Introduction to Enigma

Chris Christensen
Department of Mathematics
Northern Kentucky University
Germany Adopted Machine Encryption

- Germany selected a commercial encryption machine called Enigma.
- After modification it became a primary encryption method for Germany’s military.
Each Enigma cipher is a permutation of the letters of the alphabet

abcdefghijklmnopqrstuvwxyz

OHELCPYBSURDZTAFXKINJWVQGM

Enigma
Enigma

Enigma has a period of about 17576.
The Key

- At first there were 3 rotors.
- 6 ways to order the rotors.
Setting the Rotors
The Key

- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
The Plugboard

<table>
<thead>
<tr>
<th>$n$</th>
<th>Number of connections</th>
<th>$n$</th>
<th>Number of connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>7</td>
<td>1,305,093,289,500</td>
</tr>
<tr>
<td>1</td>
<td>325</td>
<td>8</td>
<td>10,767,019,638,375</td>
</tr>
<tr>
<td>2</td>
<td>44,850</td>
<td>9</td>
<td>53,835,098,191,875</td>
</tr>
<tr>
<td>3</td>
<td>3,453,450</td>
<td>10</td>
<td>150,738,274,937,250</td>
</tr>
<tr>
<td>4</td>
<td>164,038,875</td>
<td>11</td>
<td>205,552,193,096,250</td>
</tr>
<tr>
<td>5</td>
<td>5,019,589,575</td>
<td>12</td>
<td>102,776,096,548,125</td>
</tr>
<tr>
<td>6</td>
<td>100,391,791,500</td>
<td>13</td>
<td>7,905,853,580,625</td>
</tr>
</tbody>
</table>
The Key

- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
- 100,391,791,500 ways to set the plugboard.
The positions of the turnover notches was part of the key.
The Key

- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
- 100,391,791,500 ways to set the plugboard.
- 676 ways to set the turnover notches.
- 7,156,755,732,750,624,000 ways to set the key.
The sender and receiver must set their machines in exactly the same way.
Checking one setting per second

- Would take 22,693,900,000 years.
- A better plan was needed.
- Need a machine to attack a machine.