ArticleCitation Format
Tudunkaya, S. M. (2019): On the Discrete Logarithm Problem of the Finite Groups of Rhotrices over Z_p.
Journal of Advances in Mathematical & Computational Sciences
Vol. 7,No.3. Pp 9-18

Article Progression Time Stamps

Article Type: Research Article
Manuscript Received 11th July, 2019
Final Acceptance: 13th August, 2019
Article DOI: dx.doi.org/10.22624/AIMS/MATHS/V7N3P2

On the Discrete Logarithm Problem of the Finite Groups of Rhotrices over Z_p

Tudunkaya, S. M.
Ahmadu Bello University
Zaria, Nigeria
E-mail: tudunkayaunique@yahoo.com

ABSTRACT

The Discrete Logarithm Problem (DLP) of finite groups of rhotrices over Z_p was explored. The representation and manipulation of these groups were provided in order to lay a solid foundation for the study. Numerical examples were also given to further substantiate the DLP.

Keywords: Group; Finite group; Cyclic group; Cryptography; Discrete logarithm problem.

1. INTRODUCTION

Clearly, the security of the Discrete Logarithm Problem (DLP) depends heavily on the group (finite) G under consideration. The more difficult the DLP the more secured it is. The group $G = {F^*}_{p^l}$ for a chosen prime p and exponent l or the group of points of a suitably chosen elliptic curve over a finite field can be used [1]. Hence, if the DLP is made easier it becomes more insecure. In this paper, emphases were put on the suitable choice of groups, description on how group elements are stored and manipulated. It was hoped that this effort will further enrich the pedagogical aspect of cryptography.

2. REVIEW OF RELATED LITERATURE

A rhotrix is an object:

$$A = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle$$

belonging to the set R where $a, b, c, d, e \in \mathfrak{R}$ [2]. Rhotrices is the plural of rhotrix and the central entry is called heart. If A and $B = \left\langle \begin{matrix} & g & \\ h & j & k \\ & l & \end{matrix} \right\rangle$ are two rhotrices, then

$A+B = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle + \left\langle \begin{matrix} & g & \\ h & j & k \\ & l & \end{matrix} \right\rangle = \left\langle \begin{matrix} & a+g & \\ b+h & c+j & d+k \\ & e+l & \end{matrix} \right\rangle$, this addition is commutative. Moreover,

$A + (-A) = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle + \left\langle \begin{matrix} & -a & \\ -b & -c & -d \\ & -e & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 0 & \\ 0 & 0 & 0 \\ & 0 & \end{matrix} \right\rangle$ implies that $-A$ is the additive inverse of A. The pair $(R,+)$ is a commutative group. If α is a scalar, then

$\alpha A = \alpha \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle = \left\langle \begin{matrix} & \alpha a & \\ \alpha b & \alpha c & \alpha d \\ & \alpha e & \end{matrix} \right\rangle$.

For two rhotrices A and B, $AB = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle \left\langle \begin{matrix} & g & \\ h & j & k \\ & l & \end{matrix} \right\rangle = \left\langle \begin{matrix} & aj+gc & \\ bj+hc & c+j & dj+kc \\ & ej+lc & \end{matrix} \right\rangle$, this multiplication is also commutative and was adopted in this work. It also has the following identity element:

$$I = \left\langle \begin{matrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{matrix} \right\rangle$$

This means if B is the multiplicative inverse of A, then $AB = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle \left\langle \begin{matrix} & g & \\ h & j & k \\ & l & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{matrix} \right\rangle$ implying that

$B = A^{-1} = -\frac{1}{c^2} \left\langle \begin{matrix} & a & \\ b & -c & d \\ & e & \end{matrix} \right\rangle, c \neq 0.$

The definition of rhotrix was generalized in [3] under the same operations as

$$A(n) = \left\langle \begin{matrix} & & & a_1 & & & \\ & & a_2 & a_3 & a_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_{\left\{\frac{(t+1)}{2}\right\}-\frac{n}{2}} & \cdots & \cdots & a_{\left\{\frac{(t+1)}{2}\right\}} & \cdots & \cdots & a_{\left\{\frac{(t+1)}{2}\right\}+\frac{n}{2}} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & a_{t-3} & a_{t-2} & a_{t-1} & & \\ & & & a_t & & & \end{matrix} \right\rangle$$

where $t = \frac{(n^2+1)}{2}$, $n \epsilon 2Z^+ + 1$ and $\frac{n}{2}$ is the integer value upon division of n by 2

An element of the set $M = \left\{ \left\langle \begin{matrix} & & & m_1 & & & \\ & & m_2 & m_3 & m_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ m_{\alpha} & \cdots & \cdots & m_{\beta} & \cdots & \cdots & m_{\pi} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & m_{t-3} & m_{t-2} & m_{t-1} & & \\ & & & m_t & & & \end{matrix} \right\rangle : m_1, m_1, \dots, m_1 \in Z_n \right\}$

where addition(+) and multiplication(•) are done modulo n under the addition and multiplication of rhotrices, such that $\alpha = \frac{n^2-2n+5}{4}$, $\beta = \frac{1}{4}(n^2+3)$ and $\pi = \frac{n^2+2n+1}{4}$ was defined as modulo rhotrix [4].

