



2018/2019

# MÁQUINA ENIGMA

UC Criptografia

PROFESSORA ISABEL OITAVEM



Iuri Simões, Nº 47897, MIEGI  
Pedro Rodrigues, Nº 48614, MIEGI

# SÍNTSE



Fonte: BBC News, Warsaw



$\sin \alpha = BC = \frac{a}{c};$   
 $\cos \alpha = OB = \frac{b}{c};$   
 $\operatorname{tg} \alpha = OB = \frac{b}{a};$   
 $\operatorname{ctg} \alpha = OA = \frac{a}{b};$

$\alpha^{\circ} = \frac{180}{\pi} \alpha; \quad \alpha = \frac{\pi}{180} \alpha^{\circ};$   
 $360^{\circ} = 2\pi; \quad 180^{\circ} = \pi;$

$\sin^2 \alpha + \cos^2 \alpha = 1;$   
 $\frac{\sin \alpha}{\cos \alpha} = \operatorname{tg} \alpha;$   
 $\sin \alpha \cdot \csc \alpha = 1;$

$\frac{\cos \alpha}{\sin \alpha} = \operatorname{ctg} \alpha$

$\sin \alpha = a \sin \omega t; \quad u = a \sin \omega t + b \cos \omega t$

$\cos \alpha = b \cos \omega t; \quad x = -\frac{b}{a} \cos \omega t$

$\operatorname{tg} \varphi = \frac{a}{b} \alpha^2; \quad \Delta = 4ac - b^2; \quad a > 0;$

# SEGUNDA GUERRA MUNDIAL E CRIPTOGRAFIA



2<sup>a</sup> Guerra Mundial



# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

Primeira patente para a Enigma, por *Arthur Scherbius*



*Arthur Scherbius*

# ACONTECIMENTOS



Fevereiro

Marinha Alemã começa a usar a Enigma



# ACONTECIMENTOS



15 de Julho

Exército Alemão começa a usar a enigma

Departamento de Criptografia Polaco (*Biuro Szyfrow*)  
reconhece o uso da Enigma pelos alemães



## ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

*Biuro Szyfrow adquire uma cópia da Enigma*

## ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

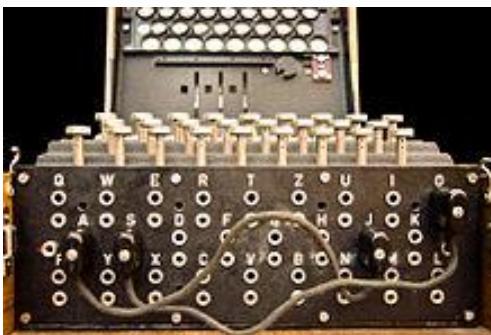
 *Biuro Szyfrow* organiza um curso de criptografia para cerca de 20 estudantes de matemática

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

1 de Junho

Exército Alemão acrescenta uma *plugboard* e a máquina  
começa a ser usada na sua forma final



# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

## Outubro

Departamento Criptográfico Alemão envia documentos aos Serviços Secretos Franceses (S.R.F.)

## 8 de Novembro

S.R.F. recebe os primeiros documentos secretos alemães

## Novembro – Dezembro

Departamento Criptográfico francês declara a Enigma inquebrável e fornece os documentos aos Britânicos

## 7 – 11 de Dezembro

Diretor do S.R.F. fornece os documentos a *Biuro Szyfrow* e França e Polónia concordam em partilhar informação

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940



Marian Rejewski



Jerzy Różycki



Henryk Zygalski

**1 Setembro**

Os 3 melhores alunos do curso de criptografia polaco são contratados para criptoanalisar a Enigma

Criação de um modelo matemático de permutações

**Dezembro**

S.R.F consegue obter as configurações iniciais da máquina. Informação é partilhada com os Polacos e avanços foram feitos no modelo matemático → descoberta das ligações internas dos rotores

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

Polacos desenvolvem o Método da Grelha

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

Construída a primeira réplica da Enigma

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • **1935** • 1936 • 1937 • 1938 • 1939 • 1940

Polacos desenvolvem o **Método do Relógio**  
(permitia descobrir a configuração do rotor à direita)

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

Polacos desenvolvem o método **Ciclómetro**  
(permitia encontrar as configurações diárias)

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • **1937** • 1938 • 1939 • 1940

**1 de Novembro**

Alemães desenvolvem e implementam  
uma nova Placa Refletora



# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

15 de Setembro

Alemães alteram o procedimento da Enigma,  
inviabilizando todos os métodos desenvolvidos até então

Novembro

Polacos desenvolvem a *Bombe*

Novembro – Dezembro

Método das Folhas de Zygalsky, baseado na *Bombe*

15 de Dezembro

São introduzidos 2 novos rotores, passam a ser  
escolhidos 3 de um conjunto de 5

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

1 de Janeiro

Ligações na *Plugboard* passam a variar entre 7 e 10

25 – 26 de Julho

**Polacos entregam** replicas da máquina e **métodos desenvolvidos**  
aos **Franceses e Britânicos**

1 de Setembro

Invasão da Polónia marca **o início da Segunda Guerra Mundial**

Setembro – Outubro

Os 3 criptógrafos Polacos mudam-se para França, onde continuam  
a trabalhar na criptoanálise da Enigma

# ACONTECIMENTOS

1918 • 1926 • 1928 • 1929 • 1930 • 1931 • 1932 • 1933 • 1934 • 1935 • 1936 • 1937 • 1938 • 1939 • 1940

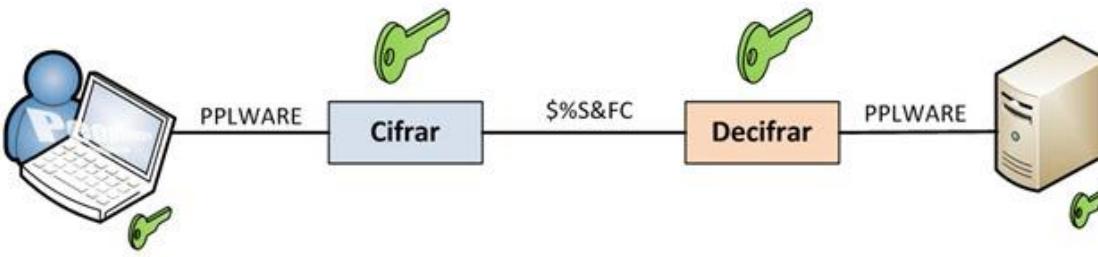


Maio

Criptógrafos Polacos retiram-se por força das invasões.  
Trabalho Polaco na criptoanálise da enigma termina

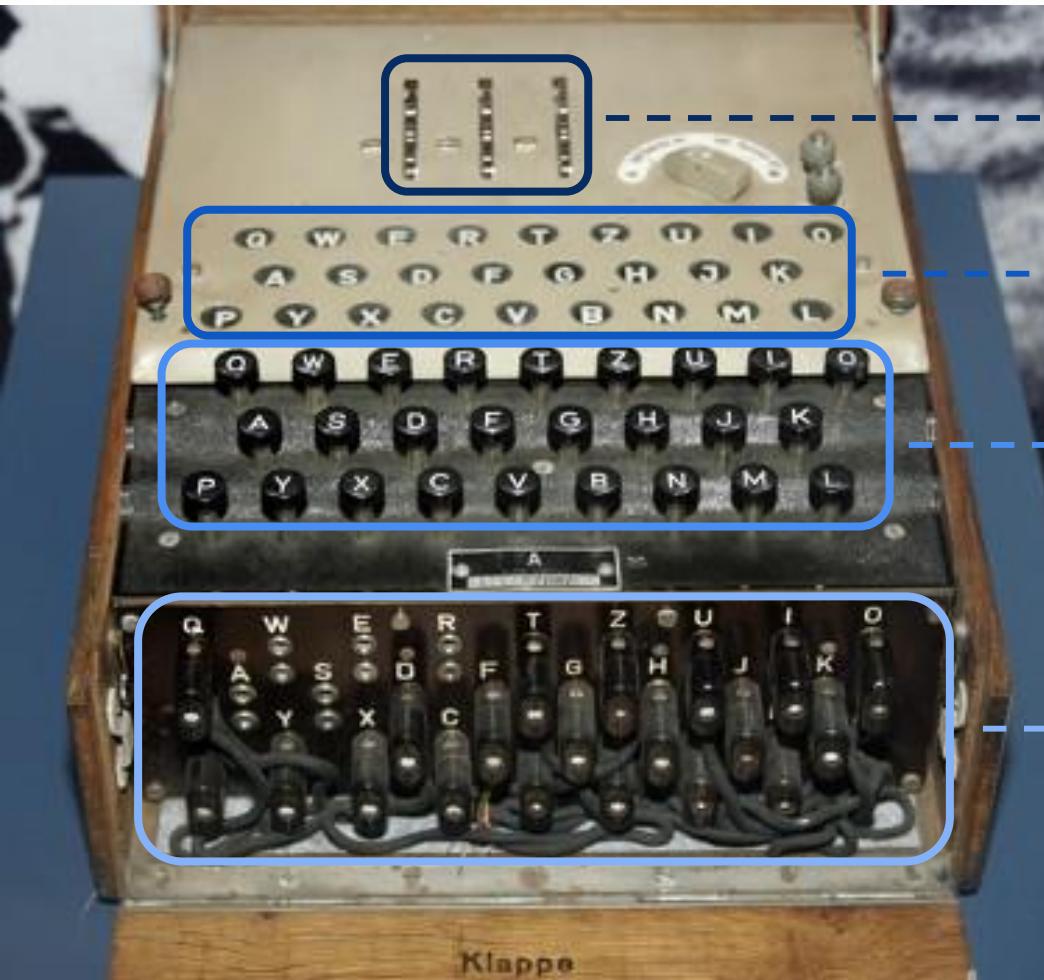
*Alan Turing* e a sua equipa **decifram a Enigma** com a  
**Bombe**

# ENIGMA – CRIPTOGRAFIA DE CHAVE SIMÉTRICA



- Mesma chave para encriptar e desencriptar a mensagem
- A Enigma desencripta uma mensagem através da mensagem original, se a máquina estiver na mesma configuração da máquina original.

# A MÁQUINA ENIGMA



3 Rotores + Placa reflectora

Painel retroiluminado

Teclado de escrever

Plugboard

# PLUGBOARD



- Permutação entre 2 letras
- 10 fios
  - Permuta 20 letras
  - 6 letras mantêm o seu valor
  - (Esta configuração “maximiza” o número de possibilidades)

# COMBINAÇÕES PLUGBOARD

Número de pares/fios	Número de possibilidades
1	325
2	44 850
3	3 453 450
4	164 038 875
5	5 019 589 575
6	100 391 791 500
7	1 305 093 289 500
8	10 767 019 638 375
9	58 835 098 191 875
10	<b>150 738 274 937 250</b>
11	205 552 193 096 250
12	102 776 096 548 125
13	7 905 853 580 625

## ROTORES



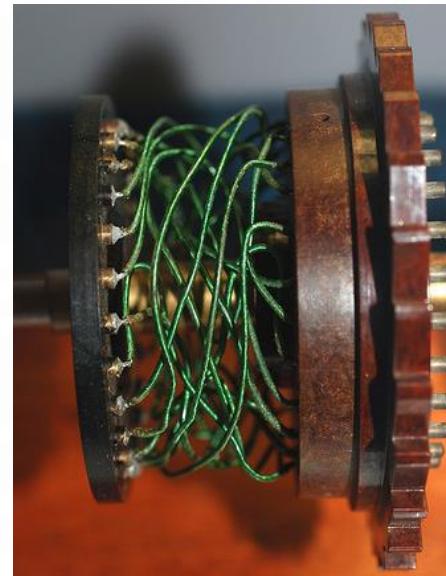
- 3 Rotores por Enigma (escolhidos de um conjunto de 5 rotores);
- Posições do rotor numeradas de 0 a 25;
- De cada lado do rotor existem **26 contactos elétricos** (cada contacto representa uma letra), logo o rotor efetua uma **substituição monoalfabética**;
- Movimentação dos rotores → Transformação criptográfica diferente em cada posição → **Substituição polialfabética**,

