The ENIGMA Code and its Cryptanalysis

Steve Tindale G8XEV
IVARC 25 Oct 2019

CONTENTS

- Preamble:
  - Enigma timeline
  - Codes, Early Cyphers and their vulnerabilities
- What ENIGMA is and how it works
  - Machine mechanics
  - Some very large numbers
  - The Cryptographic system
- ENIGMA Vulnerabilities & Cryptanalysis
  - Cypher
  - System weaknesses
  - The Crib Attack
- Bletchley workflow
- Great Achievements

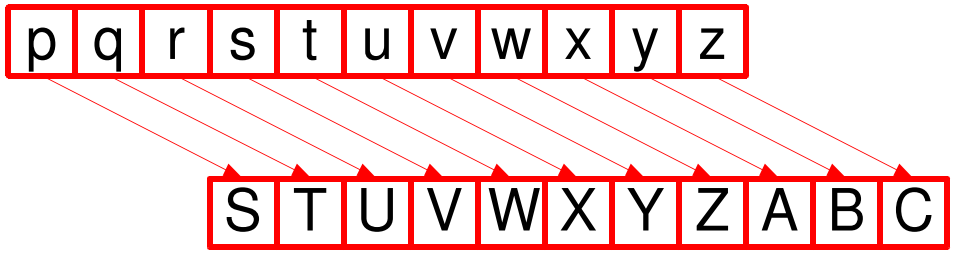
ENIGMA Timeline

- 1918 First Patent
- 1923-4 Machine development & commercial use
- Intervening years: Continuous improvement and widening of use
- 1932 Adoption of TYPE 1 by the Wehrmacht
- 1934 – 41 adoption by all parts of the German armed forces and security apparatus
- 1941 - 45 Ongoing development and introduction of the four rotor navy Kriegsmarine machines

CODE vs CYPHER

- A CODE is a substitution for a word or phrase e.g. Q Code: “My location is” = “QTH”
- A CYPHER is a character by character substitution of plaintext so Morse “code” is in fact a cypher
- A code requires a CODEBOOK
- In general a cypher requires both an an ALGORITHM and a KEY

Ceasar Cypher



- A single alphabet substitution cypher
- ALGORITHM: Add (modu26) a fixed offset
- KEY: The number (or letter) of the offset: 0-25

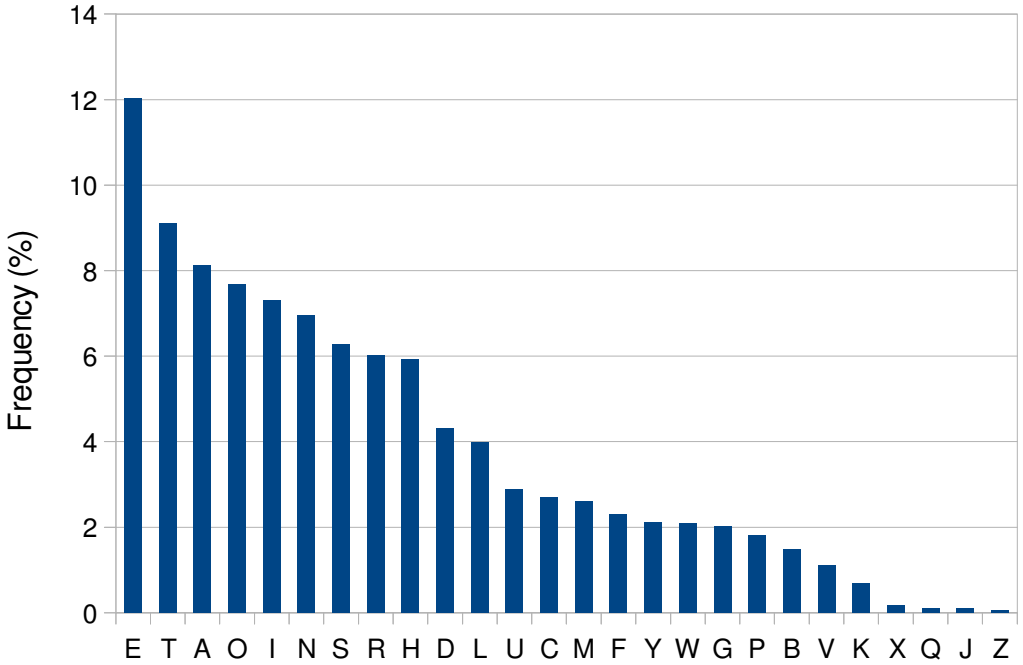
h e l l o x i v a r c		plaintext
+ + + + + + + + + + +		
D D D D D D D D D D D		Offset (=3 in this example)
= = = = = = = = = = =		
L I P P S B M Z E V G		CYPHERTEXT
L I P P S B M Z E V G		CYPHERTEXT
- - - - - - - - - - -		
D D D D D D D D D D D		Modulo 26 subtraction
= = = = = = = = = = =		
h e l l o x i v a r c		plaintext

Caesar Cypher vulnerabilities

Most common bi-grams and quad-grams in English (%)

th	1.52
he	1.28
in	0.94
er	0.94
an	0.82
re	0.68
nd	0.63
at	0.59
on	0.57
nt	0.56
ha	0.56
es	0.56
st	0.55

tion	0.31
nthe	0.27
ther	0.24
that	0.21
ofth	0.19
fthe	0.19
thes	0.18
with	0.18
inth	0.17
atio	0.17

