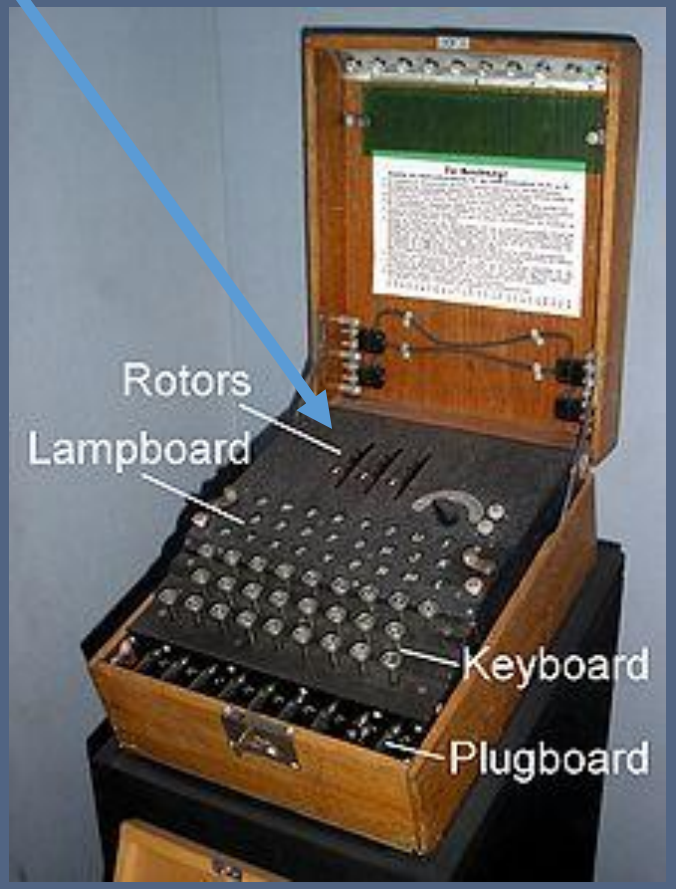
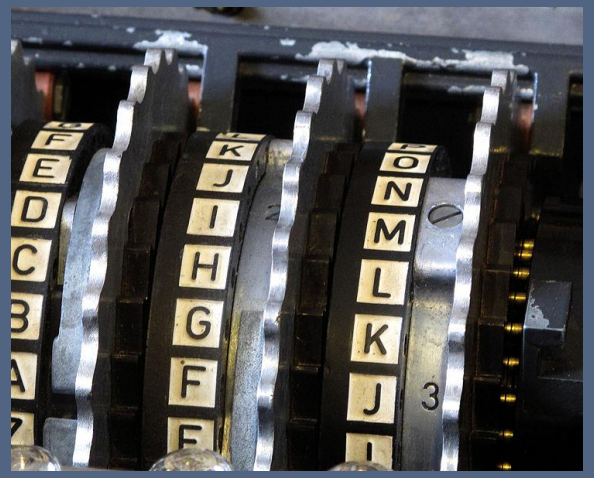
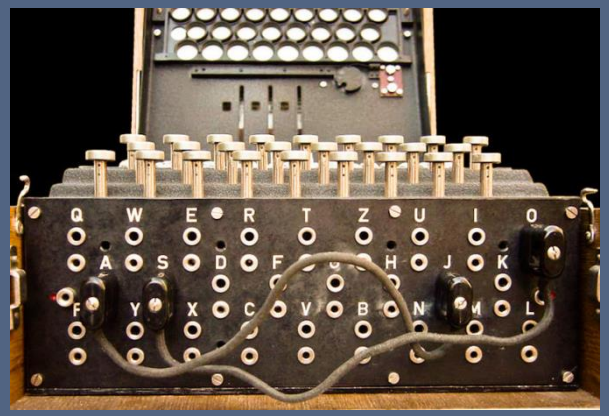
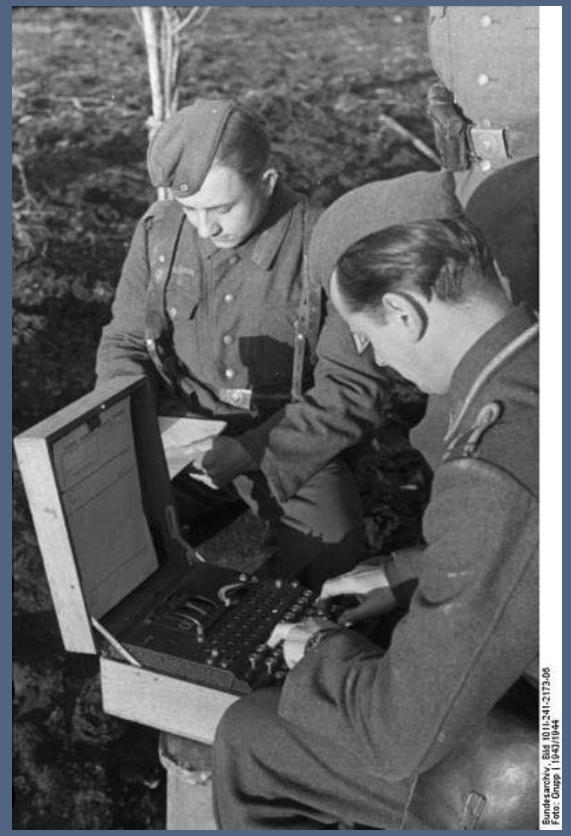
Enigma