# ATRIBUIÇÃO DE CÓDIGOS ÀS LETRAS

Letra	a	b	c	d	e	f	g	h	i	j	k	l	m
Número	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	n	o	p	q	r	s	t	u	v	w	x	y	z
Número	13	14	15	16	17	18	19	20	21	22	23	24	25

# SUBSTITUIÇÕES EFETUADAS PELOS ROTORES

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

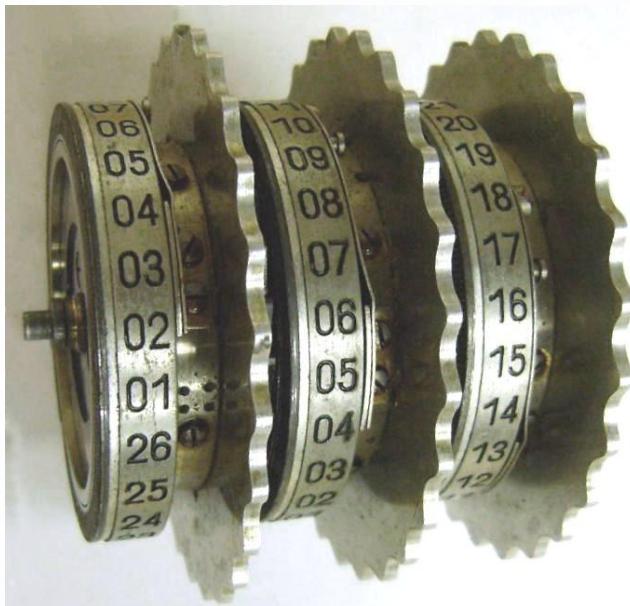


# MOVIMENTAÇÃO DOS ROTORES

Rotor 3

Roda 1/26 voltas por cada volta do rotor 2

(Rotor Lento)



Rotor 1

Roda 1/26 voltas sempre que é pressionada uma tecla

(Rotor Rápido)

Rotor 2

Roda 1/26 voltas por cada volta do rotor 1

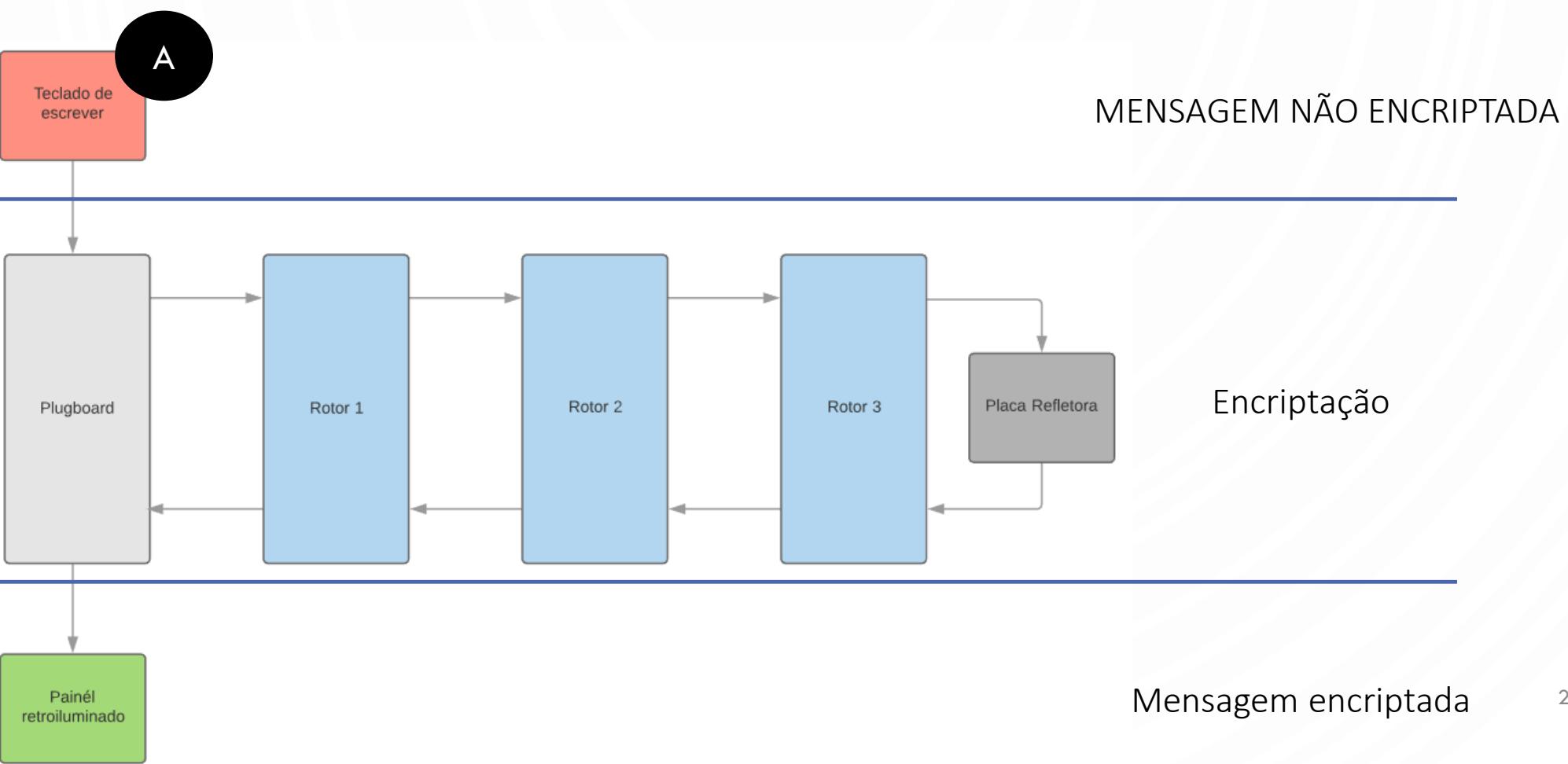
Roda ao mesmo tempo que o rotor 3 → Duplo passo

# PLACA REFLETORA

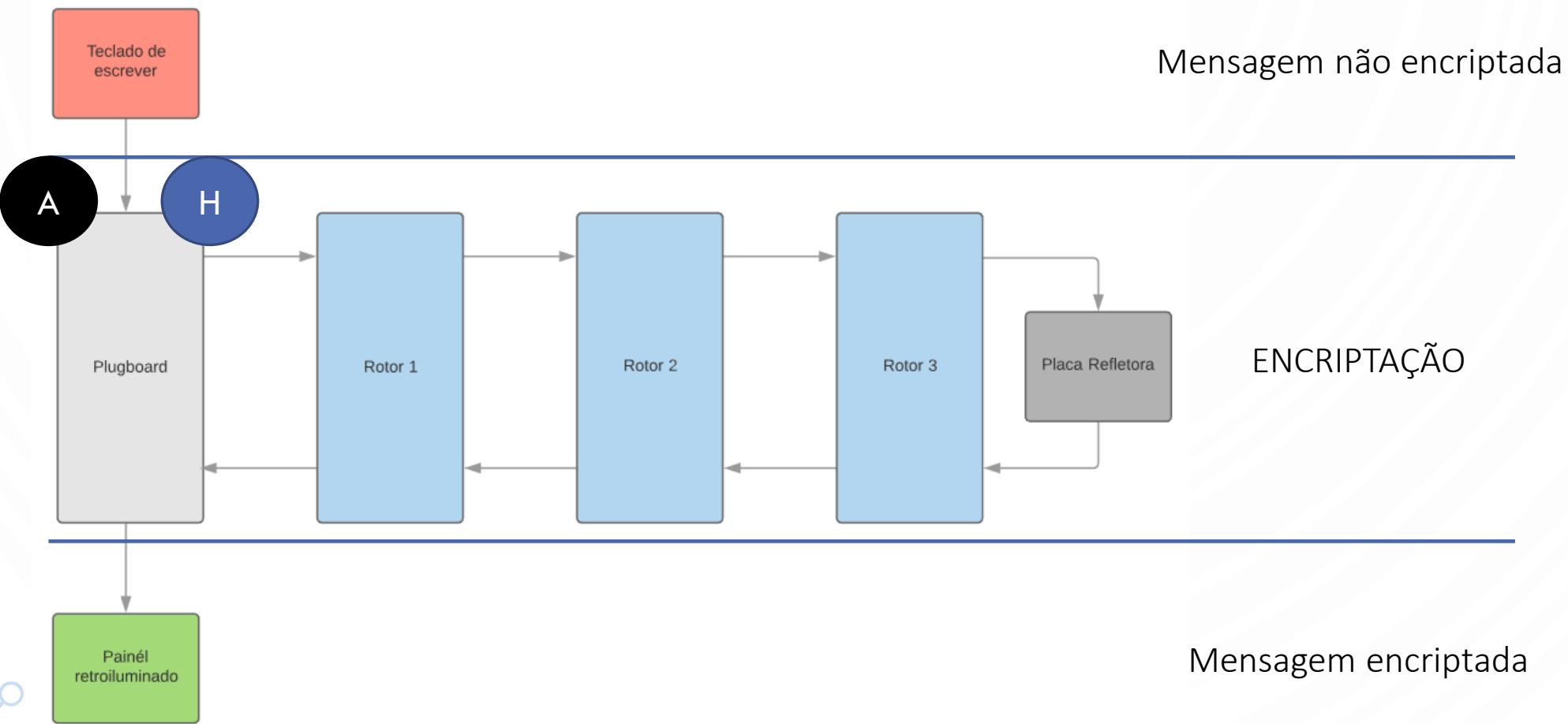


- Permutação de letras aos pares (produto de ciclos de comprimento 2)
- Propriedades da placa refletora:
  1. Não pode transformar a letra nela própria;
  2. É involutiva → se transforma x em y, então também transforma y em x.

