Cryptography - Day 6: The Fish and Beale Ciphers

MA 111: Intro to Contemporary Math

October 9, 2013
Encryption Method: Fish Cipher

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

Definition

A **Fish Cipher** encrypts like a Vigenère Cipher, but uses two (or more) keywords. The process of encryption involves stages:

(i) First, encrypt the plaintext using the first **keyword**;

(ii) Next, encrypt the result of Step (i) with the second **keyword**.

Example

Use the keywords **MONEY** and **CASH** to:

- Encrypt “MOOLAH”
- Decrypt “IMHT”
Least Common Multiples

Definition
The **Least Common Multiple** of two numbers \( a \) and \( b \), often written as \( \text{lcm}(a, b) \) is the smallest number that is a multiple of both \( a \) and \( b \).

Theorem (Counting Possibilities for the Fish Cipher)
*The number of different ways a letter can be encrypted using the Fish Cipher is at most the \( \text{lcm} \) of the lengths of the keywords being used.*

Example
What are the possible ways to encrypt a letter using the following pairs of keywords?

- “RED” and “DEVILS”
- “RED” and “BETTER”
- “RED” and “HUVHUV”
Code Summary: Fish Cipher

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>Key Secrecy</th>
<th>Letter Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caesar</td>
<td>3</td>
<td>23</td>
<td>Private</td>
<td>Normal</td>
</tr>
<tr>
<td>Shift</td>
<td>∆</td>
<td>∇</td>
<td>Private</td>
<td>Normal</td>
</tr>
<tr>
<td>Vigenère</td>
<td>∆₁Δ₂ . . .</td>
<td>∇₁∇₂ . . .</td>
<td>Private</td>
<td>Less Predictable</td>
</tr>
<tr>
<td>Fish</td>
<td>∆₁Δ₂ . . .</td>
<td>∇₁∇₂ . . .</td>
<td>Private</td>
<td>Even Less Predictable</td>
</tr>
</tbody>
</table>
The Legend of the Beale Ciphers

Another National Treasure?

http://www.youtube.com/watch?v=sKMXtFMSPoM
1. Homework 7 - Cryptography 3 - due Fri 10/11 - 11:59 PM

2. Decrypt the message SEVXKSA using a Fish Cipher with keywords **MONEY** and **CASH** to figure out what surprise you all are getting on Friday.