

Colossus

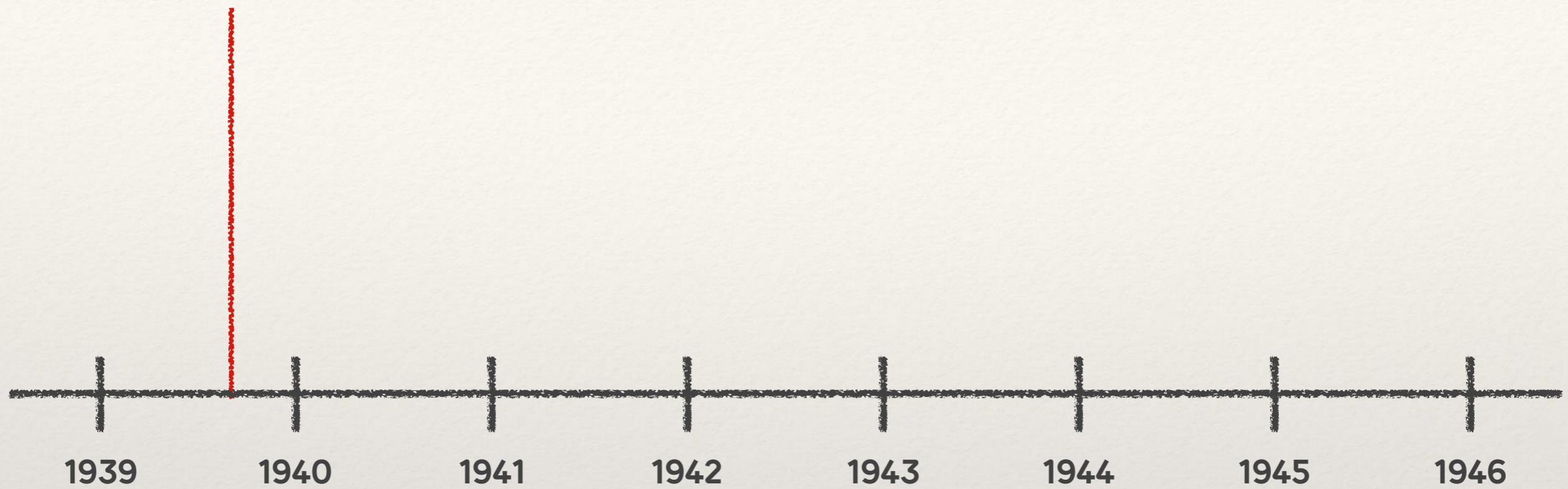
The codebreaking computer
from Bletchley Park





Codebreakers arrive at Bletchley Park

August 1939





Codebreakers arrive at Bletchley Park

August 1939



**Non-morse transmissions
intercepted in Britain**



LORRENZ T32 TELEPRINTER
(Circa 1936)



		KEYS								KEYS					
Letters Figures		V	IV	I	II	III	Letters Figures		V	IV	I	II	III		
A	1			○			P	+	○	○	○	○	○		
B	8		○		○		Q	/	○	○	○	○	○		
C	9	○		○	○		R	-	○	○			○		
D	0		○	○	○	○	S	?	○				○		
E	2			○			T	z	○		○		○		
F	3	○		○	○		U	4			○		○		
G	7	○		○			V	'	○		○	○	○		
H	1	○		○	○		W	?	○		○		○		
I	3/			○	○		X	g	○			○			
J	6		○	○			Y	3					○		
K	(○	○	○			Z	:	○		○	○	○		
L	=	○	○	○	○		-	.	○		○		○		
M)	○	○		○		*	*	○	○				(Erasure)	.
N	£	○	○		○	○	Figure shift & space								
O	5			○	○	○	Letter shift & space		○						
/	1			○	○										

FIG. 22.

BAUDÔT SIGNALLING CODE OR ALPHABET (BRITISH).

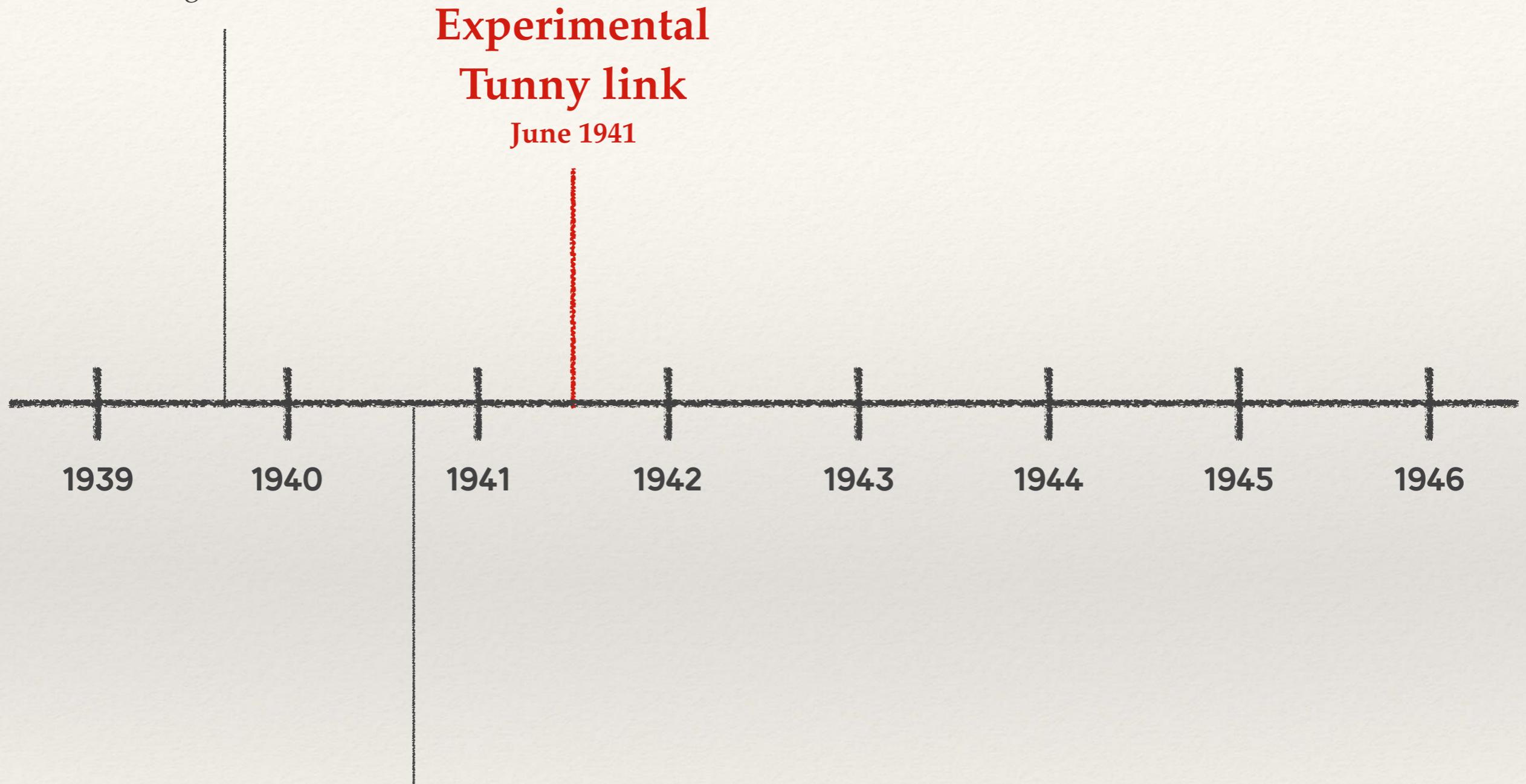


The background of the image is a dense, swirling school of small, silvery fish, likely sardines or anchovies, swimming in a clear, light blue ocean. The fish are oriented horizontally, creating a sense of movement and depth.

Tunny Sturgeon Thrasher

Codebreakers arrive at Bletchley Park

August 1939

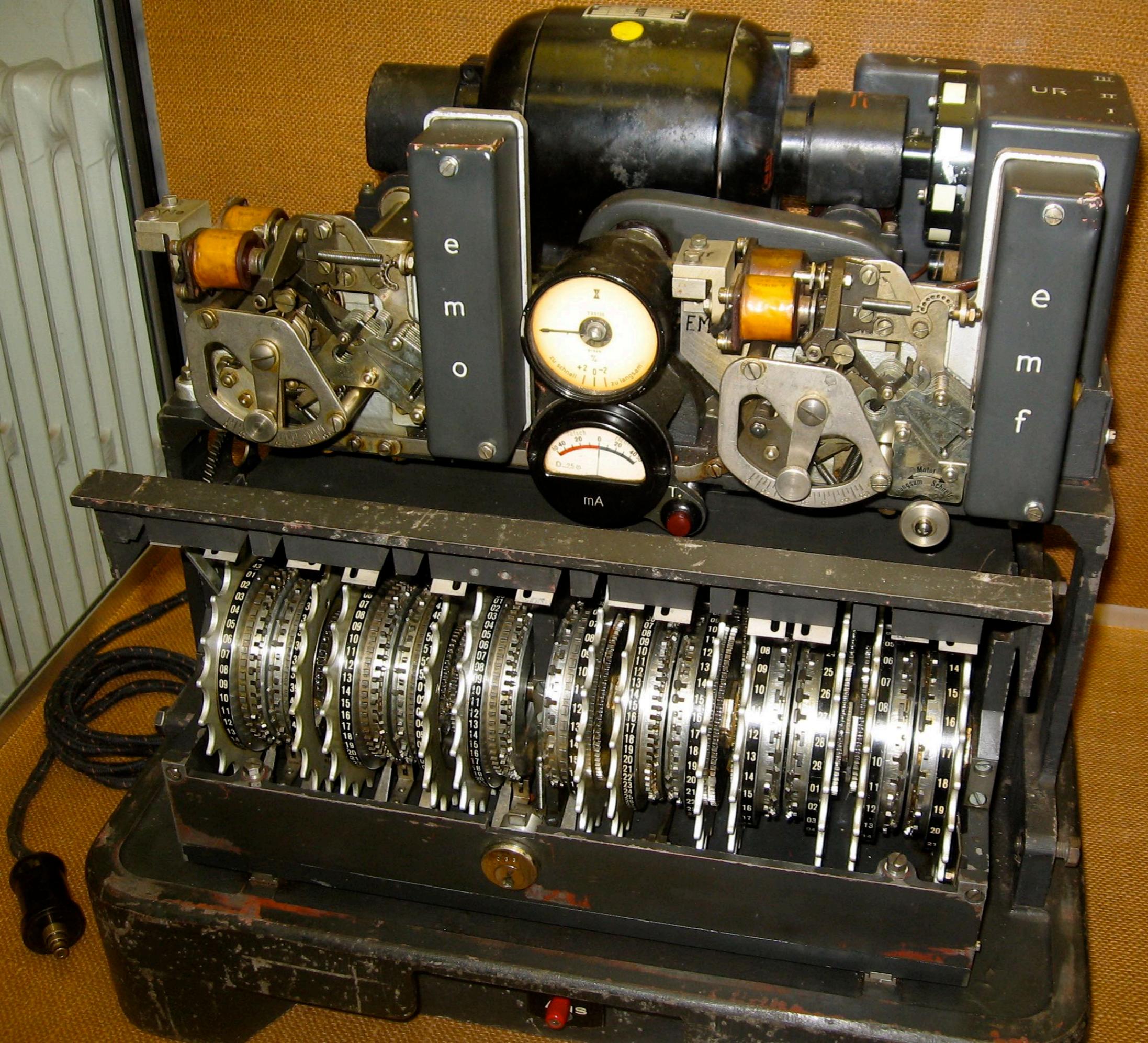


Late 1940

Non-morse transmissions
intercepted in Britain

**Experimental
Tunny link**

June 1941



message

S

.

.

X

.

X

message

S

. . X . X

key

K

X . . X X

message

S

.

.

X

.

X

key

K

X

.

X

X

ciphertext

C

X

.

