Nigerian Journal of Mathematics and Applications
Volume **25**, (2016), 131 – 139. *Printed by Unilorin press*
©*Nig. J. Math. Appl.* *http : //www.njmaman.com*

Concerning Certain Finite Groups and the Elgamal Cryptosystem

S. M. Tudunkaya

Abstract

This paper presented a modification of the ElGamal cryptosystem with the aid of finite multiplicative groups of rhotrices defined over Z_p for a prime p. This system may have an additional advantage of higher security.

1. Introduction

The ElGamal cryptosystem was based on the Diffie-Helman Key. It has the property that a single plain text can be encrypted to many possible cipher texts. It has two as the expansion factor. Some basic definitions and results were given in the first section to equip the reader with the basics. In the second section, the actual building blocks for the adjusted ElGamal cryptosystem were discussed and numerical examples were given to further buttress how these groups are represented, stored and manipulated. And in the third section, the adjusted ElGamal cryptosystem was described and was implemented in the fourth section.

1.1. **Review of Related Literature.** The idea about rhotrices appeared first (Ajibade 2003) as an object of the form

$$A = \left\langle \begin{matrix} & a & \\ b & h(A) & d \\ & e & \end{matrix} \right\rangle \tag{1}$$

Received: 01/10/2016, Accepted: 12/12/2016, Revised: 17/12/2016.
2015 *Mathematics Subject Classification.* 20DXX; 11T71. * Corresponding author.
Key words and phrases. Group, Cyclic group, Cryptography, ElGamal cryptosystem
Department of Science Education, Ahmadu Bello University, Zaria, Nigeria.

Email: tudunkayaunique@yahoo.com

belonging to the set R where $a, b, h(A), d, e$ are real numbers, the entry $h(A)$ is called heart.

$$A + B = \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & f & \\ g & h(B) & j \\ & k & \end{array} \right\rangle$$

$$= \left\langle \begin{array}{ccc} & a+f & \\ b+g & h(A)+h(B) & d+j \\ & e+k & \end{array} \right\rangle \tag{2}$$

which is commutative.

$$A + (-A) = \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & -a & \\ -b & -h(A) & -d \\ & -e & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 0 & 0 \\ & 0 & \end{array} \right\rangle \tag{3}$$

the zero of R. Therefore $-A$ is the additive inverse of A. It follows that $(R, +)$ is a commutative group.

$$\alpha A = \alpha \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & \alpha a & \\ \alpha b & \alpha h(A) & \alpha d \\ & \alpha e & \end{array} \right\rangle \tag{4}$$

where α is a scalar.

$$A \bullet B = \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle \bullet \left\langle \begin{array}{ccc} & f & \\ g & h(B) & j \\ & k & \end{array} \right\rangle$$

$$= \left\langle \begin{array}{ccc} & ah(B)+fh(A) & \\ bh(B)+gh(A) & h(A)h(B) & dh(B)+jh(A) \\ & eh(B)+kh(A) & \end{array} \right\rangle \tag{5}$$

which is also commutative and was adopted in this paper. The multiplicative identity of R is

$$I = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle \tag{6}$$

And if

$$A \bullet B = \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle \bullet \left\langle \begin{array}{ccc} & f & \\ g & h(B) & j \\ & k & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle \tag{7}$$

then

$$B = A^{-1} = -\frac{1}{h(A)^2} \left\langle \begin{array}{ccc} & a & \\ b & -h(A) & d \\ & e & \end{array} \right\rangle \tag{8}$$

where $h(A) \neq 0$. This means

$$f = -\frac{a}{h(A)^2}$$

$$g = -\frac{b}{h(A)^2}$$

$$h(B) = -\frac{1}{h(A)}$$

$$j = -\frac{d}{h(A)^2}$$

$$k = -\frac{k}{h(A)^2}$$

The above definition of R was generalized later (Mohammed 2011) under the same operation as

$$G(t) = \left\langle \begin{matrix} & & & g_1 & & & \\ & g_2 & g_3 & g_4 & & \\ g^{\left\{\frac{t+1}{2}\right\}-n\backslash 2} & \cdots & \cdots & g^{\left\{\frac{t+1}{2}\right\}} & \cdots & \cdots & g^{\left\{\frac{t+1}{2}\right\}+n\backslash 2} \\ & \cdots & g_{t-3} & g_{t-2} & g_{t-1} & \cdots & \\ & & & g_t & & & \end{matrix} \right\rangle \tag{9}$$