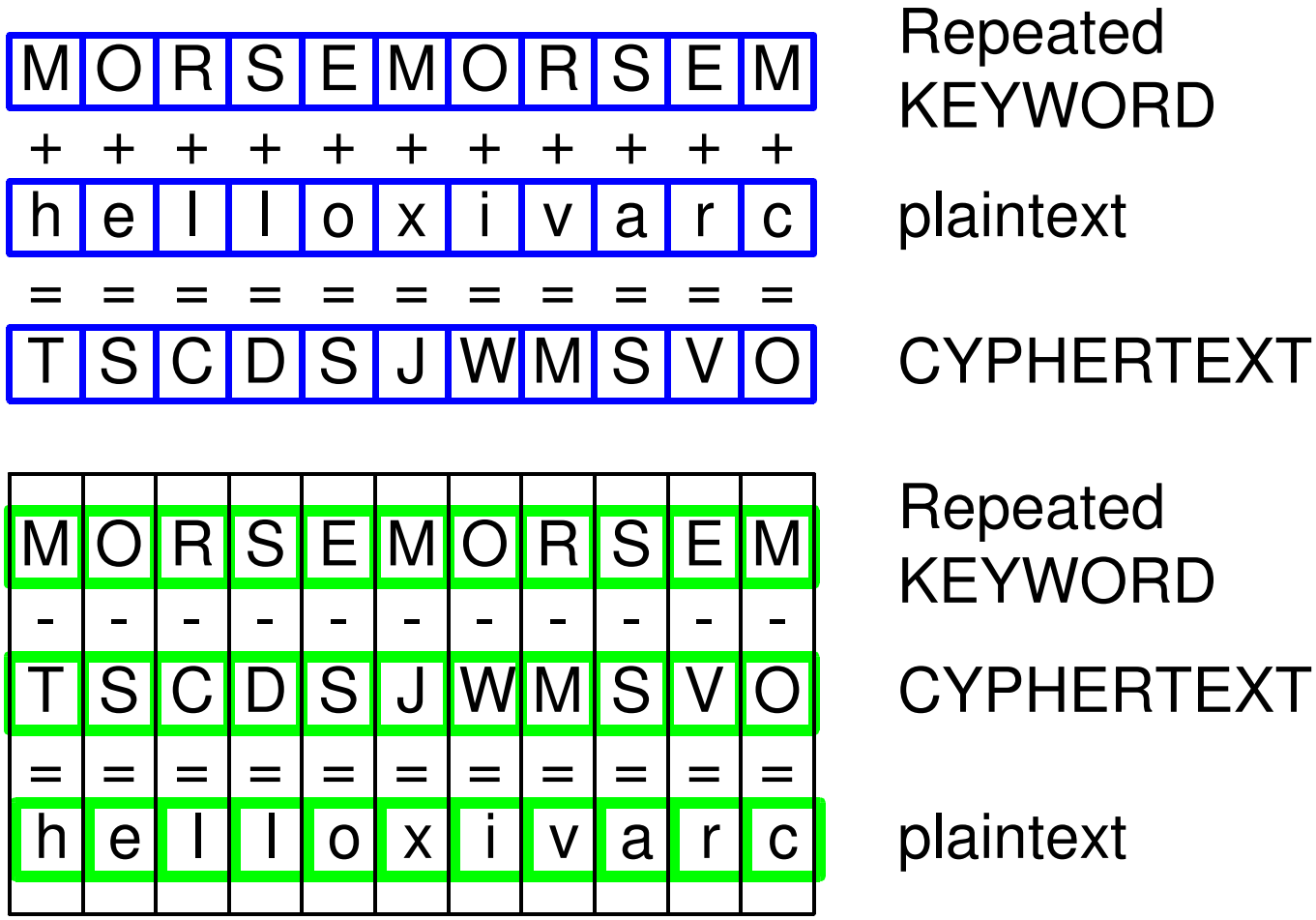


- Letter Frequency Analysis
- N-Gram recognition
- Brute Force Attack

Belasso/Vigenere Cypher

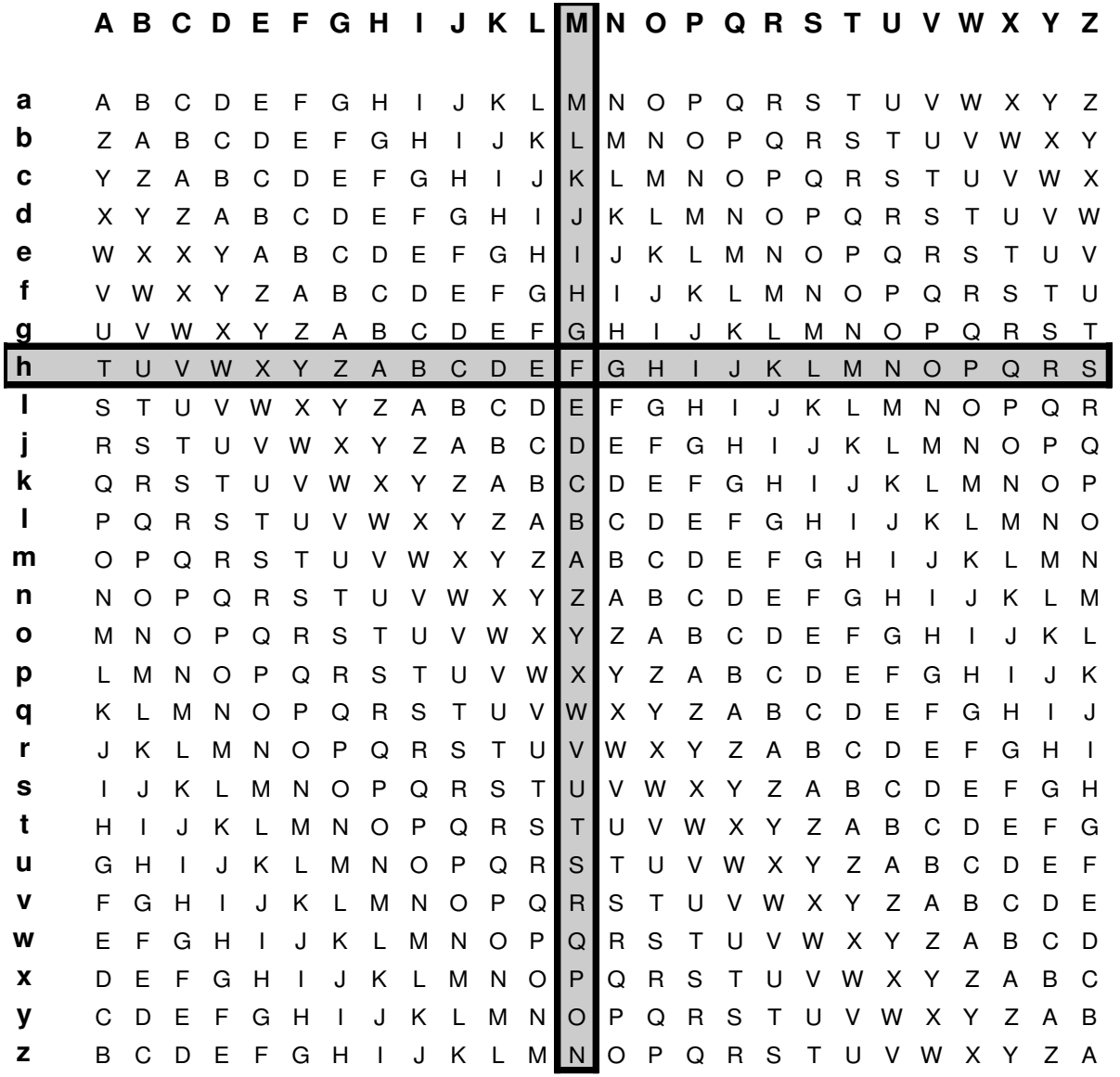
(1553 & 1586 a.d.)

- A POLYalphabet substitution cypher
- ALGORITHM: Add (modu26) a variable offset
- KEY: Variable offset defined by a repeated KEYWORD



Belasso/Vigenere Cypher (2)

- Performed using either a Tabula Recta or a codewheel
- Repeated keyword exposes vulnerability to guessing the key length
