Enigma, a Máquina e a Cifra

António Machiavelo

Centro de Matemática da Universidade do Porto
Departamento de Matemática da Faculdade de Ciências do Porto

Colóquios de Matemática

Universidade do Minho

12/10/2012

A máquina Enigma

Inventada em 1918, pelo engenheiro electrotécnico alemão Arthur Scherbius (1878–1929).

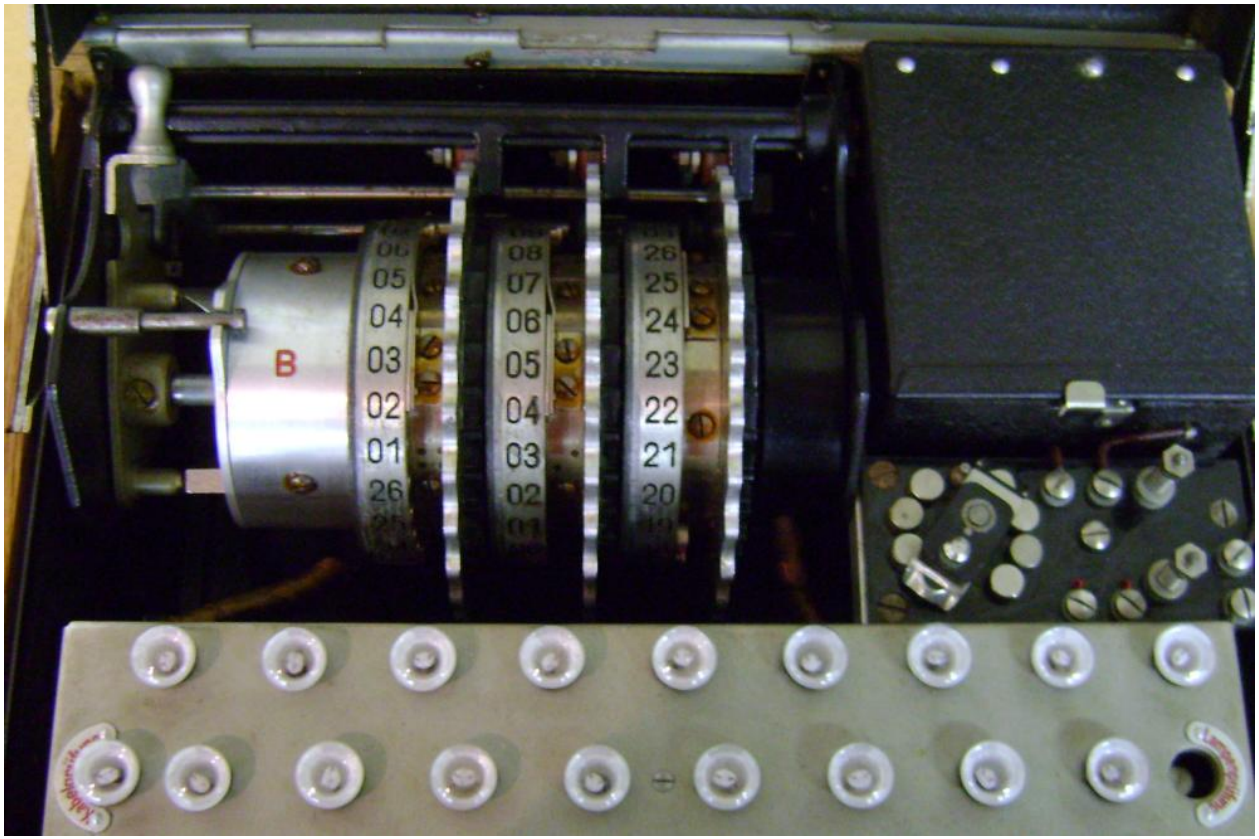
Comercializada a partir de 1923, com o nome de *Enigma*, será remodelada por diversas vezes, vindo a versão D a ser usada, a partir de 1927, para fins comerciais, diplomáticos e militares.

Em particular, a Enigma D foi usada na guerra civil espanhola.