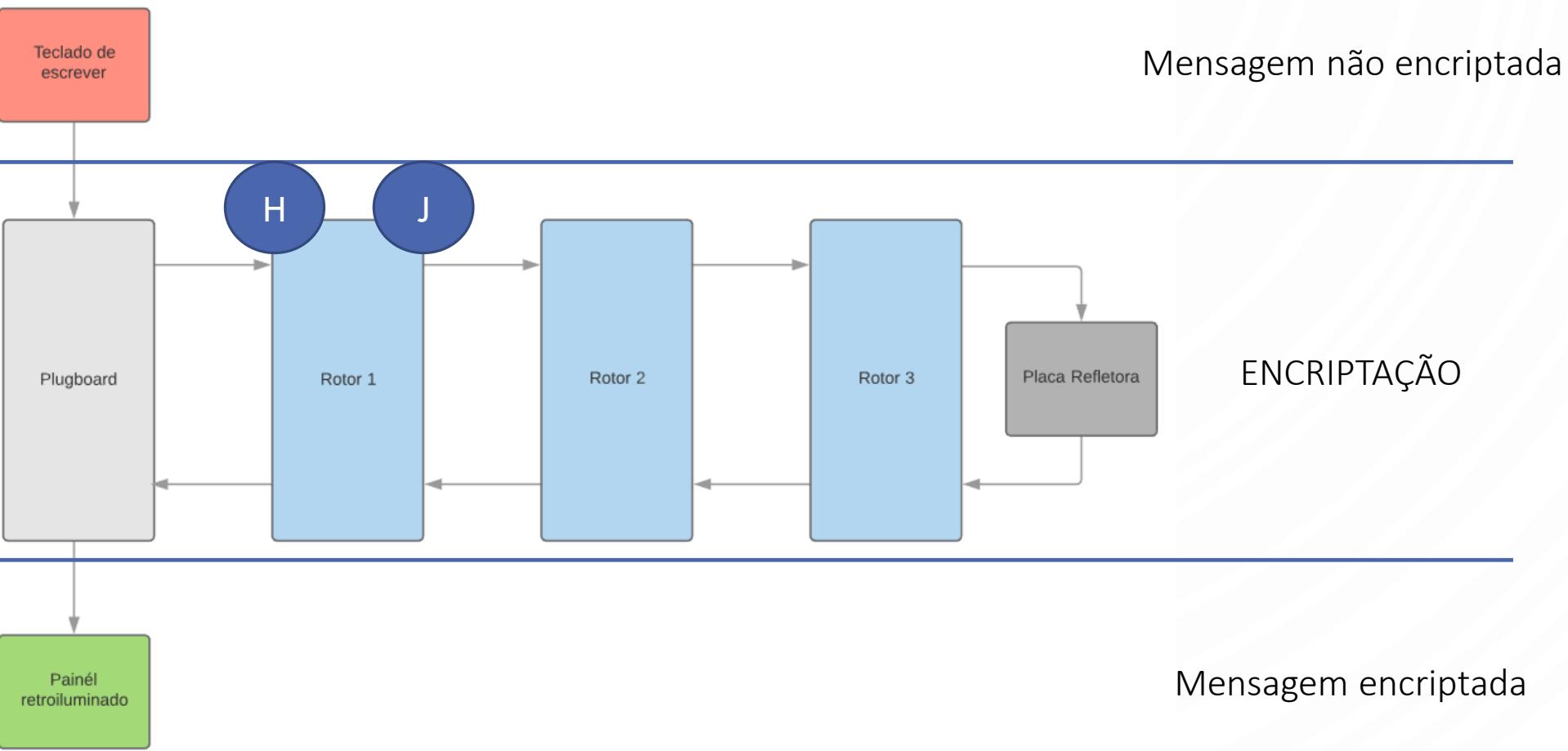
# FUNCIONAMENTO DA MÁQUINA



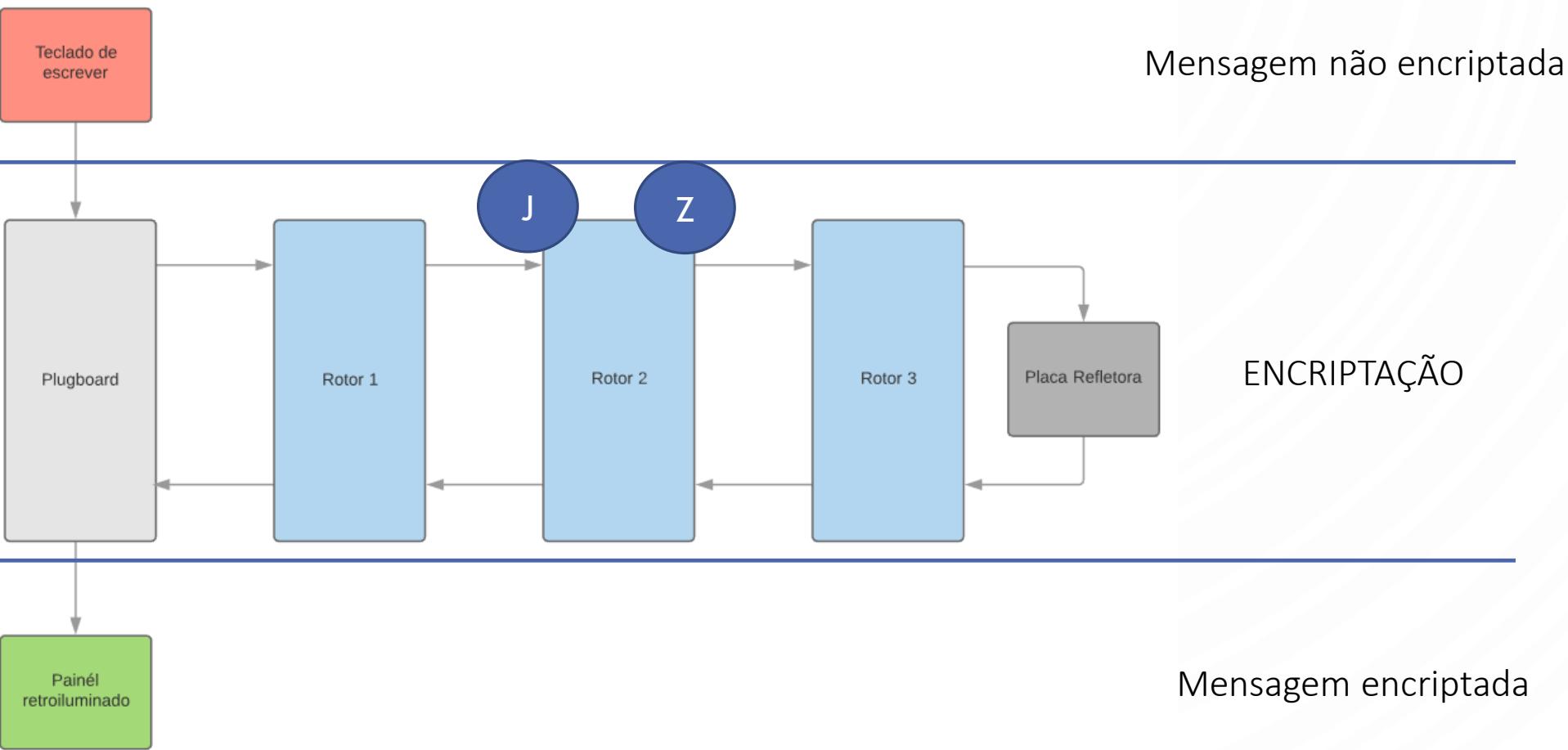
# FUNCIONAMENTO DA MÁQUINA



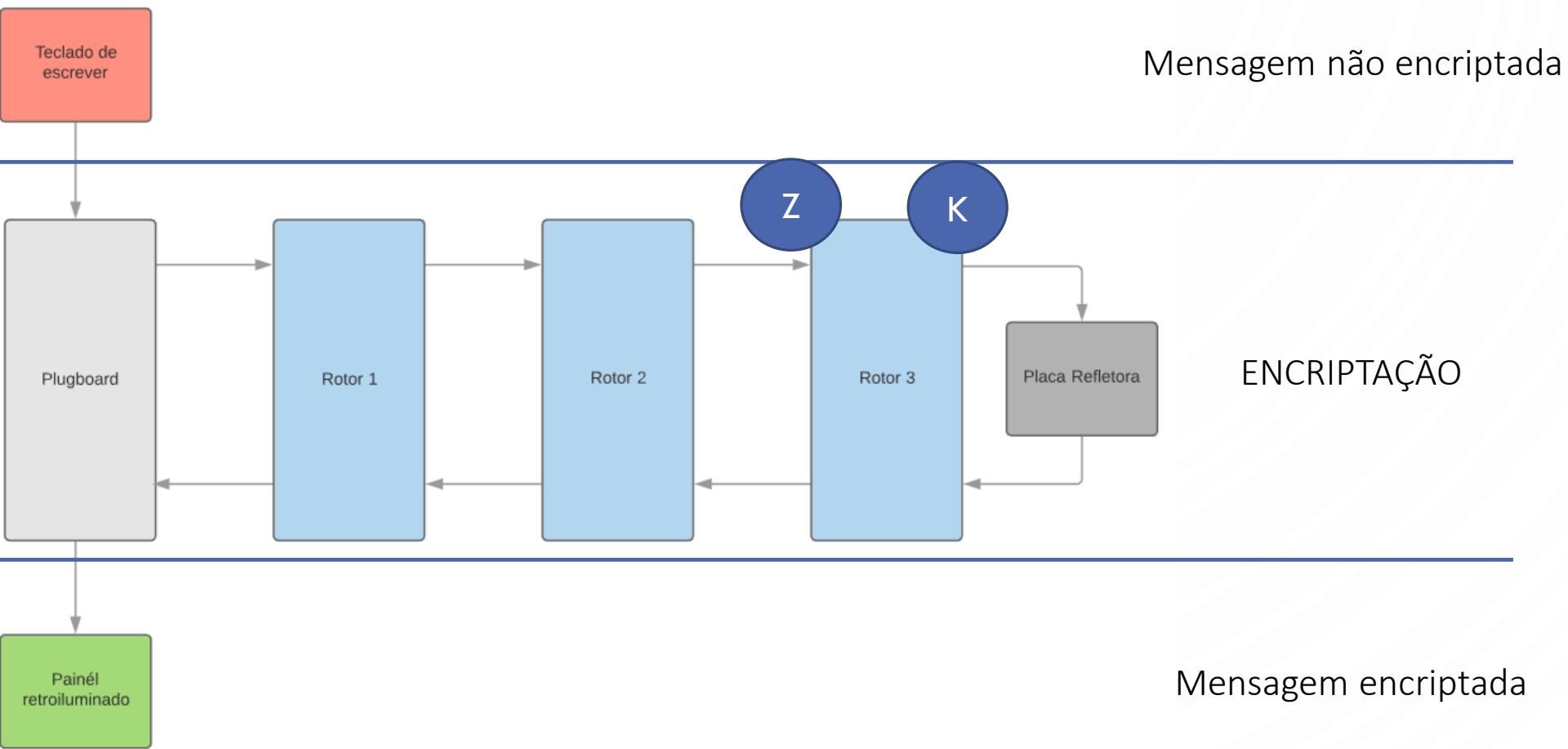
# FUNCIONAMENTO DA MÁQUINA



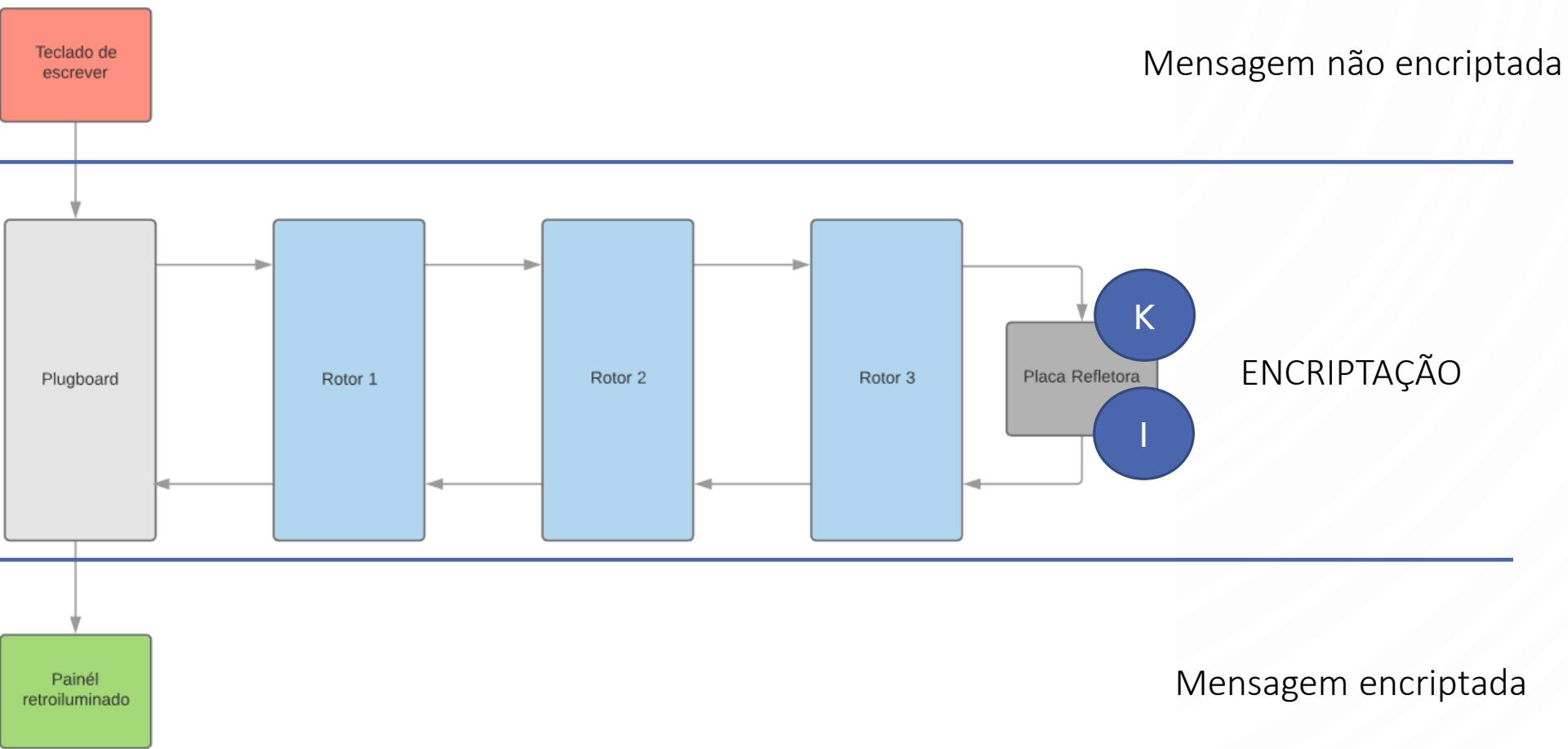
# FUNCIONAMENTO DA MÁQUINA



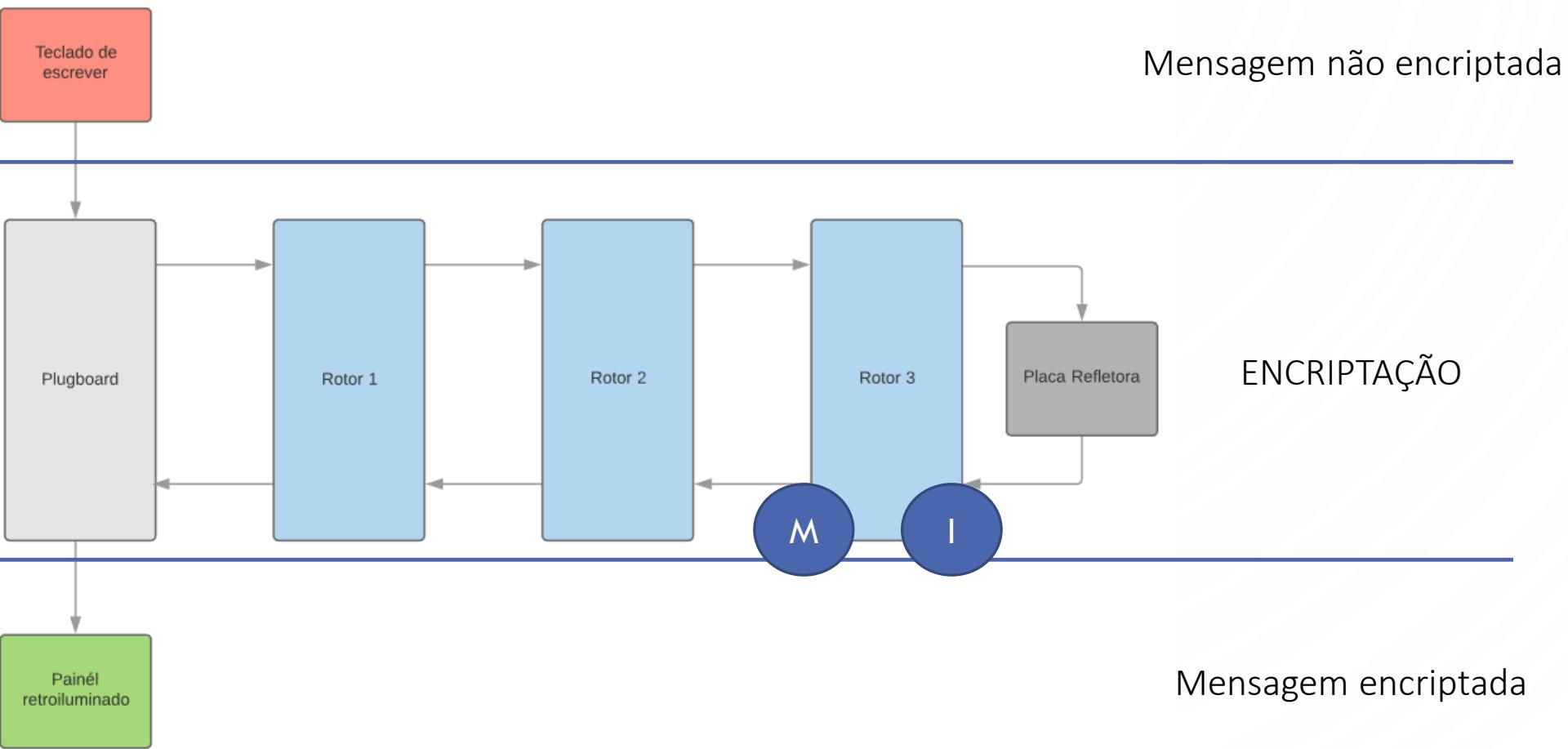
# FUNCIONAMENTO DA MÁQUINA



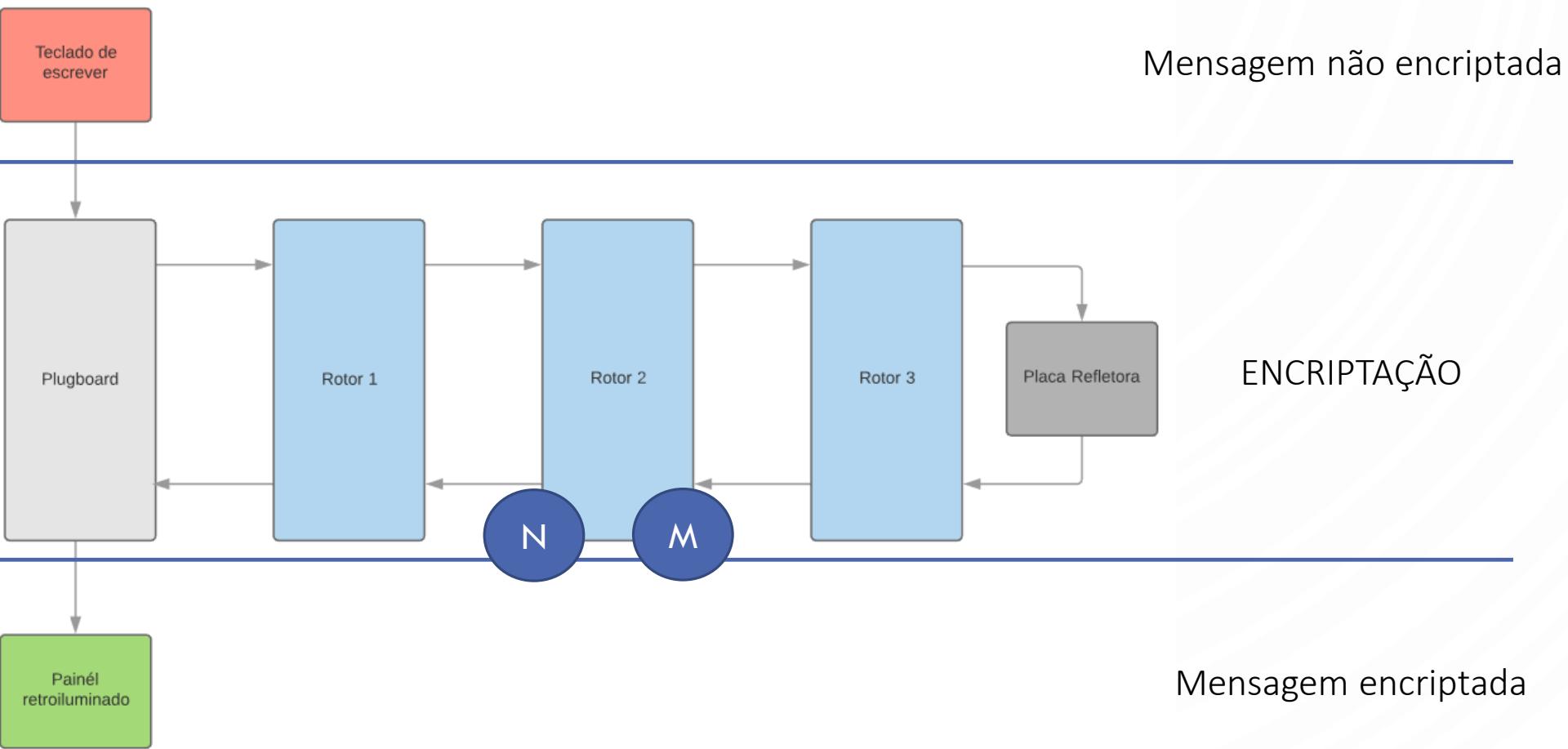
# FUNCIONAMENTO DA MÁQUINA



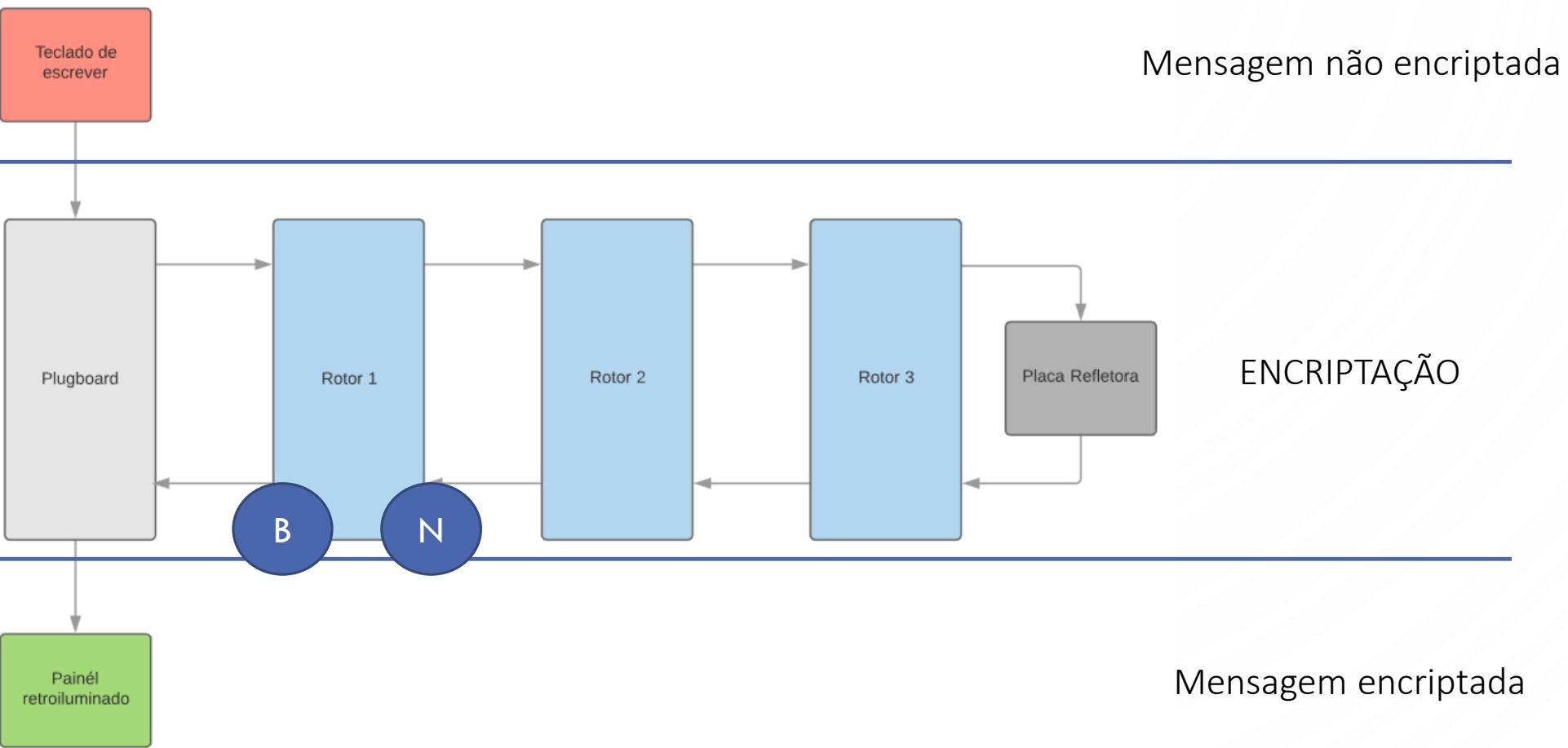
# FUNCIONAMENTO DA MÁQUINA



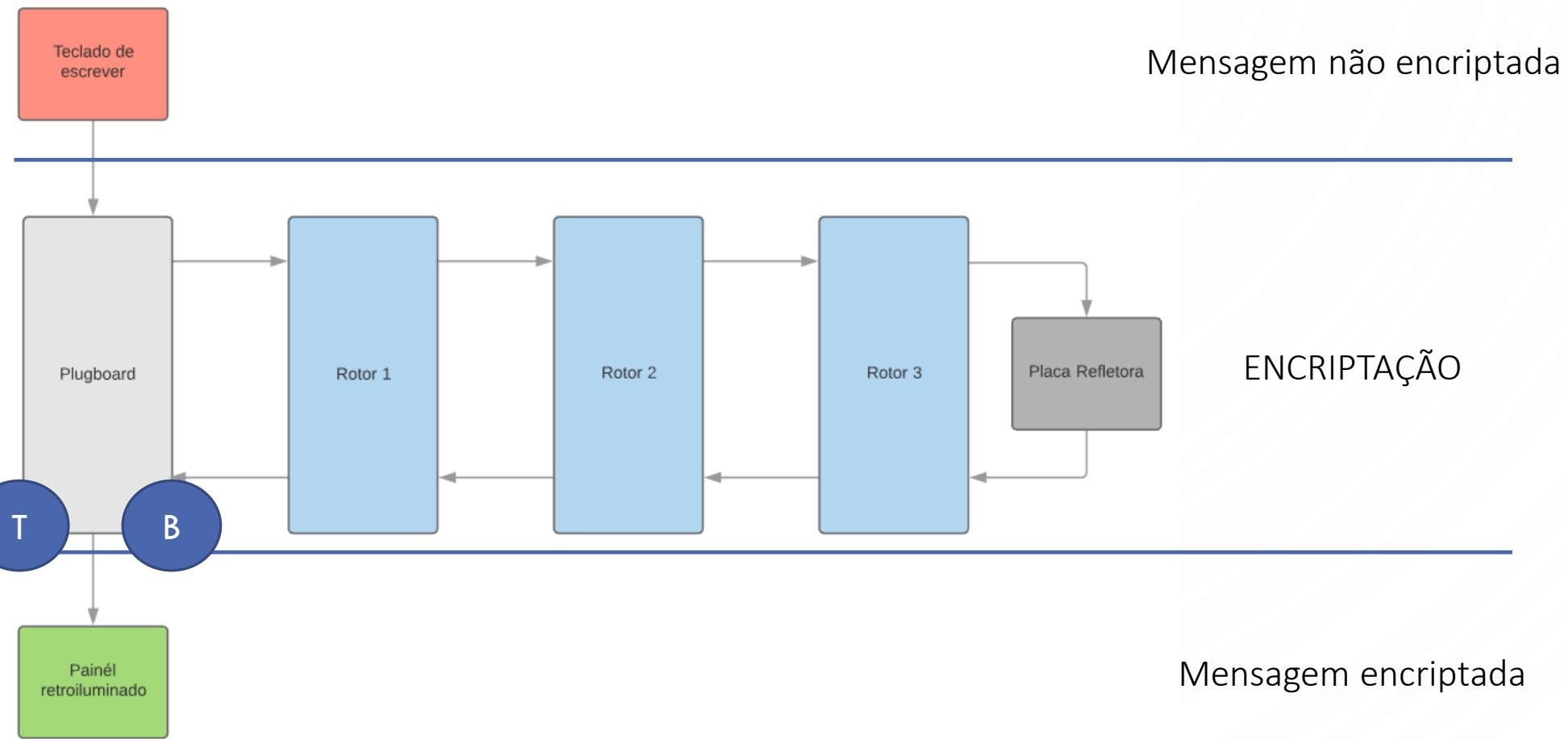
# FUNCIONAMENTO DA MÁQUINA



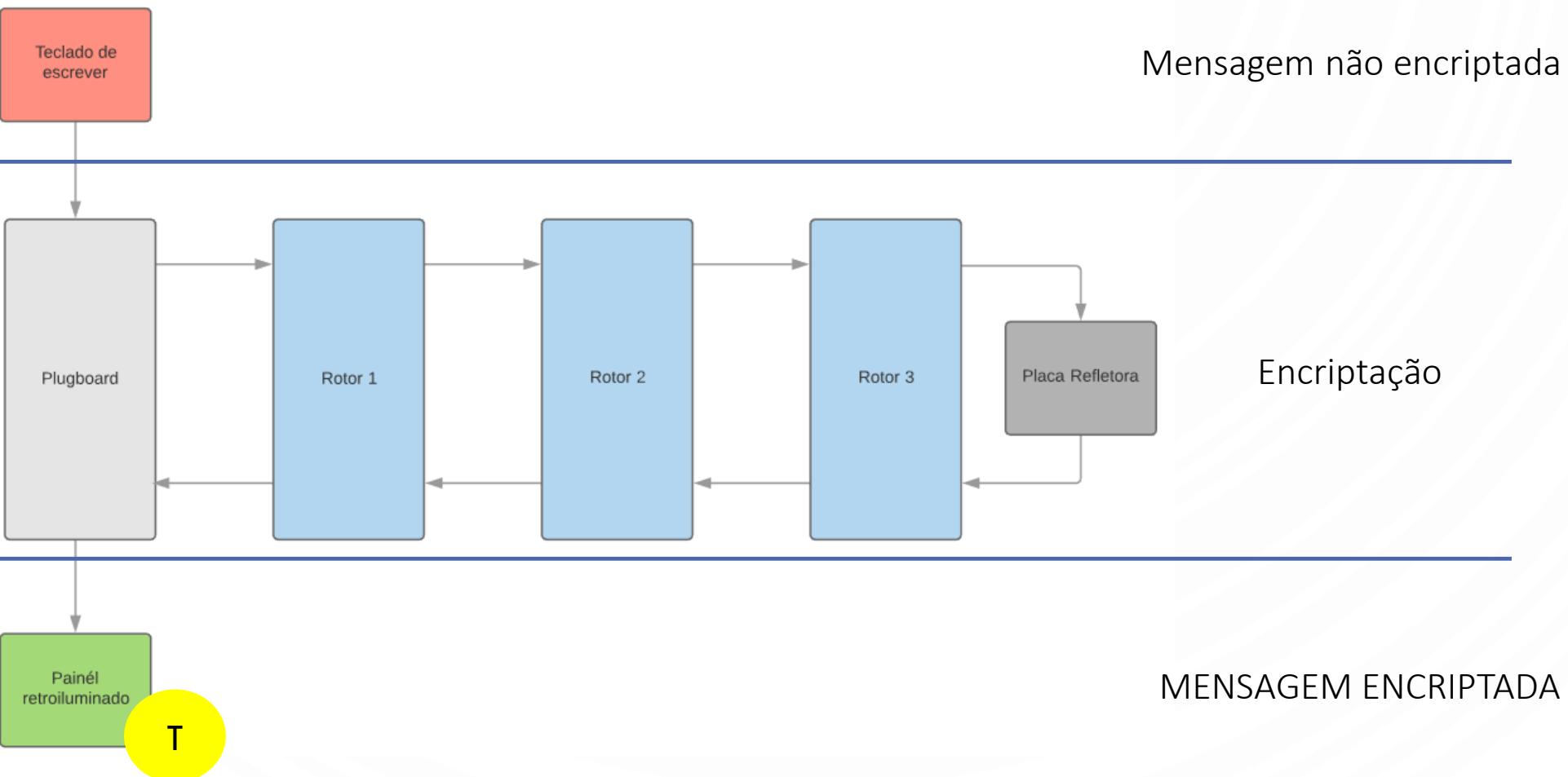
# FUNÇÃO DA MÁQUINA



# FUNÇÃO DA MÁQUINA



# FUNCIONAMENTO DA MÁQUINA





**COMBINAÇÕES POSSÍVEIS**

**158 962 555 217 826 360 000**

# NOÇÕES MATEMÁTICAS DA MÁQUINA

Permutação inicial nos Rotores

$$b = [(a + r_1) \pmod{26}]^{\alpha_1}$$

$$c = [(b + r_2) \pmod{26}]^{\alpha_2}$$

$$d = [(c + r_3) \pmod{26}]^{\alpha_3}$$

$$e = (d)^{\beta}$$

Permutação na Placa Refletora

$$e = (d)^{\beta}$$

Segunda Permutação nos Rotores

$$c' = [(e^{\alpha_3^{-1}} - r_3) \pmod{26}]^{\alpha_1}$$

$$b' = [(c'^{\alpha_2^{-1}} - r_2) \pmod{26}]^{\alpha_2}$$

$$a' = [(b'^{\alpha_1^{-1}} - r_1) \pmod{26}]^{\alpha_3}$$

$a$  corresponde ao valor proveniente da plugboard (ou, se não houver plugboard, corresponde ao valor da letra original)

$r_i$  corresponde ao valor inicial do Rotor  $i$

Elevar a  $\alpha_i$  significa localizar o termo no conjunto  $\alpha_i$  e substituir pelo termo seguinte

Elevar a  $\beta$  significa localizar o termo no conjunto  $\beta$  e substituir pelo termo seguinte

# ATRIBUIÇÃO DE CÓDIGOS ÀS LETRAS

Letra	a	b	c	d	e	f	g	h	i	j	k	l	m
