Cryptography during the two world wars, and wrap-up of classical ciphers.
Math 4440/5440.

First World War German Cipher: ADFGVX Cipher

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

3	4	2	1
D	G	X	G
X	G	D	G
A	A	D	D
D	G	X	G
F	X	D	G
F	D	F	A

Plaintext: ATTACK AT DAWN

Step 1: DG XG XG DG AA DD DG XG FX DG FD FA

Ciphertext: GGDGGAXDDXDFDXADFFGGAGXD

Comments

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

3	4	2	1
D	G	X	G
X	G	D	G
A	A	D	D
D	G	X	G
F	X	D	G
F	D	F	A

1. The thing on the left is a Polybius square; dates back to ancient greece.
2. It's purpose was coding theory: reduce the number of symbols in the alphabet from 26 to 5.
3. Long-distance signalling (e.g. holding up 1-5 firey torches) was less prone to error with a smaller alphabet.
4. Message length increases but error rate decreases.

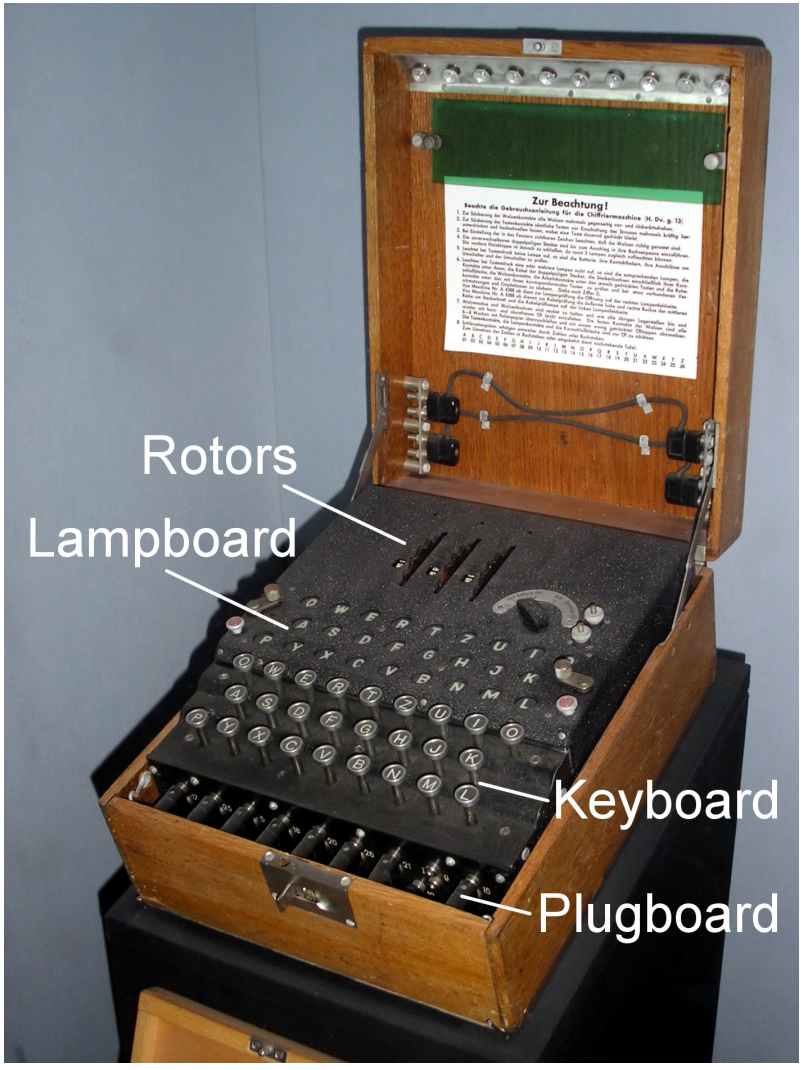
Some clues to cryptanalysis (French broke it)

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	1	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

3	4	2	1
D	G	X	G
X	G	D	G
A	A	D	D
D	G	X	G
F	X	D	G
F	D	F	A

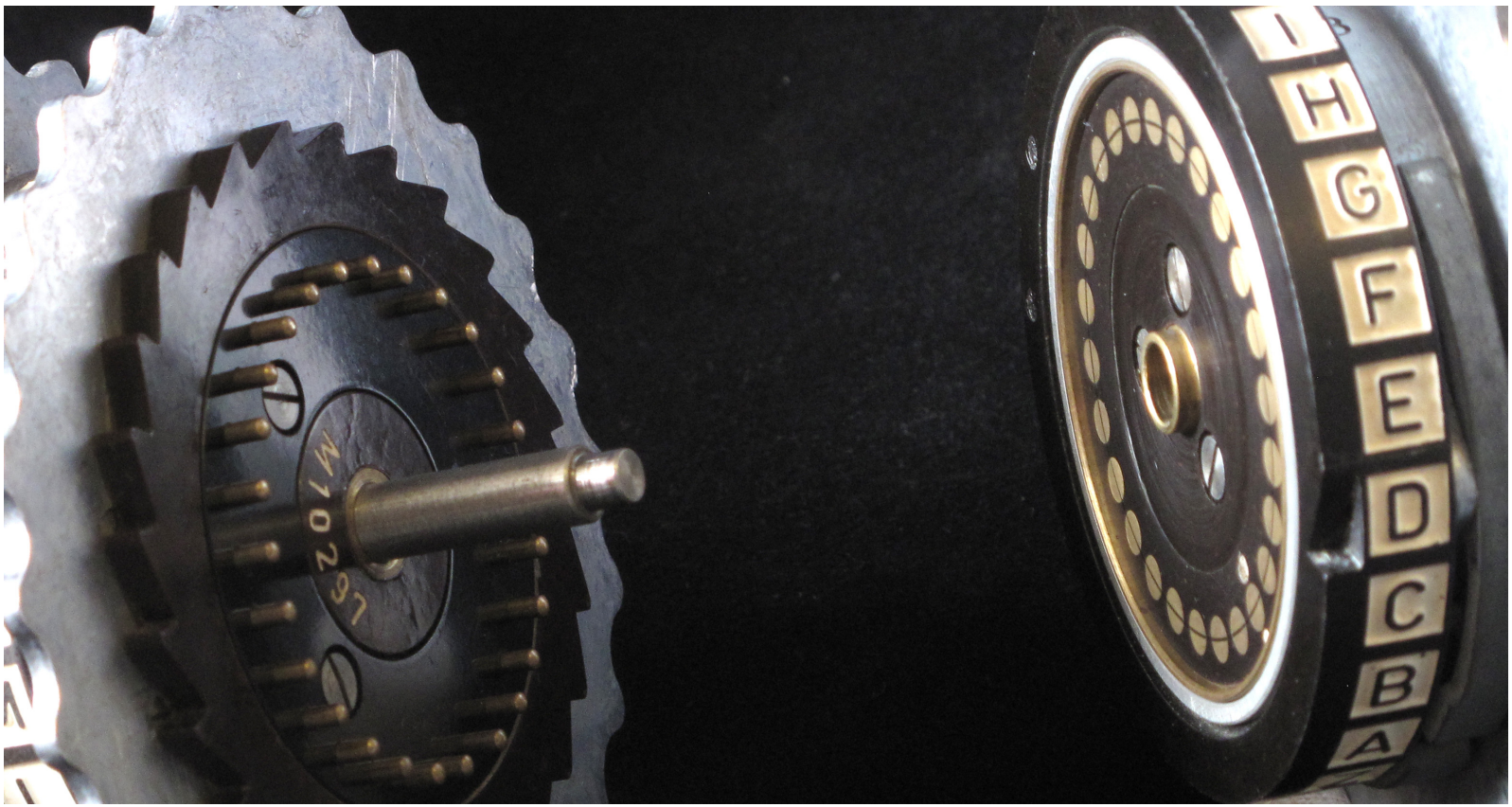
1. Because the keylength (3421) is even here, the letters in one column are either all column headers or all row headers.
2. Column header D has a different frequency than row header D.
3. Use frequency analysis to identify the likely columns.
4. Pair columns (e.g. put 3 next to 4) and do frequency analysis on the digraphs (DG, XG etc.) to see if the pairing is correct.