where $t = \frac{1}{2}(n^2+1)$, $\quad n \in 2Z^+ + 1$ and $n\backslash 2$ is the integer value upon division of n by 2. The inverse and the identity elements were defined in the same way as above and in accordance with the sizes of the rhotrices under consideration. In Tudunkaya and Makanjuola (2012), a modulo rhotrix was defined as an element of the set

$$M[R_{z^t}] =$$

$$\left\{ \left\langle \begin{matrix} & & & a_1 & & & \\ & a_2 & a_3 & a_4 & & \\ a_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & a_\pi \\ & \cdots & a_{t-3} & a_{t-2} & a_{t-1} & \cdots & \\ & & & a_t & & & \end{matrix} \right\rangle : a_1, \ldots, a_t \in Z_n \right\} \tag{10}$$

where addition($+$) and multiplication($\bullet$) 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 $\pi = \frac{n^2+2n+1}{4}$.

The additive identity is

$$0 = \left\langle \begin{matrix} & & & 0_1 & & & \\ & 0_2 & 0_3 & 0_4 & & \\ 0_\alpha & \cdots & \cdots & 0_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & 0_{t-3} & 0_{t-2} & 0_{t-1} & \cdots & \\ & & & 0_t & & & \end{matrix} \right\rangle \tag{11}$$

The multiplicative identity is

$$I = \left\langle \begin{matrix} & & & 0_1 & & & \\ & 0_2 & 0_3 & 0_4 & & \\ 0_\alpha & \cdots & \cdots & 1_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & 0_{t-3} & 0_{t-2} & 0_{t-1} & \cdots & \\ & & & 0_t & & & \end{matrix} \right\rangle \tag{12}$$

and if $n = p$, the multiplicative inverse of

$$M = \left\langle \begin{matrix} & & & m_1 & & & \\ & m_2 & m_3 & m_4 & & & \\ m_\alpha & \cdots & \cdots & \cdots & \cdots & \cdots & m_\pi \\ & \cdots & m_\beta & \cdots & \cdots & & \\ & m_{t-3} & m_{t-2} & m_{t-1} & & & \\ & & m_t & & & & \end{matrix} \right\rangle \tag{13}$$

will be

$$N = \left\langle \begin{matrix} & & & n_1 & & & \\ & n_2 & n_3 & n_4 & & & \\ n_\alpha & \cdots & \cdots & \cdots & \cdots & \cdots & n_\pi \\ & \cdots & n_\beta & \cdots & \cdots & & \\ & n_{t-3} & n_{t-2} & n_{t-1} & & & \\ & & n_t & & & & \end{matrix} \right\rangle \tag{14}$$

such that when $i = \beta$,

$$m_\beta n_\beta \equiv 1 \quad mod \quad p \tag{15}$$

and when $i \neq \beta$ $i = 1, 2, \cdots, t$ $i \neq \beta$ then

$$m_i n_\beta + n_i m_\beta \equiv 0 \quad mod \quad p \tag{16}$$

2. Finite Groups of Rhotrices Over Z_p

Suppose $m_1, m_2, \cdots, m_t \in Z_p$, for some prime p and

$$M = \left\langle \begin{matrix} & & & m_1 & & & \\ & m_2 & m_3 & m_4 & & & \\ m_\alpha & \cdots & \cdots & \cdots & \cdots & \cdots & m_\pi \\ & \cdots & m_\beta & \cdots & \cdots & & \\ & m_{t-3} & m_{t-2} & m_{t-1} & & & \\ & & m_t & & & & \end{matrix} \right\rangle \tag{17}$$

where $a_1 = m_2 = \cdots = m_t \neq 0$ and $m_\beta \geq 2$. If G is the set of all elements generated by M under the multiplication $(\circ)$ of rhotrices modulo p, then $(G, \circ)$ is a group (Tudunkaya 2016). Also, $(G, \circ)$ is cyclic and thus abelian. The order of the group G is $o(G) = (p-1)p$, therefore G is a finite group. Since G is cyclic there exist(s) some element(s) $m \in G$ (primitive element) that generates G.