- Interleaved Ceasar Cypher structure means fundamental vulnerabilities remain
- Remained unbroken for three centuries (1863)
- Many variants including the One Time Pad



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

Is there an unbreakable Cypher??

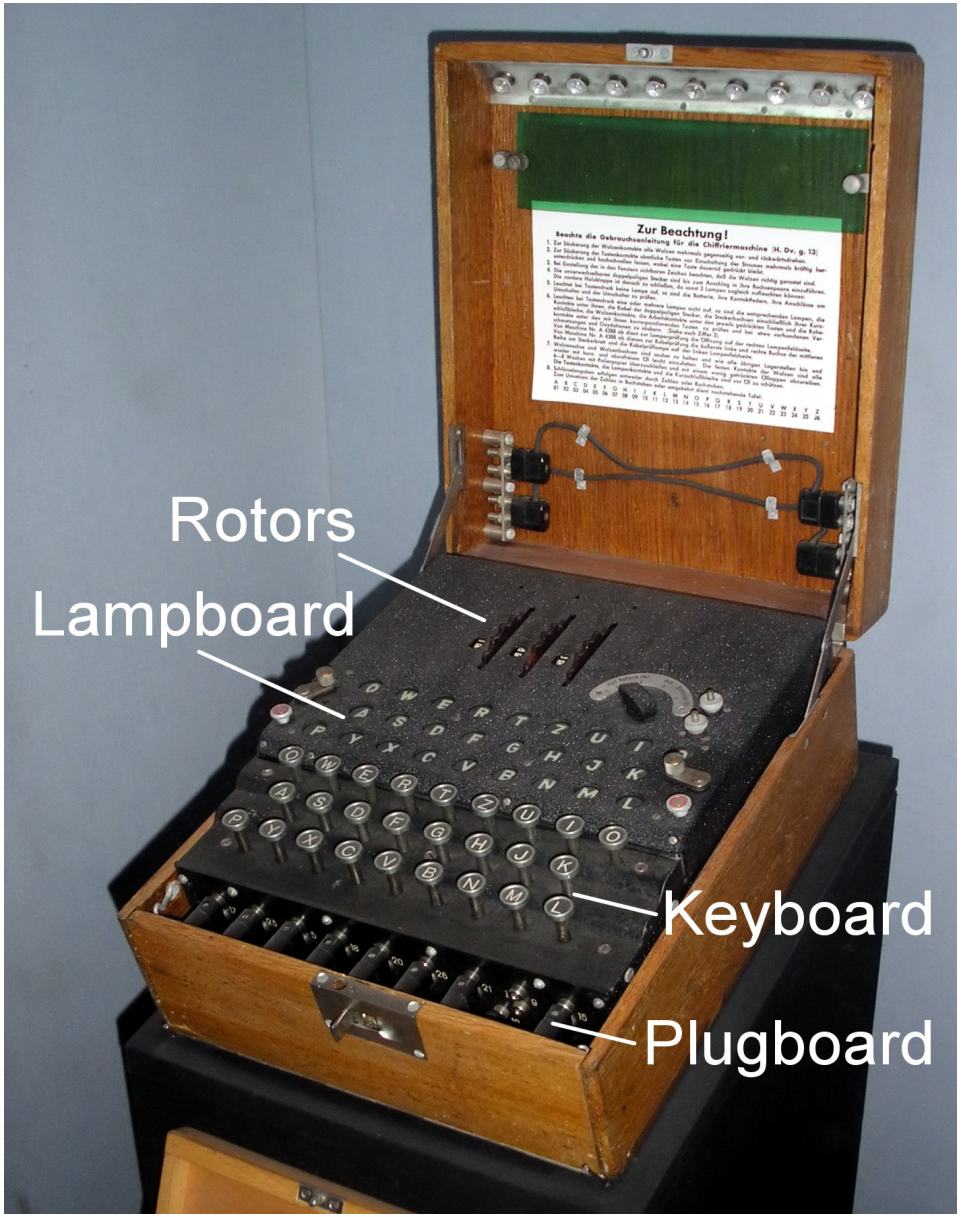
- GOOD:
  - Use Polyalphabetic substitution
  - Many possible keys
  - Each available key to be random and longer than the message
  - Use the key only once then discard
  - Flat statistics
  - A solid Cryptographic System (incl. key distribution)