X

X

.

message

S

. . X . X

key

K

X . . X X

ciphertext

C

X . X X .

key

K

X . . X X

message

S

. . X . X

key

K

X . . X X

ciphertext

C

X . X X .

key

K

X . . X X

message

S

. . X . X

message

S

. . X . X

key

K

X . . X X

ciphertext

C

X . X X .

key

K

X . . X X

message

S

. . X . X

message

S

0 0 1 0 1

key

K

1 0 0 1 1

ciphertext

C

1 0 1 1 0

key

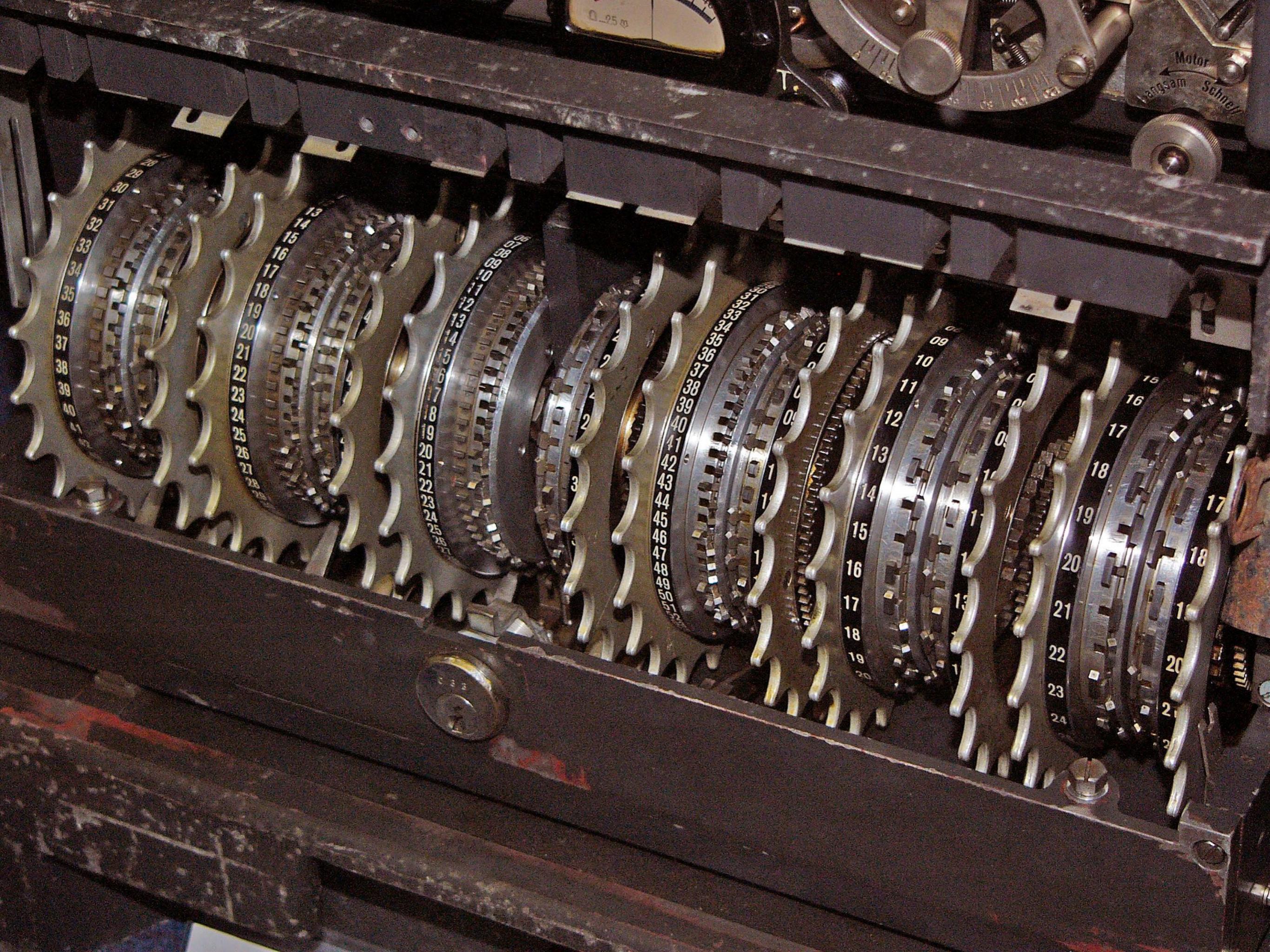
K

1 0 0 1 1

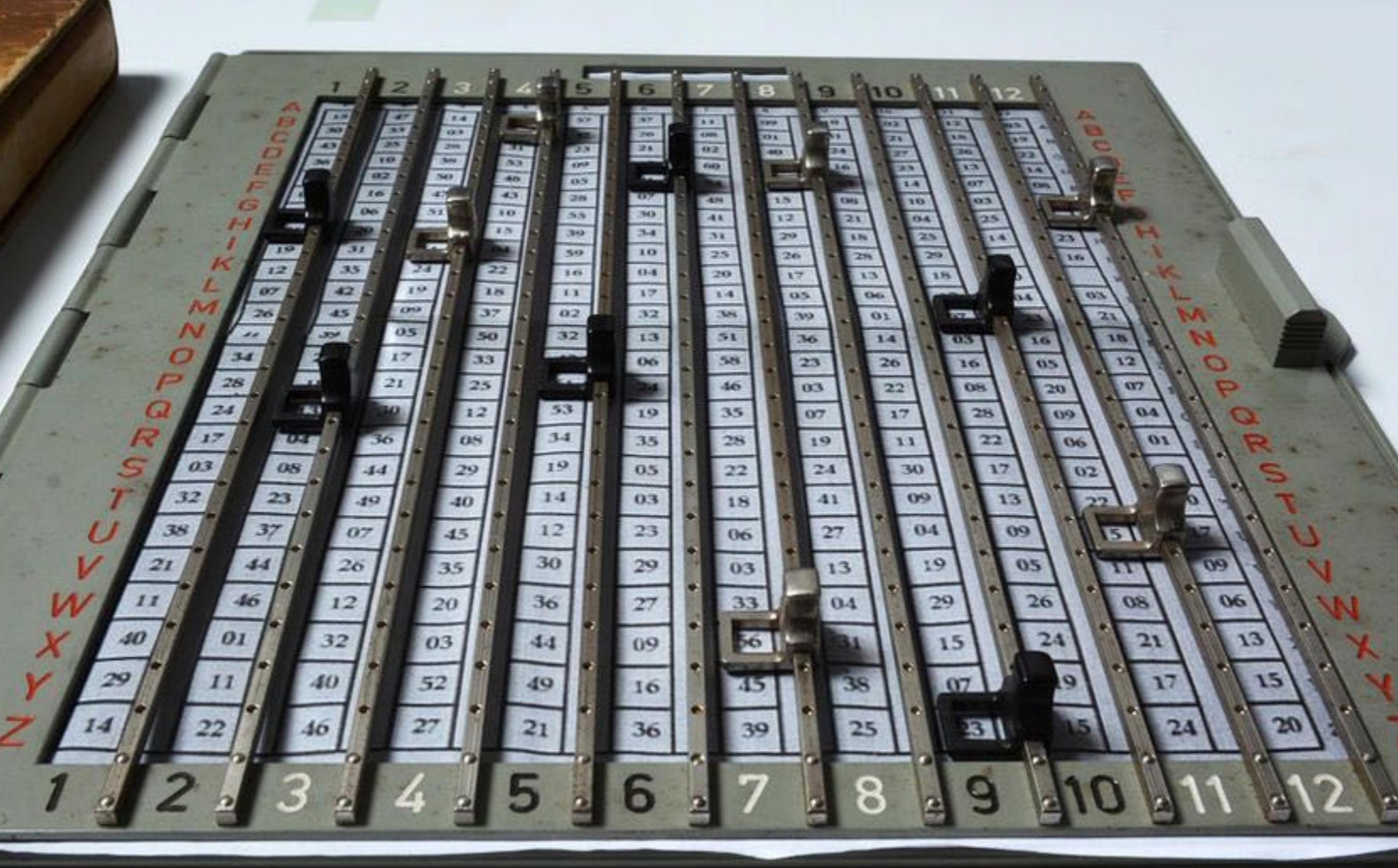
message

S

0 0 1 0 1







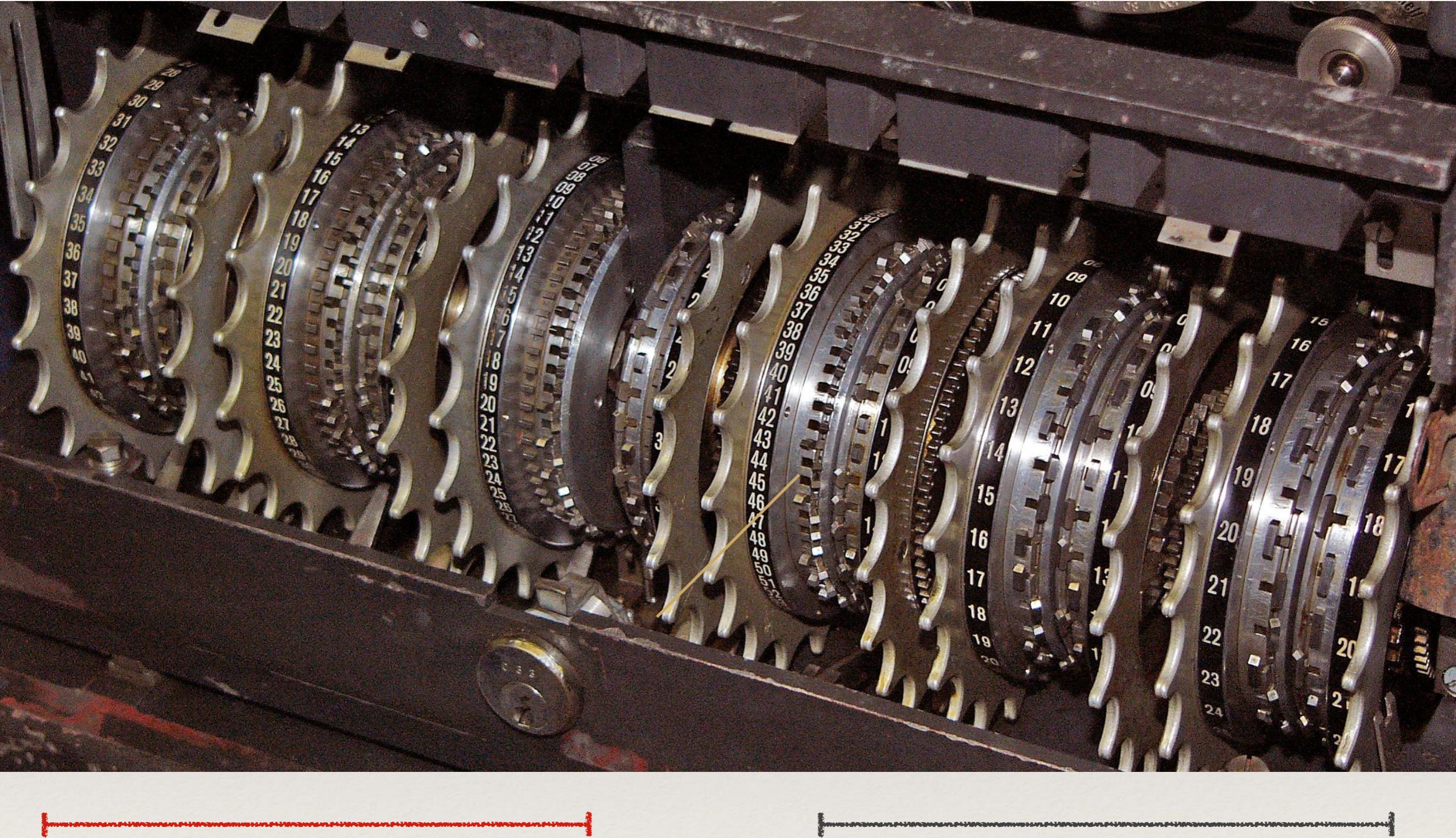
M	26	45	69	37	62
N	22	39	65	50	32
O	34	51	17	33	13
P	28	41	21	25	66
Q	24	38	50	12	24
R	17	64	36	68	19
S	03	68	44	29	35
T	32	23	49	40	05
U	38	37	67	45	19
V	21	44	26	14	03
W	11	46	12	23	29
X	40	01	32	30	27
Y	29	11	40	03	09
Z	14	22	46	52	16

