Vol 8. No. 2 Issue 2 – August, 2015
African Journal of Computing & ICT

www.ajocict.net

Design of the Affine Ciphers of Rhotrices

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

ABSTRACT

This paper presented a new way in the implementation of affine ciphers. These ciphers have the advantage of rich key space and easier way of computing inverses. Moreover, the multiplication here (of rhotrices) is commutative which may serve as another advantage. Some basic concepts in rhotrices were given to acquaint the reader with what is needed basically to grasp the content of the paper.

Keywords: Group; Cryptography; Affine Cipher

African Journal of Computing & ICT Reference Format:
S. M. Tudunkaya (2015) Design of the Affine Ciphers of Rhotrices. Afr J. of Comp & ICTs. Vol 8, No. 2, Issue 2. Pp 79-82

1. INTRODUCTION

In [1], an entity $A = \left\langle \begin{matrix} & a & \\ b & h(A) & d \\ & e & \end{matrix} \right\rangle \in R$ where $a, b, c, d, e \in \Re$ was introduced as rhotrix.

The entry $h(A)$ is called heart.

The sum

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

was defined as the addition of two rhotrices and it is commutative.

By this definition of addition, the additive inverse of $A = \left\langle \begin{matrix} & a & \\ b & h(A) & d \\ & e & \end{matrix} \right\rangle$ is $-A = -\left\langle \begin{matrix} & a & \\ b & h(A) & d \\ & e & \end{matrix} \right\rangle$.

The zero of R was given by $0 = \left\langle \begin{matrix} & 0 & \\ 0 & 0 & 0 \\ & 0 & \end{matrix} \right\rangle$ and was termed the zero rhotrix. The ordered pair $(R, +)$ is a commutative group.

Scalar multiplication was given as

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

The multiplication of two rhotrices A and B was given by

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

This multiplication method is also commutative and was adopted in this paper. The identity of R with respect to this multiplication is

$I = \left\langle \begin{matrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{matrix} \right\rangle$. The Multiplicative inverse of $A = \left\langle \begin{matrix} & a & \\ b & h(A) & d \\ & e & \end{matrix} \right\rangle$ is

$A^{-1} = -\frac{1}{h(A)^2} \left\langle \begin{matrix} & a & \\ b & -h(A) & d \\ & e & \end{matrix} \right\rangle$ such that $h(A)^2 \neq 0$.

The set R is not an integral domain [20]. In Mohammed [2], a generalised definition of a rhotrix R of dimension n with the operations defined above, was presented as the set

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

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

Vol 8. No. 2 Issue 2 – August, 2015
African Journal of Computing & ICT

www.ajocict.net

In [16], modulo rhotrix was introduced as a rhotrix in form of

$$M[R_3t] = \left\{ \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & a_t & & & \end{array} \right\rangle \forall a \in Z_n \right\}$$

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 identity is

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

The multiplicative identity is

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

And if $n = p$, 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,

$$a_\beta\, b_\beta \equiv 1 \bmod p$$
$$a_1\, b_\beta + b_1\, a_\beta \equiv 0 \bmod p$$
$$a_2\, b_\beta + b_2\, a_\beta \equiv 0 \bmod p$$
$$a_3\, b_\beta + b_3\, a_\beta \equiv 0 \bmod p$$
$$a_4\, b_\beta + b_4\, a_\beta \equiv 0 \bmod p$$
...
...
...
$$a_{t-3}\, b_\beta + b_{t-3}\, a_\beta \equiv 0 \bmod p$$
$$a_{t-2}\, b_\beta + b_{t-2}\, a_\beta \equiv 0 \bmod p$$
$$a_{t-1}\, b_\beta + b_{t-1}\, a_\beta \equiv 0 \bmod p$$
$$a_t\, b_\beta + b_t\, a_\beta \equiv 0 \bmod p$$

Various works have been conducted on rhotrices with the aid of the adopted multiplication method which can be found in [2, 5-7]. More studies have been conducted in the areas of algebra and that of mathematical analysis which appeared in [8- 13, 15-19].

2. RHOTRIX AFFINE CIPHERS (LINEAR CIPHERS)

Some discussions and ideas from [3-4, 13-14] have been useful here. The letter A was represented by the number 1, B by the number 2, C by the number 3 and so on, where lastly Z was represented by 0. Arithmetic operations were done modulo 26. The discussion holds on rhotrices of any size but here rhotrices where t = 5 were used. To encrypt, let

$Y = AX + B$ (mod 26) such that X and Y are input (plain text) and output (cipher text) rhotrices of t entries. A is a fixed key invertible rhotrix also B is a fixed key rhotrix. To decrypt there we compute

$X = A^{-1}(Y - B)$ (mod 26) such that A^{-1} is the inverse of A in the key space $RL(5, Z_{26})$, the set of all rhotrices of order $t=5$ that are invertible over Z_{26} mod 26. In other words, the encryption keys are A, B and those of decryption are A^{-1}, $-B$ respectively. Clearly, the Hill cipher is a special case of the affine cipher where B is the zero rhotrix. The plaintext was represented in the column major throughout the study but row major can also be used.