So does this miracle Crypto exist?

The Germans thought so...

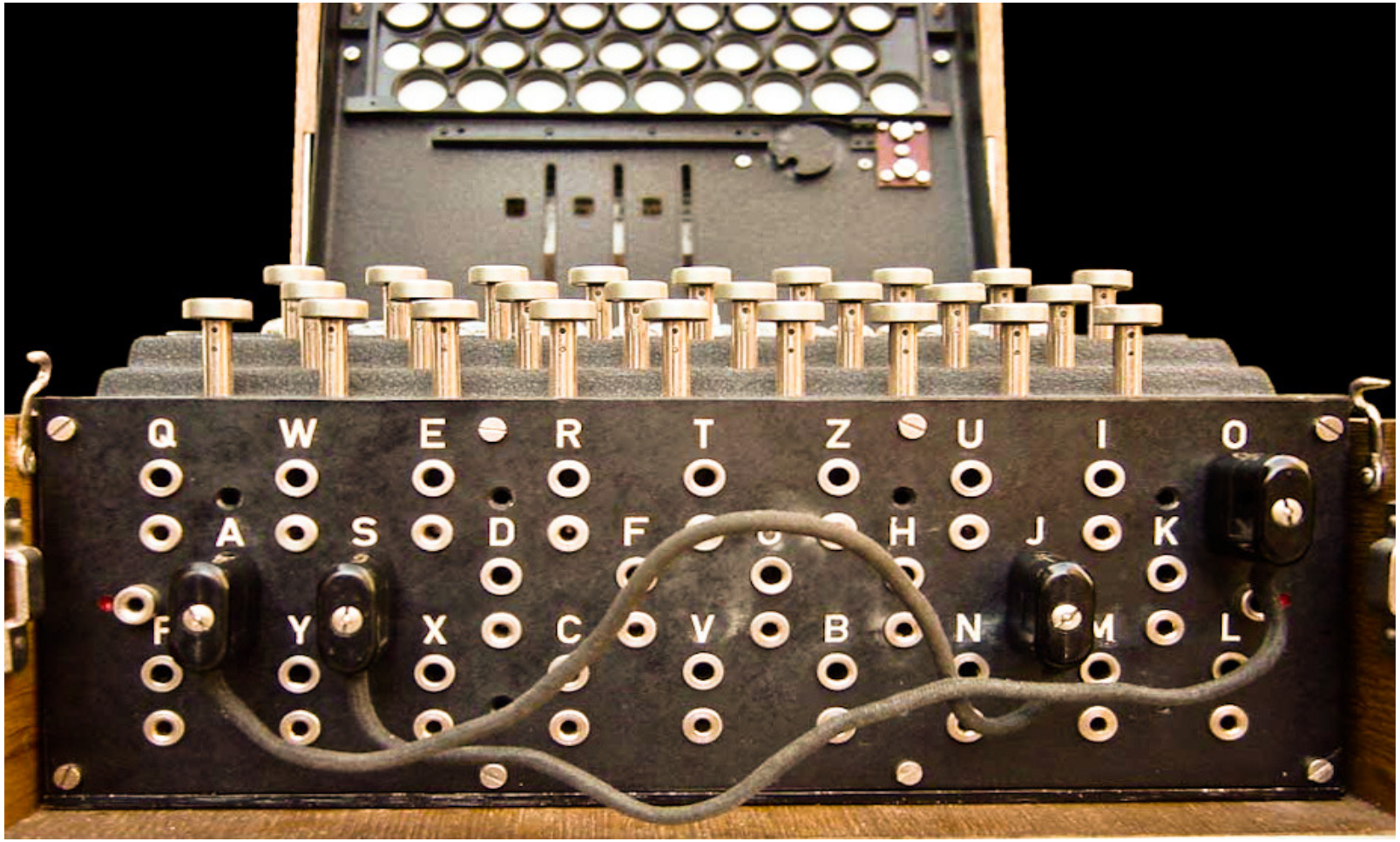
Kriegsmarine
4 Rotor Enigma

Wehrmacht & Luftwaffe
3 Rotor Enigma



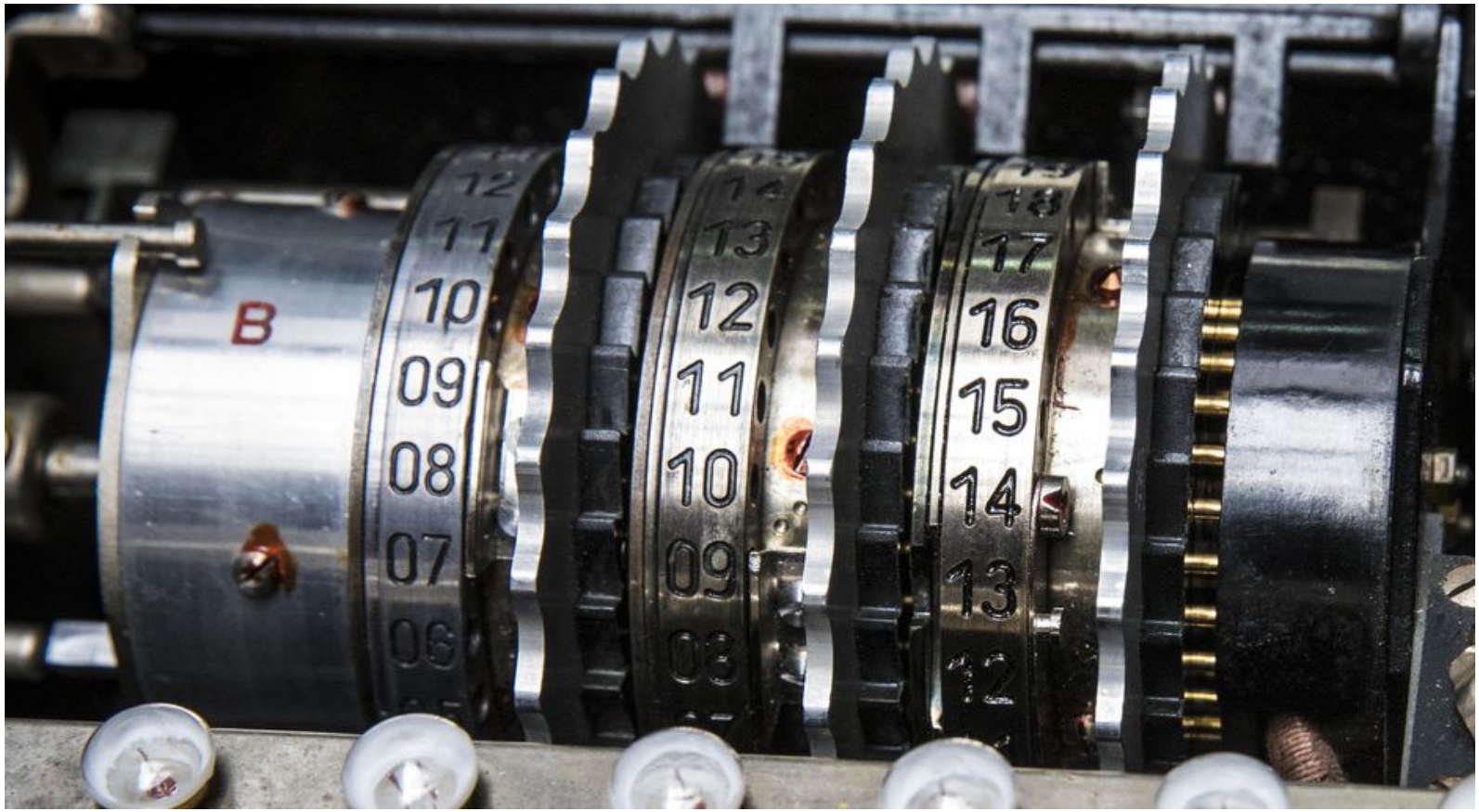

Nur Glühlampen mit 12 mm Durchmesser verwenden.
B
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
A

Steckerbrett



Steckerbrett substantially increases complexity (and therefore security) as the wiring could be changed

ENIGMA Rotor Set

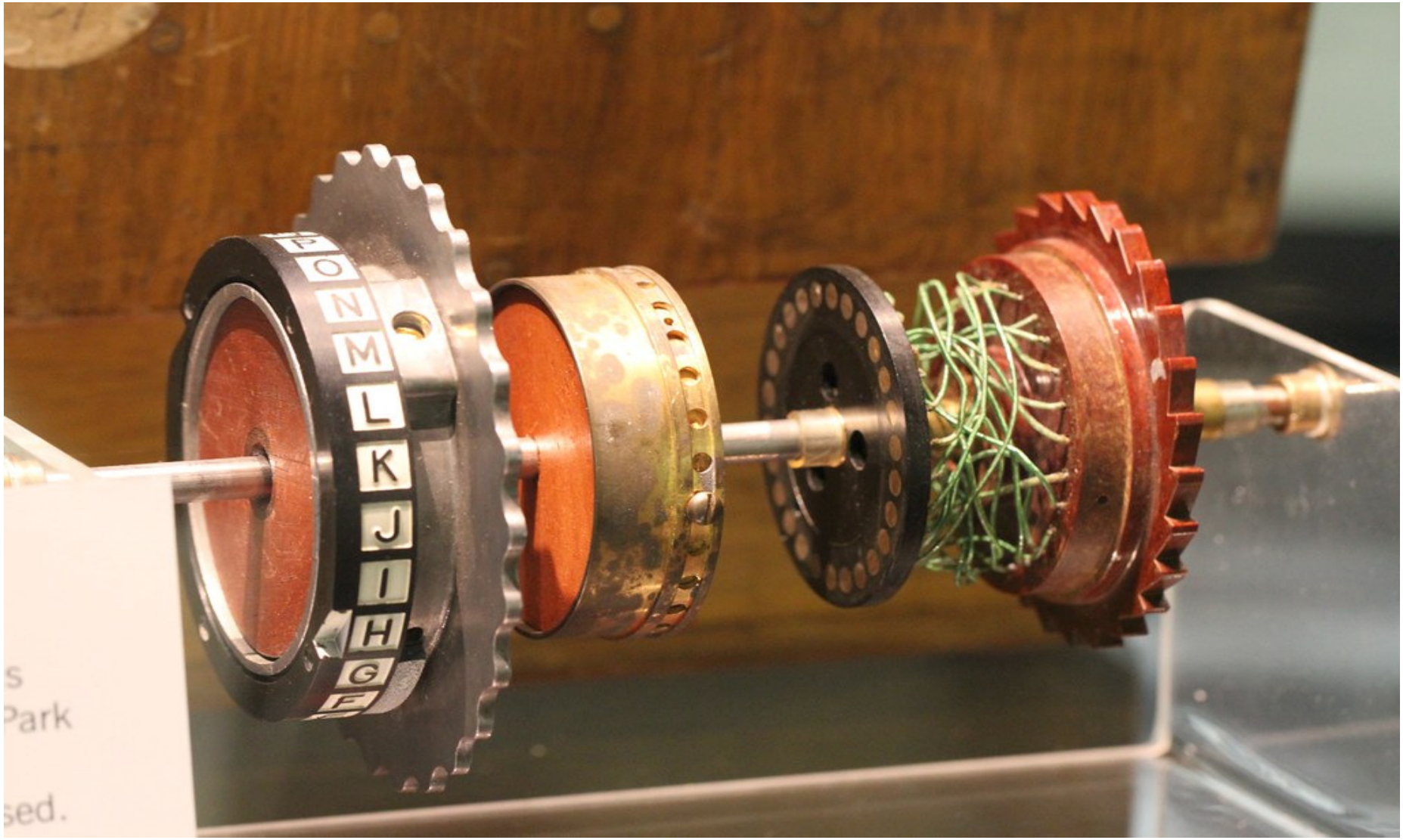


Entry ring is fixed and mapped straight through (A to A)

Rotors have internal scrambling wiring

The reflector folds back the current path for a second (backward) pass through the Rotors

