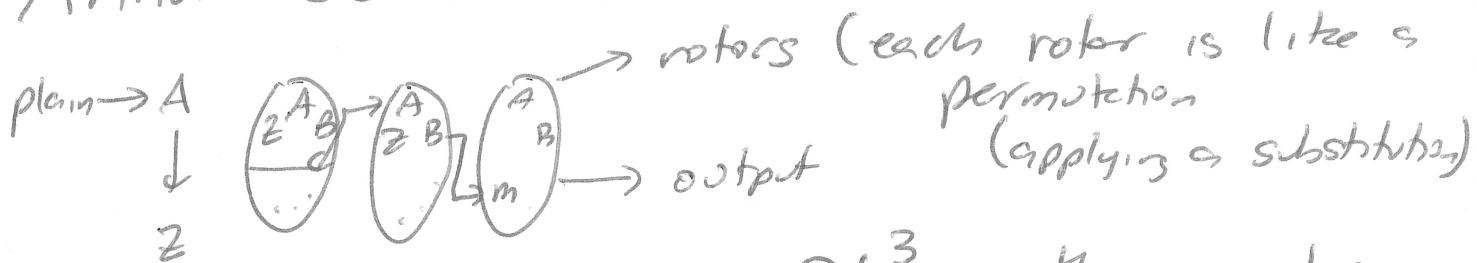


CIS 3362 9/15/23

Enigma

Germans used from early 1920s through WWII

Arthur Scherbius



A A A

A A B

⋮

A A Z

A B A

⋮

A Z Z

B A A

⋮

Z Z Z

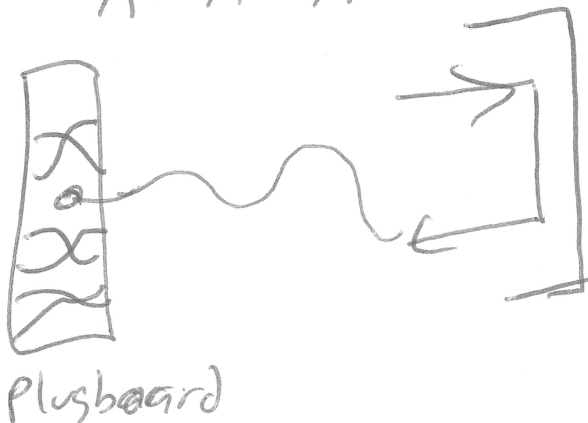
A A A

26^3 settings rotors

17,576

like a Vigenere
w/ keyword length of
17,576 but it's
worse because an
arbitrary substitution
is being used @
each slot.

Reflector



How was it used?

Day	code	Published	book
		1/1/1925	GCM
		1/2/1925	BQQ
		etc.	

① Operator sets Rotors to the Day Code.

G C M
↪ ↪ ↪

② Pick a msg code that is a different random setting of the rotors
msg code = RMB

③ Send 6 chars "RMBRMB", msg code twice

④ Reset the rotors to "RMB"

⑤ Send msg.

late 1920s, early 1930s

French + Polish - piece time information sharing pact.

French secret agents

Hans Thilo Schmidt - worked German cipher group

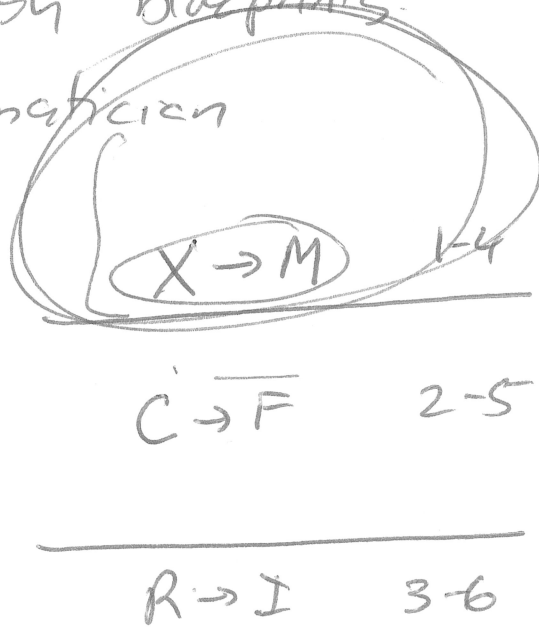
Hans paid by French agent
took back blueprint of Enigma. Met secret
agent hotel room. $\Rightarrow$ Photographed the blueprints

French says $\Rightarrow$ CRAZY no way we're
breaking it

French $\Rightarrow$ give Polish blueprints

Marian Rejewski - mathematician

Plain	R	M	B	R	M	B
Cipher	X	C	R	M	F	I



mapped out cycles in perm

$X \rightarrow M \rightarrow Q \rightarrow R \rightarrow X$

$A \rightarrow B \rightarrow C \rightarrow A$

2, 3, 4, 8, 9 pos 8, 256



4	} cycle length gcd 26
3	
2	
8	
9	

Rotors could be permuted in $3!$ ways
Space key $3! \times 26^3$

Polish were able to read German messages
for most of the 1930s.

Circa 1939, Germans add 2 rotors
rotors 1, 2, 3, 4, 5

$$\begin{array}{ccc} \text{first} & \text{second} & \text{third} \\ \hline 5 & \times 4 & \times 3 = 60 \text{ rotor settings} \\ & & \text{of which 6 were} \\ & & \text{the original settings} \end{array}$$

WAR!

Polish $\Rightarrow$ Info about Enigma
to the Allies!

Alan Turing amongst scientists that worked
on breaking the new Enigma!
(Imitation Game)

Turing $\Rightarrow$ automated process of
building the necessary "books
of cycles"

Weather report sent the morning

① structure report was same
knew some plaintext

② Some operators always used the same
message code!

③ letter never encrypts to itself!