayley tables:

Table 5

α^3 $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	3	0	2	5	1	4	6
1	6	3	1	2	5	0	4
2	0	5	4	6	3	1	2
3	4	1	3	0	2	6	5
4	2	4	0	1	6	5	3
5	5	2	6	4	0	3	1
6	1	6	5	3	4	2	0

Table 6

β^6 $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	2	5	3	0	1	4	6
1	1	2	6	3	5	0	4
2	4	6	0	5	3	1	2
3	3	0	4	1	2	6	5
4	0	1	2	4	6	5	3
5	6	4	5	2	0	3	1
6	5	3	1	6	4	2	0

Table 7

$(\gamma^5)^{-1}$ $(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	6	1	0	4	3	2	5
1	3	6	5	0	1	4	2
2	2	5	4	1	0	3	6
3	0	4	2	3	6	5	1
4	4	3	6	2	5	1	0
5	5	2	1	6	4	0	3
6	1	0	3	5	2	6	4

Encryption. To send a message $b = 630512403$, Bob computes from the known $T = (\alpha, \beta, \gamma)$:

$T^{(r,s,t)}$ for random $r = 5, s = 3, t = 6$, i.e. $T^{(5,3,6)}$:

$\alpha^5 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 5\,6\,4\,2\,3\,1\,0 \end{pmatrix}$; $\beta^3 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 1\,2\,3\,0\,4\,6\,5 \end{pmatrix}$; $\gamma^6 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 6\,4\,1\,2\,5\,0\,3 \end{pmatrix}$.

Then he calculates $T^{(mr,ns,kt)}$ using the public key $T^{(m,n,k)}$:

$\alpha^{5m} = \alpha^5 = (0\,6\,1\,5)$; $\beta^{3n} = \beta^3 = (0\,2)\,(1\,3)$; $\gamma^{6k} = (0\,4\,2\,6\,5\,1\,3)$, $(\gamma^{6k})^{-1} = (0\,3\,1\,5\,6\,2\,4)$.

As a result of the application of the new isotopy $T^{(5m,3n,6k)}$ to the quasigroup (Q, f) we obtain:

Table 8

$\alpha^{5m}(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	3	0	2	5	1	4	6
1	6	3	1	2	5	0	4
2	0	5	4	6	3	1	2
3	4	1	3	0	2	6	5
4	2	4	0	1	6	5	3
5	5	2	6	4	0	3	1
6	1	6	5	3	4	2	0

Table 9

$\beta^{3n}(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	2	5	3	0	1	4	6
1	1	2	6	3	5	0	4
2	4	6	0	5	3	1	2
3	3	0	4	1	2	6	5
4	0	1	2	4	6	5	3
5	6	4	5	2	0	3	1
6	5	3	1	6	4	2	0

Table 10

$(\gamma^{6k})^{-1}(\cdot)$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	4	6	1	3	5	0	2
1	5	4	2	1	6	3	0
2	0	2	3	6	1	5	4
3	1	3	0	5	4	2	6
4	3	5	4	0	2	6	1
5	2	0	6	4	3	1	5
6	6	1	5	2	0	4	3

To obtain $(T^{(mr,ns,kt)}(Q, f)b$, Bob uses the Markovski algorithm known to Alice, with the known leader value $l = 3$, then the ciphertext for $b = 630512403$ will look like:

$v_1 = 3 \circ 6 = 6$; $v_2 = 6 \circ 3 = 2$; $v_3 = 2 \circ 0 = 0$; $v_4 = 0 \circ 5 = 0$; $v_5 = 0 \circ 1 = 6$, $v_6 = 6 \circ 2 = 5$; $v_7 = 5 \circ 4 = 3$; $v_8 = 3 \circ 0 = 1$; $v_9 = 1 \circ 3 = 1$.

Bob gets: $b' = 620065311$.

Decryption. Alice knows $m = 3, n = 6, k = 5$, so if she gets an isotopy $T^{(r,s,t)}$ and ciphertext $b' = 620065311$, she will calculate the isotopy first $T^{(mr,ns,kt)}$ using $T^{(r,s,t)}$:

$$(\alpha^{**})^3 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 6\,5\,2\,3\,4\,0\,1 \end{pmatrix};$$

$$(\beta^{**})^6 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 2\,3\,0\,1\,4\,5\,6 \end{pmatrix};\ (\gamma^{**})^5 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6 \\ 4\,3\,6\,0\,2\,1\,5 \end{pmatrix}$$

As a result, it receives the same table(table 10) as Bob received in the encryption process.

