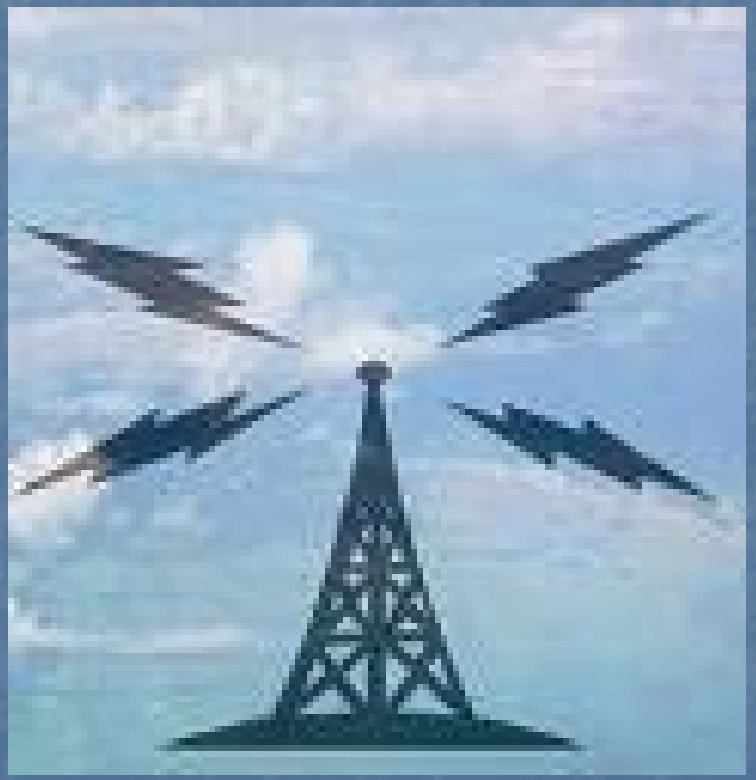
The Evolution of the Cryptologic Bombe

Chris Christensen
Department of Mathematics
Northern Kentucky University

Electronic Communications

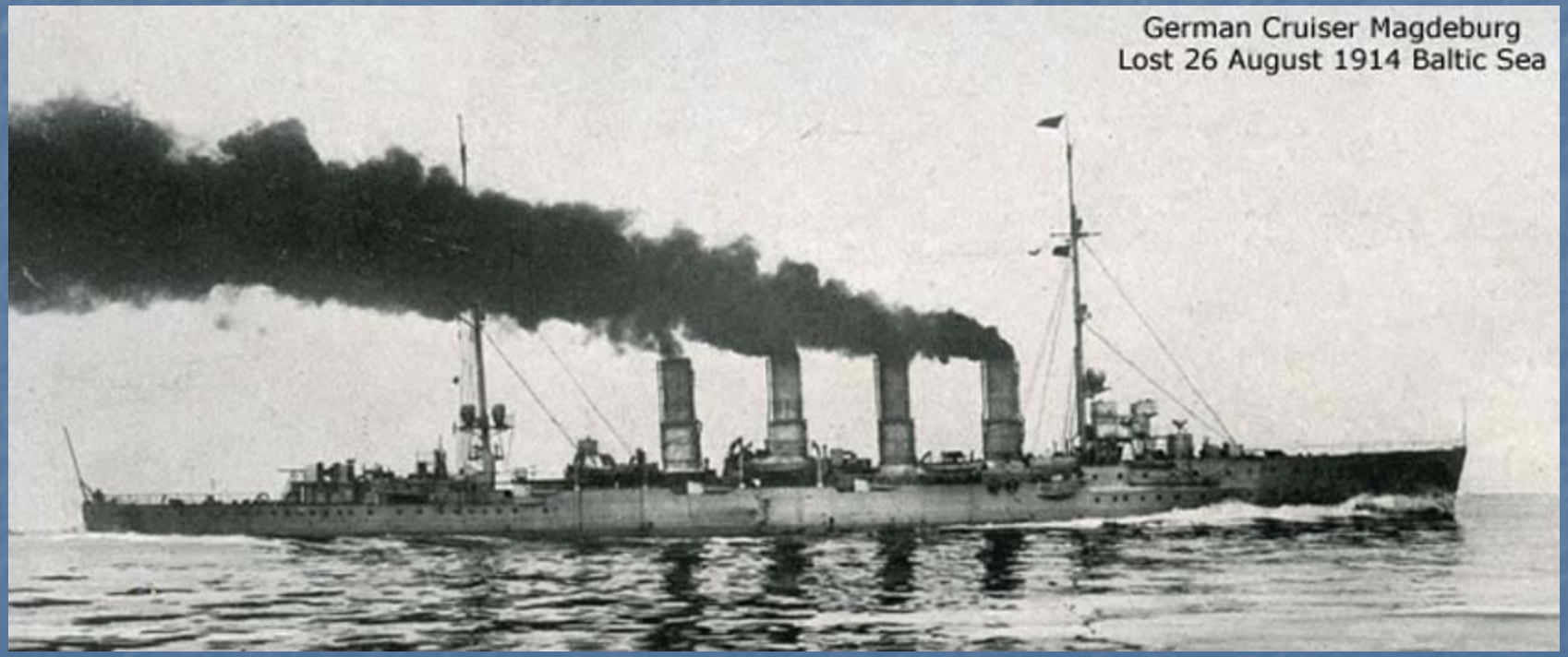
- 1844 Samuel F. B. Morse: “What hath God Wrought?” Telegraph.
- 1876 Alexander Graham Bell: Telephone.
- 1895 Guglielmo Marconi: Wireless Telegraphy.
- 1915 Bell Telephone: Radio telephone.



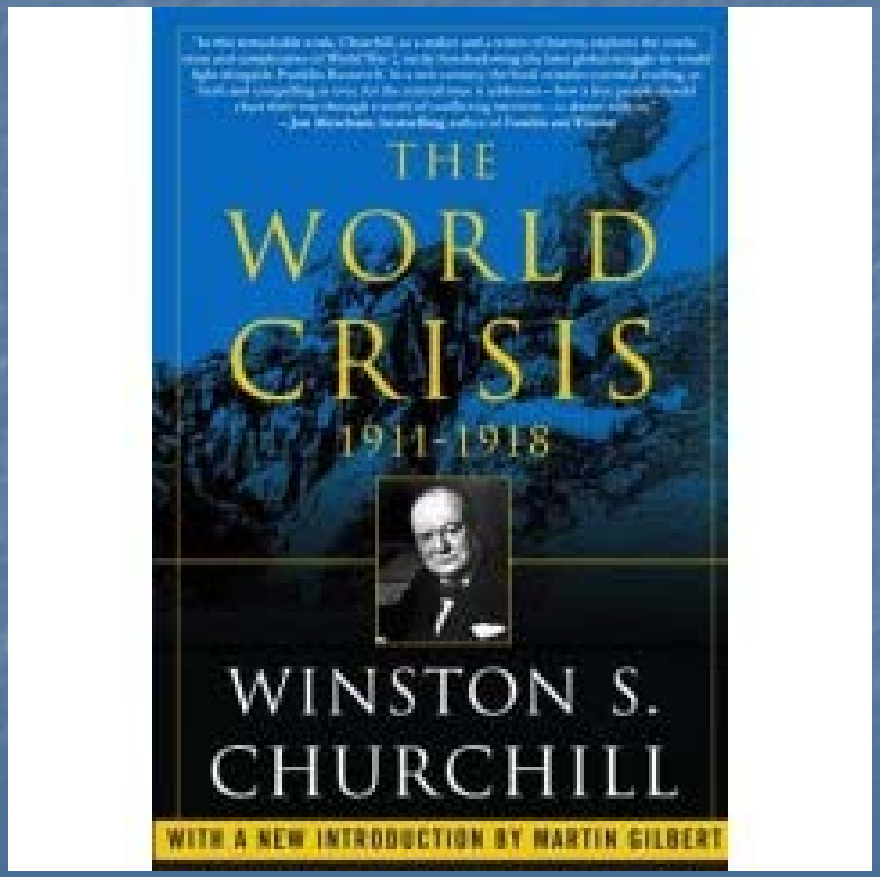
The Admiralty

- During World War I, cryptology became a powerful weapon of war.
- Germany suffered many cryptologic defeats.