Número	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	n	o	p	q	r	s	t	u	v	w	x	y	z
Número	13	14	15	16	17	18	19	20	21	22	23	24	25

# COMUNICAÇÃO DAS CONFIGURAÇÕES DA MÁQUINA

Geheime Kommandosache! Jede einzelne Logeschlüssel ist geheim. Mitte' v im Flugzeug verboten!										Nr. 00190																
Luftwaffen-Maschinen-Schlüssel Nr. 649																										
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.																										
Menge	Zeit	Ort	Wetter	Flugrichtung	Stellverbindungen an der Umkehrrolle										Gruppen											
					1	2	3	4	5	6	7	8	9	10												
649	31	I	V	III	14	09	24		SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg				
649	30	IV	III	II	05	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktr	acw	zsi	wao				
649	29	III	II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	fn	bh	ioc	zcn			
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU	BX	LP	GJ	irb	cld	ude	rzh	
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis	
649	26	I	IV	V	17	22	19		VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm				
649	25	IV	III	I	08	25	12		OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit				
649	24	V	I	IV	05	18	14		TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rw1	vci	tiq				
649	23	IV	II	I	24	12	04		QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo				
649	22	II	IV	V	01	09	21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve	
649	21	I	V	II	13	05	19	PT	OX	EZ	CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf	
649	20	III	IV	V	24	01	10	MR	KN	BQ	PW	DF	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh	
