Enigma

World War I

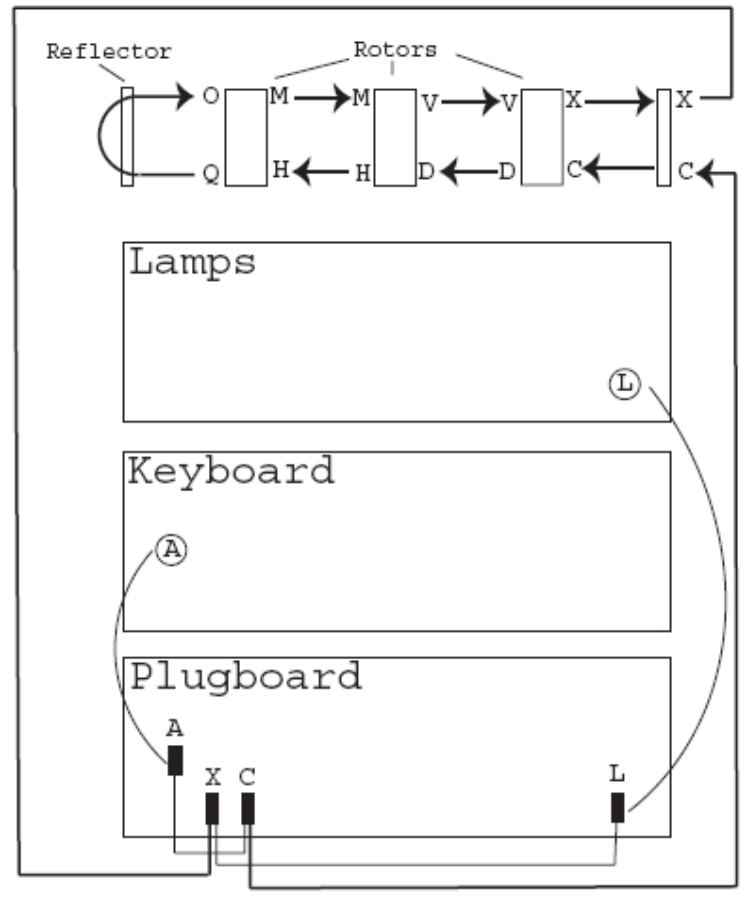
Enigma

An advertising brochure for commercial Model D of the Enigma cipher machine.

This American advertising brochure for the commercial Enigma cipher machine hugely underestimates its performance.

Enigma

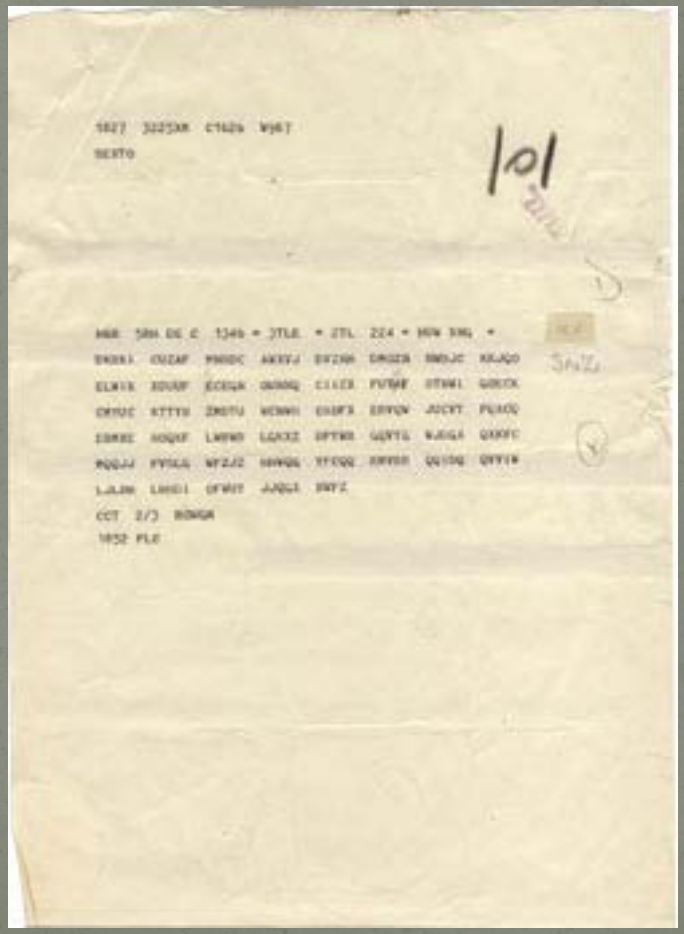
Enigma


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


A 12405

Security

Enigma has a period of about 17576.



