Voting Systems, Mass Murder, and the Enigma Machine

Jordan Schettler

Department of Mathematics
University of Arizona

3/22/11

Outline

Der Reichstag

German Parliamentary Election Results

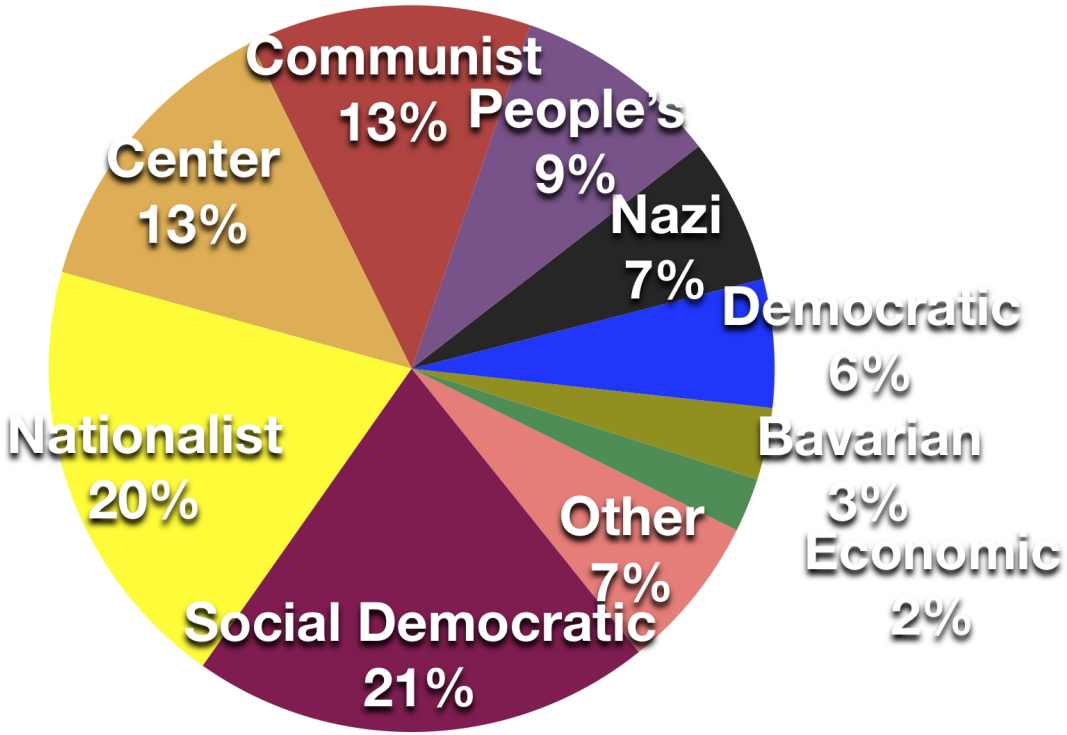


Figure: SPRING 1924

German Parliamentary Election Results

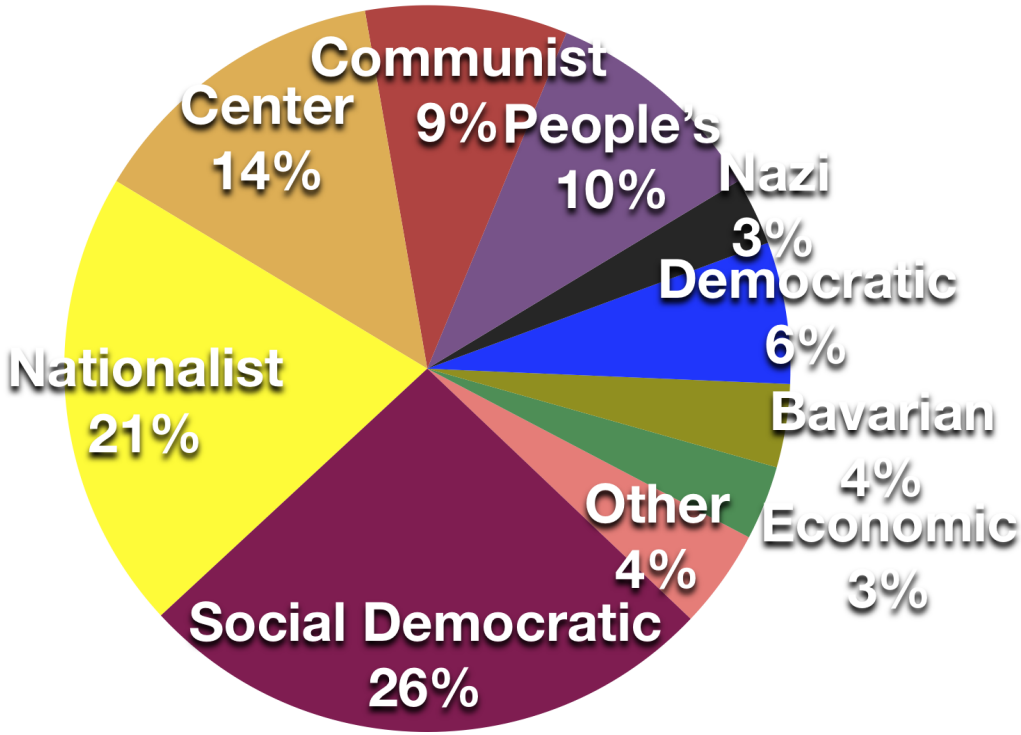


Figure: WINTER 1924

German Parliamentary Election Results

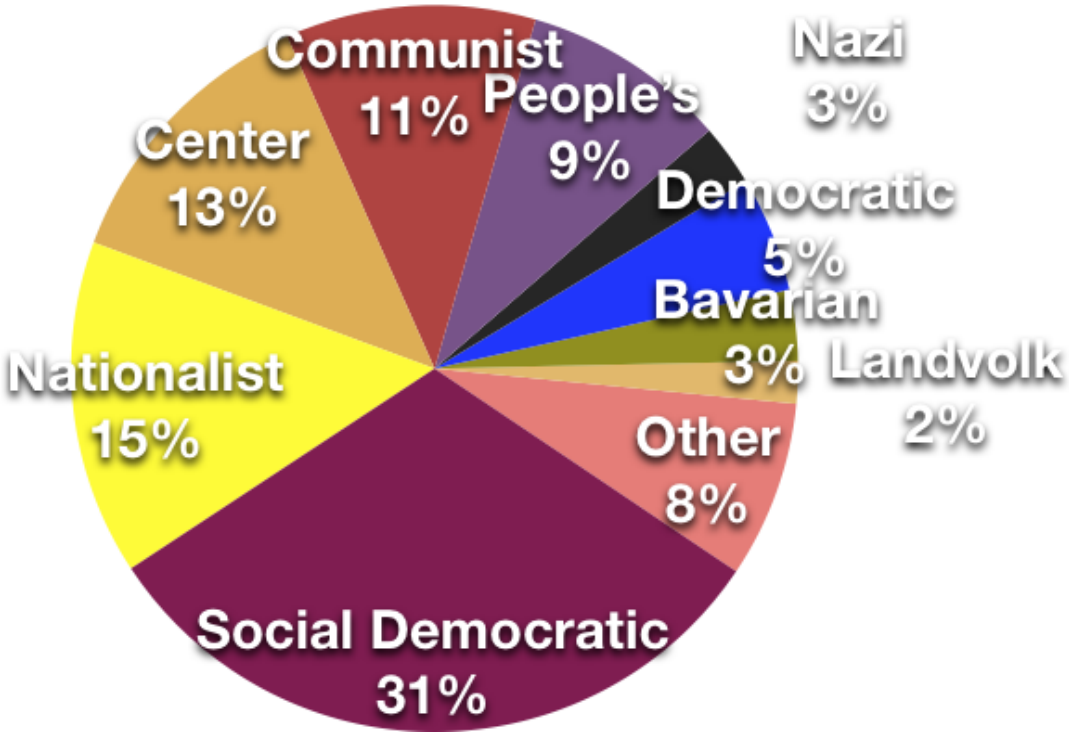


Figure: SPRING 1928

German Parliamentary Election Results

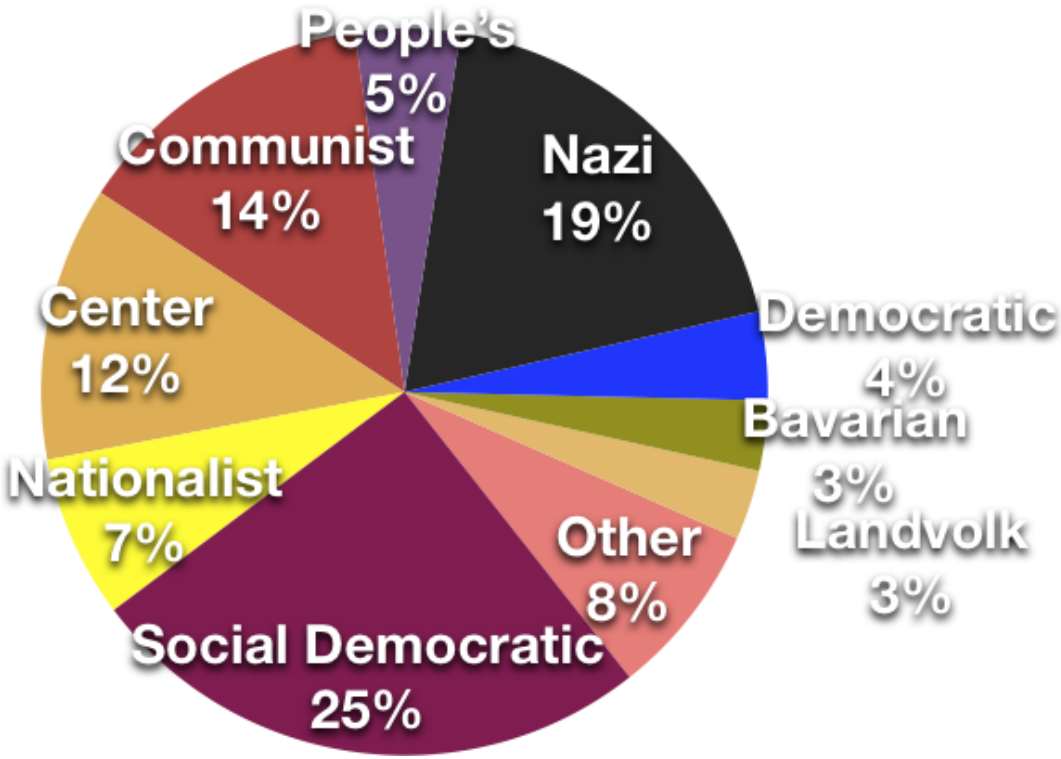


Figure: FALL 1930