Rotor Wiring Matrix

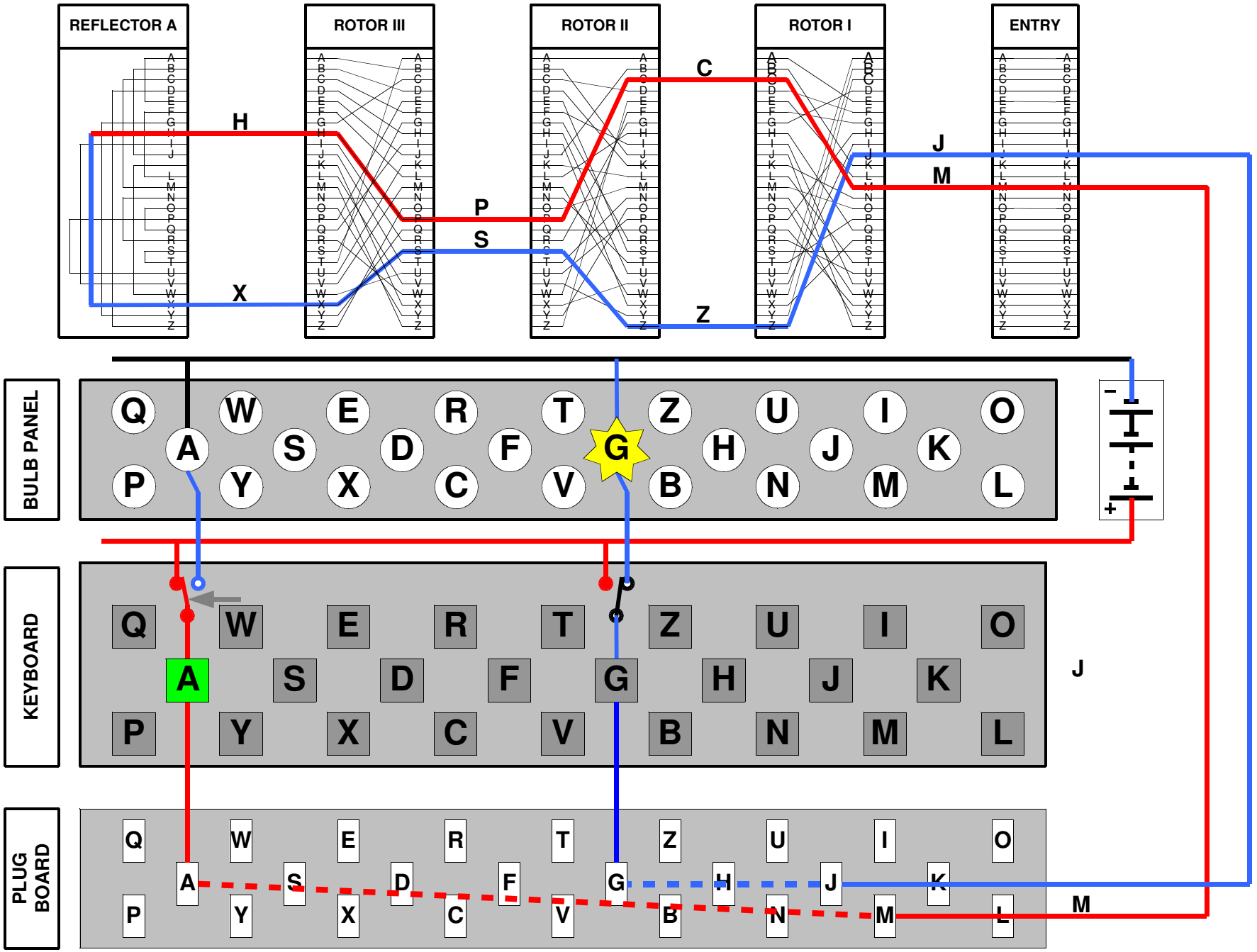


Three rotors are cascaded on an axle

Wiring Matrix can be in any one of 26 positions relative to the turnover notch (position of the turnover notch w.r.t. letter labels is fixed)

Pawl Mechanism for advancing Rotors

ENIGMA WIRING DIAGRAM



A > M > C > P > H > X > S > Z > J > G

Cryptanalytic search space

- The number of keys that the Enigma architecture is able to generate is set by:
  - Rotor wiring
  - Rotor selection and order
  - The ring setting (notch/turnover position)
  - Rotor start settings
  - Reflector wiring
  - Plugboard settings
- The German cryptographers believed the Enigma was unbreakable because this results in such a large number of permutations

Rotor Wiring and Selection

- Each rotor has 26 contacts wired to 26 pins so, assuming three rotors and no duplicates, there are:

(26!-1)x(26!-2)x(26!-3) possible options:

65,592,937,459,144,468,297,405,473,480,371,753,615,896,841,298,988,710,328,553,805,190,043,271,168,000,000

= 6.56x10^79

Rotor Settings

- The ring settings (notch position) can be one of 26 for each rotor HOWEVER the third (slow) rotor cannot rotate the reflector so only the fast and middle rotors contribute:

$$26x26 = 676$$

- Each rotor can be placed in any one of 26 start positions:

$$26x26x26 = 17,756$$

Reflector Wiring

- The first end of the first wire can be placed in one of 26 positions and the second end in any one of the remaining 25 positions HOWEVER a>j is the same as j>a so there are only half as many INDEPENDENT options as first appear: 26x25/2
- For the first swap there are 13 wires to choose from and using say wire #5 to connect a>j has exactly the same effect as using any of the other wires resulting in a further reduction in the number of INDEPENDENT OPTIONS by a factor of 13. So for the first wire there are 26x25/2/13 options
- The first end of the second wire can be placed in one of 24 positions and the second end in any one of 23 positions. The same duplications occur so there are 24x23/2/12 INDEPENDENT options for the second wire... and so on
- The total number of options is then:

26x25/2/13 x 24x23/2/12.....2x1/2/1 = 26!/(2^13x13!) =7.91x10^12

Plugboard

- The Plugboard calculation is the same as the reflector calculation EXCEPT that letters can be mapped to themselves (no wire). This increases the number of options which becomes dependent on the number of wires used:

0:	1	7:	1,305,093,289,500
1:	325	8:	10,767,019,638,375
2:	44,850	9:	53,835,098,191,875
3:	3,453,450	10:	150,738,274,937,250
4:	164,038,875	11:	205,552,193,096,250
5:	5,019,391,791,500	12:	102,776,096,548,125
6:	100,391,791,500	13:	7,905,853,580,625

- Notice the maximum at 11 wires
- As we do not know how many wires are used on a particular day the total number of options is the sum of all these:

=5.33x10^14

In Total...

- Rotor wiring and selection: 6.56x10^79
- Ring setting (turnover notch position): 676
- Rotor start position: 17,576
- Reflector wiring: 7.91x10^12
- Plugboard: 5.33x10^14

=3.28x10^114 available keys

(The naval machine offers 2.33x10^145)

The Cryptographic system or... How to use the machine...

- ...it is necessary for both the sender and the receiver to agree:
  - Which rotors to use and in what order
  - The turnover notch position for each rotor
  - The Rotor start position in the machine
  - Which Reflector to use
  - The Plugboard settings

These were distributed as quarterly then weekly then daily keys and subject to a randomisation protocol

Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

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 IM 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

Early Enigma Encryption Protocol

- Set machine according to the day key
  - rotor selection, rotor order, ring settings, start position, stecker settings
- Choose a RANDOM three letter message key
- Encrypt the key twice – why???:
  - plaintext: dqtdqt
  - cyphertext: VMOWEK
- Reset the wheel positions using the trigram
- Encrypt the message using the new settings

Early Enigma Decryption Protocol

- Decrypt the dual-trigram using the day key
  - cyphertext: VMOWEK
  - recovered plaintext: dqtdqt
- Check that the first trigram equals the second >> machine settings correct and trigram properly received.
- Use the trigram to re-set the rotor start positions
- Decrypt the message

Later Enigma Protocol

- Setup the machine according to the day key
  - rotor selection, rotor order, ring settings, stecker settings
- Choose one tri-gram from the four available then add two random letters ahead to make a five character group
- Send the five character group IN THE CLEAR as a header to the main message
- Set the rotor start positions to the selected trigram and encrypt the main message
- Receive the header, extract the trigram, set the wheel positions using the trigram then decrypt the message

Enigma Emulator

So...how to solve the impossible?

“The objective is not to solve the cypher per se but to reduce the number of options to such a manageable number that manual methods can succeed”

By the time of the outbreak of hostilities...

- In the 1930s there was no Plugboard and keys were changed six monthly or quarterly
  - A German spy had supplied the French with a training manual and sample day keys which helped reveal the operation of the machine and its protocols
  - By a phenomenal feat of mathematical cryptanalysis the Poles had determined the entry wheel, rotor and reflector wiring the Poles exploited the repeated trigram protocol
  - By the outbreak of war the machine mechanics and wiring were known
- The same five rotors were distributed with every machine
- Three reflectors were available but in practice only one was used: Reflector B
- Ten cables were always used for the Plugboard
- The repeated tri-gram method was being used to specify the ring start positions (used until May 1940)
- The same day key was used for the whole of a given network