Each Enigma cipher is a simple substitution

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

Setting Sheets

GEHEIM! SONDER-MASCHINENSCHLUSSEL: ENIGMA OKTOBER 2009

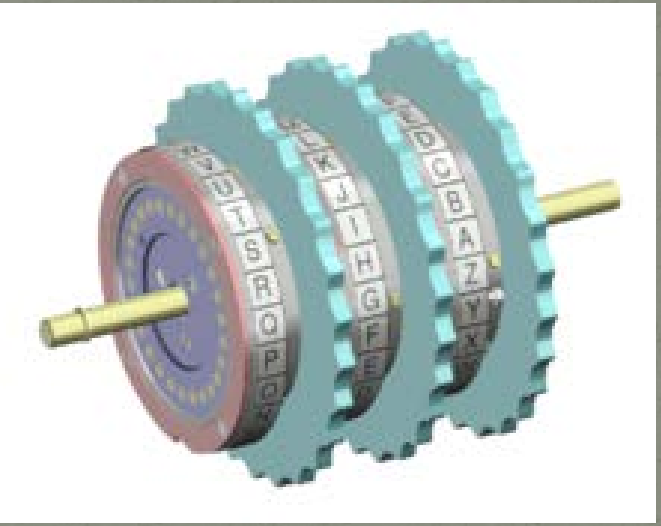
Tag	UKW	Walzenlage	Ringstellung	Steckerverbindungen	Spruchschlussel
31	B	Beta V VIII VI	A T B M	01-08 02-20 03-21 04-05 06-24 07-26 10-17 13-23 14-15 18-22	F V U G
30	B	Gamma VIII III IV	N B Z L	01-08 02-12 03-26 04-18 05-09 06-13 07-10 14-24 15-21 17-23	S B Z F
29	C	Gamma II IV V	N M E Y	01-11 03-16 04-13 05-19 06-08 07-21 09-17 12-14 15-18 22-24	J F R F
28	C	Gamma V I VII	Q X H D	01-15 03-16 04-17 06-11 07-12 09-21 10-20 14-26 18-23 19-24	W E T C
27	C	Beta IV VI I	V F L K	01-11 02-09 03-15 05-26 06-24 07-10 08-23 12-19 17-21 18-20	B L C Y
26	B	Gamma IV II I	W E T C	01-09 02-21 04-14 05-25 06-26 08-15 10-17 11-24 12-18 13-23	V Q G A
25	C	Beta VIII V II	X H U R	01-02 03-07 04-13 06-26 08-19 10-23 12-18 14-22 16-20 17-25	O K F R
24	C	Gamma IV V I	F V U G	01-18 02-06 03-07 04-11 09-25 12-13 14-17 16-26 19-22 21-23	N B Z L
23	C	Beta I V IV	P P Q N	01-11 02-19 04-26 05-18 06-24 07-20 10-16 12-25 15-17 21-22	O K F R
22	B	Gamma I IV VI	O S S H	01-12 02-18 03-07 04-21 05-09 08-16 14-25 17-20 19-26 23-24	W B P Q
21	B	Gamma II I VI	J F R F	01-18 02-06 07-14 08-19 09-13 10-23 11-21 16-25 17-22 20-26	A T B M
20	C	Gamma II I VI	A S J X	02-03 04-21 07-19 08-14 09-13 10-26 11-17 12-15 16-20 23-24	H N W S
19	B	Gamma IV VII II	A Q O J	02-10 03-14 06-20 07-26 08-21 09-13 11-15 12-16 18-23 19-24	D G K V
18	C	Beta II IV V	Q P B B	01-02 04-25 05-10 06-23 08-09 12-19 13-20 14-15 16-17 18-26	H N W S