649	19	V	III	I	17	25	20	OX	PR	FH	WY	DL	CM	AE	TZ	JS	GI	idt	fpx	jwg	tig					
649	18	IV	II	V	15	23	26	EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	bw	vcj	rxn					
649	17	I	IV	II	21	10	06		IR	KZ	LS	EM	OV	OY	QX	AF	JP	BU	mae	hzi	sog	ysi				
649	16	V	II	III	08	16	13		HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	tdp	dhb	fkf	uiv				
649	15	II	IV	I	01	03	07		DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg				
649	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk	
649	13	I	III	II	13	20	03	FW	EL	DG	KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgr	gjo	ryq	
649	12	V	I	IV	18	10	07	RZ	OQ	CP	SX	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	zdy	rkf	tjw	xtl	
649	11	II	IV	III	02	26	15	KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	zea	rjy	soi	wvh					
649	10	III	V	IV	23	21	01	LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc	zbx	vbm	rzo					
649	9	V	I	III	16	04	08	QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	vby	tlh					
649	8	IV	II	V	13	19	25		FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli				
649	7	I	IV	II	09	03	22		UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi				
649	6	III	I	V	11	18	14		DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj				
649	5	V	II	IV	23	02	25		MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj				
649	4	II	IV	I	04	21	09		QT	WZ	KV	GM	AC	BL	OZ	EK	QW	GP	SU	DH	JM	tx	lsb	zby	vcy	ujb
649	3	V	I	II	19	11	06		BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	IW	AV	GJ	lo	lap	owd	iwu	wak
649	2	IV	V	I	16	14	02		BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdf	iyf	xtd				
649	1	II	I	III	23	12	10		DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv				