Second World War

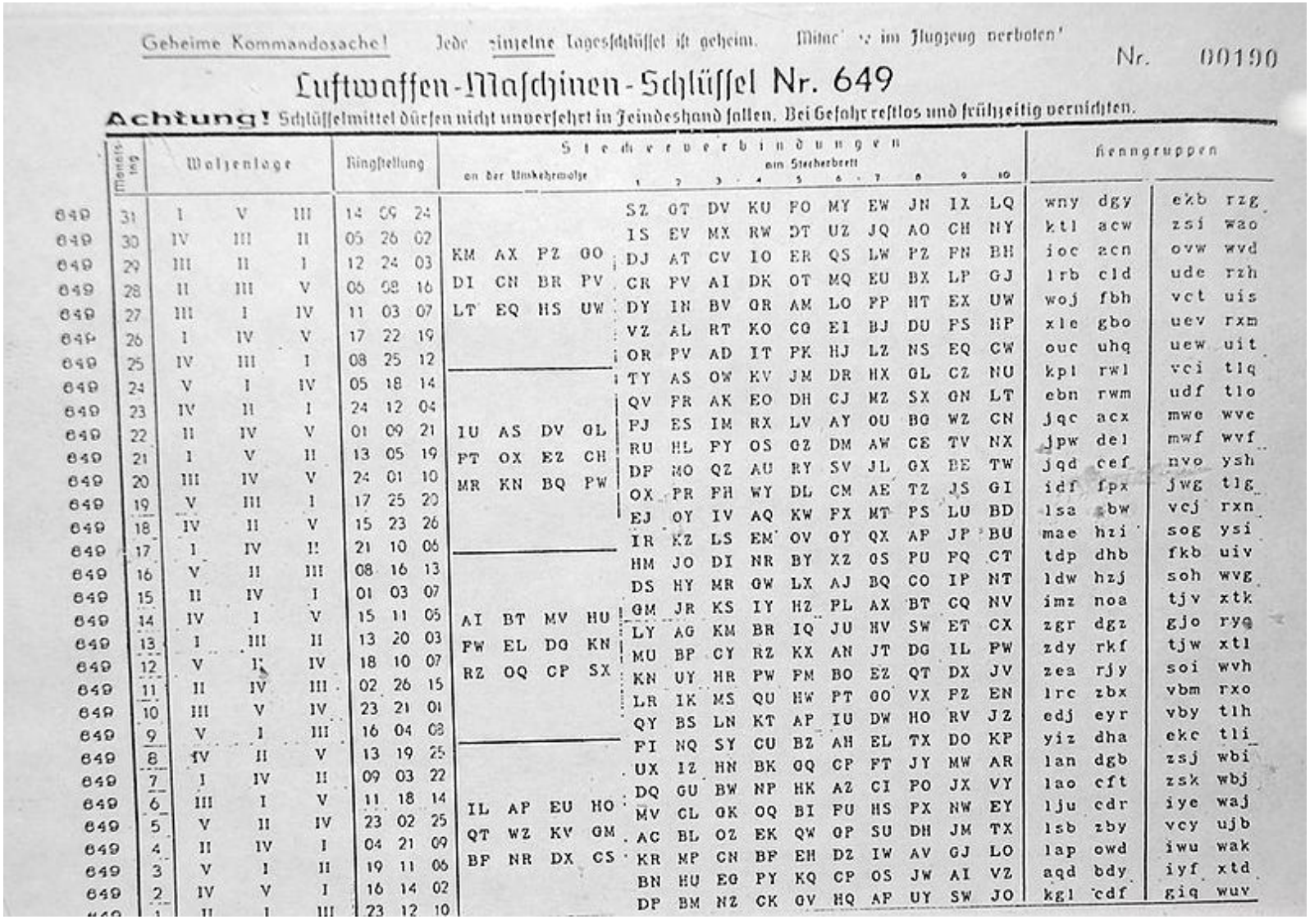


Wartime Enigma Machine

Second World War



Second World War



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

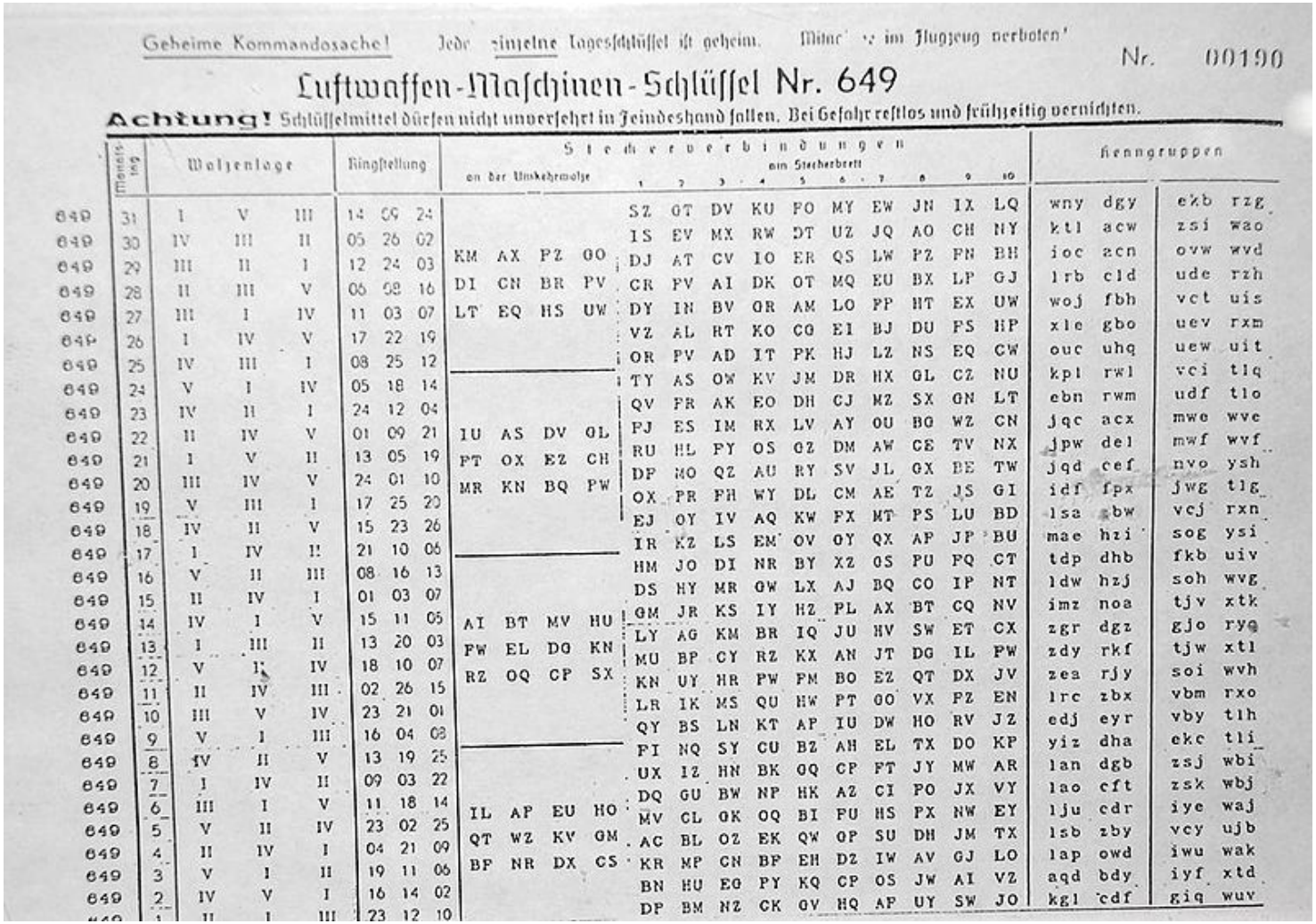
Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

	Monats-tag	Walzenlage			Ringstellung			Steckerverbindungen an der Umkehrwalze				Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31	I	V	III	14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	IV	III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	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	lrb	cld	ude	rzh
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	FP	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	rwl	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	PJ	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	DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	25	20					OX	PR	PH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26					EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	sbw	vcj	rxn
649	17	I	IV	II	21	10	06					IR	KZ	LS	EM	OV	OY	QX	AP	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	fkb	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	dgz	gjo	ryq
649	12	V	II	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	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	PZ	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	GU	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	IL	AP	EU	HO	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
		II	I	III	23	12	10					DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl	cdf	giq	wuv

Second World War



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

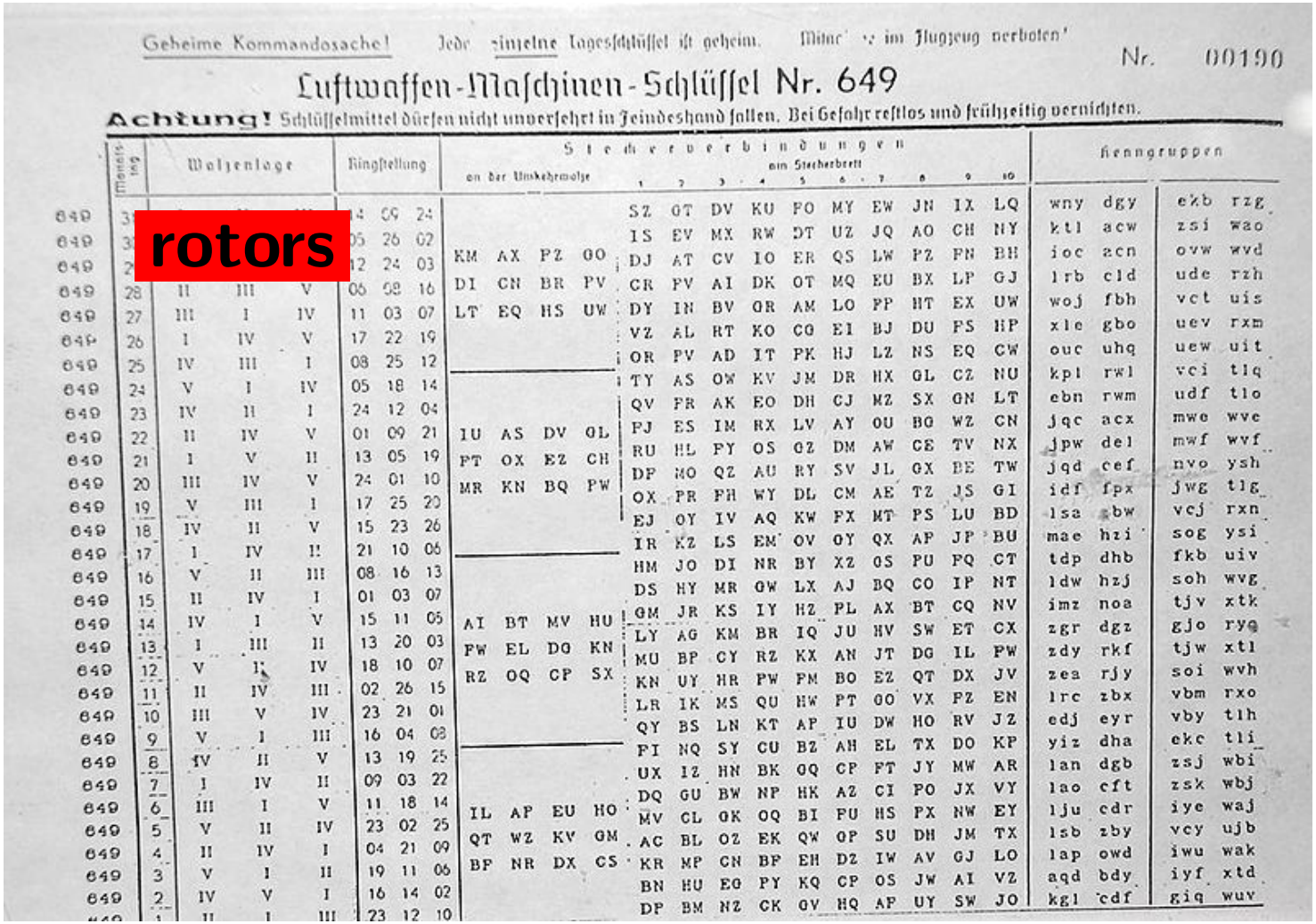
Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