17	C	Gamma III II I	S B Z F	01-20 02-03 04-05 06-19 07-08 09-22 10-25 11-17 12-15 14-24	R B S O
16	C	Beta II VII I	F X B I	01-12 02-19 03-24 04-06 05-21 07-17 10-15 13-23 18-20 22-26	Z T C N
15	C	Beta VII V IV	V Q G A	01-18 03-12 04-05 06-10 07-17 11-25 14-20 19-24 21-22 23-26	N M E Y
14	C	Gamma V IV VII	W B P Q	01-07 02-15 05-25 06-26 08-23 09-13 10-18 11-14 17-20 19-22	O U W H
13	C	Gamma VII V IV	D G K V	01-10 03-09 05-08 07-17 11-21 13-18 14-15 16-23 19-20 22-24	O S S H
12	C	Gamma VI IV II	O U W H	02-23 03-19 04-26 05-21 07-16 08-15 10-12 13-24 14-25 20-22	P P Q N
11	B	Gamma VIII II V	O Q Z X	01-02 03-11 04-24 05-09 06-18 07-21 08-20 12-14 13-15 16-26	M L T L
10	B	Beta V IV VI	U T Q H	01-02 03-16 04-20 05-26 06-24 08-10 09-15 11-14 12-22 18-21	X H U R
09	C	Gamma VIII III IV	R A S H	01-14 02-15 03-16 04-17 05-18 06-19 07-20 08-21 09-22 10-23	C I T O
08	C	Gamma II I III	R B S O	02-05 03-26 04-24 06-13 07-11 09-20 10-25 14-18 15-23 19-21	A S J X
07	B	Beta IV VII I	B L C Y	01-20 02-10 04-22 05-06 07-11 09-16 12-19 13-21 14-18 17-26	Q X H D
06	B	Gamma I III IV	O K F R	01-03 04-23 06-22 07-08 09-24 12-15 13-19 14-26 16-17 20-21	Q P B B
05	B	Gamma VII V VI	H N W S	03-08 04-26 05-21 06-22 10-11 12-16 13-24 15-17 18-19 23-25	F X B I
04	C	Gamma VIII V VI	Z T C N	01-09 02-14 03-12 04-22 06-20 07-16 08-10 13-23 15-18 17-21	O S S H
03	C	Beta II IV III	M L T L	01-06 02-18 03-12 07-19 08-21 09-20 10-25 11-22 15-24 17-23	X B A I
02	B	Gamma II V VIII	A F D D	04-20 06-24 07-12 08-23 09-10 11-25 13-14 15-18 16-17 21-26	V F L K
01	B	Gamma III IV VII	X B A I	01-24 02-06 03-26 05-25 08-16 10-20 11-22 13-19 14-15 18-21	A Q O J

