IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EXTENSION OF HILL CIPHER USING RHOTRICES

Satish Kumar
Assistant Professor
Department of Mathematics
Govt. Degree College Dharampur (H.P.) India

Abstract: In the classical cryptography the basic Hill cipher is vulnerable to plain text attack due to symmetric key substitution algorithm which based upon the matrix multiplication which is not secure. This paper illustrates extension of Hill Cipher using the rhotrices with heart oriented multiplication.

Keywords*:* Plain text, symmetric key, Rhotrices, Invertible, encryption, decryption, message.
MSC 2010. : 11T71, 15A09, 14G50

I. INTRODUCTION

Cryptography is the study of building ciphers to ensure the confidentially and integrity of information. With the advent of e-commerce and electronic transactions, the need for development of secured system has grown tremendously. This paper describes an activity build around one of the techniques that illustrates on security of Hill cipher using rhotrices. The method involves the concept rhotrices of which one is used to encrypt the plaintext and the other one to decrypt the cipher text. The characters, in the original message or stream are assigned numerical values and the rhotrix must be invertible for use in decryption. The proposed method is very simple representing great potential age is done confidentially. We mathematically analyze some problems from the field of theory of rhotrices. In this context we study the basic properties of rhotrices and investigate some application of rhotrices in cryptography. The study of the problem involves the multiplication of two rhotrices and its basic properties and relationship between invertible rhotrices and associated non-singular rhotrices. The concept of Secure communication & Digital signature verification through RSA discussed by Kumar and Sharma (2013). Rhotrix is a new concept introduced in the literature of mathematics (Ajibade 2003). It is a mathematical object which is in some way between 2×2 - dimensional and 3×3 - dimensional matrices. A rhotrix of dimension 3 is defined as

$$P_3 = \left\langle \begin{array}{ccc} & a_1 & \\ a_2 & a_3 & a_4 \\ & a_5 & \end{array} \right\rangle$$

where $a_1, a_2, a_3, a_4, a_5 \in \mathrm{R}$.

The investigations on rhotrices were given by various authors viz. concept of heart-oriented rhotrix multiplication (Absalom et al, 2011), natural rhotrix (Isere , 2016), Rhotrix to a coupled matrix, (Sani 2018) linear system over rhotrices, circulent rhotrisces, circulent –like, cauchy rhotrices, Sylvester, toeplitz rhotrices over finite fields (Sharma et al, 2015, Sharma et al, 2017, Sharma 2017ab, Sharma and Gupta 2017), On the linear systems over non commutative rhotrices (Okon et al, 2018), even dimensional rhotrix (Isere 2018), general rhotrix (Aminu and Michael 2015) and rhotrix system of equation (Aminu 2009, 2012). On constructions of MDS matrices from companion matrices for lightweight cryptography is discussed by Gupta and Ray (2013). On constructions of MDS matrices from circulant-like matrices for lightweight cryptography discussed by Gupta and Ray (2014). On generalization and algorithmatization of heart-based method for multiplication of rhotrices given by Mohammed *et al.* (2011). An alternative method for multiplication of rhotrices discussed by Sani (2004). Theoretical development and applications of rhotrices, Ph. D. Thesis is prescribed by Mohammed (2011). The row-column multiplication for high dimensional rhotrices is discussed by Sani (2007). On construction of involuntary MDS matrices from Vandermonde matrices is given by Sajadieh et al. (2012). Algebra and analysis of rhotrices is discussed in literature (Sharma and Kanwar 2013, Sharma and Kumar 2013, Sharma and Kumar 2014 abc, Sharma et al, 2013 ab, Sharma et al, 2014, Sharma et al, 2015ab). Applications of Hill Cipher algorithm in securing text messages discussed in (Siahaan and Siahaan 2018).

II. HIGHER DIMENSIONAL RHOTRICES:

Ezugwu et al. (2011) introduces the concept of heart –oriented rhotrix multiplication and the the n–dimensional rhotrix represented as

$$R_n = \left\langle \begin{array}{ccccccccc} & & & & a_1 & & & & \\ & & & a_2 & a_3 & a_4 & & & \\ & & a_{31} & a_6 & a_7 & a_8 & a_9 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_{\frac{1}{4}(n^2+3)-\frac{n-1}{2}} & \cdots & \cdots & \cdots & a_{\frac{1}{4}(n^2+3)} & \cdots & \cdots & \cdots & a_{\frac{1}{4}(n^2+3)+\frac{n-1}{2}} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & a_{\frac{1}{2}(n^2+1)-8} & a_{\frac{1}{2}(n^2+1)-7} & a_{\frac{1}{2}(n^2+1)-6} & a_{\frac{1}{2}(n^2+1)-5} & a_{\frac{1}{2}(n^2+1)-4} & & \\ & & & a_{\frac{1}{2}(n^2+1)-3} & a_{\frac{1}{2}(n^2+1)-2} & a_{\frac{1}{2}(n^2+1)-1} & & & \\ & & & & a_{\frac{1}{2}(n^2+1)} & & & & \end{array} \right\rangle$$

REMARK-1: The total number of entries in a rhotrix R_n is equal to $\dfrac{n^2+1}{2}$.

