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 involv

II. HIGHER DIMENSIONAL RHOTRICES:

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

$$
R_n = \begin{pmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n1} & a_{n2} & \cdots & a_{nn} \\
  a_{2n+1} & a_{2n+2} & \cdots & a_{2n+n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n2n+1} & a_{n2n+2} & \cdots & a_{n2n+n} \\
  a_{n2n+2} & a_{n2n+3} & \cdots & a_{n2n+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n}+1} & a_{n^{2n}+2} & \cdots & a_{n^{2n}+n} \\
  a_{n^{2n}+2} & a_{n^{2n}+3} & \cdots & a_{n^{2n}+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n}+n} & a_{n^{2n}+2n} & \cdots & a_{n^{2n}+n^{2n}} \\
  a_{n^{2n}+n} & a_{n^{2n}+2n} & \cdots & a_{n^{2n}+n^{2n}} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2}+1} & a_{n^{2n^2}+2} & \cdots & a_{n^{2n^2}+n} \\
  a_{n^{2n^2}+2} & a_{n^{2n^2}+3} & \cdots & a_{n^{2n^2}+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2}+n} & a_{n^{2n^2}+2n} & \cdots & a_{n^{2n^2}+n^{2n}} \\
  a_{n^{2n^2}+n} & a_{n^{2n^2}+2n} & \cdots & a_{n^{2n^2}+n^{2n}} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2}n} & a_{n^{2n^2}n+1} & \cdots & a_{n^{2n^2}n+n} \\
  a_{n^{2n^2}n+1} & a_{n^{2n^2}n+2} & \cdots & a_{n^{2n^2}n+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2n}+1} & a_{n^{2n^2n}+2} & \cdots & a_{n^{2n^2n}+n} \\
  a_{n^{2n^2n}+2} & a_{n^{2n^2n}+3} & \cdots & a_{n^{2n^2n}+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2n^2}+1} & a_{n^{2n^2n^2}+2} & \cdots & a_{n^{2n^2n^2}+n} \\
  a_{n^{2n^2n^2}+2} & a_{n^{2n^2n^2}+3} & \cdots & a_{n^{2n^2n^2}+2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n^{2n^2n^2}n} & a_{n^{2n^2n^2}n+1} & \cdots & a_{n^{2n^2n^2}n+n}
\end{pmatrix}
$$

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

A. HEART ORIENTED MULTIPLICATION:

and

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

$$
P_3 \circ Q_3 = \begin{pmatrix}
  a & b & c & d \\
  e & f & g & h \\
  i & j & k & l \\
\end{pmatrix} \circ \begin{pmatrix}
  p & q & r & s \\
  t & u & v & w \\
  x & y & z & \sigma \\
\end{pmatrix} = \begin{pmatrix}
  ar + pe & br + qc & cr + dr + sc & er + tc \\
  aq + pe & bq + qc & cq + dr + sc & eq + tc \\
  aq + pe & bq + qc & cq + dr + sc & eq + tc \\
\end{pmatrix}
$$

(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

$$
P \circ Q = Q \circ P = I,
$$

then $Q$ is called the inverse of $P$.

$$
Q = P^{-1} = \frac{-1}{c^3} \begin{pmatrix}
  a & b & c \\
  e & f & g \\
  i & j & k
\end{pmatrix}
$$
Table 1
Numerical values for alphabets and some symbols used in the Paper

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

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 \( n \geq L \) 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 encrypted 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

Step 1. Sender considers the non singular rhotix of order seven \( K \) and shares it with receiver.

\[
K = \begin{bmatrix}
8 & 9 & 10 & 11 \\
12 & 13 & 14 & 15 & 16 \\
6 & 5 & 4 & 1 & 0 & 2 & 3 \\
17 & 18 & 19 & 20 & 21 \\
22 & 23 & 24 \\
25
\end{bmatrix}
\]

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

\[
M = \begin{pmatrix}
6 & 7 & 11 & -1 \\
1 & 6 & -1 & 10 & 14 \\
16 & -1 & 2 & 3 & 17 & 6 & 19 \\
12 & 7 & 20 & 3 & 16 \\
17 & 7 & 18 \\
23
\end{pmatrix}
\]

\[
MK = \begin{pmatrix}
30 & 34 & 41 & 32 \\
37 & 45 & 41 & 55 & 62 \\
34 & 14 & 14 & 3 & 17 & 12 & 28 \\
63 & 61 & 77 & 63 & 79 \\
83 & 76 & 90 \\
98
\end{pmatrix} = G(\text{say})
\]

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

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

**DECRIPTION**

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

\[
MK = \begin{pmatrix}
30 & 34 & 41 & 32 \\
37 & 45 & 41 & 55 & 62 \\
34 & 14 & 14 & 3 & 17 & 12 & 28 \\
63 & 61 & 77 & 63 & 79 \\
83 & 76 & 90 \\
98
\end{pmatrix} = G(\text{say})
\]

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

\[
K^{-1} = \begin{pmatrix}
-8 & -9 & -10 & -11 \\
-12 & -13 & -14 & -15 & -16 \\
-6 & -5 & -4 & 1 & -0 & -2 & -3 \\
-17 & -18 & -19 & -20 & -21 \\
-22 & -23 & -24 & & & & \\
-25
\end{pmatrix}
\]

Step 3. Receiver multiply the rhotrix \( G \) with the with the inverse of the key \( K \).
$GK^{-1} = \begin{pmatrix}
6 & 7 & 11 & -1 \\
1 & 6 & -1 & 10 & 14 \\
16 & -1 & 2 & 3 & 17 & 6 & 19 \\
12 & 7 & 20 & 3 & 16 \\
17 & 7 & 18 \\
23
\end{pmatrix}$

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 study of 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