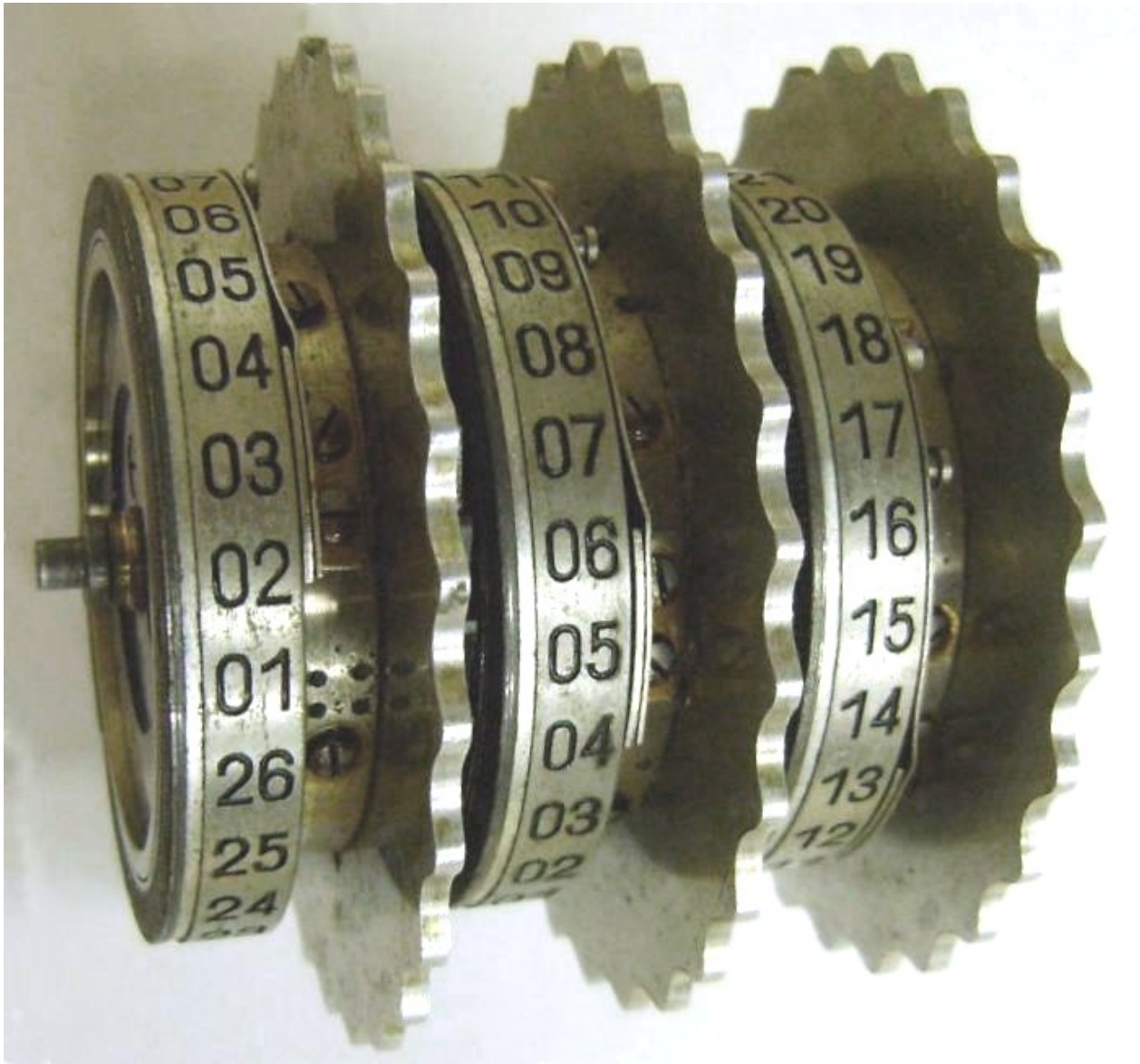
Versões um pouco mais sofisticadas foram usadas por várias unidades do exército, da força aérea e da marinha alemãs durante a segunda guerra mundial.