For example, If $p = 3$ and $t = 5$ then $\partial = \left\langle \begin{matrix} & 1 & \\ 1 & 2 & 1 \\ & 1 & \end{matrix} \right\rangle \in G$ the order of G is $2 \times 3 = 6$ therefore:

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

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

$$\partial^3 = \left\langle \begin{matrix} & 1 & \\ 1 & 1 & 1 \\ & 1 & \end{matrix} \right\rangle \left\langle \begin{matrix} & 1 & \\ 1 & 2 & 1 \\ & 1 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 0 & \\ 0 & 2 & 0 \\ & 0 & \end{matrix} \right\rangle$$

$$\partial^4 = \left\langle \begin{matrix} & 0 & \\ 0 & 2 & 0 \\ & 0 & \end{matrix} \right\rangle \left\langle \begin{matrix} & 1 & \\ 1 & 2 & 1 \\ & 1 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 2 & \\ 2 & 1 & 2 \\ & 2 & \end{matrix} \right\rangle$$

$$\partial^5 = \left\langle \begin{array}{ccc} & 2 & \\ 2 & 1 & 2 \\ & 2 & \end{array} \right\rangle \left\langle \begin{array}{ccc} & 1 & \\ 1 & 2 & 1 \\ & 1 & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & 2 & \\ 2 & 2 & 2 \\ & 2 & \end{array} \right\rangle$$

$$\partial^6 = \left\langle \begin{array}{ccc} & 2 & \\ 2 & 2 & 2 \\ & 2 & \end{array} \right\rangle \left\langle \begin{array}{ccc} & 1 & \\ 1 & 2 & 1 \\ & 1 & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle$$

This means

$$G = \{\partial^1, \partial^2, \partial^3, \partial^4, \partial^5, \partial^6\}$$

Whether by the left or by the right, G is a group, for example the inverse of ∂^2 is ∂^4 and vice-versa because

$$\partial^2\partial^4 = \partial^6 = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle$$

on the left hand side. Also by the right,

$$\partial^2\partial^4 = \left\langle \begin{array}{ccc} & 1 & \\ 1 & 1 & 1 \\ & 1 & \end{array} \right\rangle \left\langle \begin{array}{ccc} & 2 & \\ 2 & 1 & 2 \\ & 2 & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle$$

Hence, each of the two sides can be used depending on the need and convenience.

Note that the entries of G can be rhotrices themselves (Tudunkaya and Makanjuola 2013), even if this happens, the properties of G are preserved (Tudunkaya 2016). The order of G can be increased over and over in such away that operations defined on it are possible, this is also property preserving.

In other words, G can be defined as the set of all elements generated by R under the multiplication ($\circ$) of rhotrices modulo p where

$$R_r = \left\langle \begin{array}{ccccccccc} & & & & r_1 & & & & \\ & & & r_2 & r_3 & r_4 & & & \\ r_\alpha & \cdots & & \cdots & \cdots & \cdots & \cdots & r_\pi & \\ & & \cdots & r_{t-3} & r_{t-2} & r_{t-1} & \cdots & & \\ & & & & r_t & & & & \end{array} \right\rangle \tag{18}$$

such that $h(r_\beta) \geq 2$ and for each i,

$$r_i = \left\langle \begin{array}{ccccccccc} & & & & a_1 & & & & \\ & & & a_2 & a_3 & a_4 & & & \\ a_\alpha & \cdots & & \cdots & \cdots & \cdots & \cdots & a_\pi & \\ & & \cdots & a_{t-3} & a_{t-2} & a_{t-1} & \cdots & & \\ & & & & a_t & & & & \end{array} \right\rangle \tag{19}$$

$a_i \in Z_p$, for some prime p and $a_i \neq 0$ for all i.

