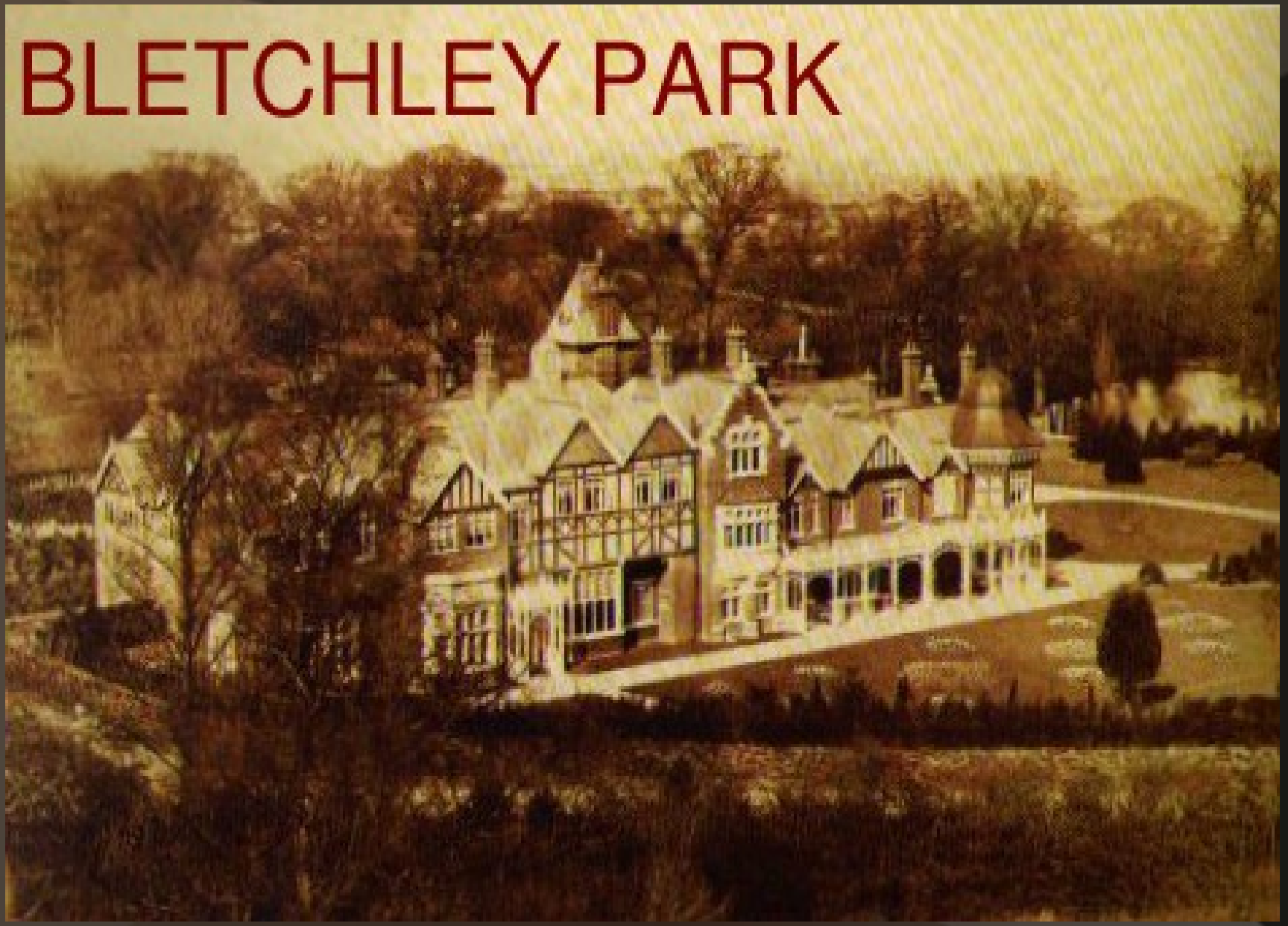
BLETCHLEY PARK



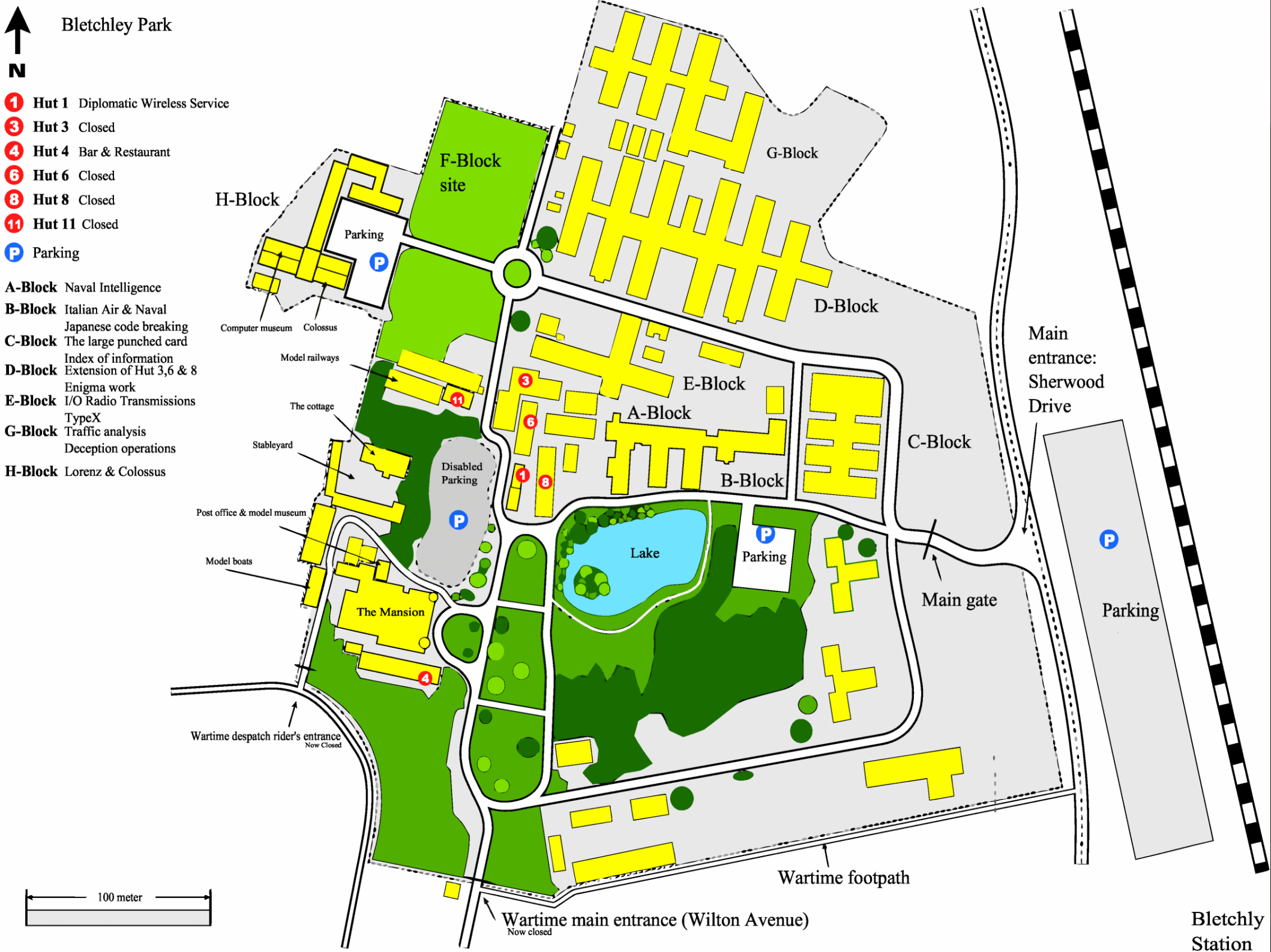
General, later President, Eisenhower
said after the war:

"The intelligence... from you (Bletchley Park)... has been of priceless value. It has saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually forced to surrender... (It was a) very decisive contribution to the Allied war effort."

A war costing around 10 million lives a year and which Bletchley Park's Lorenz decrypts played a significant role in ending.

Bletchley Park Facts

- Sir Hugh Sinclair, Director of Naval Intelligence and Head of MI6, bought the property in 1938.
- The 581 acre estate was centrally located among Cambridge, London, and Oxford and easily accessible by rail.
- A total of 12,000 people worked at Bletchley (80% being women); peak work force was 9,000 in 1945.
- No details about its purpose or its operation were available until 1970!


Bletchley Park
N
1 Hut 1 Diplomatic Wireless Service
3 Hut 3 Closed
4 Hut 4 Bar & Restaurant
6 Hut 6 Closed
8 Hut 8 Closed
11 Hut 11 Closed
P Parking
A-Block Naval Intelligence
B-Block Italian Air & Naval
Japanese code breaking
C-Block The large punched card
Index of information
D-Block Extension of Hut 3,6 & 8
Enigma work
E-Block I/O Radio Transmissions
TypeX
G-Block Traffic analysis
Deception operations
H-Block Lorenz & Colossus
F-Block site
G-Block
H-Block
Parking
D-Block
Computer museum
Colossus
Model railways
E-Block
A-Block
B-Block
C-Block
The cottage
Stableyard
Disabled Parking
Post office & model museum
Model boats
Lake
Parking
Main entrance: Sherwood Drive
Main gate
The Mansion
Parking
Wartime despatch rider's entrance
Now Closed
Wartime footpath
100 meter
Wartime main entrance (Wilton Avenue)
Now closed
Bletchly Station

HUT 8

home to
many code breakers
And
Alan Turing's office

HUT 11

housed Bombe machines

BLOCK H

housed Colossus machines
now National Museum of Computing

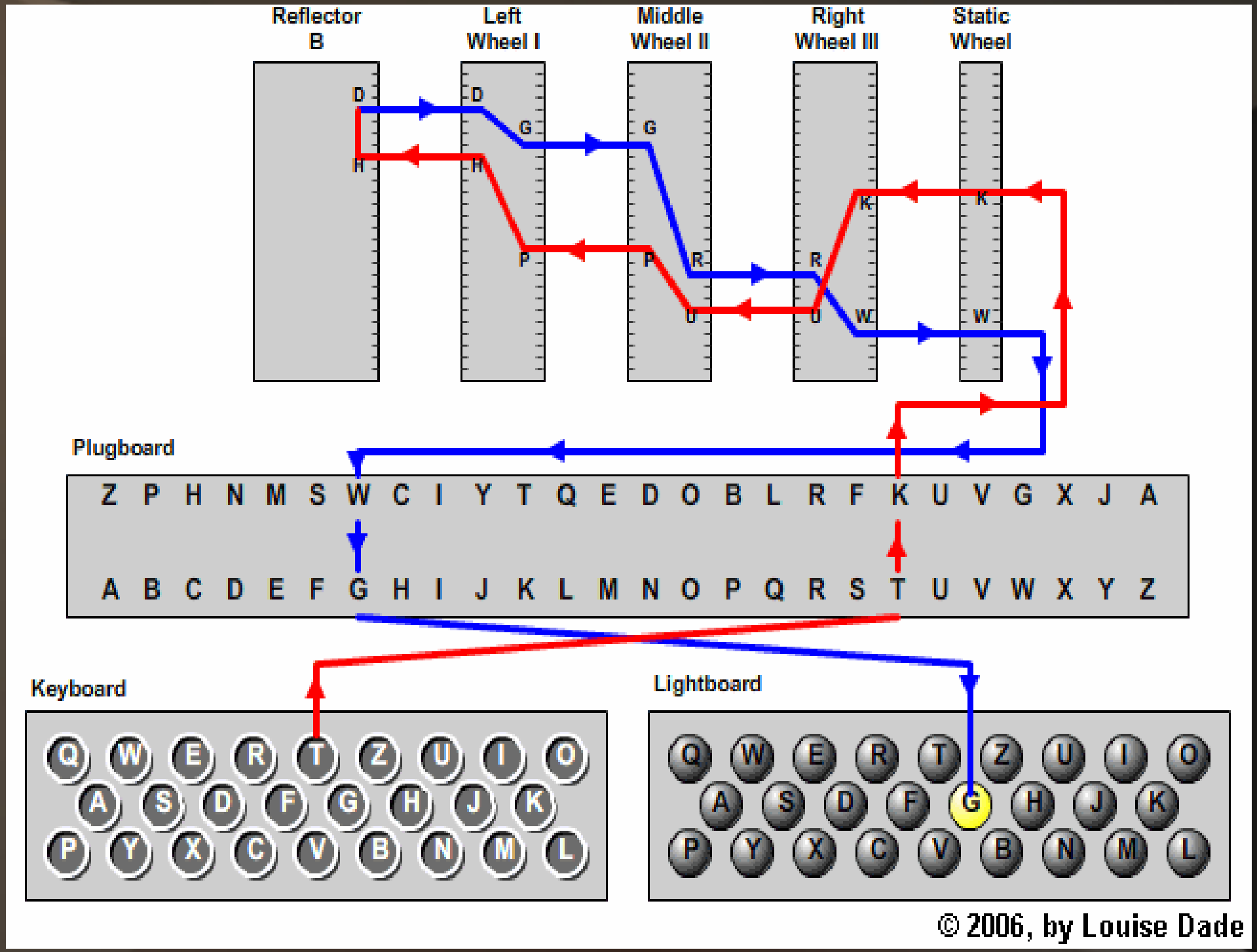
Overview of Communication

- Front Line
  - highly portable => wireless
  - utilized Morse Code
- High Command
  - stationary => wired (if possible)
  - required greater security / greater speed
  - utilized teletype (Baudot Code) and paper tape!

