The Road to the Cryptologic War of World War II
World War I
World War I Cryptology

German Cruiser Magdeburg
Lost 26 August 1914 Baltic Sea
On January 16, 1917, German Foreign Secretary Arthur Zimmerman sent a telegram to the German ambassador in the United States.
World War I Cryptology

French cryptologist Georges Painvin (1886 – 1980) broke the German ADFGVX cipher in June 1918.
Churchill Revealed the Secret

The World Crisis
1911-1918

Winston S. Churchill

With a new introduction by Martin Gilbert
Rotor Machines

- Arthur Scherbius  
  (1878 – 1929)  
  23 February 1918
- Hugo Alexander Koch  
  (1870 – 1928)  
  7 October 1919
- Arvid Gerhard Damm  
  (d. 1927)  
  10 October 1919
- Edward Hebern  
  (1869 – 1952)  
  1919
Enigma

An advertising brochure for commercial Model D of the Enigma cipher machine.

This American advertising brochure for the commercial Enigma cipher machine hugely underestimates its performance.
Germany after World War I
Blitzkrieg
Enigma
Poland
In 1929, the Polish government selected three mathematicians from Poznan University to attack Enigma.
The Polish Codebreakers

Marian Rejewski
(1905 – 1980)

Henryk Zygalski
(1908 – 1978)

Jerzy Rozycki
(1909 – 1942)
Tools

Zyglaski Sheets

Bomba

Cyclometer

Fig. 8. Diagram of the perforated sheet
Warsaw
Pyry Forest Meeting
A Polish Double
1 September 1939

GERMAN INVASION OF POLAND SEPTEMBER 1, 1939

0 100 MILES

Invasion Routes

Greater Germany

Soviet Union

GERMAN forces invaded Poland September 1, 1939

Soviet Union occupied Eastern Poland September 17, 1939
On September 5, 1939, the Polish codebreakers evacuated Warsaw on a special train.

They crossed into Romania, traveled through Italy, and crossed into France.
On October 20, 1939, the Polish codebreakers resumed their attack on German ciphers from a site near Paris.

On May 10, 1940, Germany ended the Phony War.

On June 24, 1940, the Polish codebreakers were flown to North Africa.
North Africa and France

- On October 22, 1940, French Premier Petain signed an armistice which divided France.

- In Algiers, they took on new identities and returned to France to resume signals intelligence in Vichy France. They operated from a site near the town of Uzes.
9 January 1942

Rozyscki died when the French ship Lamorciere carrying him and other staff back to France from Algeria was sunk.
Fleeing France

- Just prior to the German occupation of the free zone of France (November 1942), Rejewski and Zygalski fled to the Italian zone.

- Then back to France.

- On January 29, 1943, they set out for the Spanish border.
On the trip to Spain, the smuggler demanded more money from them at gunpoint.

Upon arrival in neutral (but sympathetic to Germany) Spain, the Poles were arrested.

Upon their release they made their way to Madrid.
Near the end of July, 1943, the Polish codebreakers made their way to Portugal and were taken by boat to a British naval vessel waiting off the coast.

For the remainder of the war, Rejewski and Zygalski worked at the Polish Signals Battalion in Boxmoor near London.
Zygalski remained in England after the war and taught in London.
After the war, Rejewski returned to Poland in November, 1946.
Rejewski

... for reasons of practical and family nature, it proved difficulty for Rejewski to find employment as a mathematician at an institution of higher learning, and, in the early postwar period, he felt it imprudent to apply for a job in cryptology.
... for 20 years Rejewski worked in the administrations of various concerns in Bydgoszcz, and in February, 1967, he retired.
He died in 1980.
This plaque commemorates the work of Marian Rejewski, Jerzy Rozcki, and Henryk Zygalski, mathematicians in the Polish intelligence service, in first breaking the Enigma code. Their work greatly assisted the Bletchley Park codebreakers and contributed to the allied victory in World War II.
Bletchley
Bletchley Station

Welcome to Bletchley
The House
The Huts
Hut 8
B Block
Bletchley Park Mathematicians

Turing-Welchman Bombe
February 1942
4-Rotor Naval Enigma
Dayton, OH
US Navy Cryptologic Bombe

Joseph Desch
(1907 – 1987)
Enigma
Enigma
Enigma Rotor
Enigma Rotor
Rotor System
Rotor Setting

\[ 6 \times 26 \times 26 \times 26 = 105,456 \]
Reflector
Reflector
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>
Ringsetting
The Key

- 6 ways to order the rotors.
- 17,576 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.
Sender and Receiver Must Use the Same Settings
## Setting Sheet

<table>
<thead>
<tr>
<th>Tag</th>
<th>UKW</th>
<th>Walzenlage</th>
<th>Ringstellung</th>
<th>Steckerverbindungen</th>
<th>Spruchschlüssel</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>ATBM</td>
<td>FYUG</td>
</tr>
<tr>
<td>30</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VIII VII</td>
<td>NBZL</td>
<td>SBEF</td>
</tr>
<tr>
<td>29</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>V IV</td>
<td>NMEY</td>
<td>JFRF</td>
</tr>
<tr>
<td>28</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VIII VII</td>
<td>QXHD</td>
<td>WETC</td>
</tr>
<tr>
<td>27</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>V IV</td>
<td>QXHD</td>
<td>WETC</td>
</tr>
<tr>
<td>26</td>
<td>E</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>BLCY</td>
</tr>
<tr>
<td>25</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>VQGA</td>
</tr>
<tr>
<td>24</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>OXFR</td>
</tr>
<tr>
<td>23</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>NBLZ</td>
</tr>
<tr>
<td>22</td>
<td>E</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>OKFR</td>
</tr>
<tr>
<td>21</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>WPQQ</td>
</tr>
<tr>
<td>20</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>JFRE</td>
</tr>
<tr>
<td>19</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>TBMH</td>
</tr>
<tr>
<td>18</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>TNMS</td>
</tr>
<tr>
<td>17</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>DGRK</td>
</tr>
<tr>
<td>16</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>15</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>14</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>13</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>12</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>11</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>10</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>9</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>8</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>7</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>6</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>5</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>4</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>3</td>
<td>C</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>2</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
<tr>
<td>1</td>
<td>B</td>
<td>Gamma VIII III IV</td>
<td>VII VI</td>
<td>VFLK</td>
<td>HNST</td>
</tr>
</tbody>
</table>
Brute Force?
22,693,900,000 years!
Enigma Message
Enigma Ciphers

abcdefghijklmnopqrstuvwxyz
OHELCYPYSURDZTAFXKINJWVQGM
No letter enciphers as itself!