German Parliamentary Election Results

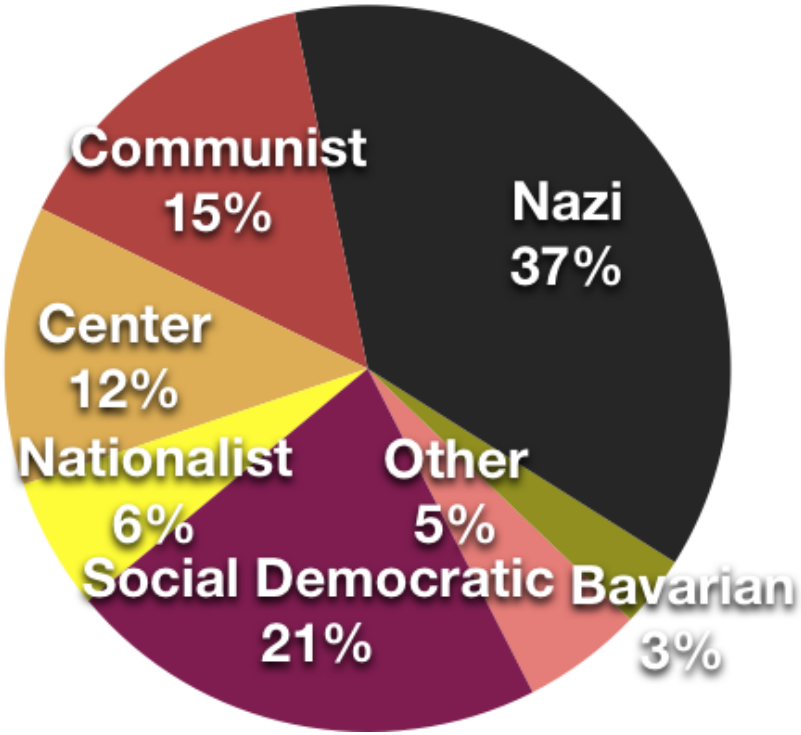


Figure: SUMMER 1932

German Parliamentary Election Results

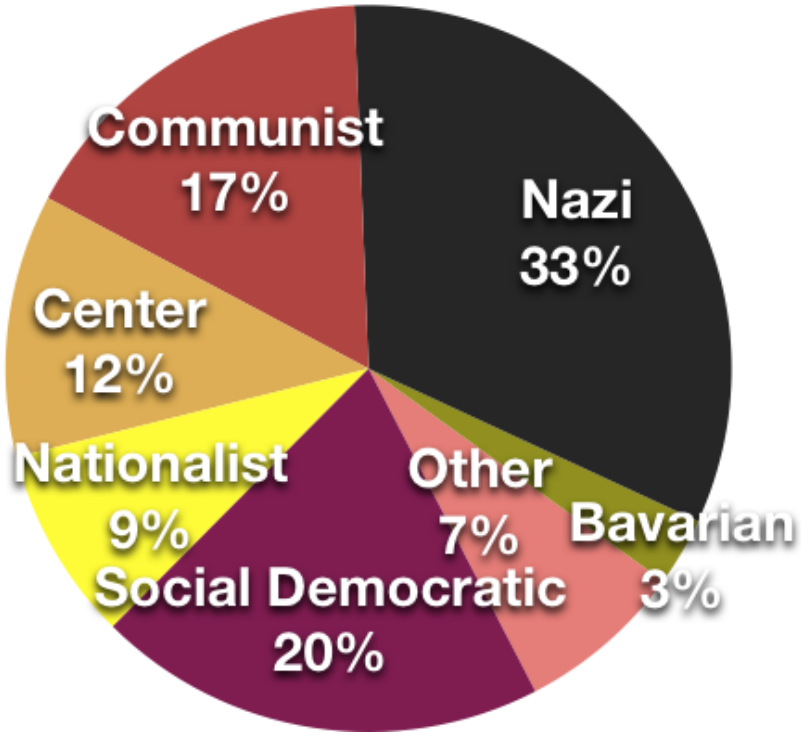


Figure: FALL 1932

German Parliamentary Election Results

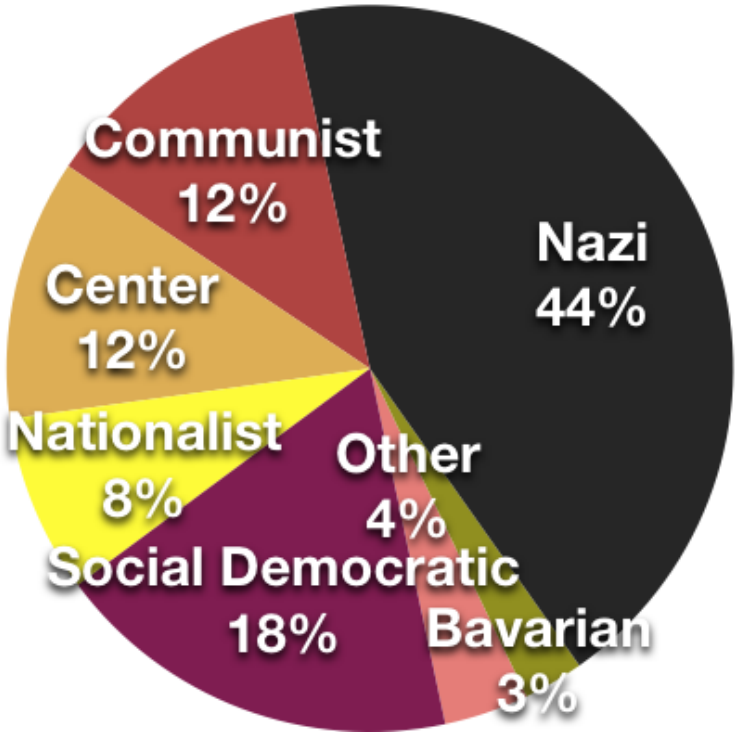


Figure: SPRING 1933

German Parliamentary Election Results

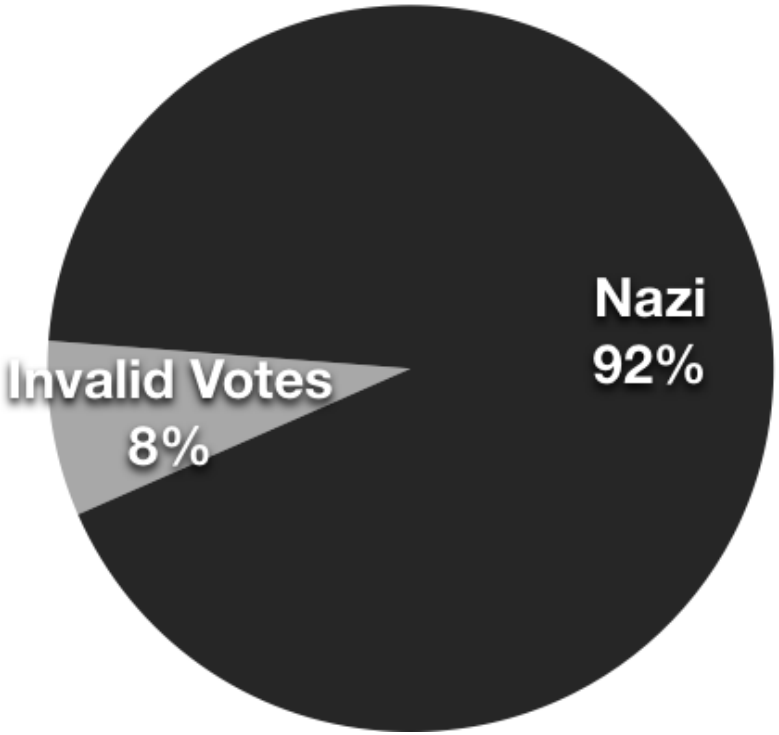


Figure: FALL 1933

“I consider it completely unimportant who in the party will vote, or how; but what is extraordinarily important is this — who will count the votes, and how.”

Figure: Joseph Stalin

1932 German Presidential Runoff: Round One

Candidate	# of votes	%
Hindenberg	18,651,497	49.6
Hitler	11,339,446	30.2
Thälmann	4,983,341	13.2
Düsterberg	2,557,729	6.8

No **majority**; Düsterberg withdraws; a revote is held.

1932 German Presidential Runoff: Round Two

Candidate	# of votes	%
Hindenberg	19,359,983	53.1
Hitler	13,418,517	36.7
Thälmann	3,706,759	10.1

Hindenberg wins with majority...

but if no Thälmann supporters changed their votes, round 3 would have given Hitler another chance to make up ground.

This an example of **tactical voting**.