Front Line: The ENIGMA Machine

DESIGN: The ENIGMA Machine

- three **alphabetic** permutation **rotors**
  - selected from five possible rotors
  - rotors possibly advanced after each letter encryption
- **reflector** permutation **rotor**
  - returned signal back through the rotors
- **keyboard** (input) and **light panel** (output)
- ***Military Only***: ten switch plugs
  - to interchange ten pairs of letters at both input/output


Reflector B
Left Wheel I
Middle Wheel II
Right Wheel III
Static Wheel
D
H
D
G
P
G
P
R
U
R
K
U
W
K
W
Plugboard
Z P H N M S W C I Y T Q E D O B L R F K U V G X J 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
Keyboard
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
Lightboard
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
© 2006, by Louise Dade

Total Number of Settings to Analyze

Rotors: C(5,3) = 5x4x3 = 60

Start Positions: 26^3 = 17,576

Step Positions: 26^2 = 676

Plugs: $\frac{C(26,20)}{10!\ 2^{10}} = \frac{26x25x24x...x7}{10!\ 2^{10}}$

= 150,738,274,937,250

Total: 158,962,555,217,826,360,000

≈ 159 quintillion

Initial Work by Polish Mathematicians

- three Poznań University students figured out the configuration for the alphabetic permutation rotors
  - Rajewski, Zygalski, and Rozycki
- the three were seriously hampered in their work by the German upgrading of the security on the Enigma
  - increased the number of alphabetic permutation rotors from three to five
- the Polish mathematicians shared their work with Britain and France prior to the German invasion of Poland

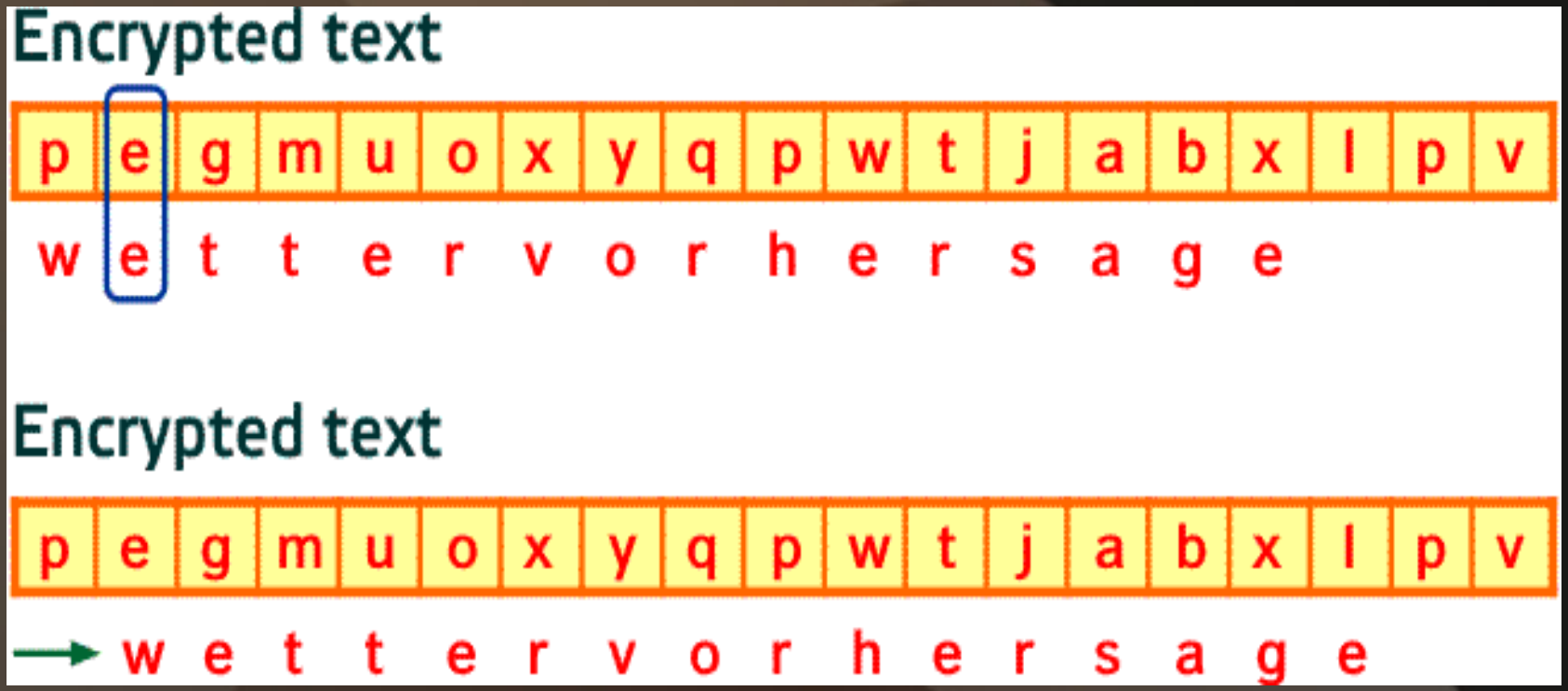
British Insights

- The Achille's heel of the Enigma machine was its reflector permutation rotor
  - the electric current could not return along the original path
  - hence, the reflector had to change the incoming character to another value
  - hence, the Enigma could not encrypt any letter back to itself!

British Insights (cont'd)

- Key words or phrases often appeared at the beginning or the end of a message
  - "weather report" or "heil Hitler"
- Compare the key words / phrases (called ***cribs***) with the encrypted message to find potential locations
  - if location is correct, then it is mathematically possible to determine all the Enigma settings!