1 2 3 4 5 6



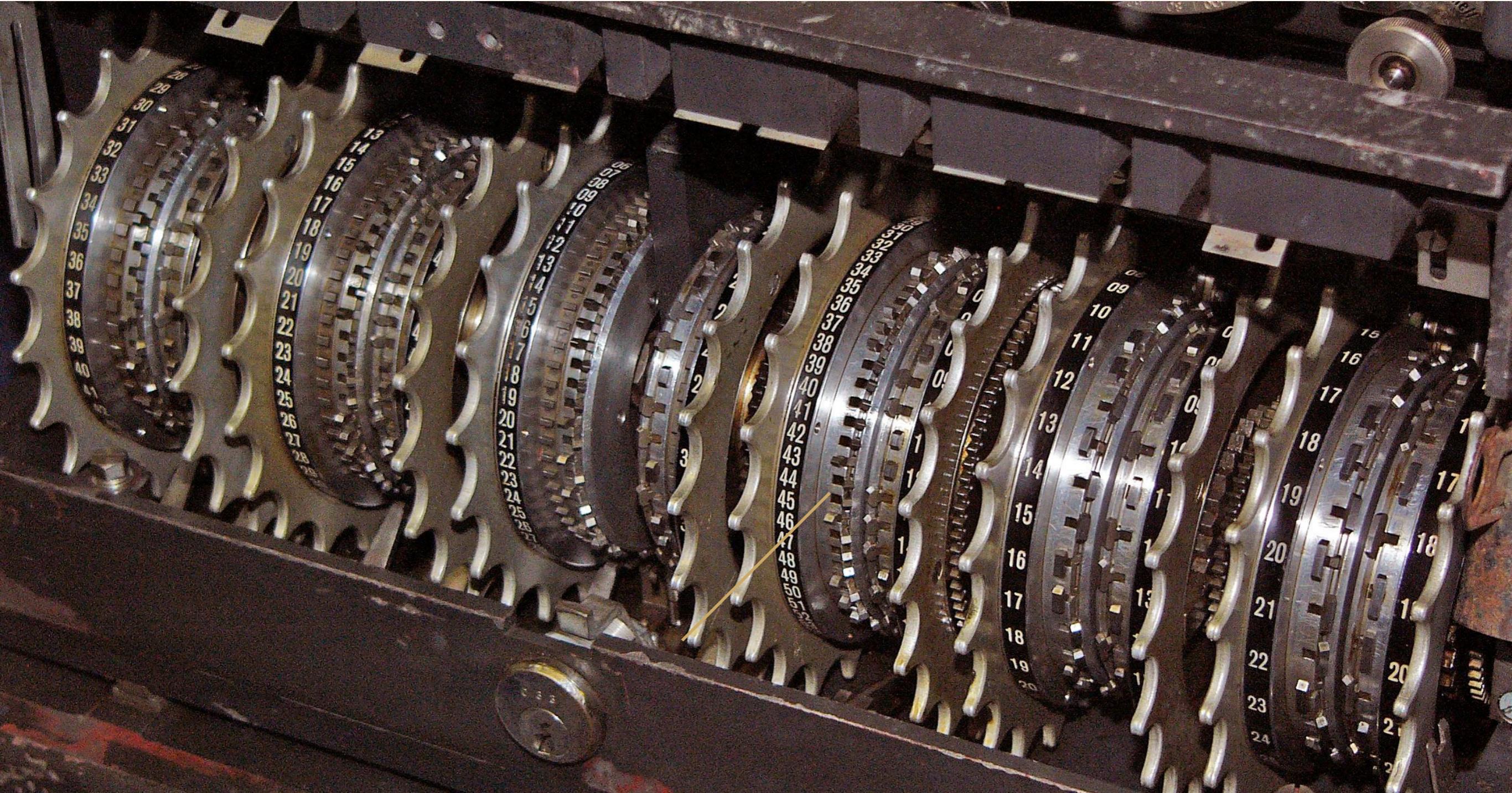


x-wheels



ψ -wheels

χ -wheels



ψ -wheels

μ -wheels

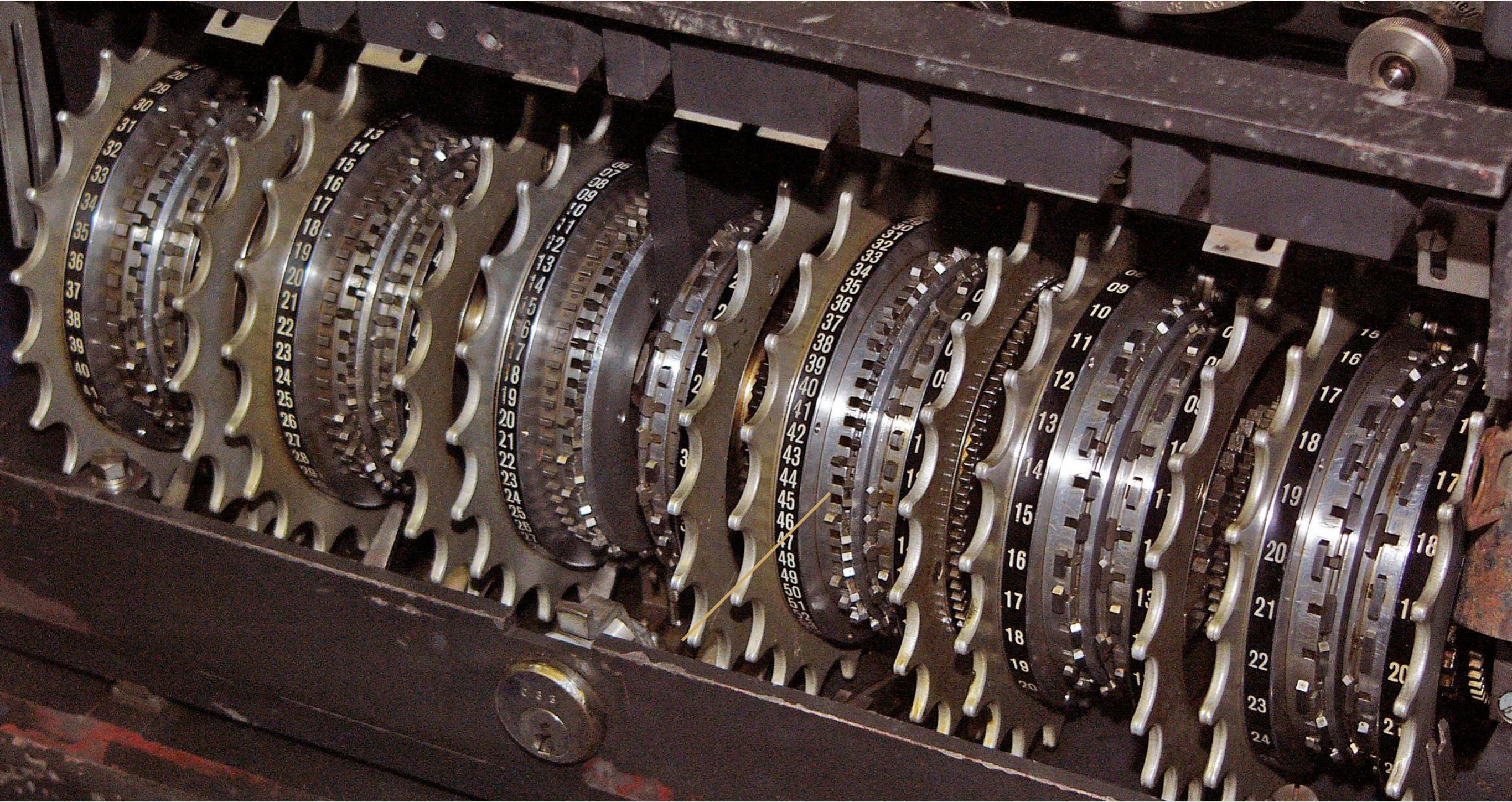
χ -wheels



ψ -wheels

μ -wheels

χ -wheels



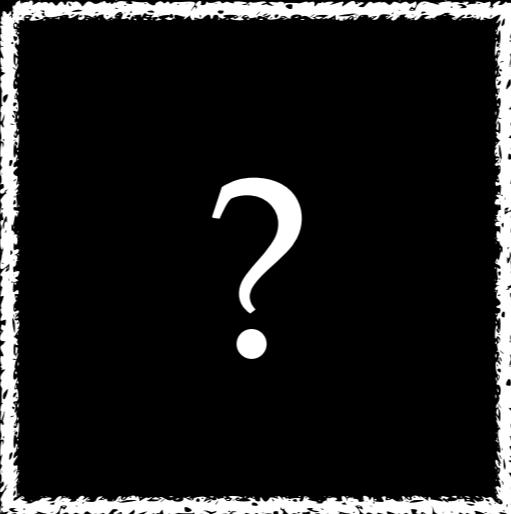
$$\text{key} = \chi\text{-key} + \psi\text{-key}$$

?



