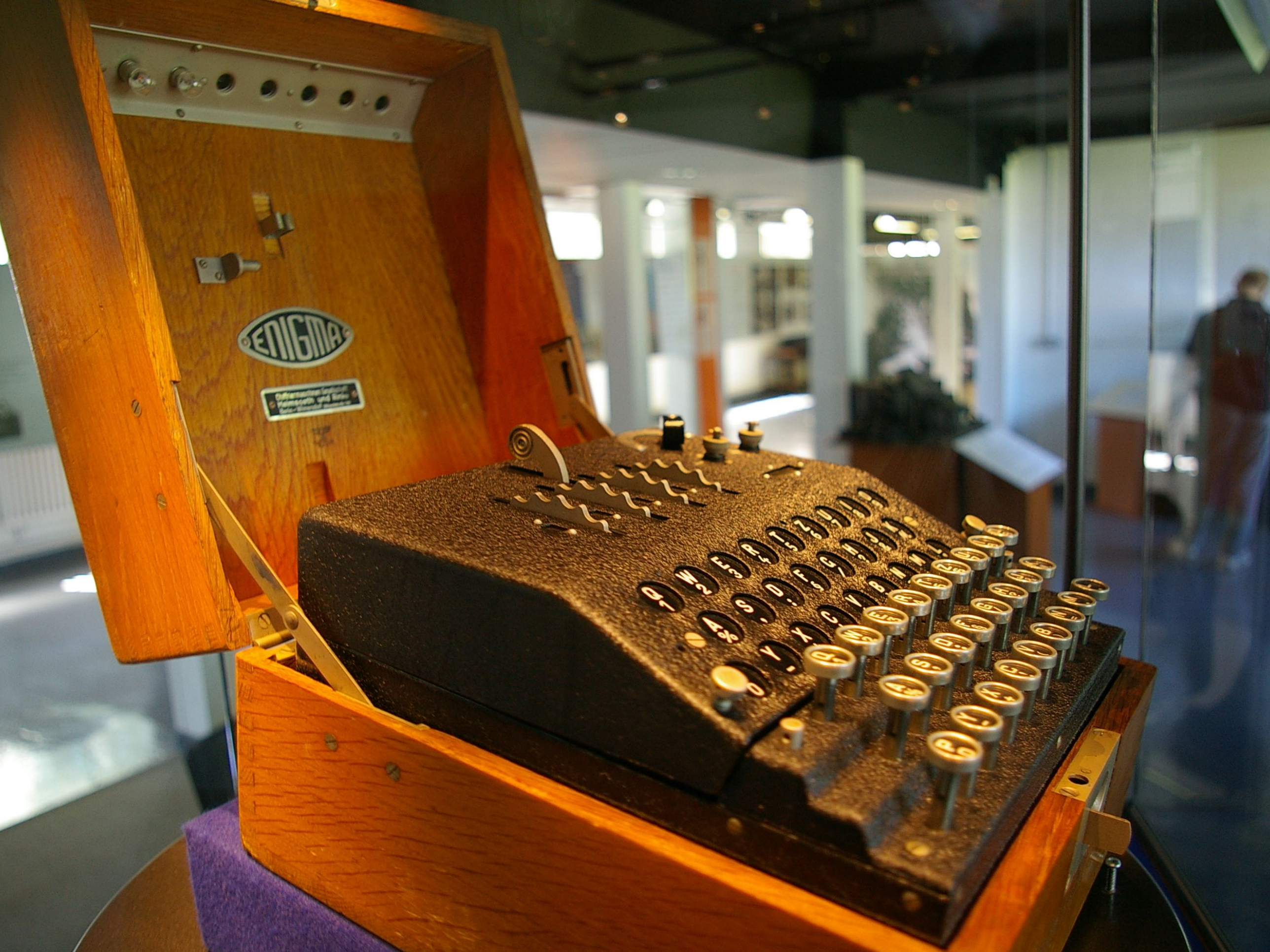
Colossus

The codebreaking computer from Bletchley Park

Codebreakers arrive at Bletchley Park

August 1939


ENIGMA

Codebreakers arrive at Bletchley Park

August 1939

Late 1940

Non-morse transmissions intercepted in Britain

ENZ T32 TELEPRINTER

(Circa 1936)

Springschreiber T32

System Morkrum-Kleinschmidt

C. Lorenz A.G.

Berlin-Tempelhof

50 Baud

Letters	Figures	KEYS						Letters	Figures	KEYS					
		V	IV		I	II	III			V	IV		I	II	III
A	1				●			P	+	●	●		●	●	●
B	8		●				●	Q	/	●	●		●		●
C	9		●		●		●	R	–	●	●				●
D	0		●		●	●	●	S	7	●					●
E	2					●		T	2	●			●		●
F	½		●			●	●	U	4				●		●
G	7		●			●		V	'	●			●	●	●
H	1		●		●	●		W	?	●				●	●
I	⅓					●	●	X	⅔	●				●	
J	6		●		●			Y	3						●
K	(	●	●		●			Z	:	●			●	●	
L	=	●	●		●	●		–	.	●			●		
M	)	●	●			●		✱	✱	●	●		(Erasure)		.
N	£	●	●			●	●	Figure shift & space			●				
O	5				●	●	●	Letter shift & space		●					
/	¼				●	●									

FIG. 22.

BAUDÔT SIGNALLING CODE OR ALPHABET (BRITISH).

Tunny

Sturgeon

Thrasher

Codebreakers arrive at Bletchley Park

August 1939

Experimental Tunny link

June 1941

1939 1940 1941 1942 1943 1944 1945 1946

Late 1940

Non-morse transmissions intercepted in Britain


e
m
o
e
m
f
mA
Motor
langsam
Schnell

message S . . x . x

message	S	.	.	x	.	x
key	K	x	.	.	x	x

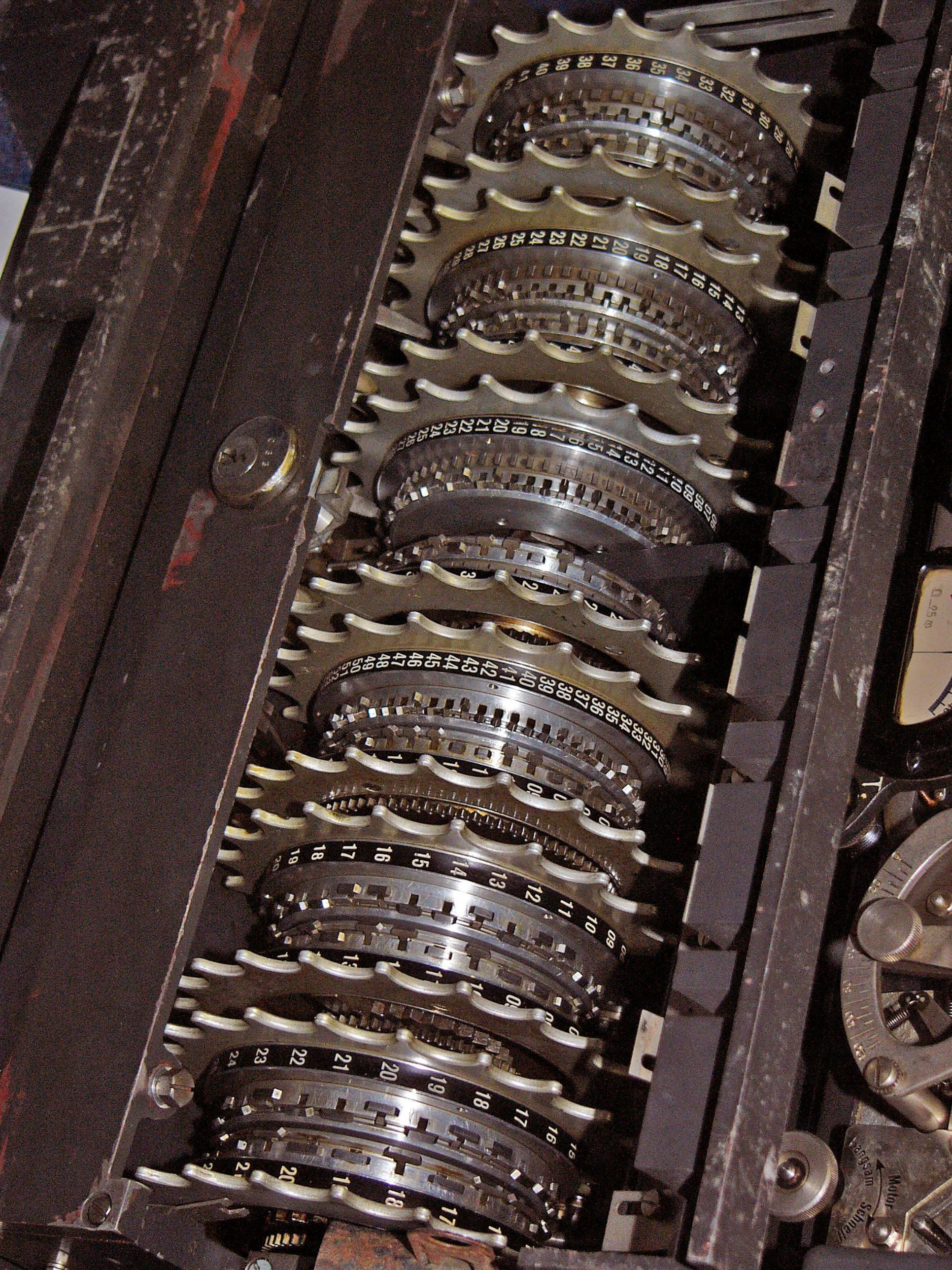
message	S		.	.	x	.	x
key	K	x	.	.	x	x	
ciphertext	C	x	.	x	x	.	