Three letters show through the windows:





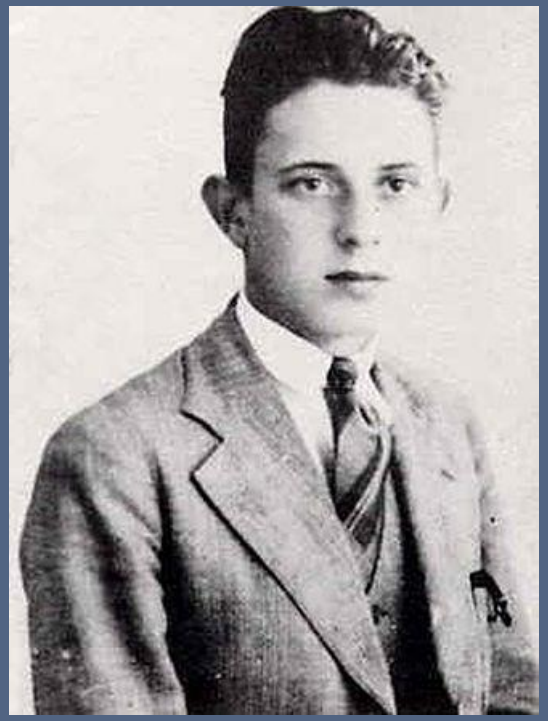




The Polish Codebreakers

- Marian Rejewski,

- Jerzy Rozycki,



- Henryk Zygalski

Photos: Wikipedia

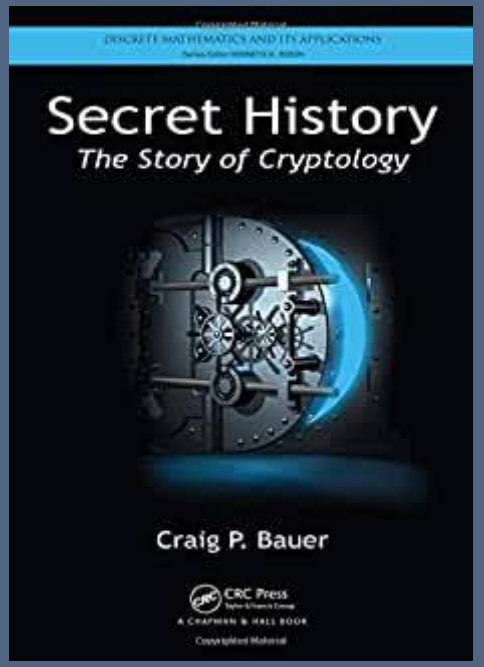
The Poles' Story

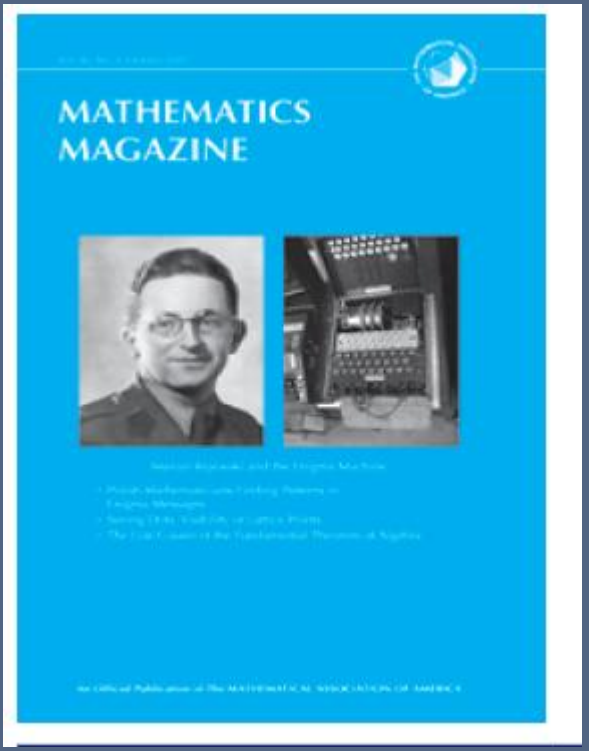
- Involves classic espionage (secret agents stealing documents and passing them off to other government agencies)
- Daring escapes from the advancing German army
- Some unfortunate deaths…
- And…

… mathematicians as real life war heroes!

For more details and mathematical descriptions see:

1. “Polish Mathematicians Finding Patters in Enigma Messages”, Chris Christensen, Mathematics Magazine, 80:4, 2007.
2. Secret History: The Story of Cryptology, Craig Bauer, 2013.





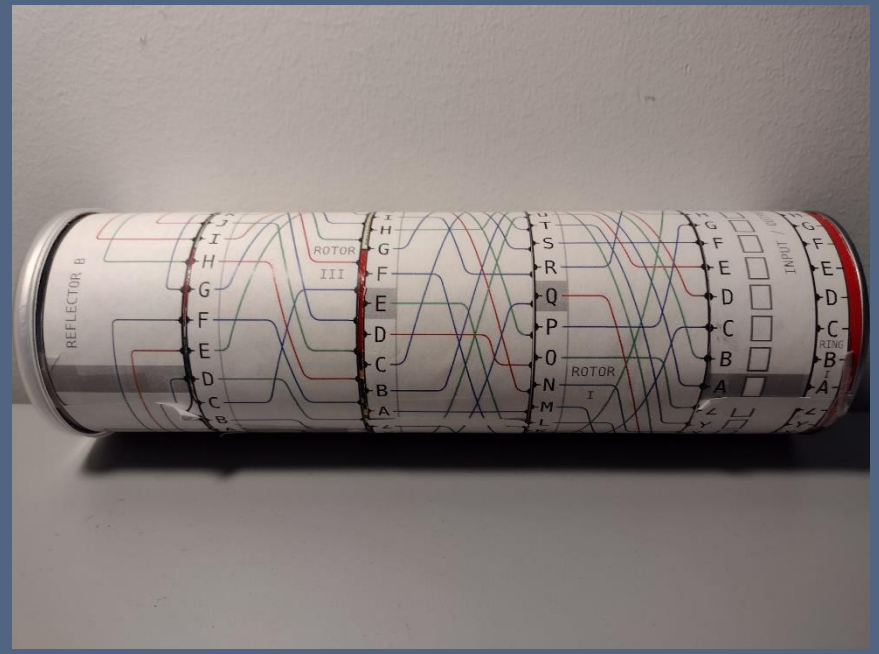
Today:

Goal: Share an assignment I used as the final assignment in a 10 week (once a week) Mathematics Seminar on Enigma.

- No real mathematical prerequisites.
- Synchronous meetings on Zoom, once a week.
- A weekly assignment/discussion.
- We learned how Enigma worked, built our own working Enigma machines (Pringle Can Enigma), and worked through the Polish Codebreakers attack on Enigma (pre 1939).

