Cryptanalysis of some stream ciphers

Nadeghda N. Malyutina

Abstract. We show that the Vojvoda attacks (attacks with selected plaintext and selected ciphertext) on Markovski cipher can be modified on generalized Markovski cipher based on left and right quasigroups. We give a comparative analysis, identifying positive and negative points in these attacks.

1. Introduction

Today, various cryptosystems based on quasigroups have appeared, which show that the use of quasigroups opens new ways in the construction of stream and block ciphers. For example, S. Markovski [1] (see also E. Ochodkova and V. Snashel [2]) proposed a new stream cipher to encrypt the file system. The cipher has a very large key space. M. Vojvoda has given a cryptoanalysis of the file encoding system based on quasigroups [5] and showed how to break this cipher.

Let $(Q,*)$ be a finite quasigroup. Individual plaintext characters $u_1, u_2, \ldots, u_k$ and ciphertext characters $v_1, v_2, \ldots, v_k$ are represented by the elements of Q, i.e., $u_i, v_i \in Q$, $1 \leqslant i \leqslant k$. The key of this cipher is the operation $*$ defined in the set Q and represented by its Caley table. The keyspace is enormously large.

The authors stated that such a cipher was resistant to any attack [2], although they only studied resistance against brute force attacks and performed some statistical tests on this cipher. From the point of view of cryptanalysis, a good cipher must be strong, at least against known attacks. The best approach is to match only the obvious pairs of elements, and then partially decrypt the encrypted text.

Basic concepts and definitions can be found in [4].

2. Chosen ciphertext attack on Markovski cipher

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext:

$$\begin{array}{c} q_1q_1q_1q_2q_1q_3\cdots q_1q_n \\ q_2q_1q_2q_2q_2q_3\cdots q_2q_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ q_nq_1q_nq_2q_nq_3\cdots q_nq_n \end{array}$$

and enter it into the decryption device.

2010 Mathematics Subject Classification: 20N05
Keywords: Quasigroups, left (right) quasigroups, cryptoatacks, cryptoanalysis.

The decryption device gives the following plaintext:

$$\begin{array}{l} l\backslash q_1 \quad q_1\backslash q_1 \quad q_1\backslash q_1 \quad q_1\backslash q_2 \quad q_2\backslash q_1 \quad q_1\backslash q_3 \dots q_1\backslash q_n \\ q_n\backslash q_2 \quad q_2\backslash q_1 \quad q_1\backslash q_2 \quad q_2\backslash q_2 \quad q_2\backslash q_2 \quad q_2\backslash q_3 \dots q_2\backslash q_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ q_n\backslash q_n \quad q_n\backslash q_1 \quad q_1\backslash q_n \quad q_n\backslash q_2 \quad q_2\backslash q_n \quad q_n\backslash q_3 \dots q_n\backslash q_n \end{array}$$

It is easy to see that the Caley table of the operation $\backslash$ defined on Q is completely found. The construction of the Caley table of the operation $*$ is straightforward.

The ciphertext used in the attack consists of $2n^2$ characters. Of course a shorter ciphertext can be constructed. The main requirement of M. Vojvoda is that all the pairs of adjacent elements will appear in the ciphertext.

Example 2.1. Let $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and let the quasigroup $(Q, \backslash)$ with which the decryption is performed have the following Cayley table:

\	0	1	2	3
0	2	0	3	1
1	3	1	0	2
2	1	3	2	0
3	0	2	1	3

Let $l \in Q$, $l = 2$. Enter the following text into the decryption device:

00010203
10111213
20212223
30313233

At the output we get: 12203311230110321133022030122103

Having broken the text into four blocks we will receive:

12203311
23011032
11330220
30122103

Thus, the rows of the table of quasigroups $(Q, \backslash)$ are displayed sequentially in even positions.

However, for a complete reconstruction of the Cayley table for the quasigroup $(Q, \backslash)$ it is enough to input only $2n^2 - 4n + 1 = 2n(n-2) + 1$ characters instead of $2n^2$ (in our example, only the first 17 characters will be used instead of 32 characters). Leader l is the solution to the equation: $l\backslash 0 = 1 \Rightarrow l = 2$. Knowing the table for a quasigroup $(Q, \backslash)$, the quasigroup encryption table is easily restored:

*	0	1	2	3
0	1	3	0	2
1	2	1	3	0
2	3	0	2	1
3	0	2	1	3

Thus, the ciphertext known to us is easily decrypted.

