CHAPTER-3

MULTIPLE ENCRYPTIONS OF AFFINE CIPHER AND VIGENERE CIPHER WITH FIBONACCI NUMBERS
CHAPTER-3

MULTIPLE ENCRYPTIONS OF AFFINE CIPHER AND Vigenere CIPHER WITH FIBONACCI NUMBERS

3.1 Introduction:

Multiple encryptions [12] are the process of encrypting the plain text more than once. If the plaintext is encrypted twice, then the process of the first encryption is usual encryption and the process of second-time encryption is referred as the super-encryption. For multiple encryptions, same or different algorithms can be used. If the same key is used for multiple encryptions, for an attacker it is not that hard to recover the plain text. In this paper, a symmetric cryptosystem is proposed using Fibonacci numbers for the first level of encryption and Affine or Vigenere cipher is employed for super encryption.

Fibonacci numbers [6],[20],[21] play an important role in various branches of research. The aesthetic appearance of the sequence has lead to many important results which were used by many researchers and scientists.

The golden ratio [20],[21] which is the limit of ratios of consecutive Fibonacci numbers, has many applications in different areas including nature to classify the plants having different spiral patterns.

The concept of Fibonacci sequence when clubbed with matrix has lead to many generalizations which has played vital role in research.
Fibonacci sequence starts with 1 and 1 as the first two terms and all the other terms are obtained by adding the two previous terms then, the sequence is as 1,1,2,3,5,8,13,…

Another interesting fact about Fibonacci sequence is that \( f_n \) is always a factor of \( f_{2n} \). And also in general \( f_n \) is always a factor of \( f_k \) for any positive natural number \( k \).

In chapter-1, we discussed about super-encryption of Affine and Vigenere cipher using Fibonacci matrix. In this chapter, we introduced super-encryptions of Affine and Vigenere cipher with Fibonacci numbers.

In this chapter, the symmetric cryptosystem is proposed using Fibonacci numbers for the first level of encryption and Affine or Vigenere cipher is the second level encryption.

3.2 Key Generation for Affine cipher, Vigenere cipher with Fibonacci numbers

Let A(Alice) and B(Bob) are two dissemination parties. For multiple encryptions initially both the parties initially agree upon Fibonacci numbers and the Affine cipher or Vigenere cipher. Fibonacci numbers sequential order and the values of \( a, b \) of the affine cipher Vigenere key will be sent to B as the private keys.

1\textsuperscript{st} level of encryption: A encrypt the plain text \( P=(p_1, p_2, p_3,..., p_n) \) with using offset rule to Fibonacci numbers key \( K_1 \) as sequential order. A gets primary encrypted message \( C_1 \) and A sends (the key \( K_1 \) through secure channel) \( P_i+F_i=C_1 \) to B.
2\textsuperscript{nd} level of encryption or Super-encryption: As a second layer of encryption, A encrypts the first encrypted message \( C_1 \) as super-encryption with Affine cipher \( E(x) = (ax+b) \mod 26 \) or Vigenere cipher with key \( K_2 \) (the values of \( a,b \)).

1\textsuperscript{st} level of decryption: B decrypts the Super-encrypted message \( C_2 \) by using the inverse of \( a,b \) in \( K_2 \), which is the inverse of affine cipher or using reverse offset rule with Vingere key to get the first decrypted message \( P_1 \).

2\textsuperscript{nd} level of decryption: Again B decrypts first decrypted message \( P_1 \) using reverse offset rule with key \( K_1 \) get plaintext message \( P \).

3.3 Algorithm:

Algorithm of enciphering:

Step-1: Let the plain text is \( P = p_1 p_2, p_3 ... p_m \)

Step-2: A uses the offset rule with Fibonacci numbers \( F=f_1,f_2,f_3...f_n \) to each value in sequential order to get the 1\textsuperscript{st} ciphertext.

Step-3: A enumerates \( C_i = P_i + F_i \) for \( i=1,2,3,...m \) where \( C_{1i} \) is the first cipher text.

Step-4: Now, again A performs super-encryption with the Affine cipher or Vigenere cipher to get super-encrypted message \( C_2 \).

Step-5: A sends the super-encrypted message \( C_2 \) to Bob.

Algorithm of deciphering:

Step-1: B receives the super-encrypted message \( C_2 \).