For instance, let $p = 3$, define

$$y = \left\langle \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 1 & \\ & 2 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 2 & \\ & 2 & \end{matrix} \right\rangle \right\rangle \in \xi$$

the order of ξ is $2 \times 3 = 6$ and

$$y^1 = \left\langle \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 1 & \\ & 2 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 2 & \\ & 2 & \end{matrix} \right\rangle \right\rangle$$

$$y^2 = \left\langle \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 1 & \\ & 2 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 2 & \\ & 2 & \end{matrix} \right\rangle \right\rangle$$

$$\circ \left\langle \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 1 & \\ & 2 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 2 & 2 & 2 \\ & 2 & \\ & 2 & \end{matrix} \right\rangle \right\rangle$$

$$= \left\langle \left\langle \begin{matrix} 0 & 0 & 0 \\ & 1 & \\ & 0 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \right\rangle$$

similarly,

$$y^3 = \left\langle \left\langle \begin{matrix} 0 & 0 & 0 \\ & 0 & \\ & 0 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 0 & 0 & 0 \\ & 0 & \\ & 0 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 2 & \\ & 0 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 0 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 0 & 0 & 0 \\ & 0 & \\ & 0 & \end{matrix} \right\rangle \right\rangle$$

$$y^4 = \left\langle \left\langle \begin{matrix} 2 & 2 & 2 \\ & 2 & \\ & 2 & \end{matrix} \right\rangle \begin{matrix} \left\langle \begin{matrix} 1 & 1 & 1 \\ & 2 & \\ & 1 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 2 & 2 & 2 \\ & 1 & \\ & 2 & \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & 0 & 0 \\ & 1 & \\ & 0 & \end{matrix} \right\rangle \end{matrix} \left\langle \begin{matrix} 1 & 1 & 1 \\ & 1 & \\ & 1 & \end{matrix} \right\rangle \right\rangle$$

$$y^5 = \left\langle \left\langle \begin{matrix} 0 & \begin{matrix}0\\2\\0\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 2 & \begin{matrix}2\\2\\2\end{matrix} & 2 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 2 & \begin{matrix}2\\2\\2\end{matrix} & 2 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 2 & \begin{matrix}2\\1\\2\end{matrix} & 2 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\1\\0\end{matrix} & 0 \end{matrix} \right\rangle \right\rangle$$

$$y^6 = \left\langle \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\1\\0\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle \right\rangle$$

Therefore, $\xi = \left\{y^1, y^2, y^3, y^4, y^5, y^6\right\}$

2.1. **The Key Establishment.** After the Diffie-Hellman key exchanged one most popular key in public key cryptography is the Elgamal key algorithm. It was proposed in 1984 by Taher Elgamal and its cryptanalysis depends on the Discrete Logarithm Problem. It is an asymetric key encryption based on one way function. The need for both parties to associate before they compute a common private key informed the need for such key encryptions as Elgamal. The Elgamal key algorithm can be developed by one party without the active participation of the other party. Only the receiver needs to create and publish his/her key in advance. If Alice and Bob share a secret key $K \in S$, define a harsh function $H : S \longrightarrow \{0,1\}^n$ from the set of finite binary strings S to a fixed finite set $X = \{0,1\}^n$ of length n which can be made sufficiently large say $log_2 |S|$. S is now the key space of the cryptosystem.

2.1.1. *Encryption.* For encryption of the message X to Bob, Alice obtains Bob's public key (p, g, g^b) through any official or trusted key server. Write the message X as set of integers $x_1, x_2, x_3, ...$ in the range $1, ..., p-1$ to be encoded individually. Alice now selects a random exponent k and computes $g^k \mod p$, combines it with the cipher text to be sent to Bob. The set C of all $c_i = x_i * (g^b)^k$ where i is greater than 0 and less than or equal to the absolute value of X is the cipher text. This together with $g^k \mod p$ will be sent to Bob. It is advisable to use different k for each i.

2.1.2. *Decryption.* Since the shared key equation is $(g^k)^{p-1-b} = (g^k)^{-b} = g^{-bk}$ therefore for each c_i Bob computes $x_i = (g^k)^{-b} * c_i \mod p$. The set X of all x_i is the message sent by Alice.

3. The Improved ElGamal Cryptosystem

The description of ElGamal key given in Grewal (2015), Myasnikov et al (2007) and Blackburn (2009) were adapted here. Suppose a and b are positive integers, the description of the adjusted ElGamal cryptosystem is:

1) Alice and Bob agreed on an arbitrary group G as described in section 2 above and a generating element g in G.

