Enigma 9/17/2021

Machine Germans used to encrypt messages.
Arthur Scherbius - Machine
Dec. - Substitution but different subs each time.

Key: Plugboard

Output (Simplified)

Reflector (Ensured that no letter ever encrypted to itself)

(Rotors) Disks - performs a permutation
Go through 3 perms.

A A A

After encrypting one letter the 3 rotors advance to

A A B
A A C

\[26^3 = 17,576\]
How to Use
Book of DAYCODES

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

To encrypt a msg
1. Pick a message code (YQM)
2. Encrypt YQMYYQM (msg code twice)
   starting machine at the day code setting
3. Change rotors to message code.
4. Send msg with this setting

Skilled use [1918]
Germans use regularly in late 20s early 30s.

German Hans Thilo-Schmidt
French Secret Agent offered Hans 10,000 Gemes
(tax at money) to share enigma blueprints
late 1920s.

French -> polish (information sharing)
Polish cryptanalyzed Enigmas

Marian Rejewski starting 1932 or 1933

msgcod

NYXNYX
BARBQR
MRSMRS
TADTAD

0->3
1->4
2->7
3->5
4->1
5->6
6->0
7->2

4,2,2

BAR

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

WHOLE YEAR

before WWII, Germans added 2 rotors!

3, 5, 1
2, 0, 4

5 choice
4 choice
3 choice

5x4x3 = 60
British used to break enigmas

1. Weather Report

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