We suggest using a different text in the decryption procedure:

$$\begin{array}{l}
q_1q_1q_2q_2q_3q_3\cdots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n\\
q_2q_1q_3q_2q_4q_3\cdots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n\\
q_3q_1q_4q_2q_5q_3\cdots q_nq_{n-2}q_1q_{n-1}q_2q_n\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}$$

The decryption device provides the following plaintext at the output:

$$\begin{array}{cccc}
l\setminus q_1 & q_1\setminus q_1 & q_1\setminus q_2 & q_2\setminus q_2\cdots q_n\setminus q_n\\
q_n\setminus q_2 & q_2\setminus q_1 & q_1\setminus q_3 & q_3\setminus q_2\cdots q_1\setminus q_n\\
q_n\setminus q_3 & q_3\setminus q_1 & q_1\setminus q_4 & q_4\setminus q_2\cdots q_2\setminus q_n\\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots
\end{array}$$

The last symbol depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: $q_k\setminus q_n$, where $k=\left[\frac{n}{2}\right]+1$. If n is an even number, then the last operation will be: $q_{\frac{n}{2}}\setminus q_n$.

The Cayley table of the operation $\setminus$ defined on Q is completely located, after which it is easy to find the Cayley table of the operation $*$. The presented attack requires $n^2-2(n-1)$ operations $\setminus$. Compared to M. Vojvoda's attack, the number of characters used is reduced to $(n+1)^2-3$ characters, i.e., quite significantly. And this number does not depend on the leader.

Example 2.2. For our example, the following text is introduced into the decryption device:
00112233
10
At the output we get: 1201020323
So, instead of 32 characters, 10 characters will be used.

A cryptographic attack on a stream cipher uses the assumption that the cryptanalyst knows the statistics of the language in which the plaintext message is written.

3. Chosen plaintext attack on Markovski cipher

Suppose a cryptanalyst has access to an encryption device with an unknown key. In his PhD thesis [6], M. Vojvoda presented the following text for encryption:

$$\begin{array}{l}
q_1q_1;q_1q_2;q_1q_3;\ldots q_1q_n;\\
q_2q_1;q_2q_2;q_2q_3;\ldots q_2q_n;\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
q_nq_1;q_nq_2;q_nq_3;\ldots q_nq_n.
\end{array}$$

This text is entered into the encryption device discretely by two characters. Thanks to this input, we have the following ciphertext:

$$\begin{array}{l}
l*q_1\quad ((l*q_1)*q_1);l*q_1\quad ((l*q_1)*q_2);\ldots l*q_1\quad ((l*q_1)*q_n);\\
l*q_2\quad ((l*q_2)*q_1);l*q_2\quad ((l*q_2)*q_2);\ldots l*q_2\quad ((l*q_2)*q_n);\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
l*q_n\quad ((l*q_n)*q_1);l*q_n\quad ((l*q_n)*q_2);\ldots l*q_n\quad ((l*q_n)*q_n);
\end{array}$$

The Cayley table of the operation $*$ defined on Q is completely located. The presented attack requires $2n^2$ operations $*$. However, shorter encrypted text can be built.

Example 3.1. Let $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and let the quasigroup $(Q, *)$ with which the decryption is performed, have the following Cayley table:

$*$	0	1	2	3
0	1	3	0	2
1	2	1	3	0
2	3	0	2	1
3	0	2	1	3

Let $l \in Q$, $l = 2$.

Consider the plaintext attack. Enter the following text into the encryption device:

$$00; 01; 02; 03;$$
$$10; 11; 12; 13;$$
$$20; 21; 22; 23;$$
$$30; 31; 32; 33.$$

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

$$30; 32; 31, 33;$$
$$01; 03; 00; 02;$$
$$23; 20; 22; 21;$$
$$12; 11; 13; 10.$$

The Cayley table of the operation $*$ defined on Q is completely located. Then it is easy to find the Cayley table of the operation $\backslash$. The presented attack requires $2n^2$ operations $*$. The plaintext used in the attack consists of $2n^2$ characters divided into pairs.

