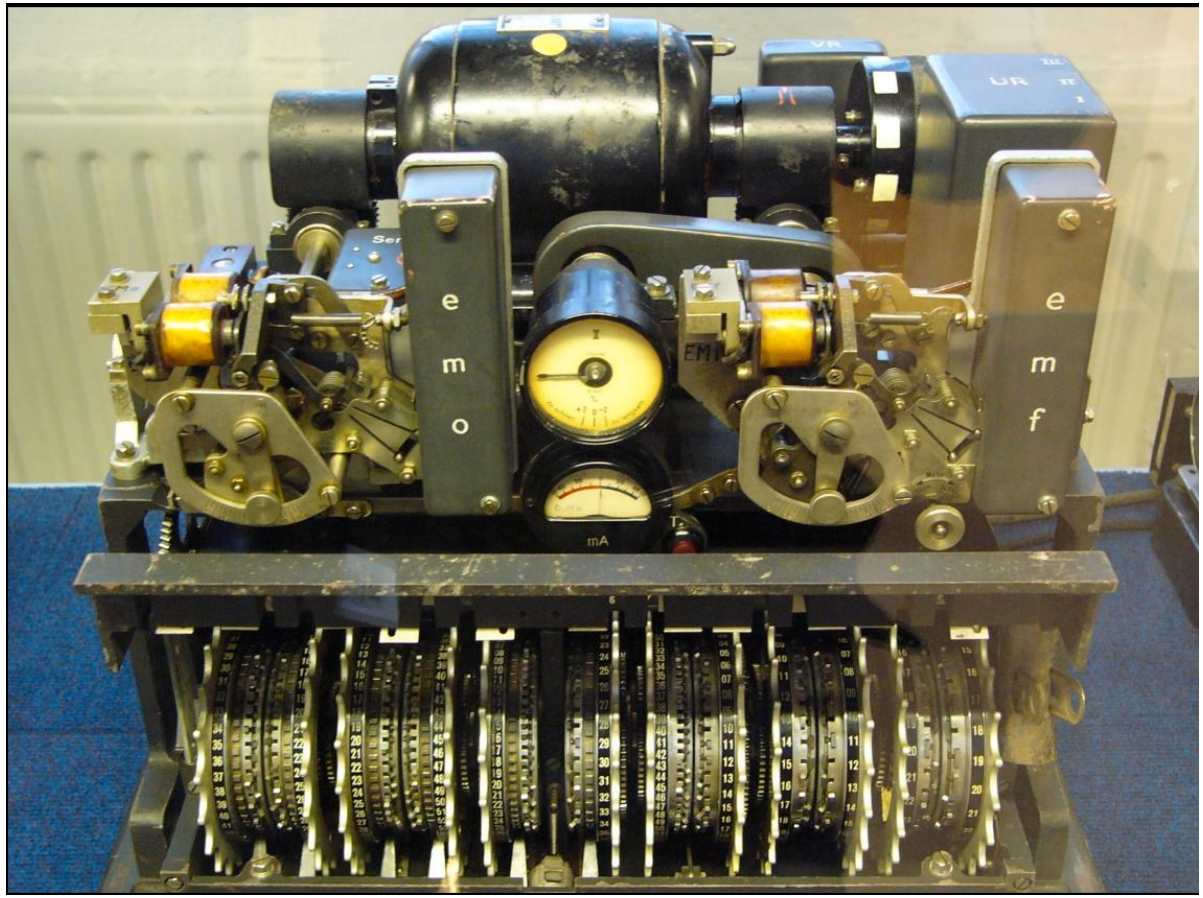
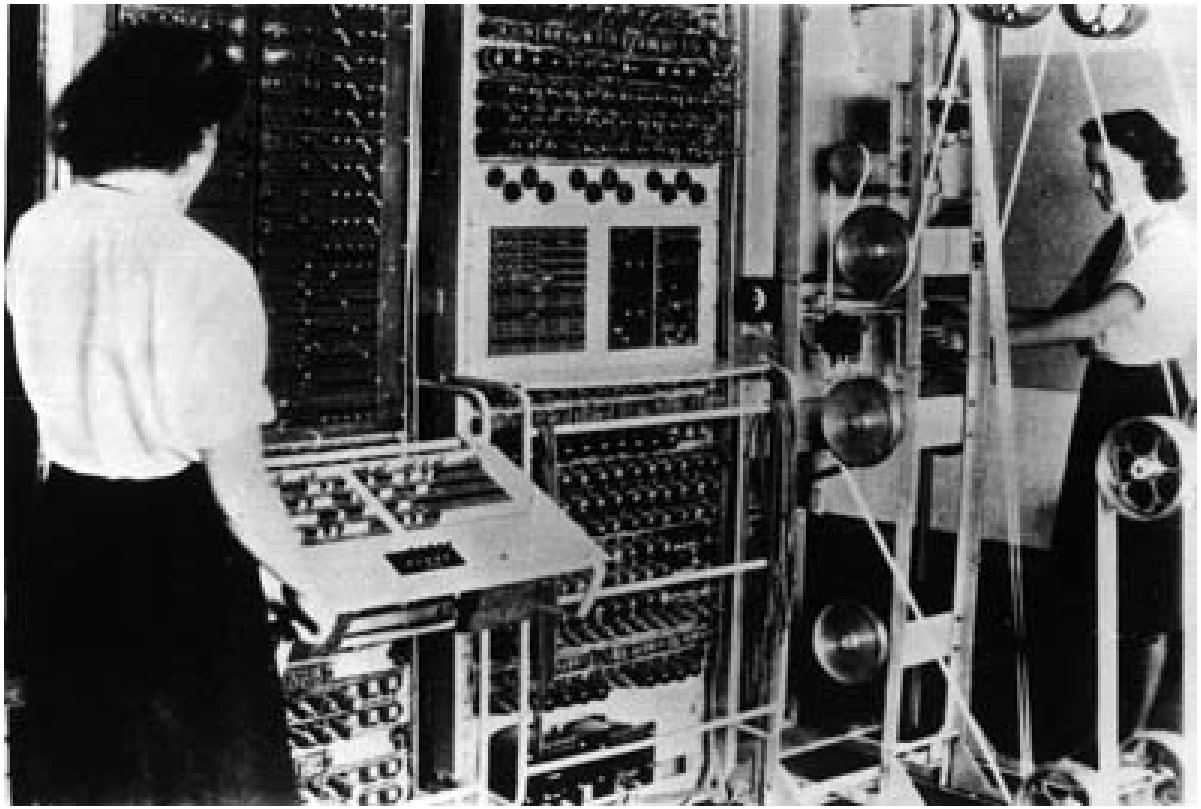
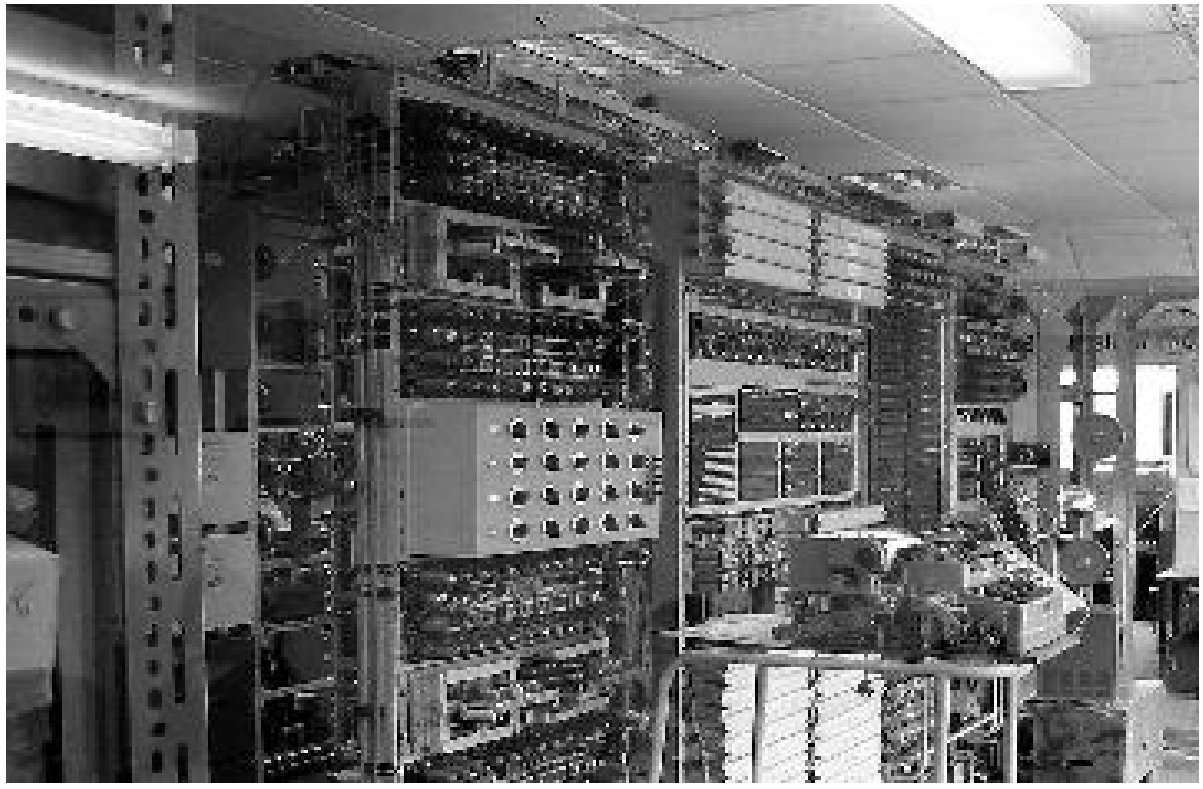