In US presidential elections, we only require **plurality** (largest percentage) to win a state. This leads to spoiler situations:

Candidate	%
Clinton	43.01
Bush	37.45
Perot	18.91
Other	0.63

Table: Popular Vote, 1992

Candidate	%
Bush	48.847
Gore	48.838
Nader	1.635
Buchanan	0.293
Other	0.387

Table: Florida Results, 2000

2009 Burlington, VT Mayoral Race: Round One of IRV

1 2 3	Montroll Kiss Wright	Montroll Wright Kiss	Kiss Montroll Wright	Kiss Wright Montroll	Wright Kiss Montroll	Wright Montroll Kiss
#	1621	935	1890	1091	1397	1897
#	2554		2981		3294	

Table: A Possible Preference Schedule

Montroll (D) is eliminated despite being the **Condorcet winner**; votes split among Kiss and Wright.

2009 Burlington, VT Mayoral Race: Round Two of IRV

1 2	Kiss Wright	Wright Kiss
#	2981 + 1621	3294 + 935
#	4602	4229

Table: A Possible Preference Schedule

Wright (R) is eliminated despite having plurality; Kiss (P) wins.

What if Kiss (the winner) had done better?

1 2 3	Montroll Kiss Wright	Montroll Wright Kiss	Kiss Montroll Wright	Kiss Wright Montroll	Wright Kiss Montroll	Wright Montroll Kiss
#	1621	935	1890	1841	647	1897
#	2554		$2981 + 750$		$3294 - 750$	
#	2554		3731		2544	

Table: A Possible Preference Schedule

Wright (R) is eliminated; votes split among Kiss and Montroll.

What if Kiss (the winner) had done better?

1 2	Montroll Kiss	Kiss Montroll
#	2554 + 1897	3731 + 647
#	4451	4378

Table: A Possible Preference Schedule

Kiss (P) is eliminated despite doing better; Montroll (D) wins!

This is a violation of **monotonicity**.

Atrocities

Who were the Nazis?

Figure: Hitler, Himmler, & others

- pro-military: regain lost territories and ignore war reparations

Who were the Nazis?

Figure: Hitler, Himmler, & others

- pro-military: regain lost territories and ignore war reparations
- used simplified and symbolic propaganda, fear, repetition, vague promises

Who were the Nazis?

Figure: Hitler, Himmler, & others

- pro-military: regain lost territories and ignore war reparations
- used simplified and symbolic propaganda, fear, repetition, vague promises
- anti-Semitic, anti-Roma, anti-Socialist, anti-Gay, ...: deported/arrested/killed