It was given that

$$0=\left\langle\begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \dots & \dots & \dots & \cdots & \\ 0_\alpha & \cdots & \dots & 0_\beta & \dots & \cdots & 0_\pi \\ & \cdots & \dots & \dots & \dots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array}\right\rangle$$ is the additive identity of M and its

multiplicative identity is

$$I=\left\langle\begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \dots & \dots & \dots & \cdots & \\ 0_\alpha & \cdots & \dots & 1_\beta & \dots & \cdots & 0_\pi \\ & \cdots & \dots & \dots & \dots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array}\right\rangle$$

and if $n=p$ where p is a prime, then the multiplicative inverse of

$$A=\left\langle\begin{array}{ccccccc} & & & a_1 & & & \\ & & a_2 & a_3 & a_4 & & \\ & \cdots & \dots & \dots & \dots & \cdots & \\ a_\alpha & \cdots & \dots & a_\beta & \dots & \cdots & a_\pi \\ & \cdots & \dots & \dots & \dots & \cdots & \\ & & a_{t-3} & a_{t-2} & a_{t-1} & & \\ & & & a_t & & & \end{array}\right\rangle\in M$$

will be

$$B=\left\langle\begin{array}{ccccccc} & & & b_1 & & & \\ & & b_2 & b_3 & b_4 & & \\ & \cdots & \dots & \dots & \dots & \cdots & \\ b_\alpha & \cdots & \dots & b_\beta & \dots & \cdots & b_\pi \\ & \cdots & \dots & \dots & \dots & \cdots & \\ & & b_{t-3} & b_{t-2} & b_{t-1} & & \\ & & & b_t & & & \end{array}\right\rangle\in M$$

Such that for $i=\beta$

$$a_\beta d_\beta = 1 \text{ mod } p$$

and for each $i=1,2,\dots,t$ and $i\neq\beta$

$$a_i d_\beta + a_\beta d_i = 0 \text{ mod } p$$

The following definitions are presented according to [5]: if G is a group and there exists an element a in G such that $G = \{a^m : m \in Z\}$, then G is called a cyclic group and the element a is said to be the generator of G. Also recall that, a reflexive, symmetric and transitive relation R in the set X is called an equivalence relation. Moreover, if $\sim$ is an equivalence relation on a set X, for $a \in X$, the equivalence class of a is the set of all elements $b \in X$ such that $a \sim b$ and is denoted by $[a]$.

FINITE GROUPS OF RHOTRICES OVER Z_p

By [6], let

$$x = \left\langle \begin{array}{ccccccc} & & & x_1 & & & \\ & & x_2 & x_3 & x_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ x_{\alpha} & \cdots & \cdots & x_{\beta} & \cdots & \cdots & x_{\pi} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & x_{t-3} & x_{t-2} & x_{t-1} & & \\ & & & x_t & & & \end{array} \right\rangle$$

$x_i \in Z_p, i = 1,2, \ldots t$ for some prime p, $x_i \neq 0$ for each i, $x_\beta \geq 2$ such that either all the $x_i{}'s$ are equal or they are all equal with the exception x_β. In this paper, the case where $x_i \in Z_p, i = 1,2, \ldots t$ for some prime p, $x_i \neq 0$ for each i, $x_\beta \geq 2$ such that the $x_i{}'s$ may or may not be equal to each other was studied.

1. Let G be the set of order $p(p-1)$, generated by x under the multiplication (o) of rhotrices modulo p, then G is a group. For example, suppose $p = 5$, $t = 5$, then the order of G is $5 \times 4 = 20$. Meanwhile, Let μ= $\left\langle \begin{array}{ccc} & 3 & \\ 4 & 3 & 2 \\ & 1 & \end{array} \right\rangle \in G,$ be the generator of G, then

$$\mu^1 = \left\langle \begin{array}{ccc} & 3 & \\ 4 & 3 & 2 \\ & 1 & \end{array} \right\rangle$$

$$\mu^2 = \left\langle \begin{array}{ccc} & 3 & \\ 4 & 4 & 2 \\ & 1 & \end{array} \right\rangle$$

$$\mu^3 = \left\langle \begin{matrix} & 1 & \\ 3 & 2 & 4 \\ & 2 & \end{matrix} \right\rangle$$