Enigma Rotor

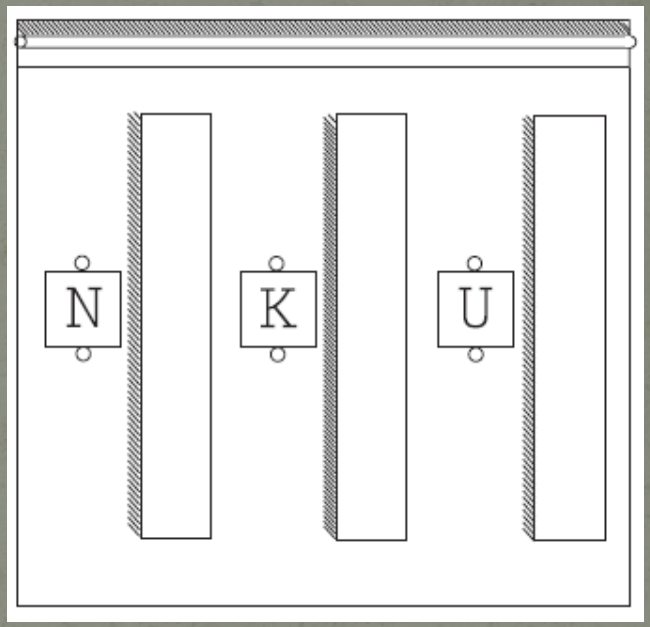
The Key

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

Enigma Rotors



Setting the Rotors



The Key

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

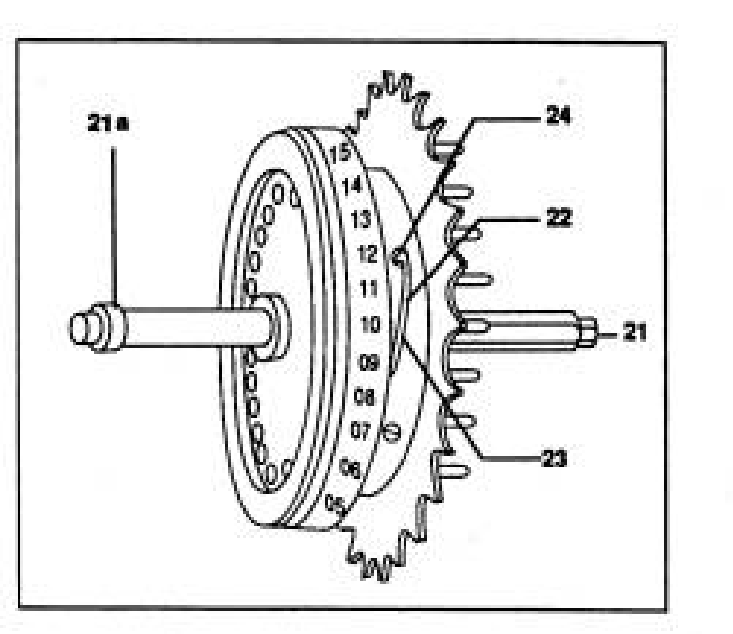
The Plugboard

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.

The Key

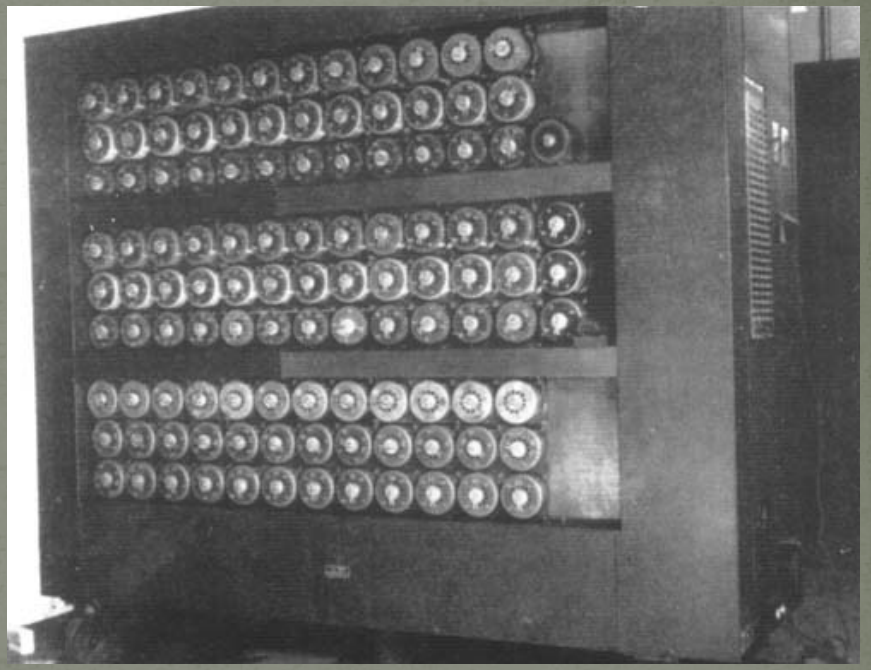
- 6 ways to order the rotors.
- 17576 ways to select the rotor setting.
- 100,391,791,500 ways to set the plugboard.
- 676 ways to set the turnover notches.
- 7,156,755,732,750,624,000 ways to set the key.

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

Brute Force Attack

Would take 22,693,900,000 years.

The Turing Bombe



Cribs

CIPHERTEXT

VWHCD IUGHL UVFAO BNEWN AGZWY ZUXNN
PYZWN LKMUO FRIIL OJPAE

Plaintext

markworthxattackedxbyxtwoxpursuitxplanes

Crib Placement

```
VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
markworthxattackedxbyxtwoxpurs

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
 markworthxattackedxbyxtwoxpurs

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
  markworthxattackedxbyxtwoxpurs
```