World War I Cryptology

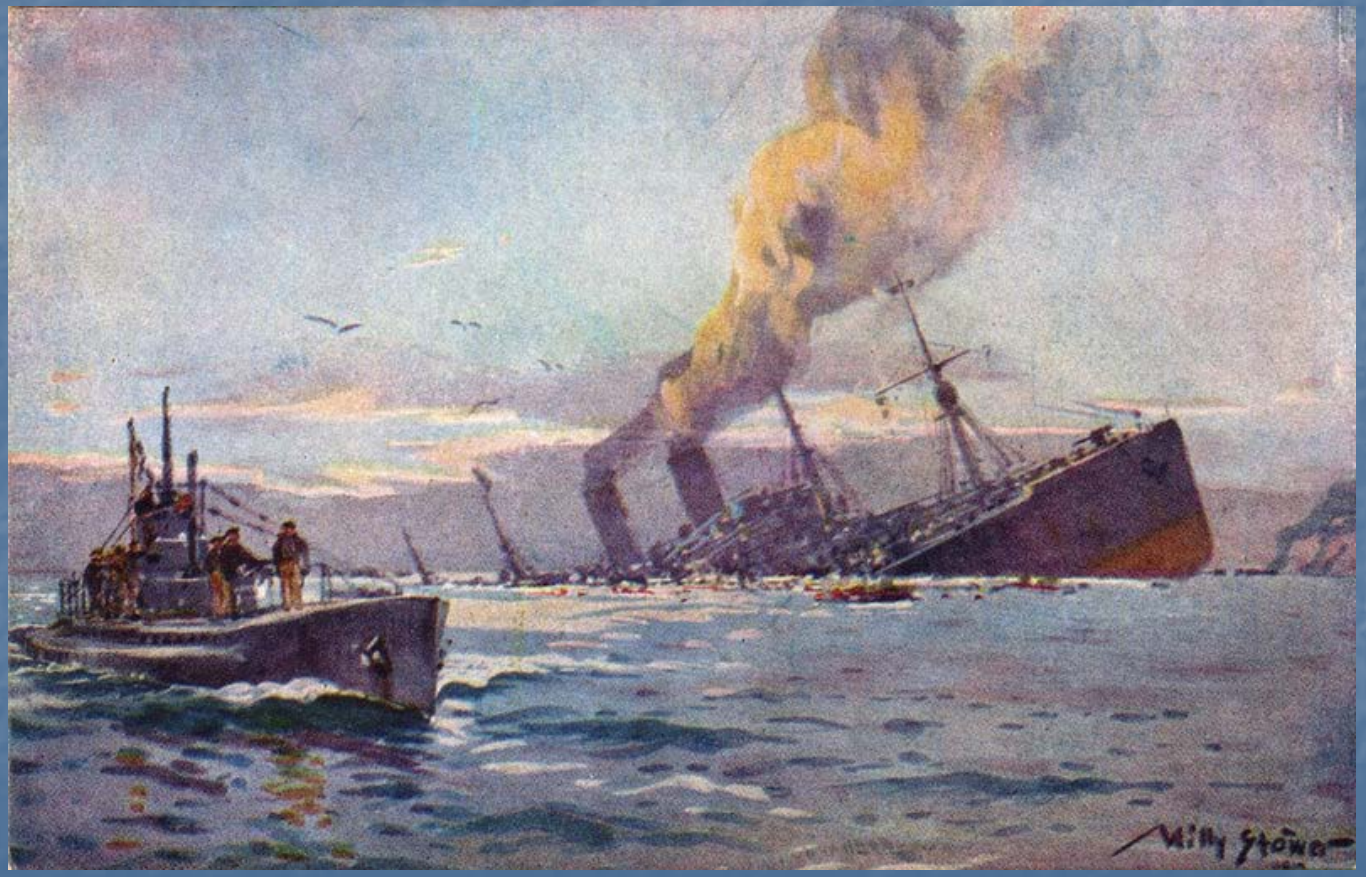


Churchill told the secret



Blitzkrieg

U-Boat Attacks



Cryptography

Code

Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
führung	17166
Ganz geheim	17214
Gebeit	17388
geheim	4377
Gemeinsame	4458

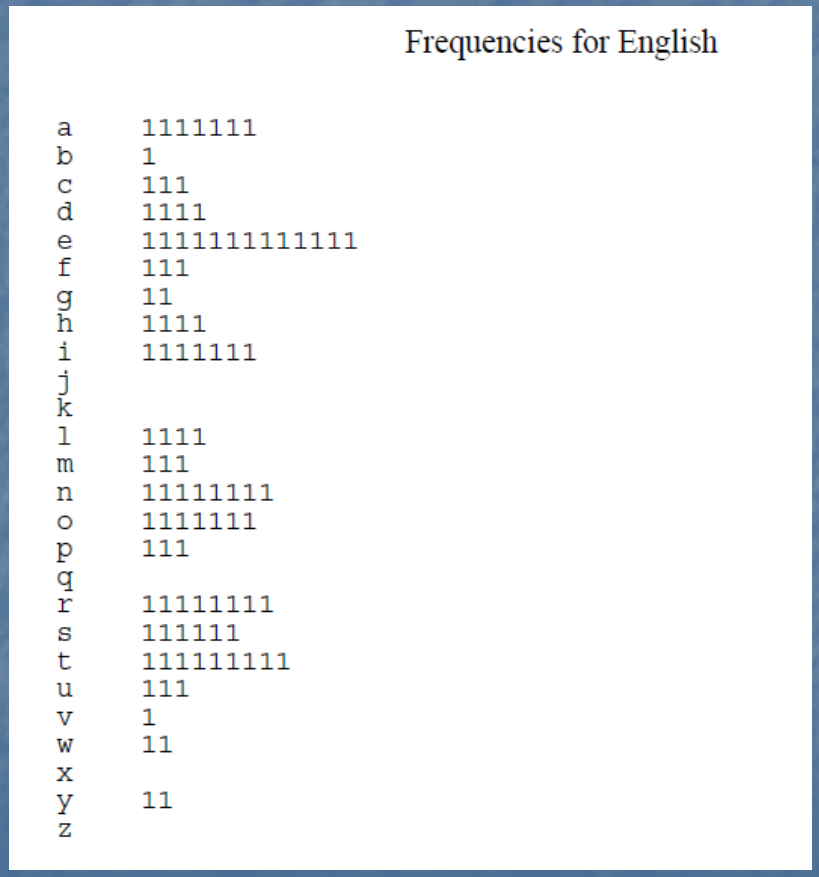
Cipher

```
abcdefghijklmnopqrstuvwxyz
KPFHIGLDEXCVTOUBJQZMRNAYSW
```

Ciphertext

```
VRRQS  HRSOH  EHJDQ  VOLGL  QJWKH  DOSKD  EHWEB
DPRXQ  WVGLI  IHUHQ  WWKDQ  WKUHH  WRGHW  HUPLQ
HFLSK  HUHTX  LYDOH  QWV
```

Frequencies for English



Cryptanalysis

Ciphertext

```
VRRQS  HRSOH  EHJDQ  VOLGL  QJWKH  DOSKD  EHWEB
DPRXQ  WVGLI  IHUHQ  WWKDQ  WKUHH  WRGHW  HUPLQ
HFLSK  HUHTX  LYDOH  QWV
```

Frequency Analysis

```
A
B    1
C
D    111111
E    111
F    1
G    111
H    111111111111111
I    11
J    11
K    11111
L    111111
M
N
O    1111
P    11
Q    11111111
R    11111
S    1111
T    1
U    1111
V    1111
W    111111111
X    11
Y    1
Z
```

Cryptanalysis

Ciphertext

```
OINRF   HORXH   ONAPF   VHLHM   NZOFU   OINAN
GRLZI   PYNJL   HOINM   KVBLY   GMKVB   SFLAG
LAALY   BNRNY   OVHNG   SXPO
```

Frequency Analysis

A	11111
B	111
C	
D	
E	
F	1111
G	1111
H	111111
I	1111
J	1
K	11
L	1111111
M	111
N	1111111111
O	11111111
P	111
Q	
R	1111
S	11
T	
U	1
V	1111
W	
X	11
Y	1111
Z	11

Cryptanalysis

A	11111
B	111
C	
D	
E	
F	1111
G	1111
H	111111
I	1111
J	1
K	11
L	1111111
M	111
N	1111111111
O	11111111
P	111
Q	
R	1111
S	11
T	
U	1
V	1111
W	
X	11
Y	1111
Z	11

- Ciphertext N corresponds to plaintext e?
- Ciphertext O corresponds to plaintext t?
- Most frequent trigraph is OIN.

Cipher Disk


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 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
G S A
S. S.

Germany Adopted Machine Encryption

- Germany selected a commercial encryption machine called Enigma.
- After modification it became a primary encryption method for Germany's military.