$$\mu^4 = \left\langle \begin{matrix} & 4 & \\ 2 & 1 & 1 \\ & 3 & \end{matrix} \right\rangle$$

$$\mu^5 = \left\langle \begin{matrix} & 0 & \\ 0 & 3 & 0 \\ & 0 & \end{matrix} \right\rangle$$

$$\mu^6 = \left\langle \begin{matrix} & 4 & \\ 2 & 4 & 1 \\ & 3 & \end{matrix} \right\rangle$$

$$\mu^7 = \left\langle \begin{matrix} & 4 & \\ 2 & 2 & 1 \\ & 3 & \end{matrix} \right\rangle$$

$$\mu^8 = \left\langle \begin{matrix} & 3 & \\ 4 & 1 & 2 \\ & 1 & \end{matrix} \right\rangle$$

$$\mu^9 = \left\langle \begin{matrix} & 2 & \\ 1 & 3 & 3 \\ & 4 & \end{matrix} \right\rangle$$

$$\mu^{10} = \left\langle \begin{matrix} & 0 & \\ 0 & 4 & 0 \\ & 0 & \end{matrix} \right\rangle$$

$$\mu^{11} = \left\langle \begin{matrix} & 2 & \\ 1 & 2 & 3 \\ & 4 & \end{matrix} \right\rangle$$

$$\mu^{12} = \left\langle \begin{matrix} & 2 & \\ 1 & 1 & 3 \\ & 4 & \end{matrix} \right\rangle$$

$$\mu^{13} = \left\langle \begin{matrix} & 4 & \\ 2 & 3 & 1 \\ & 3 & \end{matrix} \right\rangle$$

$$\mu^{14} = \left\langle \begin{matrix} & 1 & \\ 3 & 4 & 4 \\ & 2 & \end{matrix} \right\rangle$$

$$\mu^{15} = \left\langle \begin{matrix} & 0 & \\ 0 & 2 & 0 \\ & 0 & \end{matrix} \right\rangle$$

$$\mu^{16} = \left\langle \begin{matrix} & 1 & \\ 3 & 1 & 4 \\ & 2 & \end{matrix} \right\rangle$$

$$\mu^{17} = \left\langle \begin{matrix} & 1 & \\ 3 & 3 & 4 \\ & 2 & \end{matrix} \right\rangle$$

$$\mu^{18} = \left\langle \begin{matrix} & 2 & \\ 1 & 4 & 3 \\ & 4 & \end{matrix} \right\rangle$$

$$\mu^{19} = \left\langle \begin{array}{ccc} & 3 & \\ 4 & 2 & 2 \\ & 1 & \end{array} \right\rangle$$

$$\mu^{20} = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle$$

mod p are the 20 elements of the group G.

3. THE DISCRETE LOGARITHM PROBLEM (DLP)

Theorem:

Let G be as defined in section 2 above. Let $g = \left\langle \begin{array}{ccccccc} & & & g_1 & & & \\ & & g_2 & g_3 & g_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ g_{\alpha} & \cdots & \cdots & g_{\beta} & \cdots & \cdots & g_{\pi} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & g_{t-3} & g_{t-2} & g_{t-1} & & \\ & & & g_t & & & \end{array} \right\rangle$ be a generator of G: If an element $y = \left\langle \begin{array}{ccccccc} & & & y_1 & & & \\ & & y_2 & y_3 & y_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ y_{\alpha} & \cdots & \cdots & y_{\beta} & \cdots & \cdots & y_{\pi} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & y_{t-3} & y_{t-2} & y_{t-1} & & \\ & & & y_t & & & \end{array} \right\rangle$ in G is chosen, find a positive integer n such that $g^n = y$.

Proof:

By the rhotrix exponent rule provided by [7] and the hypothesis above,

$$g^n = \left\langle \begin{array}{ccccccc} & & & g_1 & & & \\ & & g_2 & g_3 & g_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ g_{\alpha} & \cdots & \cdots & g_{\beta} & \cdots & \cdots & g_{\pi} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & g_{t-3} & g_{t-2} & g_{t-1} & & \\ & & & g_t & & & \end{array} \right\rangle^n$$

$$= {g_\beta}^{n-1}\left\langle \begin{array}{ccccccc} & & & ng_1 & & & \\ & & ng_2 & ng_3 & ng_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ ng_{\alpha} & \cdots & \cdots & ng_\beta & \cdots & \cdots & ng_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & ng_{t-3} & ng_{t-2} & ng_{t-1} & & \\ & & & ng_t & & & \end{array} \right\rangle$$

$$= \left\langle \begin{array}{ccccccc} & & & y_1 & & & \\ & & y_2 & y_3 & y_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ y_{\alpha} & \cdots & \cdots & y_\beta & \cdots & \cdots & y_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & y_{t-3} & y_{t-2} & y_{t-1} & & \\ & & & y_t & & & \end{array} \right\rangle$$