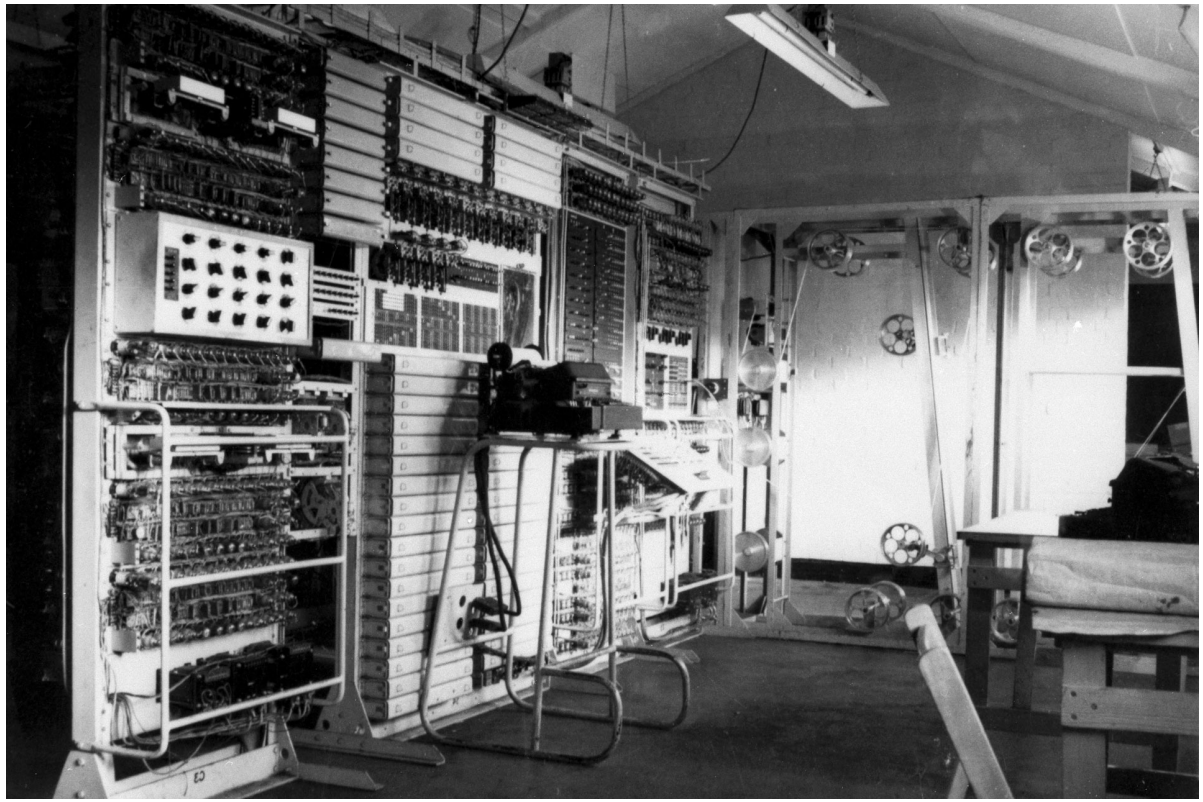
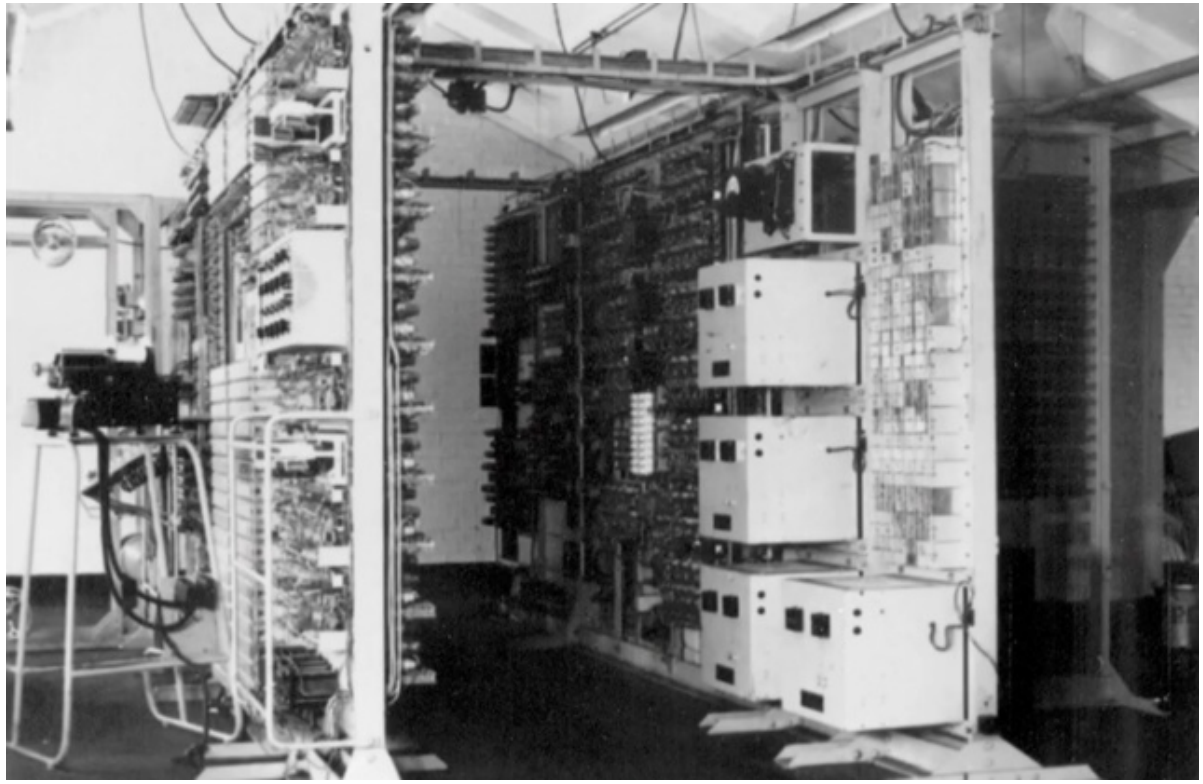