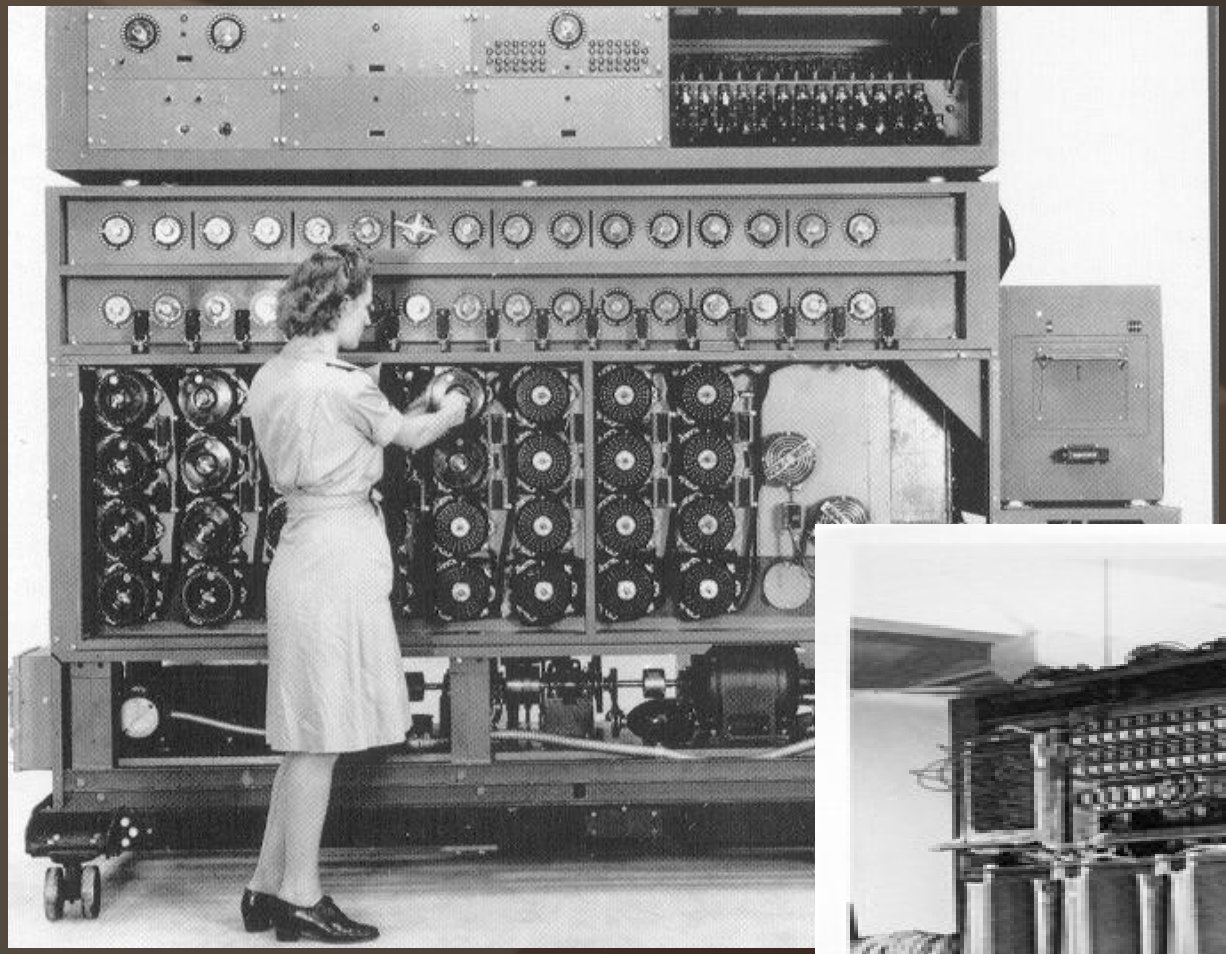
Example of a crib

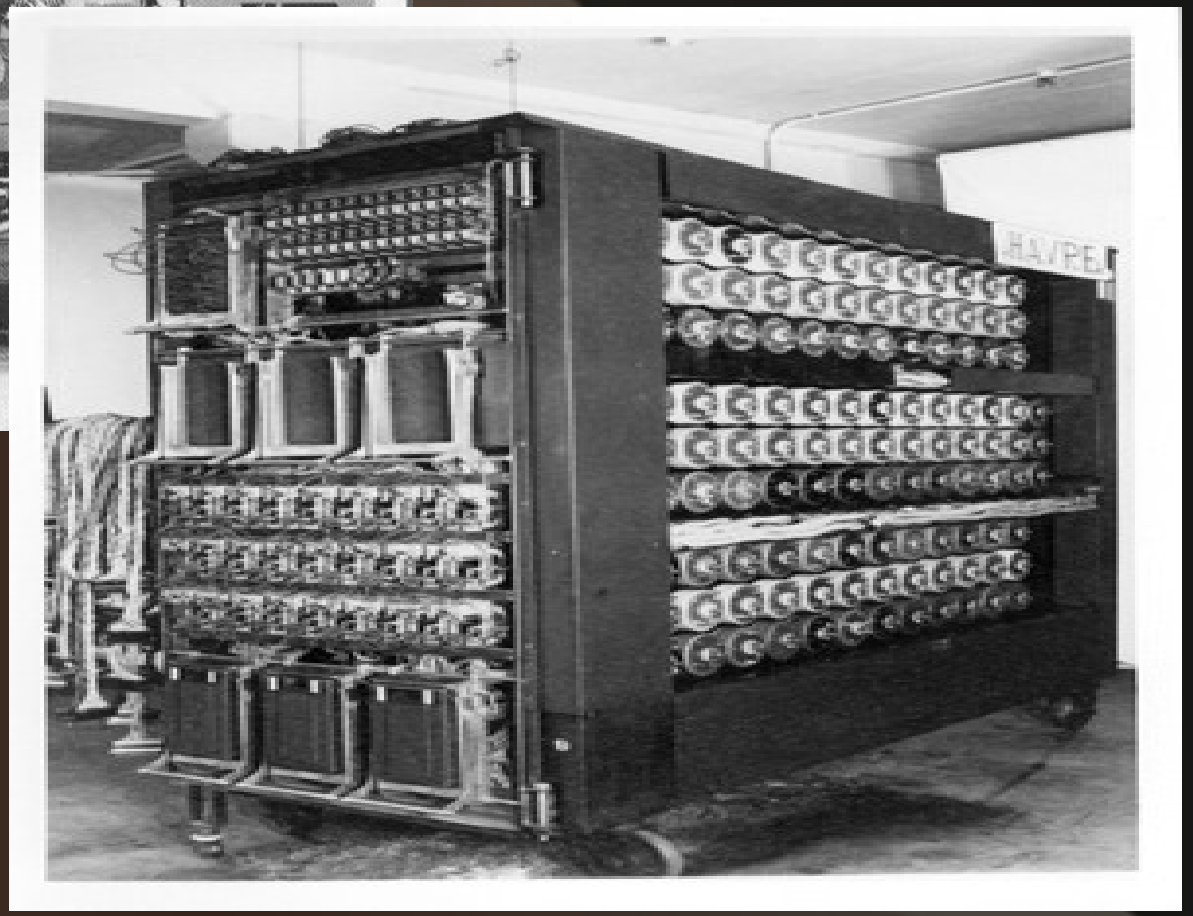


British Insights (cont'd)

- The mathematics necessary to determine the rotor settings was developed by Alan Turing.
- However the process could not be accomplished by human calculation within any reasonable time.
- The process required the use of an electro-mechanical device – called a ***bombe*** – which was also designed by Turing.

bombe





Alan Turing

- father of theoretical computer science and artificial intelligence
  - Turing Machines
  - Entscheidungsproblem
  - Automatic Computing Engine
  - stored program concept
  - Turing Test in Artificial Intelligence

Alan Turing (cont'd)

- Very few people knew of Turing's contributions during the war due to the Official Secrets Act.
- In 1952 Turing was prosecuted for homosexuality and required to undergo chemical castration.
- In 1954 Turing apparently committed suicide using an apple poisoned with cyanide.