	Monats-tag	Walzenlage			Ringstellung			Steckverbindungen an der Umkehrwalze				Steckverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen	
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	ktl	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	lrb	cld	ude	rzh
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	FP	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	rwl	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	PJ	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	FY	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	FR	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
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	AP	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	fkb	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	dgz	gjo	ryq
649	12	V	II	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	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	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
649	4	II	IV	I	04	21	09	BF	NR	DX	CS	AC	BL	OZ	EK	QW	GP	SU	DH	JM	TX	lsb	zby	vcy	ujb
649	3	V	I	II	19	11	06					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

Second World War



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnehmen im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

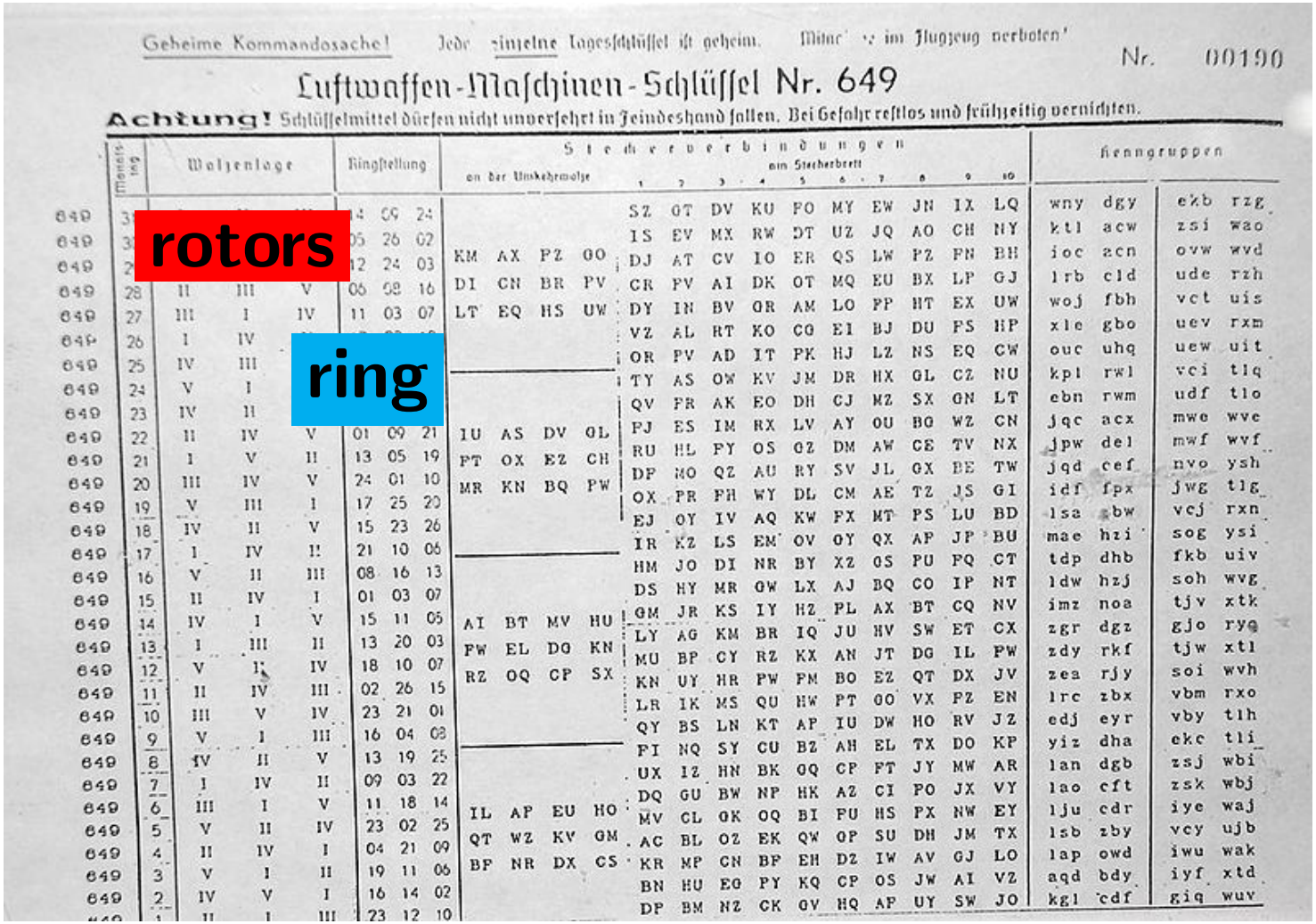
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

rotors

	Monats-tag	Walzenlage			Ringstellung			Steckverbindungen an der Umkehrwalze				Steckverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen	
649	31				14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg
649	30				05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29				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	lrb	cld	ude	rzh
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	FP	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	rwl	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	PJ	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	FY	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	FR	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26					EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae	hzi	sog	ysi
649	16	V	II	III	08	16	13					HM	JO	DI	NR	BY	XZ	GS	PU	FQ	CT	tdp	dhb	fkb	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	dgz	gjo	ryq
649	12	V	II	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	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					PI	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	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
649	4	II	IV	I	04	21	09	BP	NR	DX	CS	AC	BL	OZ	EK	QW	GP	SU	DH	JM	TX	lsb	zby	vcy	ujb
649	3	V	I	II	19	11	06					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

