Combined Encryption Algorithm Using a Generalization of the Markovski Algorithm

Nadezhda Malyutina, Victor Shcherbacov

Abstract

This article is devoted to the construction of a generalization of a cryptographic algorithm based on the use of quasigroups of a special type. Here is a more detailed description of the algorithm proposed in [1]. An example is given to illustrate the operation of the developed algorithm. Our task was to show the effectiveness and advantages of using quasigroups of a special type in cryptology.

Keywords: T-quasigroup, encryption, decryption, Markovski algorithm, system of orthogonal operations, cryptosystem.

1 Introduction

This paper generalizes a cryptographic algorithm based on the use of quasigroups of a special form and provides an example illustrating the operation of this algorithm. This algorithm simultaneously uses two cryptographic procedures: encryption using a generalization of the Markovski algorithm [2] and encryption using a system of orthogonal operations. We present an implementation of this algorithm based on T-quasigroups, more precisely, based on medial quasigroups.

2 Basic concepts and definitions

The basic concepts, definitions, theorems and their consequences, as well as a detailed description of the algorithm and an example can be found in [3].

©2024 by Nadezhda Malyutina, Victor Shcherbacov

3 Combined encryption algorithm

Below we denote the action of the left (right, middle) translation to the power of a of a binary quasigroup (Q, g_1) on an element u_1 by the symbol ${}_{g_1}T^a_{l_1}(u_1)$. And so on. Here l_1 means the leader element. Note that the algorithm works for texts with even length.

Encryption. Initially, we have the plaintext $u_1, u_2, \ldots, u_{2n}$.

Step 1

$${}_{g_1}T^{a_{11}}_{l_1}(u_1) = v_1, {}_{g_2}T^{a_{12}}_{l_2}(u_2) = v_2, F_1^{a_{13}}(v_1, v_2) = (v_1^{'}, v_2^{'});$$

Step 2

$${}_{g_3}T^{a_{21}}_{v_1^{'}}(u_3) = v_3, {}_{g_4}T^{a_{22}}_{v_2^{'}}(u_4) = v_4, F_2^{a_{23}}(v_3, v_4) = (v_3^{'}, v_4^{'}); \cdots$$

Step N

$${}_{g_{2n-1}}T^{a_{n_1}}_{v_{2n-1}^{'}}(u_{2n-1}) = v_{2n-1}, {}_{g_{2n}}T^{a_{n_2}}_{v_{2n}^{'}}(u_{2n}) = v_{2n},$$

$$F_n^{a_{n_3}}(v_{2n-1}, v_{2n}) = (v_{2n-1}^{'}, v_{2n}^{'}).$$

We get the ciphertext $v_1^{'}, v_2^{'}, \ldots, v_{2n}^{'}$.

Thus, to encrypt a plaintext of length $2n$, we need $2n$ different operations on the quasigroups used in Combined encryption algorithm, n different values of the function F, 2 leader elements, and $3n$ different powers used in the translation algorithm.

Decryption. Let us have a ciphertext of the form $v_1^{'}, v_2^{'}, \ldots, v_{2n}^{'}$.

Step 1

$$F_1^{-a_{13}}(v_1^{'}, v_2^{'}) = (v_1, v_2), {}_{g_1}T^{-a_{11}}_{l_1}(v_1) = u_1, {}_{g_2}T^{-a_{12}}_{l_2}(v_2) = u_2;$$

Step 2

$$F_2^{-a_{23}}(v_3{}', v_4{}') = (v_3, v_4), {}_{g_3}T^{-a_{21}}_{v_1^{'}}(v_3) = u_3, {}_{g_4}T^{-a_{22}}_{v_2^{'}}(v_4) = u_4, \cdots$$

Step N

$$F_n^{-a_{n3}}(v'_{2n-1}, v'_{2n}) = (v_{2n-1}, v_{2n}), {}_{g_{2n-1}}T^{-a_{n1}}_{v'_{2n-1}}(v_{2n-1}) = u_{2n-1},$$

$${}_{g_{2n}}T^{-a_{n2}}_{v'_{2n}}(v_{2n}) = u_{2n}.$$

From Combined encryption algorithm we obtain the classical Markovski algorithm if we take only one quasigroup, one kind of quasigroup translation (left translations), each of which is taken to the first degree, and if the system of orthogonal operations (crypto procedures F) is not used. The Markovski algorithm is a special case of Combined encryption algorithm. The powers $a_{11}, a_{12}, \ldots, a_{n3}$ must be different to protect this algorithm from chosen plaintext and ciphertext attacks [4].