$$C_1 = M_1 + K$$

$$C_2 = M_2 + K$$

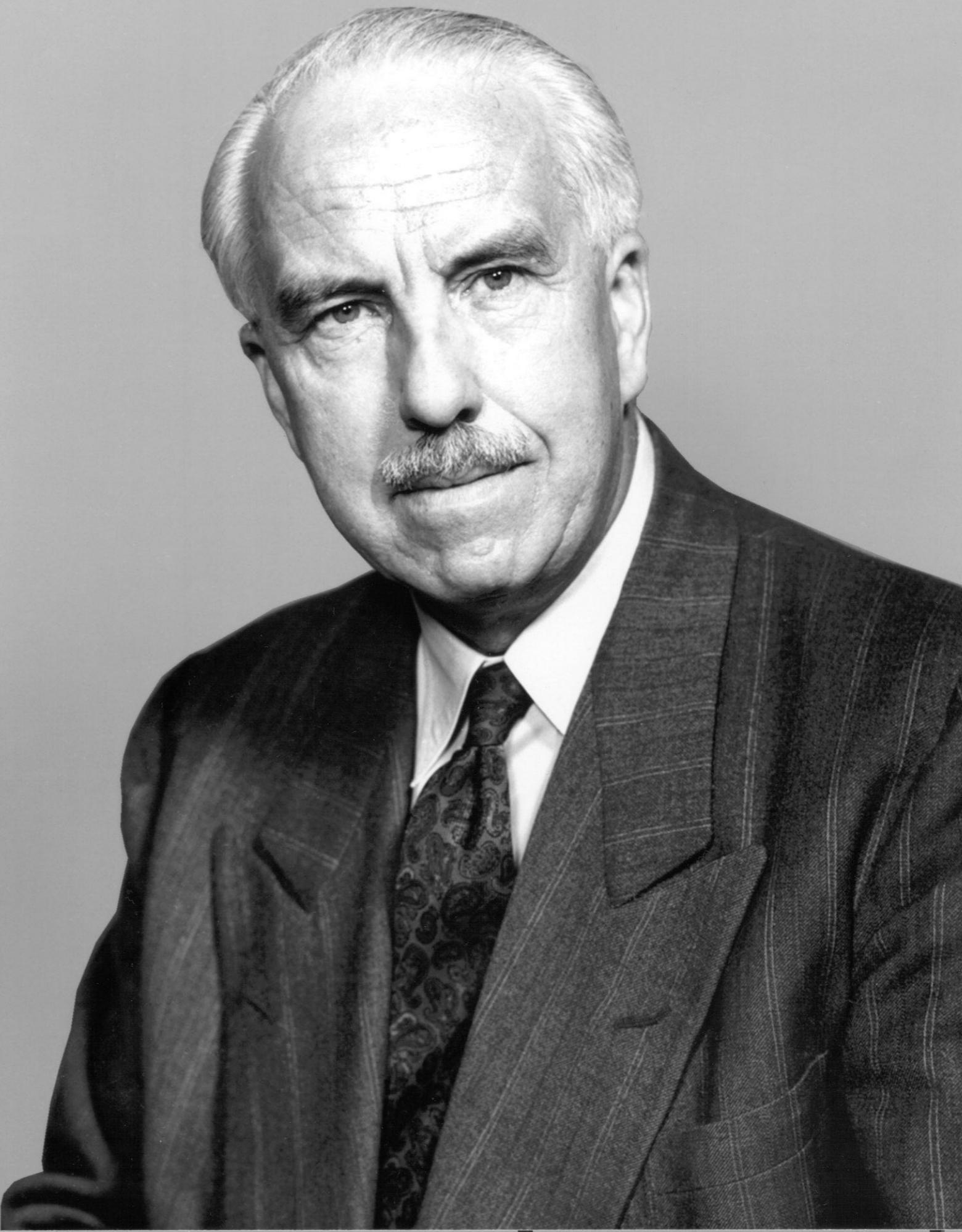


$$C_1 = M_1 + K$$

$$C_2 = M_2 + K$$

$$C_1 + C_2 = M_1 + M_2$$

John Tiltman



Codebreakers arrive at Bletchley Park

August 1939

Experimental
Tunny link

June 1941

1939

1940

1941

1942

1943

1944

1945

1946

August 1941

The German
mistake

Late 1940

Non-morse transmissions
intercepted in Britain

Bill Tutte



“

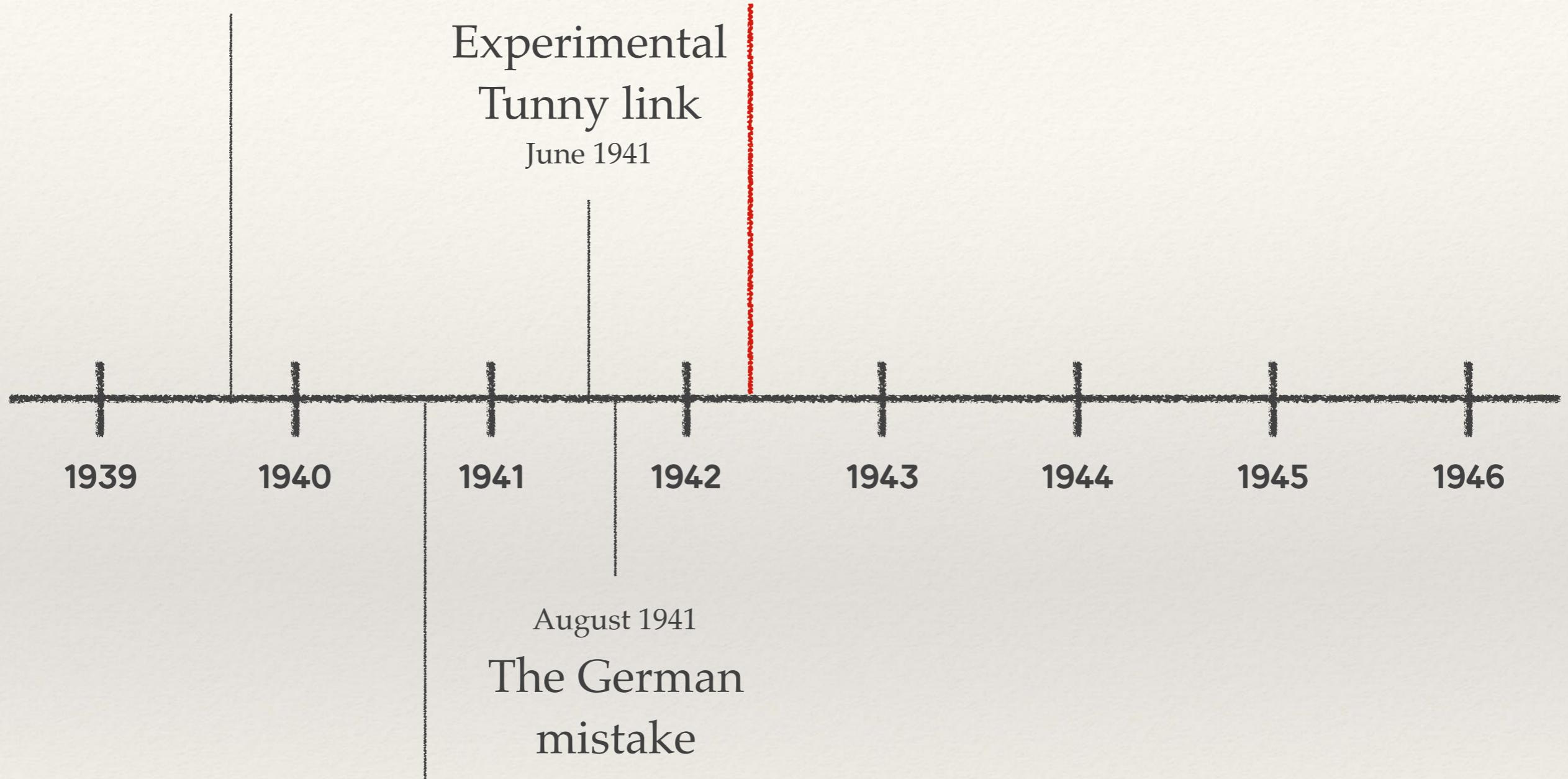
He used to sit staring into the middle distance, twirling a pencil about in his fingers. I used to wonder whether he was getting anything done.

– Jerry Roberts

Codebreakers arrive
at Bletchley Park

August 1939

Complete analysis
of Tunny
January 1942



Non-morse transmissions
intercepted in Britain

Breaking Tunny, a how-to

1. Find the pin settings of the χ -wheels
2. Find the start positions of the χ -wheels
3. Peel off the effect of the χ -wheels
4. Strip off the intermittent ψ -stream

Start positions of the χ -wheels

ciphertext

. X . X X X . X X .

χ -stream

. X . . X X . X X X

Start positions of the χ -wheels

ciphertext

. **X** . X X

X . X X .

χ -stream

. **X** . . X

X . X X X

Start positions of the χ -wheels

ciphertext

. **X** . X X

X . X X .

χ -stream

. **X** . . X

X . X X X

. + X + X + . + . + X + X + . = .

Start positions of the χ -wheels

ciphertext $M_1 + \chi_1 + \psi_1'$ $M_2 + \chi_2 + \psi_2'$

χ -stream 

$. + X + X + . + . + X + X + . = .$

Start positions of the χ -wheels

$$\text{ciphertext} \quad M_1 + \chi_1 + \psi_1' \quad M_2 + \chi_2 + \psi_2'$$

$$\chi\text{-stream} \quad \chi_1 \quad \chi_2$$

$$. + \mathbf{x} + \mathbf{x} + . + . + \mathbf{x} + \mathbf{x} + . = .$$

Start positions of the χ -wheels

$$\text{ciphertext} \quad M_1 + \chi_1 + \psi_1' \quad M_2 + \chi_2 + \psi_2'$$

$$\chi\text{-stream} \quad \chi_1 \quad \chi_2$$

$$(M_1 + \chi_1 + \psi_1') + \chi_1 + (M_2 + \chi_2 + \psi_2') + \chi_2$$

Start positions of the χ -wheels

ciphertext	$M_1 + \chi_1 + \psi_1'$	$M_2 + \chi_2 + \psi_2'$
------------	--------------------------	--------------------------

χ -stream	χ_1	χ_2
----------------	----------	----------

$$(M_1 + \chi_1 + \psi_1') + \chi_1 + (M_2 + \chi_2 + \psi_2') + \chi_2$$

Start positions of the χ -wheels

$$\text{ciphertext} \quad M_1 + \chi_1 + \psi_1' \quad M_2 + \chi_2 + \psi_2'$$

$$\chi\text{-stream} \quad \chi_1 \quad \chi_2$$

$$\begin{aligned} & (M_1 + \cancel{\chi_1} + \psi_1') + \cancel{\chi_1} + (M_2 + \cancel{\chi_2} + \psi_2') + \cancel{\chi_2} \\ &= (M_1 + M_2) + (\psi_1' + \psi_2') \end{aligned}$$

Start positions of the χ -wheels

$$\text{ciphertext} \quad M_1 + \chi_1 + \psi_1' \quad M_2 + \chi_2 + \psi_2'$$

$$\chi\text{-stream} \quad \chi_1 \quad \chi_2$$

$$\begin{aligned} & (M_1 + \cancel{\chi_1} + \psi_1') + \cancel{\chi_1} + (M_2 + \cancel{\chi_2} + \psi_2') + \cancel{\chi_2} \\ &= (M_1 + M_2) + (\psi_1' + \psi_2') \end{aligned}$$

Start positions of the χ -wheels

ciphertext	$M_1 + \chi_1 + \psi_1'$	$M_2 + \chi_2 + \psi_2'$
------------	--------------------------	--------------------------

χ -stream	χ_1	χ_2
----------------	----------	----------

$$\begin{aligned} & (M_1 + \cancel{\chi_1} + \psi_1') + \cancel{\chi_1} + (M_2 + \cancel{\chi_2} + \psi_2') + \cancel{\chi_2} \\ &= (M_1 + M_2) + (\underline{\psi_1'} + \underline{\psi_2'}) \\ &= M_1 + M_2 \end{aligned}$$

Start positions of the χ -wheels

ciphertext

. **X** . X X

X . X X .

χ -stream

. **X** . . X

X . X X X

. + X + X + . + . + X + X + . = .