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

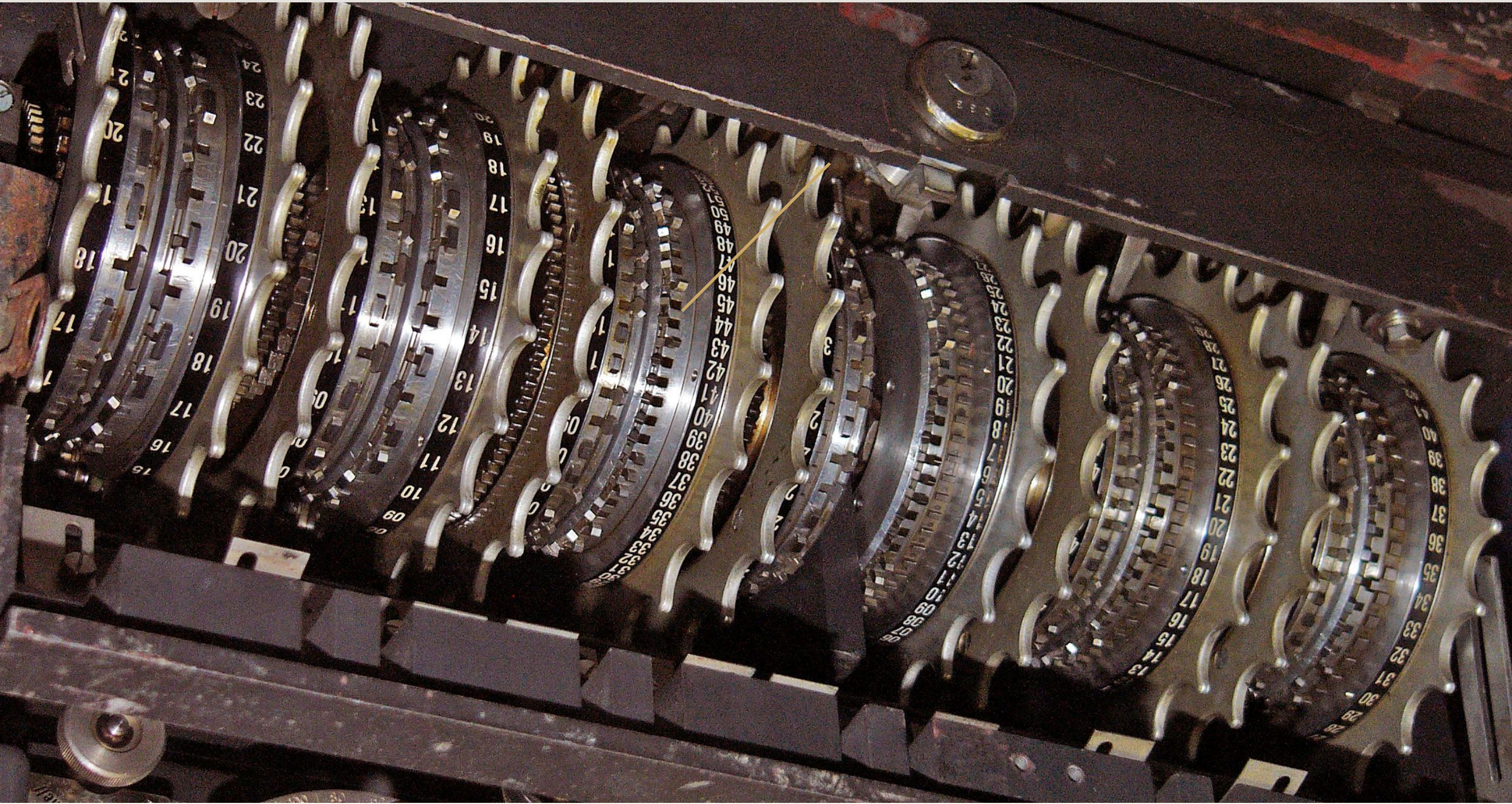
message	S	0 0 1 0 1
key	K	1 0 0 1 1
ciphertext	C	1 0 1 1 0
key	K	1 0 0 1 1
message	S	0 0 1 0 1

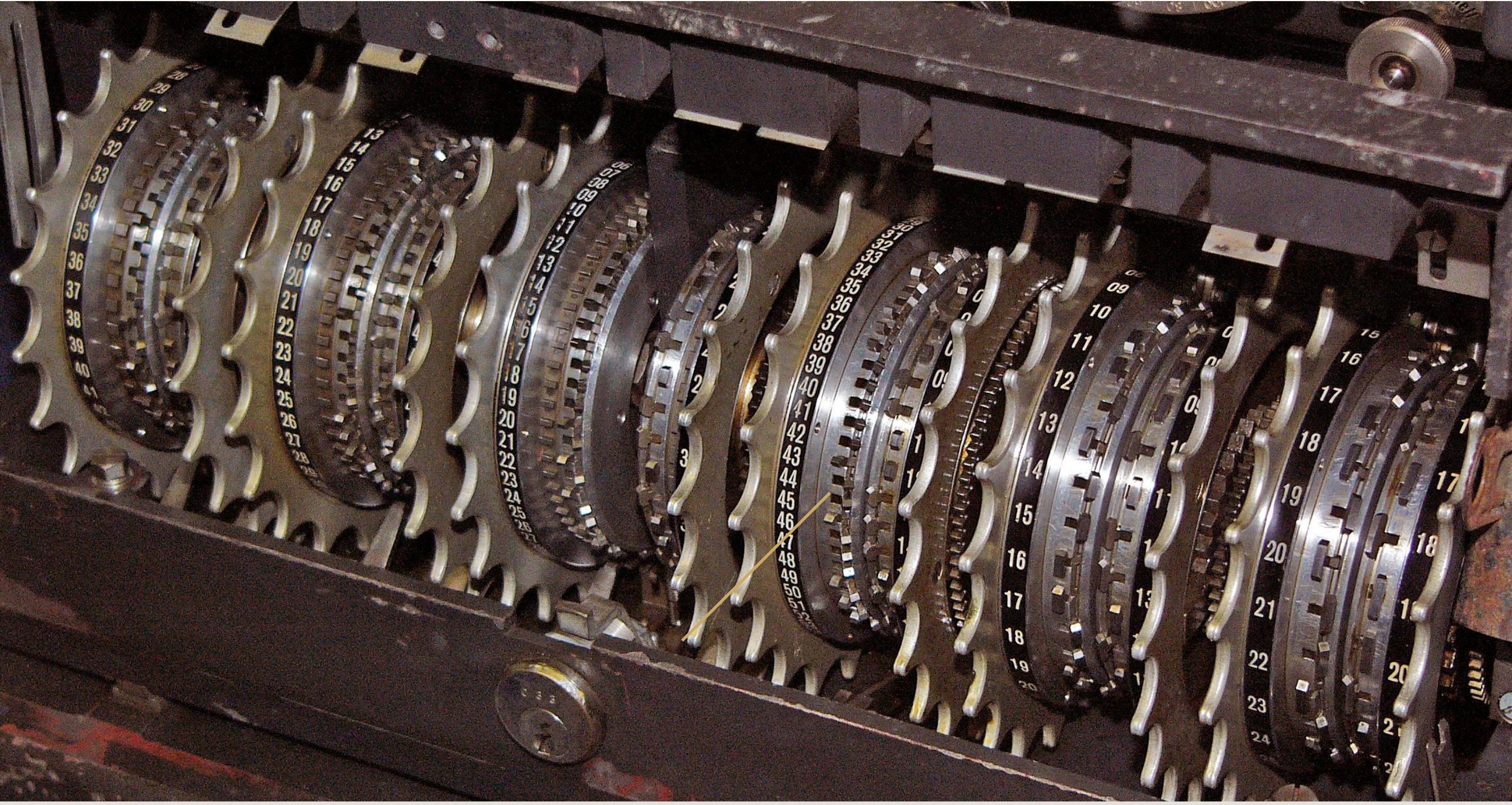

Schnell
Langsam
Motor


08
09
10
11
12
27
28

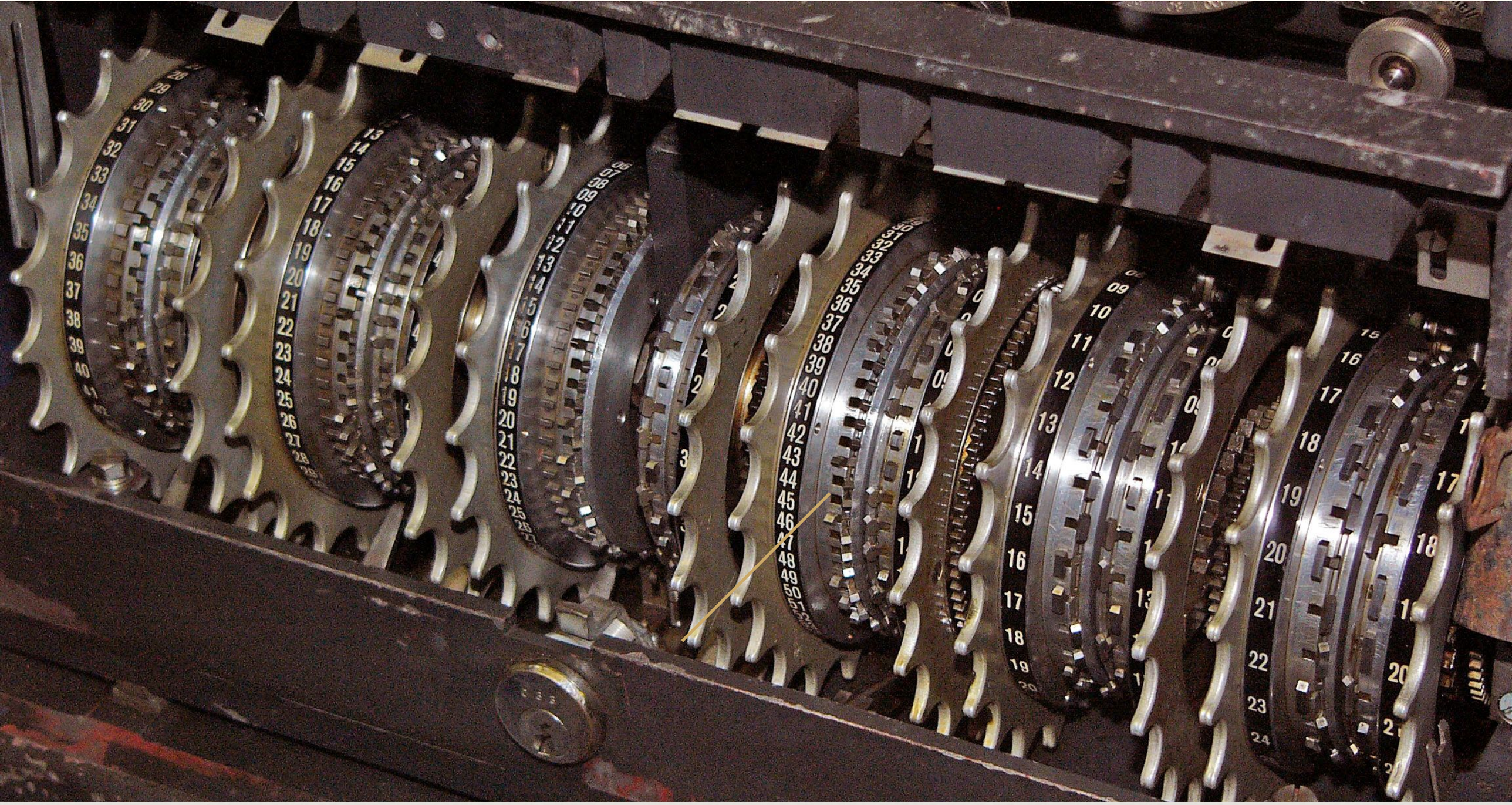

1 2 3 4 5 6 7 8 9 10 11 12
A B C D E F G H I K L M N O P Q R S T U V W X Y Z

1 14 28 40 11 21 38 32 03 17 24 28 34 11 26
2 22 11 10 46 44 37 23 08 04 45 32 45
3 46 40 32 12 26 07 48 44 36 10 21 17 05 02
4 27 52 03 20 35 45 40 29 08 12 25 33 50 37
5 21 49 44 36 30 12 14 19 14 53 42 02
6 36 16 09 27 29 23 03 05 35 19 06 13 12