German Flag and Coat: 1918-1933

Nazi Flag and Insignia: 1933-1945

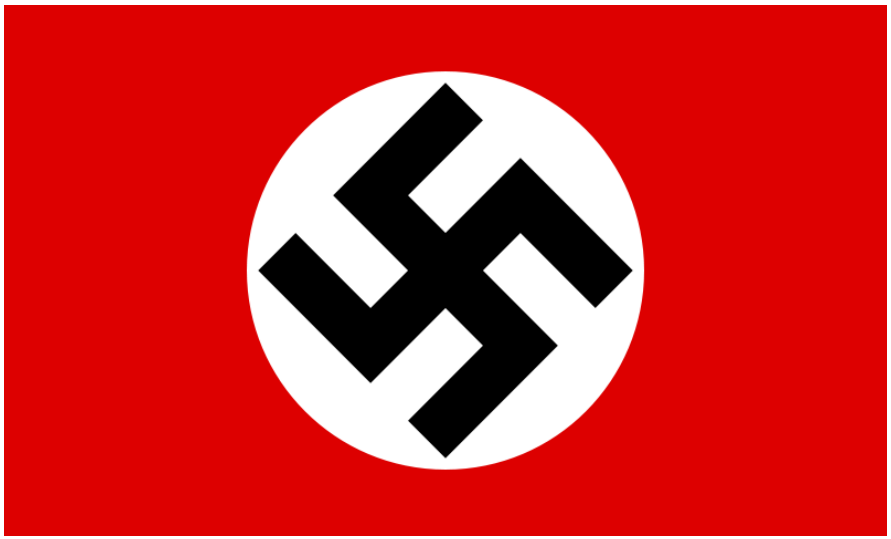


Figure: Nazi Postcard

Figure: Nazi Propaganda Poster

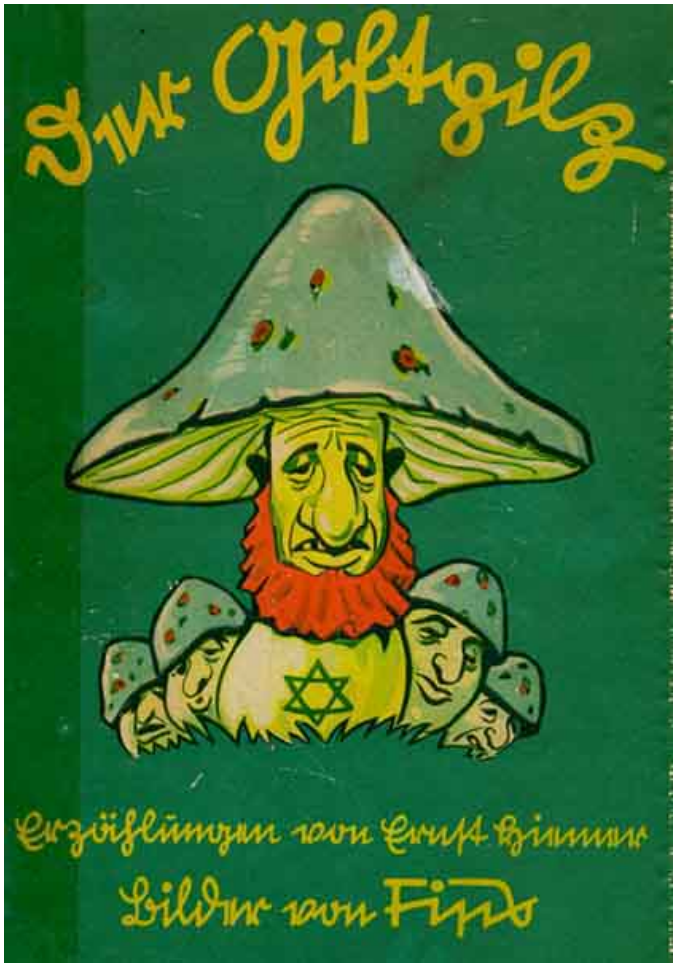


Figure: Nazi Children's Book

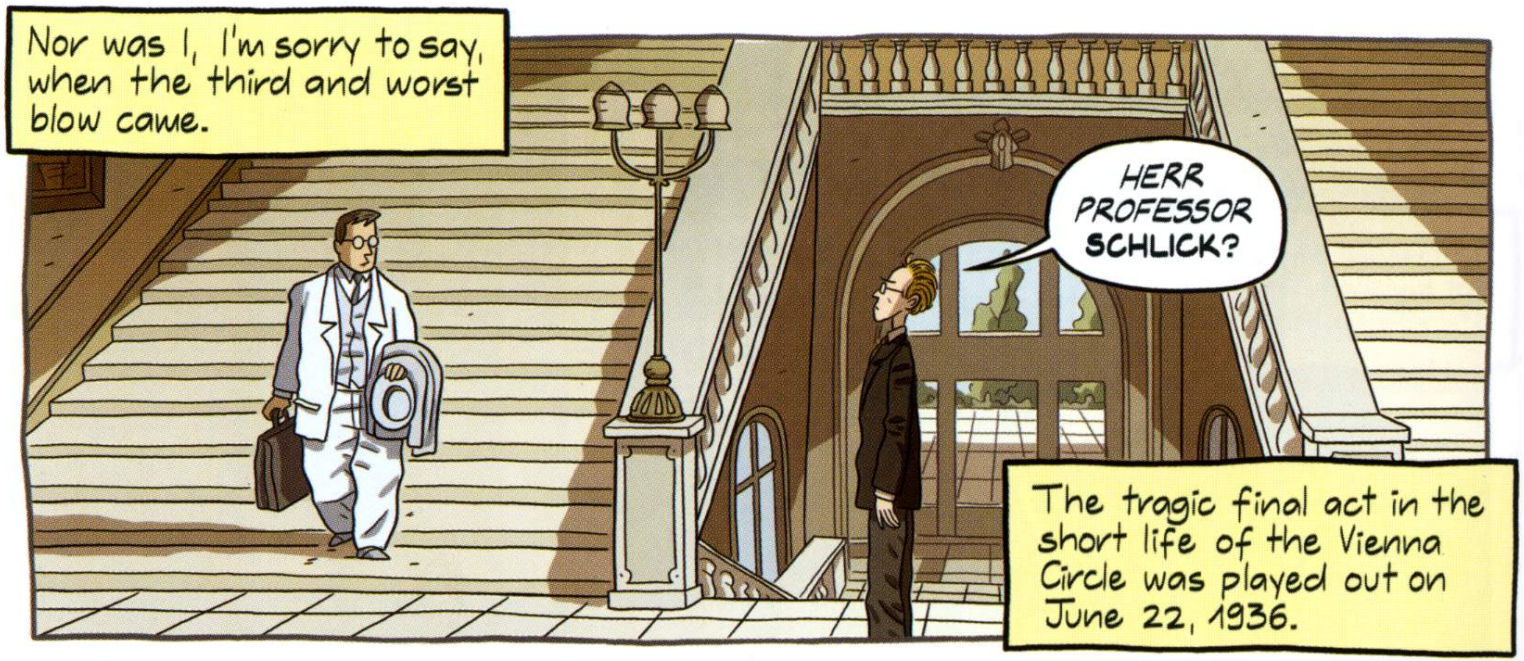
Moritz Schlick was a German philosopher and physicist interested in the foundations of mathematics.

Moritz Schlick was a German philosopher and physicist interested in the foundations of mathematics.

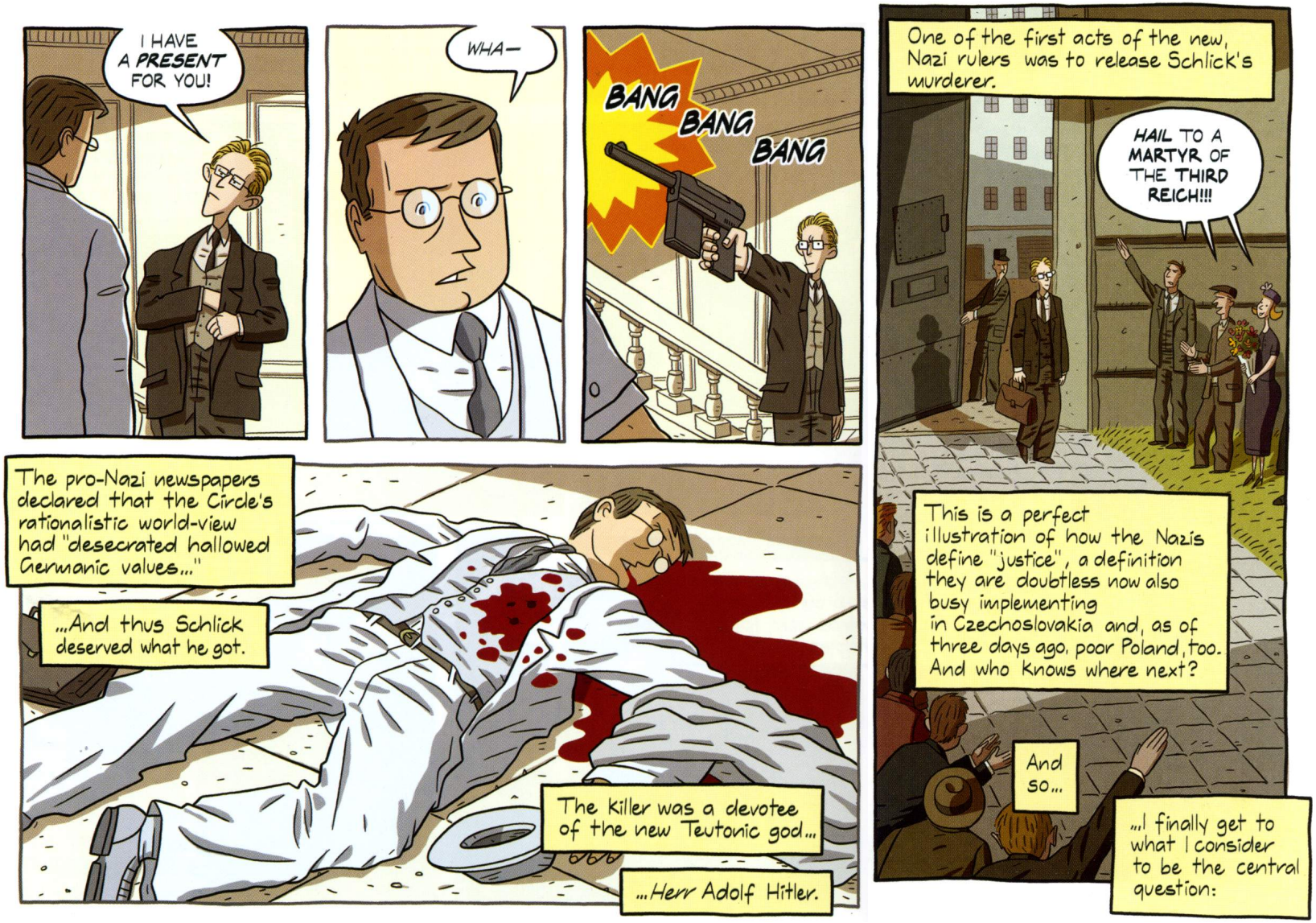
He organized the Vienna Circle, a regular gathering of some of the world's most most preeminent critical thinkers.