A Lorenz Machine









The Mathematical Complexity of the Enigma Machine and the First Polish Successes in Cracking the Cipher

I. The Enigma Machine
II. Its Mathematical Complexity

Next Time:

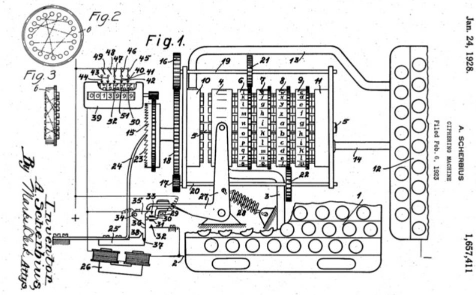
III. How Polish Mathematicians Cracked The Enigma (An Introduction)

I. The Enigma Machine

Arthur Scherbius

October, 20 1878 - May 13,1929

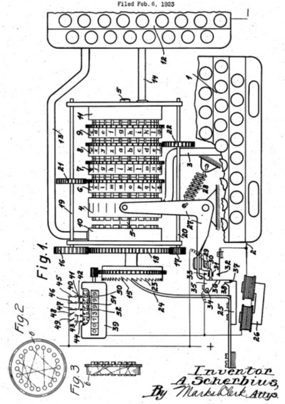
Patent Application Filed February 23, 1918



