Enigma

CMSC 28400, Autumn 2021, Lecture 2

David Cash

University of Chicago

Enigma

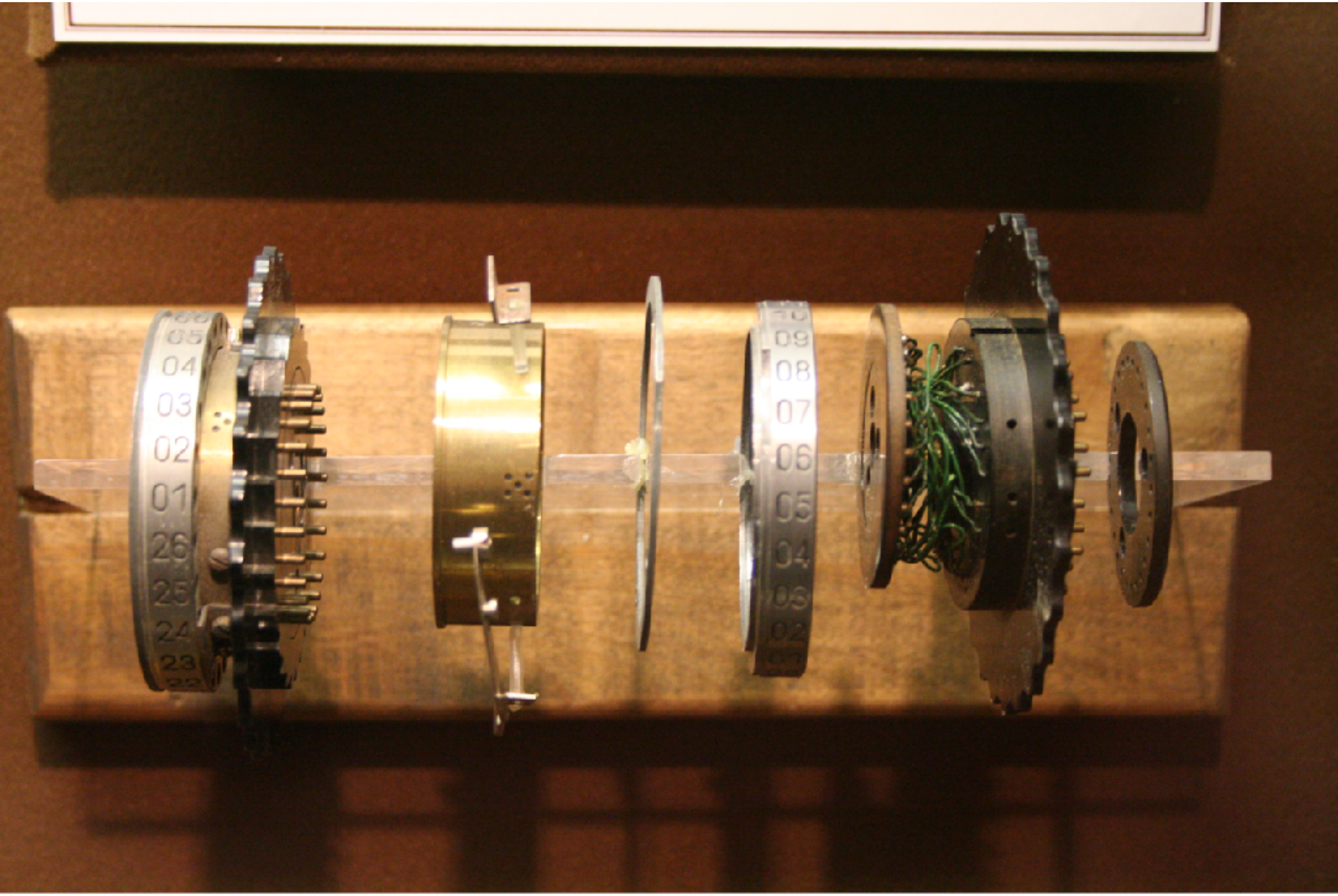
Reflector (*Umkehrwalze*, not visible)

Three rotors (*Walzen*)