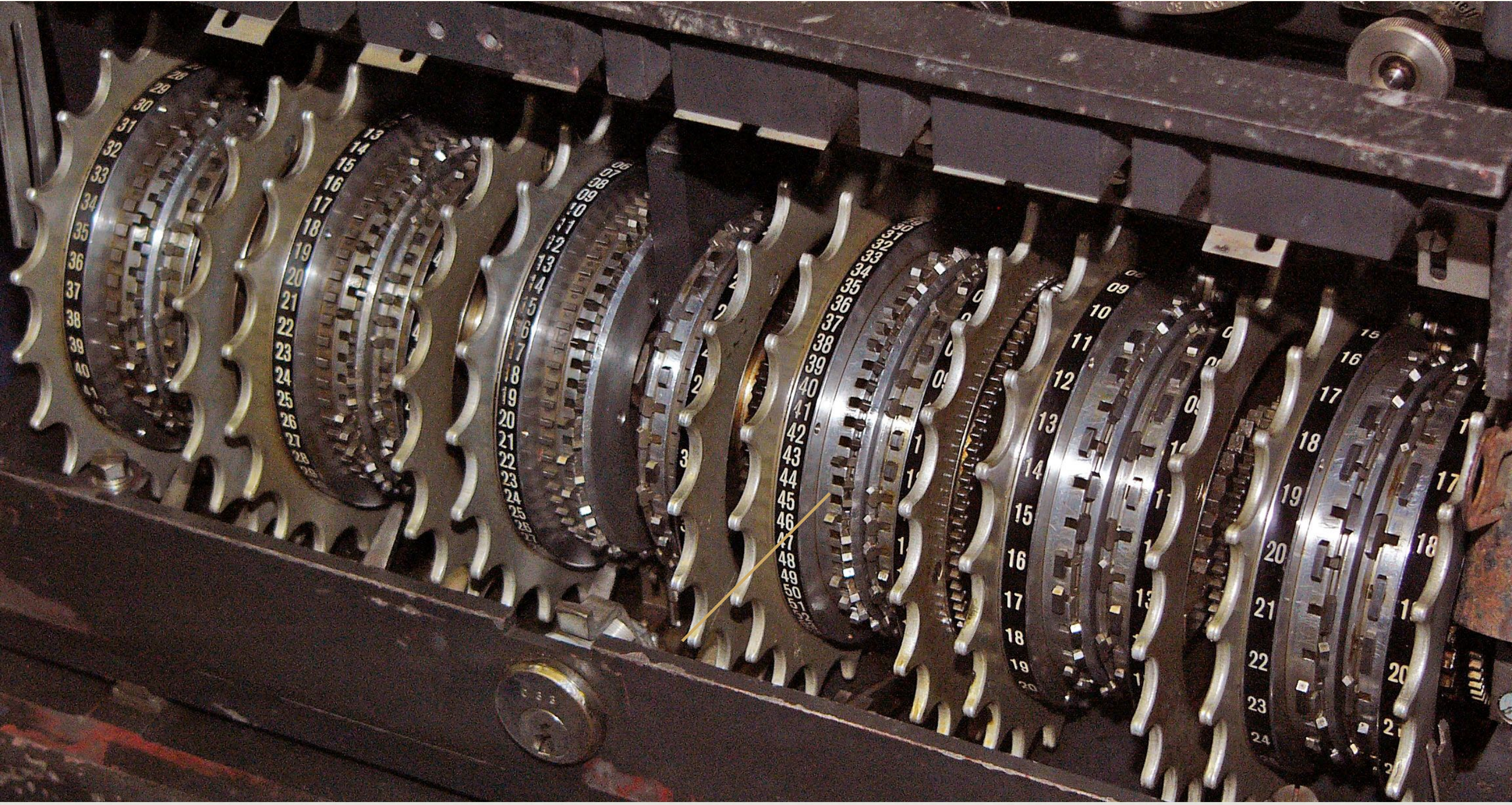


χ-wheels

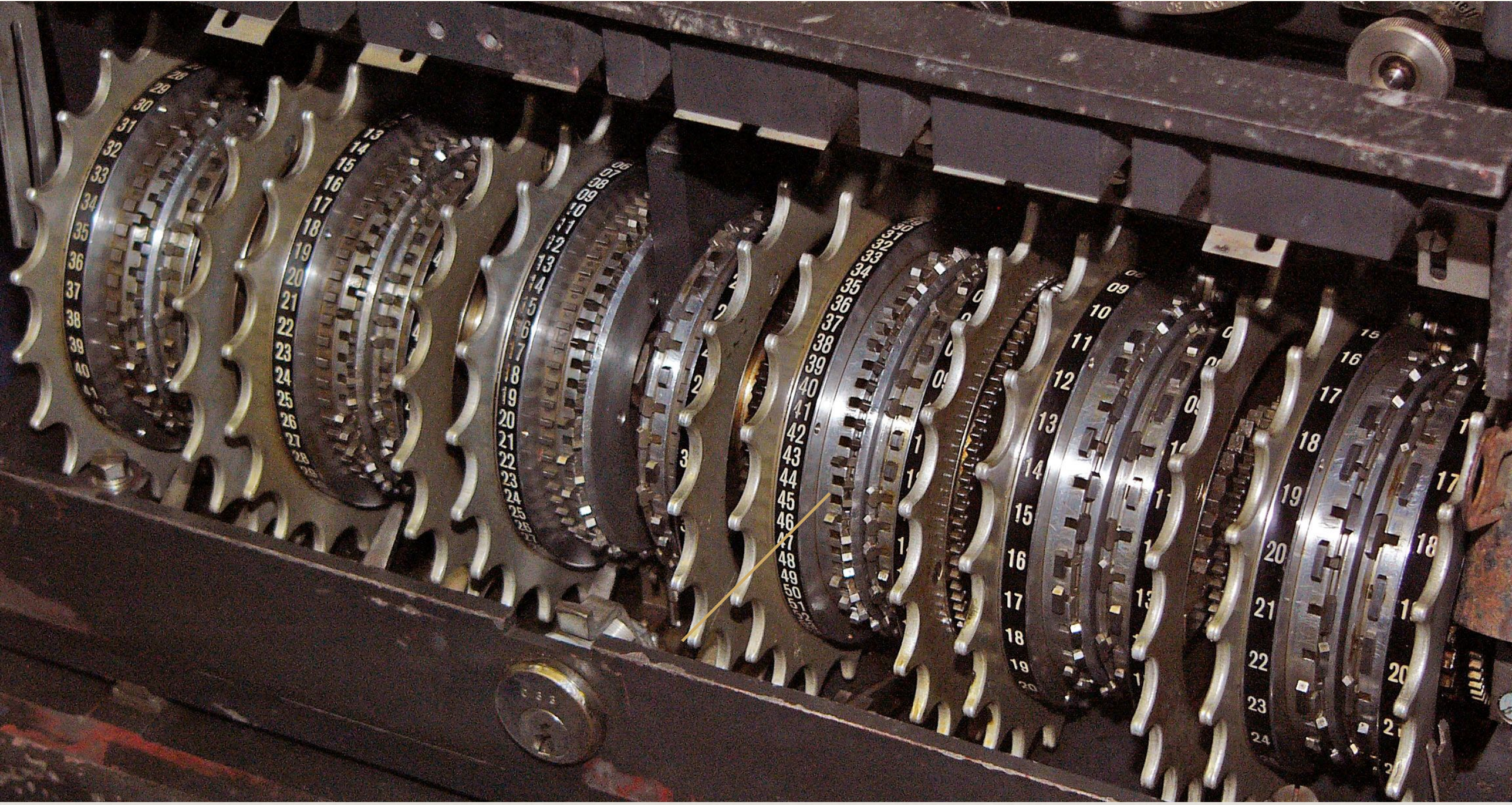


ψ-wheels

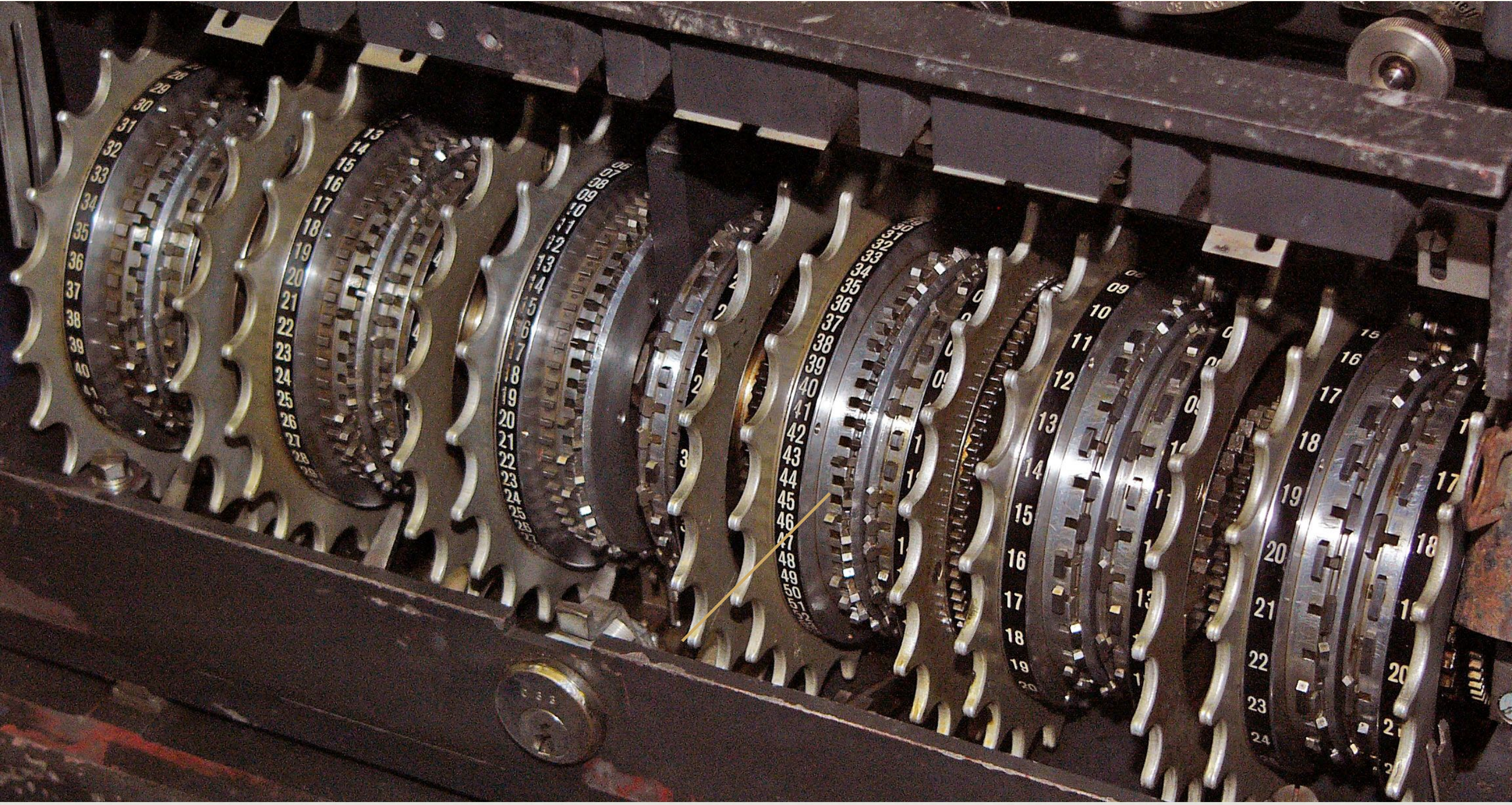
χ-wheels



ψ-wheels μ-wheels χ-wheels



ψ-wheels μ-wheels χ-wheels



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

?