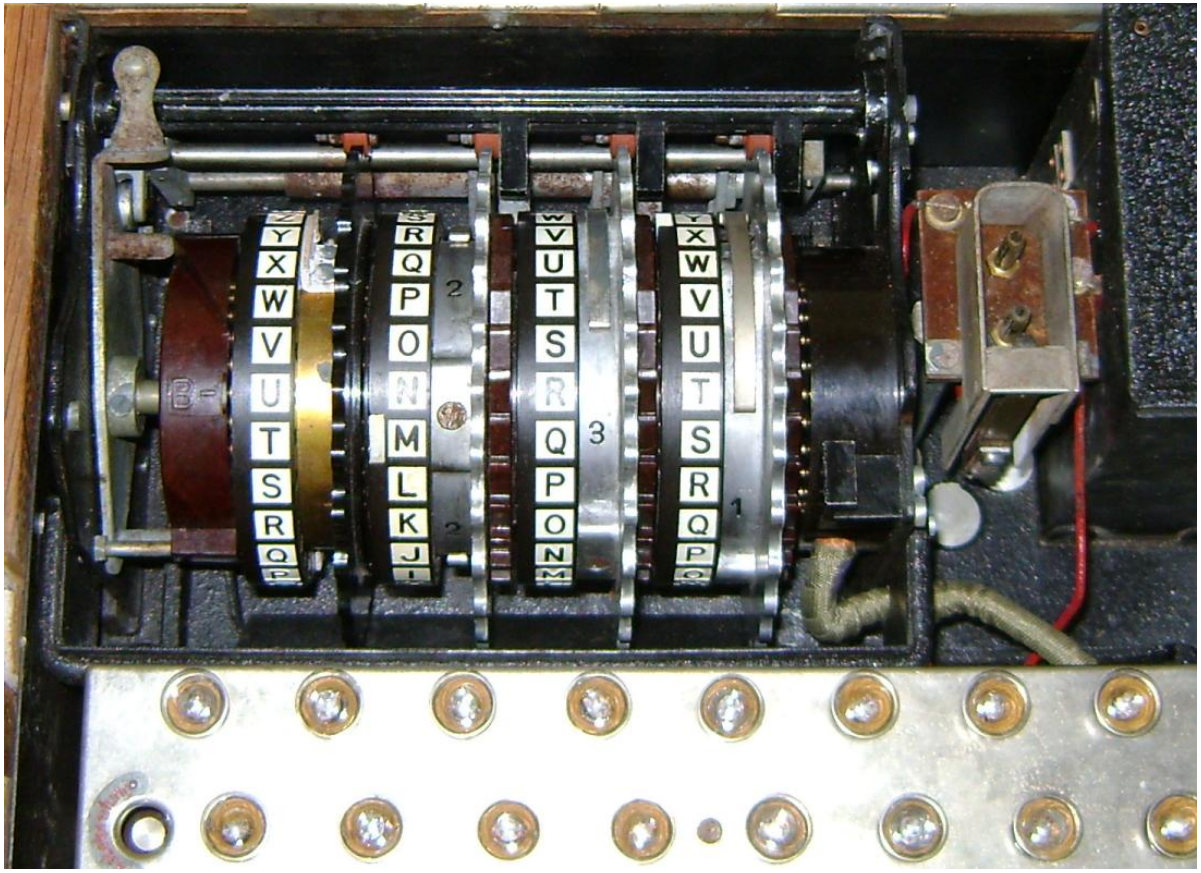
Jan. 24, 1928. A. SCHERBIUS 1,657,411

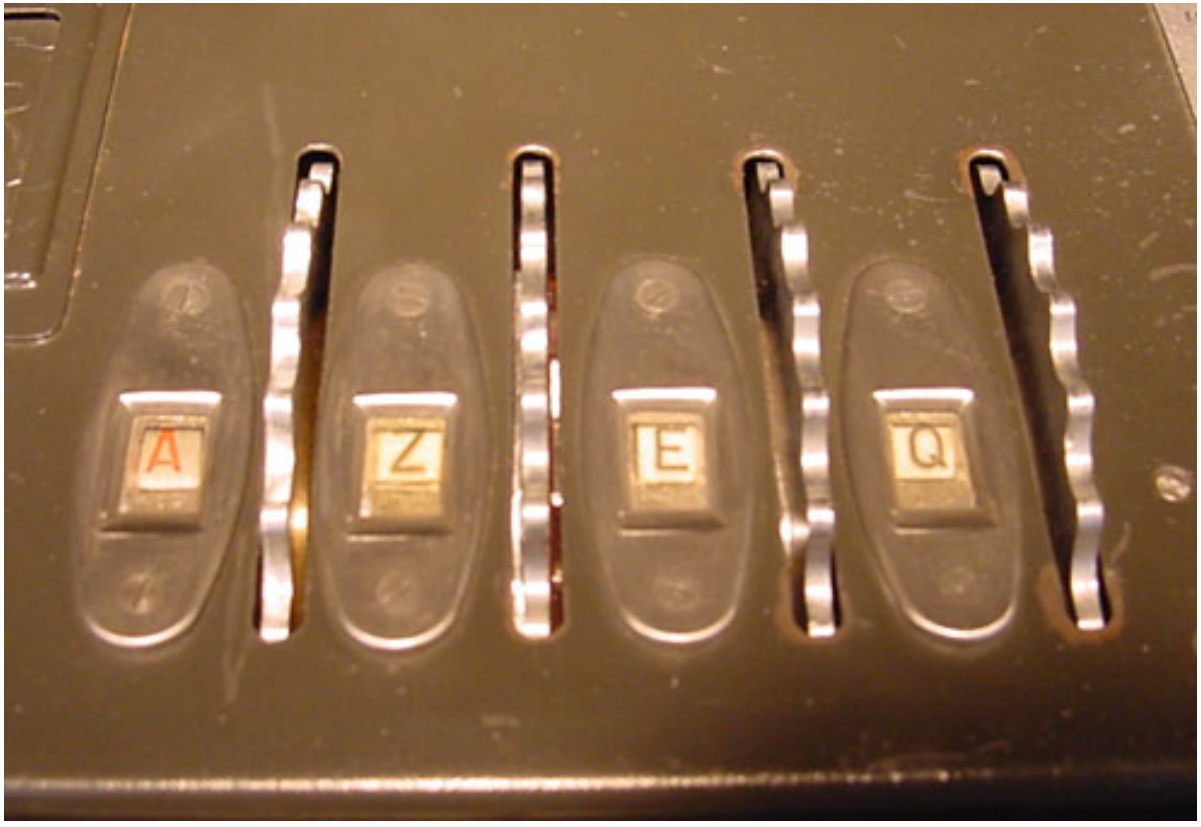
CIPHERING MACHINE

Filed Feb. 6, 1923



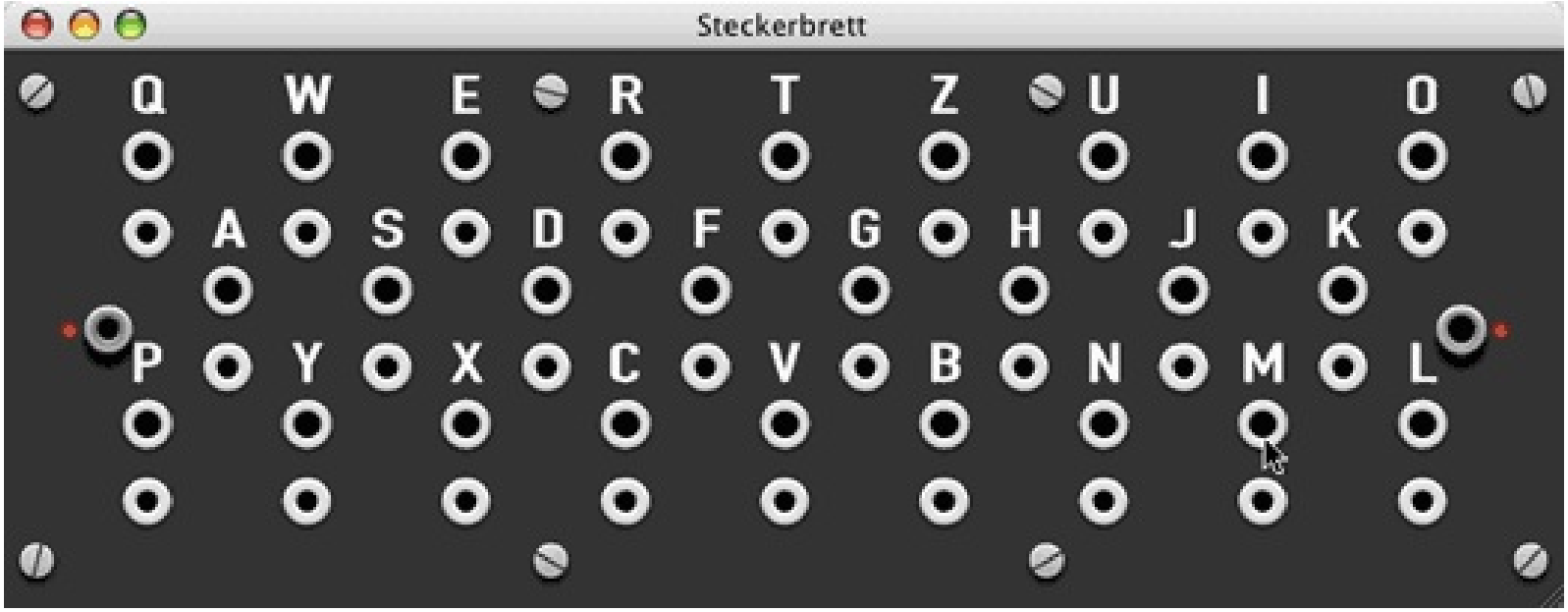

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L


Z Y X W V U T S R Q P
R Q P O N M L K J I
2
2
W V U T S R Q P O N M
3
X W V U T S R Q P
1


A
Z
E
Q


Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L


A1
B2
C3
D4
E5
F6
G7
H8
I9
J10
K1
N14


Steckerbrett
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vcc tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ HM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

II. Mathematical Complexity of the Enigma Machine

Let me count the ways. . .

Simple Multiplication Principle

If there are exactly **a** ways of doing a first task and for each of these ways there are exactly **b** ways of doing another task, then there are **a** $\times$ **b** ways of performing both tasks.

Example 3 shirts: Blue, **Yellow**, Green
2 pants: **Khaki**, Navy

$2 \times 3 = 6$ outfits

General Multiplication Principle

Suppose n choices must be made
with m_1 ways to make choice 1,
and for each of these ways,
m_2 ways to make choice 2,
and so on, with
m_n ways to make choice n.
Then there are
$m_1 \times m_2 \times ... \times m_n$
different ways to make the entire sequence of choices.