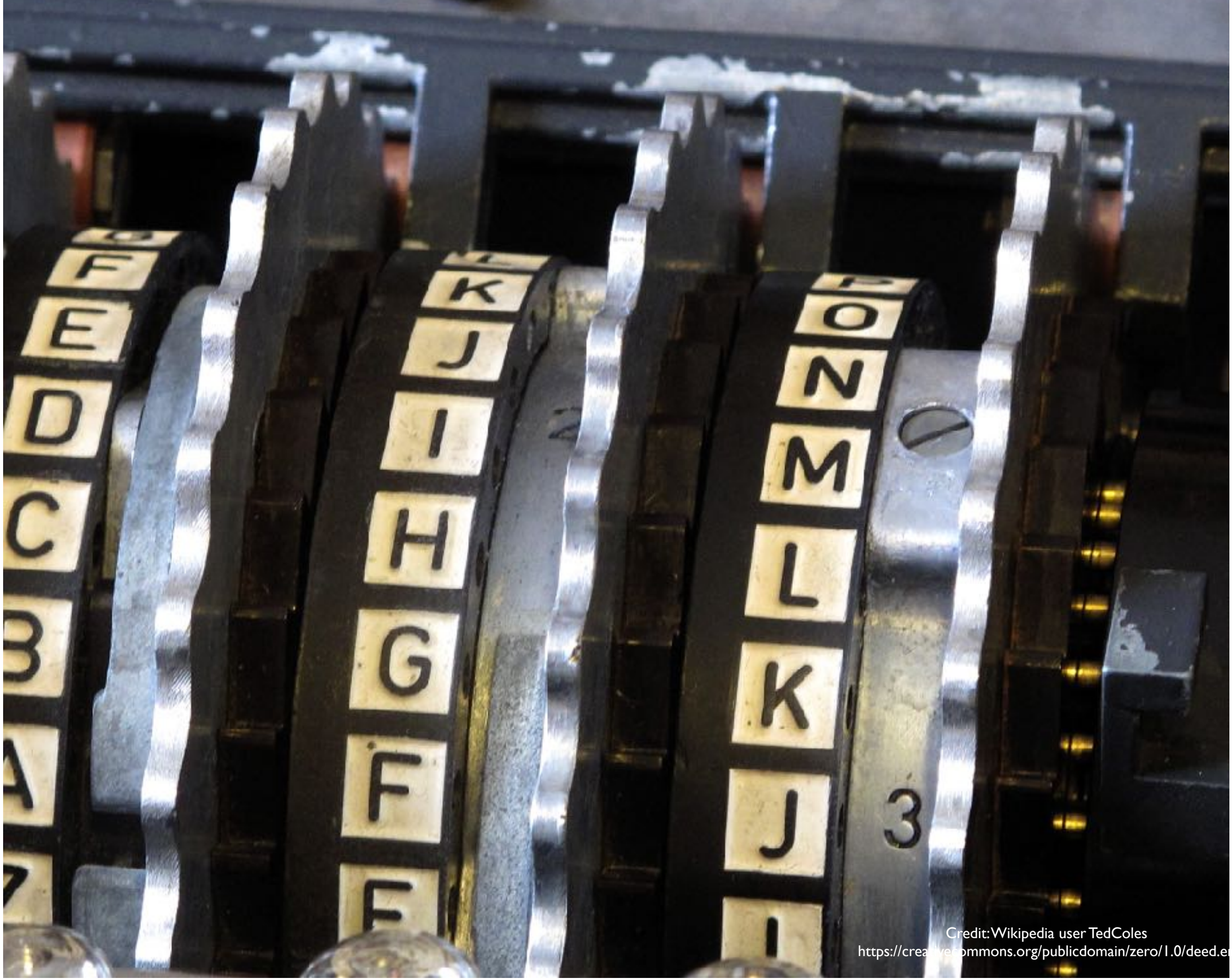
Lightboard (output)