However, a shorter encrypted text consisting of $2(n-1)^2$ characters can be constructed (in our example, 18 characters can be used instead of 32 characters). The output, that is line by line at an odd position, is the line number, and at an even position - is the element of the quasigroup $(Q, *)$. Unlike an attack with the selected ciphertext, in this attack the output of lines is not ordered.

Now consider the option when characters are launched into the encryption device by the stream, i.e., as in the case of an attack with the selected ciphertext:

$$q_1q_1q_1q_2q_1q_3 \dots q_1q_n$$
$$q_2q_1q_2q_2q_2q_3 \dots q_2q_n$$
$$\dots\dots\dots\dots\dots\dots\dots$$
$$q_nq_1q_nq_2q_nq_3 \dots q_nq_n$$

The encryption device provides the following ciphertext at the output:

$v_1 = l * q_1, v_2 = v_1 * q_1, v_3 = v_2 * q_1, v_4 = v_3 * q_2, v_5 = v_4 * q_1, v_6 = v_5 * q_3, \dots,$
$v_{2n} = v_{2n-1} * q_n,$
$v_{2n+1} = v_{2n} * q_2, \dots, v_{4n} = v_{4n-1} * q_n, \dots, v_{2n^2-2n} = v_{2n^2-2n-1} * q_n, \dots,$
$v_{2n^2} = v_{2n^2-1} * q_n.$

Example 3.2. For our example, simply type the following text into the encryption device:
00010203
10111213
At the output we have the following encrypted text: 3011223323203110

The Cayley table of the operation $*$ defined on Q is completely located. After that, it is easy to find the leader and the Cayley table of the operation $\backslash$. The presented attack requires 16 operations $*$, which is exactly half as much as in the attack proposed by M. Voivoda. In our example, instead of 32 characters, 16 characters are used. However, it should be noted that the number of symbols used depends on the value of the leader. In our example, $l = 2$, we get the same result for $l = 1$ and $l = 3$, but for $l = 0$, not 16 characters, but 21 characters are needed.

Consider another option for plaintext:
03020100
1312
At the output we have the following encrypted text: 330011232113

The presented attack requires operations $*$ less than in the attack proposed by M. Vojvoda, but everything depends on the chosen leader. In our example, instead of 32 characters, 12 characters are used.

Consider another option for plaintext:

$$\begin{array}{llllll} q_1q_1 & q_2q_2 & q_3q_3 \cdots q_{n-2}q_{n-2} & q_{n-1}q_{n-1} & q_nq_n \\ q_2q_1 & q_3q_2 & q_4q_3 \cdots q_{n-1}q_{n-2} & q_nq_{n-1} & q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3 \cdots q_nq_{n-2} & q_1q_{n-1} & q_2q_n \cdots \end{array}$$

The plaintext used in the attack consists of $2(n-1)^2$ characters divided into pairs. In this attack the output of lines is not ordered.

The encryption device provides the following ciphertext at the output:

$$\begin{aligned} & v_1 = l * q_1, v_2 = v_1 * q_1, \\ & v_3 = l * q_2, v_4 = v_3 * q_2, \\ & v_5 = l * q_3, v_6 = v_5 * q_3, \ldots, \\ & v_{2n-1} = l * q_n, v_{2n} = v_{2n-1} * q_n, \\ & v_{2(n-1)^2-1} = l * q_{n-1}, \ldots, v_{2(n-1)^2} = v_{2(n-1)^2-1} * q_1. \end{aligned}$$

Example 3.3. For our example, simply type the following text into the encryption device:

00	11	22	33
10	21	32	03
20			

At the output we have the following encrypted text:

30 03 22 10 01 20 13 33 23

In our example, instead of 32 characters, 18 characters are used. This result coincides with the result of reduced attack by M. Vojvoda.

Thus, even in the binary case, when carrying out attacks with a selected ciphertext or selected plaintext, the number of symbols used can be reduced.

4. Generalized Markovski cipher and left quasigroups

Example 4.1. Let the key left quasigroup with which the decryption is performed, have the following Cayley table:

$\backslash$	0	1	2	3
0	0	2	1	3
1	1	0	2	3
2	0	3	1	2
3	2	1	3	0

Here $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and $l = 3$.

Enter the following text into the decryption device:

00010203
10111213
20212223
30313233.