Uma enigma no campo de batalha

Os rotores

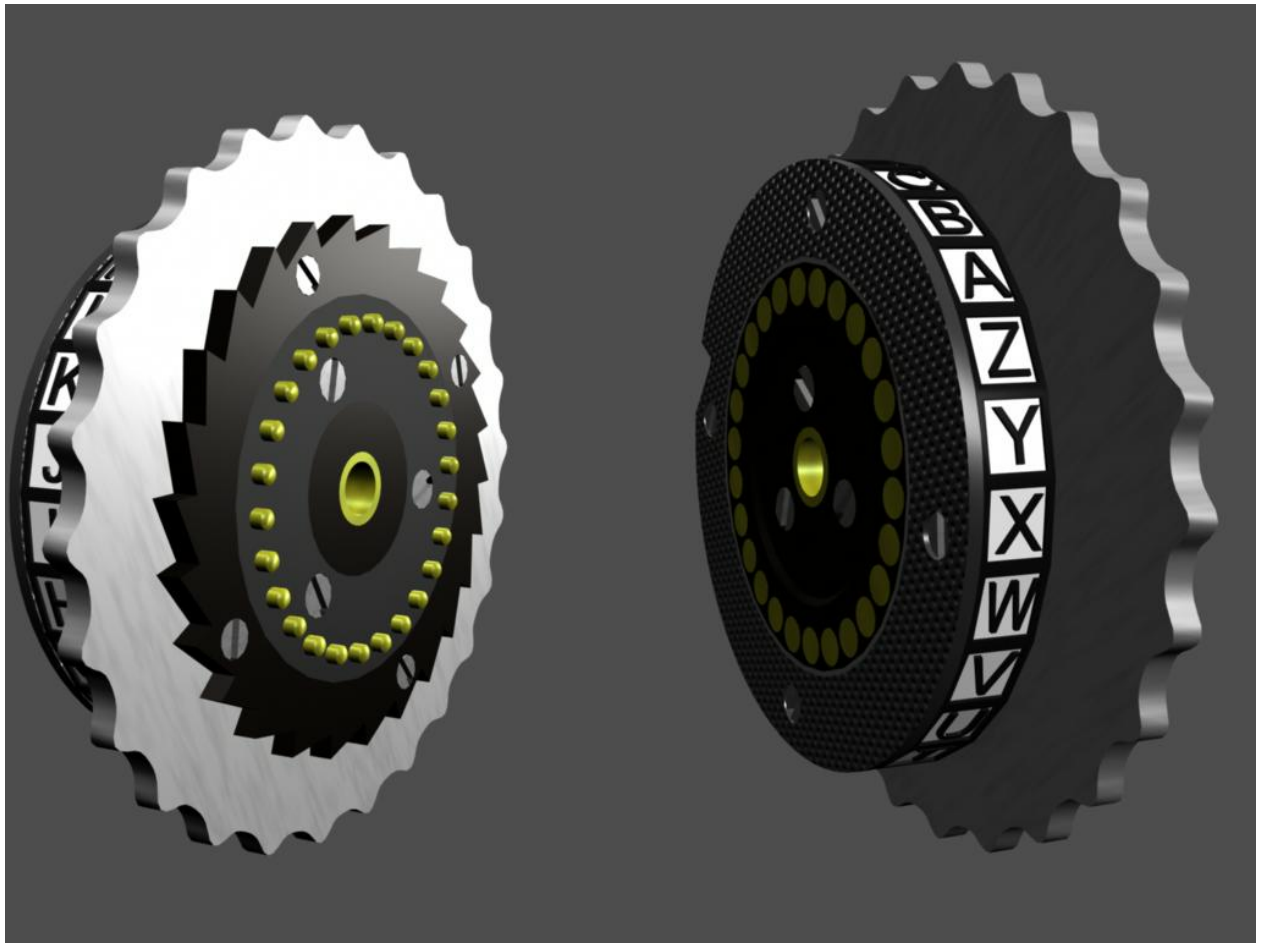


Os rotores


06
05
04
03
02
01
26
25
24
10
09
08
07
06
05
04
03
02
20
19
18
17
16
15
14
13
12

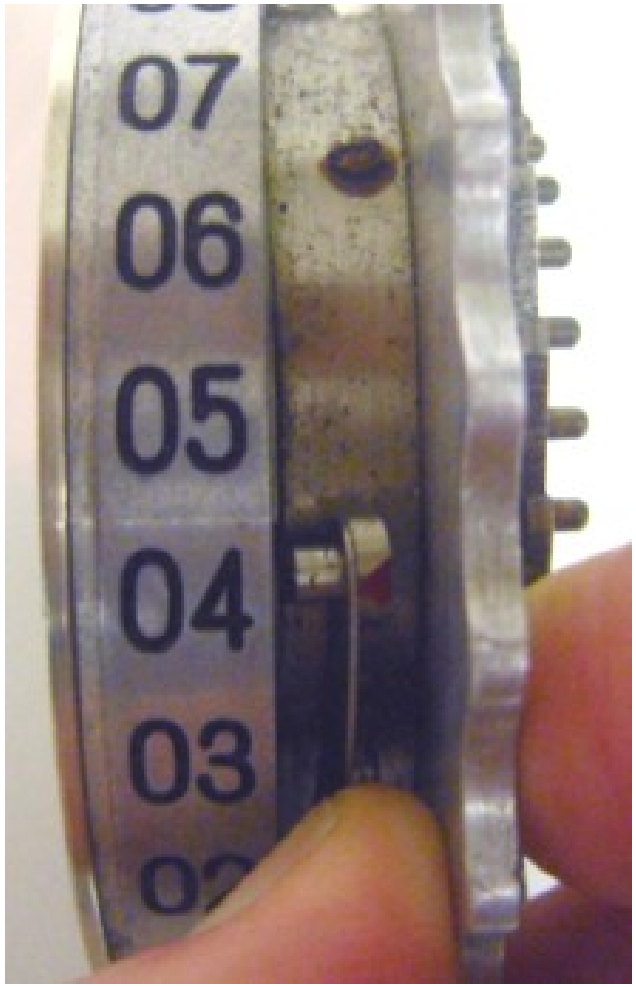
Os rotores

Os rotores



Mostrar animação...

Os rotores



Caixa de rotores

As permutações dadas por rotores e reflectores

$$
\begin{aligned}
\text{rotor I} &= (\texttt{AELTPHQXRU})(\texttt{BKNW})(\texttt{CMOY})(\texttt{DFG})(\texttt{IV})(\texttt{JZ})(\texttt{S}) \\
\text{rotor II} &= (\texttt{A})(\texttt{BJ})(\texttt{CDKLHUP})(\texttt{ESZ})(\texttt{FIXVYOMW})(\texttt{GR})(\texttt{NT})(\texttt{Q}) \\
\text{rotor III} &= (\texttt{ABDHPEJT})(\texttt{CFLVMZOYQIRWUKXSG})(\texttt{N}) \\
\text{rotor IV} &= (\texttt{AEPLIYWCOXMRFZBSTGJQNH})(\texttt{DV})(\texttt{KU}) \\
\text{rotor V} &= (\texttt{AVOLDRWFIUQ})(\texttt{BZKSMNHYC})(\texttt{EGTJPX})
\end{aligned}
$$