The Possible Number of Enigma Configurations

5 Variable Components of Enigma

- 3 Ordered (left to right) Rotors: wired 26 input contact points to 26 output contact points on alternate faces of a disc
- 26 serrations: around periphery of the rotors, to specify initial positions of the rotors.
- Moveable ring on each rotor: controlled rotational behavior of the rotor immediately to the left by means of a notch.
- Reflector: fold inputs and outputs back onto the same face of contact points.
- Plugboard: 0 to 13 dual-wired cables

Ordered Rotors I

Wire 26 input contact points to 26 output contact points

Choices for wire from A: 26
Choices for wire from B: 25
Choices for wire from C: 24
. . . Choices for write from Y: 2
Choices for wire from Z: 1

Number of possible different discs:
$26 \times 25 \times 24 \times \ldots 3 \times 2 \times 1$
$26!$
403,291,461,126,605,635,584,000,000
$4.032914611 \times 10^{26}$

Ordered Rotors II

Of these 26!, pick any one to occupy leftmost position.
Then 26! - 1 are available for middle position
and 26! -2 for the rightmost slot.
The total number of ways of ordering all possible disc
combinations in a 3 rotor Enigma:

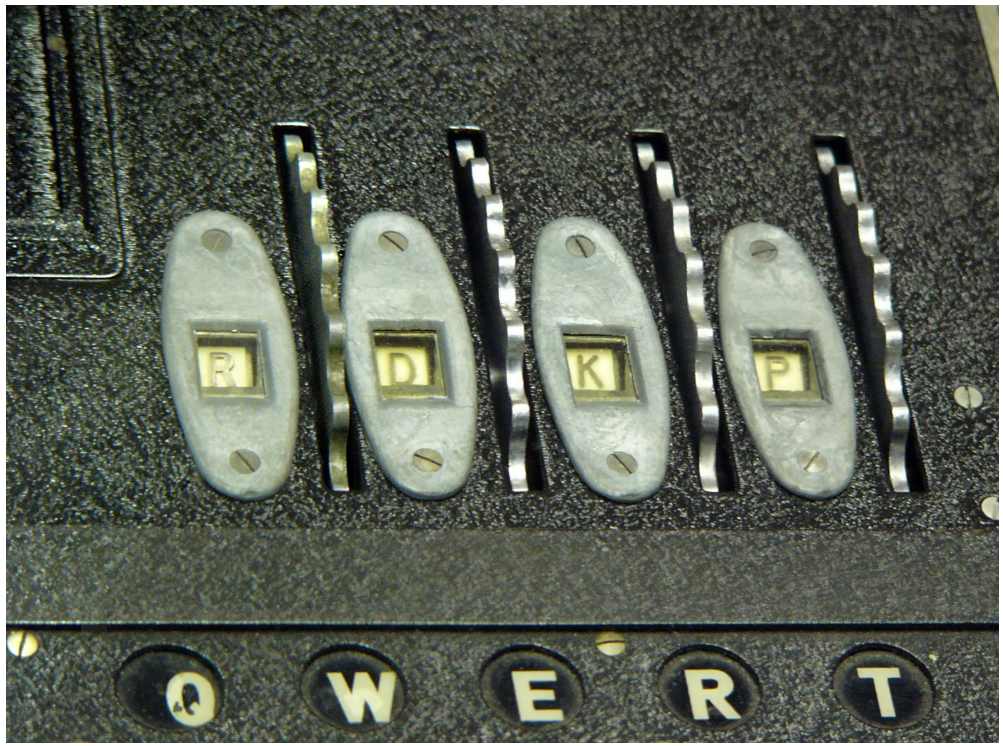
$$26! \times (26! - 1) \times (26! - 2)$$