At the output we get: 20021103112002333013211202313320

Having broken the text into four blocks we will receive:

20021103 11200233 30132112 02313320

So, rows of the table of the left quasigroup $(Q, \backslash)$ are output sequentially in even positions.

However, for a complete reconstruction of the Cayley table for the left quasigroup $(Q, \backslash)$, it suffices to input only $2n^2 - 2n + 1 = n^2 + (n-1)^2$ characters at the input instead of $2n^2$ (in our example instead of 32 characters, only the first 25 characters will be used). The rest of the table is easily restored, taking into account the fact that the elements are not repeated in the lines of the left quasigroup. The leader l is a solution to the equation: $l \backslash 0 = 2 \Rightarrow l = 3$. In addition, knowing the table for a quasigroup $(Q, \backslash)$ easily restores the quasigroup table of encryption $(Q, *)$:

$*$	0	1	2	3
0	0	2	1	3
1	1	0	2	3
2	0	2	3	1
3	3	1	0	2

After that, the encrypted text known to us is easily decrypted.

If we run the following text on the decoder:

$$q_1q_1q_2q_2q_3q_3\dots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\dots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\dots q_nq_{n-2}q_1q_{n-1}q_2q_n\dots$$

the decryption device provides the following plaintext at the output:

$$l\backslash q_1 \quad q_1\backslash q_1 \quad q_1\backslash q_2 \quad q_2\backslash q_2\dots q_n\backslash q_n$$
$$q_n\backslash q_2 \quad q_2\backslash q_1 \quad q_1\backslash q_3 \quad q_3\backslash q_2\dots q_1\backslash q_n$$
$$q_n\backslash q_3 \quad q_3\backslash q_1 \quad q_1\backslash q_4 \quad q_4\backslash q_2\dots q_2\backslash q_n$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

The last symbol depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: $q_n \backslash q_k$, where $k = \left[\frac{n}{2}\right] + 1$. If n is an even number, then the last operation will be: $q_n \backslash q_{\frac{n}{2}+1}$.

The presented attack requires $n^2 - 2(n - 1 - \left[\frac{n}{2}\right])$. If n is an odd number, then the attack requires: $(n-1)^2 + 2\left[\frac{n}{2}\right] + 1$ operations, and if n is an even number, you will need: $n^2 - n + 2 = (n-1)^2 + n + 1$ operations \.

In comparison with the attack of M. Vojvoda, the number of used symbols is significantly reduced.

Example 4.2. For our previous example, we enter the following text into the decryption device:
00112233
102132
At the output we get: 00202120111333
So, instead of 32 characters, 14 characters will be used.

Consider the plaintext attack built in this one.

Enter the following text into the encryption device:

00	01	02	03
10	11	12	13
20	21	22	23
30	31	32	33

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

33	31	30	32
11	10	12	13
00	02	01	03
20	22	23	21

The output, that goes line by line at an odd position is the line number, and at an even position - is the element of the left quasigroup itself. The plaintext used in the attack consists of $2n^2$ characters divided into pairs. However, a shorter encrypted text consisting of $2n^2 - 2n$ characters can be constructed (in our example, the last pairs, the corresponding elements of the last column, can be omitted, which means that instead of 32 characters, you can use 24 characters). The line output is not ordered.

If we consider the attack with the following opentext:
00010203
10111213
20
at the output we have the following encrypted text: 333112031102231300.

In our example, instead of 32 characters, 18 is launched. Thus, in the binary case, when carrying out attacks with selected plaintext and selected ciphertext, the number of used characters can be reduced. But this result will change when choosing another leader and not always for the better. The question of the range of variation of the number of possible symbols used for the disclosure of a quasigroup remains open, as in the case of the usual quasigroup.