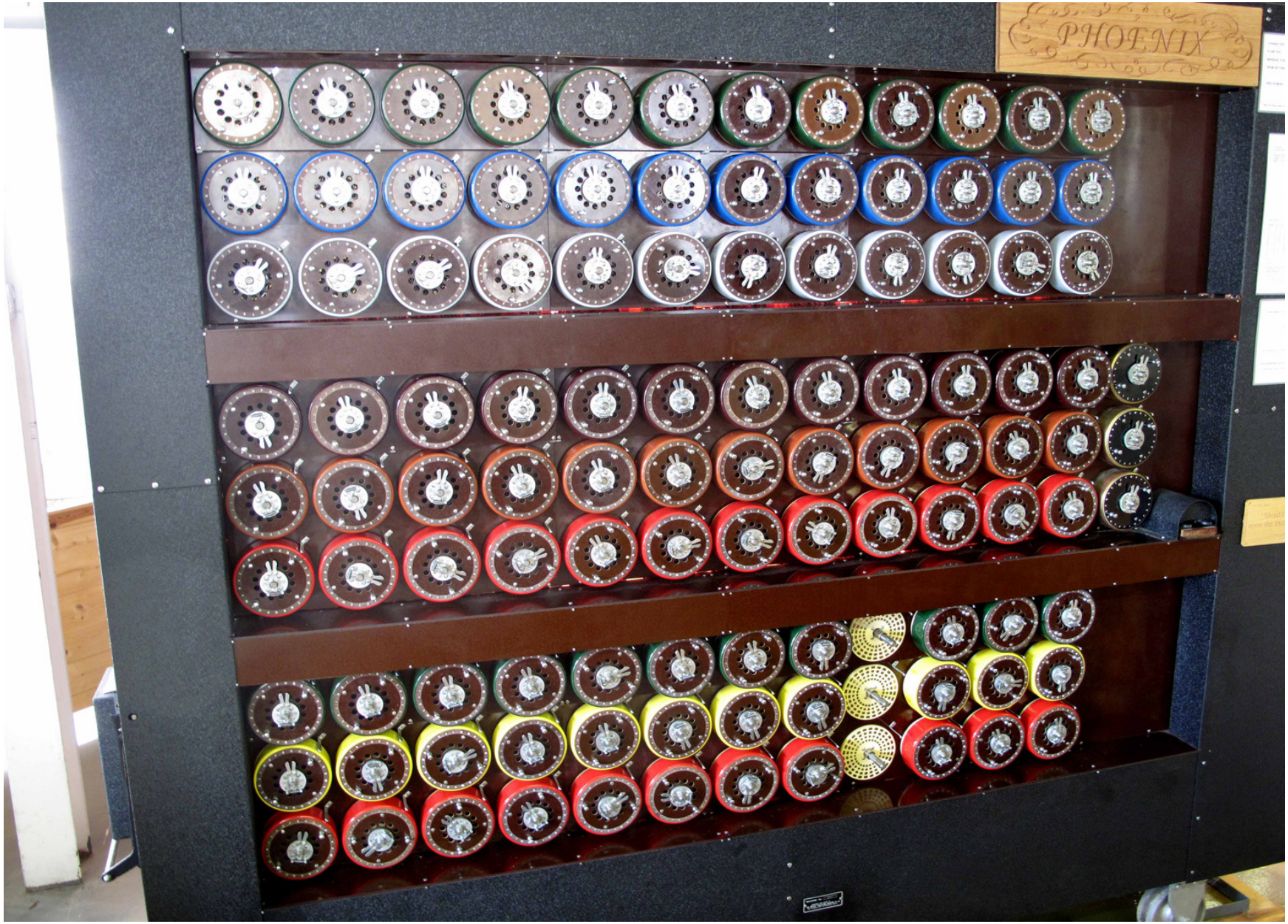
These System decisions reduced the number of possible permutations...

- Using three rotors from the a common set of five reduced the permutations from 6.56x10^79 to 5!=60
- Use of only one reflector with known wiring reduced the permutations from 7.91x10^12 to 1
- Fixing the number of plugboard cables at 10 reduced the number of permutations from 5.33x10^14 to 1.51x10^14
- The total permutations reduced from 3.28x10^114 to a trifling 1.08x10^23

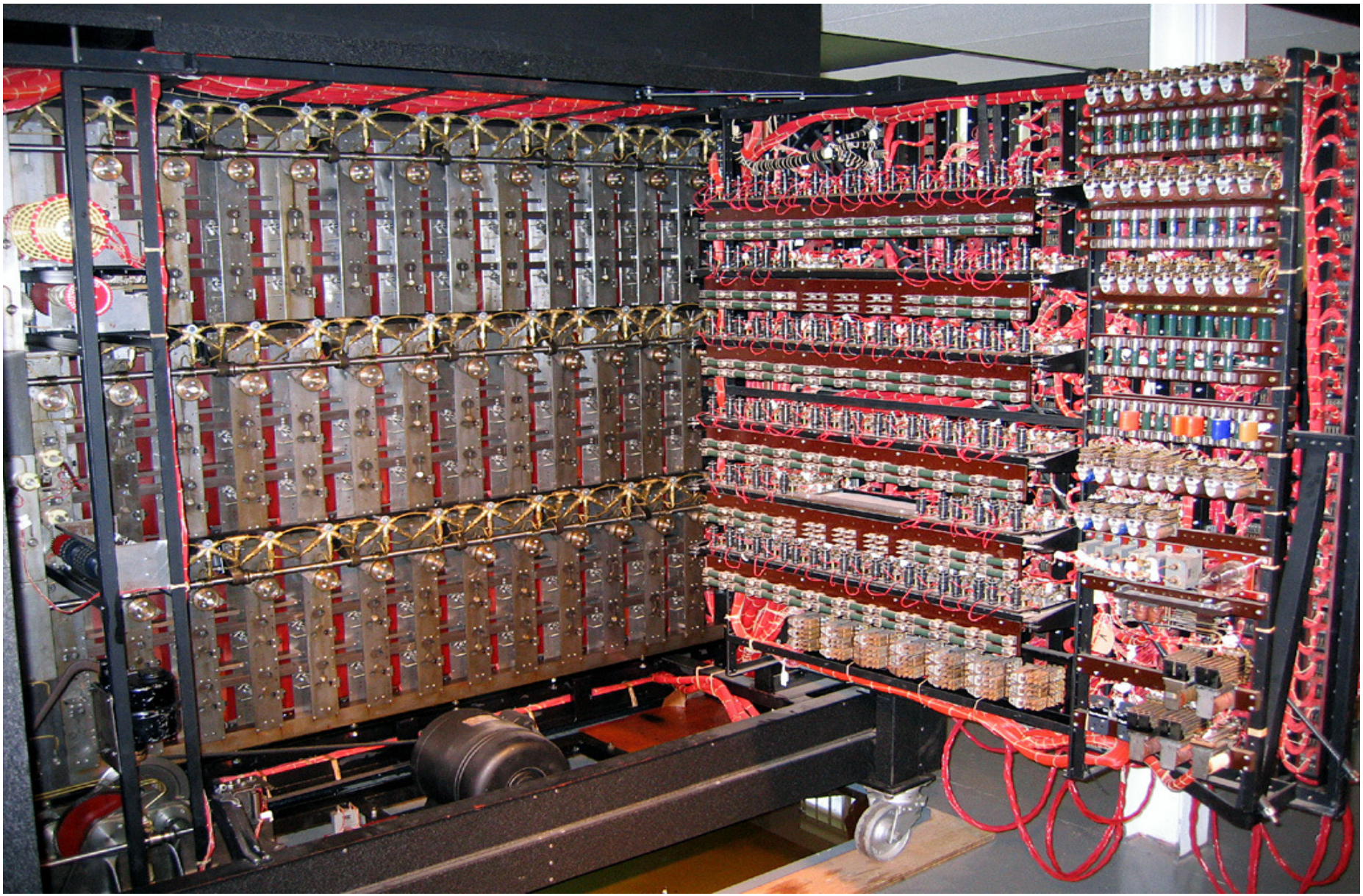
Inherent Enigma Vulnerabilities

- A letter cannot be encrypted as itself opening the door to “Crib Attack”
- The Plugboard is reciprocal which can be exploited to substantially reduce the cryptographic search space
- The turnover notches were in different places on the respective rotors which enabled the determination of wheel order
- NEVERTHELESS despite the economies of convenience, ENIGMA remained a very strong system