65,592,937,459,144,468,297,405,473,480,371,753,615,896,841,298,988,71

$$6.559293746 \times 10^{79}$$

Serrations

Initial Rotation Position of the 3 Rotors

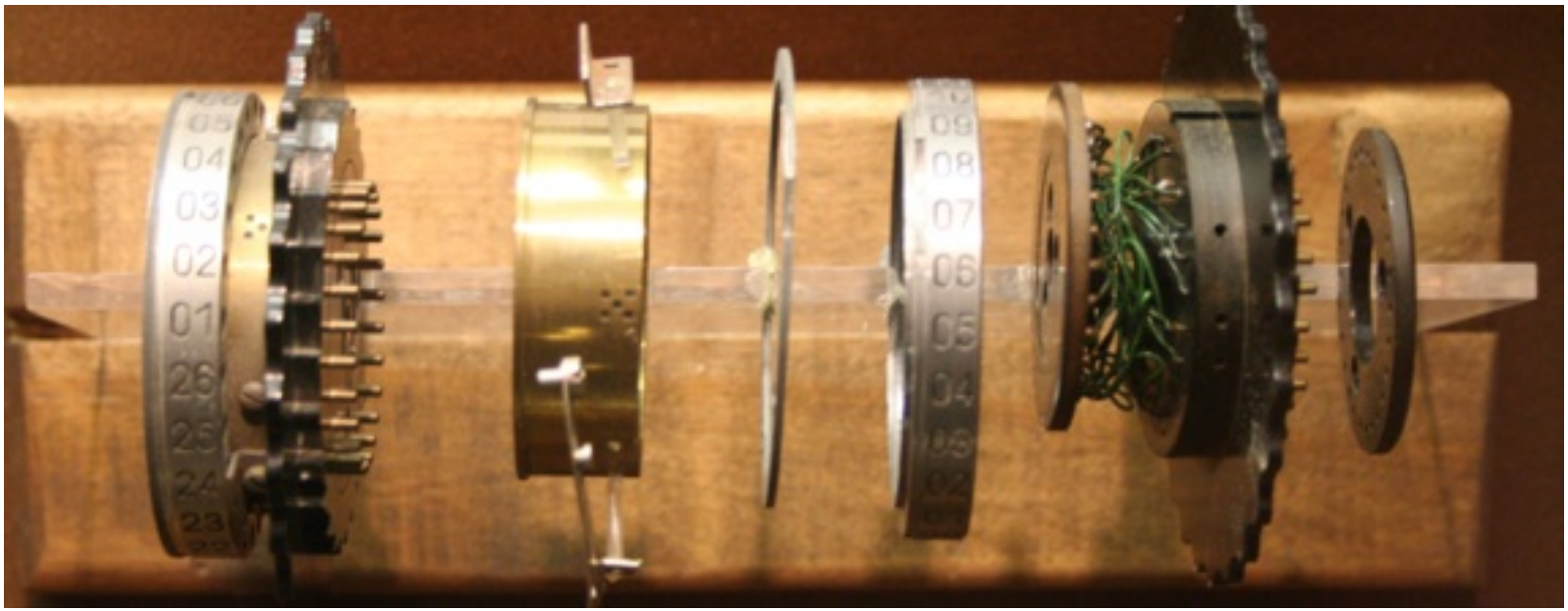


Each rotor can be set into one of 26 different positions.

Number of combinations: $26 \times 26 \times 26 = 26^3 = 17,576$

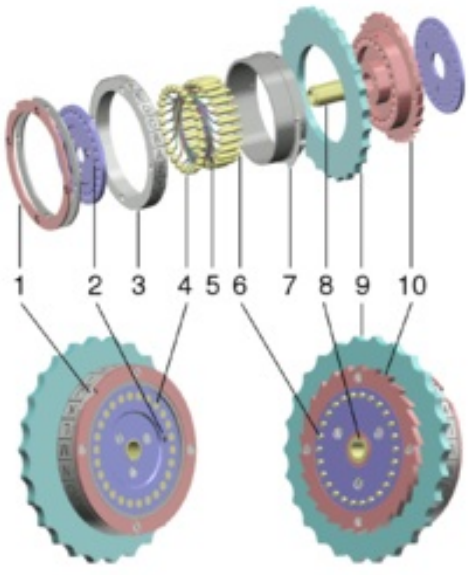
For 4 Rotors: $26^4 = 456,976$

Closer Look at Rotors



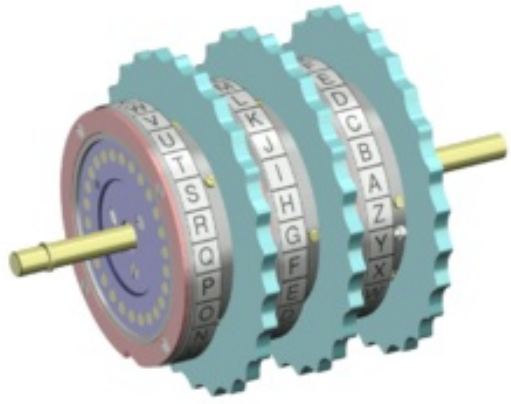
Closer Look at Rotors

Exploded view of an Enigma rotor



1. notched ring
2. marking dot for "A" contact
3. alphabet tyre
4. plate contacts
5. wire connections
6. pin contacts
7. spring-loaded ring adjusting lever
8. hub
9. finger wheel
10. ratchet wheel

Three rotors in sequence



Closer Look at Rotors

The right side of a rotor, showing the pin electrical contacts. The Roman numeral V identifies the wiring of the rotor.

The left side of an Enigma rotor, showing the flat (plate) electrical contacts. A single turnover notch is visible on the left edge of the rotor.

Notches

Initial Rotation Position of the 3 Rotors

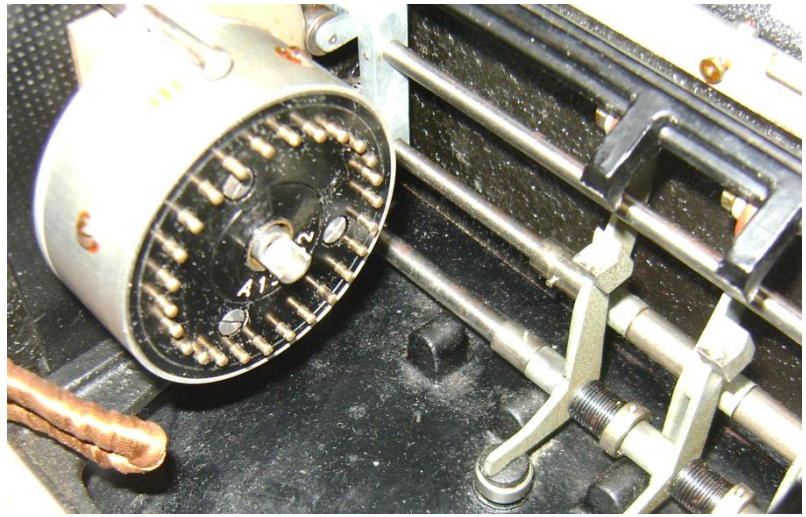
Moveable ring on each rotor: controlled rotational behavior of the rotor immediately to the left by means of a notch.

Rightmost rotor rotated every time a key was pressed.

The rightmost rotor's notch forced a rotation of the middle rotor once every 26 keystrokes.

The middle rotor's notch force a rotation of the leftmost error every $26 \times 26 = 676$ keystrokes.