Max Newman

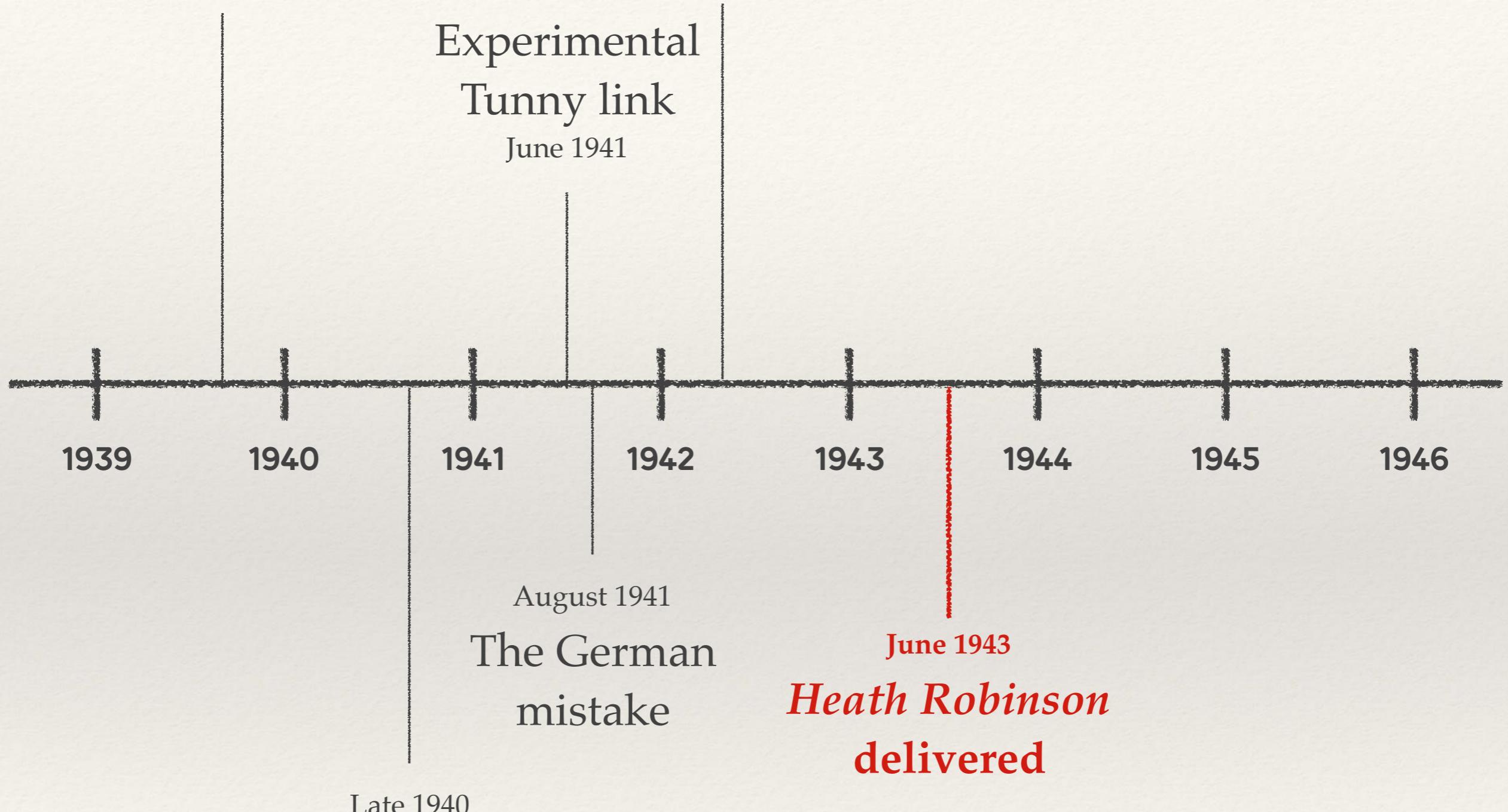


Codebreakers arrive
at Bletchley Park

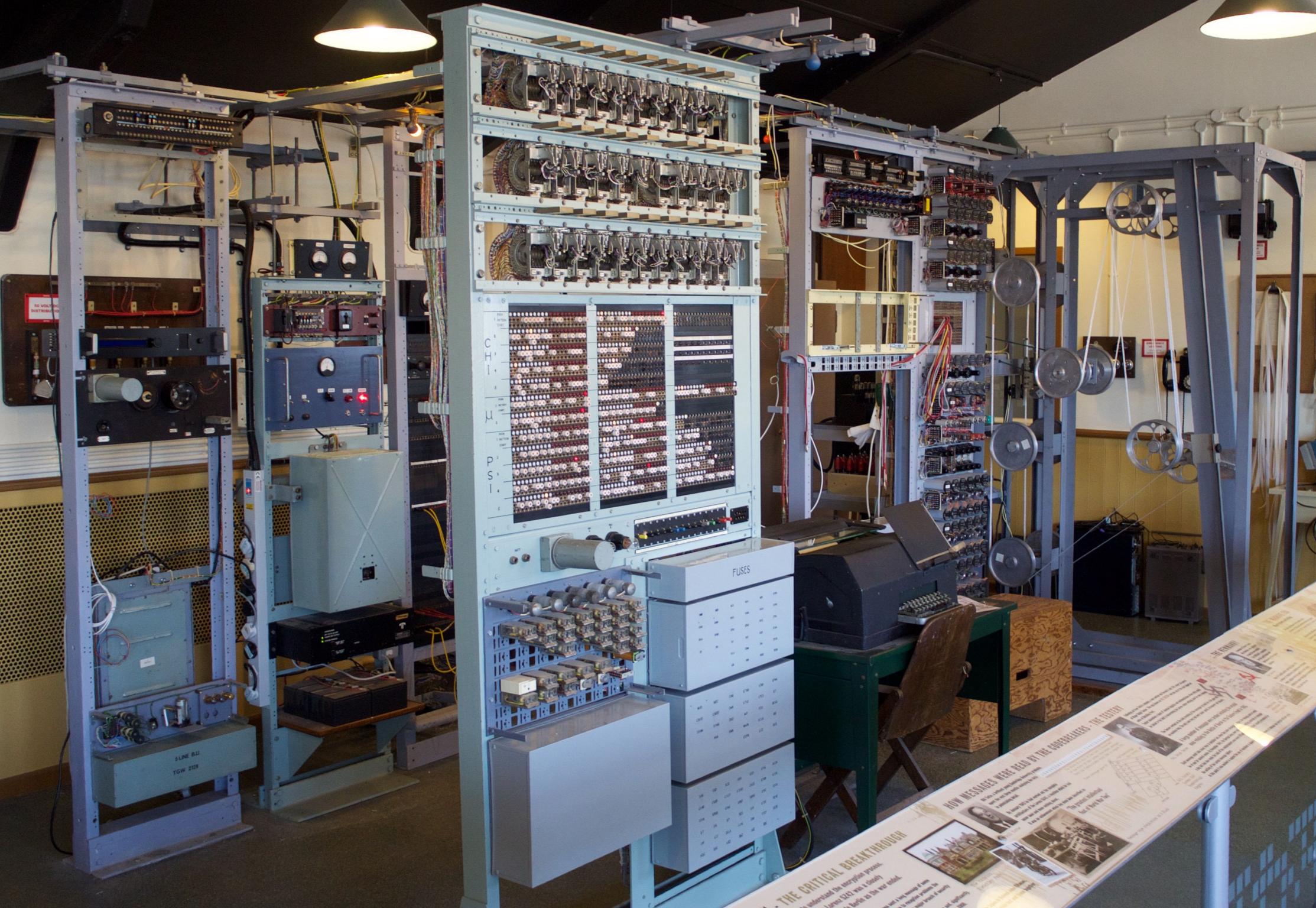
August 1939

Complete analysis
of Tunny

January 1942



Non-morse transmissions
intercepted in Britain



MESSAGE DECRYPTION - THE CRITICAL BREAKTHROUGH

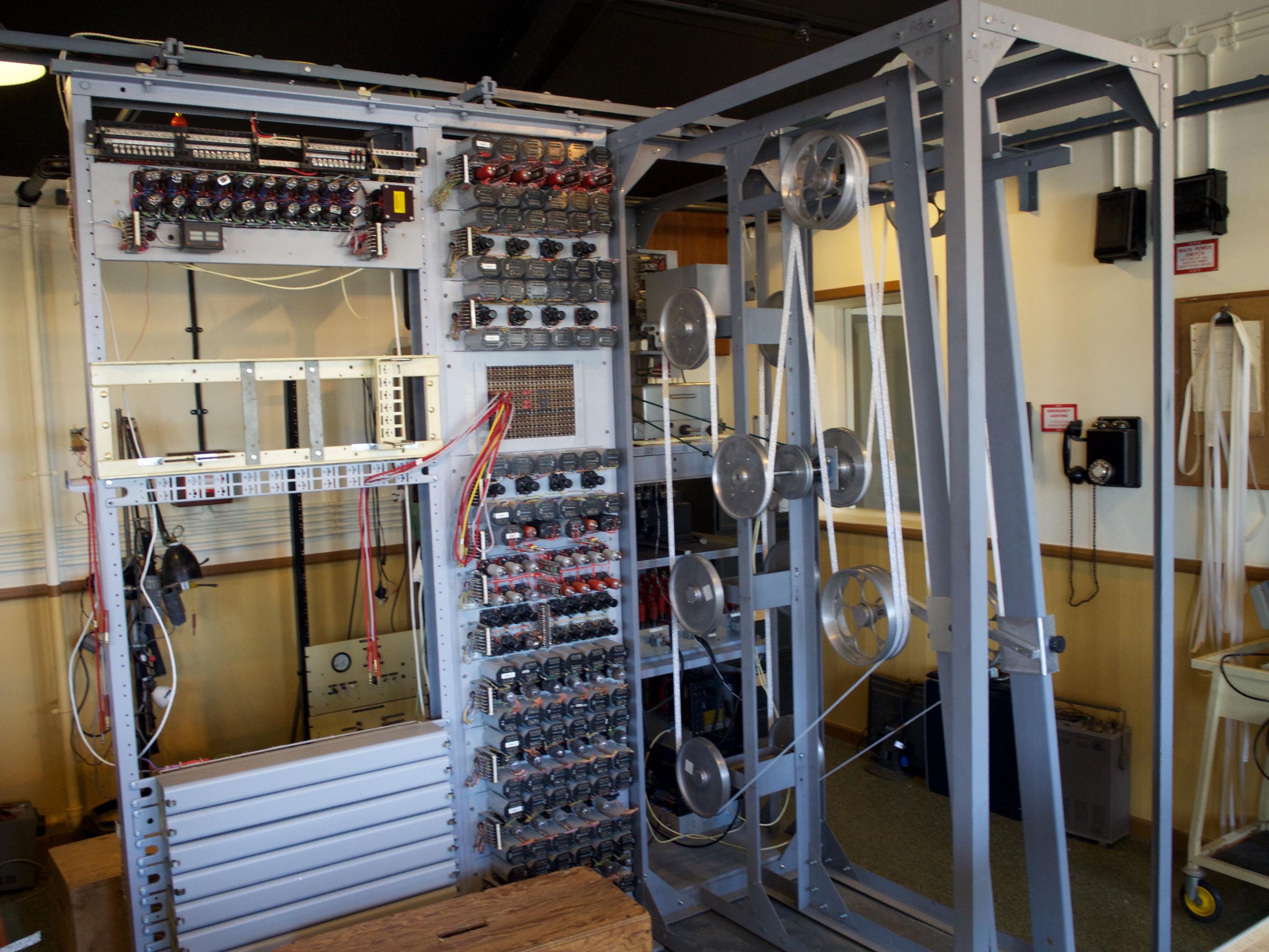
In order to decrypt the messages it was necessary to understand the encryption process. Unlike Enigma machines which were readily available, the Lorenz SZ42 was a closely guarded secret and remained so until one was captured outside Berlin on the war's end.

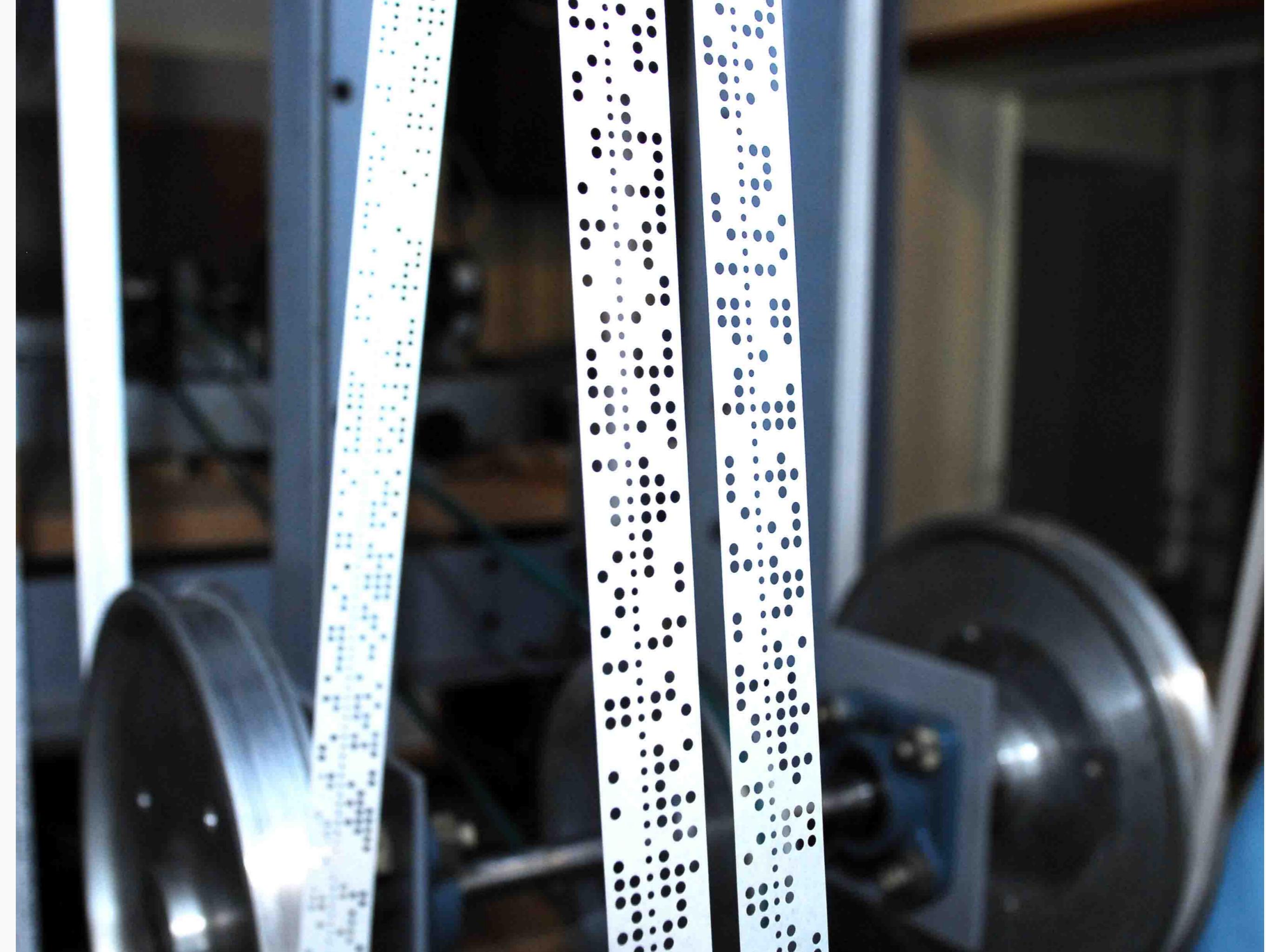
However, on August 20, 1944, a German engineer in France was given the responsibility of an Army assignment to dismantle a Lorenz machine for a British research team. Major Frank G. Clegg, who had been working on the project, was assigned to oversee the dismantling. He and his team worked through the night to complete the task. The next morning they were given the same set of the Lorenz machine and its ciphering and deciphering keys. The two men who had been working on the machine, including Clegg, were given £100 each as a reward.

The two men who had been working on the machine, including Clegg, were given £100 each as a reward.