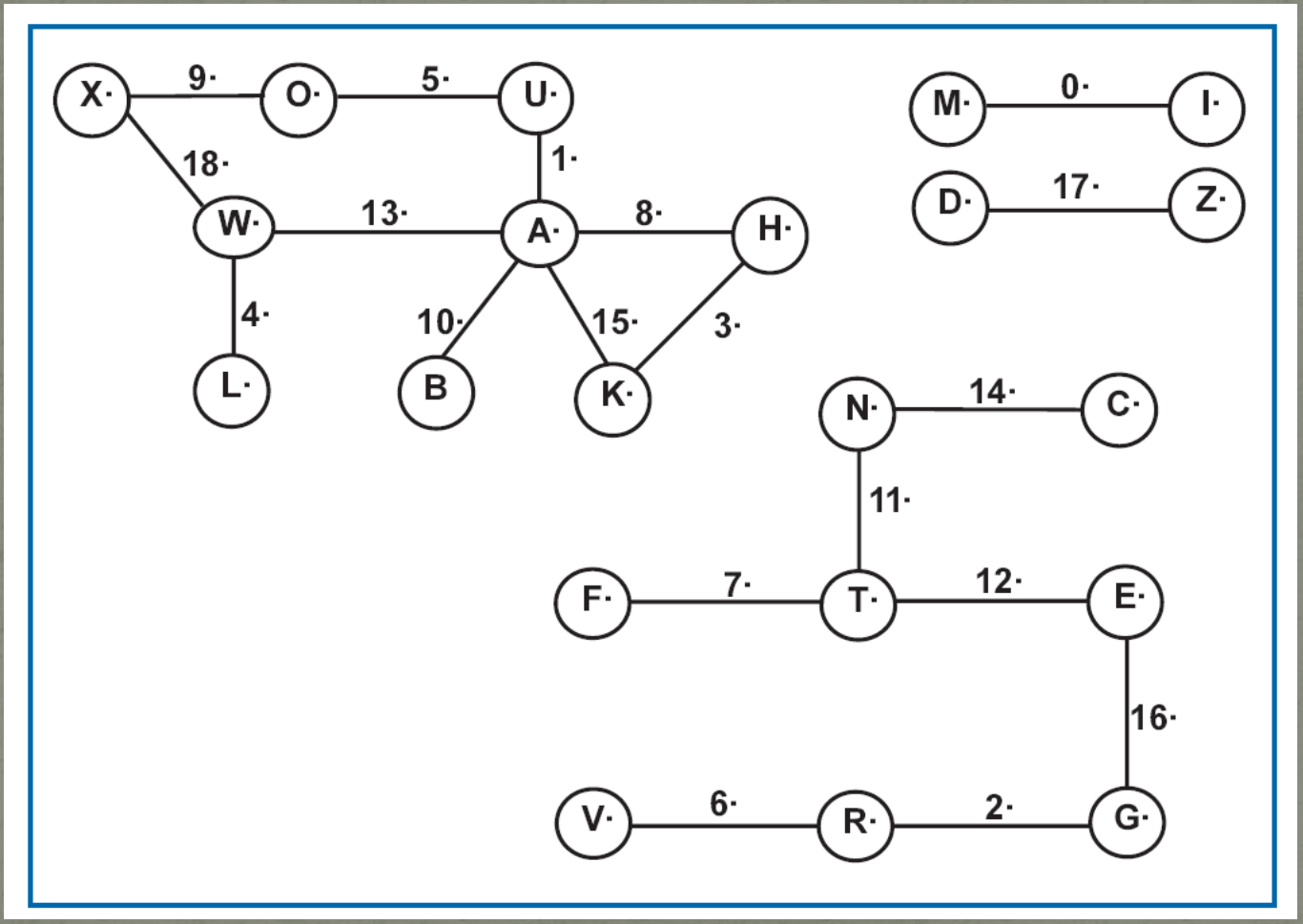
Crib Placement

```
VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
   markworthxattackedxbyxtwoxpur

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
    markworthxattackedxbyxtwoxpu

VWHCDIUGHLUVFAOBNEWNAGZWYZUXNN
     markworthxattackedxbyxtwoxp
```