Dia do mês  
(importante, uma vez que para cada dia, havia uma configuração da máquina diferente)

# COMUNICAÇÃO DAS CONFIGURAÇÕES DA MÁQUINA

Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Mitte 'z' im Flugzeug verboten!								Nr. 00190																		
Luftwaffen-Maschinen-Schlüssel Nr. 649																										
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.																										
Motoren Anordnung	Wagenlage	Feststellung	Stell der vertreibbindungen an der Umkehrrolle																							
			1	2	3	4	5	6	7	8	9	10														
649	31	I	V	III	14	09	24	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg					
649	30	IV	III	II	05	26	02	IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktr	acw	zsi	wao					
649	29	III	II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	zcn	ovw	wvd	
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU	BX	LP	GJ	irb	cld	ude	rzh	
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis	
649	26	I	IV	V	17	22	19	VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm					
649	25	IV	III	I	08	25	12	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit					
649	24	V	I	IV	05	18	14	TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rw1	vci	tlq					
649	23	IV	II	I	24	12	04	QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo					
649	22	II	IV	V	01	09	21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve	
649	21	I	V	II	13	05	19	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf					
649	20	III	IV	V	24	01	10	PT	OX	EZ	CH	DF	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh	
649	19	V	III	I	17	25	20	MR	KN	BQ	PW	OX	PR	FW	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tig	
649	18	IV	II	V	15	23	26	EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	bw	vcj	rxn					
649	17	I	IV	II	21	10	06	IR	KZ	LS	EM	OV	OY	QX	AF	JP	BU	mae	hzi	sog	ysi					
649	16	V	II	III	08	16	13	HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	tdp	dhb	fkf	uiv					
649	15	II	IV	I	01	03	07	DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg					
649	14	IV	I	V	15	11	05	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk					
649	13	I	III	II	13	20	03	AI	BT	MV	HU	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgz	gjo	ryq	
649	12	V	I	IV	18	10	07	FW	EL	DG	KN	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	zdy	rkf	tjw	xtl	
649	11	II	IV	III	02	26	15	RZ	OQ	CP	SX	KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV	zea	rjy	soi	wvh	
649	10	III	V	IV	23	21	01	LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc	zbx	vbm	rxo					
649	9	V	I	III	16	04	08	QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	vby	tlh					
649	8	IV	II	V	13	19	25	FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli					
649	7	I	IV	II	09	03	22	UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi					
649	6	III	I	V	11	18	14	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj					
649	5	V	II	IV	23	02	25	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj					
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	GP	SU	DH	JM	TX	lsb	zby	vcy	ujb	
649	3	V	I	II	19	11	06	BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak	
649	2	IV	V	I	16	14	02	BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy	iyf	xtd					
649	1	II	I	III	23	12	10	DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv					

Indicação dos Rotores a utilizar

# COMUNICAÇÃO DAS CONFIGURAÇÕES DA MÁQUINA

Geheime Kommandosache! Jede einzelne Logeschlüssel ist geheim. Mitte' v im Flugzeug verboten!				Nr. 00190											
Luftwaffen-Maschinen-Schlüssel Nr. 649															
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.															
Motortyp	Wagenlage	Ringstellung	Stellvertreibungsverbindungen an der Umkehrrolle										Benutzergruppen		
			1	2	3	4	5	6	7	8	9	10			
649	31	I V III	14 09 2	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny dgy ekb rzg	
649	30	IV III II	05 26 0	IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktr acw zsi wao	
649	29	III II I	12 24 0	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW PZ FN BH	ioc acn ude rzh
649	28	II III V	06 08 1	DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU BX LP GJ	irb cld vct uis
649	27	III I IV	11 03 0	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP HT EX UW	woj fbh uev rxm
649	26	I IV V	17 22 1	VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle gbo uew uit	
649	25	IV III I	08 25 12	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc uhq vci tlq	
649	24	V I IV	05 18 14	TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl rwl udf tlo	
649	23	IV II I	24 12 04	QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn rwm mwe wve	
649	22	II IV V	01 09 21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU BG WZ CN	jqc acx jpw del mwf wvf
649	21	I V II	13 05 19	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jqd cef nvo ysh	
649	20	III IV V	24 01 10	PT	OX	EZ	CH	DF	MO	QZ	AU	RY	SV	JL GX BE TW	idf fpz jwg tlg
649	19	V III I	17 25 20	MR	KN	BQ	PW	OX	PR	FH	WY	DL	CM	AE TZ JS GI	lsa bw vcj rxn
649	18	IV II V	15 23 26	EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	mae hzi sog ysi	
649	17	I IV II	21 10 06	IR	KZ	LS	EM	OV	OY	QX	AF	JP	BU	tdp dhh fkb uiv	
649	16	V II III	08 16 13	HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	ldw hzj soh wvg	
649	15	II IV I	01 03 07	DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	imz noa tjv xtk	
649	14	IV I V	15 11 05	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	lyz ag km br iq ju hv sw et cx zgr dgz gjo ryq	
649	13	I III II	13 20 03	AI	BT	MV	HU	LY	AG	KM	BR	IQ	JU	zdy rkf tju xtl	
649	12	V I IV	18 10 07	FW	EL	DG	KN	MU	BP	CY	RZ	KX	AN	JT DG IL PW	
649	11	II IV III	02 26 15	RZ	OQ	CP	SX	KN	UY	HR	PW	FM	BO	EZ QT DX JV	zea rjy soi wvh
649	10	III V IV	23 21 01	LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc zbx vbm rxo	
649	9	V I III	16 04 08	QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj eyr vby tlh	
649	8	IV II V	13 19 25	FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz dha ekc tli	
649	7	I IV II	09 03 22	UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	lan dgb zsj wbi	
649	6	III I V	11 18 14	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao cft zsk wbj	
649	5	V II IV	23 02 25	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju cdr iye waj	
649	4	II IV I	04 21 09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	GP	SU DH JM TX	lsb zby vcy ujb
649	3	V I II	19 11 06	BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	IW AV GJ LO	lap owd iwu wak
649	2	IV V I	16 14 02	BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd bdy iyf xtd	
649	1	II I III	23 12 10	DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl cdf giq wuv	

Indicação da configuração inicial dos Rotores

# COMUNICAÇÃO DAS CONFIGURAÇÕES DA MÁQUINA

Meldungs Nr.	Wellenlage	Ringstellung	Steckerverbindungen										Kenngruppen			
			an der Umkehrrolle im Steckerbrett													
649	31	I V III	14 09 24	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	
649	30	IV III II	05 26 02	IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktr	tzg	
649	29	III II I	12 24 03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	zsi	wao
649	28	II III V	06 08 16	DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU	ovw	wvd
649	27	III I IV	11 03 07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	ioc	zcn
649	26	I IV V	17 22 19	VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	irb	cld	
649	25	IV III I	08 25 12	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	woj	rzh	
649	24	V I IV	05 18 14	TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	vct	uis	
649	23	IV II I	24 12 04	QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	uev	rxm	
649	22	II IV V	01 09 21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU	kpl	rwj
649	21	I V II	13 05 19	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	ebn	rwm	
649	20	III IV V	24 01 10	PT	OX	EZ	CH	DF	MO	QZ	AU	RY	SV	JL	jqc	acx
649	19	V III I	17 25 20	MR	KN	BQ	PW	OX	PR	FH	WY	DL	CM	AE	jpw	del
649	18	IV II V	15 23 26	EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	jqd	cef	
649	17	I IV II	21 10 06	IR	KZ	LS	EM	OV	OY	QX	AF	JP	BU	idf	fpx	
649	16	V II III	08 16 13	HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	lza	bw	
649	15	II IV I	01 03 07	DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	tde	rxn	
649	14	IV I V	15 11 05	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	mae	hzi	
649	13	I III II	13 20 03	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	tdp	dhb	
649	12	V I IV	18 10 07	FW	EL	DG	KN	MU	BP	CY	RZ	KX	AN	IL	zdy	rkf
649	11	II IV III	02 26 15	RZ	OQ	CP	SX	KN	UY	HR	PW	FM	BO	EZ	zea	rjy
649	10	III V IV	23 21 01	LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc	zbx	
649	9	V I III	16 04 08	QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	
649	8	IV II V	13 19 25	FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	
649	7	I IV II	09 03 22	UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	lan	dgb	
649	6	III I V	11 18 14	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	
649	5	V II IV	23 02 25	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	1ju	cdr	
649	4	II IV I	04 21 09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	GP	SU	1sb	zby
649	3	V I II	19 11 06	BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	IW	lap	owd
649	2	IV V I	16 14 02	BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy	
649	1	II I III	23 12 10	DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kg1	cdf	