Alan Turing (cont'd)

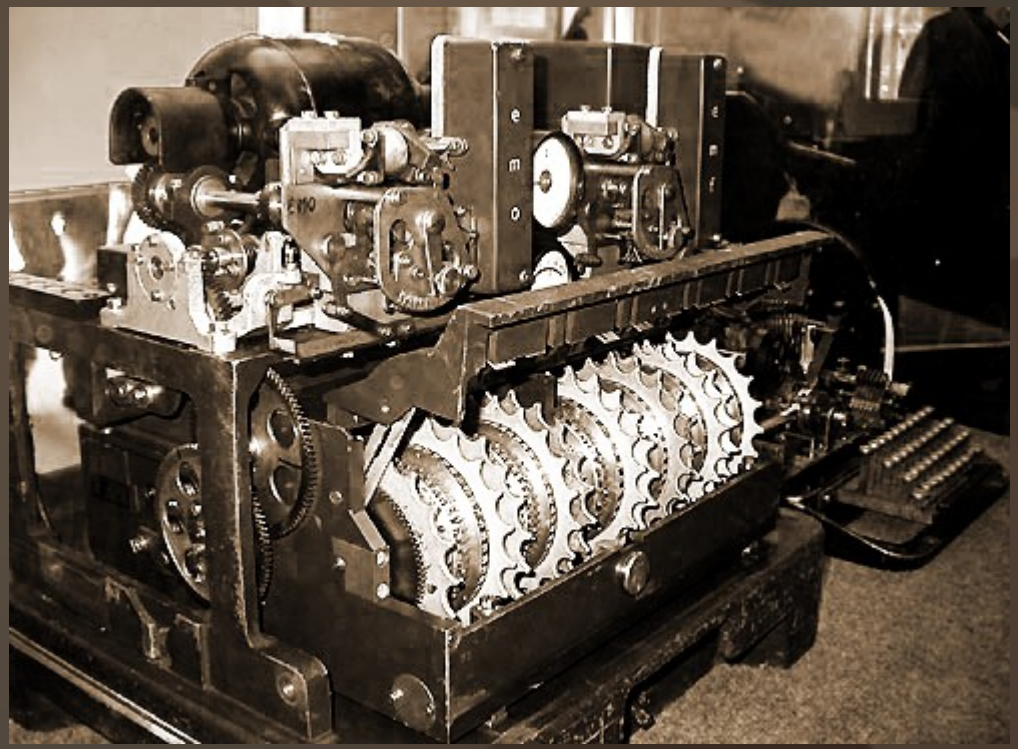
- Very few people knew of Turing's contributions during the war due to the Official Secrets Act.
- In 1952 Turing was prosecuted for homosexuality and required to undergo chemical castration.
- In 1954 Turing apparently committed suicide using an apple poisoned with cyanide.

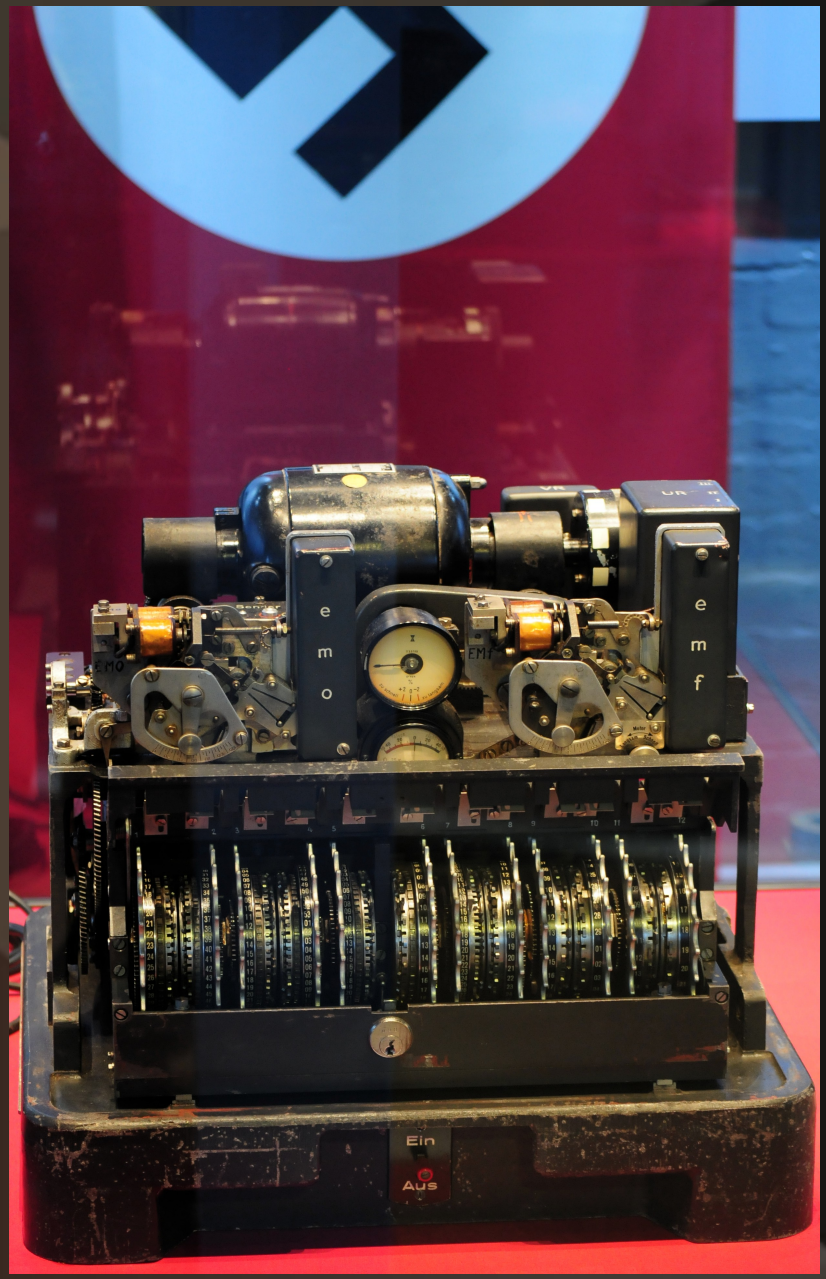
Was this logo intended to honor Alan Turing?
Steve Jobs said: "Not True!"