This implies

${g_\beta}^{n-1}ng_\beta = {g_\beta}^{n}=y_\beta$ (1)

${g_\beta}^{n-1}ng_i = y_i$ (2)

Dividing (2) by (1), we have

$$\frac{{g_\beta}^{n-1}ng_i}{{g_\beta}^{n}} = \frac{y_i}{y_\beta}$$

Implying that

$$\frac{ng_i}{g_\beta} = \frac{y_i}{y_\beta}$$

Therefore,

$$n = \frac{y_i g_\beta}{y_\beta g_i}$$

3.1 Implementation

Let Alice and Bob agree on an arbitrary finite group G of rhotrices and its generator g as described in section 2 above. To secure an exchange of information that is going to take place between both of them:

1) Alice chooses a random key y in G which can be expressed as a power of g in G and sends the message under this key to Bob
2) Bob searches for a positive integer n such that $y = g^n$ to recover the message.

3.2 Test

1) Suppose Alice and Bob agree on the group G of section 2 above. If Alice sends the message under the key

$$y = \left\langle \begin{matrix} & 4 & \\ 2 & 4 & 1 \\ & 3 & \end{matrix} \right\rangle$$

which is a power of $g = \left\langle \begin{smallmatrix} & 3 & \\ 4 & 3 & 2 \\ & 1 & \end{smallmatrix} \right\rangle$, then Bob searches for

$n = \frac{y_i g_\beta}{y_\beta g_i}$, which means $n = \frac{4\times3}{3\times4} = \frac{2\times3}{4\times4} = \frac{1\times3}{2\times4} = \frac{3\times3}{1\times4} = 1 \quad mod\ 5.$ Therefore, n falls in the equivalence class of $1\ mod\ 5$ and since n is up to 20, then $n = 1\ or\ 6\ or\ 11\ or\ 16$, but by testing, clearly n is not $1\ or\ 11\ or\ 16$ and therefore $n = 6$.

2) If $g = \left\langle \begin{smallmatrix} & 3 & \\ 4 & 3 & 2 \\ & 1 & \end{smallmatrix} \right\rangle$ and $y = \left\langle \begin{smallmatrix} & 3 & \\ 4 & 1 & 2 \\ & 1 & \end{smallmatrix} \right\rangle$, then $n = \frac{3\times3}{3\times1} = \frac{4\times3}{4\times1} = \frac{1\times3}{1} = \frac{4}{3} = \frac{2}{4} = \frac{1}{2} = \frac{3}{1} = 3\ mod\ 5$
Since for instance, $\frac{4}{3}$ is the same as multiplying 4 by the multiplicative inverse of $3\ mod\ 5$
i.e. $\frac{4}{3} = 4 \times 2 = 8 \equiv 3\ mod\ 5$. Similarly for $\frac{2}{4}$ and $\frac{1}{2}$.

Now, since $n = 3$, it implies that n falls in the equivalence class of $3\ mod\ 5$ i.e. $n = 3\ or\ 8\ or\ 13\ or\ 18$, but

4. CONCLUSION

This paper displayed the implementation of Discrete Logarithm Problem of certain finite groups of rhotrices. The implementation was tested in order to show how it works practically. Needed definitions and results were brought forward under relevant sections to either prepare or refresh the reader to have a clear understanding of the paper. The paper succeeded in showing a particular area of application of rhotrices.

REFERENCES

[1] Blackburn, S. R., Et al., (2009). Group Theory in Cryptography. arXiv:0906.5545v1 [math.GR]

[2] Ajibade, A.O., (2003). The Concept of Rhotrix in Mathematical Enrichment, Int. J. Math. Educ. Sci. Technol., 34:175-179.

[3] Mohammed, A., (2011). Theoretical Development and Application of Rhotrices, PhD Dissertation. Amazon.com

[4] Tudunkaya, S.M. and Makanjuola, S.O., (2012). Certain construction of finite fields, J. of the Nig. Mathl Phy., vol. 21: 95-104.

[5] Tudunkaya, S. M., (2018). An Extension of Certain Construction of Finite Groups, Nig. J. of Scientific Research (submitted)

[6] Godwin A. O. (2000). Algebra for Colleges and Universities: An Integrated Approach, Anachuna Educational Books, Obosi, Anambra State, Nigeria.

[7] Mohammed, A., (2007). A Note on Rhotrix Exponent Rule and its Application to Special Series and Polynomial Equations Defined over Rhotrices, Notes Num. Theo. Discrete Math., 13: 1-5