Letras de teste

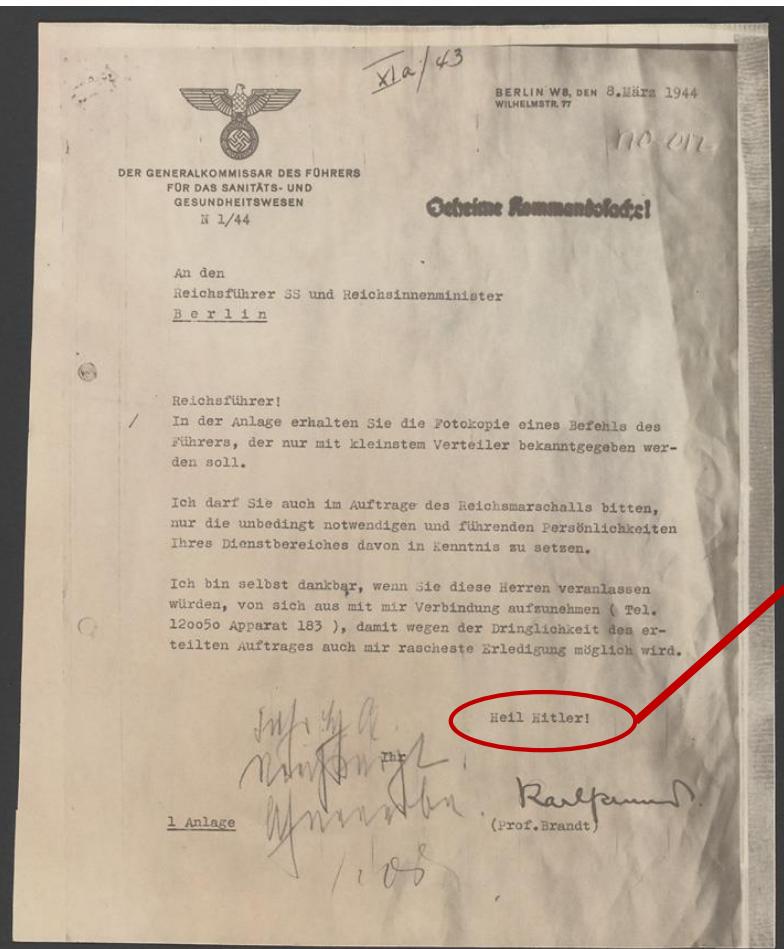
# PONTOS FRACOS

- Passo regular dos rotores
- Número fixo de plugs



- Uma letra nunca se transforma nela própria

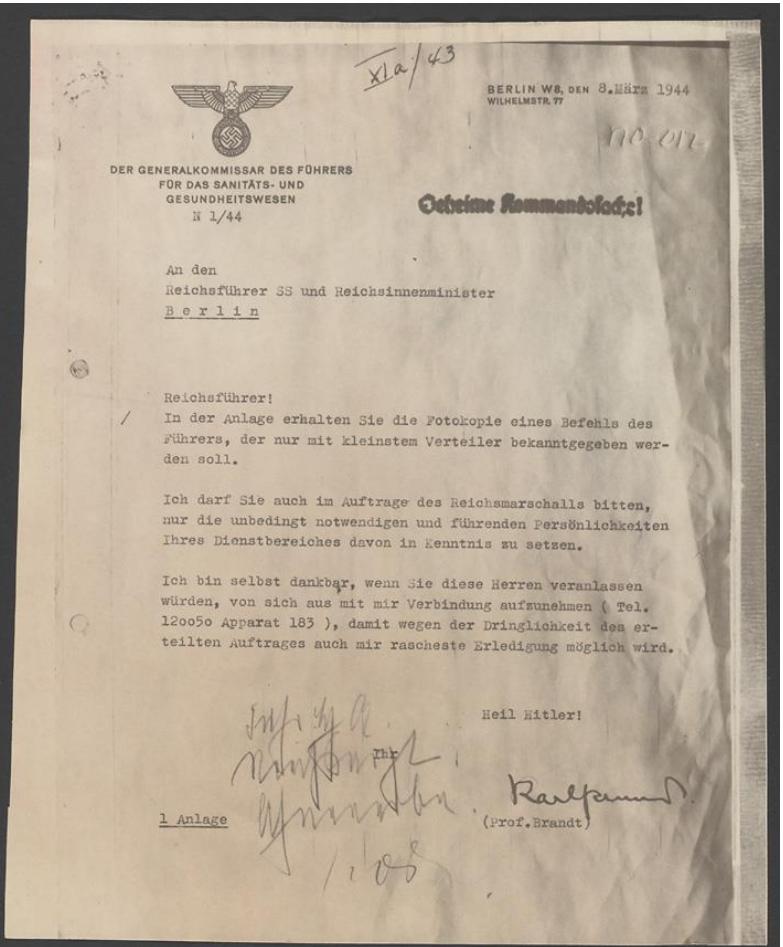
- Uma letra nunca se transforma nela própria



...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
	H	E	I	L	H	I	T	L	E	R									

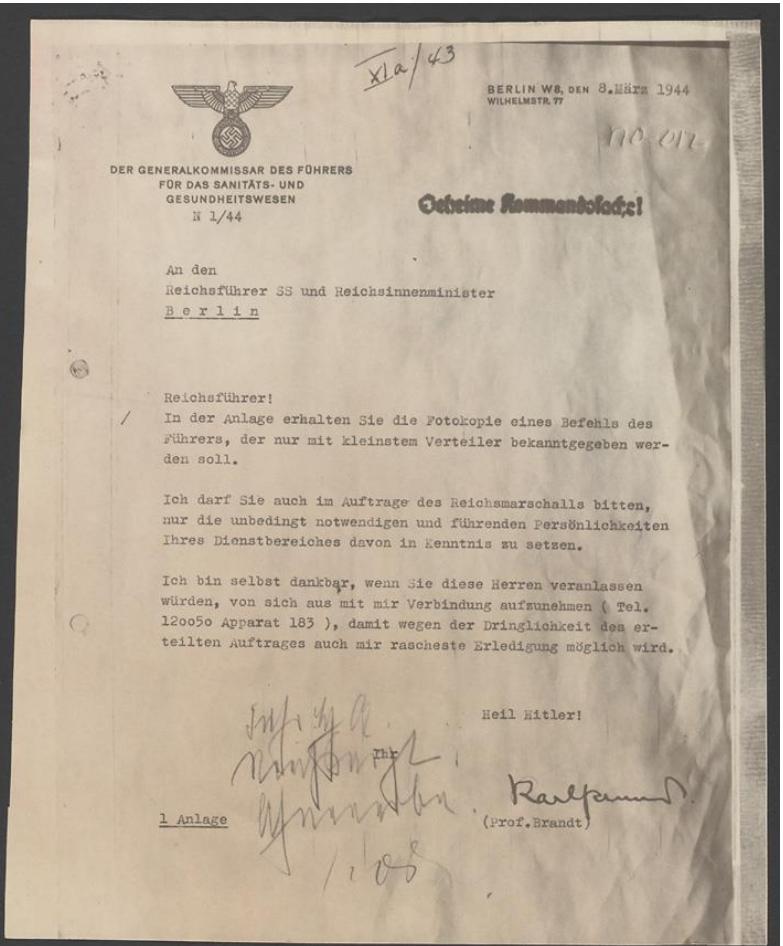


- Uma letra nunca se transforma nela própria



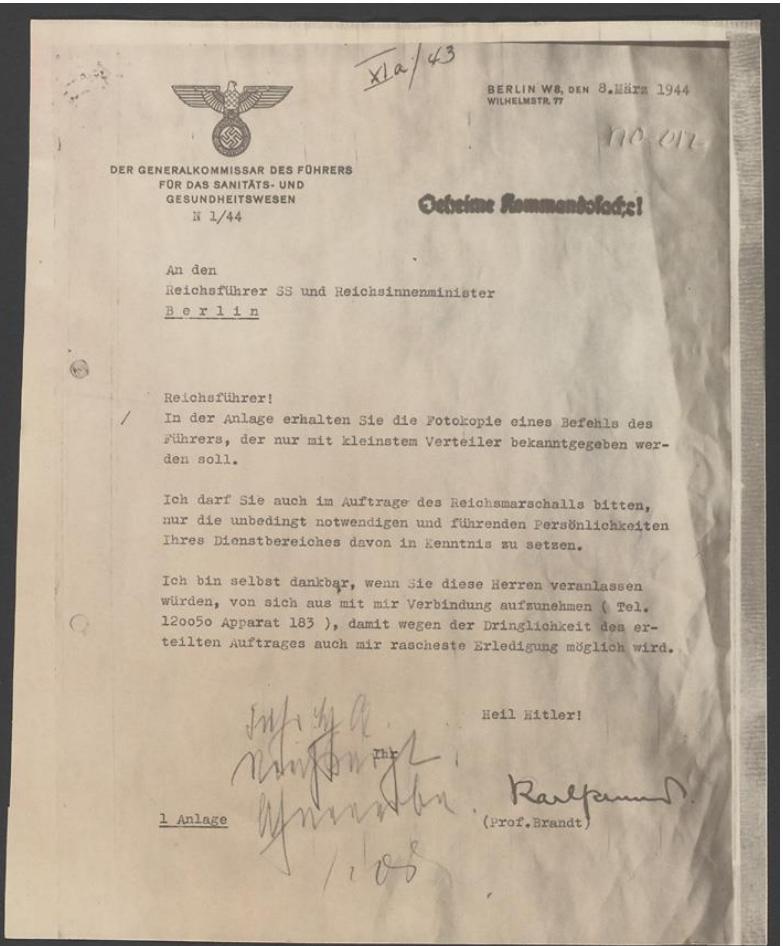
...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
	H	E	I	L	H	I	T	L	E	R									

- Uma letra nunca se transforma nela própria



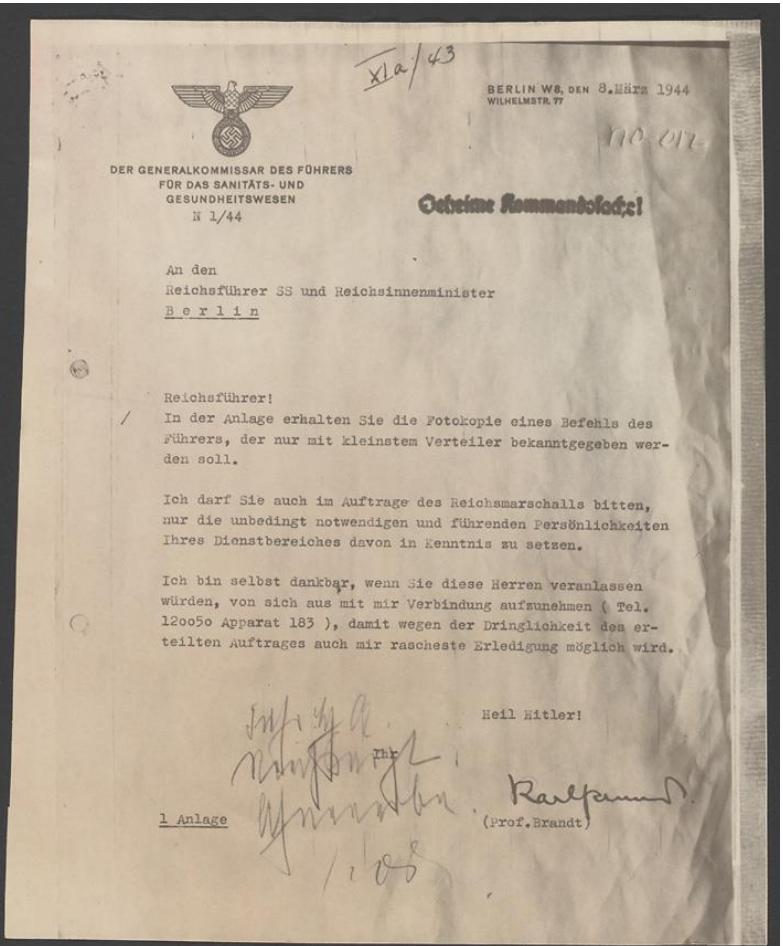
...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
		H	E	I	L	H	I	T	L	E	R								

- Uma letra nunca se transforma nela própria



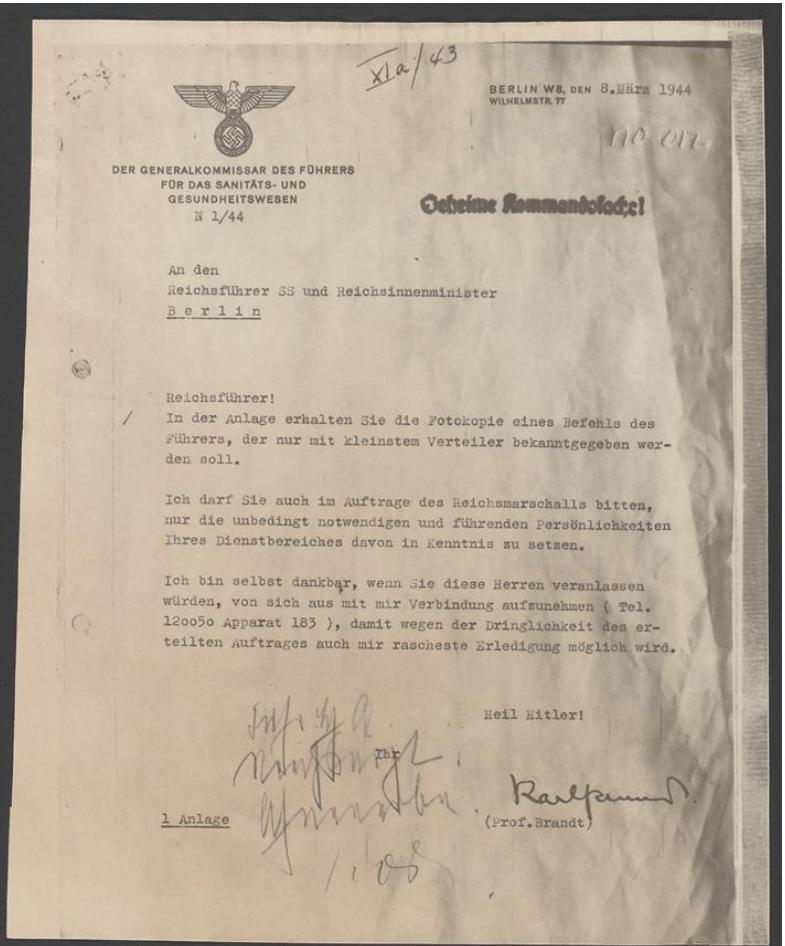
...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
			H	E	I	L	H	I	T	L	E	R							

- Uma letra nunca se transforma nela própria

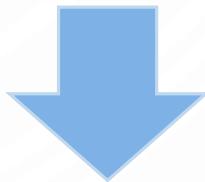


...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
						H	E	I	L	H	I	T	L	E	R				