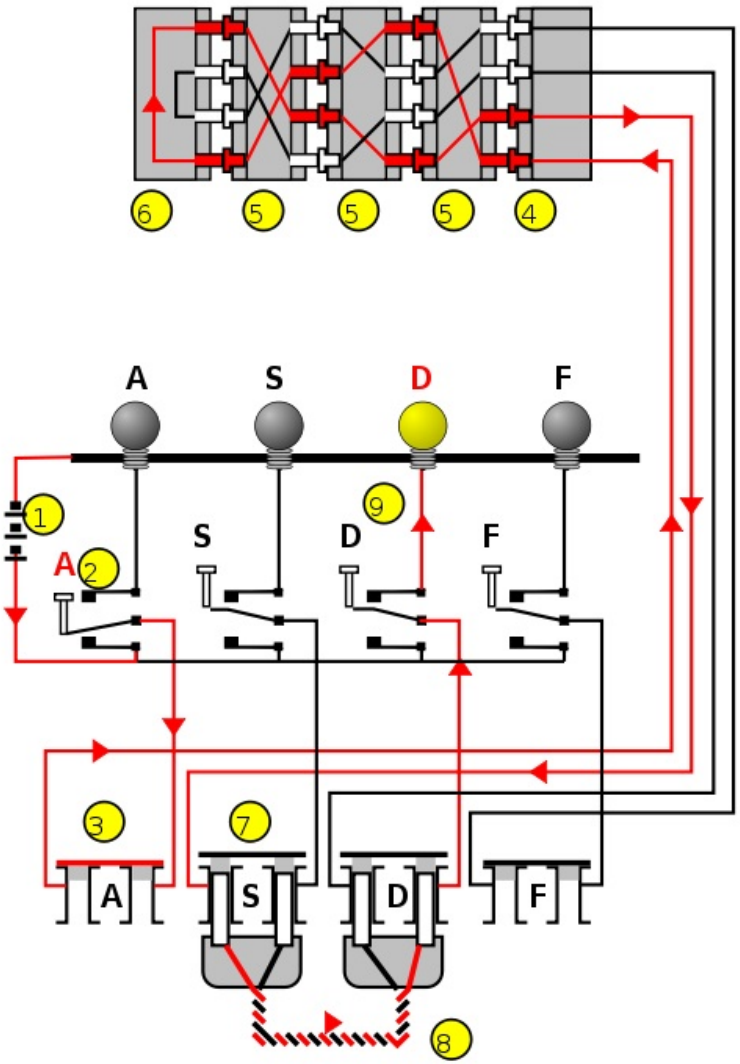
Dois reflectores comuns eram os seguintes:

$$
\begin{aligned}
\text{reflector B} &= (\texttt{AY})(\texttt{BR})(\texttt{CU})(\texttt{DH})(\texttt{EQ})(\texttt{FS})(\texttt{GL})(\texttt{IP})(\texttt{JX})(\texttt{KN})(\texttt{MO})(\texttt{TZ})(\texttt{VW}) \\
\text{reflector C} &= (\texttt{AF})(\texttt{BV})(\texttt{CP})(\texttt{DJ})(\texttt{EI})(\texttt{GO})(\texttt{HY})(\texttt{KR})(\texttt{LZ})(\texttt{MX})(\texttt{NW})(\texttt{TQ})(\texttt{SU})
\end{aligned}
$$

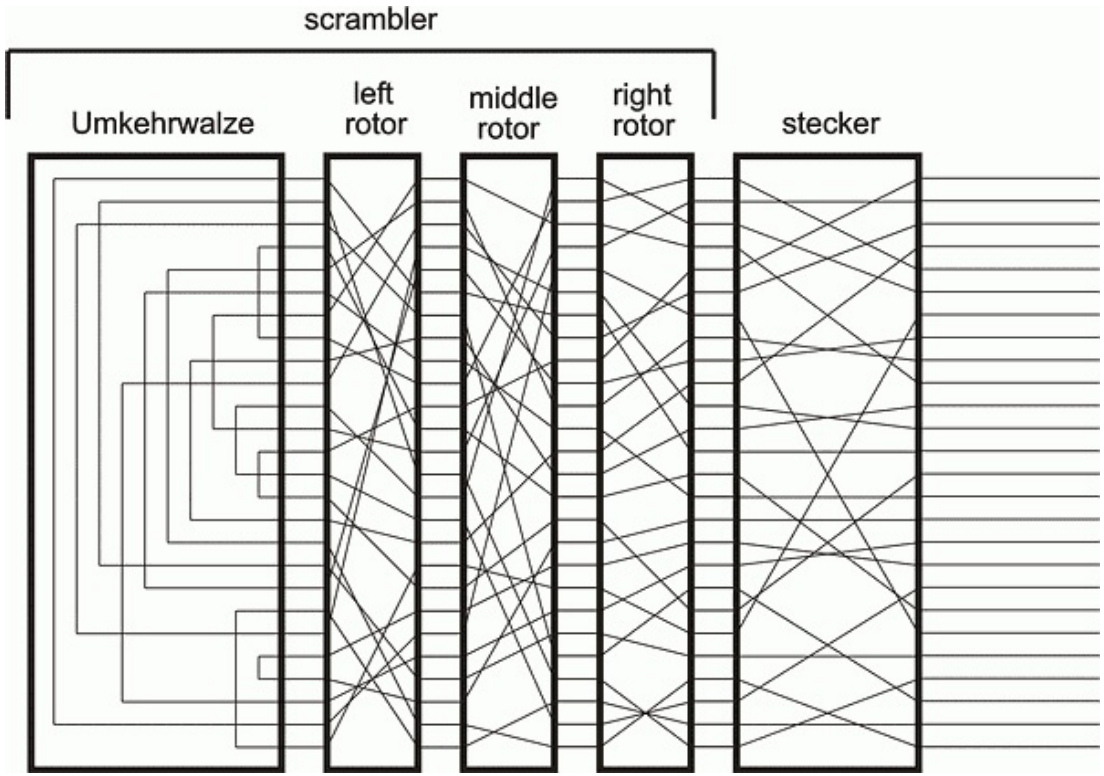
O "plugboard"