Alan Turing Epilogue

- In August 2009, a petition was started to request a pardon for Alan Turing. It won an official apology from the prime minister, Gordon Brown, who said the way Turing was persecuted over his homosexuality was "appalling"
- In December 2013, he was granted a posthumous pardon by Queen Elizabeth II.

High Command: The LORENZ Machine



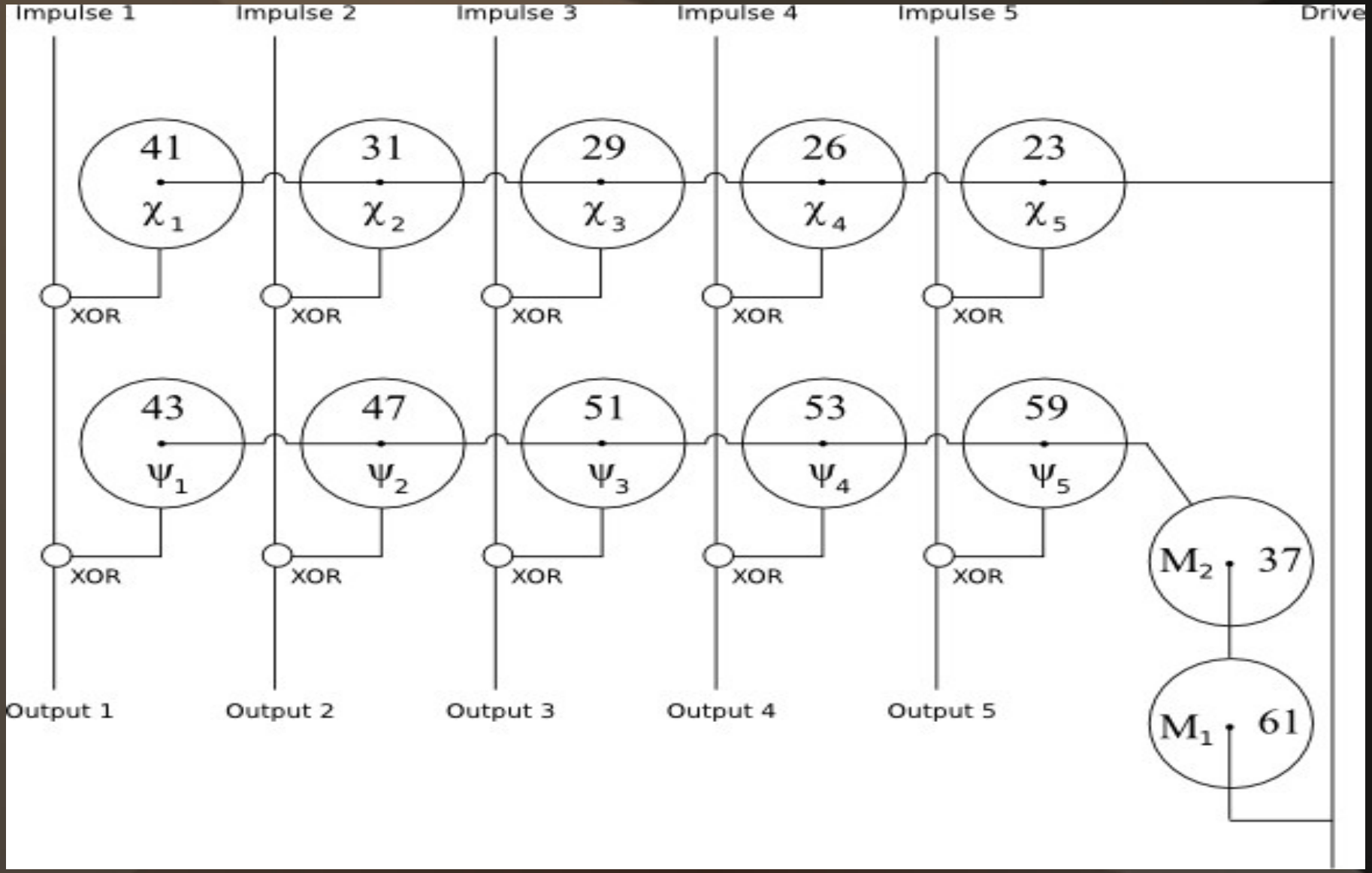


DESIGN: The LORENZ Machine

- Based on the logical operator XOR applied to the 5 bit Baudot code
- 12 wheels
  - 5 χ wheels modified the incoming Baudot character
    - wheels all advance
  - 5 ψ wheels modified the result further
    - wheels might or might not advance
  - 2 μ wheels determine whether or not to advance the ψ wheels

A	*B*	XOR
0	0	0
0	1	1
1	0	1
1	1	0

DESIGN: The LORENZ Machine



DESIGN: The LORENZ Machine

- the number in the wheels on the previous slide indicate the number of pins that can be set 0 or 1
- due to the simplicity of the XOR operator, the decryption process is ***identical*** to the encryption process

Total Number of Settings to Analyze

Wheel Settings: 41 x 31 x … x 61
≈ 1.6 x 10^19

Pin Positions: 2^(41 + 31 + … + 61)
≈ 6.5 x 10^150

Total: 1.05 x 10^170

Bletchley Park Nomenclature

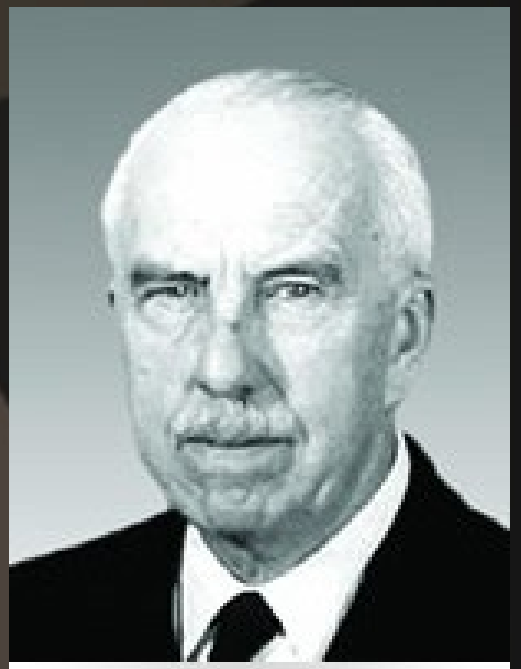
- In Germany, the Lorenz machines were called the ***Schluesselzusatz SZ40/42*** and they were relatively few in number.
- At Bletchley Park, the Lorenz machines were called ***Tunny*** and the encrypted traffic between sites was named for fish:
  - **herring, perch, codfish, bream, ...**

The British Problem

- They knew nothing about the machine! They would have to reverse engineer it!
- For any captured cypher text in the future, they would have to determine:
  - the pin positions for each cam (***wheel breaking***)
  - the starting positions for each cam (**wheel settings**)
- However, the fact that the ψ wheels all moved in unison, but not with every input character, was a major weakness.