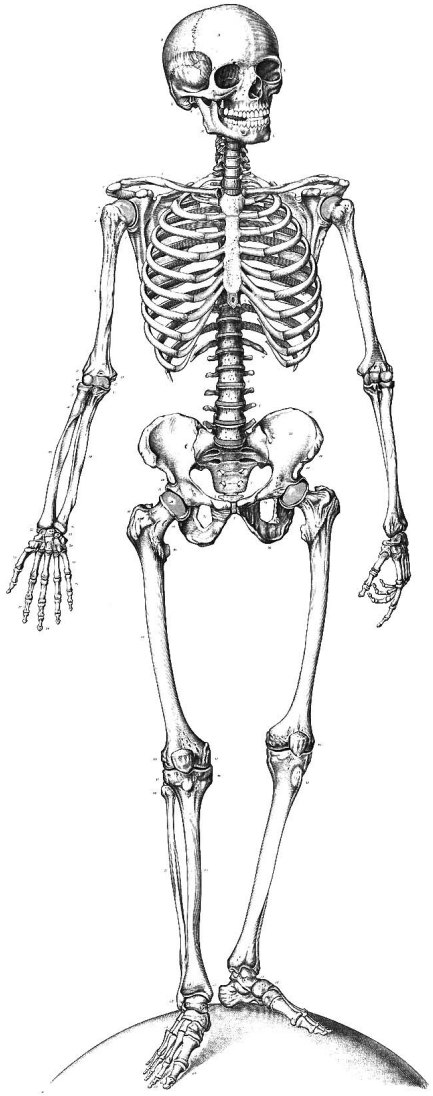
Moritz Schlick was a German philosopher and physicist interested in the foundations of mathematics.

He organized the Vienna Circle, a regular gathering of some of the world's most most preeminent critical thinkers.




I HAVE A PRESENT FOR YOU!
WHA—
BANG
BANG
BANG
The pro-Nazi newspapers declared that the Circle's rationalistic world-view had "desecrated hallowed Germanic values..."
...And thus Schlick deserved what he got.
The killer was a devotee of the new Teutonic god...
...Herr Adolf Hitler.


I HAVE A PRESENT FOR YOU!
WHA—
BANG BANG BANG
The pro-Nazi newspapers declared that the Circle's rationalistic world-view had "desecrated hallowed Germanic values..."
...And thus Schlick deserved what he got.
The killer was a devotee of the new Teutonic god...
...Herr Adolf Hitler.
One of the first acts of the new, Nazi rulers was to release Schlick's murderer.
HAIL TO A MARTYR OF THE THIRD REICH!!!
This is a perfect illustration of how the Nazis define "justice", a definition they are doubtless now also busy implementing in Czechoslovakia and, as of three days ago, poor Poland, too. And who knows where next?
And so...
...I finally get to what I consider to be the central question:



9/11 American Civil War The Holocaust

The Warsaw Cipher Bureau

Permutations

Plaintext:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext:	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J

Permutations

Plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext: E K M F L G D Q V Z N T O W Y H X U S P A I B R C J

SAKSP	VPAPV	YWMVH	QLUS
s u b s t	i t u t i	o n c i p	h e r s

Permutations

Plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext: E K M F L G D Q V Z N T O W Y H X U S P A I B R C J

SAKSP	VPAPV	YWMVH	QLUS
s u b s t	i t u t i	o n c i p	h e r s

Cycle Notation: (aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)

There are many possible substitution ciphers (permutations):

$$26! = 26 \times 25 \times 24 \cdots \times 2 \times 1 = 403291461126605635584000000$$

There are many possible substitution ciphers (permutations):

$$26! = 26 \times 25 \times 24 \cdots \times 2 \times 1 = 403291461126605635584000000$$

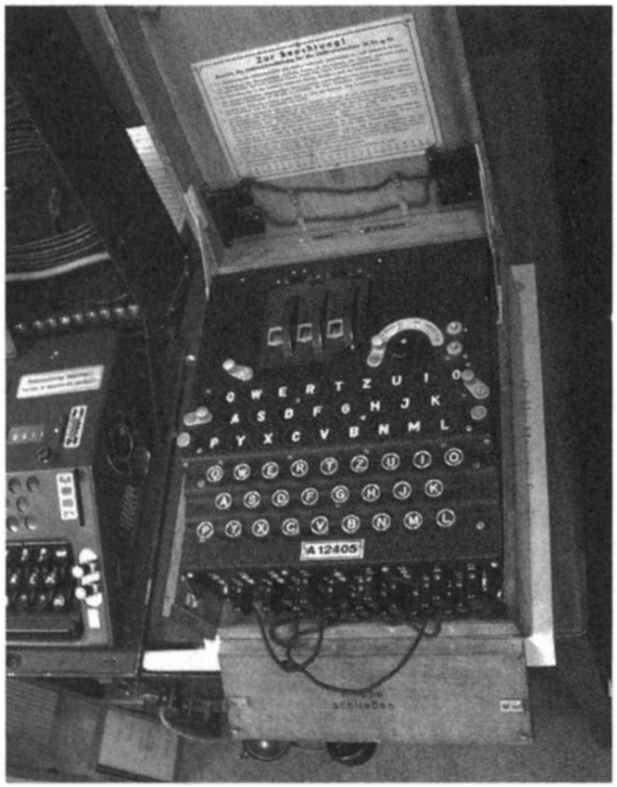
Languages have patterns: e.g., letters like e, t, a, o, i, n, s, occur often, and there are common 2- and 3-letter combos...

There are many possible substitution ciphers (permutations):

$$26! = 26 \times 25 \times 24 \cdots \times 2 \times 1 = 403291461126605635584000000$$

Languages have patterns: e.g., letters like e, t, a, o, i, n, s, occur often, and there are common 2- and 3-letter combos...

For this reason, the Germans came up with a machine to systematically generate a new permutation for every letter.