Additional information is required for the modifications proposed in this work [4, 5].

4 Example of Combined encryption algorithm

Consider the operation of Combined encryption algorithm based on T-quasigroups using a specific example.

Example *Take a cyclic group* $(Z_{1237}, +) = (A, +)$. *Initially, we have a plaintext* $u_1, u_2, u_3, u_4, u_5, u_6$ *of length* $k = 6$. *First, we define all the* T*-quasigroups we need:*

$$1.(A, g_1) = (A, *) : x * y = 513 \cdot x + 293 \cdot y + 115;$$

$$(A, *) \perp (A, \overset{(13)}{*}) : x \overset{(13)}{*} y = 938 \cdot x + 1017 \cdot y + 986.$$

$$2.(A, g_2) = (A, \circ) : x \circ y = 161 \cdot x + 1007 \cdot y + 509;$$

$$(A, \circ) \perp (A, \overset{(23)}{\circ}) : x \overset{(23)}{\circ} y = 1114 \cdot x + 1038 \cdot y + 1094.$$

$$3.(A, g_3) = (A, \star) : x \star y = 715 \cdot x + 201 \cdot y + 698;$$

$$(A, \star) \perp (A, \overset{(23)}{\star}) : x \overset{(23)}{\star} y = 298 \cdot x + 1157 \cdot y + 175.$$

$$4.(A, g_4) = (A, \Diamond) : x \Diamond y = 1111 \cdot x + 751 \cdot y + 263;$$

$$(A, \Diamond) \perp (A, \overset{(13)}{\Diamond}) : x \overset{(23)}{\Diamond} y = 1129 \cdot x + 703 \cdot y + 1190.$$

$$5.(A, g_5) = (A, \odot) : x \odot y = 451 \cdot x + 3 \cdot y + 511;$$

$$(A, \odot) \perp (A, \overset{(13)}{\odot}) : x \overset{(23)}{\odot} y = 96 \cdot x + 949 \cdot y + 424.$$

$$6.(A, g_6) = (A, \circledast) : x \circledast y = 941 \cdot x + 992 \cdot y + 189;$$

$$(A, \circledast) \perp (A, \overset{(23)}{\circledast}) : x \overset{(23)}{\circledast} y = 948 \cdot x + 722 \cdot y + 849.$$

We define 3 systems of two parastrophic orthogonal T-quasigroups:

$$1.F_1(x, y) = (123 \cdot x + 719 \cdot y + 839, 1125 \cdot x + 1077 \cdot y + 644),$$

$$F_1^{-1}(x, y) = (1210 \cdot x + 876 \cdot y + 315, 390 \cdot x + 848 \cdot y).$$

$$2.F_2(x, y) = (401 \cdot x + 711 \cdot y + 911, 671 \cdot x + 896 \cdot y + 164),$$

$$F_2^{-1}(x, y) = (858 \cdot x + 951 \cdot y + 44, 172 \cdot x + 1066 \cdot y).$$

$$3.F_3(x, y) = (1001 \cdot x + 19 \cdot y + 299, 152 \cdot x + 823 \cdot y + 321),$$

$$F_3^{-1}(x, y) = (858 \cdot x + 380 \cdot y, 566 \cdot x + 1009 \cdot y + 440).$$

Now we can use all the operations described above in Combined encryption algorithm.

Let us choose the elements as leaders: $l_1 = 599; l_2 = 1001$.

In the algorithm, we use the following values of the degrees: $a_{11} = 3; a_{12} = 1; a_{13} = 1; a_{21} = 2; a_{22} = 1; a_{23} = 2; a_{31} = 3; a_{32} = 1; a_{33} = 2$.