?

$$C_1 = M_1 + K$$

$$C_2 = M_2 + K$$

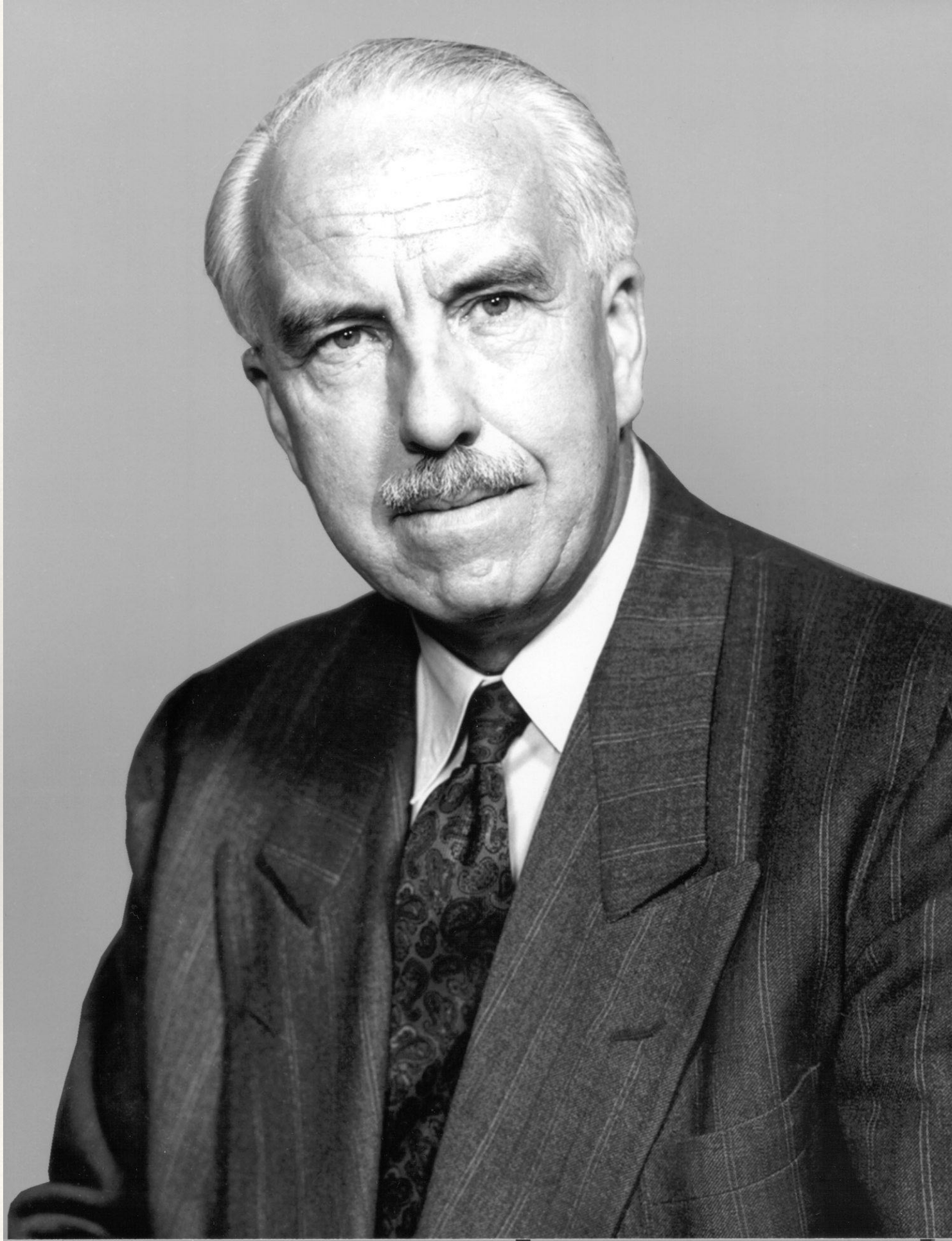
?

$$C_1 = M_1 + K$$

$$C_2 = M_2 + K$$

$$C_1 + C_2 = M_1 + M_2$$

John Tiltman

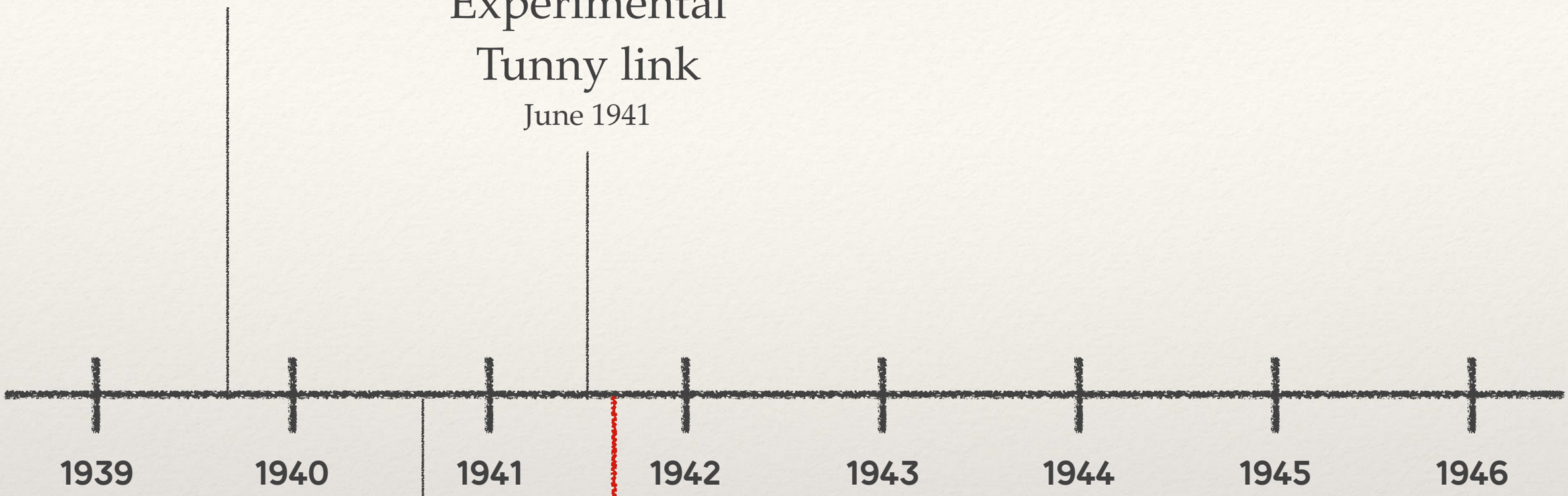


Codebreakers arrive at Bletchley Park

August 1939

Experimental Tunny link

June 1941



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

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

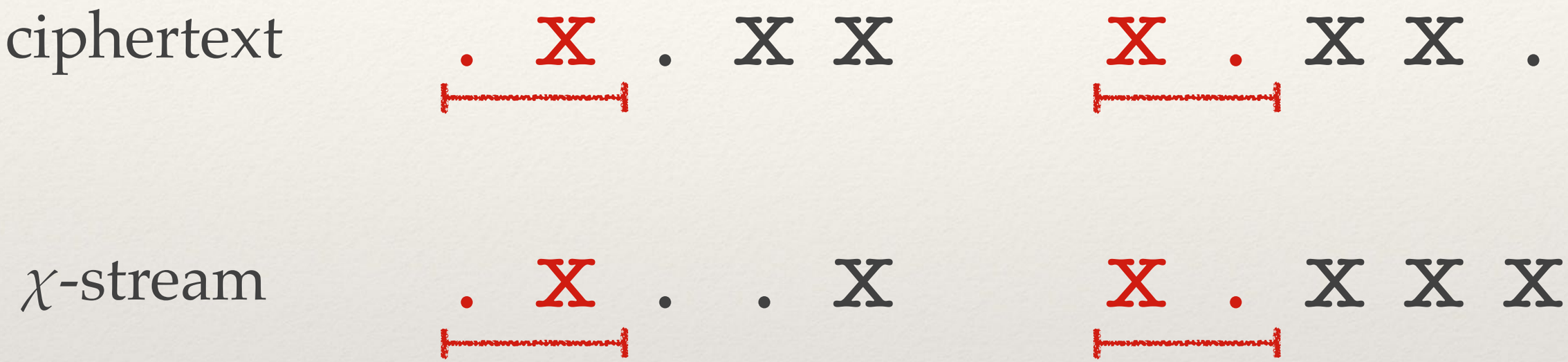
Breaking Tunny, a how-to

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



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 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	χ_1	χ_2

. + 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	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