TOP SECRET







Tommy Flowers

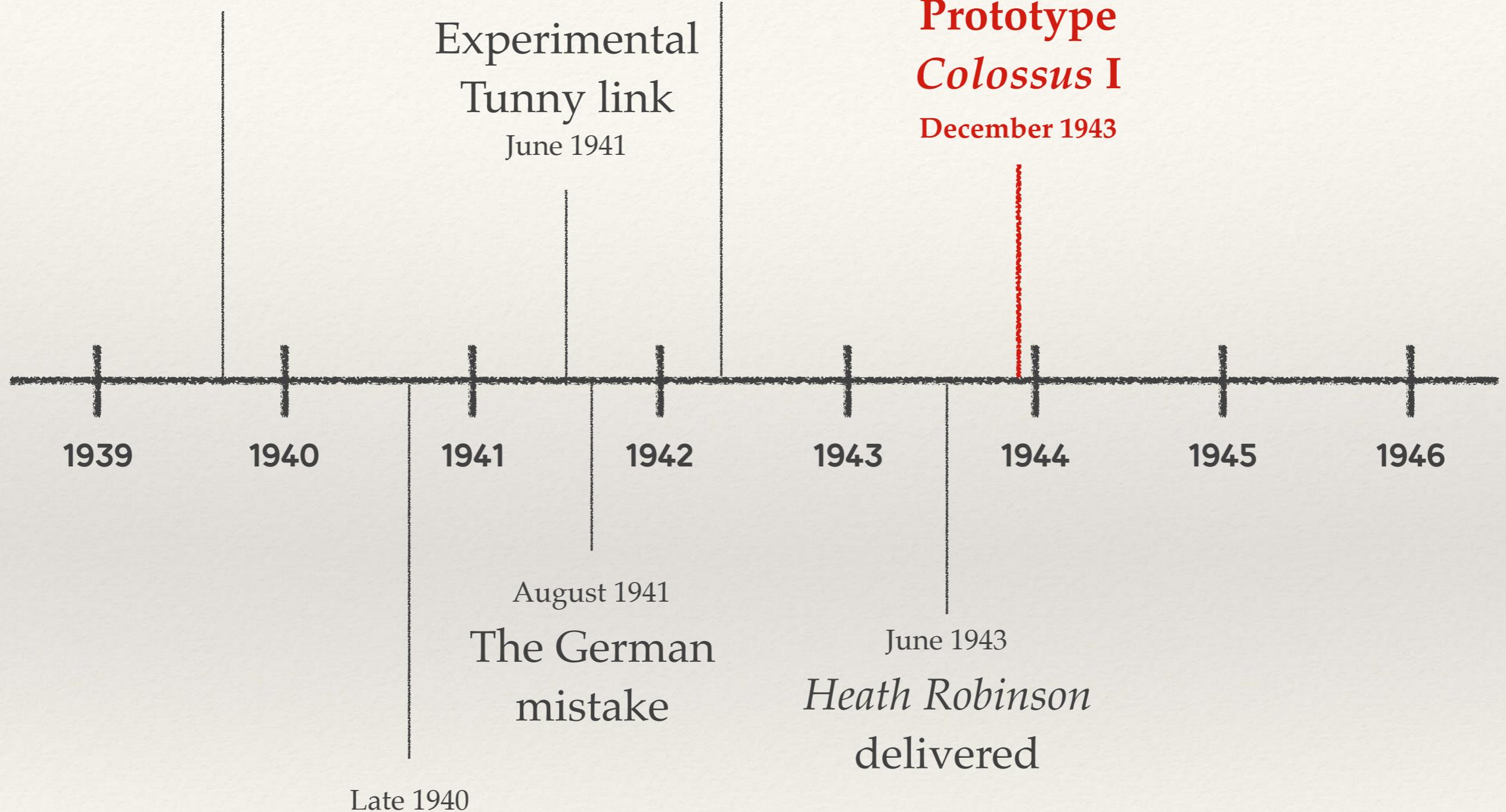


Codebreakers arrive
at Bletchley Park

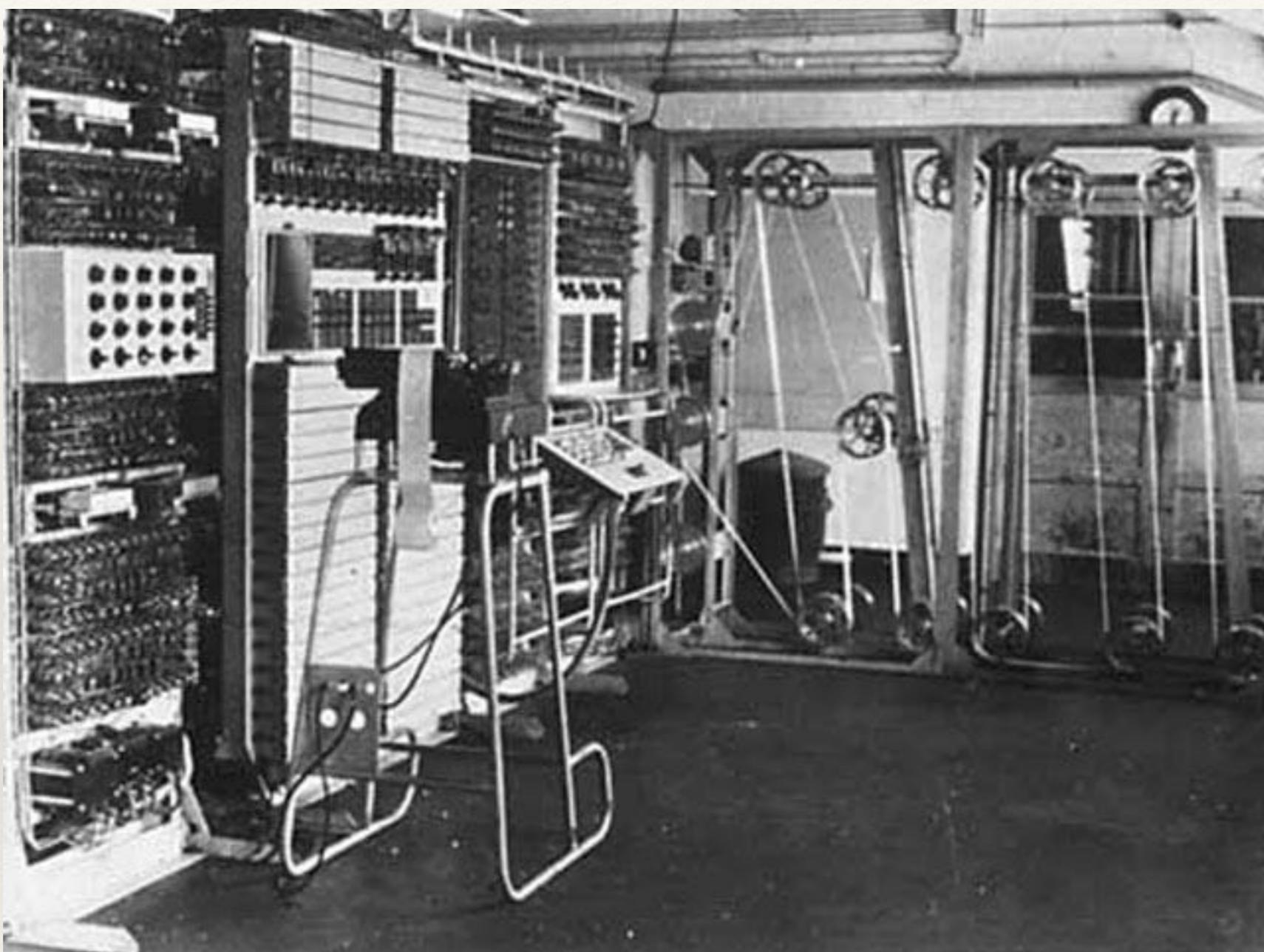
August 1939

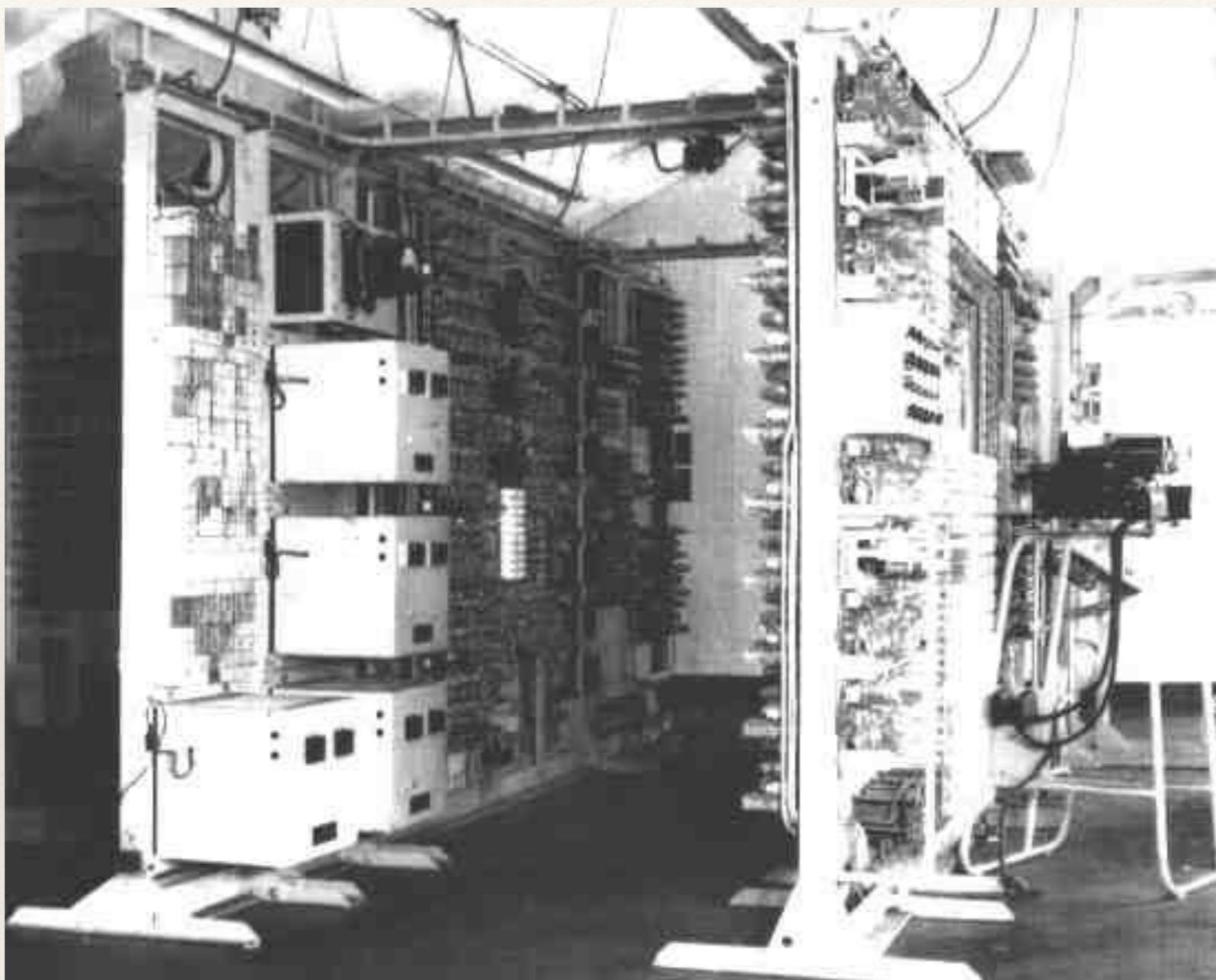