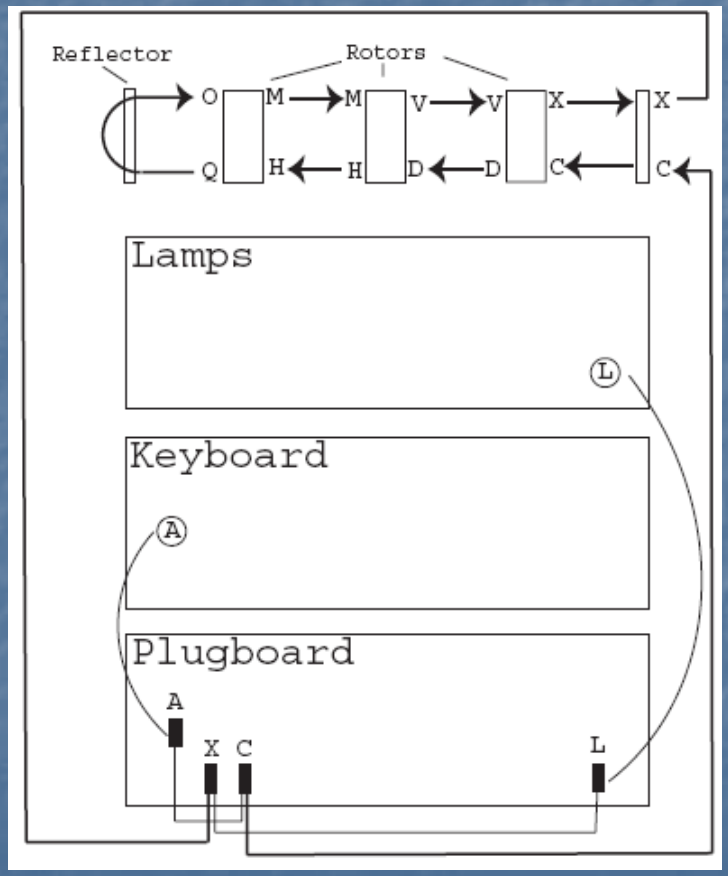
Each Enigma cipher is a permutation of the letters of the alphabet

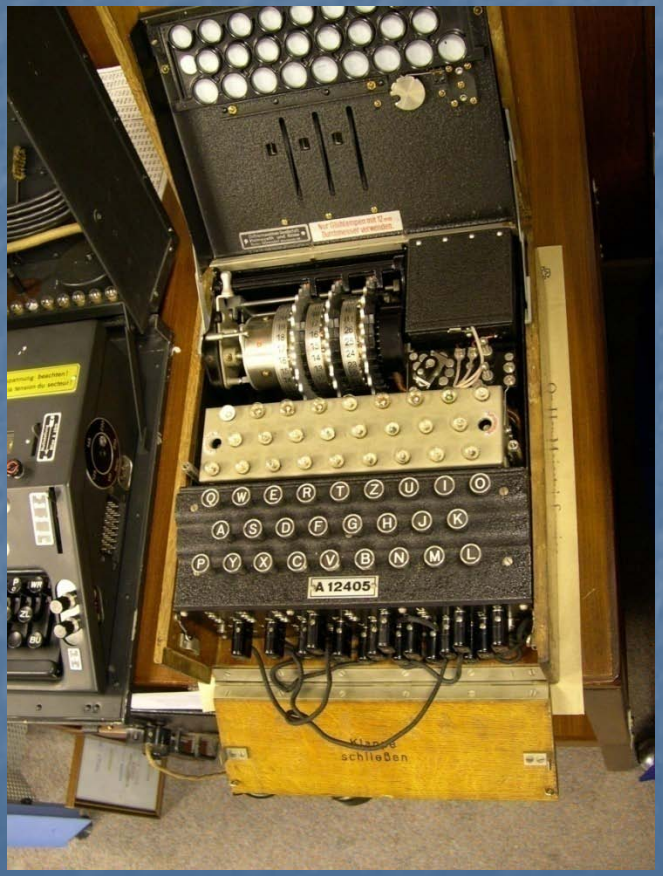
abcdefghijklmnopqrstuvwxyz

OHELCPYBSURDZTAFXKINJWVQGM

(ao)(bh)(ce)(dl)(fp)(gy)(is)(ju)(kr)(mz)(nt)(qx)(vw)

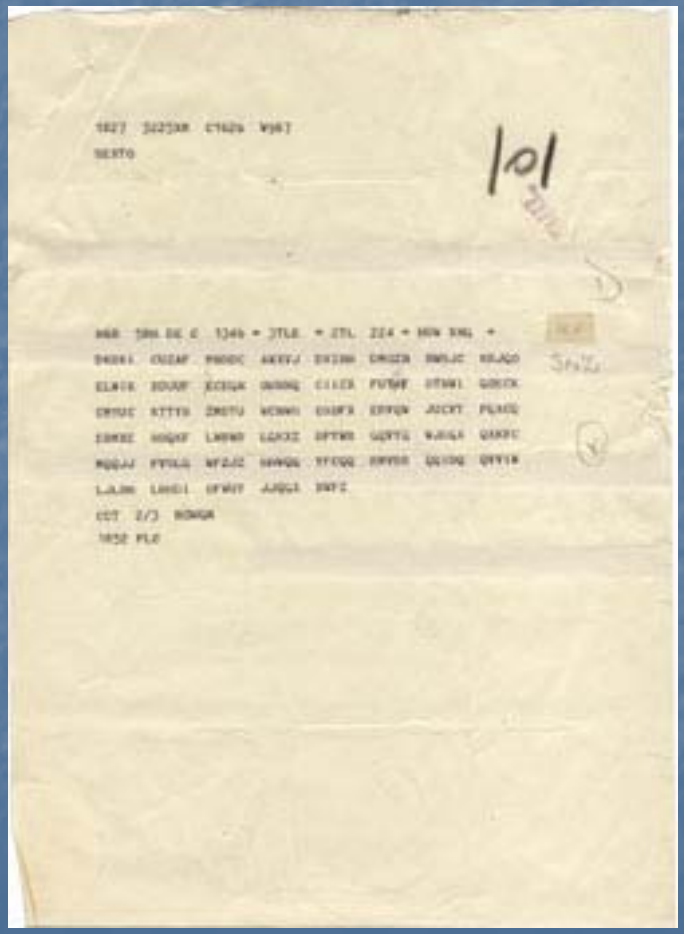
Enigma


Reflector
Rotors
O
M
M
V
V
X
X
Q
H
H
D
D
C
C
Lamps
L
Keyboard
A
Plugboard
A
X
C
L


A 12405

Enigma

Enigma has a period of about 17576.



Cipher Machines

TYPEX

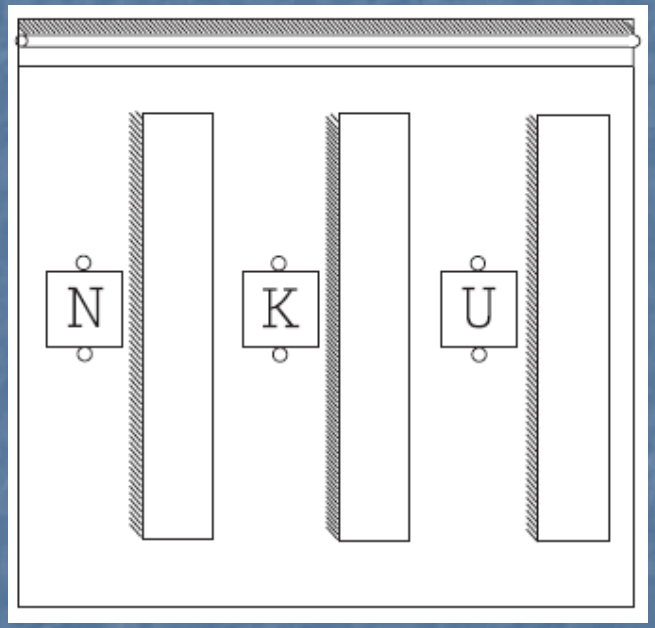
SIGABA

Enigma Rotor

The Key

- At first there were 3 rotors.
- 6 ways to order the rotors.

Setting the Rotors



The Key

- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.