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

ciphertext	$M_1 + \chi_1 + \psi_1'$	$M_2 + \chi_2 + \psi_2'$
χ-stream	χ_1	χ_2

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

$$= (M_1 + M_2) + (\psi_1' + \psi_2')$$

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

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

$$= (M_1 + M_2) + (\psi_1' + \psi_2')$$

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

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

$$= (M_1 + M_2) + \cancel{(\psi_1' + \psi_2')}$$

$$= M_1 + M_2$$

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

Experimental Tunny link

June 1941

1939 1940 1941 1942 1943 1944 1945 1946

August 1941

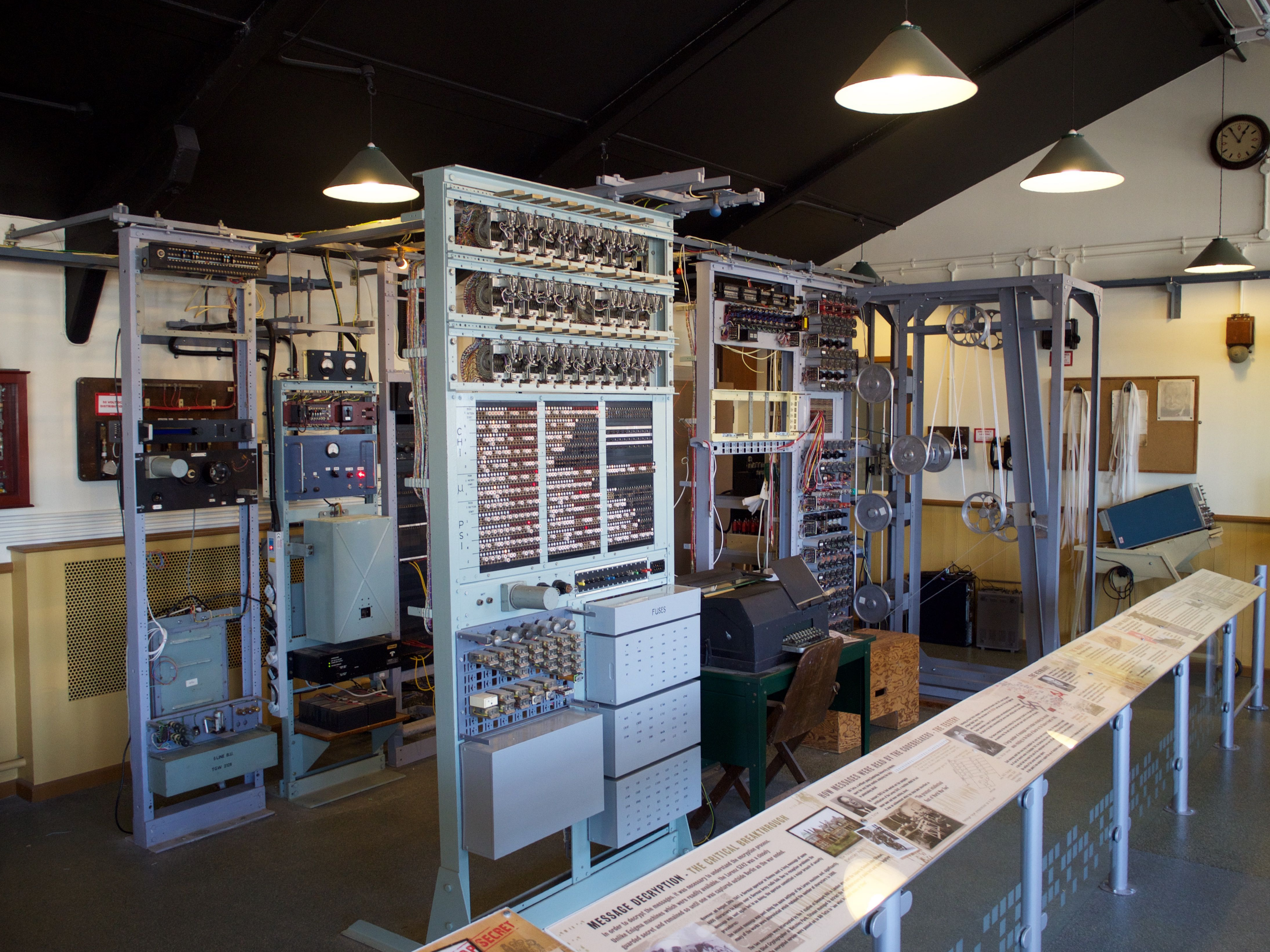
The German mistake

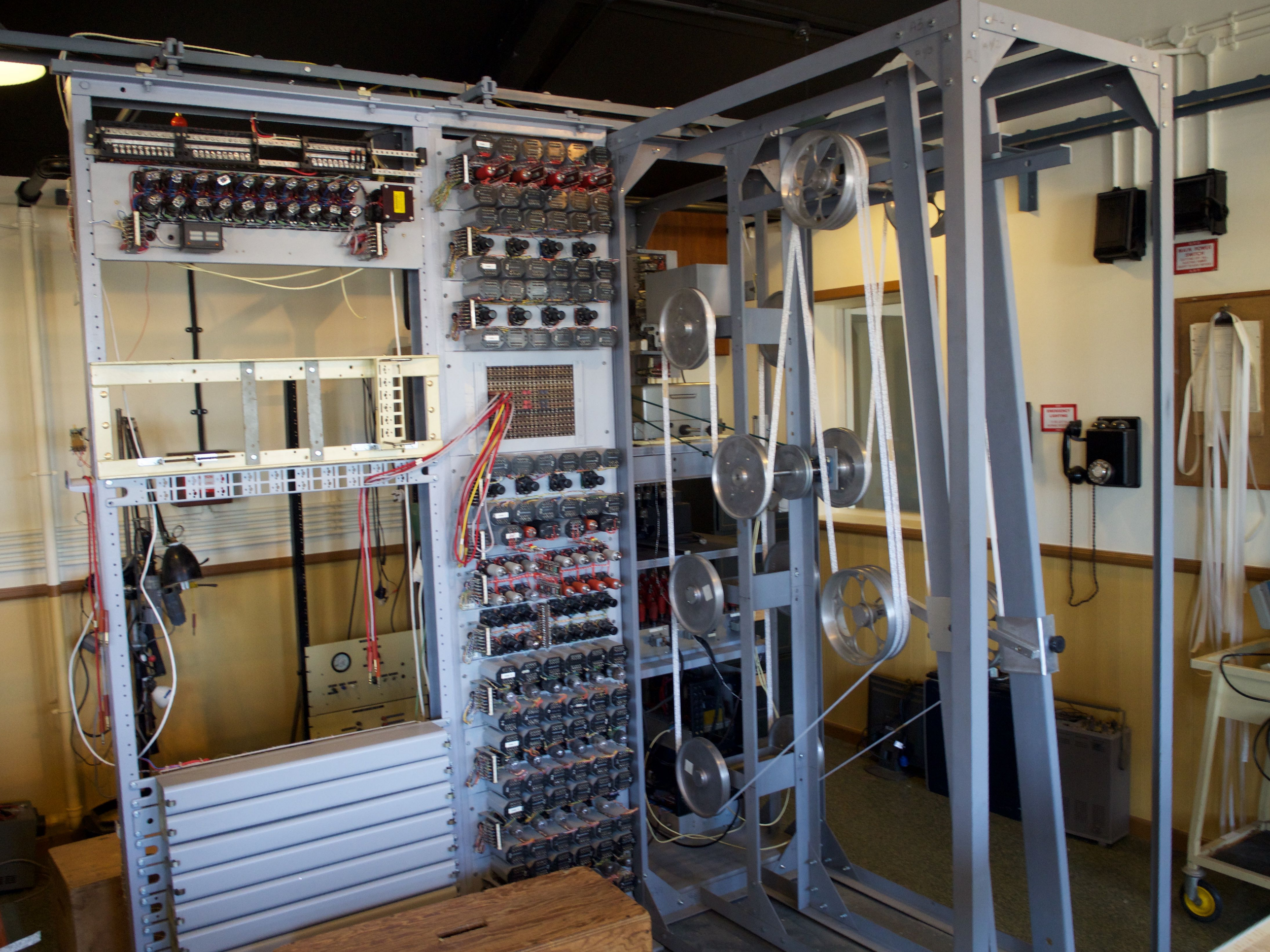
June 1943

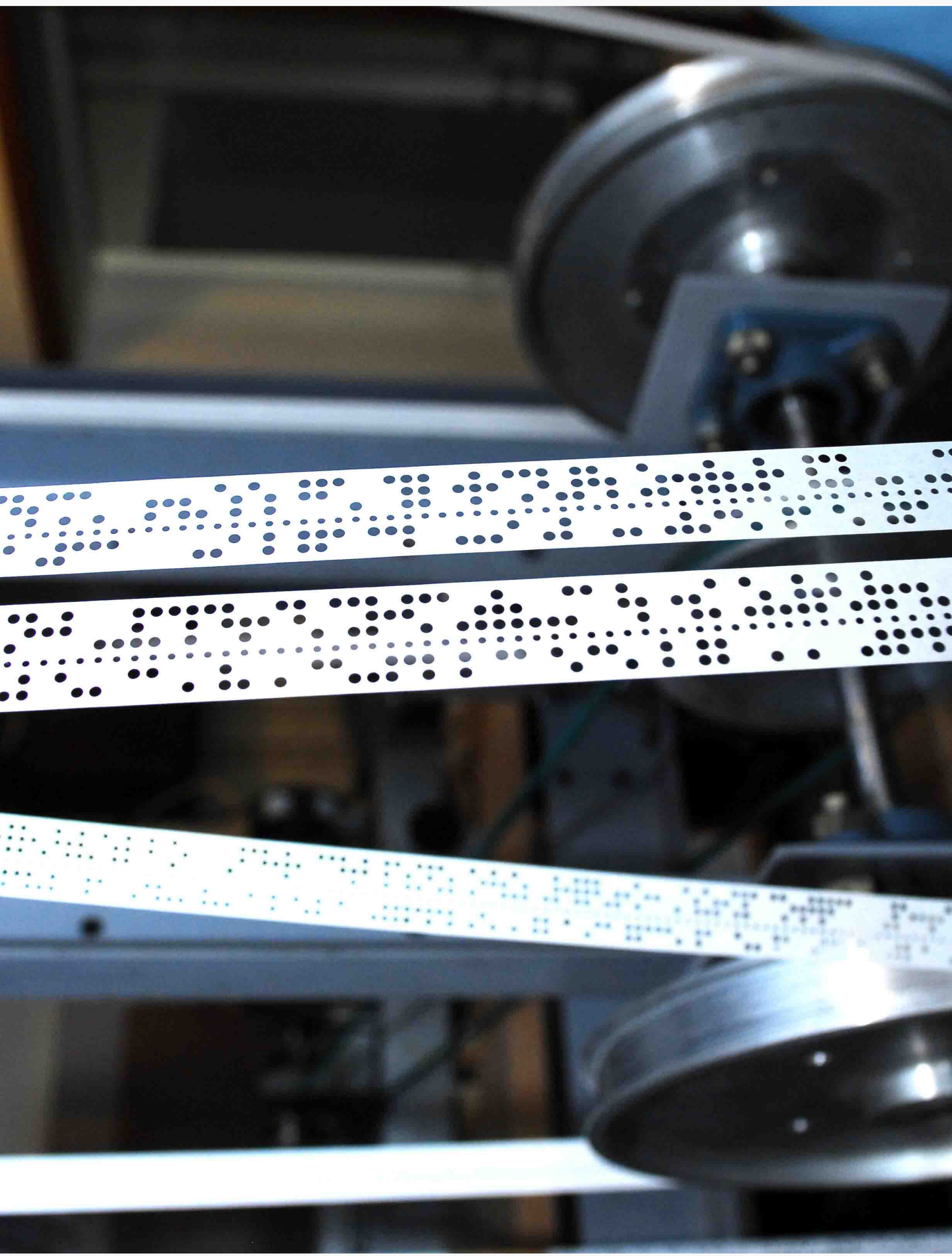
***Heath Robinson* delivered**

Late 1940

Non-morse transmissions intercepted in Britain


FUSES
MESSAGE DECRYPTION - THE CRITICAL BREAKTHROUGH
HOW MESSAGES WERE READ BY THE CODEBREAKERS - THE STATION
SECRET





Tommy Flowers