Keyboard

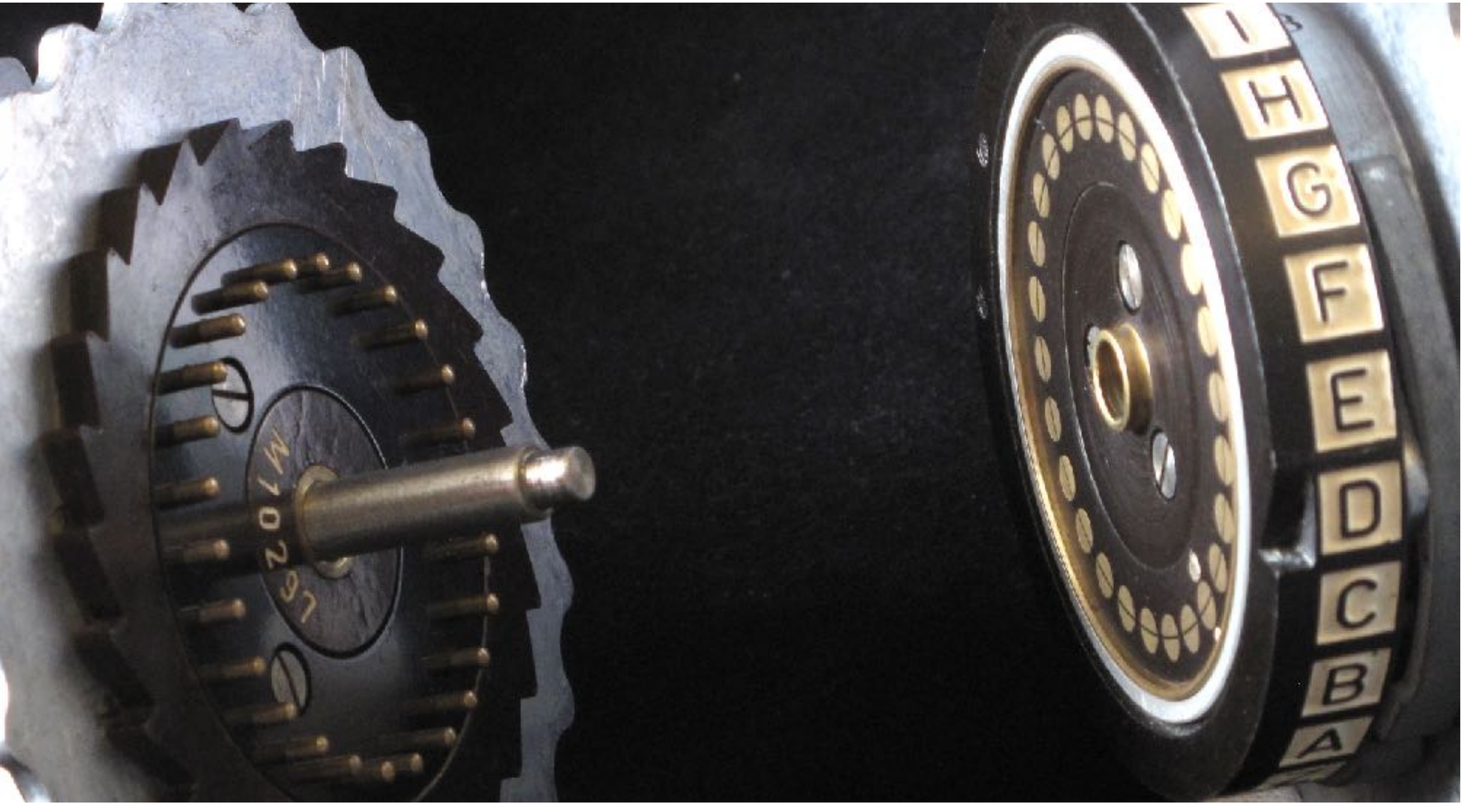
Plugboard (*Steckerbrett*)

