

CIS 3362 9/21/26

- ① A little WWI history
- * ② Enigma Machine
- * ③ Breaking Enigms
- + ④ Navajo Code
- ⑤ Exam 1 Info

} Have
typed up
Notes

ADF6VX- Introduced early February 1918.

French George Painvin - worked on this
day+night (lost 15 lbs), broke around June 2, 1918
Using info about radio signals, you can narrow
down location. Message has info about
timing of an attack.

Other WWI Story

1915 - Lusitania sunk.

Germans promise it won't happen again!

1917 - Zimmerman Telegram

transatlantic cable cut (Germans)

sent Feb ⇒ British got a hold of the message
(encrypted)

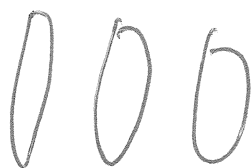
Room 40 cryptanalysis
* Zimmerman took responsibility!

1918 - Scherbius + Ritter
engineering background.

Enigma created

Downside - single machine cost \$30,000 (transferred to 1990s prices)

3 Rotors $\rightarrow$ cyclic wheels w/ 26 notches



like car odometer

A A A

A A B

A A Z

A B A

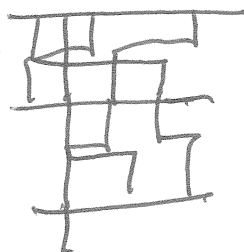
A Z Z

B A A

Z Z Z

A A A

$$\# \text{ settings} = 26^3 \approx 17,536$$



R1 (perm)

R2 (perm)

R3 (perm)

Sort of like a

"Vigenere" w/ a key word
length 17,536.

Rotors could be reordered

R1, R2, R3

R3, R1, R2

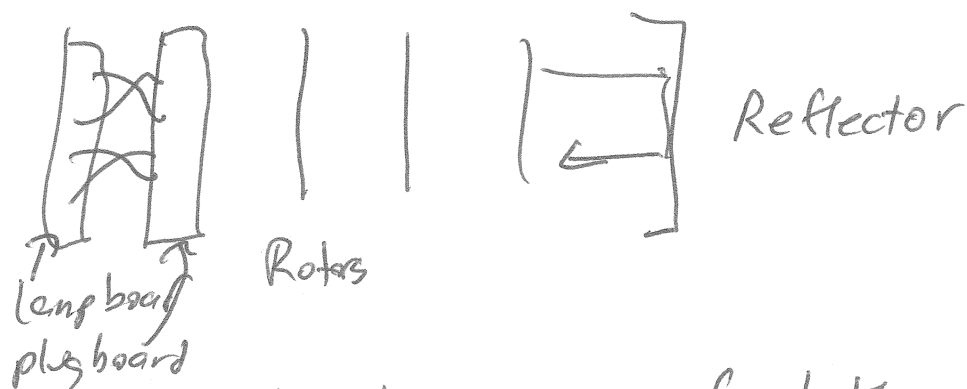
} easy to
exchange

$$3! = 6$$

total # of "substitution" charts
induced in machine = 6×26^3

$$\approx 102,000$$

Machine more details



Choose up to 10 pairs of letters to exchange.

Reflector made sure that a letter never encrypted to itself. → This helped Allies crack enigmas!

French can't read Enigma, but went to!

1932
French secret agent approaches a person in German cipher office, Hans-Thilo Schmidt offered equivalent 10,000 ~~lot~~ German currency (Deuchmark) if Hans will bring book w/ Enigma blueprint to a hotel. French take pics of every page!

French think it's impossible to break Enigma!

French + Polish had a peace time pact to share intelligence info.

1932/3 - Marian Rejewski who used Enigma blueprint.

How Enigma is Used

year - book w/ 365 day codes

3/7/32 G Q R R3 R2 R1 } Day code example

Operator for each msg picks a message code.

"ZMQ", Sets machine up at the Day Code setting. Encrypts "ZMQZMQ" message code twice. (need to be randomly selected).

Then change machine to ZMQ (msg code)

Operator "weaknesses" exploited

- 1) Some operators always used same msg code
- 2) Allies could sometimes read "first" of individual operators (sending Enigma messages)

How Rejewski Broke Enigma

Every permutation function can be viewed as a set cycles?

3, 5, 4, 1, 6, 8, 2, 7

(1 → 3 → 4 → 1) 3

(2 → 5 → 6 → 8 → 7 → 2) 5

1 → 3

2 → 5

3 → 4

4 → 1

5 → 6

6 → 8

7 → 2

8 → 7

Property of the machine uncovered by Rejewski
is that every setting on machine induced
a different set of cycle lengths.

Built his own Enigma replica.

One year, from every position, encrypted
every letter to make a chart:

R1 R2 R3 BQA 3, 12, 2, 9

2, 3, 9, 12 $\longrightarrow$ R1 R2 R3 BQA
:

3, 7, 8, 8 $\longrightarrow$ R2 R1 R3 ZAM
etc.

Polish reading Enigma 1934-1939

* 1939 - Germans added Rotor 4, Rotor 5.

$$\begin{array}{c} 5 \\ \hline \text{1st} \\ \text{rotor} \end{array} \times \begin{array}{c} 4 \\ \hline \text{2nd} \end{array} \times \begin{array}{c} 3 \\ \hline \text{3rd} \end{array} = 60$$

② Same rule - would have taken 9 more years!
TOO LONG!

1940 - Polish shared Enigma advances w/ British.

Alan Turing in charge of breaking Enigma -
he knew of Rejewski's work!

Turing built a machine called "bombe" to
automatically generate charts like Rejewski's for
all of the new settings.

* Weather Report

* fed no letter encryptions to itself

* operators who didn't use random msg codes.
(one guy used girlfriend's initials!)

Navajo Code

2 Navajo ~~ated~~ IN US MILITARY

29 recruited to help in 1st batch

1. If word existed in Navajo just say it!
2. Use code words for military specific things (started ~ 300ish grew to 700 words)
3. Spell out a word letter by letter
each letter has multiple encryptions