Now consider the option when characters are launched into an encryption device discretely, namely the following pairs:

$$\begin{array}{llllll} q_1q_1 & q_2q_2 & q_3q_3\cdots q_{n-2}q_{n-2} & q_{n-1}q_{n-1} & q_nq_n \\ q_2q_1 & q_3q_2 & q_4q_3\cdots q_{n-1}q_{n-2} & q_nq_{n-1} & q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\cdots q_nq_{n-2} & q_1q_{n-1} & q_2q_n\cdots \end{array}$$

Example 4.3. For our example, simply type the following text into the encryption device:

00 11 22 33
10 21 32 03
20 31 02 13

At the output we have the following encrypted text:

00 22 30 13 20 31 30 03 33 10 01 21

The Cayley table of the operation $*$ defined on Q is completely located. After that, it is easy to find the leader and the Cayley table of the operation $\backslash$. The presented attack requires operations $*$ less than in the attack proposed by M. Vojvoda, but everything depends on the chosen leader. The plaintext used in the attack consists of $2n^2 - 2n$ symbols divided into pairs. The output is not ordered.

In our example, instead of 32 characters, 24 characters are used. This result coincides with the result of a reduced attack by M. Vojvoda.

5. Generalized Markovski cipher and right quasigroups

Description of generalized Markovski cipher based on right quasigroups is given in [4]. Suppose that the key is right quasigroup, with which the decryption is performed, have the following Cayley table:

/	0	1	2	3	4
0	1	2	0	3	4
1	3	4	2	1	0
2	2	1	3	0	2
3	4	3	4	2	1
4	0	0	1	4	3

Here $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3, q_5 = 4\}$ and $l = 2$.

Enter the following text into the decryption device:

$$\begin{array}{lllll} q_1q_1 & q_2q_2 & q_3q_3\cdots q_nq_n & & \\ q_2q_1 & q_3q_2 & q_4q_3\cdots q_{n-1}q_{n-2} & q_nq_{n-1} & q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\cdots q_nq_{n-2} & q_1q_{n-1} & q_2q_n\cdots \end{array}$$

Example 5.1. For our example, simply type the following text into the encryption device:

0001020304
1011121314
2021222324
3031323334
4041424344.

At the output we get: 0113220430023441231020221334011341304224340002114З

Having broken the text into five blocks we will receive:

0113220430 0234412310 2022133401 1341304224 3400021143

So the columns of the table of the right quasigroup $(Q, /)$ are output sequentially in even positions. For a complete reconstruction of the Cayley table for the right quasigroup $(Q, /)$, as well as in the case of the left quasigroup, it suffices to input only $2n^2 - 2n + 1 = n^2 + (n-1)^2$ instead of $2n^2$ characters (in our example, instead of 50 characters, only 41 will be used). The leader l is a solution to the equation: $0/l = 0 \Rightarrow l = 2$. In addition, knowing the table for a quasigroup $(Q, /)$ easily restores the table of a quasigroup encryption $(Q, *)$:

$*$	0	1	2	3	4
0	4	4	0	2	1
1	0	2	2	1	3
2	2	0	1	3	2
3	1	3	2	0	4
4	3	1	3	4	0

If we run the following text on the decoder:

$$q_1q_1q_2q_2q_3q_3\dots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\dots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\dots q_nq_{n-2}q_1q_{n-1}q_2q_n\dots$$

the decryption device provides the following plaintext at the output:

$$q_1/l, \quad q_1/q_1, \quad q_2/q_1, \quad q_2/q_2, \dots q_n/q_n$$
$$q_2/q_n, \quad q_1/q_2, \dots q_n/q_1, \quad q_3/q_n, \quad q_1/q_3, \dots$$

The situation is the same as in the case of left quasigroups, i.e. the last character depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: q_k/q_n , where $k = \left[\frac{n}{2}\right] + 1$. If n is an even number, then the last operation will be: $q_{\frac{n}{2}+1}/q_n$ operations /.

Presented attack requires: $n^2 - 2(n - 1 - \left[\frac{n}{2}\right])$ operations /.

Example 5.2. For our previous example, we enter the following text into the decryption device:

0011223344
10213244304
2

At the output we get: 013413424302223011302

So, instead of 50 characters, 21 characters will be used and the result does not depend on the leaders used.

Consider the plaintext attack. Enter the following text into the encryption device:

00	01	02	03	04
10	11	12	13	14
20	21	22	23	24
30	31	32	33	34
40	41	42	43	44

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

04	00	02	01	03
41	43	42	44	40
14	12	10	13	11
20	24	21	22	23
32	31	33	30	34

The output goes column by column at an odd position, and the column number at an even position is the element of the right-hand quasigroup $(Q, *)$. After which it is easy to find the Cayley table of the operation $/$. The opentext used in the attack consists of $2n^2$ characters divided into pairs. However, a shorter encrypted text consisting of $2n^2 - 2n$ characters can be constructed (in our example, the last pairs, the corresponding elements of the last line, can be omitted, which means that instead of 50 characters, you can use 40 characters). Unlike the attack chosen by ciphertext, in this attack the output of the columns is not ordered.