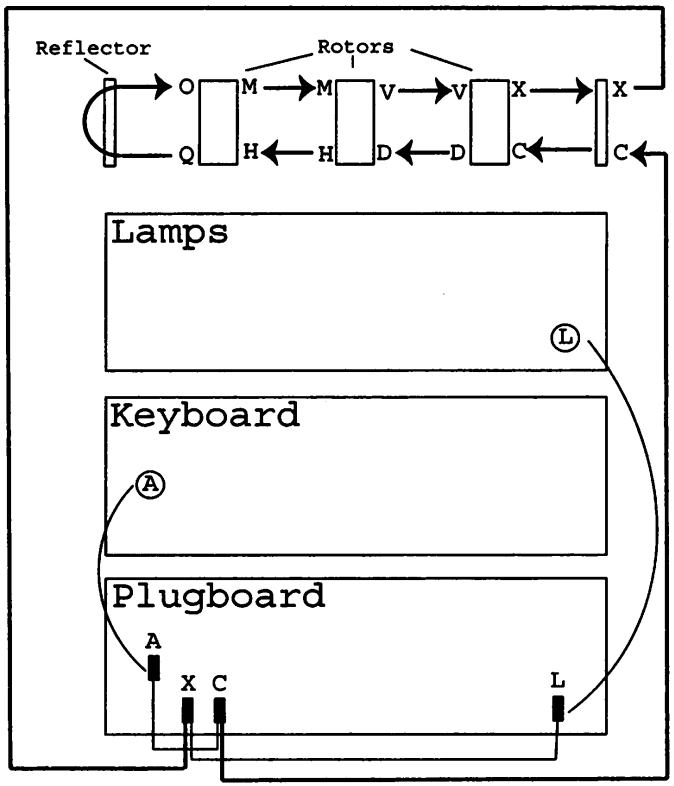


Figure: An Enigma Machine and Diagram

Enigma generates 16,900 permutations for a given setting.

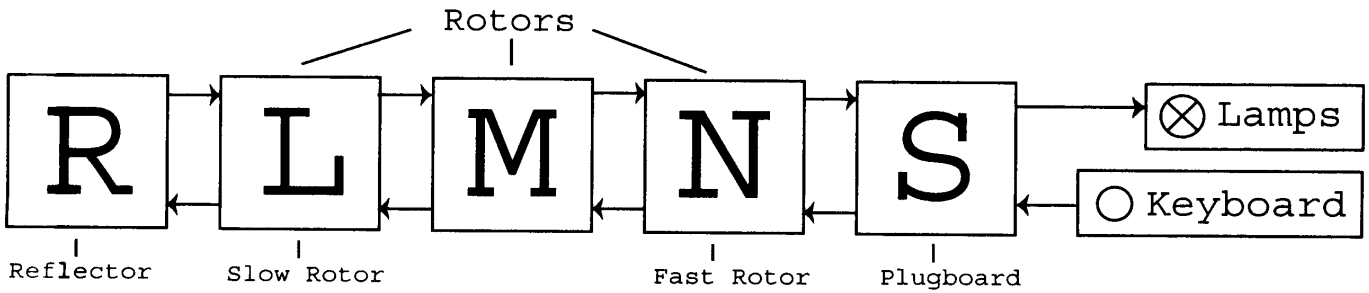


Figure: Enigma Circuit

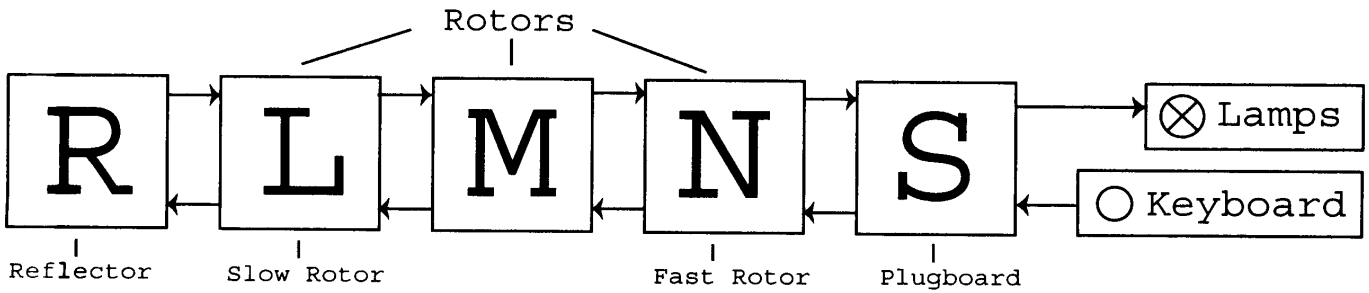


Figure: Enigma Circuit

Each component is a permutation, and composing gives

$$S^{-1}N^{-1}M^{-1}L^{-1}RLMNS,$$

a product of permutations.

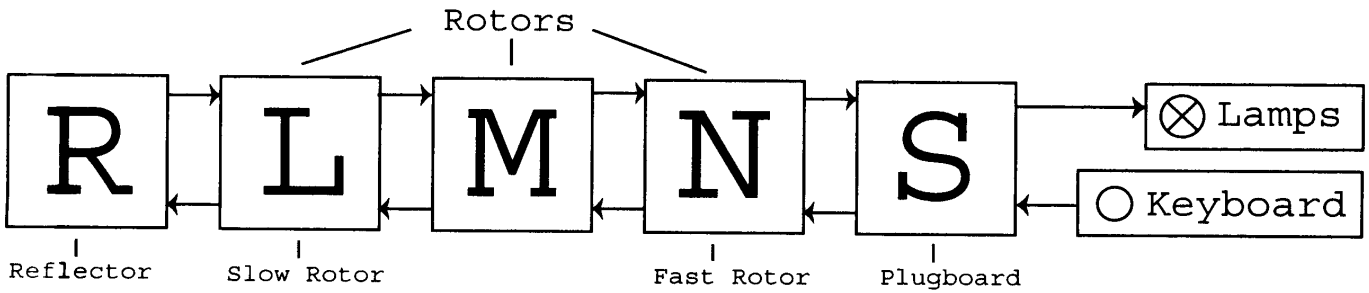


Figure: Enigma Circuit

Each component is a permutation, and composing gives

$$S^{-1}N^{-1}M^{-1}L^{-1}RLMNS,$$

a product of permutations.

Note: composition isn't commutative, so nothing cancels.