A. HEART ORIENTED MULTIPLICATION:

$$P_3 = \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle$$

and

$$Q_3 = \left\langle \begin{array}{ccc} & p & \\ q & r & s \\ & t & \end{array} \right\rangle$$

be any two 3–dimensional rhotrices, then their heart oriented multiplication is defined as

$$P_3 \circ Q_3 = \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle \circ \left\langle \begin{array}{ccc} & p & \\ q & r & s \\ & t & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & ar+pc & \\ br+qc & cr & dr+sc \\ & er+tc & \end{array} \right\rangle \qquad (2.0.2)$$

B. INVERSE OF A RHOTRIX UNDER HEART ORIENTED MULTIPLICATION:

Let P be a 3–dimensional rhotrix and $h(P) \neq 0$. If there exists a rhotrix Q such that

$$P \circ Q = Q \circ P = \mathrm{I},$$

then Q is called the inverse of P.

$$Q = P^{-1} = \frac{-1}{c^2} \left\langle \begin{array}{ccc} & a & \\ b & -c & d \\ & e & \end{array} \right\rangle$$

Table 1

Numerical values for alphabets and some symbols used in the Paper

A	B	C	D	E	F
-1	0	1	2	3	4
G	H	I	J	K	L
5	6	7	8	9	10
M	N	O	P	Q	R
11	12	13	14	15	16
S	T	U	V	W	X
17	18	19	20	21	22
Y	Z	[	/	^	@
23	24	25	26	27	28

C. ALGORITHM OF PROPOSED CRYPTOSYSTEM

ENCRYPTION

1. Converting the message M_1 of length L in to a stream of numerals using a user friendly scheme for both the sender and receiver.
2. Place the numerals in to a rhotrix of order $n \supseteq L$ where n depends on the size of the message and call it as a message rhotrix and L is length of stream numerals.
3. Multiply this message by the encrypted rhotrix of the size n (normally a induced diagonal rhotrix compatible for the product $G = MK$) and got the encrypted rhotrix G .
4. Converting the message of length L in to a stream of numbers consisting of encrypted message and send to receiver.

DECRYPTION

1. Place the encrypted stream of numbers that represent the encrypted message in to a rhotrix.
2. Multiply the enccrypted rhotrix of numbers with the G with the decoder K^{-1} (the inverse of K) to go back the message rhotrix M.
3. Converting message rhotrix in to a stream of numbers with the help of originally used scheme.
4. Converting this stream of numerals in to text of the original message.

D. ILLUSTRATION

Let us consider the message which is to be sent on the insecure channel is
HIMACHALPRADESHUNIVERSITY

Step1. Sender considers the non singular rhotix of order seven K and shares it with receiver.

$$K_1 = \left\langle \begin{array}{ccccccc} & & & 8 & & & \\ & & 9 & 10 & 11 & & \\ & 12 & 13 & 14 & 15 & 16 & \\ 6 & 5 & 4 & 1 & 0 & 2 & 3 \\ & 17 & 18 & 19 & 20 & 21 & \\ & & 22 & 23 & 24 & & \\ & & & 25 & & & \end{array} \right\rangle$$

Step 2. Sender converts the above plain text in to numerical values using Table 1 which gives 6 7 11 -1 1 6 -1 10 14 16 -1 2 3 1 17 6 19 12 7 20 3 16 17 7 18 23 . Now we rearrange these numbers in to a rhotrix .

$$M = \left\langle \begin{array}{ccccccc} & & & 6 & & & \\ & & 7 & 11 & -1 & & \\ & 1 & 6 & -1 & 10 & 14 & \\ 16 & -1 & 2 & 3 & 17 & 6 & 19 \\ & 12 & 7 & 20 & 3 & 16 & \\ & & 17 & 7 & 18 & & \\ & & & 23 & & & \end{array} \right\rangle$$

Step 3. Multiply this message M by the rhotrix of the size 7 compatible for the product $G = MK$ and got the encrypted rhotrix G_1.