O "plugboard"

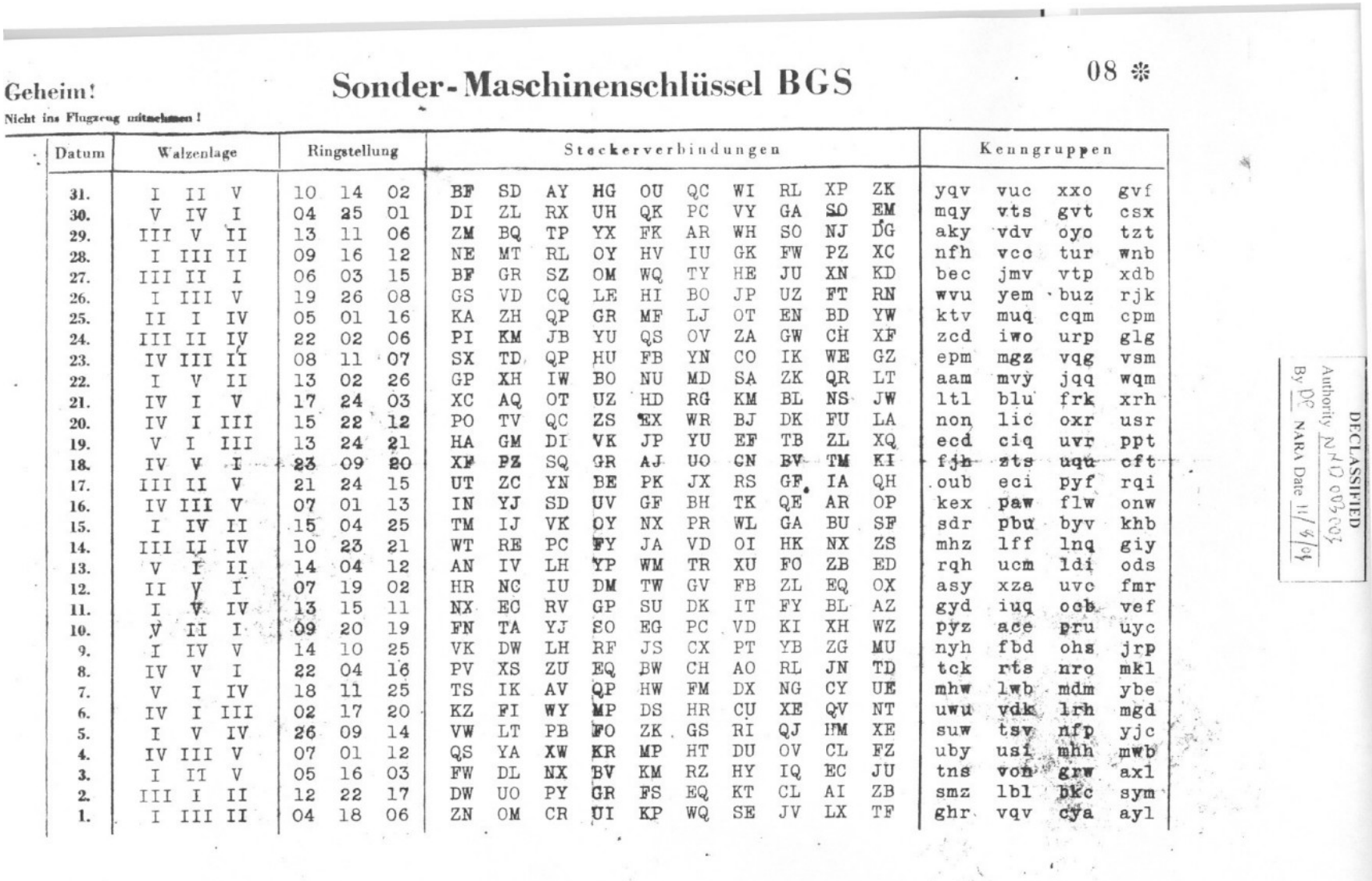
Esquema global



Esquema global



Chaves diárias



Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vcc tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ FM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

Chave e modo de operação

Chave do Dia: (depende do dia e do discriminante)

- Ordem dos rotores;
- A posição dos anéis exteriores relativamente ao cilindro central dos rotores — *ring setting*;
- As ligações no "plugboard".

Chave da Mensagem: (escolhida pelo operador)

- Escolher três letras aleatoriamente — p.ex. `QHP` — *indicator setting*;
- Rodar os rotores de modo a essas letras serem visíveis nas respectivas ranhuras;
- Escolher outras três letras ao acaso — p.ex. `MPR` — *text setting*;
- Carregar nas respectivas teclas (`MPR`) e anotar as três letras que se acendiam, digamos `WSX`;
- Voltar a colocar os rotores nas posições `MPR`.

Informação enviada no início da mensagem: discriminante, `QHP` e `WSX`.