3. ALGORITHM

Represent the plaintext and cipher text by numbers from Z_{26} according to the allocation used in the above section. Let

$$A = \begin{pmatrix} & x_1 & \\ x_2 & h(A) & x_4 \\ & x_5 & \end{pmatrix}$$

and

$$B = \begin{pmatrix} & y_1 & \\ y_2 & h(A) & y_4 \\ & y_5 & \end{pmatrix}$$

Where $x_1, h(A), h(B) \in Z_{26}$ such that
$\kappa = \{(A, B) \in Z(R)_{26} \times Z(R)_{26} : gcd(h(A), 26) = 1\}$

For $K = A, B) \in \kappa$, define the functions
$Y = AX + B$ (mod 26)
and
$X = A^{-1}(Y - B)$ (mod 26)

4. IMPLEMENTATION

The illustration of the affine cipher as stated above is of the alphabet length 26, an invertible rhotrix A of order t and a rhotrix B both with entries from Z_{26}. Plaintext can be transform to a cipher text, by grouping the plain text to k smaller groups and padding the plaintext rhotrix with zeros in all the vacant places. For instance, suppose the plaintext under consideration is 'COMPUTED' it can be broken as COM I PUT I ED and represented in rhotrix form as follows:

$$X_1 = \begin{pmatrix} & C & \\ 0 & O & 0 \\ & M & \end{pmatrix}$$

$$X_2 = \begin{pmatrix} & P & \\ 0 & U & 0 \\ & T & \end{pmatrix}$$

$$X_3 = \begin{pmatrix} & E & \\ 0 & D & 0 \\ & 0 & \end{pmatrix}$$

If the above representation is used,

$$X_1 = \begin{pmatrix} & 3 & \\ 0 & 15 & 0 \\ & 13 & \end{pmatrix}$$

$$X_2 = \begin{pmatrix} & 16 & \\ 0 & 21 & 0 \\ & 20 & \end{pmatrix}$$

$$X_3 = \begin{pmatrix} & 5 & \\ 0 & 4 & 0 \\ & 0 & \end{pmatrix}$$

Computing the product of each of the rhotrices above by the key rhotrix A modulo 26 and adding it to rhotrix B we obtain the cipher text Y. For example, suppose

$$A = \begin{pmatrix} & 3 & \\ 2 & 11 & 3 \\ & 9 & \end{pmatrix}$$

And

$$B = \begin{pmatrix} & 0 & \\ 5 & 13 & 8 \\ & 19 & \end{pmatrix}$$

The cipher text for X_1 is

$$Y = AX_1 + B = \begin{pmatrix} & 3 & \\ 2 & 11 & 3 \\ & 9 & \end{pmatrix}\begin{pmatrix} & 3 & \\ 0 & 15 & 0 \\ & 13 & \end{pmatrix} + \begin{pmatrix} & 0 & \\ 5 & 13 & 8 \\ & 19 & \end{pmatrix}$$

$$= \begin{pmatrix} & 0 & \\ 4 & 9 & 19 \\ & 18 & \end{pmatrix} + \begin{pmatrix} & 0 & \\ 5 & 13 & 8 \\ & 19 & \end{pmatrix} = \begin{pmatrix} & 0 & \\ 9 & 22 & 1 \\ & 11 & \end{pmatrix}$$

$$= \begin{pmatrix} & Z & \\ I & V & A \\ & K & \end{pmatrix}$$

Now, to decrypt this message, compute
$X = A^{-1}(Y - B)$ (mod 26)

But from the review in section one,

$$A^{-1} = -\frac{-1}{11^2}\begin{pmatrix} & 3 & \\ 2 & -11 & 3 \\ & 9 & \end{pmatrix}$$

African Journal of Computing & ICT

www.ajocict.net

And from the fact that dividing by the square of eleven is the same as multiplying by the square of its multiplicative inverse modulo 26, and also,

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

Moreover,
$\ldots, 29 \equiv 3, 28 \equiv 2, 27 \equiv 1, 26 \equiv 0, 25 \equiv -1, 24 \equiv -2, 23 \equiv -3, \ldots$

Combining these facts

$$A^{-1} = -\left\langle \begin{matrix} & 9 & \\ 6 & 19 & 9 \\ & 1 & \end{matrix} \right\rangle$$

It can be checked that
$X = A^{-1}(Y - B) \pmod{26}$

5. CONCLUSION

This paper proposed the affine ciphers of rhotrices. These ciphers have some advantages over those of matrices as the commutativity in terms of multiplication, rich key space and simplicity in the computation of inverses. In the first section, an introduction which covers the algebra of rhotrices was given followed by the description of the affine ciphers in section two. The algorithm and implementation of these ciphers were presented under sections three and four respectively. In other words, sections two, three and four contained the main contributions of the paper.

REFERENCES

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

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

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

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

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

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

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

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

[13] Mokhtari, M. and Naragi, H., Analysis and Design of Affine and Hill Ciphers. Journal of Mathematics Research, 4(1): 67-77 (2012)

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

[15] Tudunkaya, S.M., Rhotrix Polynomials and Polynomial Rhotrices, Pure and applied math journal, 1(1): 1-4 (2013)

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

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

[18] 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)

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