But…

To understand the assignment, you need to understand how the Poles attacked Enigma on a daily basis.



Polish Codebreakers' Daily Routine (pre 1939)

Early in 1938, the Poles were reading 75% of all Enigma enciphered traffic!

- Use the repeated encrypted message keys to deduce the "product permutations": DA, EB, FC
- Use the "finger theorem" and the "psychological method" to factor these permutations: A, B, C, D, E, F
- Use the cycle structure of DA, EB, FC to help determine the rotor settings.
- Use cribs or other partial decryptions to deduce the plugboard settings.

Enigma is broken for the day!

Daily Keys

- Enigma users would look up the daily key (rotor/ring/plugboard settings) in a codebook.

There are about 7,156,755,732,750,624,000 possible such keys!

But, not every message sent on a given day used the “daily key”.

Since, the first letter of every message would have been encrypted using the same cipher.

The second letter of every message would have been encrypted using the same cipher.

The third letter of every….

So, one could use simple frequency analysis to break Enigma.

How Enigma Was Used [at first]: Indicator Method

- Read the daily key from the code book and set up your Enigma (rotor settings, ring settings, plugboard settings, ground setting).
- Pick three random letters for the message key.
- Type these into the Enigma… TWICE
- Set your rotors to the message key.
- Encrypt the message.
- Send the encrypted message key (six letters) followed by the encrypted message.

Recover the product permutations

When the Enigma is set to the daily key, let:

A = the first permutation that occurs

B = the second…

C = the third

D = the fourth

E = the fifth

F = the sixth

Note:

Every Enigma permutation swaps 13 pairs of letters.

That is, the same settings are used for both encryption and decryption.

If you intercepted QGF BQP, what does this tell you?

A: ? → Q and Q → ?
B:
C:
D: ? → B

Under DA (permutation A followed by permutation D):

Q → B

We've extracted some information from "thin air"!

A look at the “Intelligence Report”

One will find:

- DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM)(L)(V)
- EB = (ASUGKHC)(DFYTZVR) (EOJM) (IQLX) (B) (N) (P) (W)
- FC = (BNQRFES) (GKHPLMY) (CWJ) (OTV) (DU) (AI) (X) (Z)

Note:

1. Cycles come in pairs.
2. Cycle structure + Polish Catalog ➔ most of the daily key (not the plugboard)!

Factoring permutations with the “finger theorem”:

- DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM) (L)(V)

A: (AM) (YT) (KJ)…. (CE) (LV)

D: (YM)(KT)…(AE) (LV)
[start over with your left finger one position to the right]

Or…

Eleven other possibilities!
You can start with your fingers anywhere!

Psychological method:

Take another look at the "Intelligence Report"

Who typed WWW?

DA = (AYKRBXHFSWDC) (EZGIOPNUQJTM)(L)(V)

EB = (ASUGKHC)(DFYTZVR) (EOJM) (IQLX) (B) (N) (P) (W)

FC = (BNQRFES) (GKHPLMY) (CWJ) (OTV) (DU) (AI) (X) (Z)

Under B: W → P, N, or B
Under C: W → O, T, or V

Op1	IVI	ORA
Op2	FBK	SBH
Op3	KMO	RET
Op4	PHS	NCB
Op5	RAJ	BSC
Op6	XKA	HHI
Op7	DQD	CLU
Op8	VYT	VTV
Op9	BPY	XPG
Op10	YFT	KYV
Op11	FRG	SDK
Op12	NBV	UBO

Operator 12!
So…. Under A: W →N

Redo the finger theorem to get A and D

Similarly, use the other intelligence “tidbits” to deduce permutations B, C, E, F.

A = (AI)(YG)(KZ)(RE)(BM)(XT)(HJ)(FQ)(SU)(WN)(DP)(CO) (LV)
D = (YI)(KG)(RZ)(BE)(XM)(HT)(FJ)(SQ)(WU)(DN)(CP)(AO) (LV)

B = (WB)(NP) (AR)(SV)(UZ)(GT)(KY)(HF)(CD) (QO)(JI)(MX)(EL)
E = (WB)(NP) (SR)(UV)(GZ)(KT)(HY)(CF)(AD) (JQ)(MI)(EX)(OL)

C = (WV)(JT)(CO) (QL)(RP)(FH)(EK)(SG)(BY)(NM) (AU)(ID) (XZ)
F = (JV)(CT)(WO) (RL)(FP)(EH)(SK)(BG)(NY)(QM) (IU)(AD) (XZ)

Whew!