Um criptograma

Informação dada pelo Operador de Intercepção

a. Frequência: 4760 KHz
b. Hora de intercepção: 11:10

Preâmbulo não Cifrado

1. Sinais de chamada: P7J a SF9 e 5KQ
2. Hora de origem: 10:30
3. Número de letras: 114
4. Única ou parte: parte 2 de 4
5. Discriminante: QXT
6. Indicador: VIN

Texto Cifrado

WQ S E U	P M P I Z	T L J J U	WQ E H G	L R B I D
F E W B O	J I E P D	J A Z H T	T B J R O	A H H Y O
J Y G S F	H Y K T N	T D B P H	U L K O H	U N T I M
O F A R L	B P A P M	X K Z Z X	D T S X L	Q W H V L
R A G U Z	Z T S G G	Y I J V		

Bletchley Park

Alguns matemáticos em Bletchley Park

A complexidade do problema

Número total de posições dos rotores:

$$26^3 = 17576$$

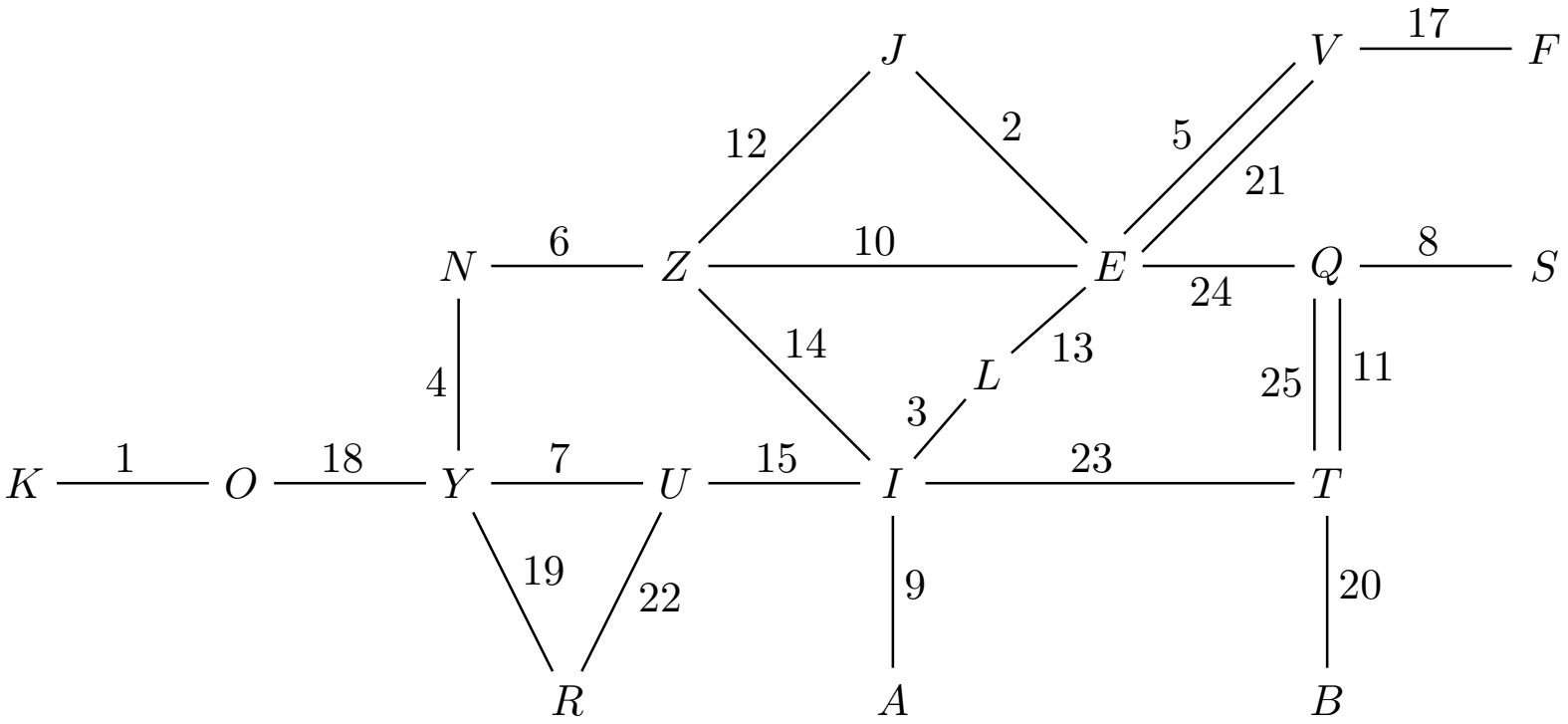
Número total de possíveis ligações do *plugboard*:

$$\frac{1}{10!}\binom{26}{2}\binom{24}{2}\cdots\binom{8}{2} = 150\,738\,274\,937\,250$$

Cábulas e menus

K E I N E Z U S A E T Z E Z U M V O R B E R I Q T
O J L Y V N Y Q I Z Q J L I I W F Y Y T V U T E Q

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



Uma observação crucial

Seja:

- Σ_k a permutação induzida pela Enigma quando cifra a k-ésima letra da mensagem;
- Γ_k a permutação induzida pelo conjunto dos rotores e reflector;
- π a permutação induzida pelo *plugboard*.