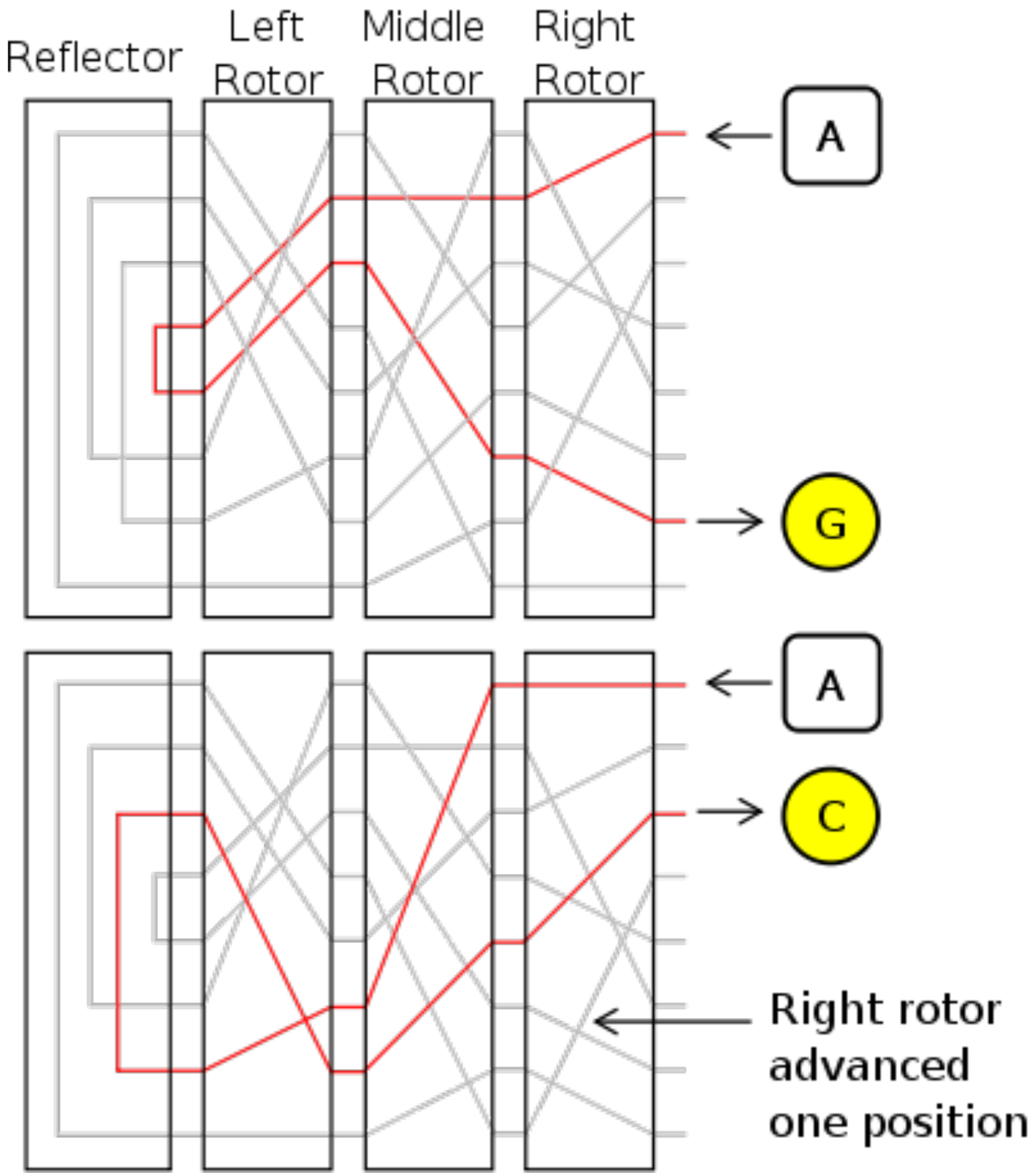


Credit: Wikipedia user RadioFan, https://creativecommons.org/licenses/by-sa/3.0/deed.en



Credit: Wikipedia user TedColes
https://creativecommons.org/publicdomain/zero/1.0/deed.e