Bombe Front View



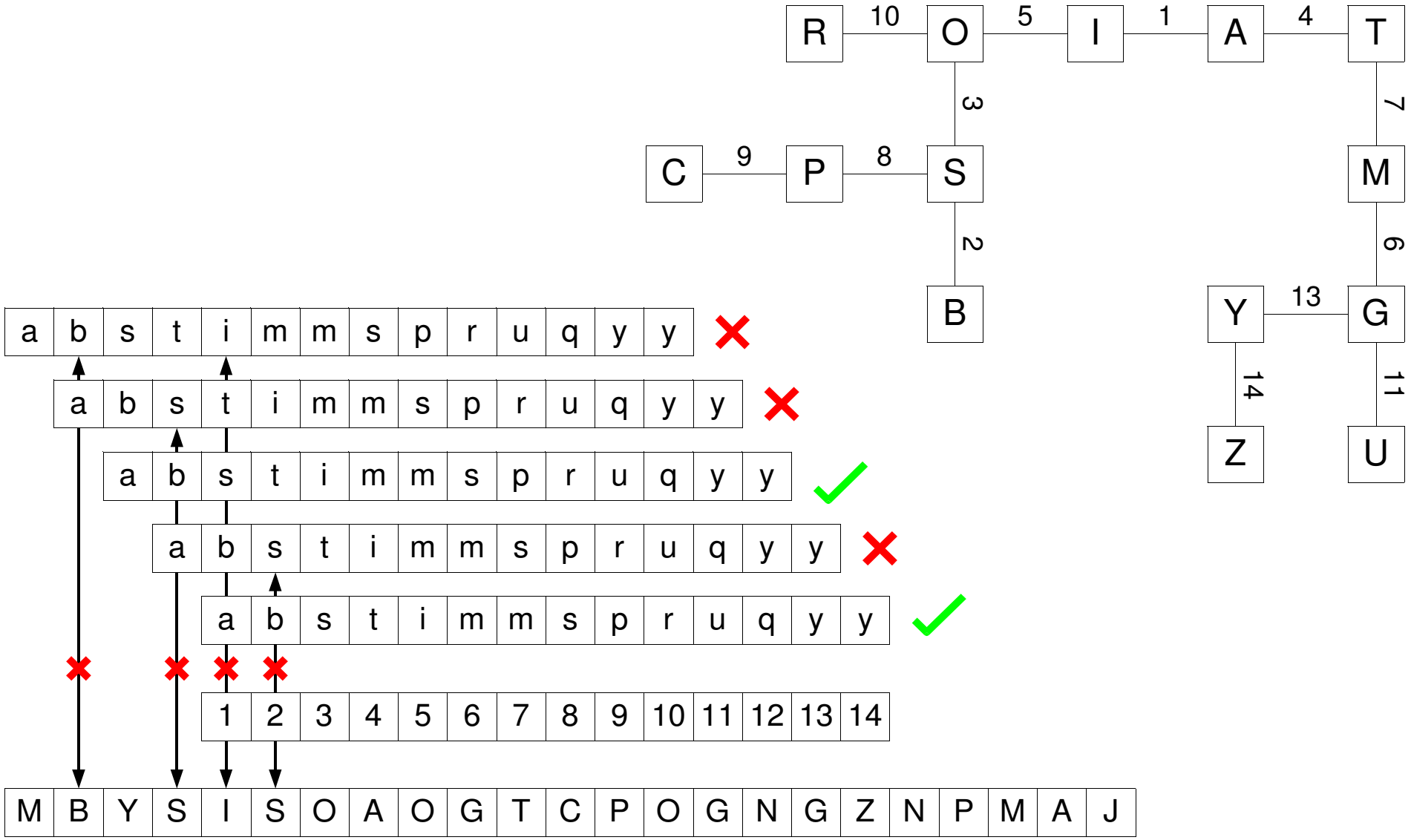
Bombe rear view



Some Key Decisions

- The Bletchley Park Team made some key decisions at the outset:
  - Not to depend on the repeated tri-gram
  - Exploit the “no letter encrypted as itself” property
  - Develop the “crib” or “known plaintext” attack
  - Cryptanalysis on an industrial scale

Crib (Known Plaintext) Attack

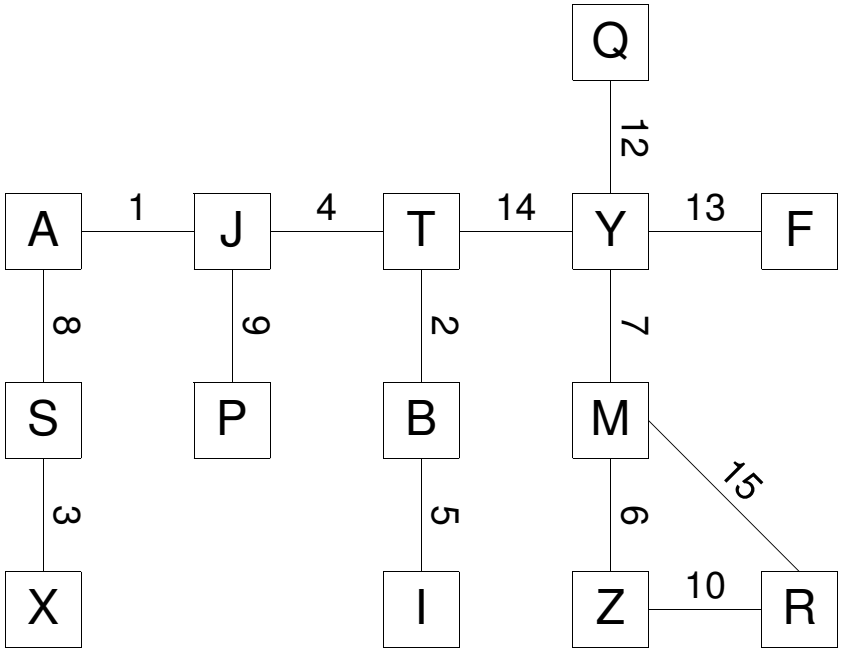


A Bombe stop is only the beginning...

- As well as the true “stop”, the Bombe would also make “false stops” - the first menu above creates 2,373 false stops
- Shorter Cribs result in a greater number of false stops
- Longer Cribs make it more likely to encounter a Rotor turnover
- The Bombe output is multiple candidate Rotor orders + One Stecker pairing

Much human post processing using checking machines (modified Type X) required to identify the correct wheel order and all stecker pairings

A better Menu?



- This menu includes a “closure”
- Closures significantly reduce the number of false stops
- This menu has 101 false stops