For the table $(\gamma^{6k})^{-1}$ Alice builds a parastrophe (23) used in the Markovski algorithm for decryption:

Table 11

\	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	5	2	6	3	0	4	1
1	6	3	2	5	1	0	4
2	0	4	1	2	6	5	3
3	2	0	5	1	4	3	6
4	3	6	4	0	2	1	5
5	1	5	0	4	3	6	2
6	4	1	3	6	5	2	0

and finally, using this table, she calculates b:

$u_1 = 3 \setminus 6 = 6;\ u_2 = 6 \setminus 2 = 3;\ u_3 = 2 \setminus 0 = 0;\ u_4 = 0 \setminus 0 = 5;\ u_5 = 0 \setminus 6 = 1;$
$u_6 = 6 \setminus 5 = 2;\ u_7 = 5 \setminus 3 = 4;\ u_8 = 3 \setminus 1 = 0;\ u_9 = 1 \setminus 1 = 3.$

In this algorithm, isostrophy [6] can also be used instead of isotopy, the modified algorithm instead of the Markovski algorithm and n-ary ($n > 2$) quasigroups [7; 8] instead of binary quasigroups. A generalization of the Diffie-Hellman public key distribution scheme is given in [9]. The generalization is based on the concepts of the left and right degrees of the elements of some non-associative groupoids. For medial quasigroups, this approach was implemented in [10]. Generalizations of the El-Gamal scheme to Moufang loops are given in [10]. In [11], the discrete logarithmic problem on Moufang loops reduces to the same problem over finite simple fields. Another generalization of the El-Gamal scheme based on quasi-automorphisms of quasigroups is presented in [10].

Conclusion. Today, different points of view on the same mathematical idea lead to different generalizations. We considered in our work an analogue of the El Gamal encryption system based on the Markovski algorithm. This algorithm is under improvement and other modifications are planned.

References:

1. MOLDOVYAN, N.A., SHCHERBACOV, A.V. AND SHCHERBACOV, V.A. On some applications of quasigroups in cryptology. In: *Workshop on Foundations of Informatics*, August 24-29, 2015, Chisinau, Proceedings, pp.331-341.
2. SHCHERBACOV, V.A. *On generalisation of Markovski cryptoalgorithm*. In: *Workshop on General Algebra*, February 26-March 1, 2015, Technische Universitat at Dresden, Technical Report, Technische Universitat at Dresden, Dresden, 36-37, 2015.
3. El GAMAL, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: *IEEE Transactions on Information Theory*, 31(4): pp.469-472, 1985.
4. RYABKO, B.Ya., FIONOV, A.N. *Cryptographic methods of information protection: a training manual*. M. Hotline-Telecom, 2005, pp. 12-34. ISBN 5-89176-233-1.
5. Wikipedia. *Elgamal encryption*, 2014. http:// en.wikipedia.org/wiki/ El Gamal_encryption.
6. SHCHERBACOV, V.A. *On the structure of left and right F-, SM- and E-quasigroups*. J. Gen. Lie Theory Appl., 3(3): pp. 197-259, 2009.
7. BELOUSOV, V.D. *n-Ary Quasigroups*. Kishinev: Stiintsa, 1971 (in Russian).
8. SHCHERBACOV, V.A. *Quasigroups in cryptology*. Comput. Sci. J. Moldova, 17(2): pp. 193-228, 2009.
9. KATYSHEV, S.Yu., MARKOV, V.T., and NECHAEV, A.A. *Utilization of nonassociative groupoids for the realization of an open key-distribution procedure*. Diskret. Mat., 26: pp.45- 64, 2014 (in Russian).
10. GRIBOV, A.V. *Algebraic Non-Associative Structures and Its Applications in Cryptology*. PhD thesis, Moscov State University, 2015 (in Russian).
11. MAZE, G. *Algebraic Methods For Constructing One-Way Trapdoor Functions.* PhD thesis, University of Notre Dame, 2003.