Tem-se:

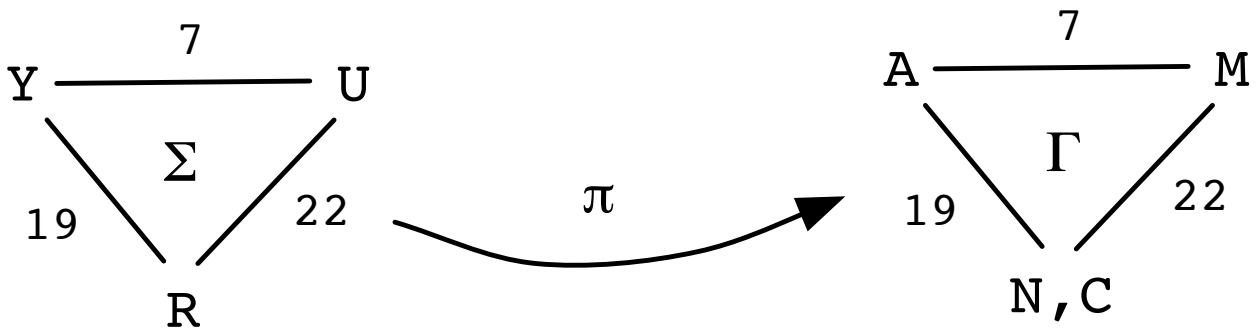
$$\Sigma_k = \pi \circ \Gamma_k \circ \pi \iff \Gamma_k = \pi \circ \Sigma_k \circ \pi$$

Ou seja,

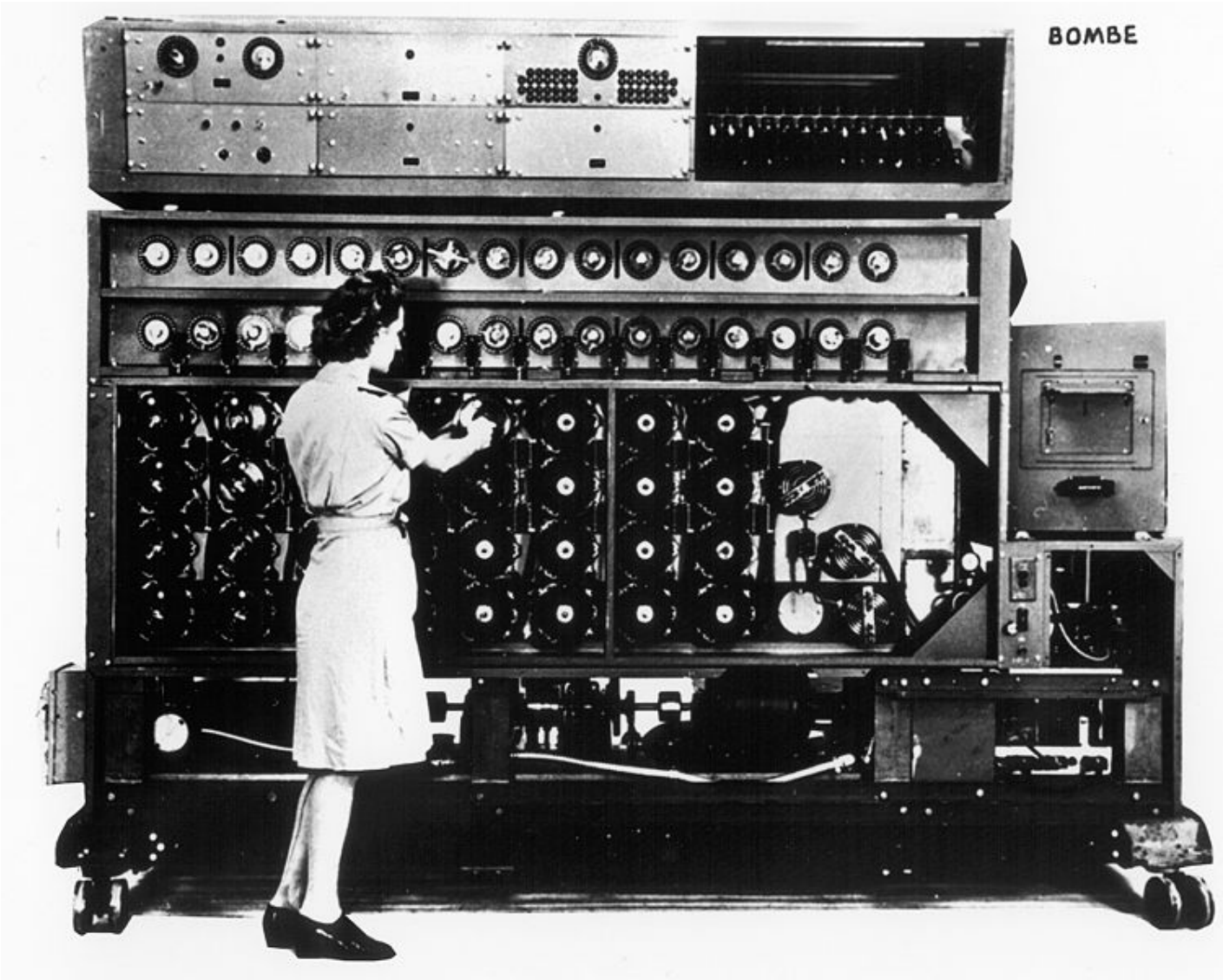
$$\begin{array}{ccc} \mathtt{Y} & \xrightarrow{\Sigma_7} & \mathtt{U} \\ \downarrow \pi & & \downarrow \pi \\ \mathtt{A} & \xrightarrow{\Gamma_7} & \mathtt{I} \end{array}$$

