3TH INTERNATIONAL CONFERENCE ON COMBINATORICS, CRYPTOGRAPHY AND COMPUTATION
Iran University of Science &Technology

Multivariate Public Key Cryptosystems by Quasigroups and Matrices

Kh. Shahbazpour, M.soltani, H. Soltani

Department of Mathematical Science, Urmia University, Urmia,
Department of Eelectrical Engineering, Iran University of Science and Technology, Tehran
Iran

E-mail : kh.shahbazpoor@urmia.ac.ir

ABSTRACT

The field of cryptography employs many disciplines. First discipline that is sometimes used in cryptography is linear algebra and secondary is quasigroup theory. This paper will show new idea and method, that these two field applies in cryptography in a confidential and a secured way.

KEYWORDS: Quasigroups, Polynomials, Cipher Text, Encryption, Decryption, Matrix, invertible**.**
AMS Classification: Primery 12Y05, 68W30; Secondary 11Y16, 12D05, 20N05, 13P05.

1 INTRODUCTION

The history of cryptography can be traced back to the secret communication among people thousands of yeras ago. With the development of human society and industrial technology, theories and methods of cryptography have changed and improved gradually. In 1949, Shannon published his seminar paper ‘ Communication theory of securety systems, which marked the beginning of the modern cryptology.
The theory of quasigroups and loops begun to be developed in 1935 after the appearance of the work of Ruth Moufang, who first discovered the close connection between nondesarguesian projective planes and non-associative quasigroups. But, as is often the case, the concept of quasigroups(really non-associative) occurs much earlier in a non-obvious form, it is enough to mention the 36-officer problem of Euler, which is equivalent to the existence of a pair of orthogonal Latin squares of side 6. In the works of Albert, Bruck, Belousov, Aczel, Evans, Sade, Belyavskaya, Drapal, Kepka and etc. quasigroups and loops was discussed and appeared many investigations devoted to the theory of quasigroups and loops. Eliska Ochodkova and Vaclav Snasel ([12]) proposed to use quasigroups for secure encoding of file system, But almost all results obtained in branch of application of quasigroups in cryptology and coding theory to the end of eighties years of the XX-th century are described in [11, 6]. Basic facts on quasigroup theory it is possible to find in more details in [2, 9, 3, 4]. Information on basic fact in cryptology it is possible to find in [5].

§1. Preliminaries

In this section we will recall some basic definitions and algorithms that useful for our main results.

§1..1 Some basic definitions on quasigroups

A set is a well-defined collection of objects. Let G be a set and Σ be the set of all operations defined on the set G. Then we can defined an Algebra as a pair (G, Σ).

Definition 1.1. An algebra Q(·) is called a quasigroup, if each of the equations, ax = b and ya = b, has a unique solution for any a, b ∈ Q. A quasigroup with an identity element is called a loop.
The quasigroup concept has two interpretation. The first interpretation is the combinatorial point of view. It is like Latin square problems. The second is the geometrical one in the form of nets.
If Q(·) is a quasigroup, then denoting the unique solution of the equation ax = b by x = a\b and denoting the unique solution of the equation ya = b by y = b/a , we get an algebra Q(·, \, /) with the following identities:

$$x(x \setminus y) = y,\ x \setminus (x \cdot y) = y,$$
$$(y/x) \cdot x = y,\ (y \cdot x)/x = y.$$

Therefore we can defined the quasigroups as following:
Definition 1.2. A groupoid (Q, ·) is called a quasigroup, if on the set Q there exist operations \ and / such that in algebra (Q, ·, \, /) the following identities are fulfilled:

$$x(x \setminus y) = y,\ x \setminus (x \cdot y) = y,$$
$$(y/x) \cdot x = y,\ (y \cdot x)/x = y.$$

It is obvious that (Q, ·), (Q, /), (Q, \) are quasigroups.
It is obvious that every quasigroup is isomorphic with one Latin square, because in the cayley table of a quasigroup each row and each column is a permutation of the set Q. For more details on quasigroup theory see [6, 2, 9, 3, 4, 13]

§1..2 Ochadkova-Snasel binary quasigroup based cryptosystem
Eliska Ochodkova and Vaclav Snasel ([12]) proposed to use quasigroups for secure encoding of file system.
Quasigroups (Q, ·) and (Q, \) satisfies the following identities:

$$x \setminus (x \cdot y) = y,\ x \cdot (x \setminus y) = y.$$

The authors propose to use this property of quasigroups to construct a stream cipher.
Definition 1.3. Let A be a non-empty alphabet, k be a natural number, $u_i , \upsilon_j \in A$, $i \in \{1, \cdots, k\}$. A fixed element l ,(l∈A), is called leader. Then $f(\upsilon_1 , \upsilon_2 , \ldots, \upsilon_k) = \upsilon_1\upsilon_2\ldots\upsilon_k \Leftrightarrow \upsilon_1 = l.u_1$, $\upsilon_{i+1} = \upsilon_l . u_{i+1}$, 1, 2, ..., k-1 is an ciphering algorithm .
An enciphering algorithm is constructed in the following way:
$F^{(\setminus)}(\upsilon_1 , \upsilon_2 , \ldots., \upsilon_k) = u_1 u_2 \ldots u_k \Leftrightarrow u_1 = l \setminus \upsilon_1 , u_{i+1} = \upsilon_i \setminus \upsilon_l , i=1 , 2 , \ldots , k-1$.
Authors say that this cipher is resist to the brute force attack and to the statistical attack. For more details on quasigroups and its application in coding theory and cryptology see[13].