The Plugboard

n	Number of connections	n	Number of connections
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	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

The Key

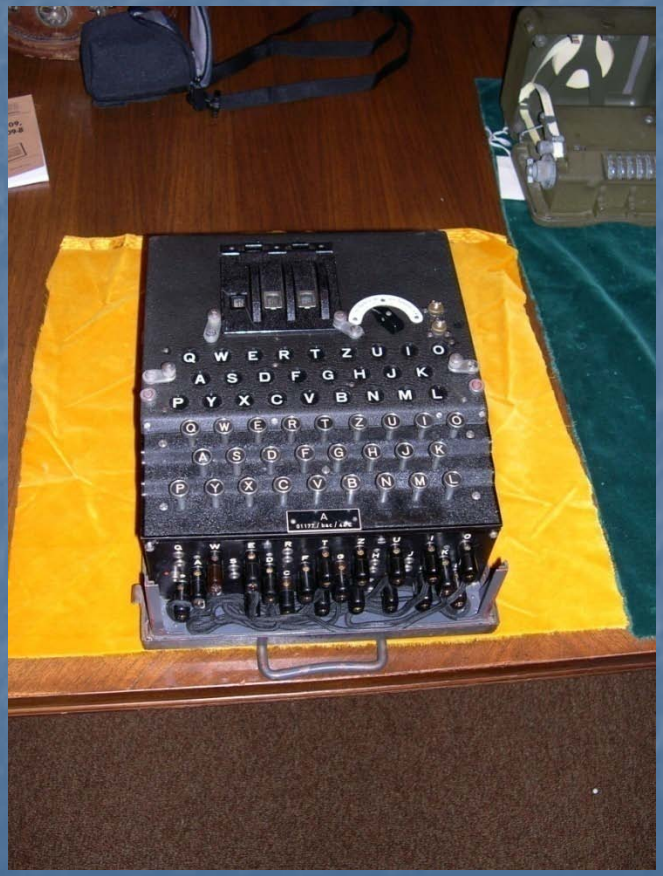
- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
- 100,391,791,500 ways to set the plugboard.

The positions of the turnover notches was part of the key.

The Key

- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
- 100,391,791,500 ways to set the plugboard.
- 676 ways to set the turnover notches.
- 7,156,755,732,750,624,000 ways to set the key.

The sender and receiver must set their machines in exactly the same way.



Checking one setting per second

- Would take 22,693,900,000 years.
- A better plan was needed.
- Need a machine to attack a machine.

In 1929, the Polish government selected three mathematicians from Poznan University to attack Enigma

- Jerzy Rozycki [1909 – 1942]
- Henryk Zygalski [1908 – 1978]
- Marian Rejewski [1905 – 1980]

Marian Rejewski

- The most famous of the Polish mathematicians was Marian Rejewski
- Rejewski used mathematical results and ideas to attack Enigma.

Message Indicators

- Each message was sent using a message setting selected by the operator.
- How did the operator transmit the message setting to the authorized receiver?
- Sent it twice encrypted with Enigma using the ground setting.

Example

- Ground setting `nku`. Transmitted in the clear.
- Message setting `wku`. Sent twice; encrypted with the ground setting.
- Say, `wku wku` is encrypted as `XFC DXS`
- Send `NKU XFC DXS`

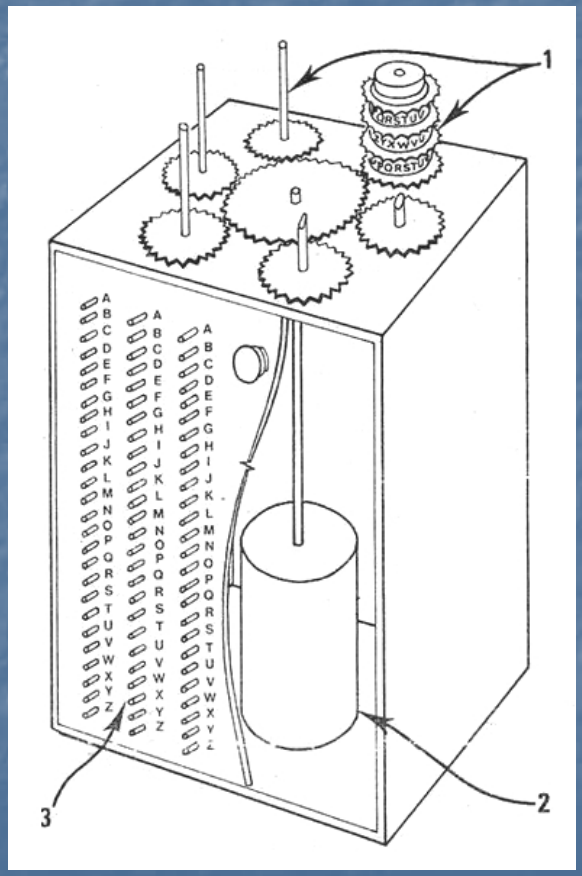
Rejewski's Example

Given sufficiently ample cipher material, it may happen that, on a given day, there will be three messages with keys such as

RTJ	WAH WIK
DQY	DWJ MWR
HPB	RAW KTW

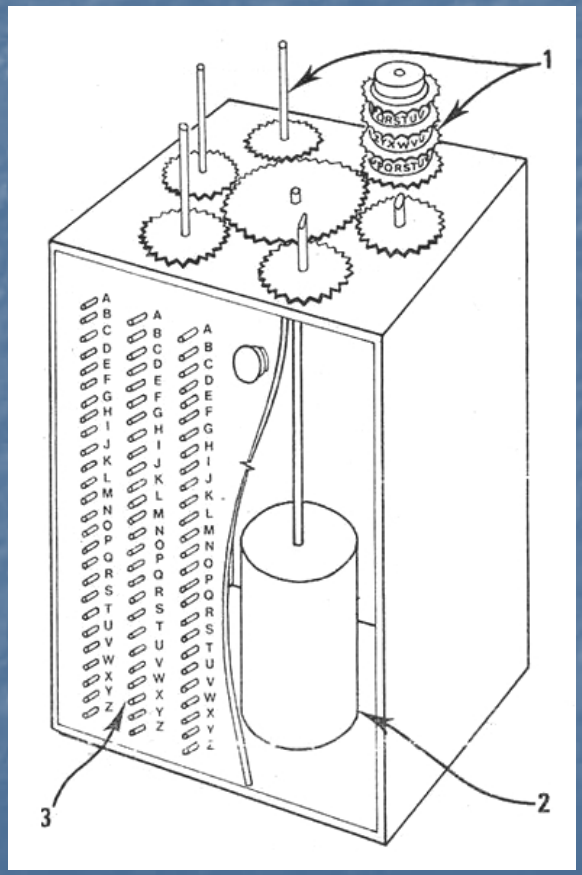
Marian Rejewski

The Polish Bomba



- 6 sets of Enigma rotors driven by a motor.
- 6 bomby – one for each possible rotor order.

Fast Rotor Offsets



RTJ WAH WIK

First Enigma pair.

n and *n* + 3

Fast Rotor Offsets

RTJ	WAH WIK	First Enigma pair.
DQY	DWJ MWR	n and $n + 3$.
		Second Enigma pair.
		$(n + 15)+1$ and
		$(n + 15)+3+1$

Fast Rotor Offsets

RTJ	WAH	WIK
DQY	DWJ	MWR
HPB	RAW	KTW

First Enigma pair.

n and $n + 3$.

Second Enigma pair.

$(n + 15)+1$ and

$(n + 15)+3+1$

Third Enigma pair.

$(n + 18)+2$ and

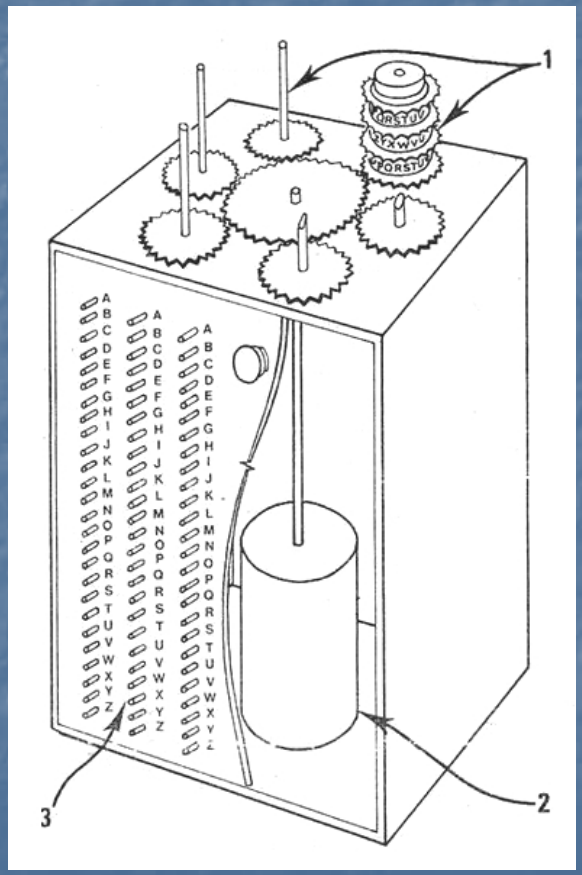
$(n + 18)+3+2$.

Other Rotor Offsets

RTJ	WAH	WIK
DQY	DWJ	MWR
HPB	RAW	KTW

- Middle rotor offsets: *m*, *m* + 23, and (*m* + 23) + 25.
- Left (slow) rotor offsets: *l*, *l* + 12, and (*l* + 12)+4

Look for Simultaneities



- Input W.
- Look for simultaneities; e.g., USA USA.
- Results in 12 hours if rotor order needed to be changed; results in 2 hours if all 6 bombe attacked the indicators.