2) The receiver Alice picks at random a natural number a and computes g^a

3) The sender Bob picks a message x and a random element g in G and sends two elements $x(g^a)^b$ and g^b to Alice.

4) Alice recovers $x = (x(g^a)^b)((g^b)^a)^{-1}$

The ElGamal encryption is probabilistic. In other words, a single message (plaintext) can be encrypted to many possible ciphertexts.

4. Implementation

1) Suppose Alice and Bob agreed on a group G for a prime $p = 5$, $p = 5$ then $|G| = 20$. If Alice picks a primitive element $g = \left\langle \begin{smallmatrix} & 3 & \\ 3 & 3 & 3 \\ & 3 & \end{smallmatrix} \right\rangle \in G$, and an integer 7, computes $g^7 = \left\langle \begin{smallmatrix} & 4 & \\ 4 & 2 & 4 \\ & 4 & \end{smallmatrix} \right\rangle$ and sends to Bob. If Bob picks an integer 2, a message x, computes

$$x(g^7)^2 = xg^{14} = x \left\langle \begin{smallmatrix} & 1 & \\ 1 & 4 & 1 \\ & 1 & \end{smallmatrix} \right\rangle = \left\langle \begin{smallmatrix} & x & \\ x & 4x & x \\ & x & \end{smallmatrix} \right\rangle$$

and sends to Alice. To retrieve x Alice computes

$$x(g^{14})(g^{14})^{-1} = \left\langle \begin{smallmatrix} & x & \\ x & 4x & x \\ & x & \end{smallmatrix} \right\rangle \left\langle \begin{smallmatrix} & 4 & \\ 4 & 4 & 4 \\ & 4 & \end{smallmatrix} \right\rangle = \left\langle \begin{smallmatrix} & 0 & \\ 0 & x & 0 \\ & 0 & \end{smallmatrix} \right\rangle = xI = x$$

2) If Alice and Bob agreed on a group G for a prime $p = 7$ then $|G| = 42$. Suppose Alice picks a primitive element $g = \left\langle \begin{smallmatrix} & 2 & \\ 2 & 3 & 2 \\ & 2 & \end{smallmatrix} \right\rangle \in G$, and an integer 13, computes $g^{13} = \left\langle \begin{smallmatrix} & 5 & \\ 5 & 3 & 5 \\ & 5 & \end{smallmatrix} \right\rangle$ and sends to Bob. If Bob picks an integer 3, a message x, computes

$$x(g^{13})^3 = xg^{39} = x \left\langle \begin{smallmatrix} & 2 & \\ 2 & 6 & 2 \\ & 2 & \end{smallmatrix} \right\rangle = \left\langle \begin{smallmatrix} & 2x & \\ 2x & 6x & 2x \\ & 2x & \end{smallmatrix} \right\rangle$$

and sends to Alice. To retrieve x Alice computes

$$x(g^{39})(g^{39})^{-1} = xI = x$$

4.1. **Conclusion.** Finite groups of rhotrices have been used in the development of the ElGamal Cryptosystem in an effort to diversify and improve the functions and applications of the ElGamal key. A reduction in the insecurity of the ElGamal may be achieved. Basic concepts were reviewed in the first section and the improved ElGamal cryptosystem was described in the last section.

References

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

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

[3] Grewal, J. K.,2015 Elgamal: Public -Key Cryptosystem. A paper presented for the degree of Master of Science, Indiana State University, Terre Haute IX, USA.

[4] Mohammed, A., 2011 Theoritical Development and Application of Rhotrices, PhD Dissertation. Amazon.com

[5] Myasnikov, A., Et al., 2007 Group-based Cryptography. Montreal, New York

[6] Tudunkaya, S.M. and Makanjuola, S.O.,2012 Certain construction of finite fields, J. of the Nig. Mathl Phy., vol 22: 95-104

[7] Tudunkaya, S. M. and Makanjuola, S. O.,2013 On the Structure of Rhotrix Rhotrices. J. of the Nig. Mathl Phy., vol. 23: 41-50

[8] Tudunkaya, S. M., 2016 A Construction of Finite Groups. J. of Advanced Maths and Appl., vol. 5(2): 159-165(7)