$5 \cdot 4 \cdot 3$

Second World War



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

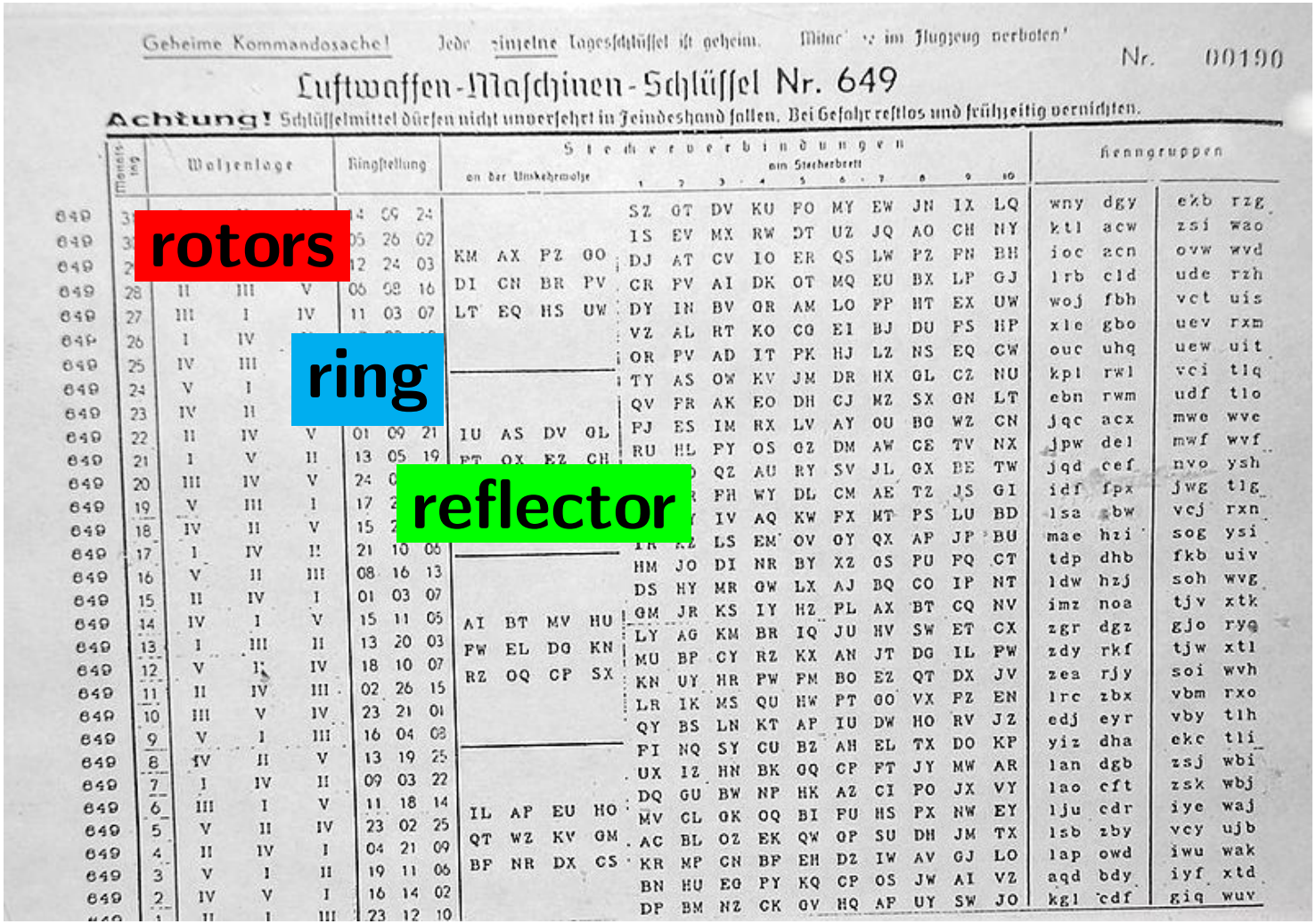
rotors

ring

Monats-tag	Walzenlage			Ringstellung	Steckverbindungen an der Umkehrwalze	Steckverbindungen am Steckerbrett 1 2 3 4 5 6 7 8 9 10	Kenngruppen	
649				14 09 24		SZ GT DV KU FO MY EW JN IX LQ	wny dgy	ekb rzg
649				05 26 02		IS EV MX RW DT UZ JQ AO CH NY	ktl acw	zsi wao
649				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	lrb cld	ude rzh
649	27	III	I	IV	11 03 07	LT EQ HS UW	DY IN BV GR AM LO FP HT EX UW	woj fbh	vct uis
649	26	I	IV				VZ AL RT KO CG EI BJ DU FS HP	xle gbo	uev rxm
649	25	IV	III				OR PV AD IT PK HJ LZ NS EQ CW	ouc uhq	uew uit
649	24	V	I				TY AS OW KV JM DR HX GL CZ NU	kpl rwl	vci tlq
649	23	IV	II				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	PJ 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 FY OS GZ DM AW CE TV NX	jpw del	mwf wvf
649	20	III	IV	V	24 01 10	MR KN BQ PW	DP MO QZ AU RY SV JL GX BE TW	jqd cef	nvo ysh
649	19	V	III	I	17 25 20		OX FR FH WY DL CM AE TZ JS GI	idf fpx	jwg tlg
649	18	IV	II	V	15 23 26		EJ OY IV AQ KW FX MT PS LU BD	lsa gbw	vcj rxn
649	17	I	IV	II	21 10 06		IR KZ LS EM OV OY QX AP JP BU	mae hzi	sog ysi
649	16	V	II	III	08 16 13		HM JO DI NR BY XZ GS PU FQ CT	tdp dhb	fkb 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 dgz	gjo ryq
649	12	V	II	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 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 PZ 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	IL AP EU HO	DQ GU BW NP HK AZ CI PO JX VY	lao cft	zsk wbj
649	5	V	II	IV	23 02 25	QT WZ KV GM	MV CL GK OQ BI FU HS PX NW EY	lju cdr	iye waj
649	4	II	IV	I	04 21 09	BF NR DX CS	AC BL OZ EK QW GP SU DH JM TX	lsb zby	vcy ujb
649	3	V	I	II	19 11 06		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
					23 12 10		DP BM NZ CK GV HQ AP UY SW JO	kgl cdf	giq wuv

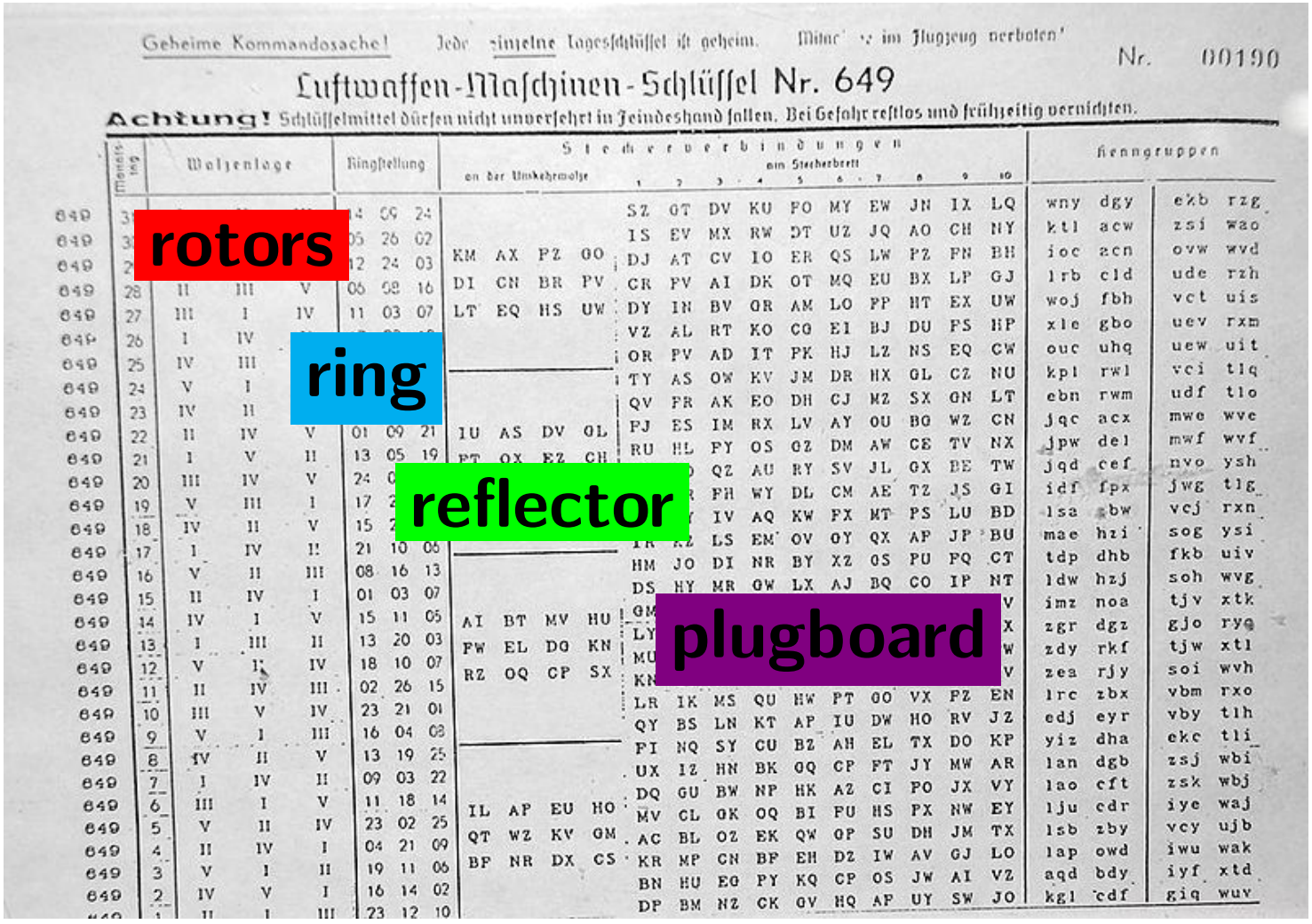
$5 \cdot 4 \cdot 3 \cdot 26^3$

Second World War



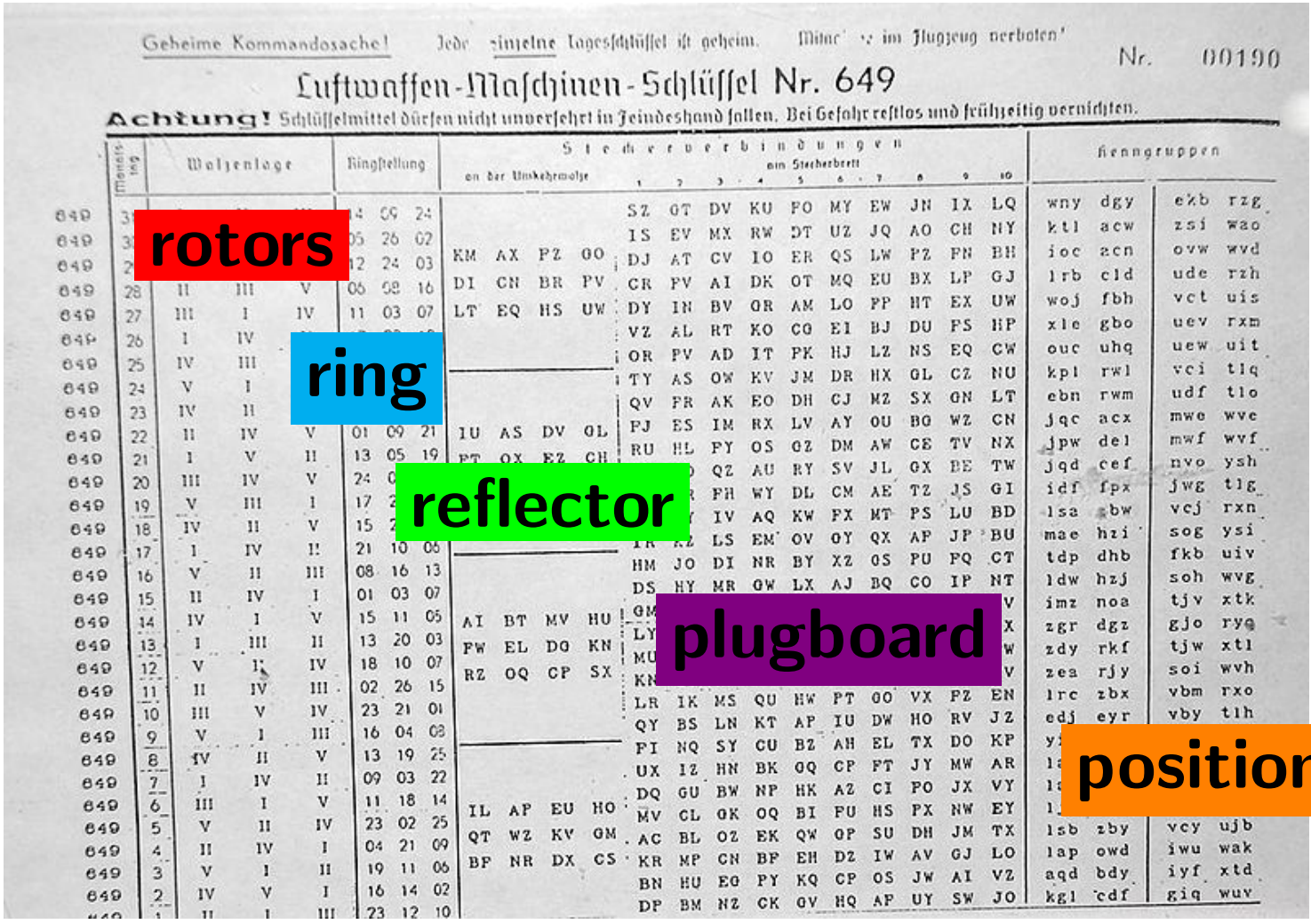
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12})$