John Tiltman

- On August 30, 1941 a message from Athens to Vienna of 4,000 characters had to be resent. The operator incorporated several abbreviations and other modifications, but he used original settings HQIBPEXEZMUG.
- In 10 days time, John Tiltman had decoded the message ***by hand***.



BRIGADIER JOHN TILTMAN

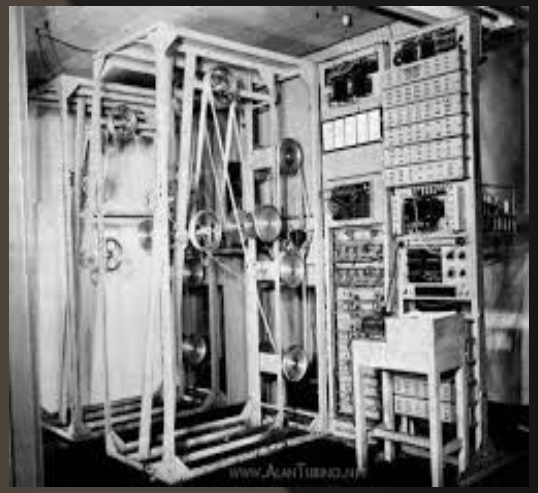
Bill Tutte

- Continued the examination of Tiltman's results using rectangular grids of various column heights (***Kasiski examination***).
  - found height of 41 replete with repetitions and determined $\chi 1$
  - conjectured a second layer $\psi 1$
- With this foothold the entire diagram previously displayed was deduced without ever seeing an actual machine.

Heath Robinson

- NOT Heath Robinson – the famous British cartoonist who envisioned crazy machines.

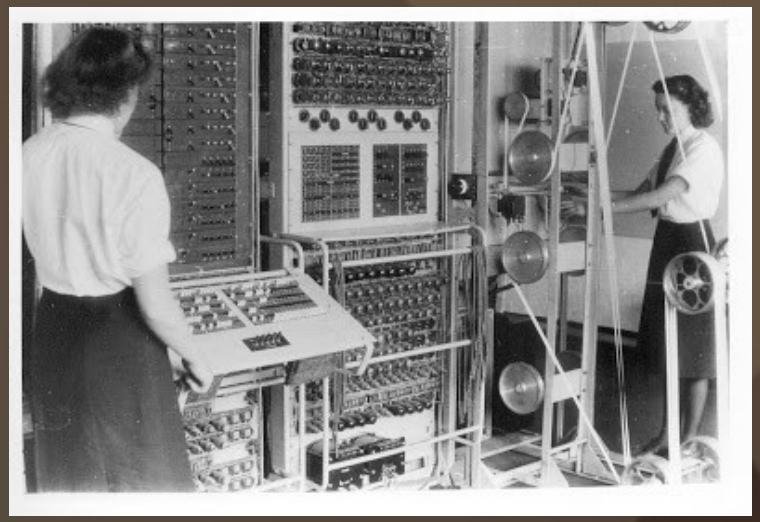
- BUT Heath Robinson – the crazy machine the people at Bletchley built to do wheel breaking and wheel setting.
  - electro-mechanical
  - paper tape input on left

