Multiple Encryptions of Fibonacci Lucas transformations

A. Chandra Sekhar¹, Ch. Pragathi², D. Chaya Kumari³ and Ashok Kumar⁴

¹Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
²Associate Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
³Assistant Professor in Mathematics, BVRIT Hyderabad College of Engineering for Women, Hyderabad, India
⁴Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India

Abstract: Multiple encryptions in a practical system refers to encrypting the data more than once i.e., twice or thrice to increase the security levels. As long as the cipher is unbreakable the encryption schemes remains strong. In view of the known attacks encrypting the data more than once will strengthen the security levels. In this paper we proposed a triple encryption scheme by using two keys generated by the mathematical structures from the number-theoretic concepts.

Keywords: Fibonacci numbers, Lucas numbers, Fibonacci-Lucas, Affine, Vignere transformations.

I. Introduction

Multilevel encryption[1][10] is a process of encrypting the information which is encrypted one or more than once. Fibonacci Lucas numbers and Fibonacci Lucas matrices play a vital role in cryptography. We construct cryptosystem Fibonacci Lucas transformation. Fibonacci Lucas matrices are used as trapdoor function in public key cryptosystem.

1. Fibonacci Numbers

The Fibonacci sequence [3][7][13] is 1, 1, 2, 3, 5, 8... Where each entry is formed by adding the two previous ones, starting with 1 and 1 as the first two terms. This sequence is called Fibonacci sequence.

1.1 Properties of Fibonacci numbers

Fibonacci numbers are given by the following recurrence relation

\[ F_{n+1} = F_n + F_{n-1} \]

with the initial conditions \( F_1 = F_2 = 1 \)

2. Lucas Number

The Lucas number [3][7][13] is defined to be the sum of its two immediate previous terms, thereby forming a Fibonacci integer sequence. The first two Lucas numbers are \( L_0 = 2 \) and \( L_1 = 1 \) as opposed to the first two Fibonacci numbers \( F_0 = 0 \) and \( F_1 = 1 \). Though closely related in definition, Lucas and Fibonacci numbers exhibit distinct properties. The Lucas numbers may thus be defined as follows:

\[
L_n = \begin{cases} 
2 & \text{if } n = 0 \\
1 & \text{if } n = 1 \\
L_{n-1} + L_{n-2} & \text{if } n > 1 
\end{cases}
\]

The sequence of Lucas numbers is: 2,1,3,4,7,11,18,29,47,76,123,189.....

3. Fibonacci-Lucas Transform

The Fibonacci-Lucas Transformation[14] can be defined the mapping \( FL: T^2 \rightarrow T^2 \) such that

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} F_{i} & F_{i+1} \\ L_{i} & L_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}
\]

Where \( x, y \in \{0, 1, 2, \ldots, N-1\} \), \( F_i \) is the \( i^{th} \) term of Fibonacci series and \( L_i \) the \( i^{th} \) term of Lucas series. Denoting \( \begin{pmatrix} F_{i} & F_{i+1} \\ L_{i} & L_{i+1} \end{pmatrix} \). Continue in this way we can form an infinitely many transformations

Affine Cipher

DOI: 10.9790/5728-1202026672 www.iosrjournals.org
An affine enciphering transformation is $C \equiv aP + b \pmod{N}$ where the pair $(a, b)$ is the encrypting key and $\gcd(a,N)=1$. If $y = E(x) = (ax+b) \mod{26}$,[1] then we can “solve for $x$ in terms of $y$” and so $E^{-1}(y)$ that is, if $y = (ax + b) \mod{26}$ then $y - b = ax \pmod{26}$ or equivalently $ax = (y - b) \pmod{26}$

3.1 Vigenere cipher
The Vigenere cipher was generated by Giovan Batista Belaso in 1553.[1]. This cipher uses a secret keyword to encrypt the plaintext. First, each letter in the plaintext is converted into a number. Then this numerical value for each letter of the plaintext is added to the numerical value of each letter of a secret keyword to get the ciphertext. The Vigenere ciphers are more powerful than substitution ciphers.

4. Proposed Work
An Algorithm for multi encryption using offset rule with Fibonacci numbers as the first layer of encryption and the affine transformation for super encryption

Multiple Encryption
Encryption algorithm:
Step-1: Alice creates plaintexts $P = p_1, p_2, p_3, \ldots, p_m$
Step-2: Alice computes $C_1 = P \times (FL)$ and get 1st ciphertext
Step-3: Now Alice perform super encryption with $C_1$ to Affine transformation $E(x) = (ax+b) \mod{26}$, $\gcd(a,N)=1$ and for $a$ and $b$ are secret, from the first level encryption message.
Step-4: Alice sends super encrypted message to Bob.

