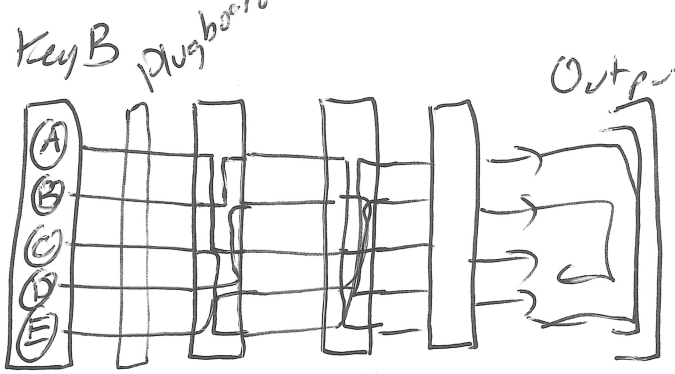
Enigma 9/17/2021

Machine Germans used to encrypt messages.

Arthur Scherbius - Machine

Idea - Substitution but different subs each time.



Output (Simplified)

Reflector (ensured that no letter ever encrypted to itself.)

(Rotors) Disks - performers a permutation

Go through 3 perms.

A A A

After encrypting one letter the rotors advance to

A A B
A A C
⋮
A Z Z
B A A
⋮
Z Z Z

$26^3 = 17,536$

How to Use

Book of DAY CODES

starting
possible settings
$26^3 \times 6$
$\sim 102{,}000$

1/1/22 : PRZ, also had 2,3,1
1/2/22 : BAM, or 1,3,2
etc.

] order of rotors

To encrypt a msg

(1) Pick a message code (YQM)

(2) Encrypt YQMYQM (msg code twice)
Starting machine at the day code setting.

(3) Change rotors to message code.

(4) Send msg with <u>this</u> setting

Started USE 1918
Germans use regularly in late 20s early 30s.

German Hans Thilo-Schmidt
French Secret Agent offered Hans 10,000 francs (ton of money) to share enigma blueprints
late 1920s.
french → polish (peace time information sharing pact)

Polish cryptanalyzed Enigma

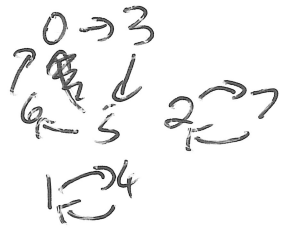
Marian Rejewski starting 1932 or 1933

msg key
NYXNYA
BQRBQR
MRSMRS
TADTAD

Given enough of these you can compute loop sizes

0→3
1→4
2→7
3→5
4→1
5→6
6→0
7→2

4, 2, 2



Built enigma
Ran encryption on all
102,000 settings of all letters
+ calculated these loop lengths.

→ 1 WHOLE YEAR

before WW2, Germans added 2 rotors!

3, 5, 1
2, 0, 4

5 choice
4 choice
3 choice

5 × 4 × 3 = 60

British used to break enigma

(1) Weather Report

(2) Some German operators always used the same msg code.