On the Hill Ciphers of Rhotrices

S. M. Tudunkaya
Department of Science Education
Ahmadu Bello University
Zaria, Kaduna State, Nigeria
Tel.: +2348035727610
Email:tudunkayaunique@yahoo.com

ABSTRACT

When Hill ciphers were described in [16] difficulties in finding the inverse of matrices were noticed to be one of its few disadvantages which made Hill to in [17] suggest the use involutory matrices as keys such that those difficulties were done away with. This reduced drastically the size of the key space of the Hill ciphers which gave rise to another disadvantage. In this paper, Hill ciphers of rhotrices were presented and were found perfectly free from the difficulties of computing inverses (computing inverses of rhotrices is easier than computing those of matrices) and the short comings of decrease in the size of the key space. These contributions, together with the provision of alternative Hill ciphers are the wealth of this paper.

Keywords: Hill Cipher; Modular arithmetic; Integral domain

African Journal of Computing & ICT Reference Format:
S. M. Tudunkaya (2015): On the Hill Ciphers of Rhotrices. Afr J. of Comp & ICTs. Vol 8, No. 2, Issue 2. Pp 109-114

1. INTRODUCTION

The purpose of this paper is to explore the possibilities of applying rhotrices in the area of cryptography. For over a decade [1], an attempt was made to present an element of the set

$$R = \left\{ \left\langle \begin{array}{ccc} & a & \\ b & h(R) & d \\ & e & \end{array} \right\rangle : a, b, c, d, e \in \Re \right\}$$

termed as rhotrix. The element $h(R)$, is called heart.. If $M = \left\langle \begin{array}{ccc} & a & \\ b & h(M) & d \\ & e & \end{array} \right\rangle$ and $N = \left\langle \begin{array}{ccc} & f & \\ g & h(N) & j \\ & k & \end{array} \right\rangle$, then

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

was defined as the addition of two rhotrices. This addition is commutative. The sum

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

the zero of R, implying that $-M$ is the additive inverse of M. Consequently, $(R, +)$ is a commutative group. Scalar multiplication was defined as

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

There are two major methods of rhotrix multiplication but the one used here is

$$M\cdot N=\left(\begin{matrix} & ah(N)+fh(M) & \\ bh(N)+gh(M) & h(N)h(M) & dh(N)+jh(M) \\ & eh(N)+kh(M) & \end{matrix}\right).$$

This multiplication method is commutative, hence the set R is a commutative algebra. The multiplicative identity of R is

$$I=\left(\begin{matrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{matrix}\right).$$

The multiplicative inverse of $M=\left(\begin{matrix} & a & \\ b & h(M) & d \\ & e & \end{matrix}\right)$ is $M^{-1}= -\frac{1}{h(M)^2}\left(\begin{matrix} & a & \\ b & -h(M) & d \\ & e & \end{matrix}\right)$ such that $h(M)^2 \neq 0$.

It is worthwhile to note that the set R is not in any way an integral domain [19](submitted).

The general definition of R appeared in [2] as

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

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. In [13], a the following type of rhotrix named modulo rhotrix was presented;

$$M[R_{Z}{}^{t}]=\left\{\left(\begin{matrix} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & a_t & & & \end{matrix}\right) \forall\, a \in Z_n\right\}$$

Where, addition (+) and multiplication (•) are done modulo n under the addition and multiplication of rhotrices. Also, $\alpha=\frac{n^2-2n+5}{4}$, $\beta=\frac{1}{4}(n^2+3)$, $\pi=\frac{n^2+2n+1}{4}$.

The additive and multiplicative identities of $M[R_z t]$ were respectively given as

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

and

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

where $n = p$, the multiplicative inverse of

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

is

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

such that,

$a_\beta\, b_\beta \equiv 1 \, mod\, p,\; a_1\, b_\beta + b_1\, a_\beta \equiv 0\, mod\, p,\; a_2\, b_\beta + b_2\, a_\beta \equiv 0\, mod\, p$ and so on.

For more on the adopted multiplication method see [4], [5], [6], [7], [8], [9], [2], [11], [12], [13], [14], and [15].