Second World War



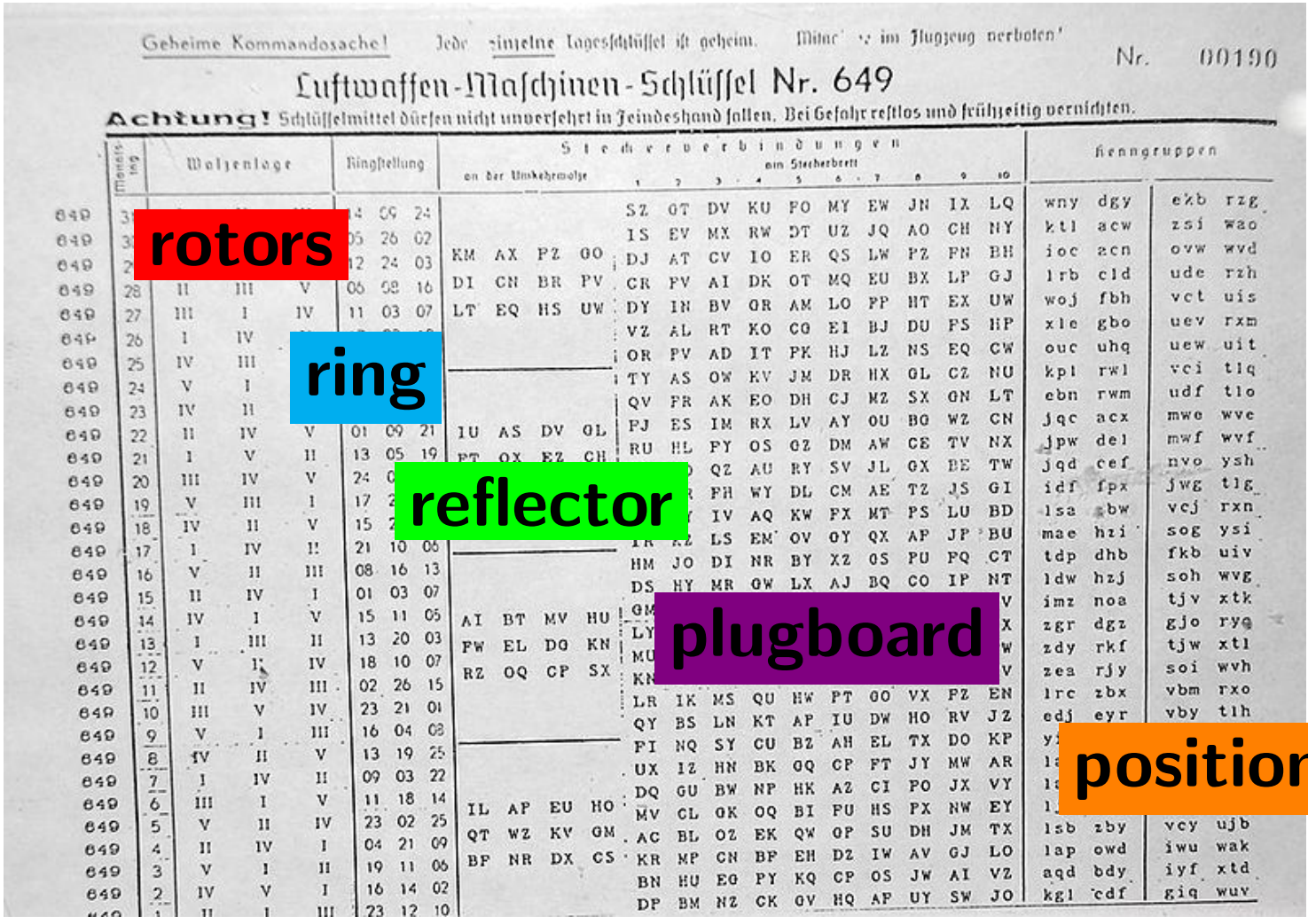
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10})$

Second World War



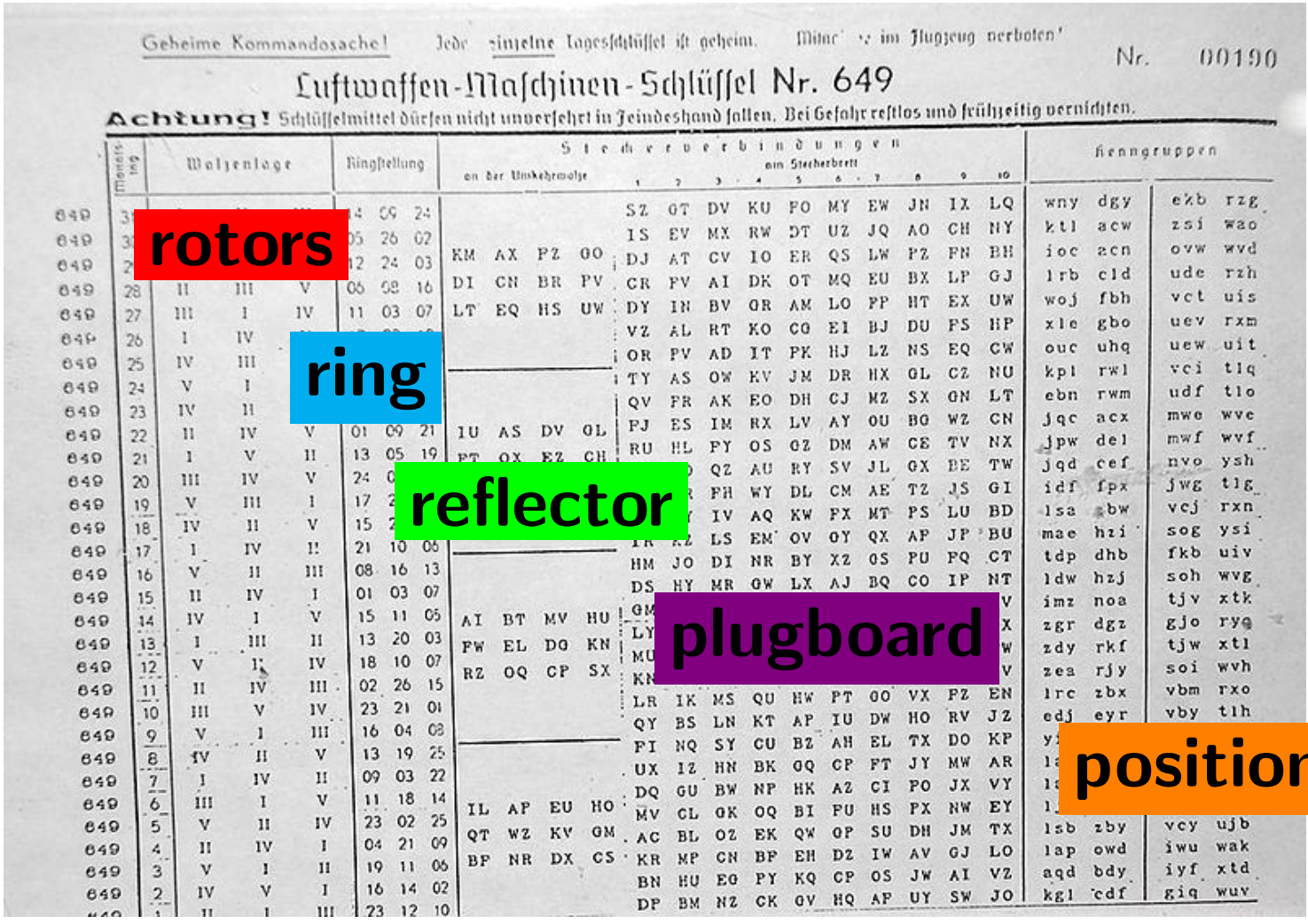
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3$