But ...

Why was it called a bomba?

The name “bomba” was given by Rozycki. [A]t [that] time there was ... in Warsaw [a very popular] ice-cream [dessert] called [a] bomba which looked like a[n] old-fashioned ..., round, with chocolate [on the] outside. [T]he idea [for] the machine came while they were eating it.

Colonel Tadeusz Lisicki

Then Germany added two more rotors.

Jerzy Rozycki [1909 – 1942]

Henryk Zygalski [1908 – 1978]

Marian Rejewski [1905 – 1980]

Enigma by Wladyslaw Kozaczuk

Bletchley

Bletchley Park

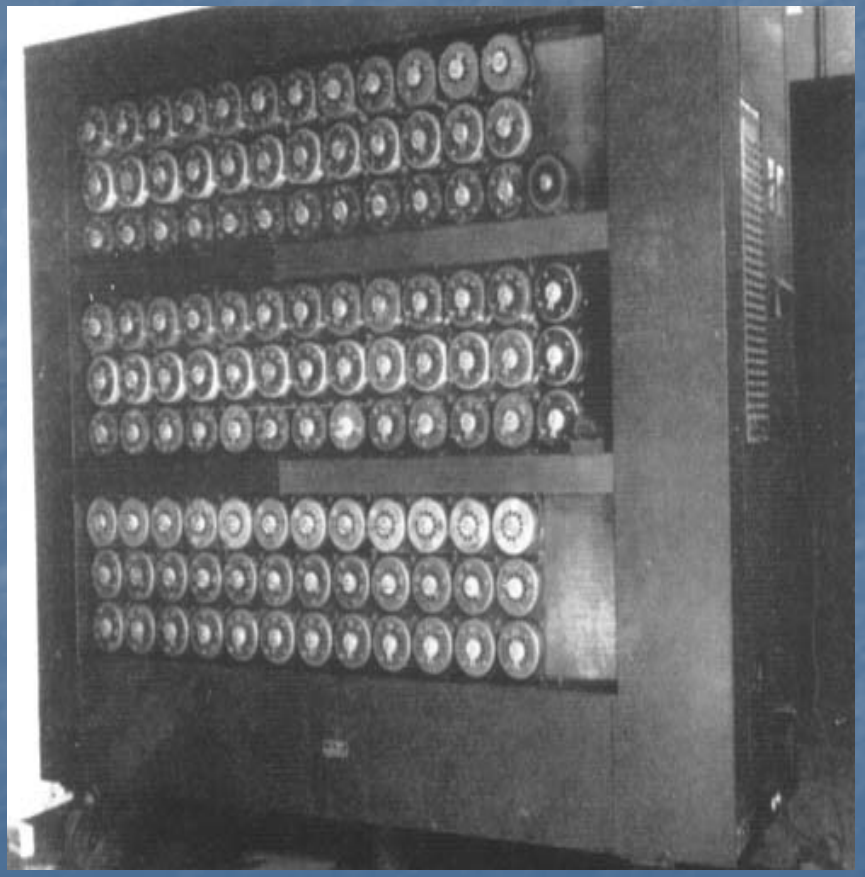
The Huts

Alan Turing [1912 – 1954]

- *Entscheidungsproblem* 1936.
- Hut 8 in 1939.

Hut 8

The Turing Bombe



Cribs

- CIPHERTEXT

  VWHCD IUGHL UVFAO BNEWN AGZWY
  ZUXNN PYZWN LKMUO FRIIL OJPAE
- Plaintext

  markworthxattawckedxbyxtwoxpurs
  uitxplanes

Crib Placement

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxpurs

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxpurs

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxpurs

Crib Placement

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxpur

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxpu

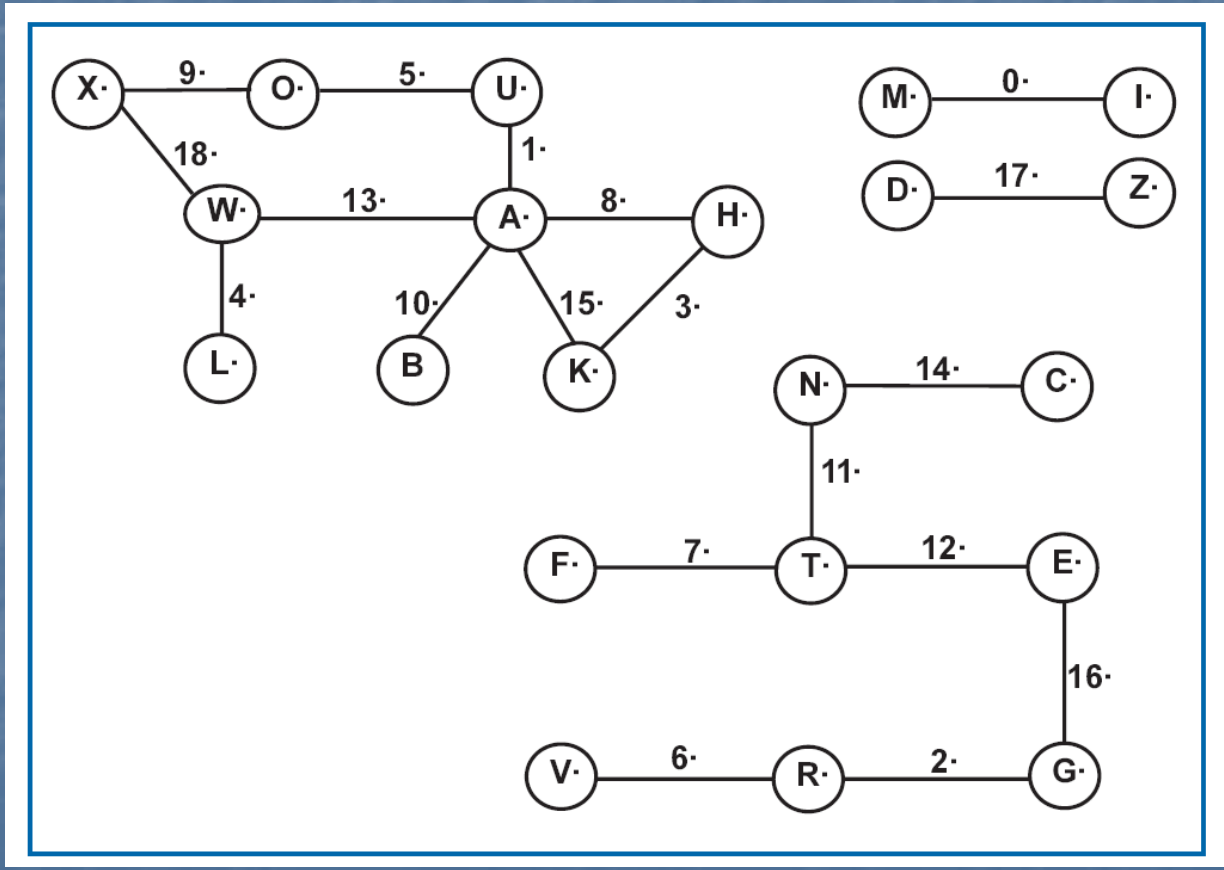
VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN

markworthxattackedxbyxtwoxp

Crib Placement

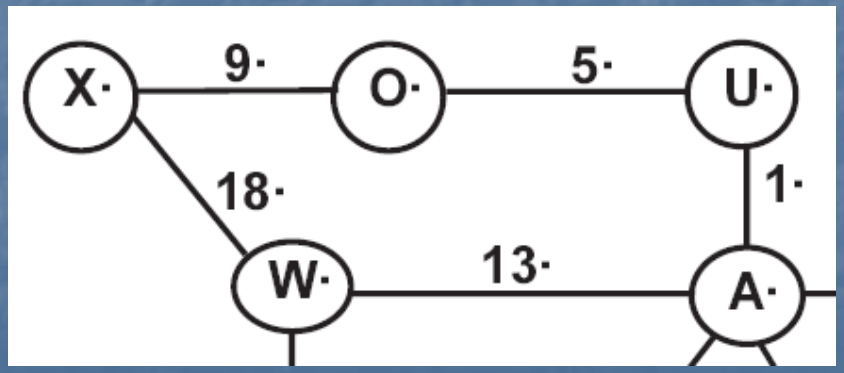
Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X