- Uma letra nunca se transforma nela própria

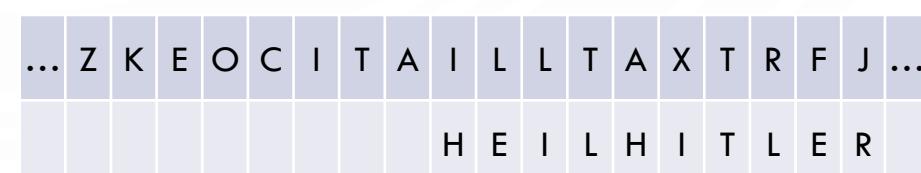
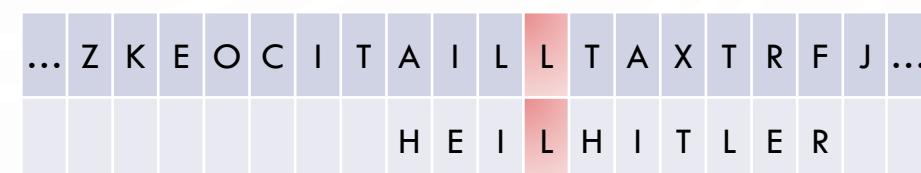
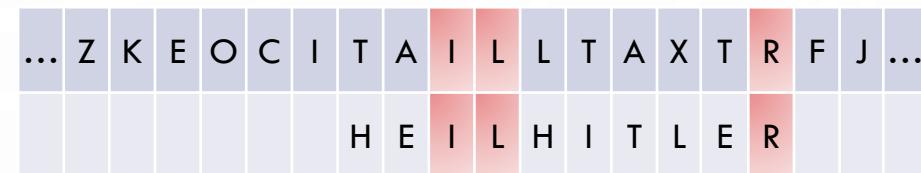
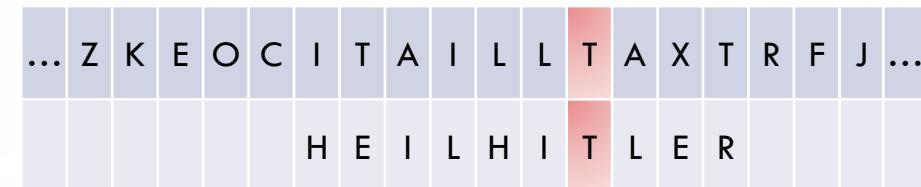
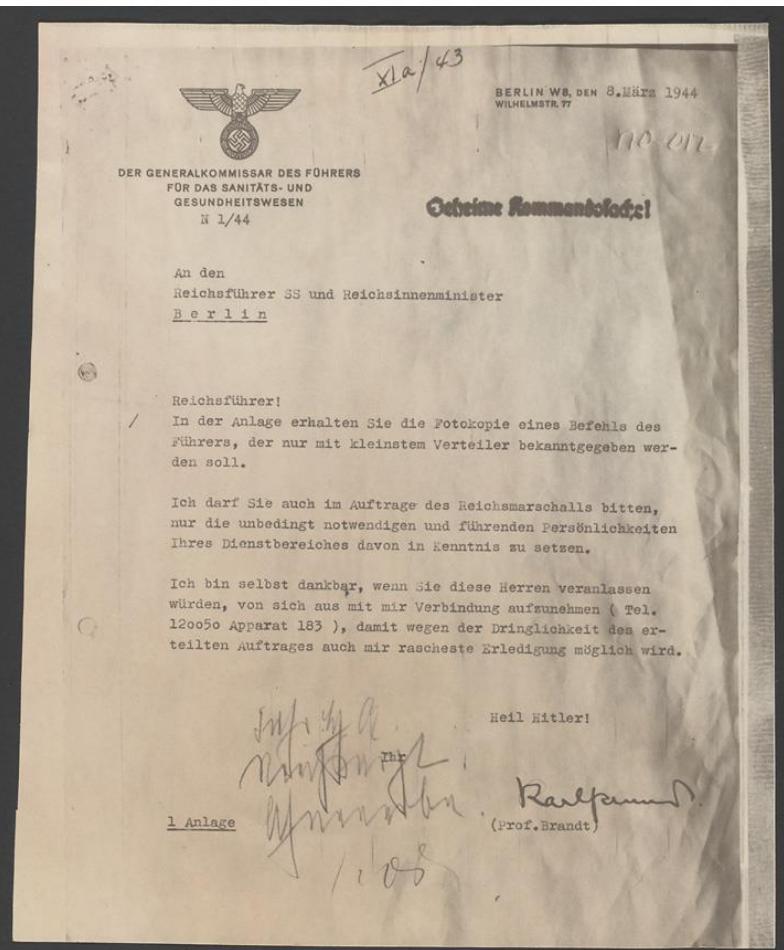


...	Z	K	E	O	C	I	T	A	I	L	L	T	A	X	T	R	F	J	...
					H	E	I	L	H	I	T	L	E	R					



Solução Possível

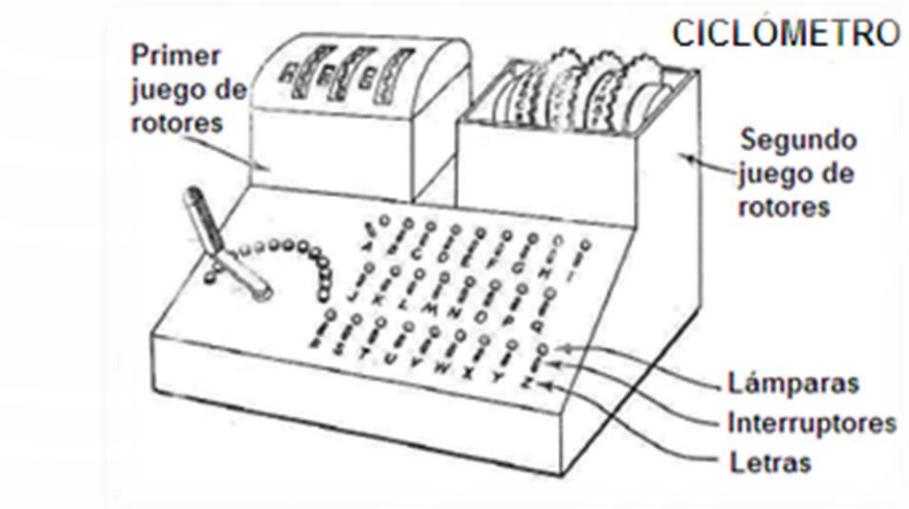
- Uma letra nunca se transforma nela própria



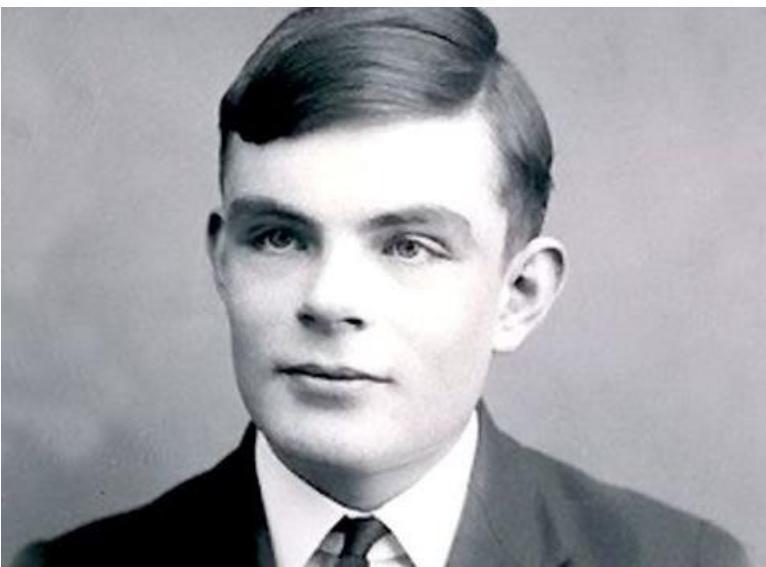
Solução Possível

# POTENCIAIS ATAQUES

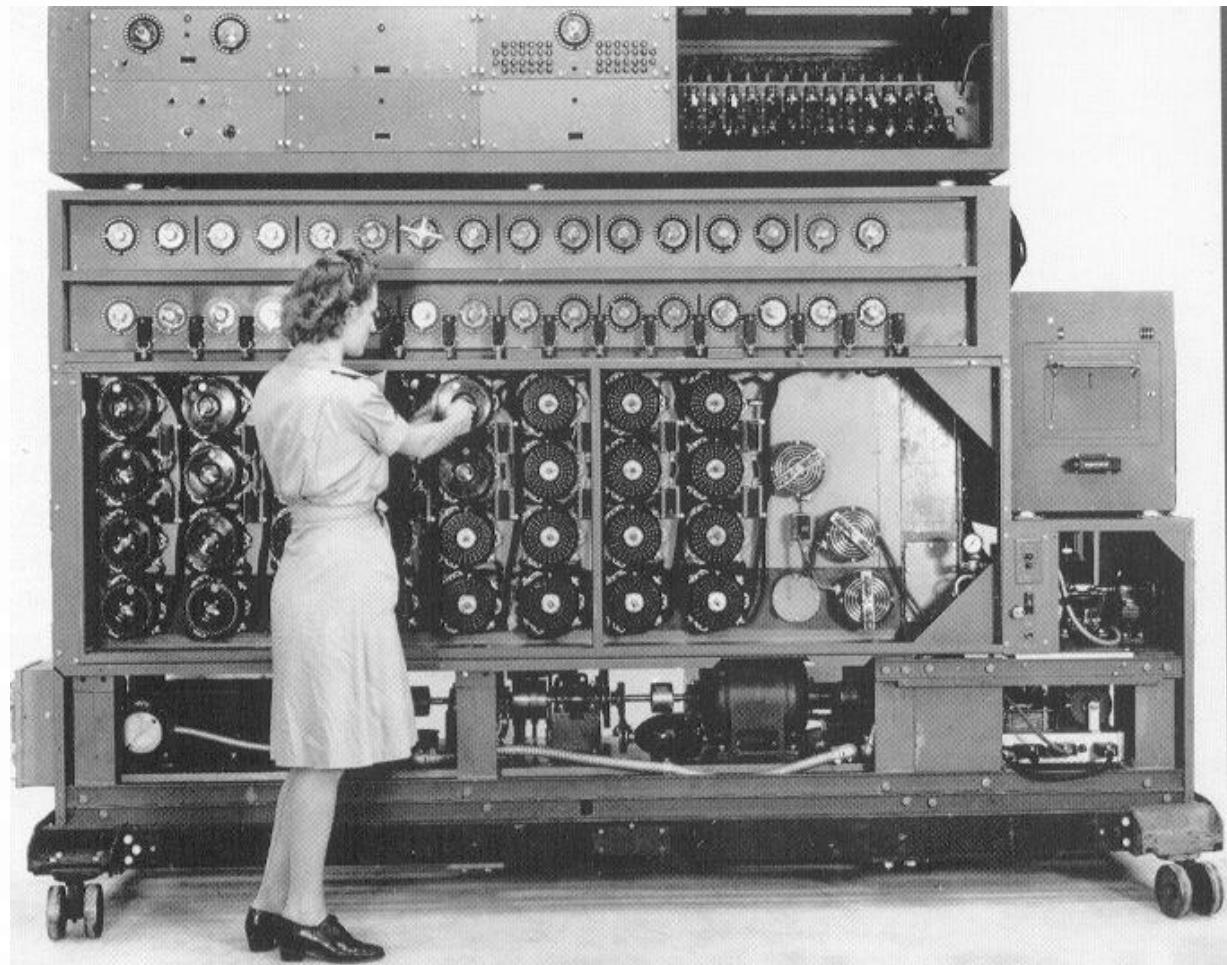
- Método da Grelha
- Método ANX
- Método do Relógio
- Ciclómetro



1938



Alan Turing



“BOMBE” – Bomba  
Eletromecânica

# TYPEX MACHINE



# TYPEX MACHINE

