CIS 3362 9/15/25

Enigma

Sources

The Code Book - Simon Singh

Code Breakers - F. H. Hinsley + Alan Stripp

The Inside Story of Bletchley Park

→ encryption machine invented in Germany ~1920 by Arthur Scherbius.

late 1920s early 1930s

Polish + French had a peacetime pact to share intelligence info.

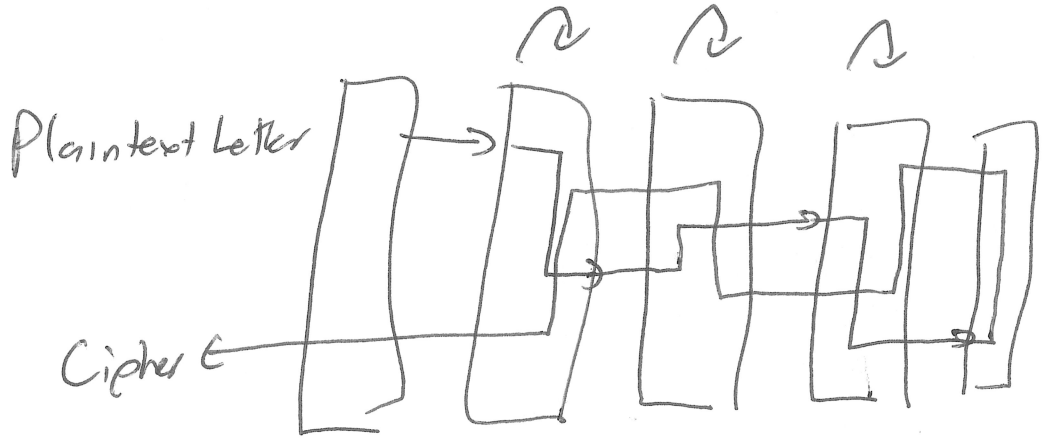
Hans Thilo Schmidt - worked at a German Office that dealt w/ Enigma.

~1929 early 30s

- little disgruntled
- French Agent named Rex offered Hans (equiv 10,000 euros) to meet him w/ Enigma blueprint so french guy could take picture.

french gave Polish Blueprint pics of Enigma!

Polish Mathematician Marian ~~Rewski~~ Rejewski, he ended noticing a pattern with Enigma which ~~up~~ ultimately allowed Polish to read German messages in the 1934-1939 time period.