Codebreakers arrive at Bletchley Park

August 1939

Complete analysis of Tunny

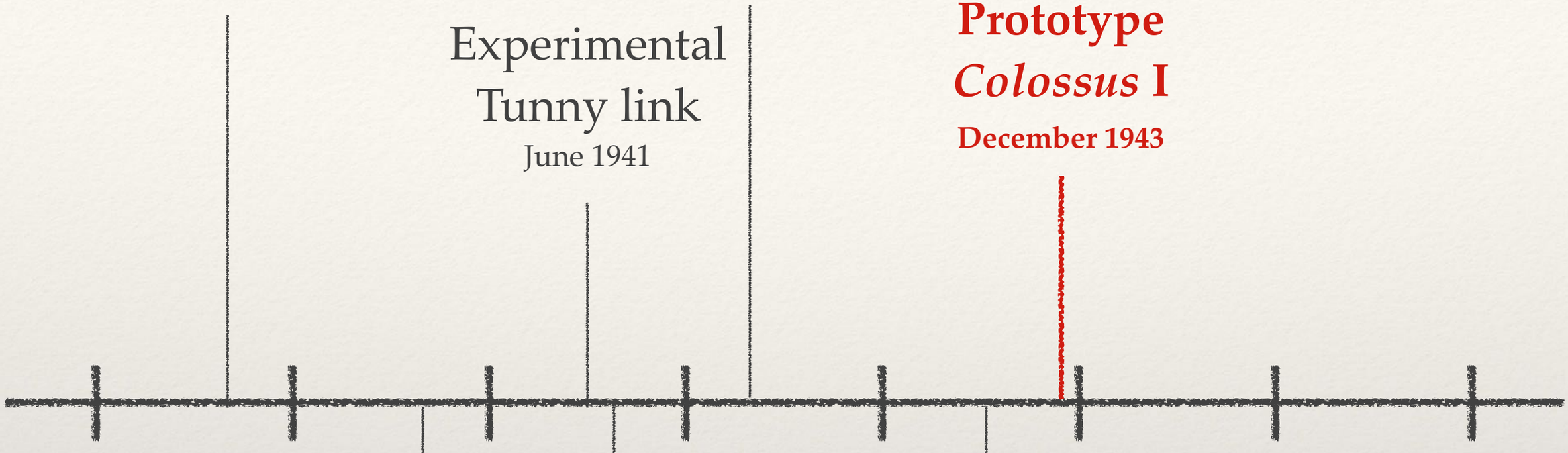
January 1942

Experimental Tunny link

June 1941

Prototype *Colossus* I

December 1943



August 1941

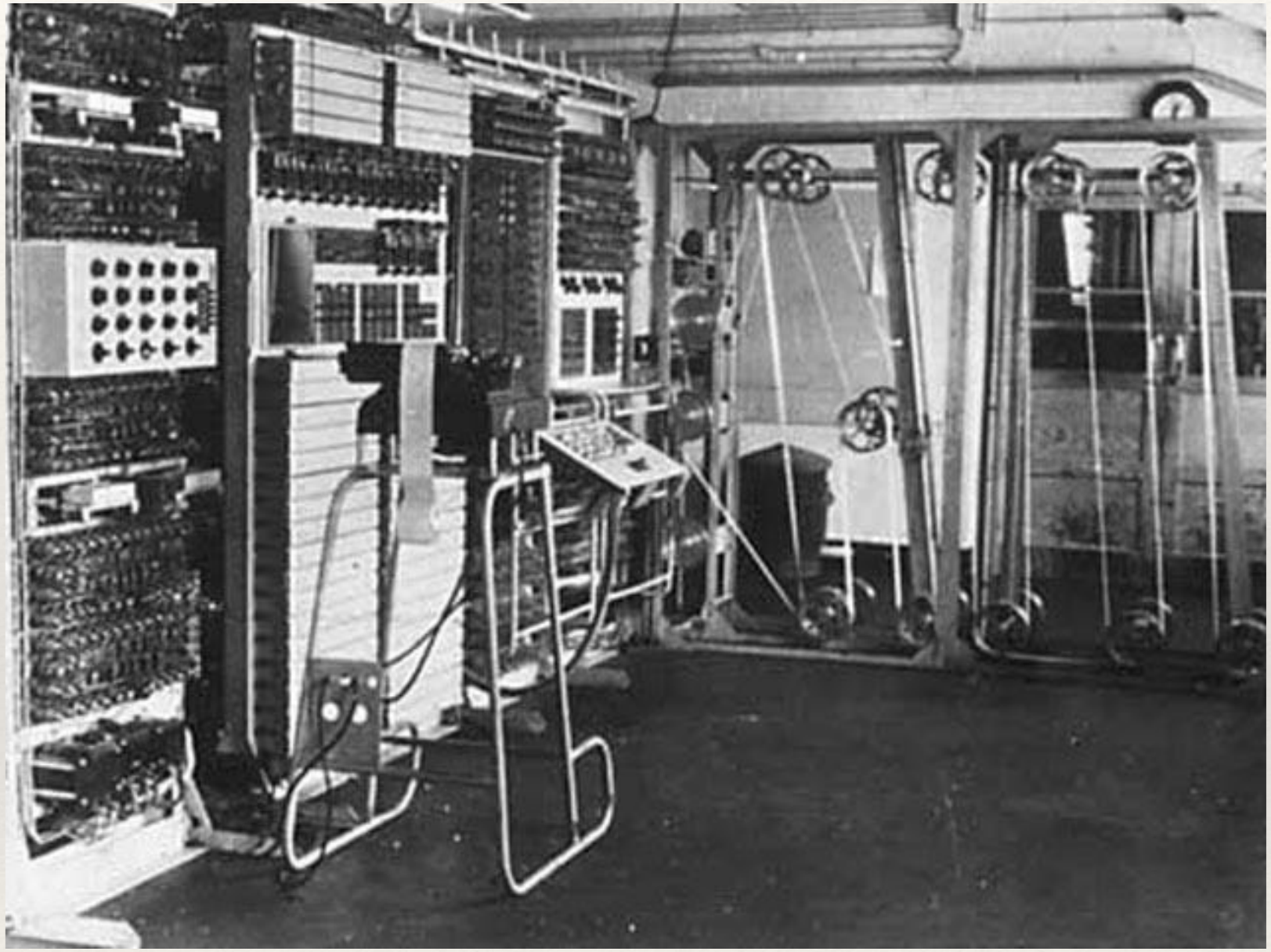
The German mistake

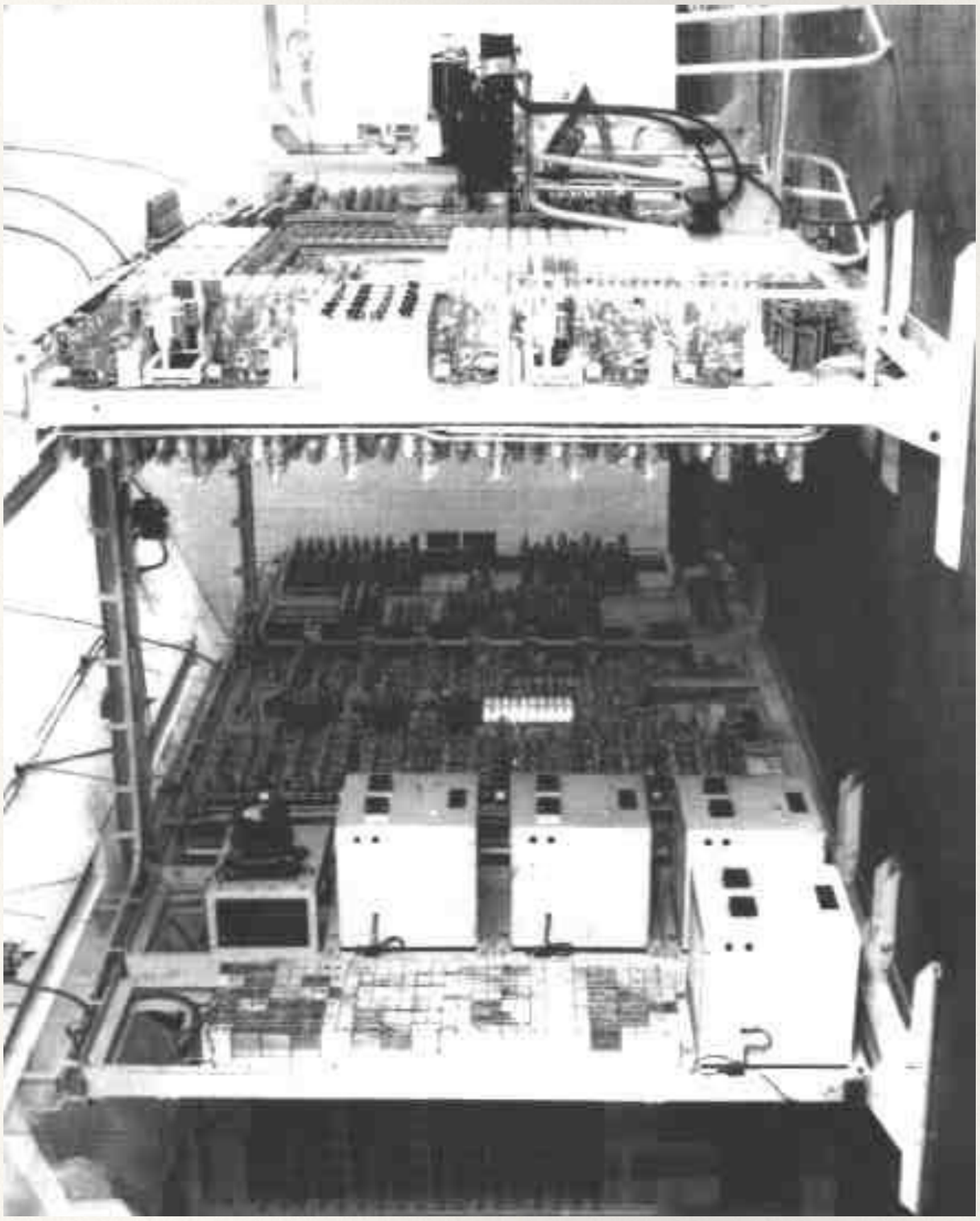
June 1943

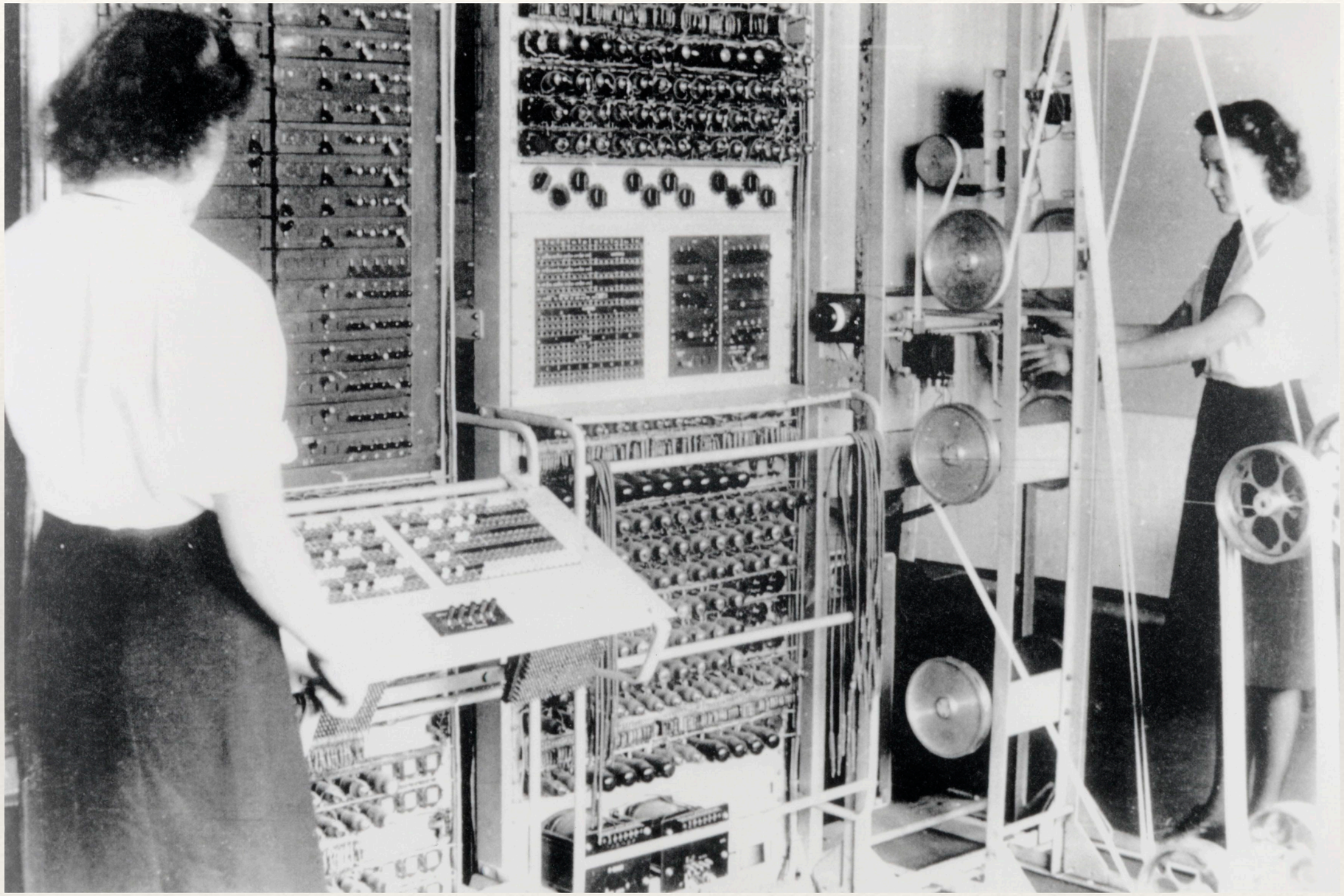
Heath Robinson delivered

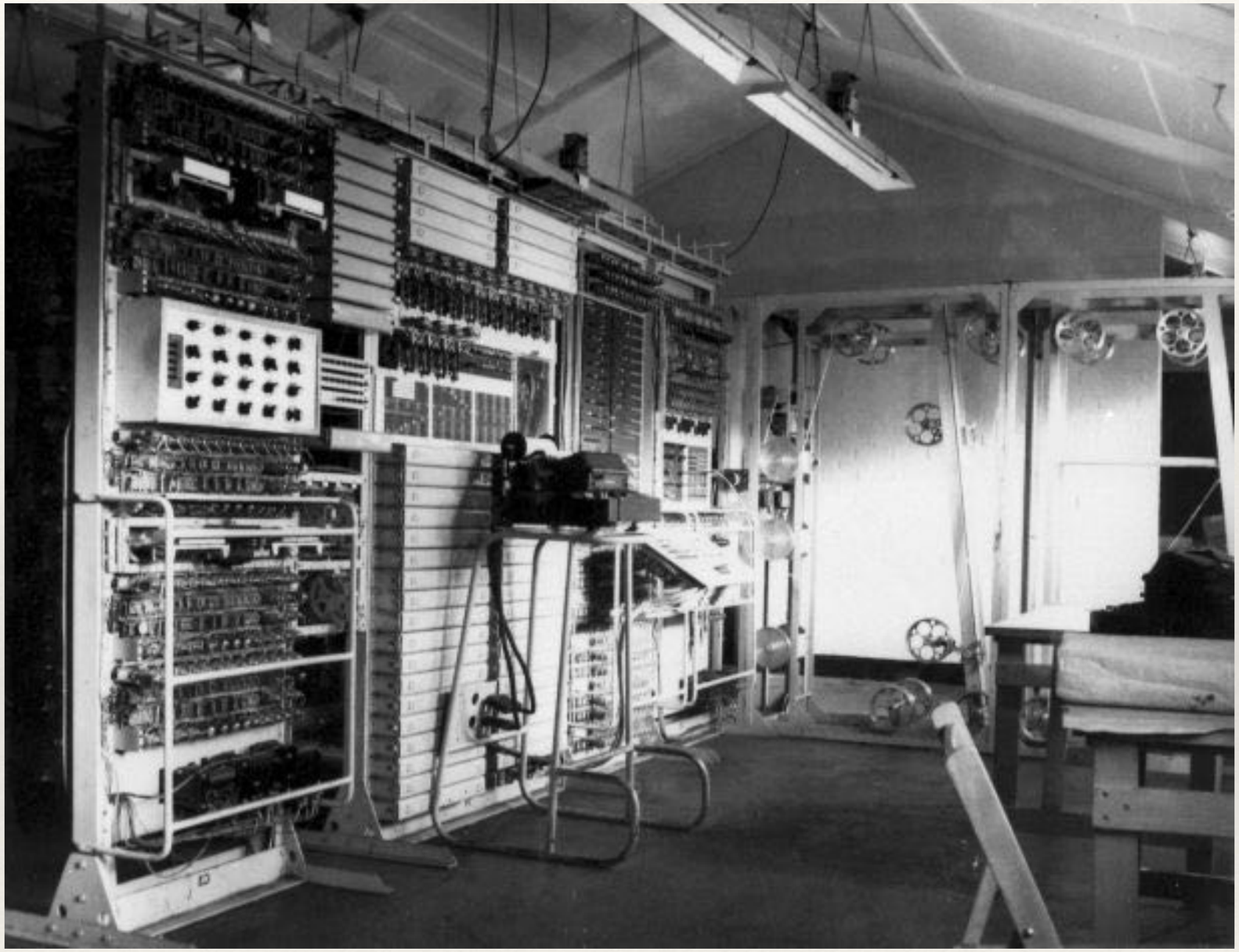
Late 1940

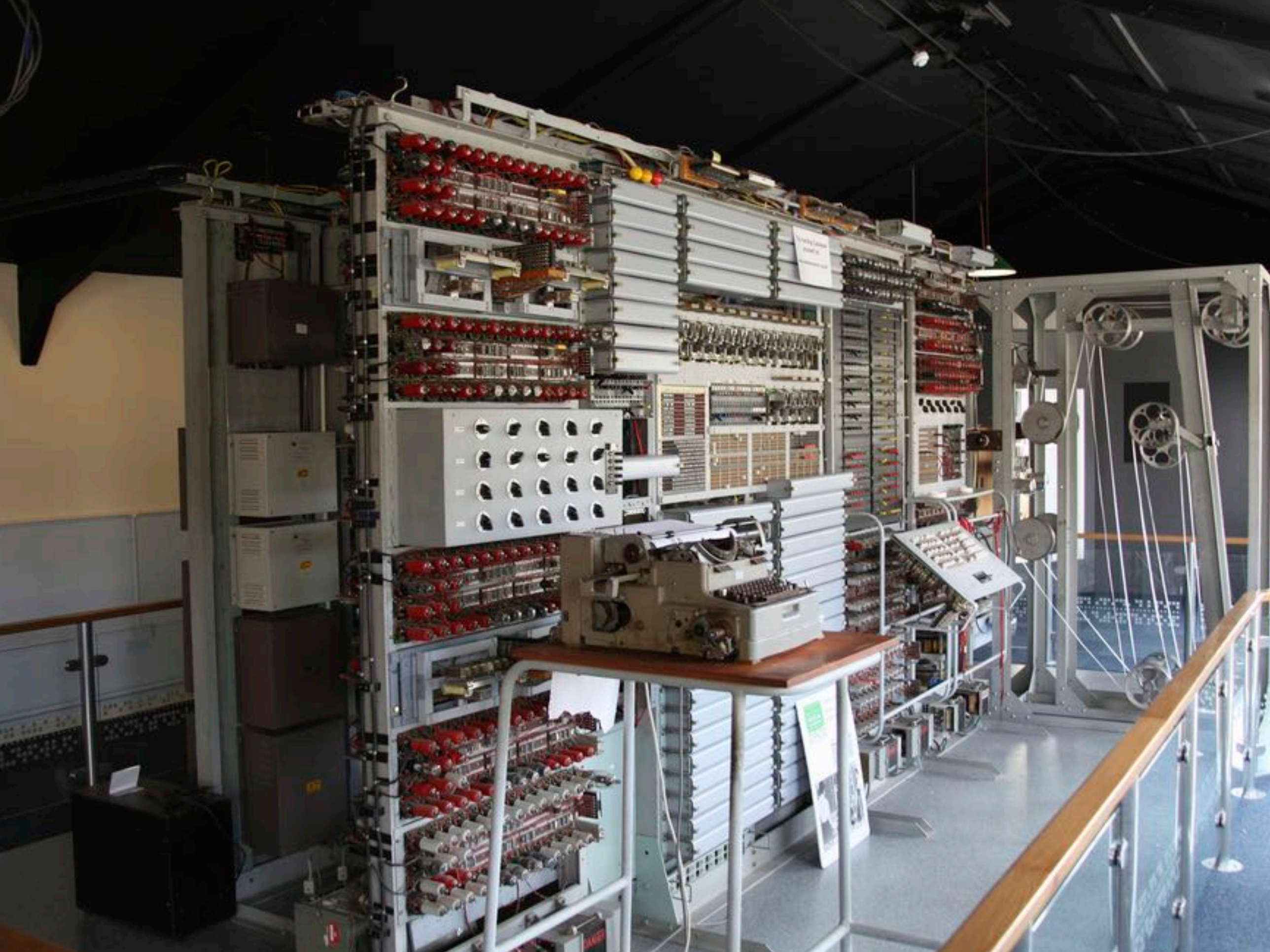
Non-morse transmissions intercepted in Britain