§1..3 Matrix cryptography
The area of cryptograqphy employs many different means of transforming normal data into hard-to-read data. Encryption is used widely by people, organizations and the government to safeguard their data from misuse.
One method of encryption by using algebra, specifically matrix operations. The method involves two matrices: one to encode, the encoding matrix, and one to decode, the decoding matrix.
First, the characters in the original message or stream are assigned numerical values. For the purposes of this document, A-Z are represented by the numbers 1-26 and a space is represented by 27.
The encoding matrix can be generated using any integers that the user desires. It can be something as simple as a 3 × 3 matrix composed of random integers. The matrix must be invertible for use in decoding. An example matrix is:

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

The message is then encoded the numbers above. An example message is:

T		M	E	S	S	A	G	E
20	27	13	5	19	19	1	7	5

The message is split up into 3 × 1 vectors as such:

$$\begin{bmatrix}20\\27\\13\end{bmatrix}\begin{bmatrix}5\\19\\19\end{bmatrix}\begin{bmatrix}1\\7\\5\end{bmatrix} \quad (1)$$

All of the vectors can then augmented into one matrix and multiplied by the encoding matrix. The resulting matrix is the encoded message.

$$\begin{bmatrix}-3 & -3 & -4\\ 0 & 1 & 1\\ 4 & 3 & 4\end{bmatrix}.\begin{bmatrix}20 & 5 & 1\\ 27 & 19 & 7\\ 13 & 19 & 5\end{bmatrix}=\begin{bmatrix}-193 & -148 & -44\\ 40 & 38 & 11\\ 203 & 153 & 45\end{bmatrix} \quad (2)$$

In order to decode this message, the receiver must multiply the decoding matrix, which is simply the inverse of the encoding matrix, by the encoded matrix. The resulting matrix, when formed back into a continous string and returned to the original characters, represents the original message.

$$\begin{bmatrix}1 & 0 & 1\\ 4 & 4 & 3\\ -4 & -3 & -3\end{bmatrix}.\begin{bmatrix}-193 & -148 & -44\\ 40 & 38 & 11\\ 203 & 153 & 45\end{bmatrix}=\begin{bmatrix}20 & 5 & 1\\ 27 & 19 & 7\\ 13 & 19 & 5\end{bmatrix} \quad (3)$$

In this paper we will consider this example for our new idea, that we will explain in the next section.

§1..4 Hill cipher

It is developed by the mathematician Lester Hill in 1929. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like a=0, b=1, ..., z=25. The substitution of cipher text letters in the place of plain-text letters leads to m linear equation. For m=3, the system can be described as follows:

$$C_1 = (K_{11}\,p_1 + K_{12}\,p_2 + K_{13}\,p_3) \bmod 26$$
$$C_2 = (K_{21}\,p_1 + K_{22}\,p_2 + K_{23}\,p_3) \bmod 26$$
$$C_3 = (K_{31}\,p_1 + K_{32}\,p_2 + K_{33}\,p_3) \bmod 26$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix}C_1\\C_2\\C_3\end{pmatrix}=\begin{pmatrix}K_{11} & K_{12} & K_{13}\\ K_{21} & K_{22} & K_{23}\\ K_{31} & K_{32} & K_{33}\end{pmatrix}\times\begin{pmatrix}p_1\\p_2\\p_3\end{pmatrix}$$

or simply we can write C = KP, where C and P are column vectors of length 3, representing the plain-text and cipher text respectively, and K is a 3 × 3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the cipher text, and then the plain-text is recovered. In general term we can write as follows:

For encryption:
$C = E_k(p) = k_p$

For decryption:
$P = D_k(C) = K^{-1}C = K^{-1}K_p = P$

If the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m-letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet.