If we consider the attack with the following opentext:

0001020304
1011121314
2021222324
3031323334
404142

at the output we have the following encrypted text:

0412020140043121224020242101030443022223411233.

The presented attack requires 46 elements to be processed in our example. But the result depends on the leader used.

Now consider the option when characters are launched into an encryption device discretely, namely the following pairs:

$$\begin{array}{llllll} q_1q_1 & q_2q_2 & q_3q_3\cdots q_nq_n & & \\ q_2q_1 & q_3q_2 & q_4q_3\cdots q_{n-1}q_{n-2} & q_nq_{n-1} & q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\cdots q_nq_{n-2} & q_1q_{n-1} & q_2q_n\cdots \end{array}$$

Example 5.3. For our example, simply type the following text into the encryption device:

00	11	22	33	44
10	21	32	43	04
20	31	42	03	14
30	41	02	13	24

At the output we have the following encrypted text:

00 43 10 22 34 41 14 21 30 03 14 24 33 01 40 20 31 02 44 11

The plaintext used in the attack consists of $2n^2-2n$ symbols divided into pairs. The output is not ordered.

In our example, instead of 50 characters, 40 characters are used. This result coincides with the result of a reduced attack by M. Vojvoda.

6. Conclusion

Thus, in the binary case, when carrying out attacks with selected plaintext and selected ciphertext, the number of symbols used can be reduced, even if it is insignificant.

The results are displayed in the following table:

The required number of characters used				
Order	Chosen ciphertext and plaintext attack M. Vojvoda	Chosen ciphertext attack M. Vojvoda (truncated)	Attack modified ciphertext	Chosen plaintext attack M. Vojvoda (truncated)
Quasigroups				
n	$2n^2$	$2n^2-4n+1$	$n^2-2(n-1)$	$2(n-1)^2$
n=128	32768	32257	16130	32258
n=256	131072	130049	65026	130050
n=512	524288	522241	261122	522242
n=1024	2097152	2093057	1046530	2093058
Left and right quasigroups				
n	$2n^2$	$2n^2-2n+1$	$n^2-2(n-1-\left[\frac{n}{2}\right])$	$2n^2-2n$
n=128	32768	32513	16258	32512
n=256	131072	130561	65282	130560
n=512	524288	523265	261634	523264
n=1024	2097152	2095105	1047554	2095104

Remark 6.1. We notice that

$$\lim_{n\to\infty}\frac{2n^2}{2n^2-4n+1}=1,$$

$$\lim_{n\to\infty}\frac{2n^2}{n^2-2n+2}=2.$$

Acknowledgement. The author thanks very much Referee for many valuable remarks including Remark 6.1.

References

[1] **S. Markovski, D. Gligoroski and S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. VIII Conf. Logic and Computer Science "LIRA'97", Novi Sad, 1997, 157 – 167.

[2] **E. Ochodkova and V. Snasel**, *Using quasigroups for secure encoding of file system*, Proc. Intern. Sci. NATO PfP/PWP Confer. "Security and Information Protection 2001", Brno, 2001, 175 – 181.

[3] **V.A. Shcherbacov**, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, 2017.

[4] **V.A. Shcherbacov and N.N. Malyutina**, *Role of quasigroups in cryptosystems. Generalization of Markovsky algorithm*, (Russian), Bull. Transnistrian Univ., **60(3)** (2018), 53 – 57.

[5] **M. Vojvoda**, *Cryptanalysis of a file encoding system based on quasigroup*, J. Electrical Engineering, **54** (2003), 69 – 71.

[6] **M. Vojvoda**, *Stream ciphers and hash functions – analysis of some new design approaches*, PHD thesis, Slovak University of Technology, 2004.

Received April 01, 2019

Department of Mathematics,
State University Dimitrie Cantemir,
Academiei str. 3/2, MD-2028 Chişinău,
Moldova

Email: 231003.Bab.Nadezhda@mail.ru