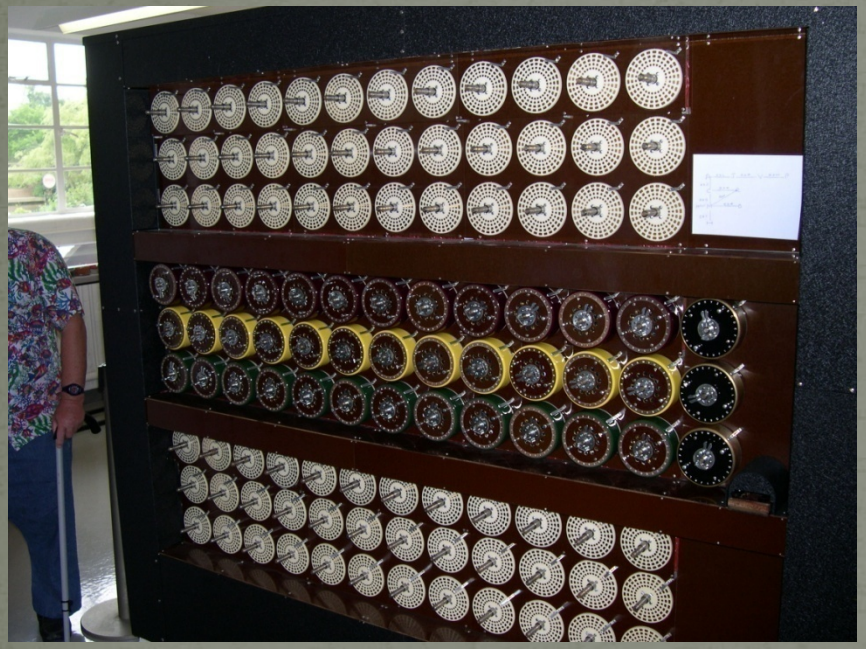
Crib Placement

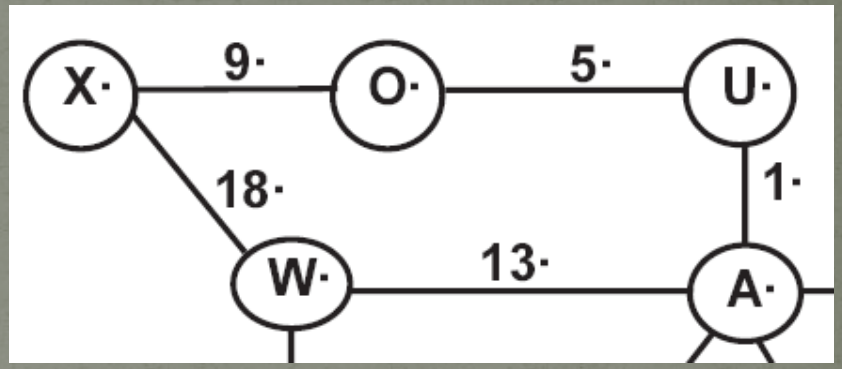
Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X

Diagram



Offsets



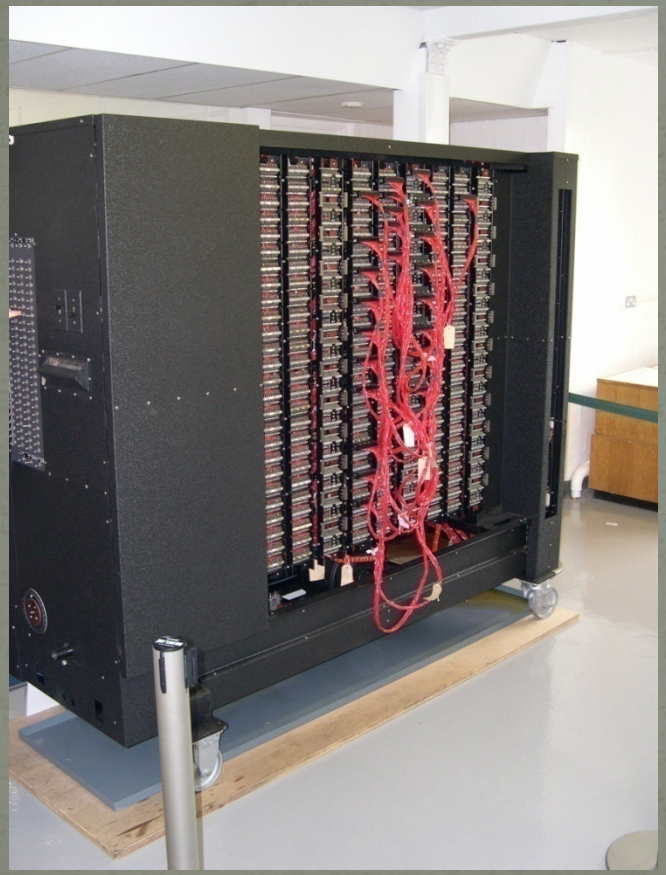


Position:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Cipher:	I	U	G	H	L	U	V	F	A	O	B	N	E	W	N	A	G	Z	W
Crib:	M	A	R	K	W	O	R	T	H	X	A	T	T	A	C	K	E	D	X

