Facts & Myths of Enigma

Breaking Stereotypes

Arkadiusz Orłowski & Kris Gaj

Who reinvented the wheel?

- U.S.A.: Edward Hugh Hebern (1869-1952)
  first ideas in 1915 and 1917, filed for U.S. patent in 1921
- Germany: Arthur Scherbius (1878-1929)
  German patent filed Feb. 23, 1918
- Netherlands: Hugo Alexander Koch (1870-1928)
  The Netherlandish patent Oct. 7, 1919
- Sweden: Arvid Gerhard Damm (1867-1927)
  Swedish patent Oct. 10, 1919

Artur Scherbius

Drawing from Scherbius’ U.S. patent

Enigma Timetable: 1918-1930

Apr 18, 1918:
  Arthur Scherbius offers Enigma machine to the German Navy

Feb 1926:
  German Navy begins using Enigma machine

Jul 15, 1928:
  German Army begins using Enigma machine

Jun 1, 1930:
  German armed forces start using significantly modified military version of Enigma
Functional diagram & dataflow

Number of possible internal connections of Enigma

3 - $10^{114}$

Estimated number of atoms in the universe

$10^{80}$

Enigma Daily Keys

Four Components of the Daily Key

Order of rotors (Walzenlage)

6 combinations

Positions of rings (Ringstellung)

$26^3$ combinations
Plugboard Connections (Steckerverbindung)

~ $0.5 \cdot 10^{15}$ combinations

Initial Positions of Rotors (Grundstellung)

26³ combinations

Total Number of Keys

$3.6 \cdot 10^{22} \approx 2^{75}$

Was Enigma more secure than DES?

How often did the “daily” keys change?

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Rotors</th>
<th>Rings</th>
<th>Plugs</th>
</tr>
</thead>
<tbody>
<tr>
<td>After Jun. 1930</td>
<td>Every quarter</td>
<td>24 hrs</td>
<td>24 hrs</td>
</tr>
<tr>
<td>After Feb. 1936</td>
<td>Every month</td>
<td>24 hrs</td>
<td>24 hrs</td>
</tr>
<tr>
<td>After Oct. 1936</td>
<td>24 hrs</td>
<td>24 hrs</td>
<td>24 hrs</td>
</tr>
<tr>
<td>1942-45</td>
<td>12 hrs</td>
<td>24 hrs</td>
<td>24 hrs</td>
</tr>
</tbody>
</table>

Message Key: Enigma’s Achilles Foot

Determines the positions of rotors where the message encryption starts
Message Key – cont.
Protects against the separate frequency analysis of all first letters, all second letters, etc.

Could be possibly sent in clear (the same as IVs in modern ciphers)

Message Key – cont.
Encrypted TWICE using initial positions of rotors
Sent in the encrypted form in the message header

Enigma Timetable: 1928-1931
1928: Polish Cipher Bureau recognizes the use of machine encryption by Germans
1929: Polish Cipher Bureau organizes a cryptology course for over 20 students of mathematics at the University of Poznan. Three of the most advanced students are later hired to work on breaking Enigma.
1928-1929?: Polish Cipher Bureau decides to purchase the commercial version of Enigma

Polish Signal Interception Stations

Marian Rejewski (born 1905)

Jerzy Różycki (born 1909)
**Henryk Zygalski (born 1907)**

Headers of messages intercepted on the same day:

1. chm g rt
2. xrw rgs
3. ow o k k
4. fkr x o a
5. ouv q ay
6. crx g gg
7. vvb z se
8. uuz y au
9. nnk m d
10. . . . . . . . .