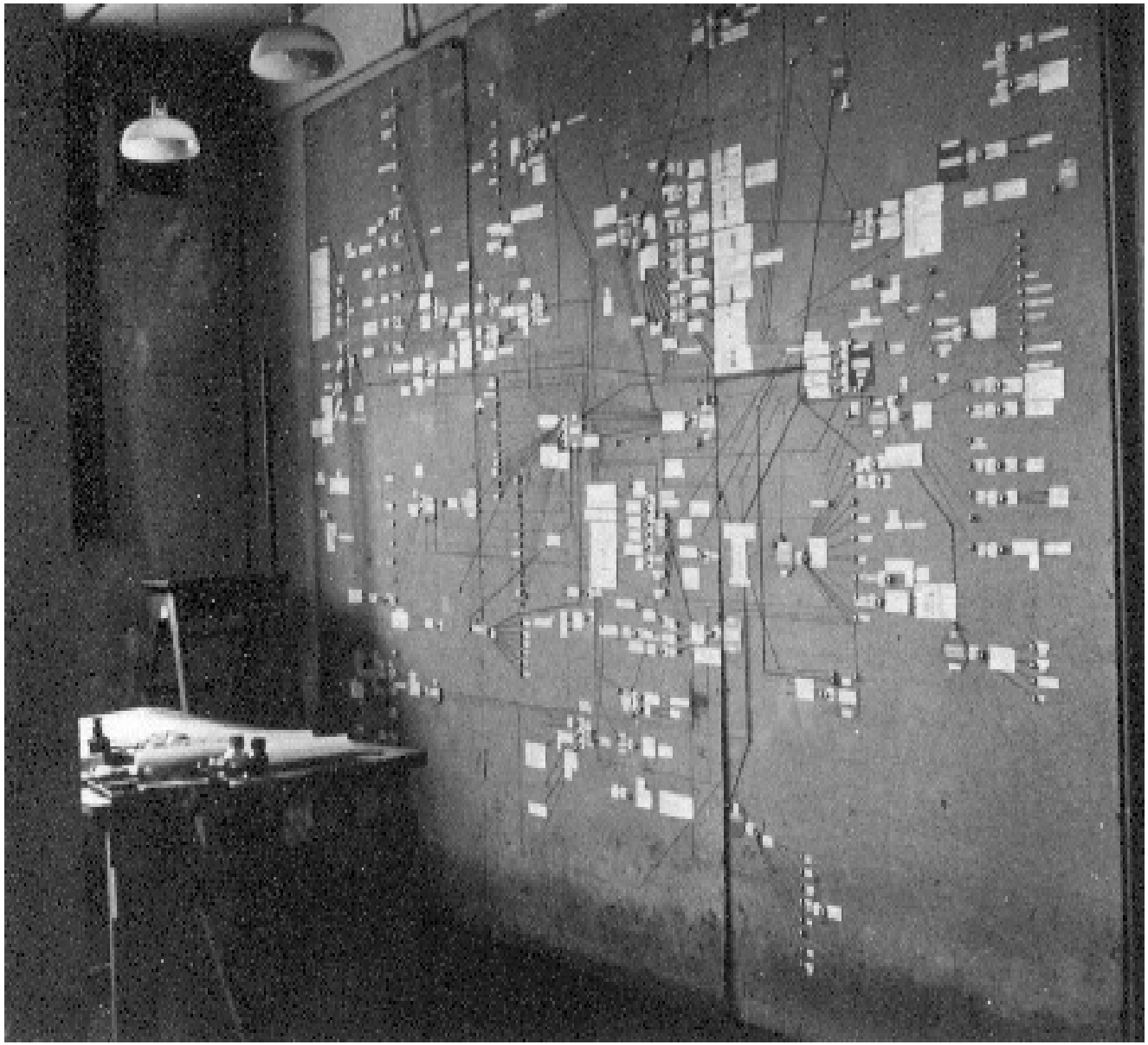
Bombe Stops per Wheel Order									
Closures	Number of Letters in the Menu								
	8	9	10	11	12	13	14	15	16
3	2.2	1.1	0.42	0.14	0.04	<0.01	<0.01	<0.01	<0.01
2	58	28	11	1.2	1.2	0.3	0.06	<0.01	<0.01
1	1,500	1,500	280	31	31	7.7	1.6	0.28	0.04
0	40,000	19,000	7,300	820	820	200	43	7.3	1

Exploiting Operating Slackness

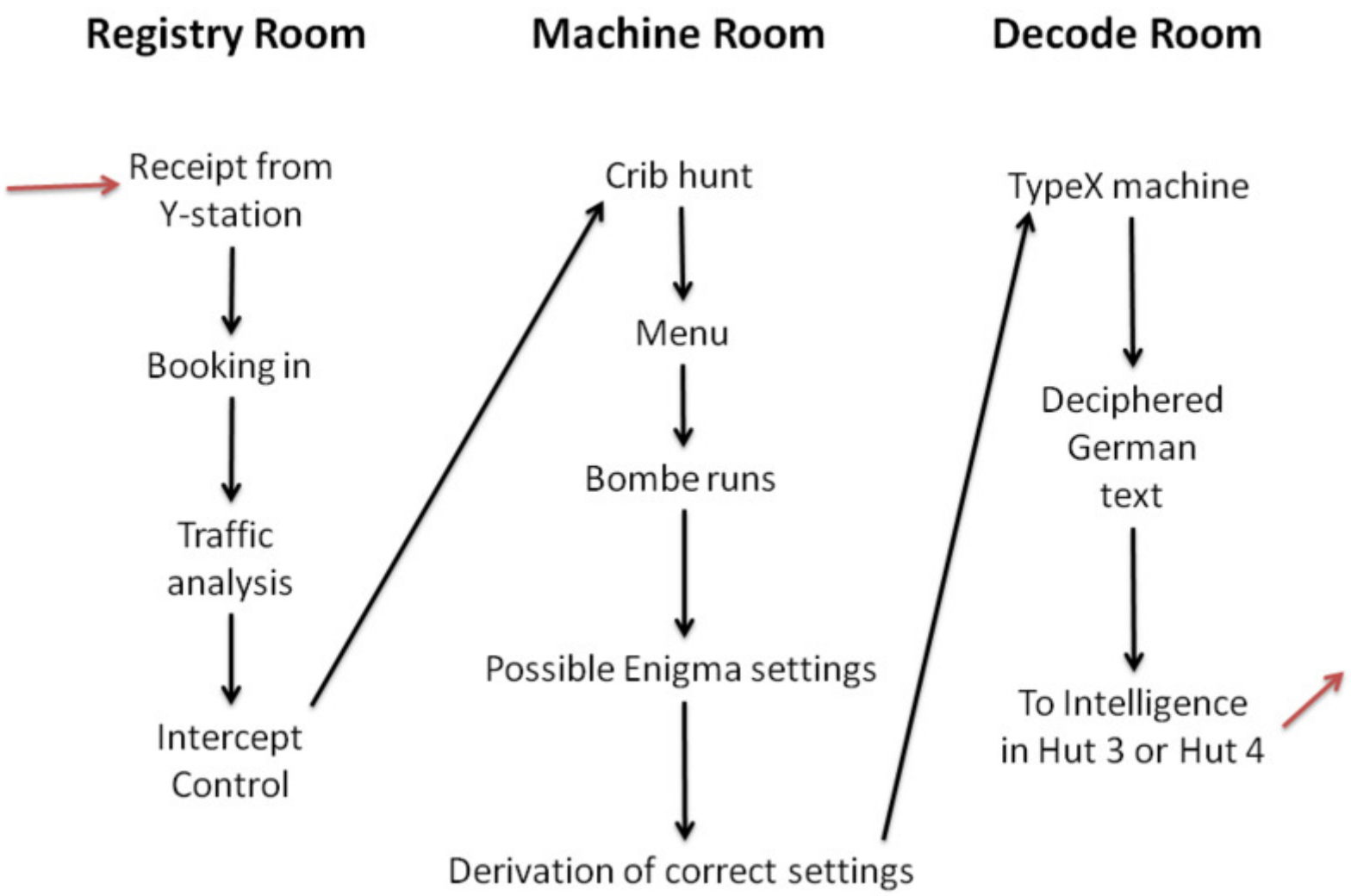
- Repeatedly using the same stereotypical expressions e.g. ANX—German for "to", followed by X as a spacer
- “Keine besonderen Ereignisse”... Nothing to report
- Repeated use of titles and courtesies
- Cillies: Using easily guessed keys such as AAA or BBB, or adjacent or diagonal keyboard keys
- Not allowing a wheel order to be repeated on a monthly setting sheet so reducing the options as the month progressed
- Some networks prohibited use of adjacent letters as stecker pairs
- The re-use of a permutation in the German Air Force METEO code as the stecker setting for the day.
- The practice of re-transmitting a message in an identical, or near-identical, form on different cipher networks
- GARDENING

SIXTA

- Mapping the German Comms networks
- DF analysis
- Keeping track of all the nets, Operators, callsigns, addressees, message history, cribs
- Data Fusion
- The origin of modern traffic analysis



Bletchley Workflow



Scale of Operations

- Massive logistical operation
- 50 nets monitored by Y and DF stations
- Over 2,000 Wrens employed in the process
- Over 200 Bombes in the UK in three locations
- Similar number in the US with dedicated transatlantic cable to commission jobs
- Many messages decrypted before breakfast

Skilful use of ULTRA so as not to reveal the decryption success

Greatest Achievements

- The Polish Cypher Bureau's pre war identification of the inner workings of the Enigma machine
- Decision to use Crib attacks
- Design of the Bombe
- Development of Traffic Analysis
- The sheer scale of the Operation
- Ultra handling protocols
- Keeping it all Secret until the 1970s

Eisenhower estimated the Bletchley Effort shortened the war by two years

The END

or maybe not...

Post script...

- Only 270 Enigma Machines survive but...
- The Russian Fialka system was in service until the fall of the Soviet Union
- Only came to light as machines came on to the market around 2000
- Overcame the vulnerabilities of the Enigma
- Shows great insight into the Bletchley exploitation

The END