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

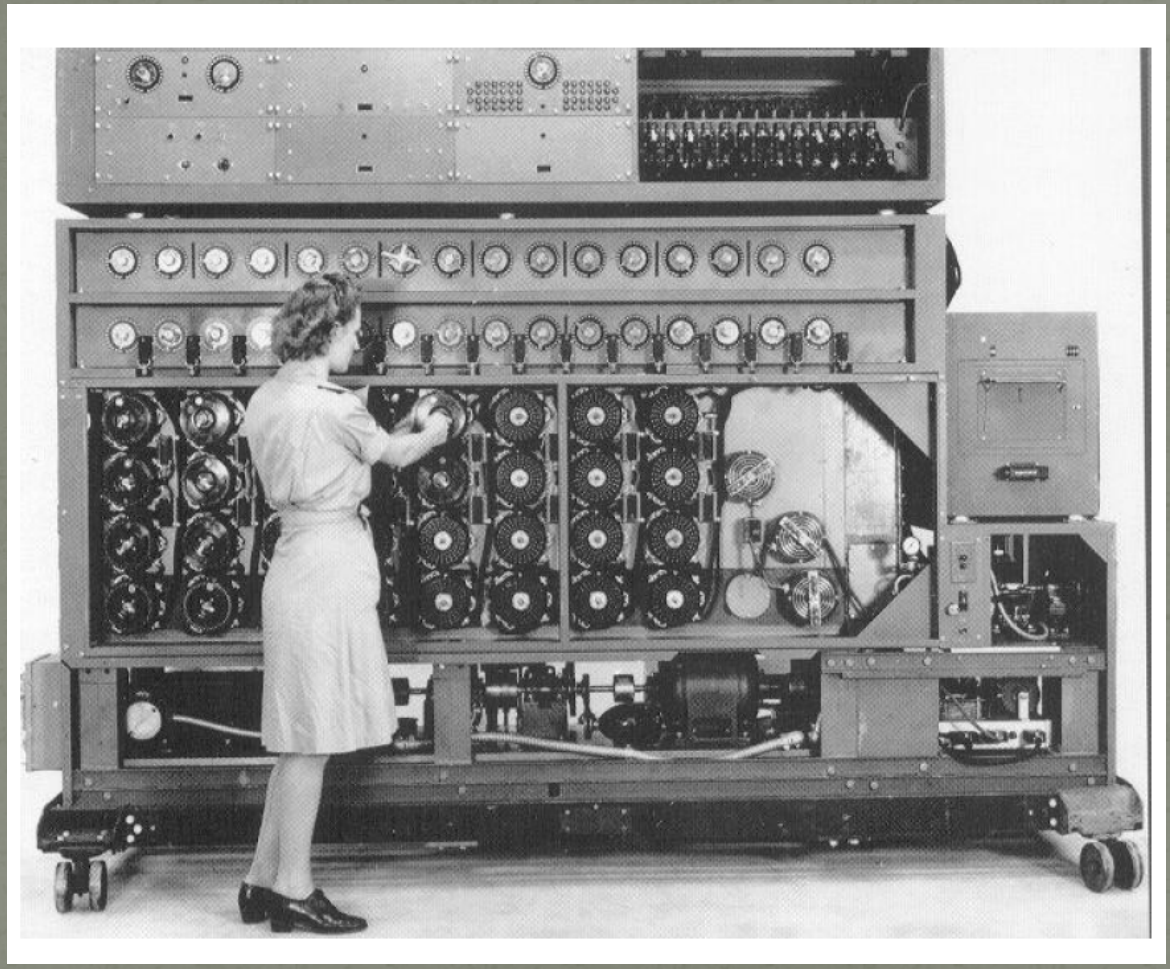


Switch Bank	Switch In	Switch Out	Wheel Settings 1	2	3	4
1	20	0	0	0	0	0
2	6	17	0	0	0	1
3	10	7	0	0	0	2
4	14	20	0	0	0	4
5	17	21	0	0	0	5
6	19	5	0	0	0	6
7	7	0	0	0	0	7
8	23	14	0	0	0	8
9	0	2	0	0	0	9
10	19	13	0	0	0	10
11	19	4	0	0	0	11
12	0	2	0	0	0	12
13	2	13	0	0	0	13
14	10	0	0	0	0	14
15	4	6	0	0	0	15
16	23	22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

February 1942

The Four-Rotor Naval Enigma

US Navy Cryptologic Bombe



NCML

Joseph Desch (1907 – 1987)

2011 Inductee

HALL OF HONOR
These Were the Giants

JOSEPH DESCH