Decryption algorithm:
Step-1: Bob receives the super encrypted message.
Step-2: Bob decrypts the super encrypted message by using $E^{-1}(y) = a^{-1}(y-b) \pmod{26}$ ($=P_1$)
Step-3: Bob computes $P = P_1 \times (FL)^{-1}$ to get the original plaintext message.

Super Encryption of Vigenere Cipher
Encryption algorithm:
Step-1: Alice creates plaintexts $P = p_1, p_2, p_3, \ldots, p_m$
Step-2: Alice computes $C_1 = P \times (FL)$ and get 1st ciphertext and get 1st ciphertext
Step-3: Now Alice apply super encryption of vigenere transformation use offset rule with the numerical value of each letter of a secret keyword to first level encryption message.
Step-4: Alice sends super encryption message to Bob.

Decryption algorithm:
Step-1: Bob receives the super encryption message.
Step-2: Bob use reverse offset rule with vigenere transformation to get first decrypted text $P_1$
Step-3: Bob computes $P = P_1 \times (FL)^{-1}$ to get the original plaintext message.

EXAMPLE
Case-1: For $i=1$ we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$

Encryption algorithm:
Step-1: Let the Plain text $P = \begin{pmatrix} H & A \\ C & K \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$
Step-2: Alice computes $C_1 = P \times (FL)$
$\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix}$
Step-3: Now applying affine transformation $E(x) = (ax+b) \mod{26}$ for $a = 5$ & $b = 25$
Multiple Encryptions of Fibonacci Lucas transformations

<table>
<thead>
<tr>
<th>x</th>
<th>7</th>
<th>14</th>
<th>12</th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td>5x+25</td>
<td>60</td>
<td>60</td>
<td>135</td>
<td>85</td>
</tr>
<tr>
<td>(5x+25)mod26</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>7</td>
</tr>
</tbody>
</table>

Second Encrypted message is I I F H

Step-4: Encrypted message is IIFH

Decryption algorithm:
Step-1: First Decrypted Message is IIFH
Step-2: Compute Inverse of Affine transformation \( E^{-1}(y) = a^{-1}(y-b) \mod 26 \)

<table>
<thead>
<tr>
<th>Message</th>
<th>I</th>
<th>I</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>y-25</td>
<td>-17</td>
<td>-17</td>
<td>-20</td>
<td>-18</td>
</tr>
<tr>
<td>21(y-25)</td>
<td>-357</td>
<td>-357</td>
<td>-420</td>
<td>-378</td>
</tr>
<tr>
<td>21(y-25)mod26</td>
<td>7</td>
<td>7</td>
<td>22</td>
<td>12</td>
</tr>
</tbody>
</table>

First Decrypted text H H W M

\[ P_1 = \begin{pmatrix} H & H \\ W & M \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix} \]

Step-3: Bob Compute \( P_1 \times (FL)^{-1} \) to get original message P

\[ \begin{pmatrix} 7 & 7 \\ 22 & 12 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 14 & 10 \end{pmatrix} \]

Case-2: For \( i=2 \) \( FL = \begin{pmatrix} F_2 & F_3 \\ L_2 & L_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \)

Encryption algorithm:
Step-1: Let the Plain text \( P = \begin{pmatrix} H & A \\ C & K \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 14 & 10 \end{pmatrix} \)

Step-2: Alice computes \( C_1 = P \times (FL) \)

\[ \begin{pmatrix} 7 & 0 \\ 14 & 10 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 12 & 34 \end{pmatrix} \]

Step-3: Now applying affine transformation \( E(x) = (ax+b) \mod 26 \) for \( a = 5 \) & \( b = 30 \)

<table>
<thead>
<tr>
<th>x</th>
<th>7</th>
<th>14</th>
<th>12</th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td>5x+30</td>
<td>65</td>
<td>100</td>
<td>90</td>
<td>200</td>
</tr>
<tr>
<td>(5x+30)mod26</td>
<td>13</td>
<td>22</td>
<td>12</td>
<td>8</td>
</tr>
</tbody>
</table>

Second Encrypted message is N W M S

Step-4: Encrypted message is NWMS

Decryption algorithm:
Step-1: First Decrypted Message is NWMS
Step-2: Compute Inverse of Affine transformation \( E^{-1}(y) = a^{-1}(y-b) \mod 26 \)

<table>
<thead>
<tr>
<th>Message</th>
<th>N</th>
<th>W</th>
<th>M</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>13</td>
<td>22</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td>y-30</td>
<td>-17</td>
<td>-8</td>
<td>-18</td>
<td>-12</td>
</tr>
<tr>
<td>21(y-30)</td>
<td>-357</td>
<td>-168</td>
<td>-378</td>
<td>-252</td>
</tr>
<tr>
<td>21(y-30)mod26</td>
<td>7</td>
<td>14</td>
<td>12</td>
<td>8</td>
</tr>
</tbody>
</table>