$$MK = \left\langle \begin{array}{ccccccc} & & & 30 & & & \\ & & 34 & 41 & 32 & & \\ & 37 & 45 & 41 & 55 & 62 & \\ 34 & 14 & 14 & 3 & 17 & 12 & 28 \\ & 63 & 61 & 77 & 63 & 79 & \\ & & 83 & 76 & 90 & & \\ & & & 98 & & & \end{array} \right\rangle = G(say)$$

Step 4. The encrypted numeric message to be sent to the receiver

30 34 41 32 37 45 41 55 62 34 14 14 3 17 12 28 63 61 77 63 79 83 76 90 98

DECRYPTION

Step 1. Place the encrypted stream of numbers that represent the encrypted message in to a rhotrix.

$$MK = \left\langle \begin{array}{ccccccc} & & & 30 & & & \\ & & 34 & 41 & 32 & & \\ & 37 & 45 & 41 & 55 & 62 & \\ 34 & 14 & 14 & 3 & 17 & 12 & 28 \\ & 63 & 61 & 77 & 63 & 79 & \\ & & 83 & 76 & 90 & & \\ & & & 98 & & & \end{array} \right\rangle = G(say)$$

Step 2. After receiving the encrypted message from the sender, receiver find the inverse of the sharing key

$$K^{-1} = \left\langle \begin{array}{ccccccc} & & & -8 & & & \\ & & -9 & -10 & -11 & & \\ & -12 & -13 & -14 & -15 & -16 & \\ -6 & -5 & -4 & 1 & -0 & -2 & -3 \\ & -17 & -18 & -19 & -20 & -21 & \\ & & -22 & -23 & -24 & & \\ & & & -25 & & & \end{array} \right\rangle$$

Step 3. Receiver multiply the rhotrix G with the with the inverse of the key $\boldsymbol{K}$.

$$GK^{-1} = \left\langle \begin{array}{ccccccc} & & & 6 & & & \\ & & 7 & 11 & -1 & & \\ & 1 & 6 & -1 & 10 & 14 & \\ 16 & -1 & 2 & 3 & 17 & 6 & 19 \\ & 12 & 7 & 20 & 3 & 16 & \\ & & 17 & 7 & 18 & & \\ & & & 23 & & & \end{array} \right\rangle$$

Step 4. Now receiver decrypt the message 6 7 11 -1 1 6 -1 10 14 16 -1 2 3 1 17 6 19 12 7 20 3 16 17 7 18 23 with the Table 1 and get original message **HIMACHALPRADESH UNIVERSITY.**

III. CONCLUSION

The proposed cryptosystem is based upon the rhotrices multiplication , which is extension of the original Hill cipher. This result is still open for the researchers in future studyof rhotrices if we use of matrix multiplication of the rhotrices instead of heart oriented multiplication.

DISCLOSURE

The authors declare no conflict of interest. The findings included in this manuscript are our own and are neither published nor under consideration for publication elsewhere.

ACKNOWLEDGMENT

The authors wish to thankful to anonymous reviewers for valuable suggestions to improve the quality of paper.

REFERENCES

1. Absalom, E. E, Sani, B. and Sahalu, B. J. 2011. The concept of heart-oriented rhotrix multiplication. Global J. Sci. Fro. Research, vol-11(2), pp. 35-42.
2. Ajibade, A. O. 2003.The concept of rhotrices in mathematical enrichment. Int. J. Math. Educ. Sci. Tech., vol-34(2), pp. 175-179.
3. Aminu, A. 2009. On the linear system over rhotrices. Notes on Number Theory and Discrete Mathematics, vol-15, pp. 7-12.
4. Aminu, A. 2012. A note on the rhotrix system of equation. Journal of the Nigerian association of Mathematical Physics, vol-21,pp. 289-296.
5. Aminu, A. and Michael, O. 2015. An introduction to the concept of paraletrix, a generalization of rhotrix. Journal of the African Mathematical Union & Springer Verla,vol- 26(5-6), pp. 871-885.
6. Ezugwu E. A., Sani, B. and Junaidu, B. S. 2011. The concept of Heart Oriented Rhotrix Multiplication. Global Journal of Science Frontier Research , XI(2), pp. 35-46.
7. Gupta, K. C., and Ray, I. G. 2013. On constructions of MDS matrices from companion matrices for lightweight cryptography. Cryptography Security Engineering and Intelligence Informatics, 8128.
8. Gupta, K. C., and Ray, I. G. 2014. On constructions of MDS matrices from circulant-like matrices for lightweight cryptography .ASU, (1).
9. Isere, A. O. 2016. Natural rhotrix. Cogent Mathematics, 3:1246074.
10. Isere, A.O. 2018. Even dimensional rhotrix. *Notes on Number Theory and Discrete Mathematics*, vol-24(2), pp. 125–133, 2018.
11. Kumar, S. and Sharma, P. L. 2013. Secure communication & Digital signature verification through RSA. International Journal of Computer Science & Information Technology Research Excellence, vol-3(2), pp. 10-16.
12. Mohammed, A. 2011. Theoretical development and applications of rhotrices. Ph. D. Thesis. Ahmadu Bello University Zaria.
13. Mohammed, A., Ezugwu, E. A. and Sani, B. 2011. On generalization and algorithmatization of heart-based method for multiplication of rhotrices. Information System, vol-2, pp. 46-49.
14. Okon, U. E., Galadima, D.J. and Malachy, M. 2018. On the linear systems over non commutative rhotrices, International organization of scientific research – Journal of mathematics, (ISOR-JM) vol-14(3), pp. 68-72.
15. Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. 2012. On construction of involutry MDS matrices from Vandermonde matrices. Des. Codes and Cry., vol-64, 2012 pp. 287-308.
16. Sani, B. 2007. The row-column multiplication for high dimensional rhotrices. Int. J. Math. Educ. Sci. Technol, vol-38,2007, pp. 657-662.
17. Sani, B. 2018 .Conversion of a rhotrix to a coupled matrix. Int. J. Math. Educ. Sci. Technol, vol-39, pp. 244-249.
18. Sani, B.2004. An alternative method for multiplication of rhotrices. Int. J. Math. Educ. Sci. Tech., vol-35(5), pp. 777-781.
19. Sharma, P. L. and Gupta, S. 2017. Constructions of maximum distance seperable toeplitz rhotrices over finite fields. Journal of Combinatorics, Information & system Sciences, vol-42(1-4), pp. 1-22.