Uma observação crucial

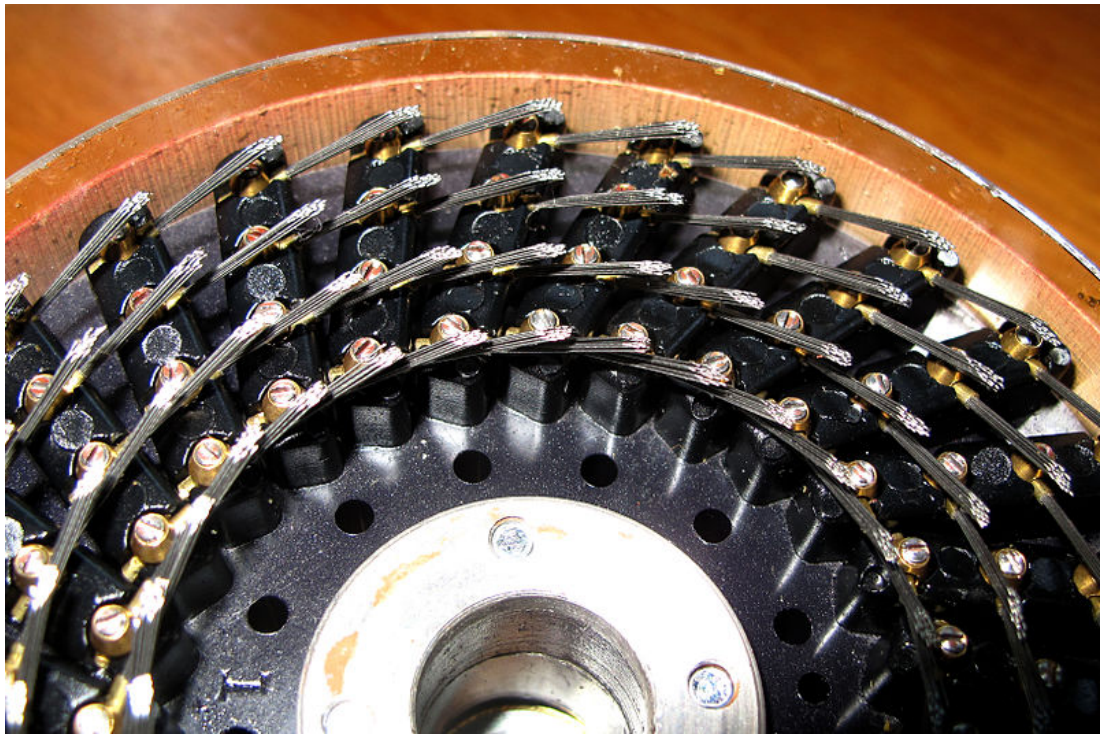
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Γ_7	M	R	V	I	Z	O	Y	X	D	U	N	W	A	K	F	T	S	B	Q	P	J	C	L	H	G	E
Γ_{19}	N	H	D	C	M	O	L	B	W	T	S	G	E	A	F	Z	V	U	K	J	R	Q	I	Y	X	P
Γ_{22}	V	S	M	Y	F	E	O	W	L	R	P	I	C	X	G	K	T	J	B	Q	Z	A	H	N	D	U



A "bomba" inglesa



A “bomba” inglesa



Harold Hall “Doc” Keen (1894–1973)

Um problema interessante

Com os devidos cuidados...

...será que a Enigma é segura?

Um enigma...

O jornalista e escritor Paul Gannon, afirma:

> *Turing was only one of the people who worked on the cipher problem for which Colossus was built and his role was tangential at best (indeed, Turing developed a hand or manual method of breaking the relevant cipher, not the machine method for which Colossus was invented).*

Enquanto que Peter Hilton, que trabalhou directamente com Turing em Bletchley Park, diz peremptoriamente:

> *It was Alan Turing who first appreciate the essential role which could be played in the elimination phase of the process by high-speed electronic machines, and who was, in fact, — and quite consciously and deliberately — inventing the computer as he designed first the "Bombe" and then the "Colossus" for our cryptanalytical purposes.*

Para saber um pouco mais...

- Peter Hilton, *Reminiscences of Bletchley Park, 1942–1945*, in Peter Duren (ed.), *A Century of Mathematics in America*, Vol. I, American Mathematical Society, 1988, pp. 291–301.
- Peter Hilton, *Working with Alan Turing*, The Mathematical Intelligencer, Vol. 13, No. 4 (1991), pp. 22–25.
- Peter Hilton, *Reminiscences and Reflections of a Codebreaker*, in W. D. Joyner (ed.), *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, Springer, 2000, pp. 1–8.
- F. H. Hinsley and Alan Stripp, Code Breakers, Oxford University Press, 1993.
- T. W. Körner, The Pleasures of Counting, Cambridge University Press, 1998.
- Bruno Ribeiro, A Criptanálise da Enigma: 1932–1939, Tese do Mestrado de Engenharia Matemática, Faculdade de Ciências da Universidade do Porto.
- Gordon Welchman, The Hut Six Story: breaking the Enigma codes, M & M Baldwin, 1998.