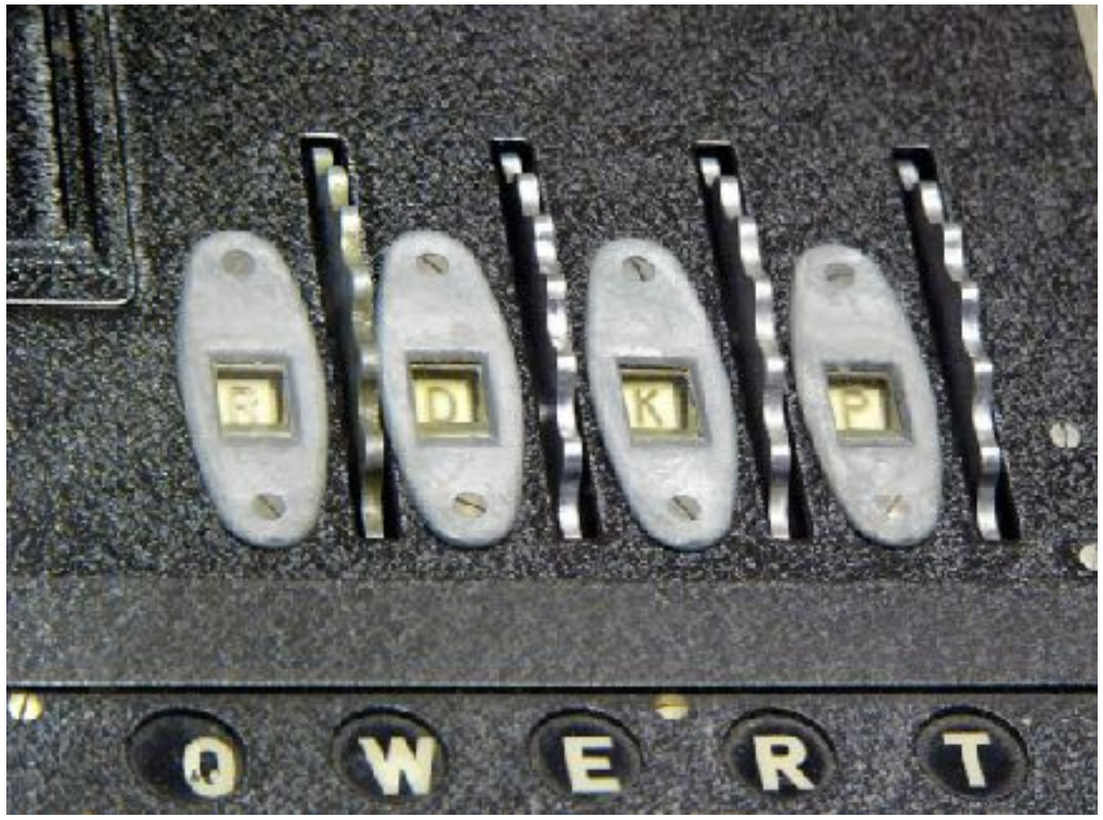

LS2 M102
H
G
F
E
D
C
B
A



Credit: Wikipedia user MesserWoland, https://creativecommons.org/licenses/by-sa/3.0/deed.en

1930s Enigma Setup (Changes each day)

1. Pick three rotors to use
2. Pick order for three rotors
3. Pick ring setting (rotate casing; changes turnovers)
4. Pick three initial rotor positions
5. Pick plugboard connections



Geheime Kommandosache

Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

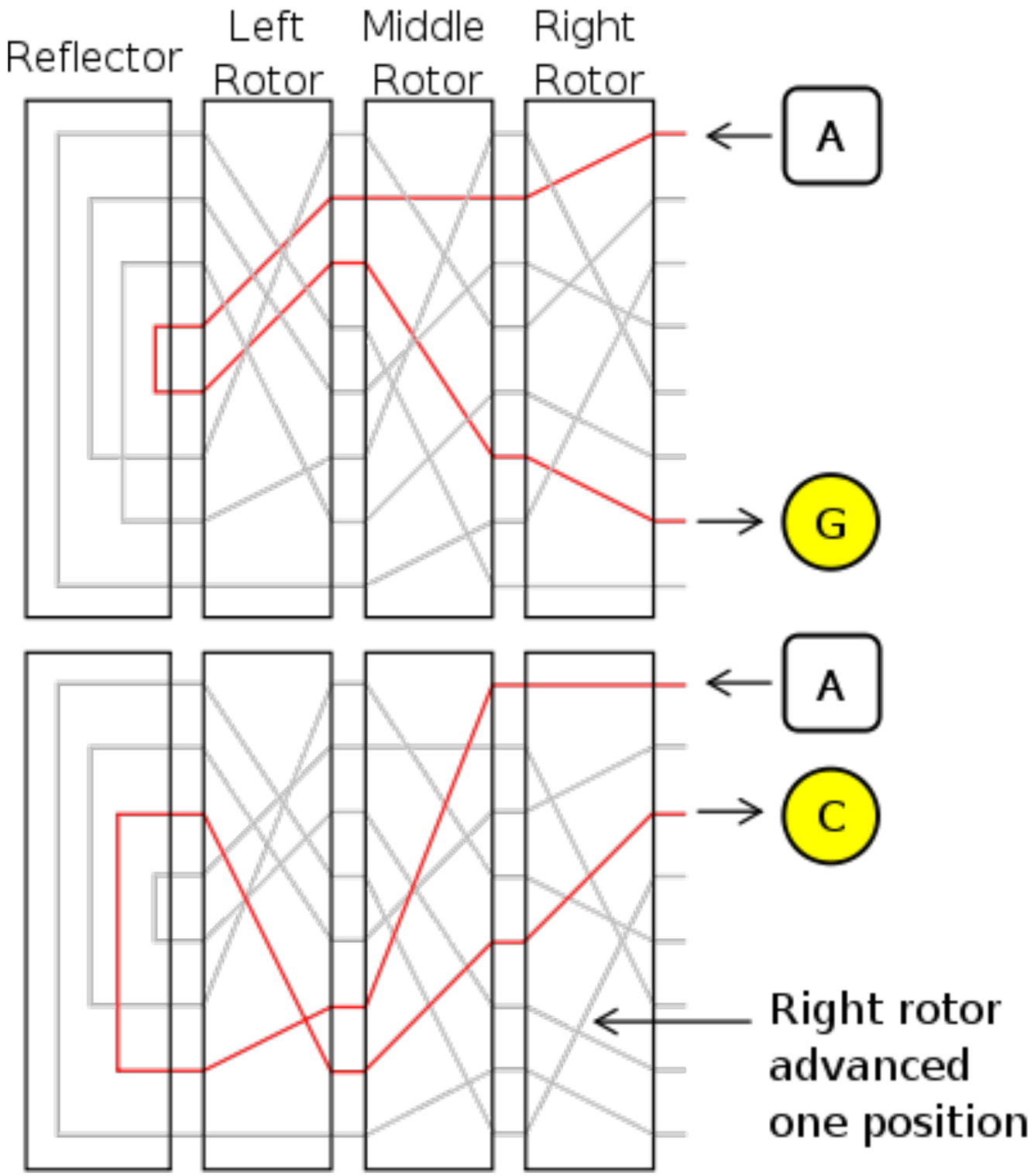
	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XG	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	occ	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	PI	SK	LD	RF	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GE	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nti	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vcx
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KF	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	leb	ieu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VI	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	LA	RX	FN	IS	WB	MH	ZV	bne	xzm	yak	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	III	V	03	25	10	CK	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	PK	PS	CM	upc	auf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NF	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CE	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PE	CU	QA	OD	NM	aty	mbb	mvc	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	ER	bok	rzw	kzc	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmc	pfw
St	3.	III	V	IV	03	23	04	DY	CF	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	FS	EK	IU	HX	AQ	GT	YO	PC	epq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PX	TR	OK	bel	ooi	ywv	sfo