The fast rotor moves forward each keystroke, so if

$$P = (\text{abcdefghijklmnopqrstuvwxyz}),$$

The fast rotor moves forward each keystroke, so if

$$P = (\text{abcdefghijklmnopqrstuvwxyz}),$$

then the next letter gets permuted by

$$\begin{aligned} & S^{-1}P^{-1}N^{-1}M^{-1}L^{-1}RLMNPS \\ = \quad & (LMNPS)^{-1}R(LMNPS) \end{aligned}$$

The fast rotor moves forward each keystroke, so if

$$P = (\text{abcdefghijklmnopqrstuvwxyz}),$$

then the next letter gets permuted by

$$\begin{aligned} & S^{-1}P^{-1}N^{-1}M^{-1}L^{-1}RLMNPS \\ = \quad & (LMNPS)^{-1}R(LMNPS) \end{aligned}$$

and the next letter gets permuted by

$$\begin{aligned} & S^{-1}P^{-2}N^{-1}M^{-1}L^{-1}RLMNP^2S \\ = \quad & (LMNP^2S)^{-1}R(LMNP^2S) \end{aligned}$$

The reflector R was self-reciprocal:

$$R^2 = 1 \text{ (the permutation sending each letter to itself)}$$

The reflector R was self-reciprocal:

$$R^2 = 1 \text{ (the permutation sending each letter to itself)}$$

so every Enigma permutation was also self-reciprocal:

$$(X^{-1}RX)^2 = X^{-1}RXX^{-1}RX = X^{-1}R^2X = X^{-1}X = 1$$

The reflector R was self-reciprocal:

$$R^2 = 1 \text{ (the permutation sending each letter to itself)}$$

so every Enigma permutation was also self-reciprocal:

$$(X^{-1}RX)^2 = X^{-1}RXX^{-1}RX = X^{-1}R^2X = X^{-1}X = 1$$

So if we start with the same setting is used to encrypt a message, we can decrypt by typing it into the keyboard.

Being self-reciprocal is convenient, but it's also a weakness.

Being self-reciprocal is convenient, but it's also a weakness.

Another weakness is that of "depth," meaning that the setting needed to be changed for every message.

Being self-reciprocal is convenient, but it's also a weakness.

Another weakness is that of "depth," meaning that the setting needed to be changed for every message.

A groundsetting was used to send 3-letter message settings.

Figure: Marian Rejewski

...found patterns in in these encrypted message settings and used permutation theory to crack the Enigma.

Figure: Marian Rejewski

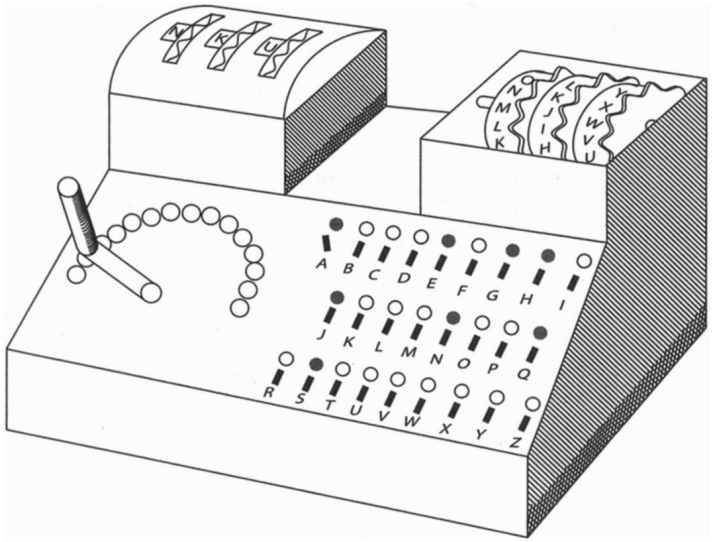


Figure: Cyclometer

...found patterns in in these encrypted message settings and used permutation theory to crack the Enigma.

...used to determine cycle types by replicating Enigma motors.

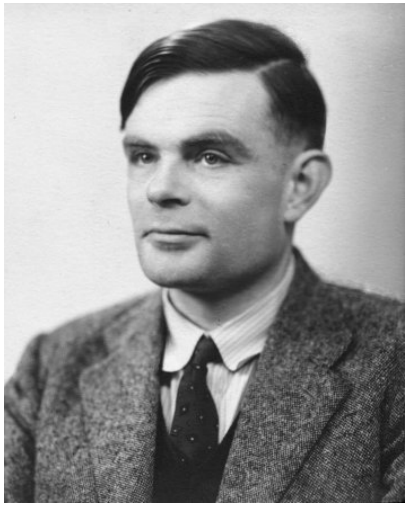


Figure: Alan Turing

... built off the work of Rejewski helping to win the war for the Allies, but he was chemically castrated by his own government for being homosexual.

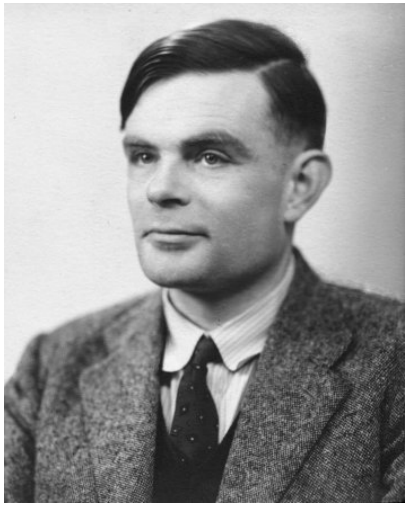


Figure: Alan Turing

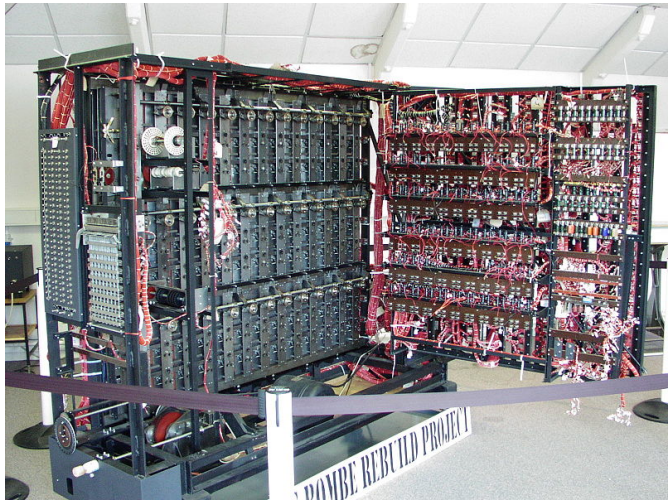


Figure: Replicated Bombe

... built off the work of Rejewski helping to win the war for the Allies, but he was chemically castrated by his own government for being homosexual.

...at Bletchley park; these electromechanical machines were used to determine daily settings by linking up Enigma copies in series.