Step-2: B decrypts the super-encrypted message \( C_2 \) by using \( E^{-1}(y) = a^{-1}(y-b) \mod 26 \) or reverse offset rule with Vigenere key to obtain the first decrypted message \( P_1 \).
Step-3: B applies the offset rule with Fibonacci number from the first decrypted message to get the original plaintext.

**Encryption**

\[ P_1 \xrightarrow{K_1} C_1 \xrightarrow{K_2} P_2 \]

\( K_1 \) is Fibonacci numbers; \( K_2 \): Affine cipher keys with a and b or vigenere key

**Decryption**

\[ C_1 \xrightarrow{K_2} P_2 \xrightarrow{K_1} C_2 \]

\( K_2 \): inverse Affine cipher with keys a and b or vigenere key; \( K_1 \): inverse Fibonacci number or vigenere key
3.4 Examples

Example for Affine cipher

Encryption:

Step-1: Let the Plain text be CRYPTOGRAPHY

Step-2: A uses the offset rule with Fibonacci numbers to get first encrypted message as $C_1$.

<table>
<thead>
<tr>
<th>C</th>
<th>R</th>
<th>Y</th>
<th>P</th>
<th>T</th>
<th>O</th>
<th>G</th>
<th>R</th>
<th>A</th>
<th>P</th>
<th>H</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>17</td>
<td>24</td>
<td>15</td>
<td>19</td>
<td>14</td>
<td>3</td>
<td>17</td>
<td>0</td>
<td>15</td>
<td>7</td>
<td>24</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>13</td>
<td>21</td>
<td>34</td>
<td>55</td>
<td>89</td>
<td>144</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>26</td>
<td>18</td>
<td>24</td>
<td>22</td>
<td>19</td>
<td>38</td>
<td>34</td>
<td>70</td>
<td>96</td>
<td>168</td>
</tr>
</tbody>
</table>

First encryption message $C_1$ as

| 3 | 18| 26| 18| 24| 22| 19| 38| 34| 70| 96| 168|

Step-3: Now A applies super-encryption with affine cipher $E(x)=(ax+b) \mod 26$ for keys are $a=5$ & $b=8$ to get the second encryption message $C_2$

<table>
<thead>
<tr>
<th>x</th>
<th>3</th>
<th>18</th>
<th>26</th>
<th>18</th>
<th>24</th>
<th>22</th>
<th>19</th>
<th>38</th>
<th>34</th>
<th>70</th>
<th>96</th>
<th>168</th>
</tr>
</thead>
<tbody>
<tr>
<td>5x+8</td>
<td>23</td>
<td>98</td>
<td>138</td>
<td>98</td>
<td>128</td>
<td>118</td>
<td>103</td>
<td>198</td>
<td>178</td>
<td>358</td>
<td>488</td>
<td>848</td>
</tr>
<tr>
<td>(5x+8) mod 26</td>
<td>23</td>
<td>20</td>
<td>8</td>
<td>20</td>
<td>24</td>
<td>14</td>
<td>25</td>
<td>16</td>
<td>22</td>
<td>20</td>
<td>20</td>
<td>16</td>
</tr>
</tbody>
</table>

second encrypted message X U I U Y O Z Q W U U Q

Step-4: A sends second encrypted message $C_2$ to B as XUIUYOZQWUUQ

Decryption:
Step-1: B receives the super-encryption message as XUIUYOZQWUUQ

Step-2: B use the inverse affine cipher $E^{-1}(y) = a^{-1}(y - b) \mod 26$ to multi-encryption message to get the first decrypted message as $P_1$.