Basic Enigma Usage: Encryption

1. Setup from key instructions
2. Type a letter
3. Board lights up with output letter, rotors move
4. Goto 2

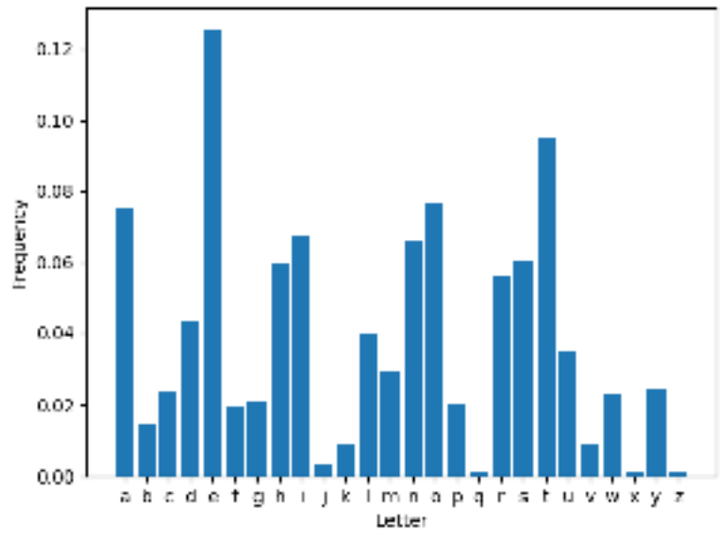
Basic Enigma Usage: Decryption - The same!

1. Setup from key instructions
2. Type a letter
3. Board lights up with output letter, rotors move
4. Goto 2



Credit: Wikipedia user MesserWoland, https://creativecommons.org/licenses/by-sa/3.0/deed.en

Enigma Randomization: Message Keys



Problem: All senders would apply same permutation to first character, then same to second etc.

Solution: Use “message keys” that randomize the initial rotor positions for each message:

1. Setup from key instructions
2. Pick a random rotor position (say **`RTP`**)
3. Encrypt and send **`RTPRTP`**
4. Reset rotor positions to **`RTP`**
5. Send message as before

Today and Tomorrow: Rejewski's Attack

Polish Cipher Bureau achieved a complete break of this version of Enigma!

We will assume:

1. We have captured many ciphertexts encrypted with the same day settings
2. We don't know any of the rotor wirings or day key settings

Our Goal: Recover message keys efficiently

We will only do one part of the attack; The entire attack involves many tedious steps.

The End