Complete analysis
of Tunny

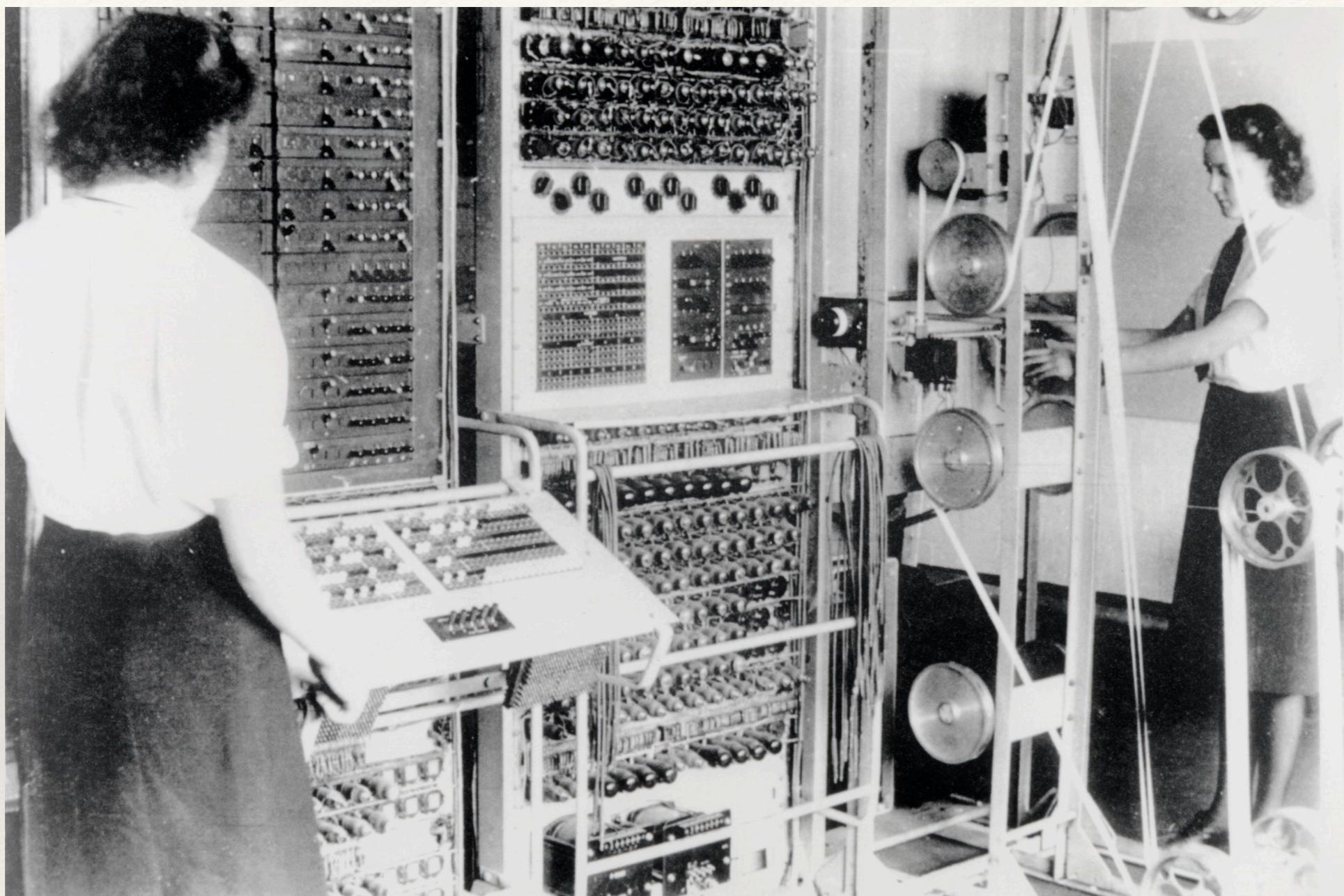
January 1942

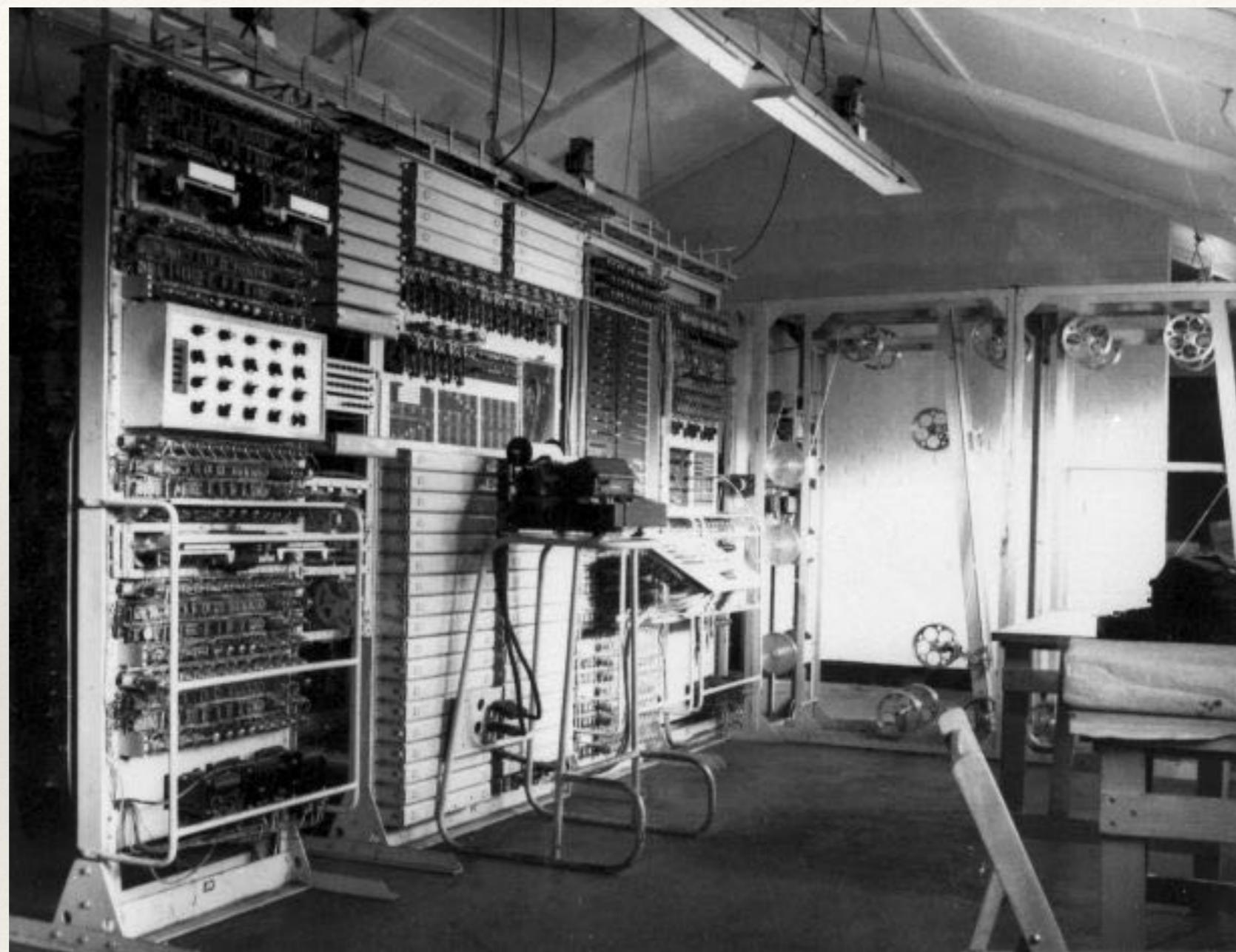


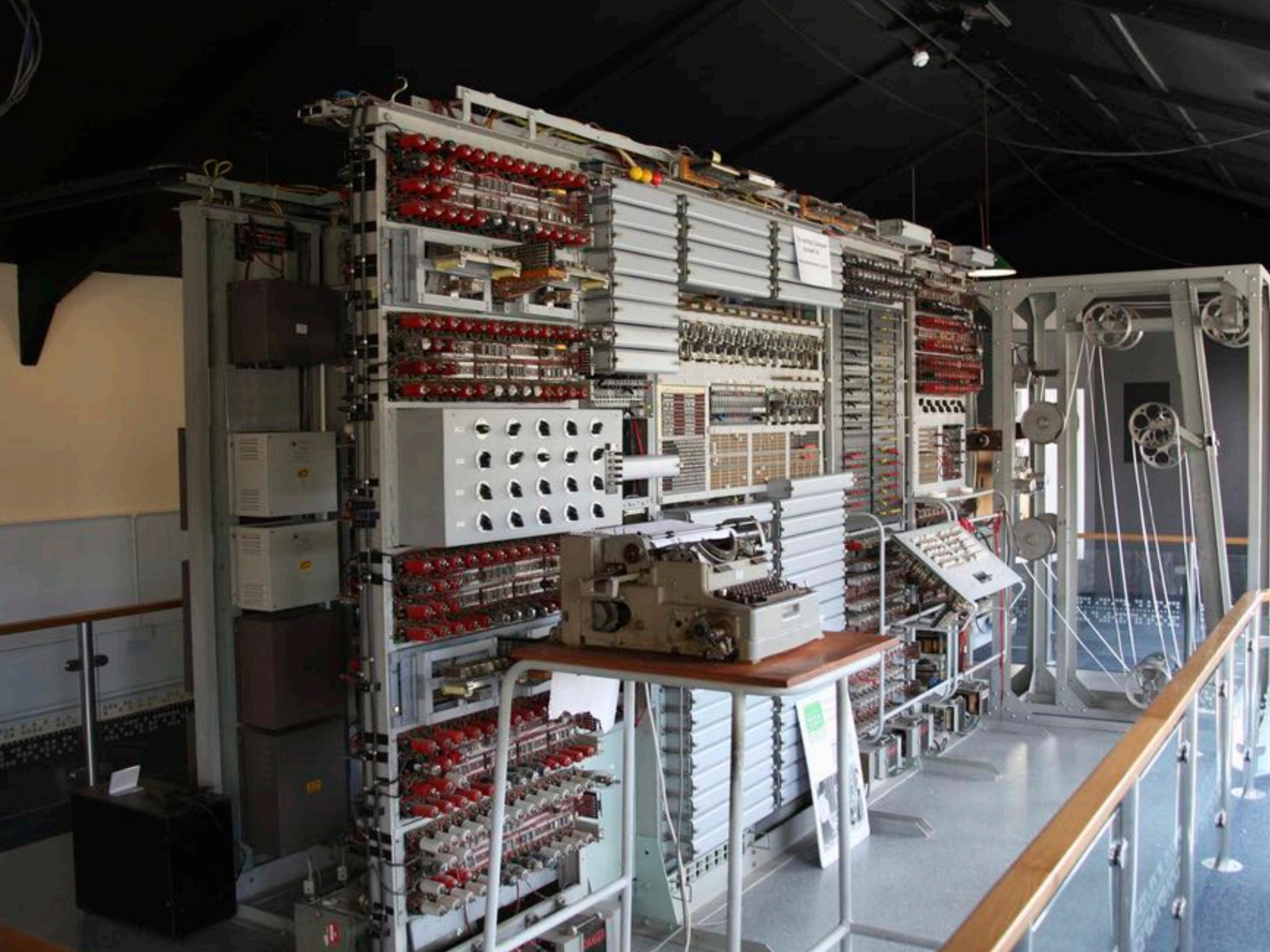
Non-morse transmissions
intercepted in Britain