2. HILL CIPHERS OF RHOTRICES

Before the actual description of these ciphers, here are some introductory discussions in accordance with the ideas in [16], [17], and [18]. The whole discussion will be based on the set of integers

$$Z = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}$$

and the set

$$Z_{26} = \{ 1, 2, 3, \ldots, 25, 26 \}$$

The later is for the fact that Hill cipher was based on the English alphabets which are 26 in number. The following assignment was done on these alphabets:

$$A = 1, B = 2, C = 3, D = 4, E = 5, F = 6, G = 7, H = 8, I = 9, J = 10,$$
$$K = 11, L = 12, M = 13, N = 14, O = 15, P = 16, Q = 17, R = 18, S = 19, T = 20,$$
$$U = 21, V = 22, W = 23, X = 24, Y = 25, Z = 26$$

Also, all multiplications are multiplication of rhotrices modulo 26. This method of assignment was adopted in the study for reasons that can be observed by the reader in the forth coming discussions. Rhotrices of size 3 that is rhotrices with $t = 5$ entries were used as this is the smallest size [1], nevertheless, the generalization presented in this paper works for any size n and for any order t of rhotrices. The plaintext will be represented in the column major but row major can also be used. Generally, the rhotrix Hill cipher is of the alphabet length 26 and an integer n. Therefore, the Hill n-cipher is given by a rhotrix A of order t with entries from Z_{26}. To convert a plaintext to a cipher text, the following algorithm was used:

i) Group the plaintext to k smaller groups. Pad the rhotrix with zeros in all unoccupied places. For example, if the plain text is 'BECAUSE' it can be grouped as BEC | AUS | E which can be represented by the following rhotrices:

$$P_1 = \left\langle \begin{array}{ccc} & B & \\ 0 & E & 0 \\ & C & \end{array} \right\rangle$$

$$P_2 = \left\langle \begin{array}{ccc} & A & \\ 0 & U & 0 \\ & S & \end{array} \right\rangle$$

$$P_3 = \left\langle \begin{array}{ccc} & E & \\ 0 & 0 & 0 \\ & 0 & \end{array} \right\rangle$$

ii) Represent each letter by the number assign to it as follows:

$$P_1 = \left\langle \begin{array}{ccc} & 2 & \\ 0 & 5 & 0 \\ & 3 & \end{array} \right\rangle$$

$$P_2 = \left\langle \begin{array}{ccc} & 1 & \\ 0 & 21 & 0 \\ & 19 & \end{array} \right\rangle$$

$$P_3 = \left\langle \begin{array}{ccc} & 5 & \\ 0 & 0 & 0 \\ & 0 & \end{array} \right\rangle$$

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

iii) Compute the product of each of the rhotrices in (ii) above by the key rhotrix K modulo 26 to obtain the ciphertext corresponding to the plaintext under consideration. For instance, suppose

$$K = \left\langle \begin{matrix} & 4 & \\ 2 & 5 & 3 \\ & 6 & \end{matrix} \right\rangle$$

Note that in choosing K one has to be careful about the choice of the heart because Z_{26} is not an integral domain. In other words, the greatest common divisor of the heart of $K$and 26 must be 1 so that the key space becomes only the set of all rhotrices of order t that are invertible over Z_{26}. This means, the heart of the key rhotrix must be relatively prime to 26.

Now, going back to the computation of the cipher text the decryption function $C = KP_1$ should be used. That is

$$C = KP_1 = \left\langle \begin{matrix} & 4 & \\ 2 & 5 & 3 \\ & 6 & \end{matrix} \right\rangle \left\langle \begin{matrix} & 2 & \\ 0 & 5 & 0 \\ & 3 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 4 & \\ 10 & 25 & 15 \\ & 19 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & D & \\ I & Y & O \\ & S & \end{matrix} \right\rangle$$

which does not have to make sense to any non-stakeholder.

iv) The function $K^{-1}C = P_1$ should be computed to decrypt (to retrieve the plain text). But from section 1,

$$K^{-1} = -\frac{1}{5^2} \left\langle \begin{matrix} & 4 & \\ 2 & -5 & 3 \\ & 6 & \end{matrix} \right\rangle$$

dividing by the square of five and multiplying by the square of its multiplicative inverse modulo 26 are the same and

$1^{-1} = 1$
$3^{-1} = 9$
$5^{-1} = 21$
$7^{-1} = 15$
$11^{-1} = 19$
$17^{-1} = 23$
$25^{-1} = 25$

Moreover,

▪
▪
▪
$29 \equiv 3$
$28 \equiv 2$
$27 \equiv 1$
$26 \equiv 0$
$25 \equiv -1$
$24 \equiv -2$
$23 \equiv -3$
▪
▪
▪

Therefore, $K^{-1} = \left\langle \begin{matrix} & 4 & \\ 2 & 21 & 3 \\ & 6 & \end{matrix} \right\rangle$ and hence $P_1 = K^{-1}C = \left\langle \begin{matrix} & 4 & \\ 2 & 21 & 3 \\ & 6 & \end{matrix} \right\rangle \left\langle \begin{matrix} & 4 & \\ 10 & 25 & 15 \\ & 19 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & 2 & \\ 0 & 5 & 0 \\ & 3 & \end{matrix} \right\rangle = \left\langle \begin{matrix} & B & \\ 0 & E & 0 \\ & C & \end{matrix} \right\rangle$

Now, it's time to generalize the Hill cipher.