Reflector



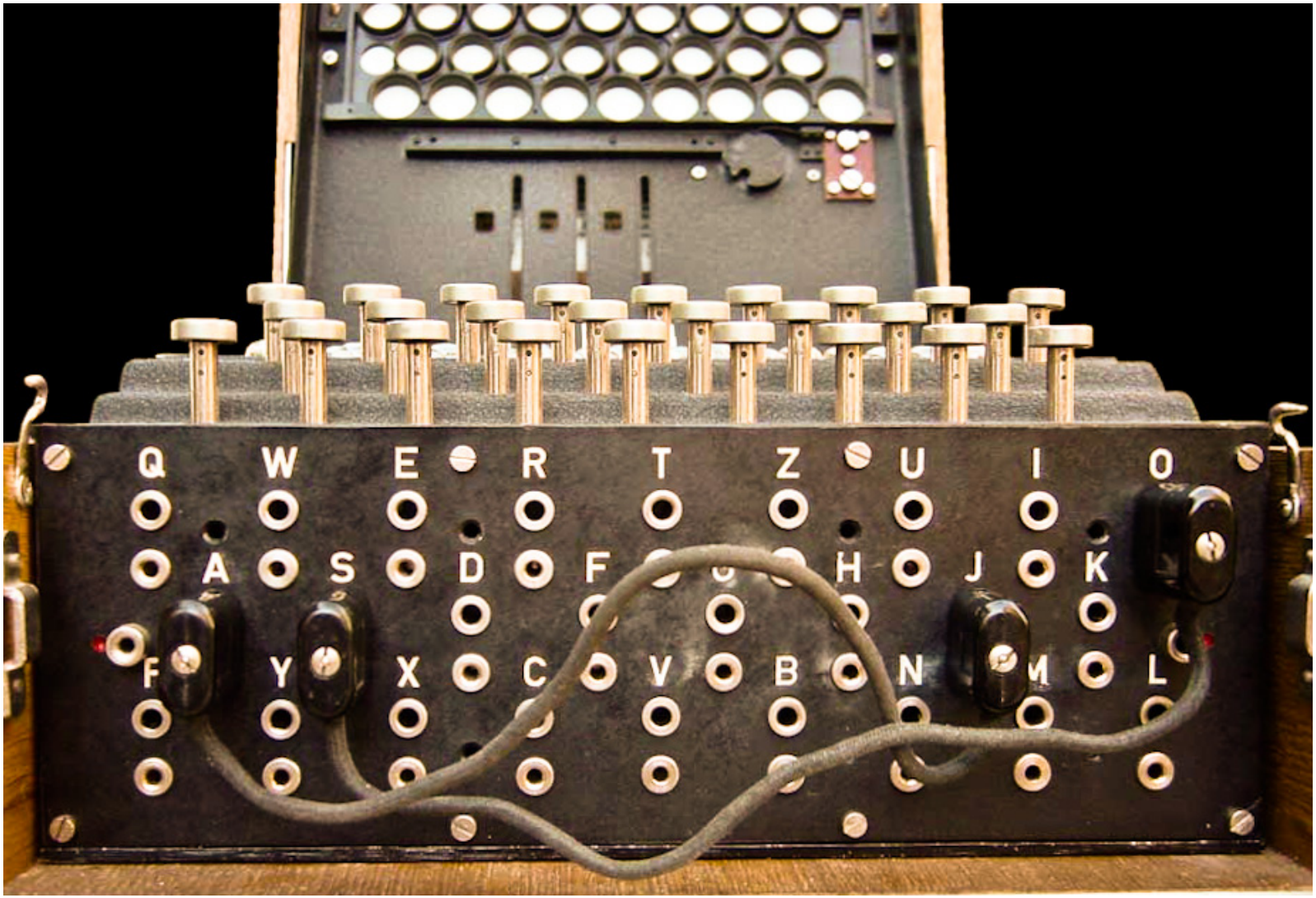
The reflector had 26 contact points like a rotor, but only on one face. 13 wires internally connected the 26 contact points together in a series of pairs so that a connection coming in to the reflector from the rotors was sent back through the rotors a second time by a different route.

The number of distinct reflectors is

$$25 \times 23 \times 21 \times ... \times 5 \times 3 \times 1 = \frac{26!}{2^{13}13!}$$

$$= 7,905,853,580,625 = 7.905853581 \times 10^{12}$$

Plugboard = Steckerbrett



$$\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}$$

$$= \frac{26!}{2!24!} \times \frac{24!}{2!22!} \times \frac{22!}{2!20!} \times \frac{20!}{2!18!}$$

$$= \frac{26!}{2^4 18!} = \frac{26!}{2^4(26-2\times 4)!}$$

$$\frac{26!}{2^4 18!} = \frac{26!}{2^4(26-2\times 4)!4!} = 164,038,875$$

With k cables:

$$\frac{26!}{2^k(26-2k)!k!}$$

$$\sum_{k=0}^{13} \frac{26!}{2^k(26-2k)!k!} = 532,985,208,200,576 = 5.329852082\times 10^{14}$$

Cables	Possibilities	Scientific Notation
0	1	1
1	325	3.25×10^{2}
2	44850	4.4850×10^{4}
3	3453450	3.453450×10^{6}
4	164038875	1.64038875×10^{8}
5	5019589575	$5.019589575 \times 10^{9}$
6	100391791500	$1.003917915 \times 10^{11}$
7	1305093289500	$1.305093290 \times 10^{12}$
8	10767019638375	$1.076701964 \times 10^{13}$
9	53835098191875	$5.383509819 \times 10^{13}$
10	150738274937250	$1.507382749 \times 10^{14}$
11	205552193096250	$2.055521931 \times 10^{14}$
12	102776096548125	$1.027760965 \times 10^{14}$
13	7905853580625	$7.905853581 \times 10^{12}$

5 Variable Components of Enigma

- 3 Rotors: $6.559293746 \times 10^{79}$
- Serrations: 26^3
- Notches: 26^2
- Reflector: $7.905853581 \times 10^{12}$
- Plugboard: $5.329852082 \times 10^{14}$

Number of Theoretically Possible Configurations:
3283883513796974198700882069882752878379955261095623685444
0553152260064336156274096669331823711548027699200000000000

$$= 3.283883514 \times 10^{114}$$