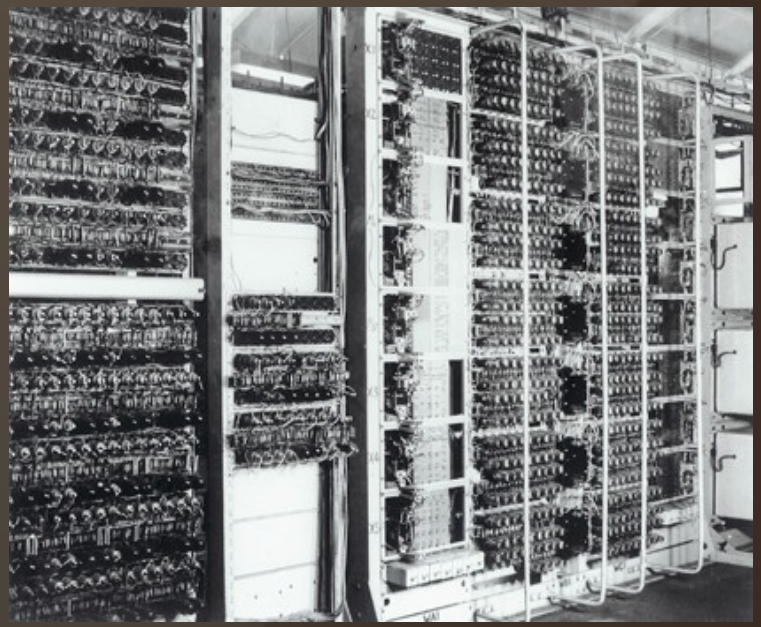


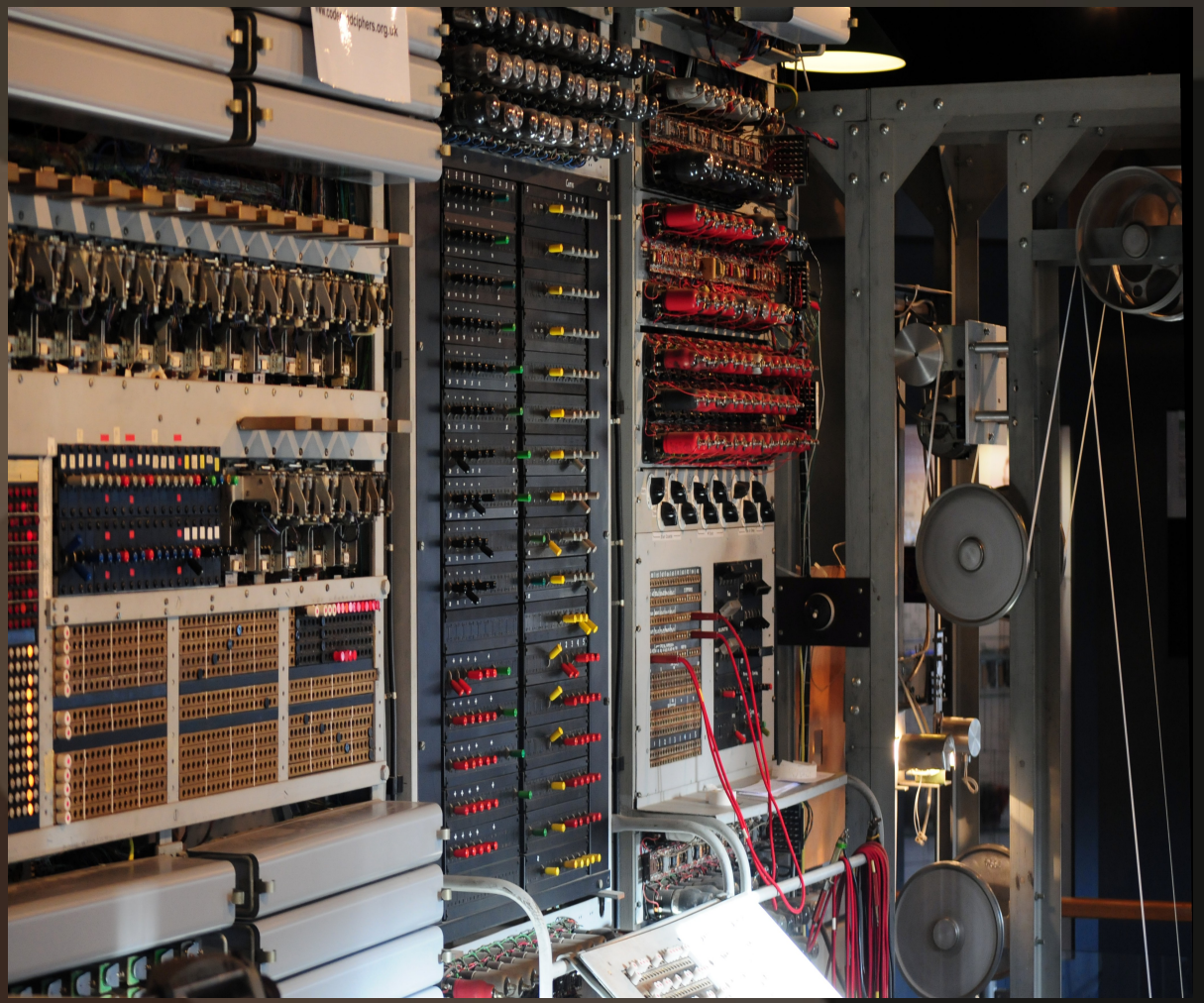
Tommy Flowers

- Tommy Flowers recognized that Heath Robinson would soon be obsolete (too slow).
- The Bletchley Park management merely encouraged Flowers to proceed on his own. He did so, using his personal money.
- He is the designer of Colossus, the world's first electronic digital computer.

Colossus

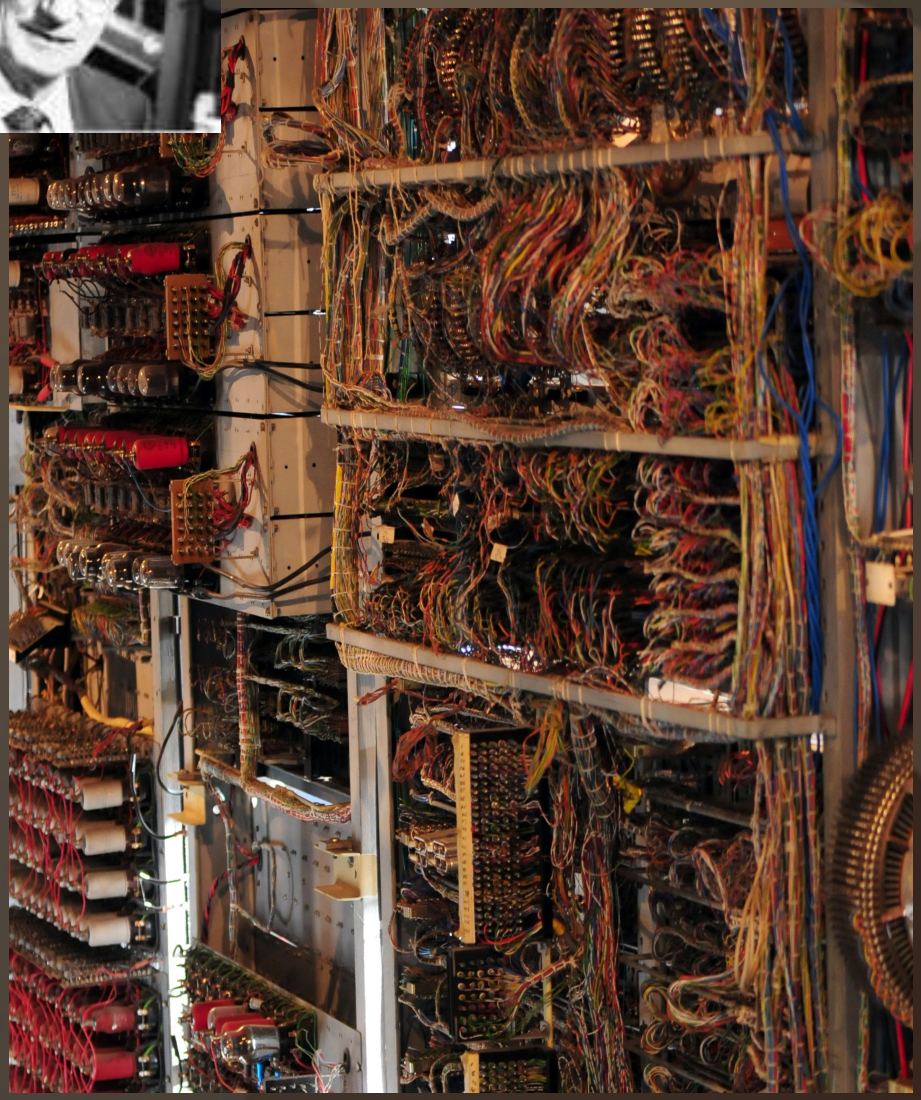






In 1993 Tony Sales and his wife Margaret decided to put their own money into the Colossus Rebuild Project.

Colossus



Interesting Links

ENIGMA

http://www.numberphile.com/videos/enigma.html
http://www.numberphile.com/videos/enigma_flaw.html
http://startpad.googlecode.com/hg/labs/js/enigma/enigma-sim.html

LORENZ

http://www.youtube.com/watch?v=NWYzwIjSk6s
http://www.youtube.com/watch?v=knXWMjIA59c

DOCUMENTARY

http://www.youtube.com/watch?v=OuEHcJ7CCzg

THE END