Second World War



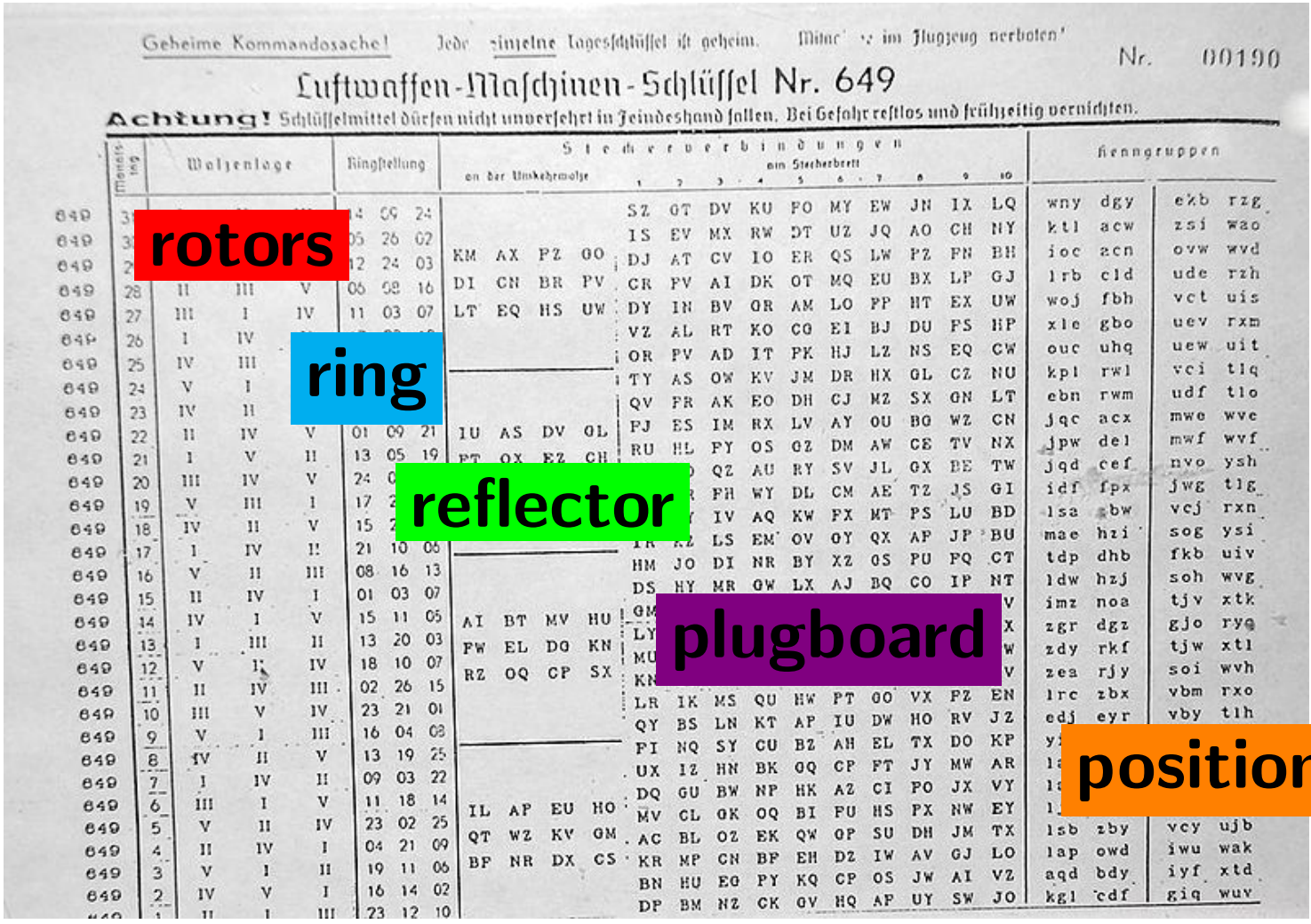
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq 150$ undecillion

Second World War



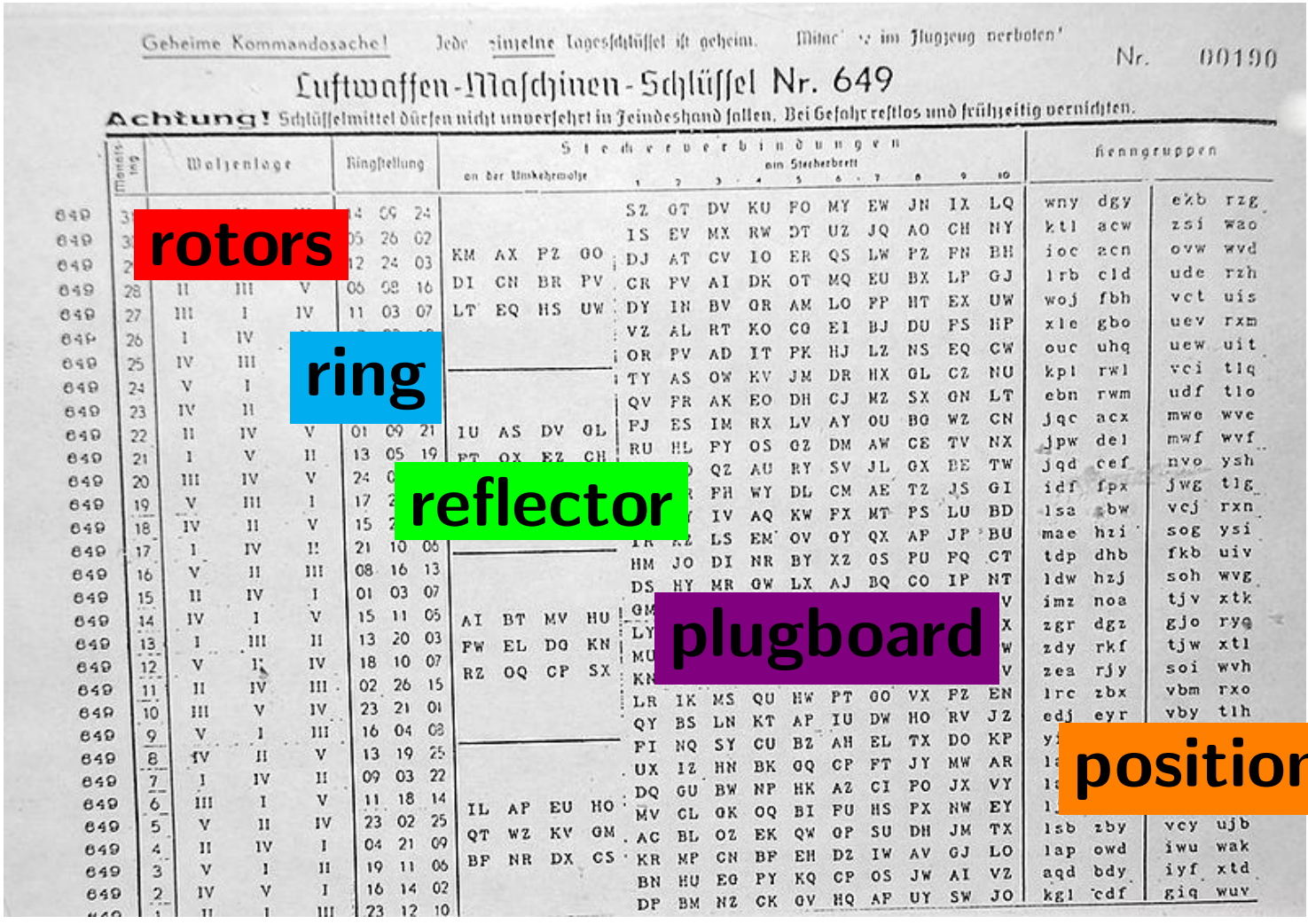
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion

