

Enigma - Transmitting Messages

9/27/19 ①

Day Code Book - [365 Codes for year]
GVX 3-1-2

To send msg

① picks a ~~DAY~~ CODE QBP

operator chooses "at random"

② Encrypt ~~DAY~~ MSG code twice "QBPQBP"
setting the rotors to the DAY CODE.

③ Change rotors to message code setting

Polish Break Enigma

circa 1932-3 Marian Rejewski

entirely focuses on 1st 6 letters (msg code)

"QBPQBP" → DAMUPR

→ U Z

1→5
2→1
3→7
4→8
5→6
6→4
7→2
8→3

1→5→6→4→8→3→7→2→1

1→4
2→1
3→5
4→2
5→3
6→6

1→4→2
3→5
6

26 letters
could be
partitioned into
several cycles.

for all 3
6×26
settings, these
set of cycle
lengths
were unique.

"2,3,6,7,8" $\Rightarrow$ 6VK 3-1-2

9/27/19(2)

Many times, the code makers don't realize hidden patterns in their codes.

Polish reading ^{German} messages 1932 - 1939

Δ to Enigma ('38-'39) = adding 2 rotors
 $\hookrightarrow$ so now $5 \times 4 \times 3 = 60$ rotor settings!
 $\uparrow \quad \uparrow \quad \uparrow$
1st 2nd 3rd

Polish didn't have resources to speed up mapping all of the new rotors.

In 1940, Polish told Allies that they had broken Enigma, but couldn't read msg anymore.

Turing built a machine (bombe) to speed up the process of making the lookup table that was much bigger now.

THINGS THAT HELPED

- ① Weather reports
- ② Enigma operators choosing same msg code every time!
- ③ Occasionally radio operators could identify individual "fists".

US had a code that wasn't broken in WWII

Officer familiar w/ Navajo asks superior about using it for a code.

Choose which Native American language.

① Tribe must have enough members to supply military need who are able.

② Able → literate in English, fit

* ③ less likely for a German to know.