§2. Cryptography using matrix and quasigroups

In this section we will define and explain new direction of application of quasigroups in cryptography using linear algebra. Consider an string of words that we want to send. By using subsections 1.2 and 1.3, we choose alphabet for our work, with respect to our language (number of alphabets, space, signs, numbers and operations). Hence if for each character we choose a unique integer from $\{0, 1, 2, \cdots, k-1\}$, all characters in the alphabet are mapped to the ring Z_k.
On the other hand, we have a Latin square of order p, which is one of $(p(p-1))!$ Possible Latin squares. Our plain text is mapped to one the possible matrices, say,

$$A_{m,n+1} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & l_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & l_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & l_m \end{pmatrix}$$

Now by subsection 1.2, $a_{i,j}$'s are calculated in the form :

$$a_{1,1} = l \cdot u_1,\ a_{1,n} = a_{1,n-1} \cdot u_{n+1},\ n = 1, 2, \cdots, k\text{-}1$$

Where l_1 is a fixed element and u_i's are our plain text. Note that l_i's, the leader of every cipher text in each row, may be different from others. Hence we have to add an column for $A_{m,n}$ consisting l_i's. Next, we can use an transformation function for $a_{i,j}$'s with respect to our Latin square. Then for suitably positive number t (mod 26), one can use the transformations $a_{i,j} \to a_{i,j} + t$ or $a_{i,j} \to a_{i,j} + 2t$ or $a_{i,j} \to a_{i,j} - 7t$, $\cdots$, etc.. Finally, we need an n×n invertible matrix K, to encode $C = K \times A_{m,n+1}$.Therefore send C to receiver.
Similar to subsection 1.3, the receiver for decoding, by knowledge of C and K^{-1}, calculates $K^{-1} \times C$ to get $A_{m,n+1}$ and then by inverse transformation $a_{i,j} - t \to a_{i,j}$ calculate $a_{i,j}$'s. Finally by quasigroup theory, $u_1 = l \setminus a_{1,1}$ and $u_{n+1} = a_{1,n-1} \setminus a_{1,n}$ in the first row. For other rows with respect to independent li's, follow similar process. Therefore receiver have a string of words $u_1u_2 \ldots u_{n+1}$. This method can be used for every plain text, and then, we will have very conflict and secure cipher text to work.

§3. Conclusion

Quasigroup cipher text is one of the powerful tools for encryption of plain text. On the other hand, Hill cipher is a block cipher that has several advantages such as disgusing letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput. This paper suggests efficient methods for combine two tools or more to get more confilict and secure ciphertext. This idea can be consider as a new way to convert all ciphertext to matrices and construct more secure ciphertext..

References

[1] Z. Brakerski, Gil Segev, Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting, J. Cryptology, DOI: 10.1007/s00145-012-9143-4, (2013), 26 .

[2] V. D. Belousov, Balanced identities on quasigroups, Mat. Sbornik, 70 (112):1, (1966), 55-97 (in Russian).

[3] V. D. Belousov, Systems of quasigroups with generalized identities, Uspekhi Mat. Nauk. 20 (1965), 75–146 (1967); English transl. in Russian Math. Surveys 20 (1965), 73–143.

[4] V. D. Belousov, J. Aczel, Generalized associativity and bisymmetry on quasigroups, Acta Mathematica, 11 (1960), 127–136, Hungary.

[5] A. Beutelspacher, Cryptology: An introduction to the science of encoding, concealing and hiding, Wiesbaden: Viewing, 2002, (in German).

[6] J. Denes, A. D. Keedwell, Latin Squares and Their Applications, Academic Press, New York (1974).

[7] S. S. Dhenkaran, M. Ilayaraja, Extension of Playfair Cipher using 16 × 16 Matrix, International Journal of Computer Applications (0975-888), Vol. 48, No. 7, (2012), 37- 41.

[8] R. B. Kallam, S. U. Kumar, A. V. Babu, V. S. Kumar, A Contemporary Polyalphabetic Cipher using Comprehensive Vigenere Table, World of Computer Science and Information Technology Journal(WCSIT), Vol. 1, No. 4, 167-171, (2011).

[9] T. Kepka, J. Jeˇzek, Quasigroups, isotopic to groups, Comm. Math. Univ. Carolinae, 16, 1 (1975), 59–76.

[10] Prakash. Kuppuswamy, Enrichment of Security through Cryptographic Public Key Algorithm based on Block Cipher, Indian J. of Compoter Science and Engineering(IJCSE), Vol.2 No.3, (2011), 347-355.

[11] K. A. Meyer, A new message authentication code based on the non-associativity of quasigroups, PhD Dissertation, Iowa State University, Ames, Iowa (2006).

[12] E. Ochadkova, V. Snasel, Using quasigroups for secure encoding of file system, Abstract of Talk on Conference "'Security and Protection of information"', Brno, Czeck Republic, 9-11.05.2001. 24 pages.

[13] V. Shcherbacov, Elements of quasigroup theory and some its application in code theory and cryptology, lecture notes, Prague, Czech Republic, 2003, 85pp.

[14] Kh. Shahbazpour An Application of Quasigroups in Constructing Secure Cipher Text, Far East J.Math. Sci. (FJMS), New Delhi, India, 2007, p.1–12.