Second World War



$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion 931 nonillion

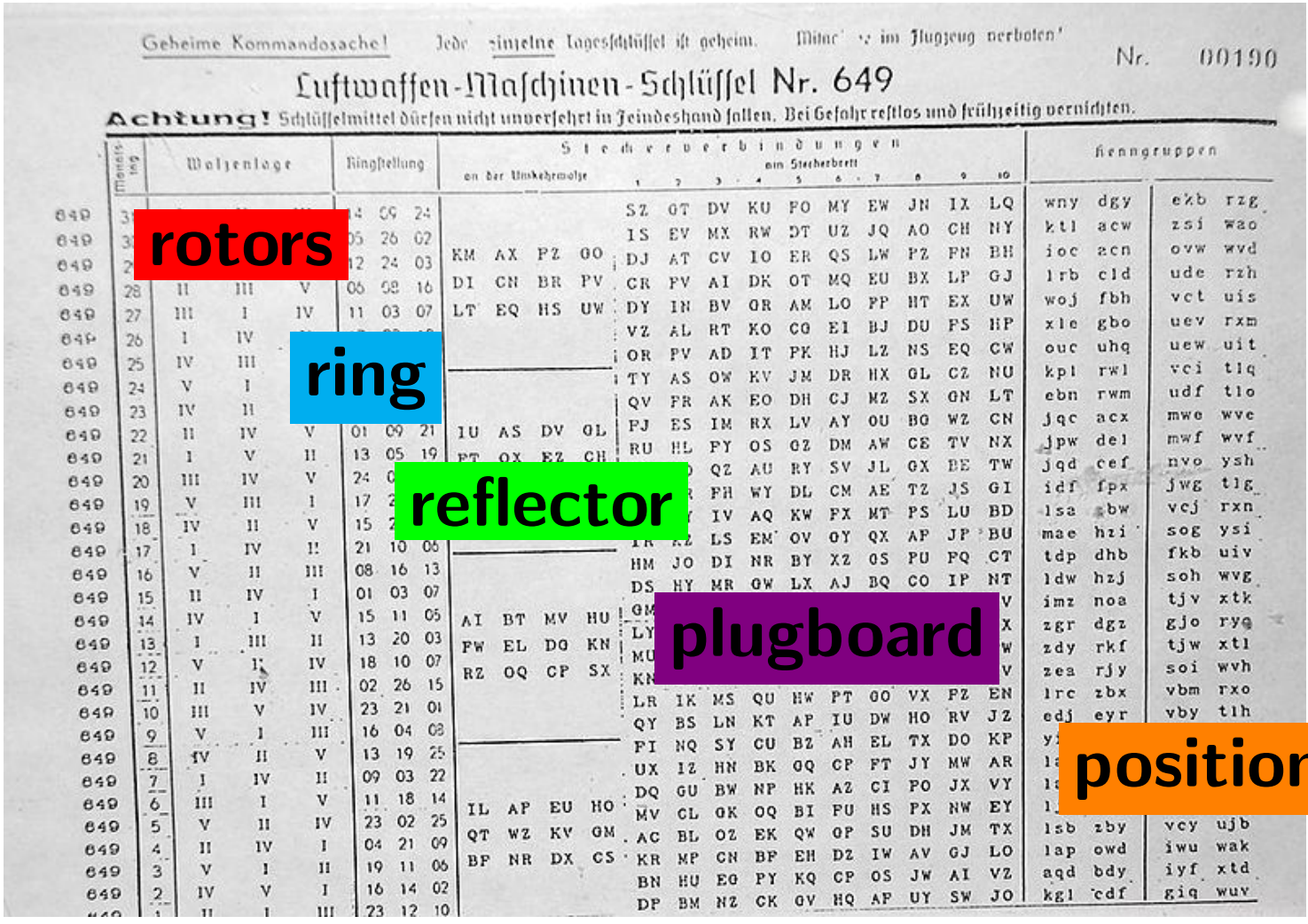
Second World War



$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion

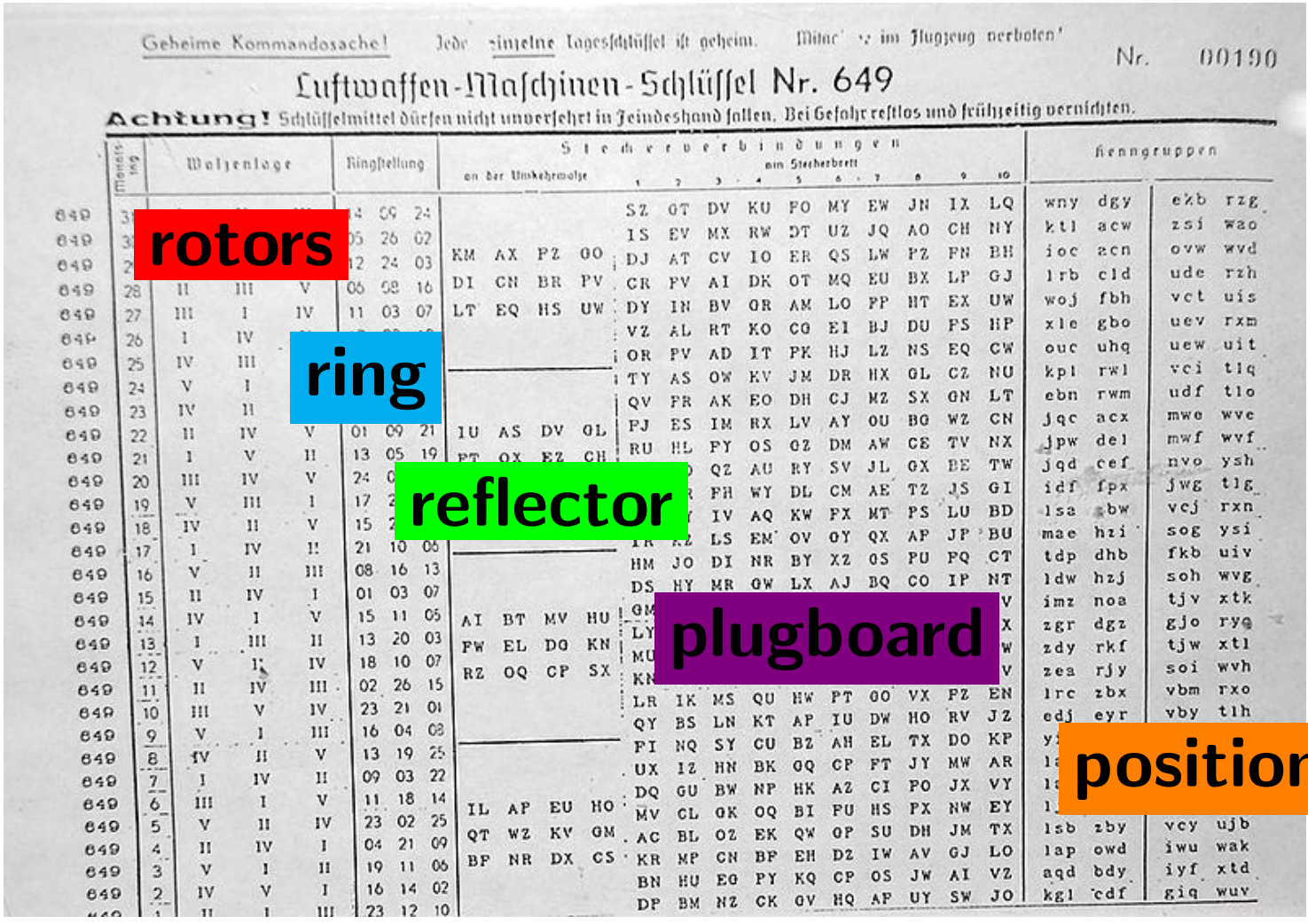
789 decillion 931 nonillion 331 octillion

Second World War



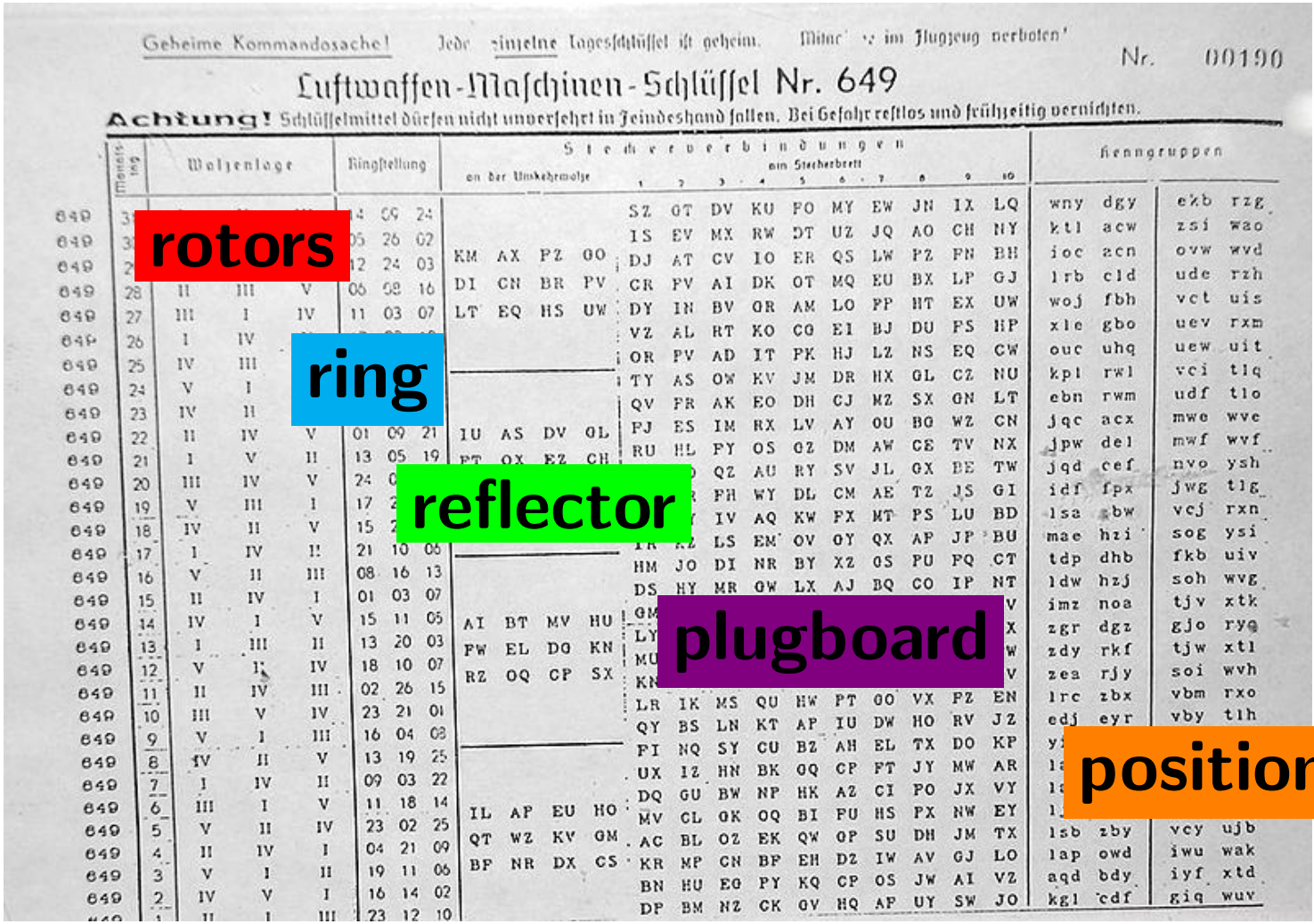
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion
789 decillion 931 nonillion 331 octillion 314 septillion