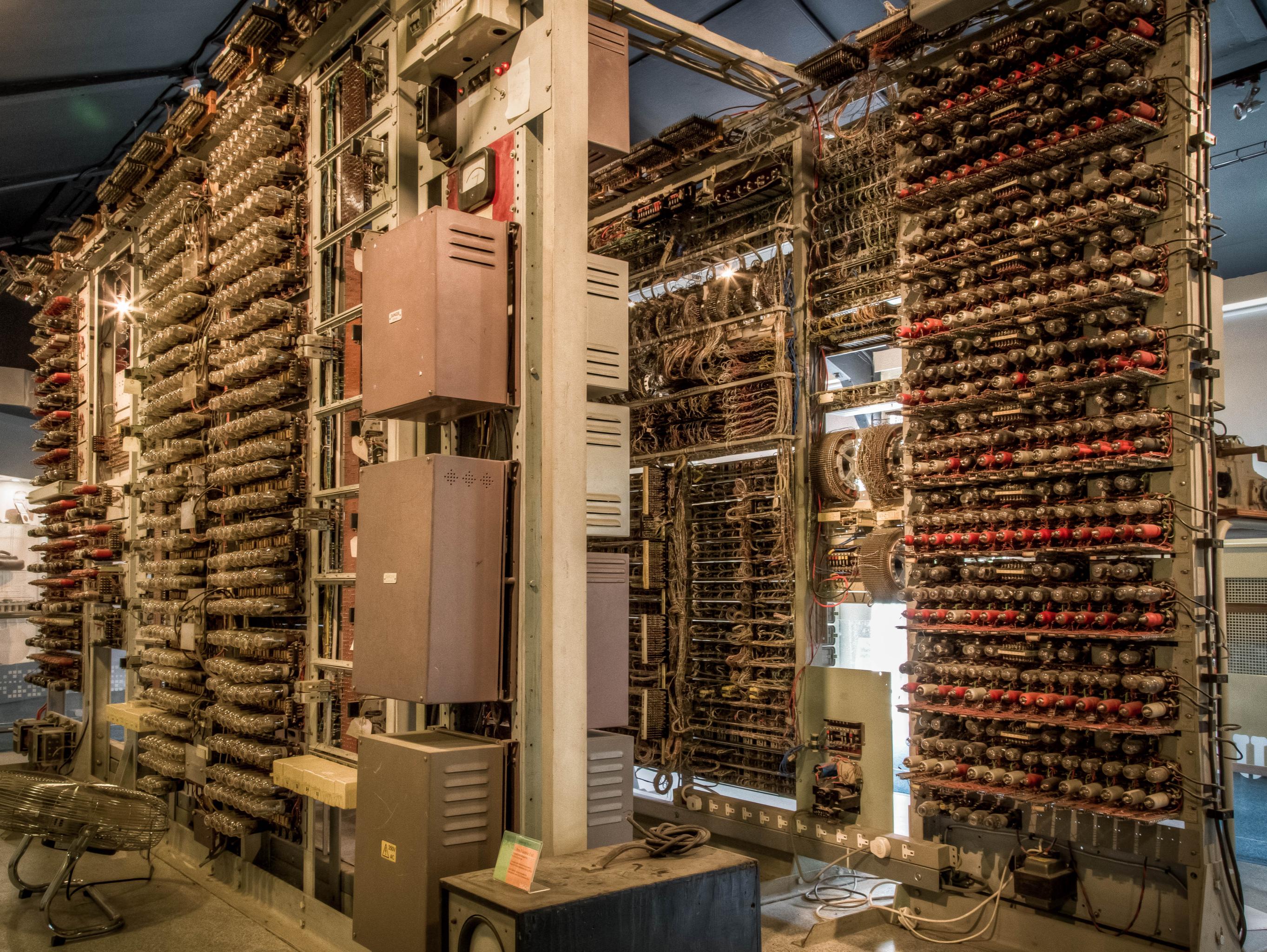








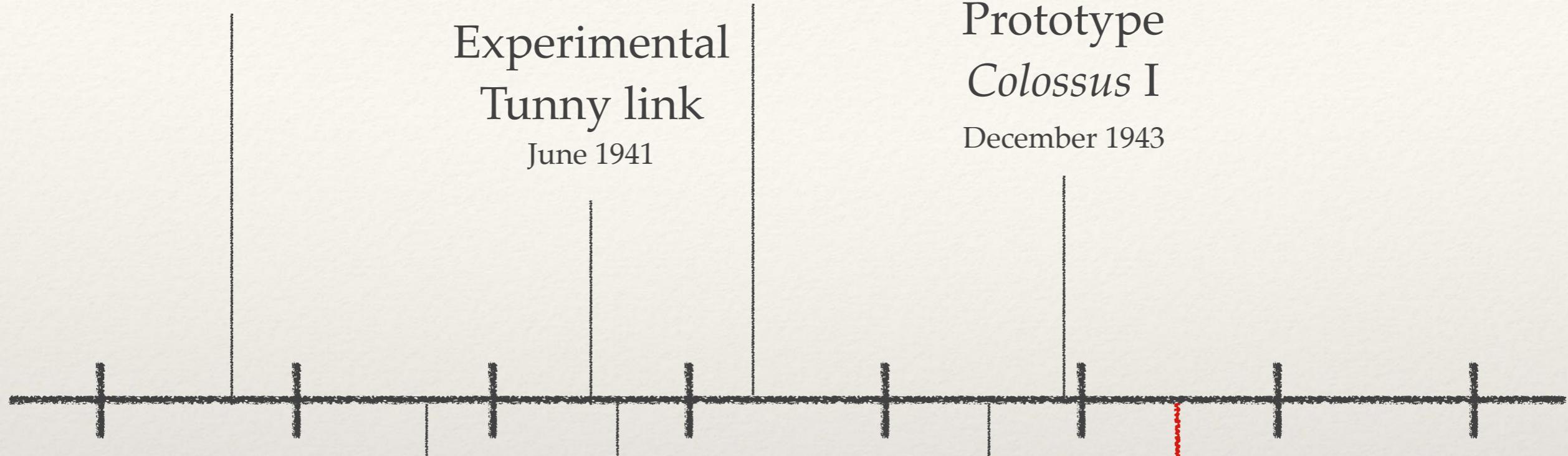




Codebreakers arrive
at Bletchley Park

August 1939

Complete analysis
of Tunny
January 1942



Non-morse transmissions
intercepted in Britain

August 1941
The German
mistake

Late 1940

Prototype
Colossus I

December 1943

June 1943
Heath Robinson
delivered

June 1944
Colossus II
& D-Day

Codebreakers arrive
at Bletchley Park

August 1939

Complete analysis
of Tunny

January 1942

Experimental
Tunny link

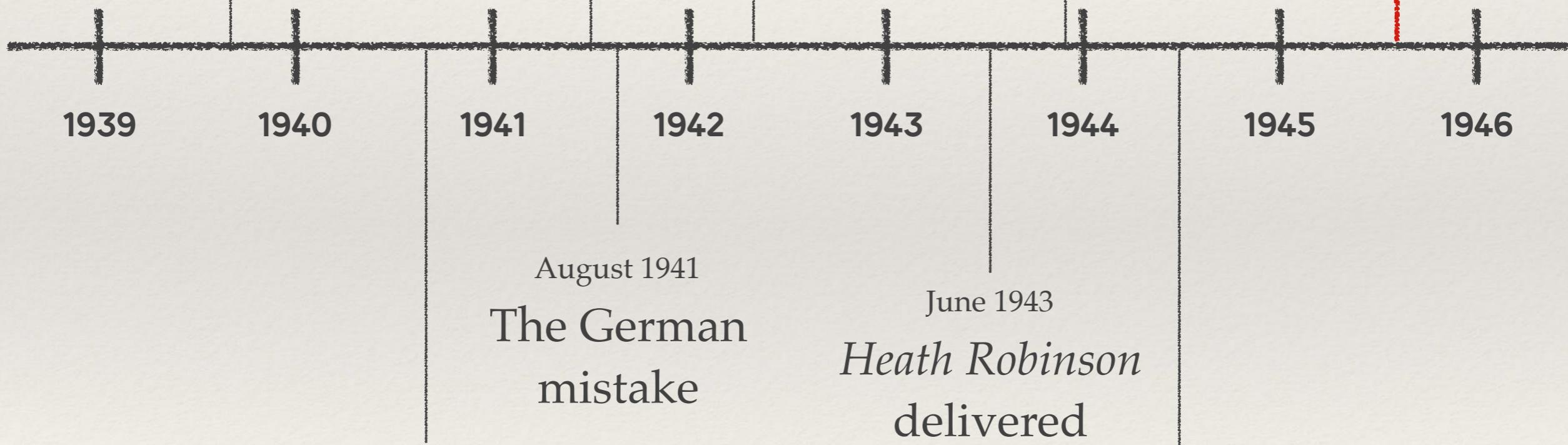
June 1941

Prototype
Colossus I

December 1943

Ten Colossi
at Bletchley
End of the war

June 1945



Non-morse transmissions
intercepted in Britain

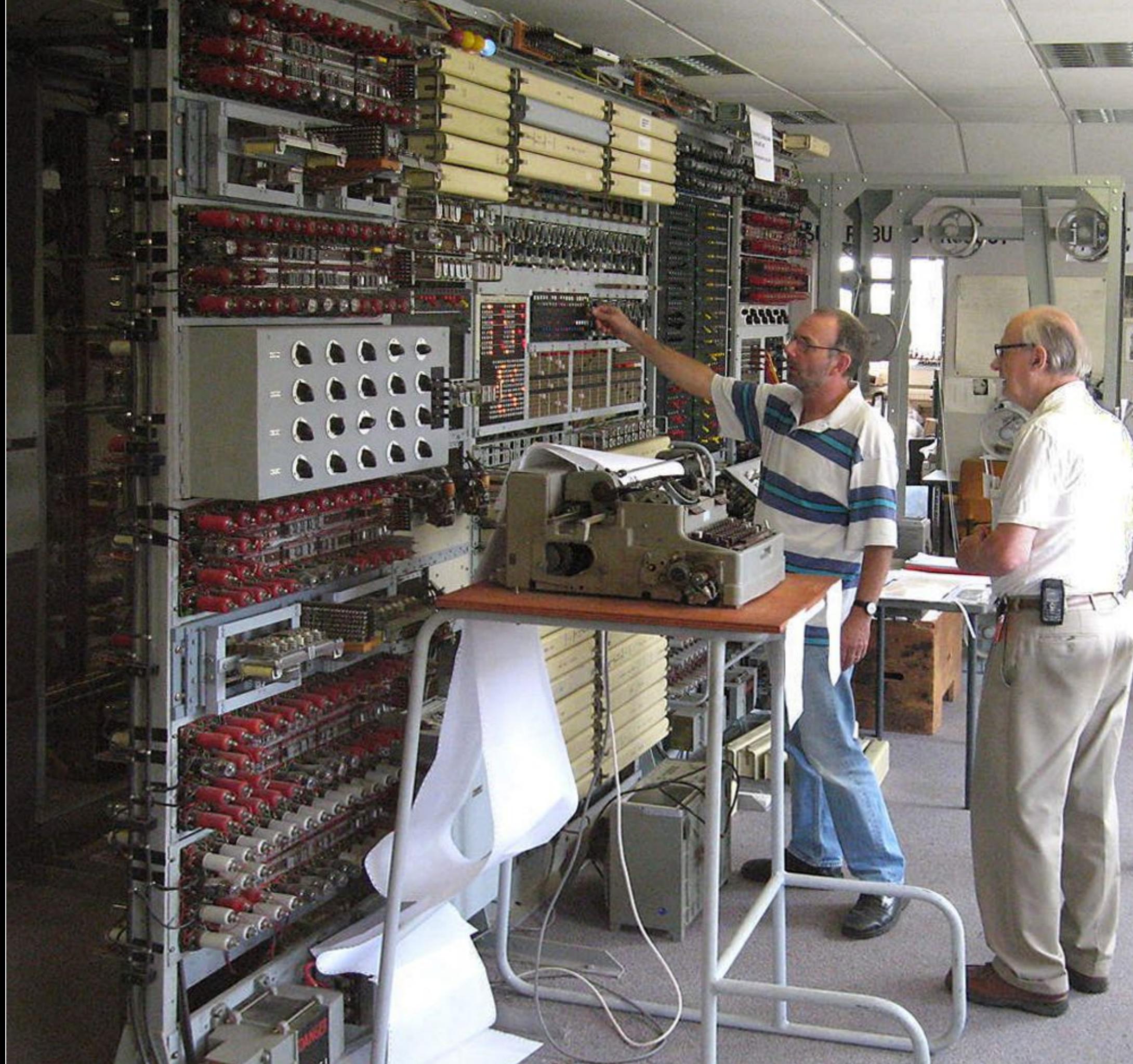
Colossus II
& D-Day

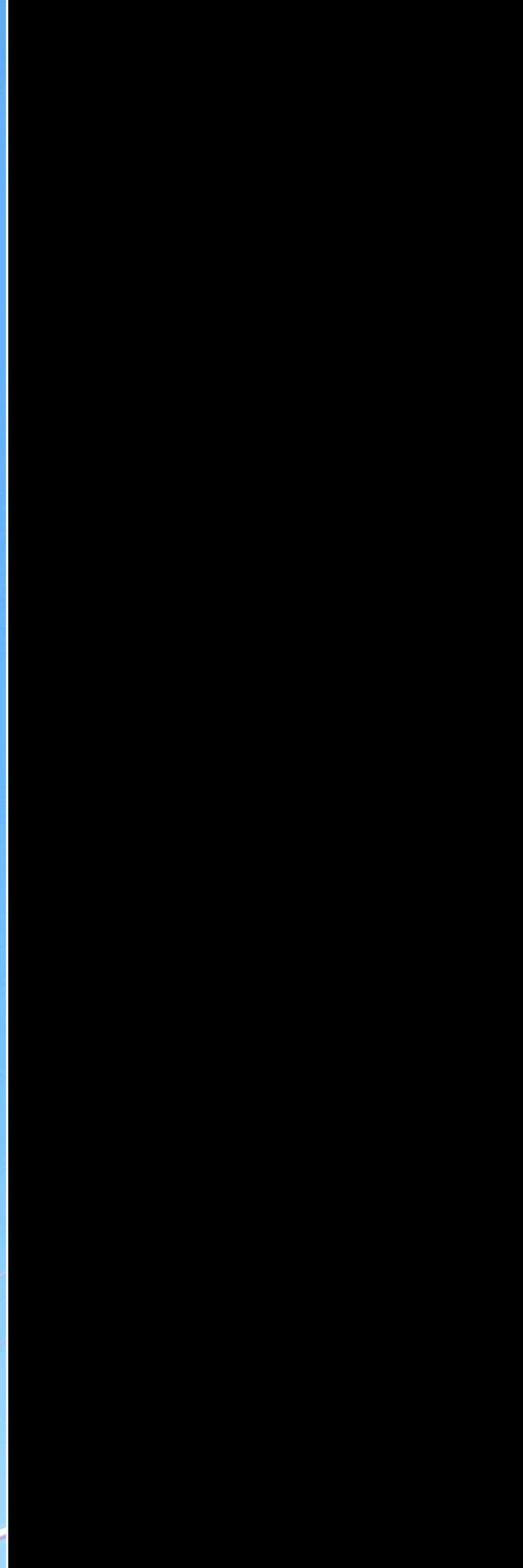


Brian Randell



Tony Sale





Colossus

The codebreaking computer
from Bletchley Park