<table>
<thead>
<tr>
<th>Message</th>
<th>X</th>
<th>U</th>
<th>I</th>
<th>U</th>
<th>Y</th>
<th>O</th>
<th>Z</th>
<th>Q</th>
<th>W</th>
<th>U</th>
<th>U</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>23</td>
<td>20</td>
<td>8</td>
<td>20</td>
<td>24</td>
<td>14</td>
<td>25</td>
<td>16</td>
<td>22</td>
<td>20</td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td>y-8</td>
<td>15</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>16</td>
<td>6</td>
<td>17</td>
<td>8</td>
<td>14</td>
<td>12</td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td>21(y-8)</td>
<td>315</td>
<td>252</td>
<td>0</td>
<td>252</td>
<td>336</td>
<td>126</td>
<td>357</td>
<td>168</td>
<td>394</td>
<td>252</td>
<td>252</td>
<td>168</td>
</tr>
<tr>
<td>21(y-8)mod26</td>
<td>3</td>
<td>18</td>
<td>0</td>
<td>18</td>
<td>24</td>
<td>22</td>
<td>19</td>
<td>12</td>
<td>8</td>
<td>18</td>
<td>18</td>
<td>12</td>
</tr>
<tr>
<td>First decrypted message</td>
<td>D</td>
<td>S</td>
<td>A</td>
<td>S</td>
<td>Y</td>
<td>W</td>
<td>T</td>
<td>M</td>
<td>I</td>
<td>S</td>
<td>S</td>
<td>M</td>
</tr>
</tbody>
</table>

First Decrypted message as DSASYWTMISSM

Step-3: Again B uses reverse offset rule with the first decrypted message to get original plaintext $P$.

<table>
<thead>
<tr>
<th>Message</th>
<th>D</th>
<th>S</th>
<th>A</th>
<th>S</th>
<th>Y</th>
<th>W</th>
<th>T</th>
<th>M</th>
<th>I</th>
<th>S</th>
<th>S</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>18</td>
<td>0</td>
<td>18</td>
<td>24</td>
<td>22</td>
<td>19</td>
<td>12</td>
<td>8</td>
<td>18</td>
<td>18</td>
<td>12</td>
</tr>
<tr>
<td>Reverse Offset rule with Fibonacci number</td>
<td>3</td>
<td>18</td>
<td>0</td>
<td>18</td>
<td>24</td>
<td>22</td>
<td>19</td>
<td>12</td>
<td>8</td>
<td>18</td>
<td>18</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>13</td>
<td>21</td>
<td>34</td>
<td>55</td>
<td>89</td>
<td>144</td>
</tr>
<tr>
<td>Mod 26</td>
<td>2</td>
<td>17</td>
<td>-2</td>
<td>15</td>
<td>19</td>
<td>14</td>
<td>3</td>
<td>-9</td>
<td>-26</td>
<td>-37</td>
<td>-71</td>
<td>-132</td>
</tr>
<tr>
<td>Second decrypted message</td>
<td>C</td>
<td>R</td>
<td>Y</td>
<td>P</td>
<td>T</td>
<td>O</td>
<td>G</td>
<td>R</td>
<td>A</td>
<td>P</td>
<td>H</td>
<td>Y</td>
</tr>
</tbody>
</table>

B gets the plaintext as CRYPTOGRAPHY

**Example for Vigenere cipher**

**Encryption:**
Step-1: Let the Plain text be MATHEMATICS
Step-2: A uses the offset rule with Fibonacci number to get first encrypted message as $C_1$.

<table>
<thead>
<tr>
<th>M</th>
<th>A</th>
<th>T</th>
<th>H</th>
<th>E</th>
<th>M</th>
<th>A</th>
<th>T</th>
<th>I</th>
<th>C</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>0</td>
<td>19</td>
<td>7</td>
<td>4</td>
<td>12</td>
<td>0</td>
<td>19</td>
<td>8</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>13</td>
<td>21</td>
<td>34</td>
<td>55</td>
<td>89</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>21</td>
<td>10</td>
<td>9</td>
<td>20</td>
<td>13</td>
<td>40</td>
<td>42</td>
<td>57</td>
<td>107</td>
</tr>
</tbody>
</table>

First encrypted message $C_1$ as

| 13| 1 | 21| 10| 9 | 20| 13| 40| 42| 57| 107|

A using vigenere key as second key

<table>
<thead>
<tr>
<th>G</th>
<th>I</th>
<th>T</th>
<th>A</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>8</td>
<td>19</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

Step-3: Again A using offset rule with the first encrypted message $C_1$ to get the second encrypted message $C_2$.