... ... ...
70. o a k q wd
71. q o f d y q
72. k s m p c t
73. u x u y p w
74. u h k y d
75. x c o r b k
76. r j j h i r
77. t t g b u c
78. w x g a p

**Encryption as a permutation**

<table>
<thead>
<tr>
<th>Message key</th>
<th>q w e q w e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td>A B C D E F</td>
</tr>
<tr>
<td>d m q v b n</td>
<td></td>
</tr>
</tbody>
</table>

**How the reflecting rotor helps?**

<table>
<thead>
<tr>
<th>Message key</th>
<th>q w e q w e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td>A B C D E F</td>
</tr>
<tr>
<td>d m q v b n</td>
<td></td>
</tr>
</tbody>
</table>

**Determining a product of permutations**

<table>
<thead>
<tr>
<th>Message key</th>
<th>q w e q w e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td>A B C D E F</td>
</tr>
<tr>
<td>d m q v b n</td>
<td></td>
</tr>
</tbody>
</table>

**How German clerks helped Polish to find A, B, C, D, E, F?**

Preference for message keys of the form:

1. qqq, aaa, etc.
2. qwe, asd, etc.
3. with all letters different
What remains is just to solve these equations...

\[
A = S H R' T' R^{-1} H^{-1} S^{-1} \\
B = S H Q R' Q^{-1} T' Q R' T^{-1} Q^{-1} H^{-1} S^{-1} \\
C = S H Q^2 R' Q^{-2} T' Q^2 R^{-1} Q^{-2} H^{-1} S^{-1} \\
D = S H Q^3 R' Q^{-3} T' Q^3 R^{-1} Q^{-3} H^{-1} S^{-1} \\
E = S H Q^4 R' Q^{-4} T' Q^4 R^{-1} Q^{-4} H^{-1} S^{-1} \\
F = S H Q^5 R' Q^{-5} T' Q^5 R^{-1} Q^{-5} H^{-1} S^{-1}
\]

How to reduce the number of unknowns?

Enigma Timetable: 1931

Oct 1931:
Hans-Thilo Schmidt, pseudonym Asche, an employee of the German Cipher Bureau approaches the agents of the French Intelligence service (S.R.F) and proposes to deliver classified documents.

Nov 8, 1931:
Captain Gustave Bertrand, head of the crypto-service of the S.R.F. receives the first set of documents from Asche.

End of 1931:
French Cipher Bureau declares Enigma unbreakable and documents useless.
British Cipher Bureau receives the documents, files them, and gives no follow-up offer of collaboration.

Dec 7-11, 1931:
Captain Bertrand visits Warsaw and supplies Polish Cipher Bureau with documents provided by Asche. Two sides agree to share all information.
Dec 1932:
Tables of keys delivered by Asche enables Rejewski to reduce the number of unknowns, solve the equations, and as a result reconstruct the internal wirings of the three Enigma rotors.
Poles begin solving German army messages.

1934:
The first replica of the Enigma machine built by AVA Radio Workshops, Polish company based in Warsaw.

Six equations, two unknowns
How difficult can it be?

\[
\begin{align*}
A &= SHR'T'R^{-1}H^{-1}S^{-1} \\
B &= SHQ'R'Q^{-1}T'Q'R^{-1}Q^{-1}H^{-1}S^{-1} \\
C &= SHQ'S'H^{-1}S^{-1} \\
D &= SHQ'R'Q^{-1}T'Q'R^{-1}Q^{-1}H^{-1}S^{-1} \\
E &= SHQ'R'Q^{-1}T'Q'R^{-1}Q^{-1}H^{-1}S^{-1} \\
F &= SHQ'R'Q^{-1}T'Q'R^{-1}Q^{-1}H^{-1}S^{-1}
\end{align*}
\]

If \( G \) & \( P \) are permutations then a permutation \( PG^{-1} \) has the same cycle structure as permutation \( G \).

1932-1939:
Three Polish cryptologists
Marian Rejewski
Henryk Zygalski
Jerzy Różycki
develop sophisticated methods of reconstructing daily keys, including
- grill method
- Rejewski’s cyclometer,
- Zygalski’s perforated sheets,
- Polish “Bomba”.