First Decrypted text H O M I

\[ P_1 = \begin{pmatrix} H & O \\ M & I \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 12 & 8 \end{pmatrix} \]

Step-3: Bob Compute \( P_1 \times (FL)^{-1} \) to get original message P
Multiple Encryptions of Fibonacci Lucas transformations

Case-3: For i=3 $FL = \begin{pmatrix} F_3 & F_4 \\ L_3 & L_4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text $P = \begin{pmatrix} H & A \\ C & K \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix}$

Step-2: Alice computes $C_1 = P \times (FL)$

$\begin{pmatrix} 7 & 0 \\ 2 & 10 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 14 & 21 \\ 34 & 46 \end{pmatrix}$

Step-3: Now applying affine transformation $E(x) = (ax+b) \mod 26$ for $a = 5$ & $b = 29$

<table>
<thead>
<tr>
<th>x</th>
<th>14</th>
<th>21</th>
<th>34</th>
<th>46</th>
</tr>
</thead>
<tbody>
<tr>
<td>5x+29</td>
<td>99</td>
<td>134</td>
<td>199</td>
<td>259</td>
</tr>
<tr>
<td>(5x+29)mod26</td>
<td>21</td>
<td>4</td>
<td>17</td>
<td>25</td>
</tr>
</tbody>
</table>

Second Encrypted message is VERZ

Step-4: Encrypted message is VERZ

Decryption algorithm:

Step-1: First Decrypted Message is VERZ

Step-2: Compute Inverse of Affine transformation $E^{-1}(x) = a^{-1}(y-b) \mod 26$

<table>
<thead>
<tr>
<th>Message</th>
<th>V</th>
<th>E</th>
<th>R</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>21</td>
<td>17</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>y-29</td>
<td>-8</td>
<td>-25</td>
<td>-12</td>
<td>-4</td>
</tr>
<tr>
<td>21(y-29)</td>
<td>-168</td>
<td>-525</td>
<td>-252</td>
<td>-84</td>
</tr>
<tr>
<td>21(y-29)mod26</td>
<td>14</td>
<td>21</td>
<td>8</td>
<td>20</td>
</tr>
</tbody>
</table>

First Decrypted text O V I U

P₁ = \begin{pmatrix} O & V \\ I & U \end{pmatrix} = \begin{pmatrix} 14 & 21 \\ 8 & 20 \end{pmatrix}

Step-3: Bob Compute $P₁ × (FL)^{-1}$ to get original message P

now $\begin{pmatrix} 14 & 21 \\ 8 & 20 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 28 & -16 \end{pmatrix}$

<table>
<thead>
<tr>
<th>7</th>
<th>0</th>
<th>28</th>
<th>-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mod 26</td>
<td>7</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Second Decrypted message is H A C K

Vigenere Cipher

Case-1: For i=1 we get $FL = \begin{pmatrix} F_1 & F_2 \\ L_1 & L_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$

Encryption algorithm:

Step-1: Let the Plain text $P = \begin{pmatrix} R & A \\ M & U \end{pmatrix} = \begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix}$

Step-2: Alice computes $C_1 = P \times (FL)$

\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 17 & 17 \\ 52 & 32 \end{pmatrix}

Using vigenere ciphers for key

\begin{pmatrix} P & A & S & S \end{pmatrix}
Multiple Encryptions of Fibonacci Lucas transformations

Step-3: Offset rule with the first decrypted message

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>15</th>
<th>0</th>
<th>18</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>17</td>
<td>52</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offset rule with key</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>17</td>
<td>70</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mod 26</td>
<td>6</td>
<td>17</td>
<td>18</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Second Encrypted message is</td>
<td>G</td>
<td>R</td>
<td>S</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

Step-3: Offset rule with the first decrypted message

| 17 | 17 | 52 | 32 |
| Offset rule with key | + | + | + | + |
| 15 | 0 | 18 | 18 |
| 32 | 17 | 70 | 50 |
| Mod 26 | 6 | 17 | 18 | 24 |
| Second Encrypted message is | G | R | S | Y |

Step-4: Encrypted message is GRSY

Decryption algorithm:

Step-1: First Decrypted Message is GRSY

Step-2: Bob use reverse offset rule with vigenere transformation to get first decrypted text.