Diagram

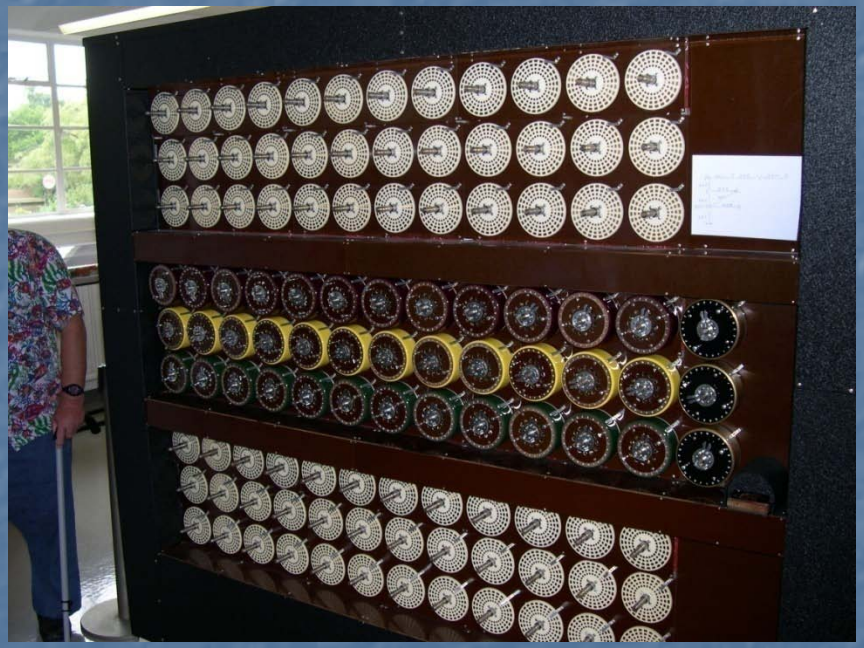


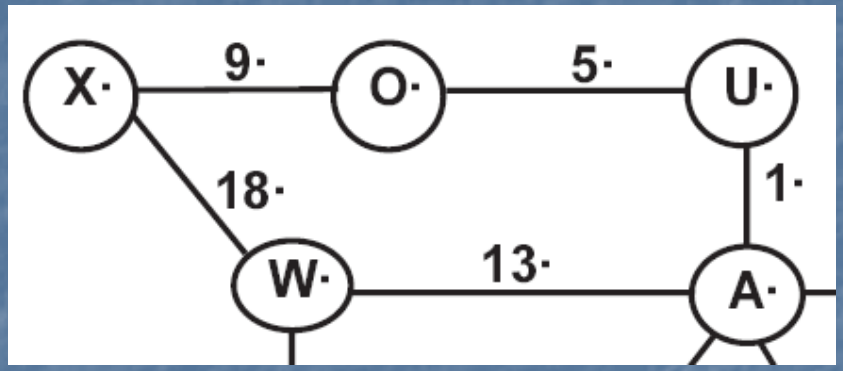
Loop

Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X



Offsets



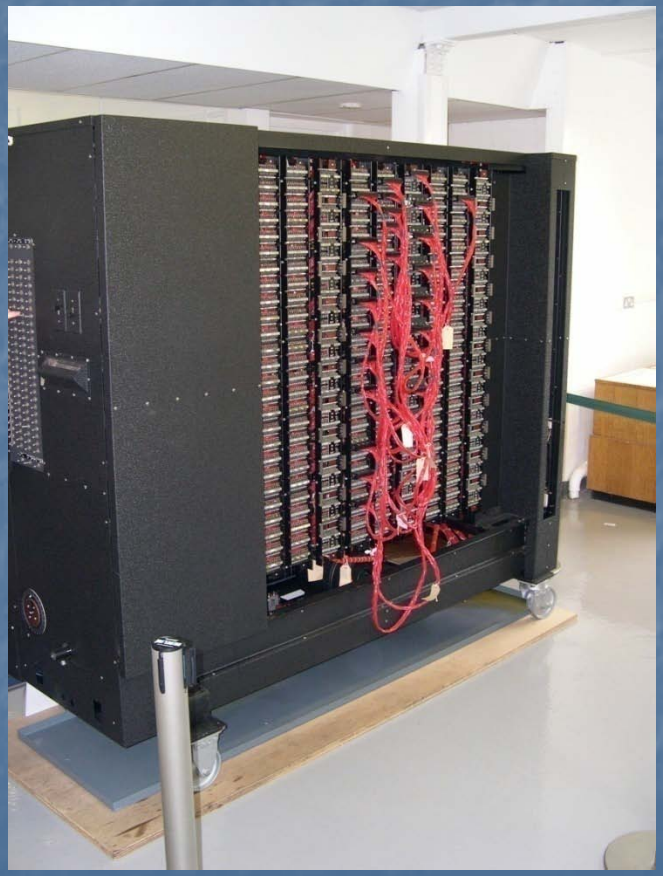


Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X

Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	8	20	6	7	11	20	21	5	0	14	2	13	4	22	13	0	6	25	22
Crib:	12	0	17	10	22	14	17	19	7	23	0	19	19	0	2	10	4	3	23

Position 1: U (20) and A (0).
Position 5: U (20) and O (14).
Position 9: O (14) and X (23).
Position 18: W (22) and X (23).
Position13: W (22) and A (0).

Plugging Up



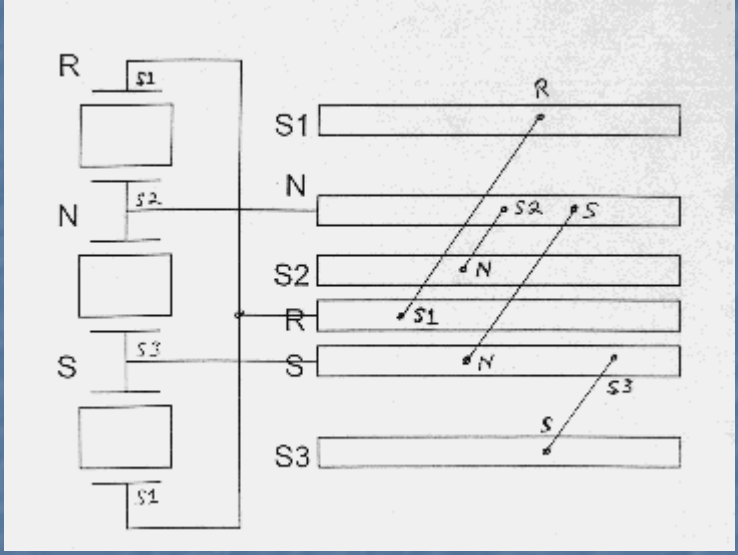
Switch Bank	Switch In	Switch Out	Wheel Settings 1	2	3	4
1	20	0	0	0	0	0
2	6	17	0	0	0	1
3	10	7	0	0	0	2
4	14	20	0	0	0	4
5	17	21	0	0	0	5
6	19	5	0	0	0	6
7	7	0	0	0	0	7
8	23	14	0	0	0	8
9	0	2	0	0	0	9
10	19	13	0	0	0	10
11	19	4	0	0	0	11
12	0	2	0	0	0	12
13	2	13	0	0	0	13
14	10	0	0	0	0	14
15	4	6	0	0	0	15
16	23	22	0	0	0	17