101 possible forms of the products \( AD, BE, CF \)

\[
\begin{align*}
AD &= (a \ o \ r \ u \ e \ h \ x \ g \ m \ d \ t \ y \ f) \\
&\quad (b \ v \ i \ z \ e \ s \ q \ k \ n \ w \ l \ p \ j) \\
&\quad \ldots \\
AD &= (a \ o \ r \ u) \ (e \ h \ g) \ (m \ d \ t) \ (y \ f \ b) \\
&\quad (v \ i) \ (z \ c) \ (s \ q) \ (k \ n) \ (w) \ (l) \ (p) \ (j) \\
&\quad \ldots \\
AD &= (a) \ (b) \ (c) \ (d) \ (e) \ (f) \ (g) \ (h) \ (i) \ (j) \ (k) \ (l) \ (m) \\
&\quad (n) \ (o) \ (p) \ (q) \ (r) \ (s) \ (t) \ (u) \ (v) \ (w) \ (x) \ (y) \ (z)
\end{align*}
\]
Number of different formats for AD, BE, CF: $101^3 = 1,030,301$

Number of initial rotor orders and settings: $6 \cdot 26^3 = 105,456$

What has changed on September 15, 1938?

Polish Bomba

Each set = 26 sheets
Each sheet = 17,576 cyclometer tests
Number of sets for all possible orders of three rotors = 6
Number of sets produced by July 1939 = 2

Zygalski’s sheet

Change in the German procedure

Since December 15, 1938 three rotors chosen from an extended set of five rotors
Number of possible combinations increases from 6 to 60
Jul 25-26, 1939:
A secret meeting takes place in the Kabackie Woods near the town Pyry (South of Warsaw), where the Poles hand over to the French and British Intelligence Service their complete solution to the German Enigma cipher, and two replicas of the Enigma machine.

Sep, 1939:

Among British mathematicians hired to work on breaking Enigma are Alan Turing and Gordon Welchman, both mathematicians from Cambridge University.
1939-1940: Alan Turing develops an idea of the British cryptological “Bombe” based on the known-plaintext attack.

Gordon Welchman develops an improvement to the Turing’s idea called “diagonal board”.

Harold “Doc” Keen, engineer at British Tabulating Machines (BTM) becomes responsible for implementing British “Bombe”.

May, 1940: First British cryptological bombe developed to reconstruct daily keys goes into operation.

Over 210 Bombes are used in England throughout the war. Each bombe weighed one ton, and was 6.5 feet high, 7 feet long, 2 feet wide.

Machines were operated by members of the Women’s Royal Naval Service, “Wrens”.
**Enigma Timetable: 1940**

Feb 12, 1940: British seize two of the three unknown rotors used in the naval Enigma from a crew member of the U-33 captured after the submarine was sunk in Scotland's Firth of Clyde.

Apr 26, 1940: British seize a canvas bag thrown overboard of the German attack vessel approached by British warships. The bag contained cryptographic documents essential in solving German naval Enigma traffic.

May, 1940: First break into Naval Enigma.

Aug, 1940: The last unknown naval rotor obtained from a naval capture.

**Enigma Timetable: 1941-1942**

May 1941: Britain captures German submarine U-110 with all its encryption equipment and keys intact.

Feb, 1942: German Navy introduces new version of the four-rotor Enigma machines and an additional code referred as "Shark".

Jul, 1942: U.S. Navy officers visit Bletchley Park and learn the details of the Bombe.

Sep, 1942: The development of the American bombe starts.

Oct, 1942: Important documents retrieved from the sunk German submarine, U-559. Blackout period ends.

**Enigma Timetable: 1943**

Apr, 1943: The production of the American Bombe starts in the National Cash Register Company (NCR) in Dayton, Ohio. The engineering design of the bombe comes from Joseph Desch.

**Joseph R. Desch (1907-1987)**

**How do we know all that?!**

Well ...

W. Kozaczuk, 1967

M. Rejewski, 1967

G. Bertrand, 1973

F. Winterbotham, 1974
Available Translations

- Yugoslavia
  - 1977
- Poland
  - 1979, 1986
- U.S.A.
  - 1984
- East Germany
  - 1977
- West Germany
  - 1987
- Bulgaria
  - 1990
- Germany

Enigma Lessons

1. Keeping machine secret did not help
2. Large number of keys did not help
3. Known-plaintext attack was easy to mount
4. Do not let people to generate keys
5. Key management is the weakest link