20. Sharma, P. L. and Kanwar, R. K. 2013. On involuntary and pascal rhotrices. International J. of Math. Sci. & Engg. Appls. (IJMSEA), vol-7(IV), pp. 133-146.
21. Sharma, P. L. and Kumar, S. 2013. On construction of MDS rhotrices. International Journal of Mathematical Sciences. vol-12 (3-4), pp. 271-286.
22. Sharma, P. L. and Kumar, S. 2014a. Some applications of Hadamard rhotrices to design balanced incomplete block. International J. of Math. Sci. & Engg. Appls. (IJMSEA), vol-8(2), 389-404.
23. Sharma, P. L. and Kumar, S. 2014b. Balanced incomplete block design (BIBD) using Hadamard rhotrices. International J. Technology, vol-4(1), pp. 62-66.
24. Sharma, P. L. and Kumar, S. 2014c. On special type of Vandermonde rhotrix and its decompositions. Recent Trends in Algebra and Mechanics, Indo-American Books Publisher New Delhi, pp. 33-40.
25. Sharma, P. L., Gupta, S. and Dhiman, N. 2017a. Sylvester rhotrices and their properties over finite fields. Bulletin of pure and applied sciences, vol- 36 (1), pp. 70-80.
26. Sharma, P. L., Gupta, S. and Dhiman, N. 2017b. On construction of maximum distance separable rhotrices using Cauchy rhotrices over finite fields. International Journal of computer applications, vol -36(1), pp. 70-80.
27. Sharma, P. L., Gupta, S. and Rehan, M. 2015. Constructions of MDS rhotrices using special type of circulent rhotrices over finite fileds. HPU J., vol- 3, pp 25-43.
28. Sharma, P. L., Gupta, S. and Rehan, M. 2017. On Circulent –like- rhotrices over finite fields. Applications and Applied Mathematics, An international journal (AAM). vol-12(1), pp. 506-520.
29. Sharma, P. L., Kumar, S. and Rehan, M. 2013a. On Hadamard rhotrix over finite field," *Bulletin of Pure and Applied Sciences*, vol-32 E (2) (Math & Stat.), pp. 181-190.
30. Sharma, P. L., Kumar, S. and Rehan, M. 2013b. On Vandermonde and MDS rhotrices over GF(2q). International Journal of Mathematics and Analysis, vol- 5(2), pp. 143-160.
31. Sharma, P. L., Kumar, S. and Rehan, M. 2014. On Construction of Hadamard Codes Using Hadamard Rhotrices. International Journal of Theoretical & Applied Sciences vol-6(1), pp.102-111.
32. Sharma, P. L., Kumar, S. and Rehan, M. 2015. On factorization of a special type of vandermonde rhotrix. Applications and Applied Mathematics, An International Journal (AAM), vol-10(1), pp. 421 – 439.
33. Siahaan, M. D. L. and Siahaan, A. P. U. 2018. Applications of Hill Cipher Algorithm in Securing Text Messages. International Journal For Innovative Research Multidisciplinary Field, vol-4.