Scramblers are wheels that rotate

A A A

encrypt 1 letter the least significant scrambler rotated 1 position

A A B
A A C
A A Z
A B A
A B B
A Z Z
B A A
Z Z Z

26^3

Settings $(3!) \times 26^3 =$ ~~101~~, 105,456

5 total scramblers interchangeable

DAY ⟹

4	1	5

beginning 3 scramblers

1-2-3
1-3-2
2-1-3
2-3-1
3-1-2
3-2-1

Protocol

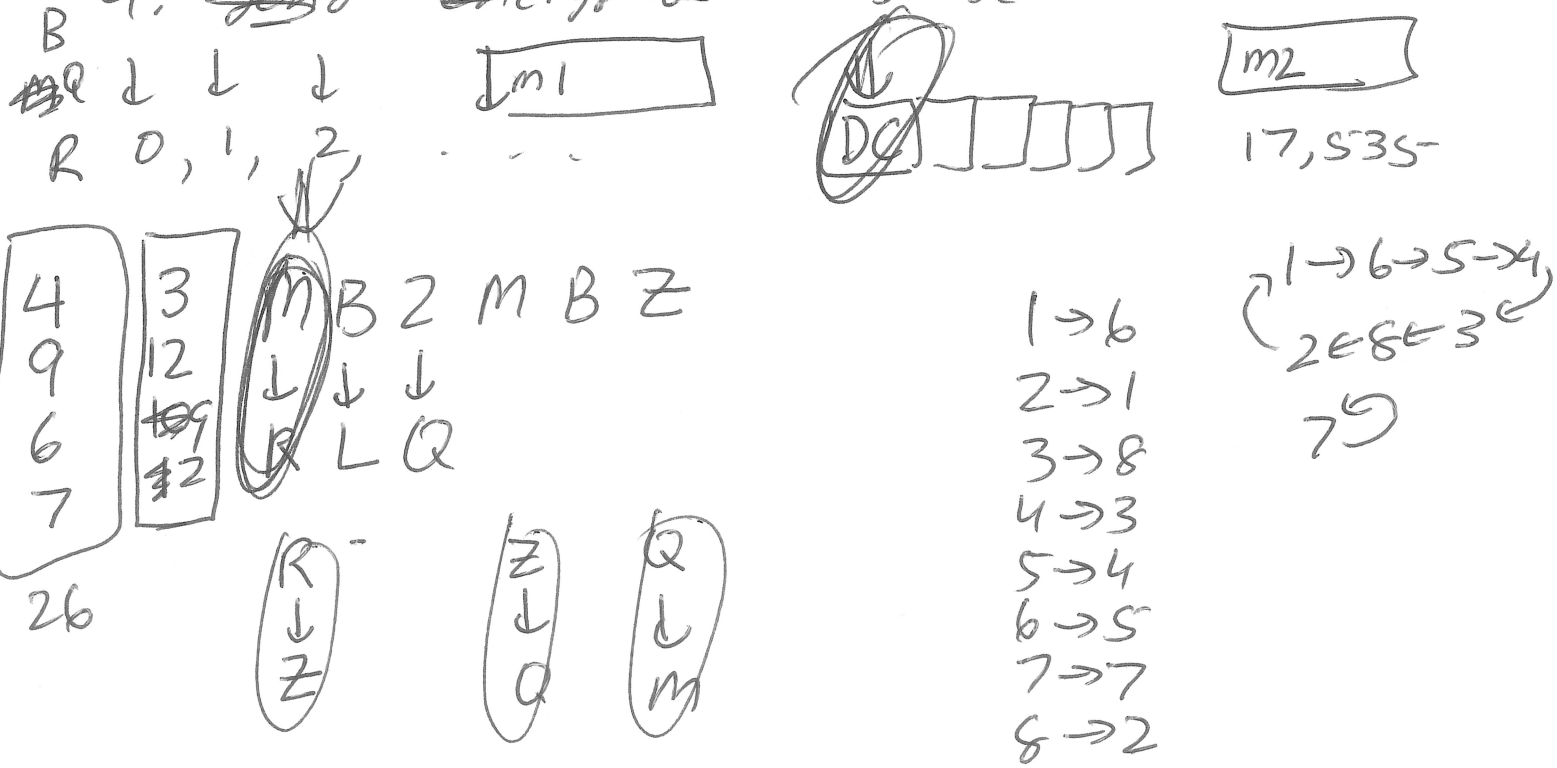
DAY CODE 2-3-1 BQR

2-3-1: scrambler order

BQR: starting pos scramblers

Operator

1. Pick a random message code (MBZ) eg.
2. Set the machine to day code (BQR) Encrypt eg. "MBZ MBZ" (msg code twice)
3. Reset Scramblers to msg code setting (MBZ)
4. ~~Send~~ encrypt ~~encrypted~~ message



Rejewski spent 1 year cataloging the cycle lengths for all $6 \times 26^3 = 105,456$ settings. Built a machine called a "bomba" to speed this up.

4, 6, 7, 9 : BQR 1-2-3
2, 4, 9, 11 : MRZ 1-2-3 etc.

↓

1939 Germans added 2 scramblers | rotors.

$3 \times 2 \times 1 = 6$ scrambler orders

$5 \times 4 \times 3 = 60$ Scrambler orders

Polish gave Allies info about breaking Enigma.

In Bletchley Park, (British gov't code breaking) Alan Turing + company used Rejewski's method and refined it to build the bank 10 times larger for all the new setting.

↳ got into late 1940 were reading messages by ~ early 1942.