<table>
<thead>
<tr>
<th>Message</th>
<th>G</th>
<th>R</th>
<th>S</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>17</td>
<td>18</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Reverse offset rule with key</td>
<td>6</td>
<td>17</td>
<td>18</td>
<td>24</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>18</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>-9</td>
<td>17</td>
<td>0</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Mod 26</td>
<td>17</td>
<td>17</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>First Decrypted message is</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>G</td>
</tr>
</tbody>
</table>

Step-3: Bob Compute $P_1(FL)^{-1}$ to get original message $P$

Now $\begin{pmatrix} 17 & 17 \\ 0 & 6 \end{pmatrix} \times \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 17 & 0 \\ 12 & -6 \end{pmatrix}$

<table>
<thead>
<tr>
<th></th>
<th>17</th>
<th>0</th>
<th>12</th>
<th>-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mod 26</td>
<td>17</td>
<td>0</td>
<td>12</td>
<td>20</td>
</tr>
<tr>
<td>Second Decrypted message is</td>
<td>R</td>
<td>A</td>
<td>M</td>
<td>U</td>
</tr>
</tbody>
</table>

Case-2: For $i=2$ $FL = \begin{pmatrix} F_2 \\ L_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$

Step-4: Encrypted message is WIYR

Decryption algorithm:

Step-1: First Decrypted Message is WIYR

Step-2: Bob use reverse offset rule with vigenere transformation to get first decrypted text.

<table>
<thead>
<tr>
<th></th>
<th>17</th>
<th>34</th>
<th>32</th>
<th>84</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset rule with key</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>8</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Mod 26</td>
<td>22</td>
<td>34</td>
<td>50</td>
<td>95</td>
</tr>
<tr>
<td>Second Encrypted message is</td>
<td>W</td>
<td>I</td>
<td>Y</td>
<td>R</td>
</tr>
</tbody>
</table>
Multiple Encryptions of Fibonacci Lucas transformations

Message | W | I | Y | R |
---------|---|---|---|---|
22       | 8 | 24| 17|
Reverse offset rule with key
22       | 8 | 24| 17|
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-9</td>
<td>-11</td>
<td>8</td>
<td>6</td>
</tr>
</tbody>
</table>
Mod 26 | 17 | 8 | 6 | 6 |
First Decryption message is | I | R | S | G |

\[
P_1 = \begin{pmatrix} R & I \\ G & G \end{pmatrix} = \begin{pmatrix} 17 & 8 \\ 6 & 6 \end{pmatrix}
\]

Step-3: Bob Compute \( P_1 \times (FL)^{-1} \) to get original message \( P \)
now \[
\begin{pmatrix} 17 & 8 \\ 6 & 6 \end{pmatrix} \times \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 43 & -26 \\ 12 & -6 \end{pmatrix}
\]

Mod 26 | 17 | 0 | 12 | 20 |
Second Decrypted message is | R | A | M | U |

Case-3: For \( i=3 \) \( FL = \begin{pmatrix} F_3 & F_4 \\ L_3 & L_4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \)

Encryption algorithm:
Step-1: Let the Plain text \( P = \begin{pmatrix} R & A \\ M & U \end{pmatrix} = \begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \)
Step-2: Alice computes \( C = P \times (FL) \)
\[
\begin{pmatrix} 17 & 0 \\ 12 & 20 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 34 & 51 \\ 84 & 116 \end{pmatrix}
\]
Using vigenere cipher for the key

<table>
<thead>
<tr>
<th>L</th>
<th>O</th>
<th>S</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>14</td>
<td>18</td>
<td>18</td>
</tr>
</tbody>
</table>

Step-3: Offset rule with the first decrypted message

Offset rule with key
34 + + + +
51 + + + +
84 + + + +
116 + + + +

Mod 26 | 19 | 13 | 24 | 4 |
Second Encrypted message is | T | N | Y | E |

Step-4: Encrypted message is TNYE
Decryption algorithm:
Step-1: First Decrypted Message is TNYE
Step-2: Bob use reverse off set rule with vigenere transformation to get first decrypted text.

Message | T | N | Y | E |
---------|---|---|---|---|
19       | 13 | 24 | 4 |
Reverse offset rule with key
19       | 13 | 24 | 4 |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>6</td>
<td>-14</td>
<td></td>
</tr>
</tbody>
</table>
Mod 26 | 8 | 25 | 6 | 12 |
First Decryption message is | I | Z | G | M |

\[
P_1 = \begin{pmatrix} I & Z \\ G & M \end{pmatrix} = \begin{pmatrix} 8 & 25 \\ 6 & 12 \end{pmatrix}
\]

Step-3: Bob Compute \( P_1 \times (FL)^{-1} \) to get original message \( P \)
now \[
\begin{pmatrix} 8 & 25 \\ 6 & 12 \end{pmatrix} \times \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 43 & -26 \\ 12 & -6 \end{pmatrix}
\]
Mod 26

<table>
<thead>
<tr>
<th>43</th>
<th>-26</th>
<th>12</th>
<th>-6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>17</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Second Decrypted message is R A M U

II. Conclusions

For this constructed cryptosystem the time complexity for encryption and decryption are same but is more secure than the symmetric cryptosystems with Fibonacci, Lucas, Pell numbers we can exiled this concept to public key cryptosystem also.

References