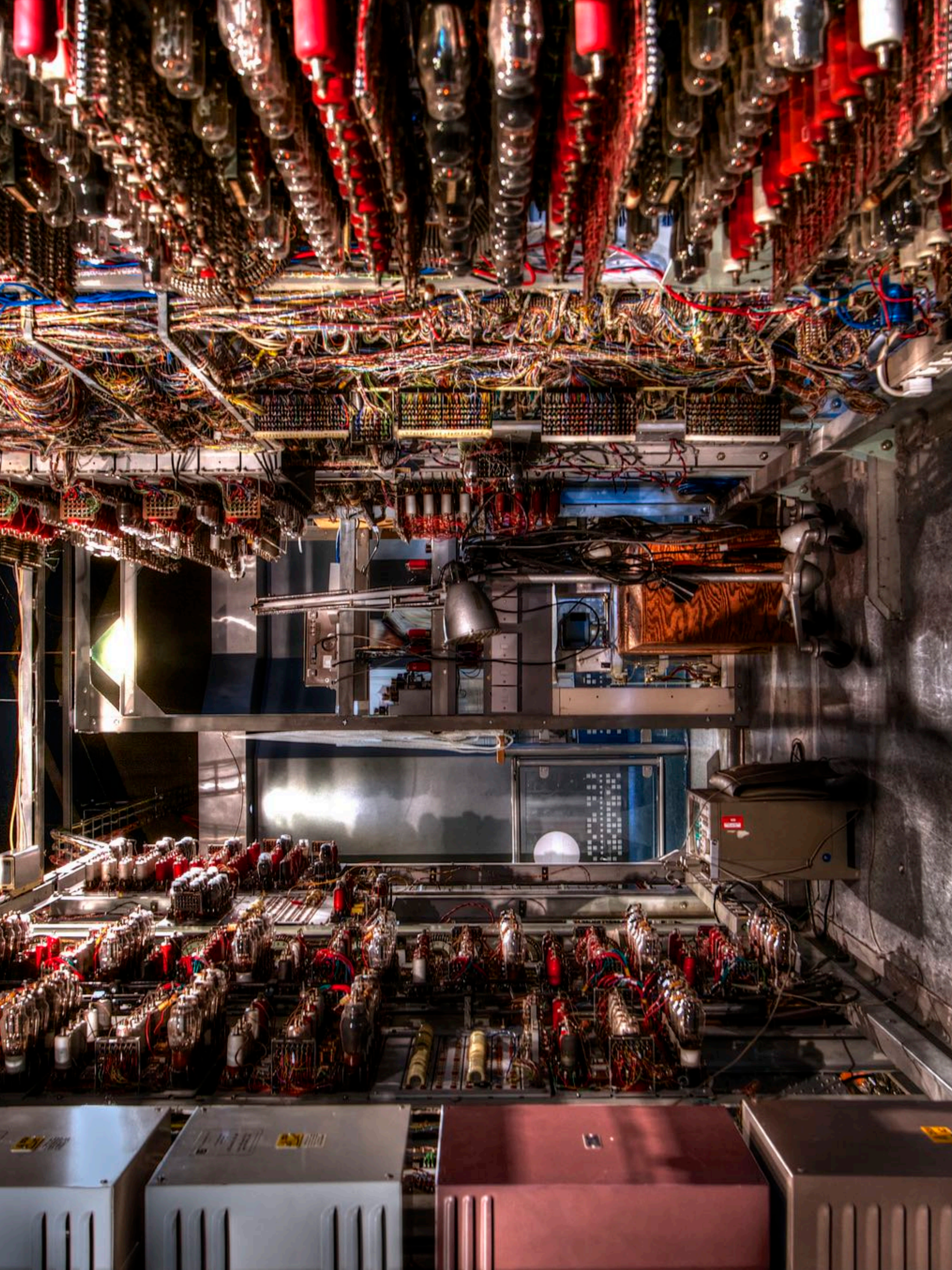


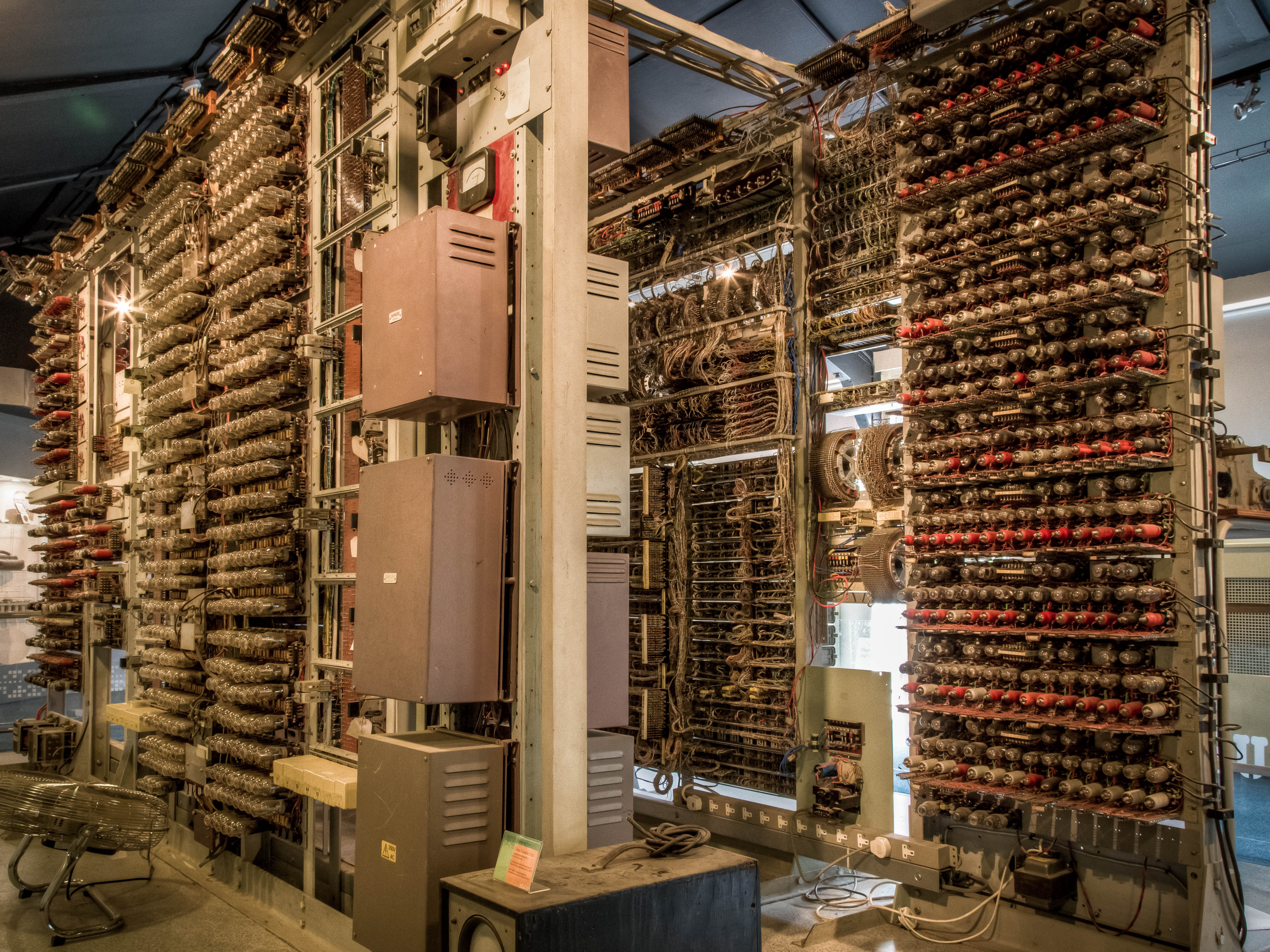












Codebreakers arrive at Bletchley Park

August 1939

Complete analysis of Tunny

January 1942

Experimental Tunny link

June 1941

Prototype *Colossus* I

December 1943

1939 1940 1941 1942 1943 1944 1945 1946

August 1941

The German mistake

June 1943

Heath Robinson delivered

Late 1940

Non-morse transmissions intercepted in Britain

June 1944

***Colossus* II & D-Day**

Codebreakers arrive at Bletchley Park

August 1939

Complete analysis of Tunny

January 1942

Experimental Tunny link

June 1941

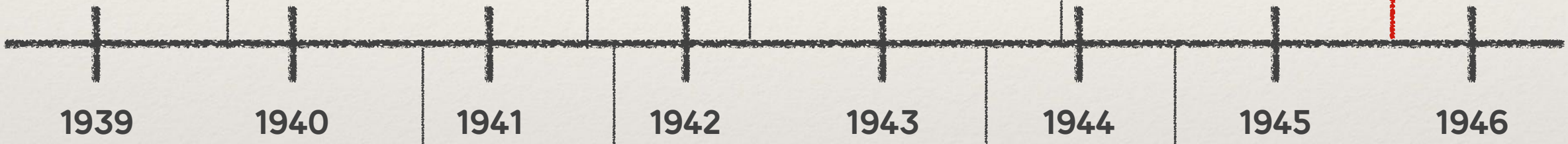
Prototype *Colossus* I

December 1943

Ten Colossi at Bletchley

End of the war

June 1945



August 1941

The German mistake

June 1943

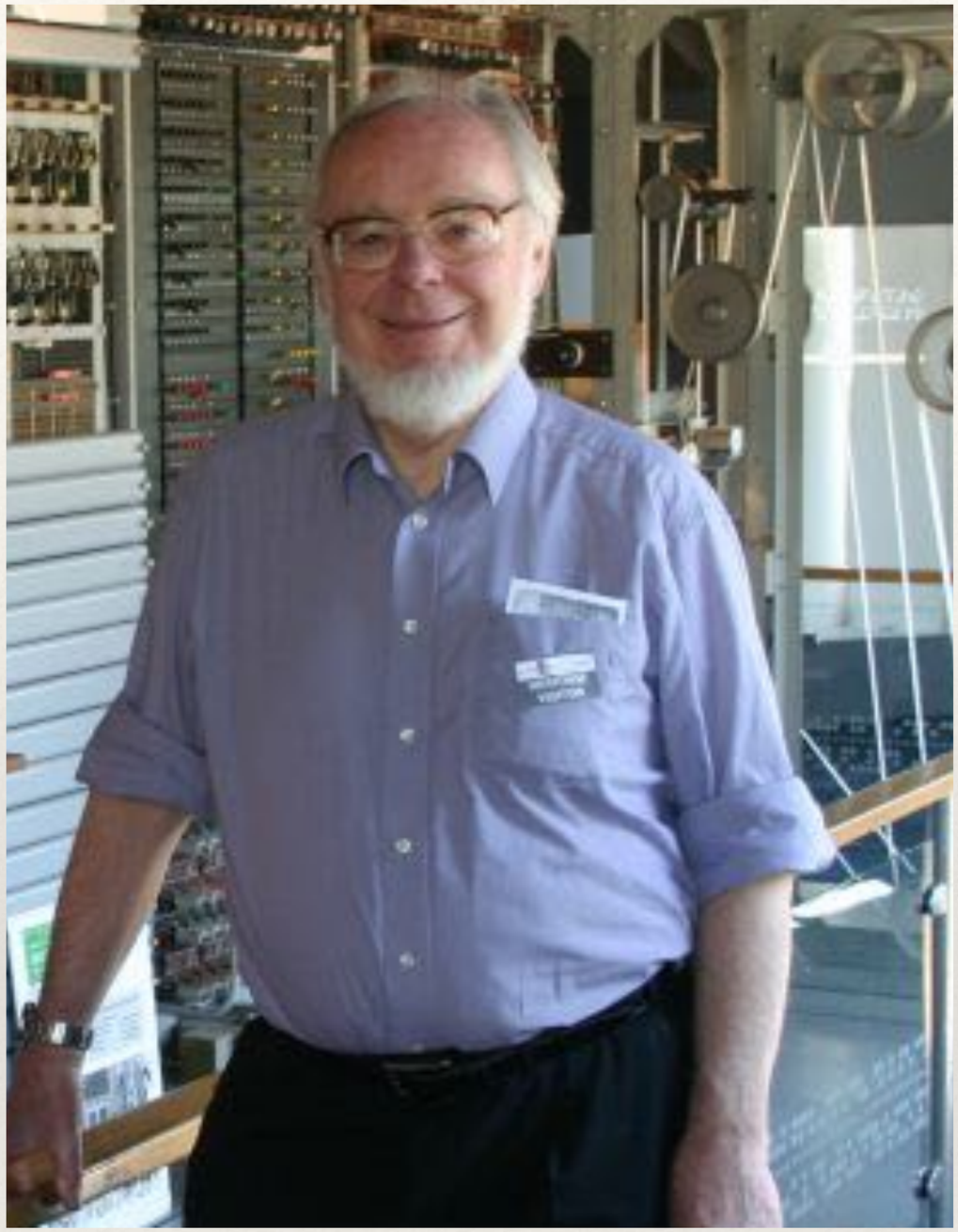
Heath Robinson delivered

Late 1940

Non-morse transmissions intercepted in Britain

June 1944

Colossus II *&* D-Day



Brian Randell

Tony Sale


THE
NATIONAL
MUSEUM
OF COMPUTING

Colossus

The codebreaking computer from Bletchley Park