Alan Turing: The Enigma by Andrew Hodges

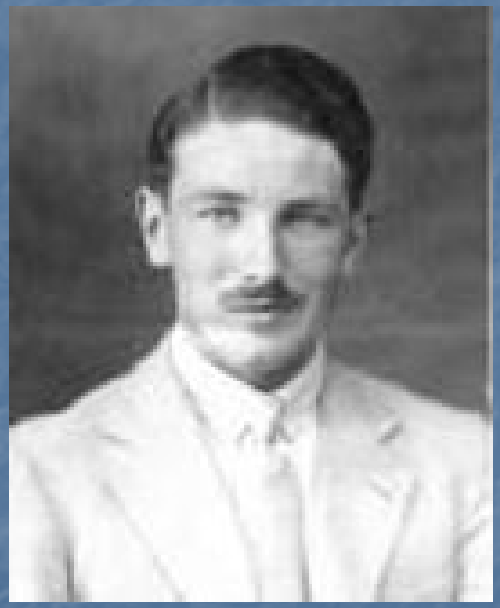
http://www.turing.org.uk/turing/

The Turing – Welchman Bombe

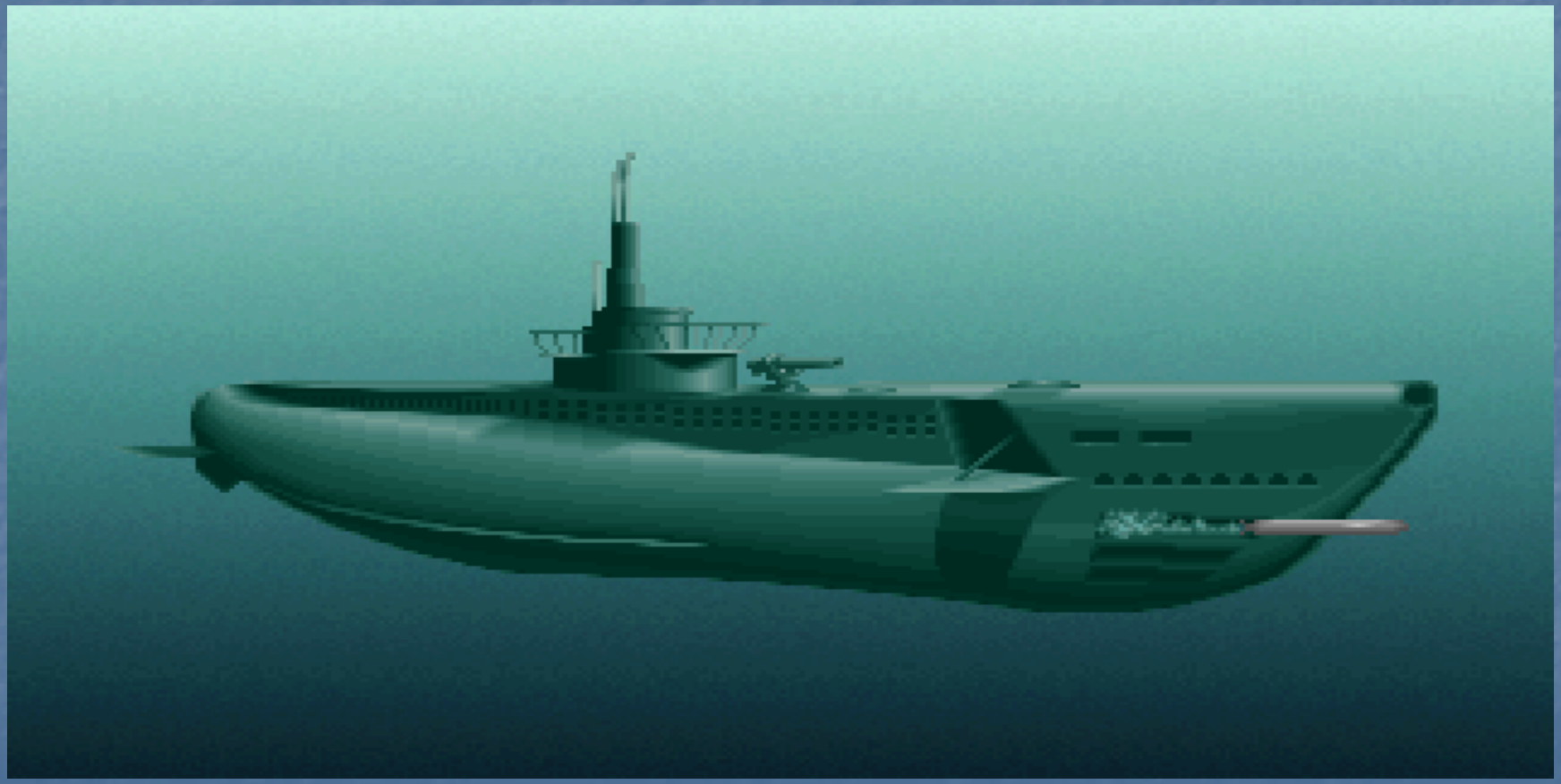
The diagonal board



Gordon Welchman
(1906 – 1985)

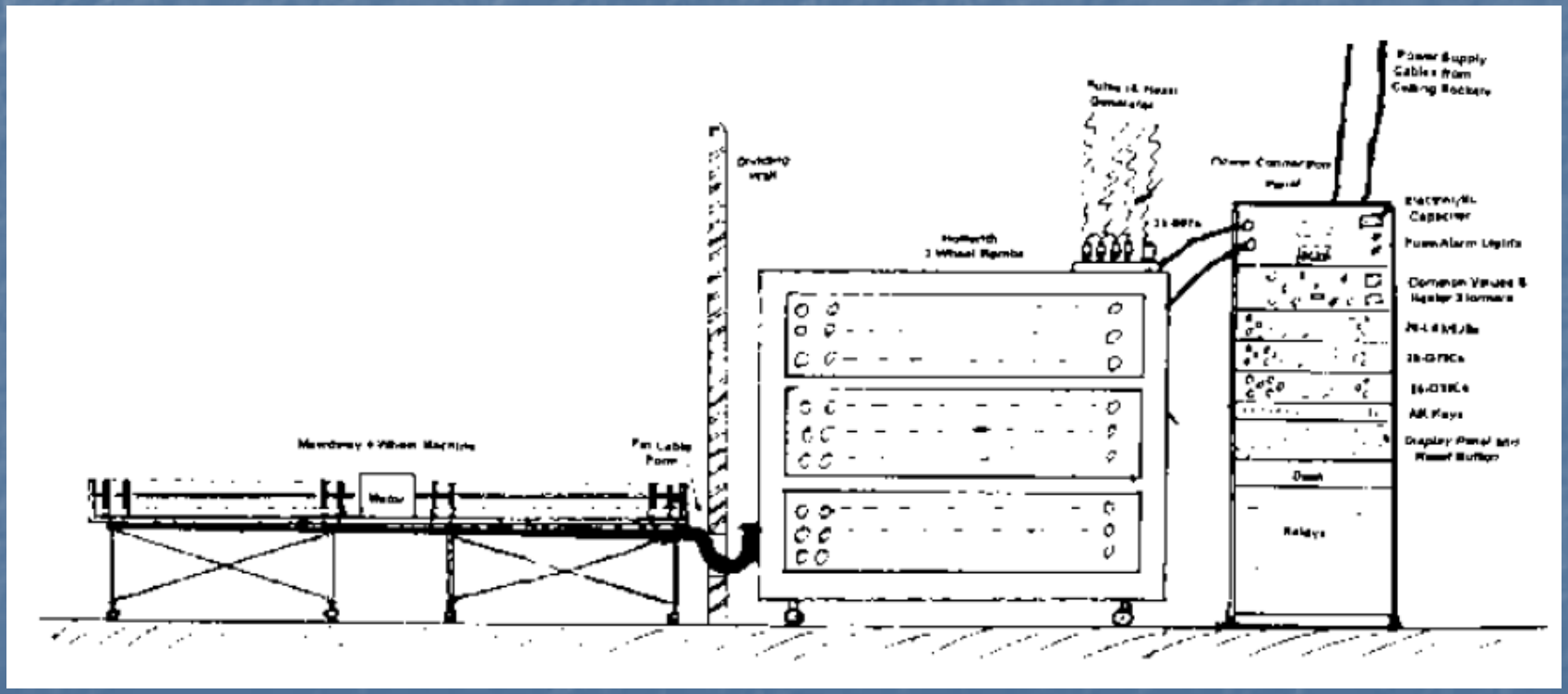


February 1942 – December 1942 – September 1943

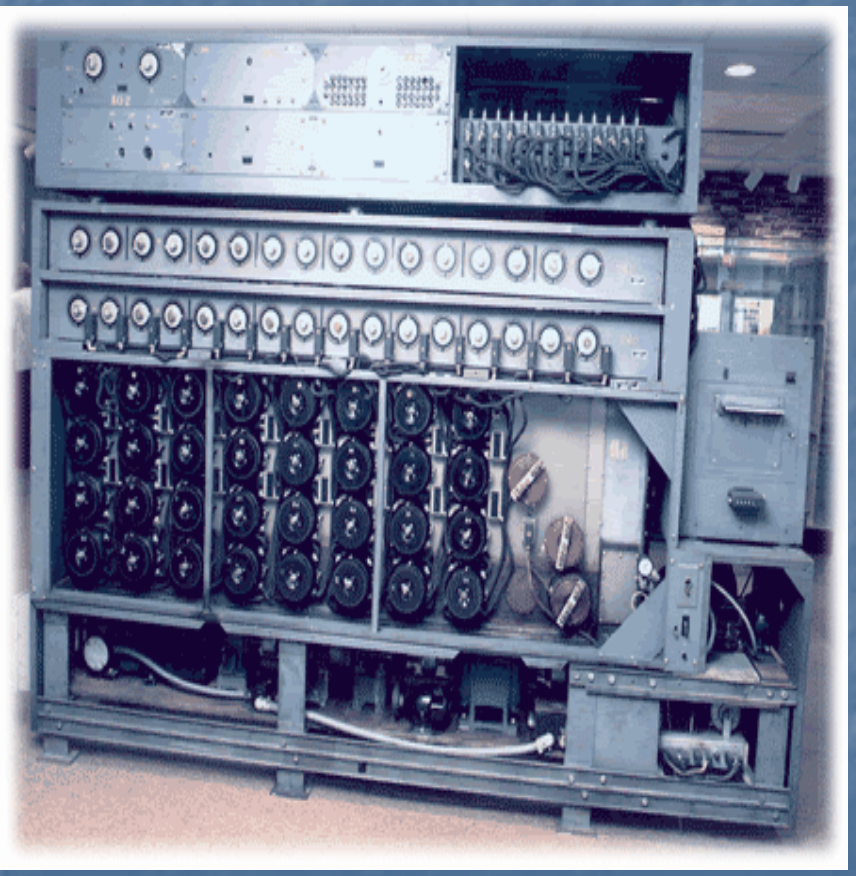


The Four-rotor Naval Enigma

Cobra



Joseph Desch [1907 – 1987]



NCR engineer in Dayton, OH.