Encryption.

Let the plaintext look like: **101; 213; 405; 79; 615; 923.**

Step 1

$$v_1 = {}_{g_1}T^3_{599}(101) = 418, v_2 = {}_{g_2}T^1_{1001}(213) = 113,$$

$$(v_1^{'}, v_2^{'}) = F_1^2(418, 113) = (1141, 72),$$

Step 2

$$v_3 = {}_{g_3}T^2_{1141}(405) = 837, v_4 = {}_{g_4}T^1_{72}(79) = 1086,$$

$$(v_3^{'}, v_4^{'}) = F_2^2(837, 1086) = (511, 96),$$

Step 3

$$v_5 = {}_{g_5}T^3_{511}(615) = 1179, v_6 = {}_{g_6}T^1_{96}(923) = 460,$$

$$(v_5^{'}, v_6^{'}) = F_3^2(1179, 460) = (866, 751).$$

We get the following ciphertext: 1141; 72; 511; 96; 866; 751.

The decryption of the text is checked in a similar way.

A more detailed description of the algorithm and an example of encryption and decryption of text can be found in [4].

5 Conclusion

A program has been developed that uses a free version of the Pascal ABC programming language. The conducted experiments show that encoding/decoding is performed quite quickly. The program works for any values of leaders, powers, and any plaintext of length 6. It can be easily modified for text of any length and any used quasigroups and functions.

Combined encryption algorithm makes it possible to obtain an almost "natural" stream cipher, i.e., a stream cipher that encodes a pair of plaintext elements at any step. It is easy to see that Combined encryption algorithm can be generalized to the n-ary case.

Proper binary groupoids are preferable to linear quasigroups in terms of the construction of the map $F(x, y)$ for greater encryption security, but in this case, decryption may be slower than in the case of linear quasigroups, and the definition of these groupoids requires more memory. The same remark is valid for the choice of the function g. Perhaps the golden mean in this choice problem is the use of linear quasigroups over non-Abelian, especially simple, groups.

In this cipher, there is a possibility of protection against the standard statistical attack. For this area, more commonly used letters or

pairs of letters can be denoted by more than one integer or more than one pair of integers [4].

Acknowledgments. The Institutional Research Program of the Moldova State University for 2024–2027 years, subprogram 011303 has supported part of the research for this paper.

References

[1] V. A. Shcherbacov. *Elements of Quasigroup Theory and Applications.* – 1st ed: Chapman and Hall // CRC. – 2017, pp. 445–454.

[2] V. A. Shcherbacov and N. A. Moldovyan. *About one cryptoalgorithm.* In: Proceedings of the Third Conference of Mathematical Society of the Republic of Moldova dedicated to the 50th anniversary of the foundation of the Institute of Mathematics and Computer Science, August 19-23, 2014, Chisinau, Institute of Mathematics and Computer Science, pp. 158–161.

[3] Nadezhda Malyutina, Alexander Popov, and Victor Shcherbacov. *An encryption algorithm using a generalization of the Markovski algorithm and a system of orthogonal operations based on T-quasigroups.* arXiv:2407.14858v1 [cs.CR], 20 Jul 2024, pp. 14.

[4] N. A. Moldovyan, A. V. Shcherbacov, and V. A. Shcherbacov. *On some applications of quasigroups in cryptology.* In: Workshop on Foundations of Informatics, August 24–29, 2015, Chisinau, Proceedings, pp. 331–341.

[5] Victor A. Shcherbacov. *Quasigroup-based crypto-algorithms.* arXiv:1201.3016, 2012, pp. 23.

Nadezhda Malyutina[1], Victor Shcherbacov[2]

[1]Transnistrian State University
E–mail: 231003.Bab.Nadezhda@mail.ru
ORCID: https://orcid.org/0009-0002-1699-8699

[2]Moldova State University, Vladimir Andrunachievici Institute of Mathematics and Computer Science
E–mail: vscerb@gmail.com
ORCID: https://orcid.org/0000-0002-5319-5951