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

3. GENERALIZED HILL CIPHERS OF RHOTRICES

Denote by $RL(t, Z_m)$ the set of all invertible rhotrices over Z_m of order t. Using the natural correspondence, a plaintext string over an alphabet of order m is represented as a vector over Z_m in either a column-major or a row-major, this vector is denoted as a rhotrix P of size t which is padded by zeros in the position of entries where there are no letters. Suppose a rhotrix $K \in RL(t, Z_m)$ is chosen to be the key rhotrix, to encrypt, compute

$C = e_k(P) = KP$

Also, represent this product (KP) as a string over the same alphabet and send or keep depending on the need. To decrypt, compute

$P = d_k(C) = K^{-1}C.$

4. CONCLUSION

This paper introduced the Hill ciphers of rhotrices. These Hill ciphers have the advantage of rich key space and easier computation of inverses. The first section of the paper covered the algebra of rhotrices to equip the reader with basic concepts and operations of rhotrices. In the second section, discussions were given on the Hill ciphers of rhotrices and finally, generalization of the Hill ciphers was presented in section three. It is hoped that the contributions of this paper will open a new chapter in the application of algebra in cryptography.

REFERENCES

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

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

[3] Tudunkaya, S.M. and Makanjuola, S.O., Certain Construction of Finite Fields, J. of the Nig. Mathl Phy., vol 22: 95-104 (2012)

[4] Ezugwu, E. A., Et al., The Concept of Heart-oriented Rhotrix Multiplication, Global journal of science frontier research, 11:35-46 (2011)

[5] Mohammed, A. Enrichment Exercise through Extension to Rhotrices, Int. J. Math. Sci. Technol., vol. 38: 131-136 (2007)

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

[7] Mohammed, A., Rhotrices and their Applications in Enrichment of Mathematical Algebra, Proceedings of the third international conference on Mathematical sciences (Alain, United Arab Emirates:ICM2008), vol. 1: 145-154 (2008)

[8] Mohammed, A., A Remark on the Classification of Rhotrices as Abstract Structures, International journal of physical science, vol. 4(9): 496-499 (2009)

[9] Mohammed, A. and Tijjani, A.A., Rhotrix Topological Spaces. International journal of advances in science and technology, vol. 2: 41-47 (2011)

[10] Mohammed, A., On the Construction of Rhomtrees as Graphical Representation of Rhotrices, Notes on Number Theory and Discrete Maths., vol. 17(1): 21-29 (2011)

[11] Mohammed, A., Et al., On Generalization and Algorithmatization of the Heart-Based Method for Multiplication of Rhotrices, International journal of Computer Information Systems, vol. 1(2):46-49 (2011)

[12] Tudunkaya, S.M. and Makanjuola, S.O., Certain Fields and Field Extensions, Asian journal of mathematics and computer science, vol. 7(4): 332-344 (2015)

[13] Tudunkaya, S.M. and Makanjuola, S.O., Certain Quadratic Extensions, J. of the Nig. Mathl Phy., vol. 21: 271-280 (2012)

[14] Tudunkaya, S.M., Rhotrix Polynomials and Polynomial Rhotrices, Pure and Applied Math Journal, 1(1): 1-4 (2013)

[15] Usaini, S. and Tudunkaya, S.M., Note on Certain field of fractions, Global journal of science frontier research, 7(7): 75-81 (2012)

[16] Hill, L.S., Cryptography in an Algebraic Alphabet. Am. Math. Mon., 36: 306-312 (1929)

[17] Hill, L.S., Concerning Certain Linear Transformation Apparatus of Cryptography. Am. Math. Mon., 38: 135-154 (1931)

[18] [18] Overbey J., Traves W., and Wojdylo J., On the Key space of the Hill Cipher. Cryptologia., 29(1): 59-72 (2005)