CIS 3362 9/16/22

(1) Hill questions?

(2) HW3A Posted due Wed

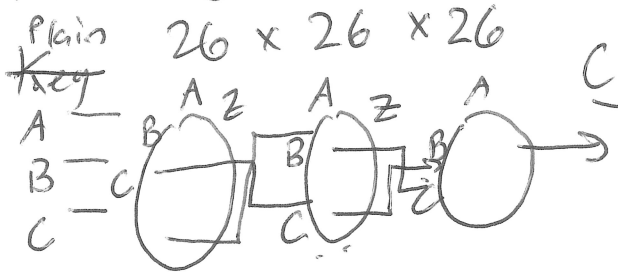
(3) Enigma

ADFGVX → WWI

1918 → Arthur Schrebius

Why not use a machine? (faster)

machines have interchangeable parts!



if disks fixed in place ⟹ a single substitution

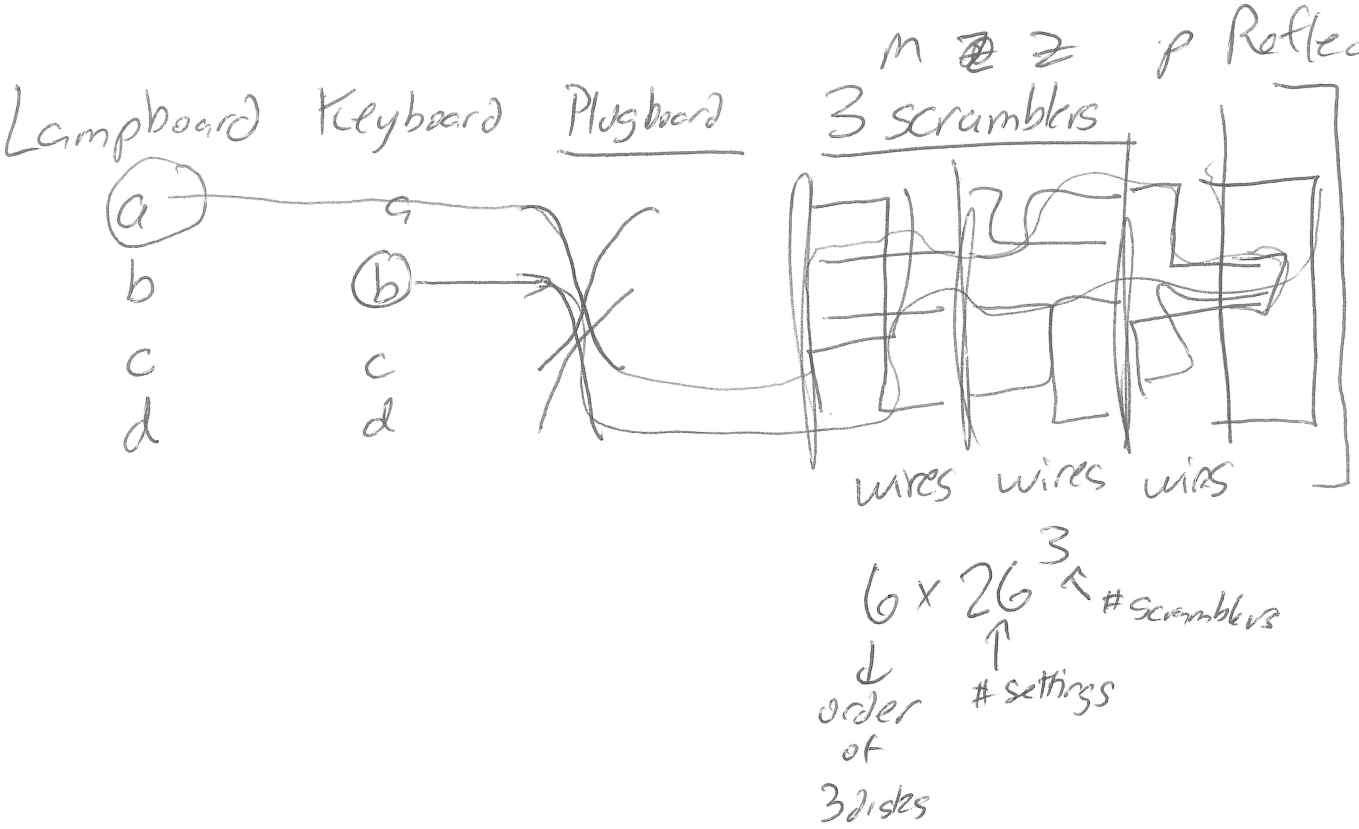
$26^3 = 17,536$ settings of the disks!

Disks can be taken out easily! So w/3 disks Disk 1, Disk 2, Disk 3, we can put them in machine in any of 6 orders (123 213 312 132 231 321)

$6 \times 26^3 = 102,$

Vigenere on Crack! Cycle len 10ish ⇝ 17,536 for each setting shift ⇝ substitution

What else was in the machine?



(1) Book Day Codes (MZP), 3-1-2

(2) Set machine to MZP 3-1-? (day code)

(3) Pick random message code (CPR)

(4) Encrypt "CPRCPR" (msg code twice) w/the day code.
Note: When one letter is encrypted, the scrambler positions "increment"
MZP → MZQ → MZR → MZS → MZT → MZU

(5) Reset scramblers to "CPR" (~~Day~~ Msg Code)
Encrypt plaintext.

19
11/8/31 - French agent "Rex" bribes Hans-Thilo Schmidt.
met in Belgium Hans brought blueprints of the machine. "Rex" took pictures.

French ⟹ Polish

Marian Rejewski (worked to break Enigma)

- many messages of six letters were encrypted with the same setting
- six letters were a repeat set of 3

Ciphertext A Q R M Z P

M Z A R Q N

First	Second	Third
A→M	Q→Z	R→P
M→R	Z→Q	A→N

7, 6
5, 8

A→B	A E
B→D	B C
C→A	C B
D→G	D A
E→C	E D
F→E	F G
G→F	G F

A → B → D → G → F

C ← E

7

A→E→D 3

B→C 2

F→G 2

In 1939, Germans added 2 rotors/discs

Discs 1, 2, 3, 4, 5

$$\frac{\text{choices}}{5} \times \frac{\text{choices}}{4} \times \frac{\text{choices}}{3}$$

$$60 \times 26^3$$

Rejewski's tables only cover 10% of these settings + took a year to compute what he had!

Polish $\xrightarrow{1940}$ Allies

Turing Built Machines to "mate" the books for the 54×26^3 settings faster.