SECRET

Dec 1942

VISIT TO NATIONAL CASH REGISTER CORPORATION

of DAYTON, OHIO

On December 21st I visited the works at Dayton, Ohio, where the Bombes are being made, with Commander Wenger, Lieutenant-Commander Engstrom, Lieutenant-Commander ~~Meteur~~ Meager, Lieutenant(jg) Eachus and Major Stevens. The weather held up our train and we arrived six hours late at 2 p.m. so that we did not have quite so long there as we might have had, but probably sufficient.

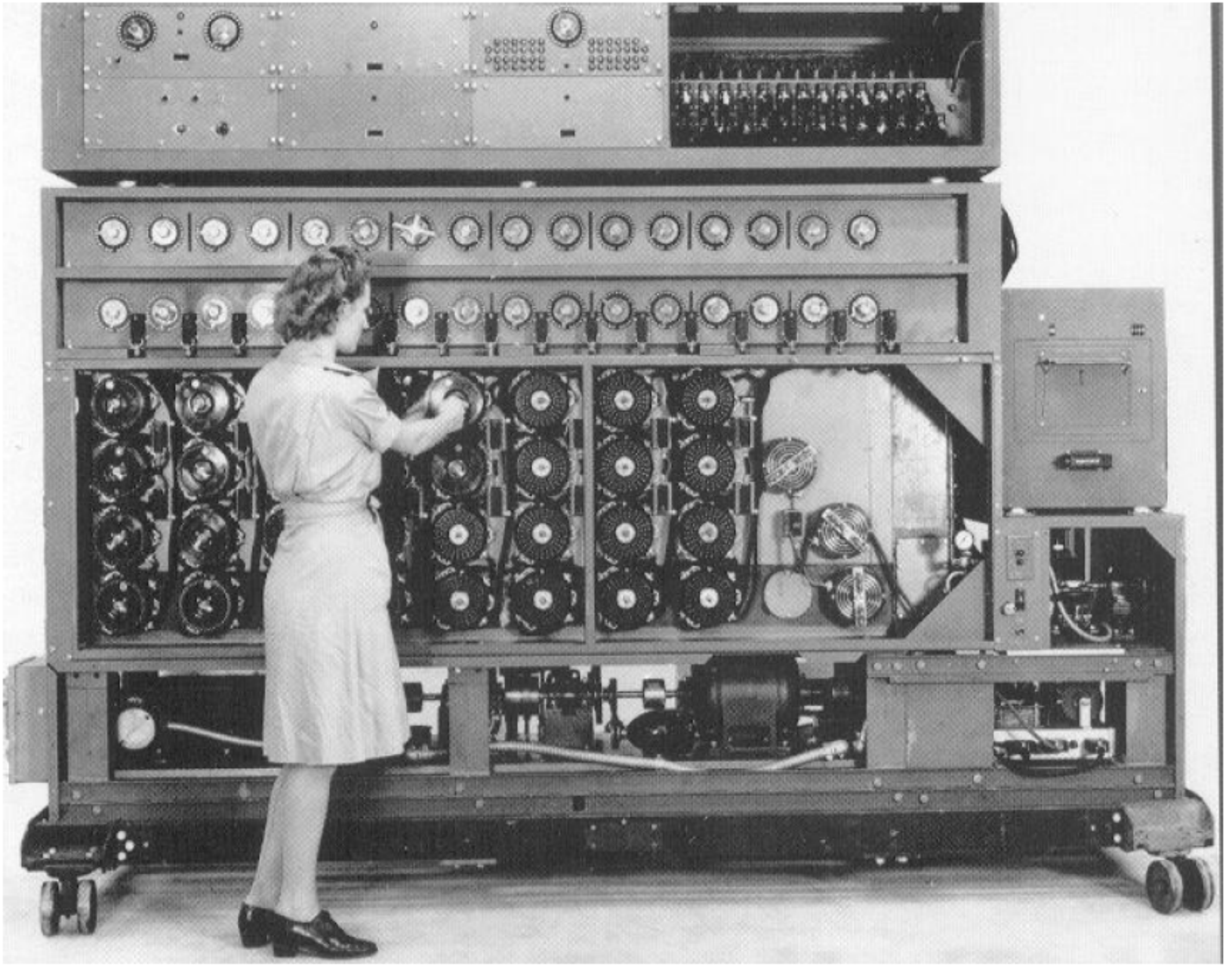
The plans for the Bombes are on the whole essentially the same as ours, but there are a number of minor differences which should be noted.

(A) As mentioned in my previous report the machine is intended to stop and reverse whenever there is a "stop", and go back to the position of the stop, and there do further twisting. Engstrom and I are still both rather unhappy about this idea. We were given a demonstration of how the motor was able to reverse and be going full speed in the reverse direction in a fraction of a second, with the full load; however this seems to me hardly to prove that all will be well when one tries to reverse the Bombe itself, e.g. the gears might get distorted under the strain.

/ They say..

part of Dr. Turing of G.C. & C.S.

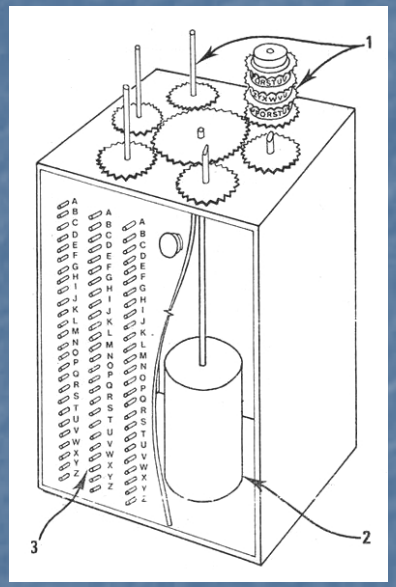
SECRET

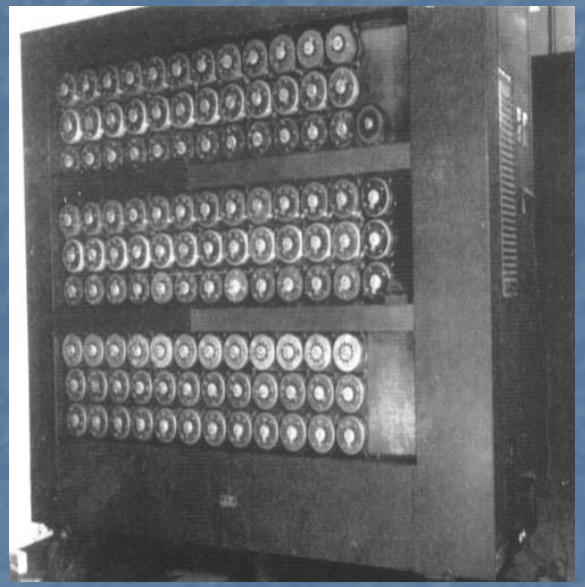


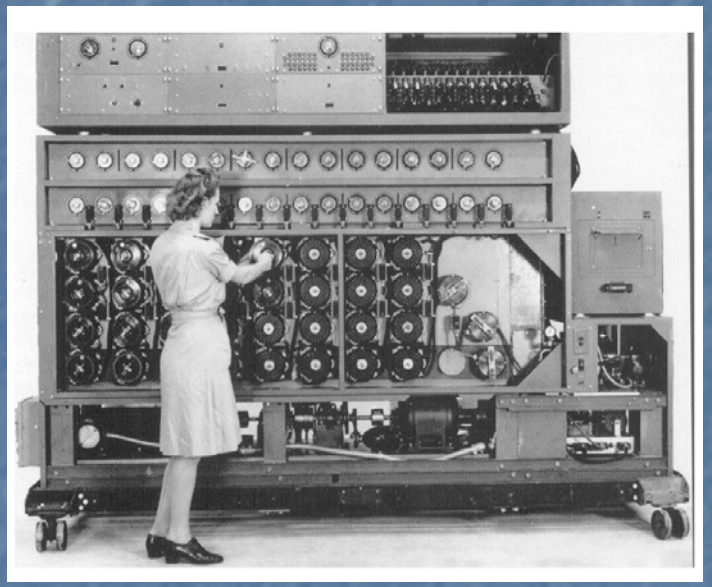
The Secret in Building 26 by Jim DeBrosse and Colin Burke.

http://www.daytoncodebreakers.org/

Evolution of the Cryptologic Bombe







IVXHS G