<table>
<thead>
<tr>
<th></th>
<th>13</th>
<th>1</th>
<th>21</th>
<th>10</th>
<th>9</th>
<th>20</th>
<th>13</th>
<th>40</th>
<th>42</th>
<th>57</th>
<th>107</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset rule with Key</td>
<td>13</td>
<td>1</td>
<td>21</td>
<td>10</td>
<td>9</td>
<td>20</td>
<td>13</td>
<td>40</td>
<td>42</td>
<td>57</td>
<td>107</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>19</td>
<td>0</td>
<td>12</td>
<td>6</td>
<td>8</td>
<td>19</td>
<td>0</td>
<td>12</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>9</td>
<td>40</td>
<td>10</td>
<td>21</td>
<td>26</td>
<td>21</td>
<td>59</td>
<td>42</td>
<td>69</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td>Mod 26</td>
<td>19</td>
<td>9</td>
<td>14</td>
<td>10</td>
<td>21</td>
<td>0</td>
<td>21</td>
<td>7</td>
<td>16</td>
<td>17</td>
<td>9</td>
</tr>
<tr>
<td>second encrypted message</td>
<td>T</td>
<td>J</td>
<td>O</td>
<td>K</td>
<td>V</td>
<td>A</td>
<td>V</td>
<td>H</td>
<td>Q</td>
<td>R</td>
<td>J</td>
</tr>
</tbody>
</table>

Step-4: A sends super-encryption message as TJOKVAVHQRJ

Decryption:
Step-1: B receives super-encryption message as TJOKVAVHQRJ

Step-2: B uses the reverse offset rule with Vigenere key to getting the first decrypted message $P_1$.

<table>
<thead>
<tr>
<th>Message</th>
<th>T</th>
<th>J</th>
<th>O</th>
<th>K</th>
<th>V</th>
<th>A</th>
<th>V</th>
<th>H</th>
<th>Q</th>
<th>R</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>19</td>
<td>9</td>
<td>14</td>
<td>10</td>
<td>21</td>
<td>0</td>
<td>21</td>
<td>7</td>
<td>16</td>
<td>17</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reverse Offset rule with Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 9 14 10 21 0 21 7 16 17 9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod 26</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 1 21 10 9 20 13 14 16 5 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>first decrypted message</th>
</tr>
</thead>
<tbody>
<tr>
<td>N B V K J U N O Q F D</td>
</tr>
</tbody>
</table>

Step-3: B applies reverse offset rule with the first decrypted message as $P_1$.

<table>
<thead>
<tr>
<th>Message</th>
<th>N</th>
<th>B</th>
<th>V</th>
<th>K</th>
<th>J</th>
<th>U</th>
<th>N</th>
<th>O</th>
<th>Q</th>
<th>F</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>13</td>
<td>1</td>
<td>21</td>
<td>10</td>
<td>9</td>
<td>20</td>
<td>13</td>
<td>14</td>
<td>16</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reverse Offset rule with Fibonacci number</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 1 21 10 9 20 13 14 16 5 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod 26</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 0 19 7 4 12 0 19 8 2 18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>second decrypted message</th>
</tr>
</thead>
<tbody>
<tr>
<td>M A T H E M A T I C S</td>
</tr>
</tbody>
</table>

B gets the plaintext MATHEMATICS
3.5 Result analysis:

For the chosen plaintext the space for memory occupation and time for executing the encryption were calculated using matlab software.

Result analysis of Fibonacci matrix with Affine Cipher

<table>
<thead>
<tr>
<th>S.No</th>
<th>First encryption</th>
<th>Super-encryption</th>
<th>Space complexity</th>
<th>First encryption time</th>
<th>Super-encryption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fibonacci number</td>
<td>Affine</td>
<td>32 bytes</td>
<td>3 MILLI SEC</td>
<td>6 MILLI SEC</td>
</tr>
</tbody>
</table>

Result analysis of Fibonacci matrix with Vigenere Cipher

<table>
<thead>
<tr>
<th>S.No</th>
<th>First encryption</th>
<th>Super-encryption</th>
<th>Space complexity</th>
<th>First encryption time</th>
<th>Super-encryption Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fibonacci number</td>
<td>Vigenere</td>
<td>32 bytes</td>
<td>3 MILLI SEC</td>
<td>6 MILLI SEC</td>
</tr>
</tbody>
</table>

3.6 Conclusions:

For super-encryption, two different algorithms were performed. Initial encryption is performed with Fibonacci numbers using offset rule whereas for super-encryption with Affine cipher are performed. In view of the known attack both are more or less the same. Compare to the previous chapter Fibonacci matrix with Affine, Vigenere cipher time complexity and space complexity is reduced by using Fibonacci number with Affine, Vigenere cipher.