We now have:

- Daily key (except plugboard)
- The first six permutations that will be performed with that key (with the plugboard).

How?

All we now need is….

… the plugboard!

We need:

1. A working Enigma: Universal Enigma
2. Some known pt/CT
    - The 47 Session key intercepts
    - The “weather report” crib

Method:

1. Type in pt/CT, compare with CT/pt.
2. If it doesn’t match, adjust the plugboard.
3. Repeat…

Example:

1. Use what we know about A,B,C,D,E,F to determine Op1's message key: ASD
2. Set Enigma to known part of the Daily Key (no plugboard), change rotors to ASD.

This yields:

Pt: `weath errep ortis asfol lows`

CT: `RTDKJ PSNMG BYUHO NBBHW SJDD`

Maybe, add IT to the plugboard?

Compare our CT with Op1's CT:

CT: `RTDKJ PSNMG BYUHO NBBHW SJDD`

OP1CT: `RINXJ PANCL BYNDT CMBHK OJDE`

The Assignment:

- Hand out the “Intelligence Report”
- Break up the entire process into four assignments (delivered over Canvas) [prompts are all in Fieldwork Assignment]
- I act as the “Catalog”. When students determine the cycle structure of the product permutations, they send them to me and I’ll respond with the correct rotors/positions.

But…

On September 15, 1938, Germany stopped using this indicator method (encrypting the message setting twice)

This method no longer worked… ☹

New techniques: Zygalski sheets, Rozycki's "Clock Method" [used IC], bomba (bombe)

And… introduced a fourth and fifth rotor…

Now there are 60 possible rotor orders!

Recovery of the daily keys are now 10 times harder!

The story continues…

- Germany invades Poland in September, 1939.
- Poles madly gather their work and flee the advancing German Army, eventually setting up in France.
- Germany invades France in 1940. Poles move to North Africa, then back to France, Portugal, and England.

Rozyski died when the ship he was traveling on from North Africa back to France was sunk in 1942.

Jerzy Rozycki memorial bench near Warsaw.

Memorial to polish cryptologists, Poznan.

Rejewski memorial unveiled in 2005

Images: Wikipedia

The story continues…

The chief cryptanalyst for the USCG was Elizebeth Smith Friedman. Her team ended up breaking a couple of different Enigma machines. Pencil/paper techniques?

- England takes over the majority of the work on breaking Enigma (Alan Turing at Bletchley Park, *The Imitation Game*)
  - Turing redesigned the Polish Bomba and by 1942 the English were decrypting around 50,000 Enigma messages a month.

- The German Navy starts using a 4-rotor Enigma…messages dry up and allied sinking in the Atlantic sky rocket!

Side story: In 1940 the USCG begins intercepting coded messages in South America. They notice that no letter was getting encrypted to itself and that the cipher was a product of transposition (encryption = decryption)

Enigma!

The story continues…

The U.S. focusses it attention on the Japanese Cipher machine,

PURPLE

Another amazing cryptographic story!

Cycle Structure Facts

1. Different initial settings produce different cycle structures in DA, EB, FC.

2. Cycle structure is unaffected by the plugboard (or rings)! ← Math Theorem!!

   This means that instead of having seven quintillion settings to worry about, there are only 105,456 initial settings!

3. There exist 21,230 different cycle structures.

4. About 92% of cycle structures correspond to unique rotor settings. But some correspond to hundreds and one to 1,771 settings.

So,

- The Poles built a catalog for each of the 105,546 settings!

"tedious…time-consuming"

"men would scrape their fingers raw and bloody"

- They finished the catalog on November 2, 1937. Whew…

Then…

- The Germans started using reflector B, instead of reflector A, and all the cycle structures changed!!!

- The Poles rebuilt the catalog.

Crypto Museum exhibit in Poznan, Poland