Second World War



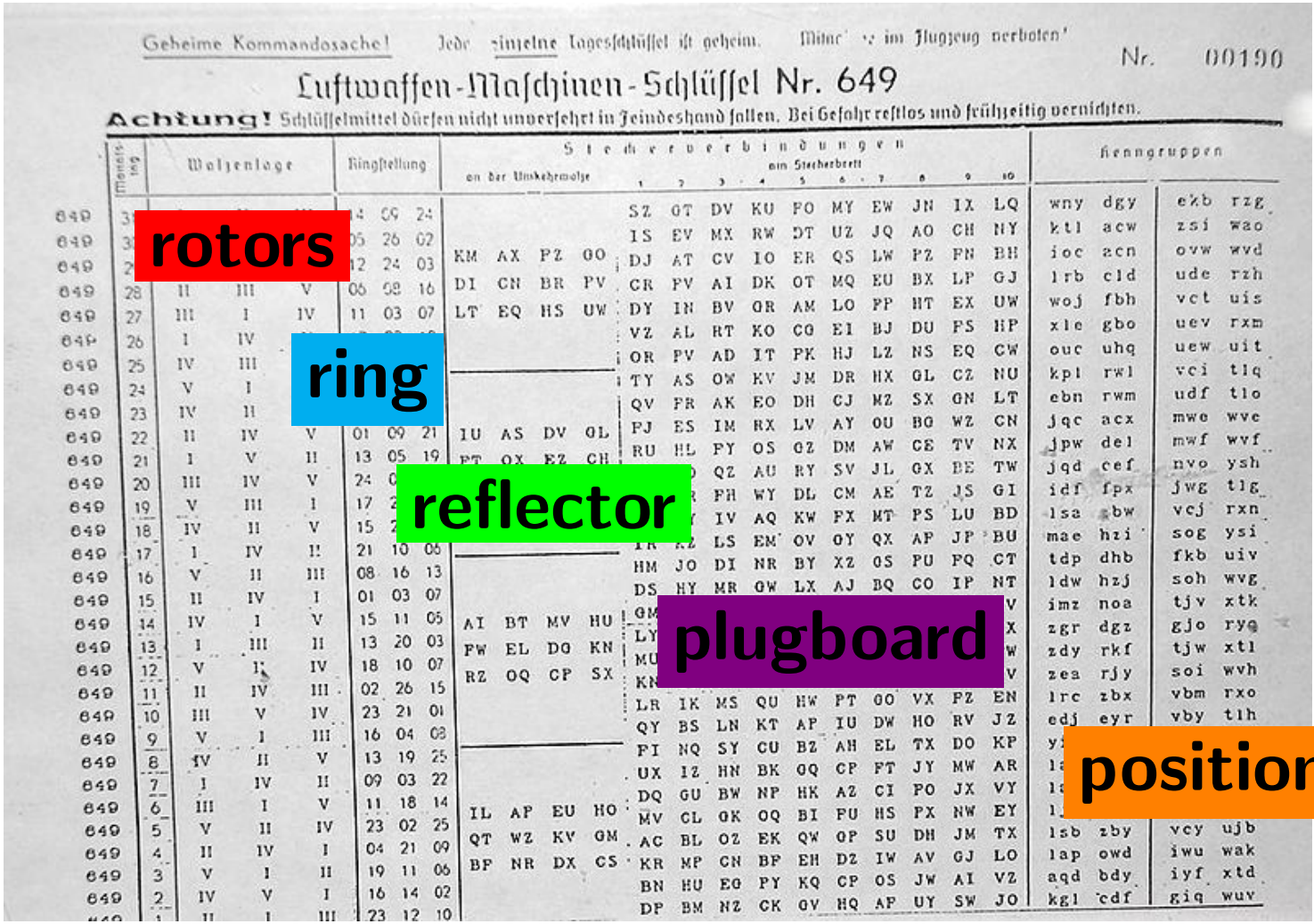
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion

Second World War



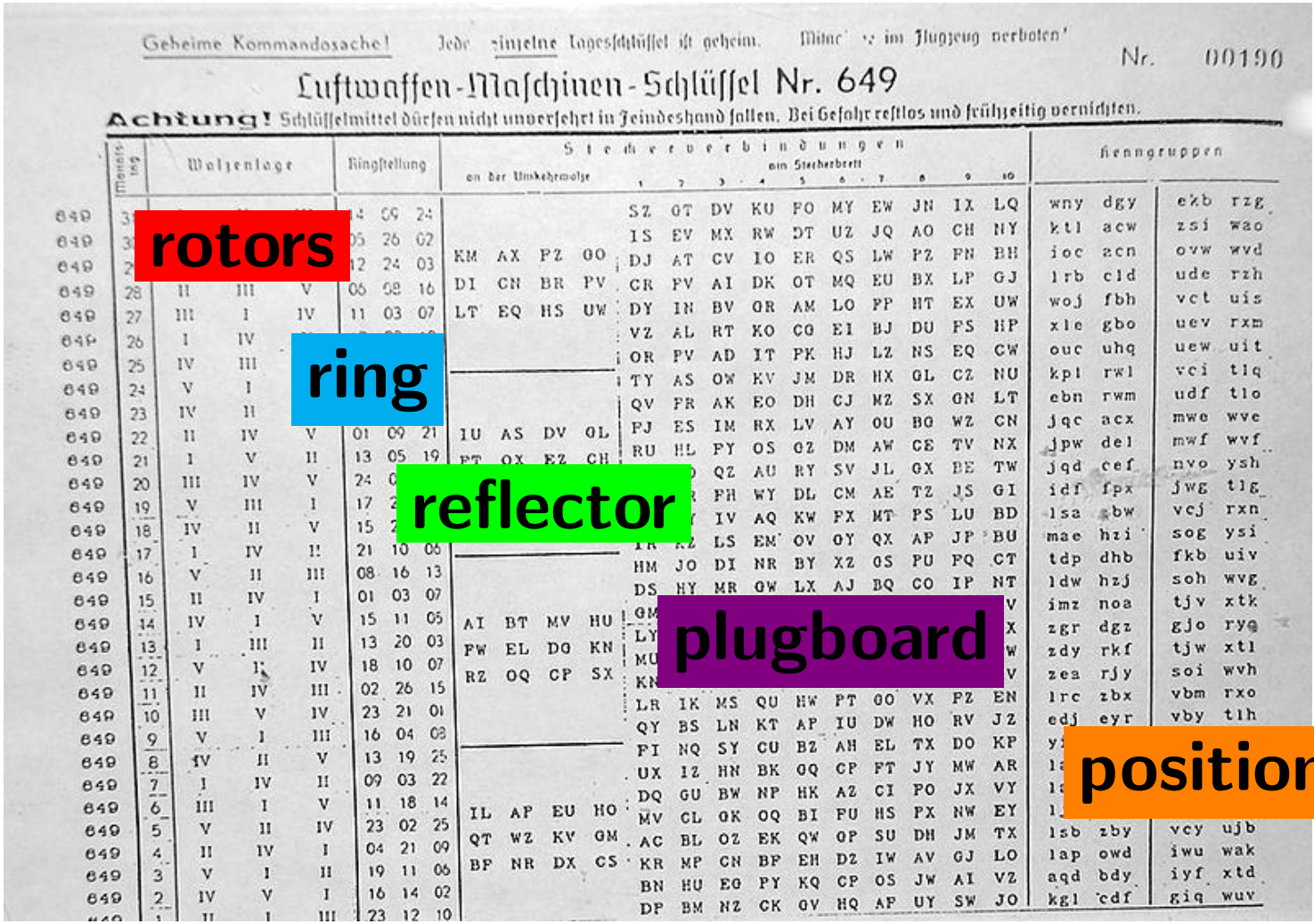
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion 42 quintillion

Second World War



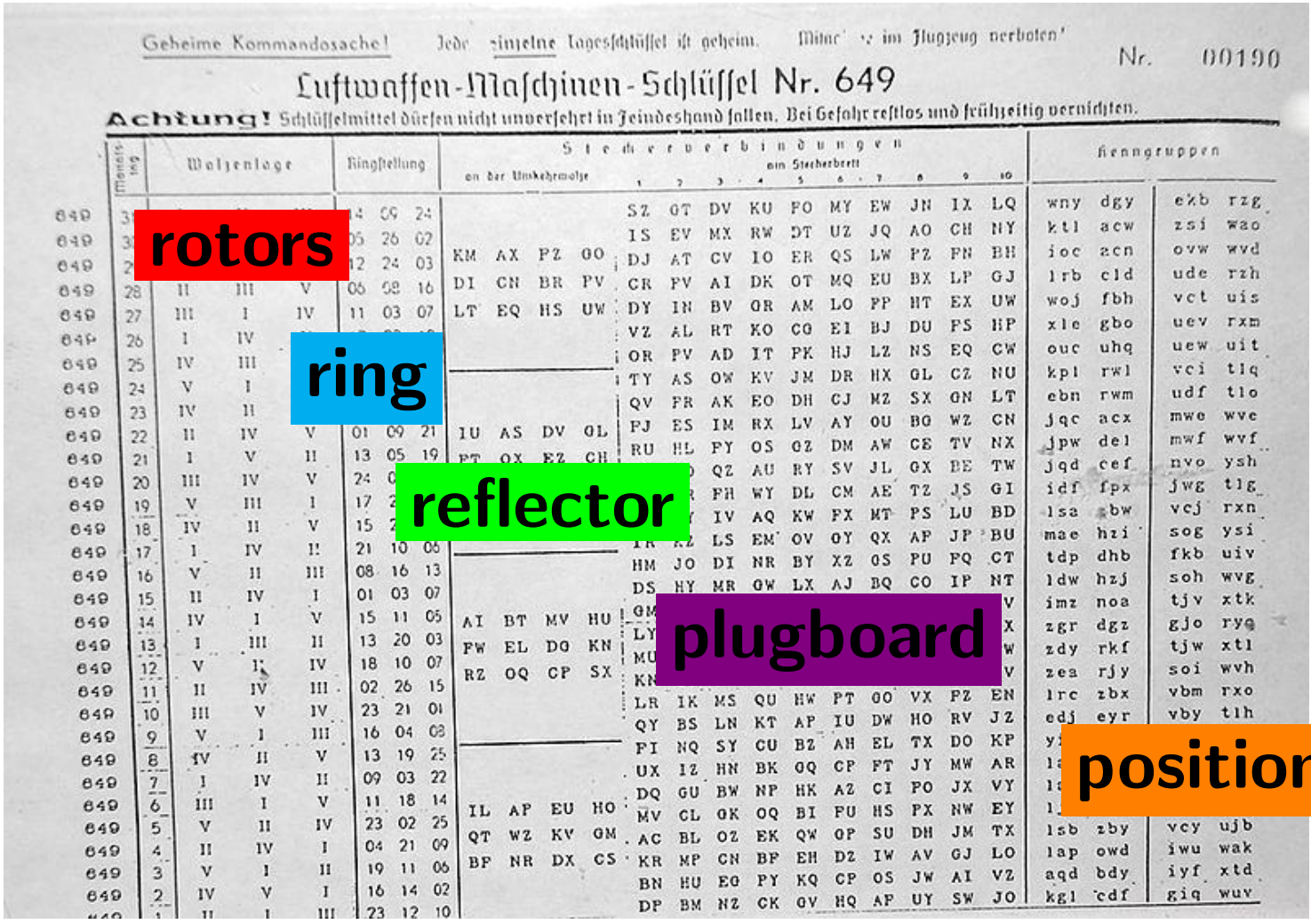
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion
789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
42 quintillion 76 quadrillion

Second World War



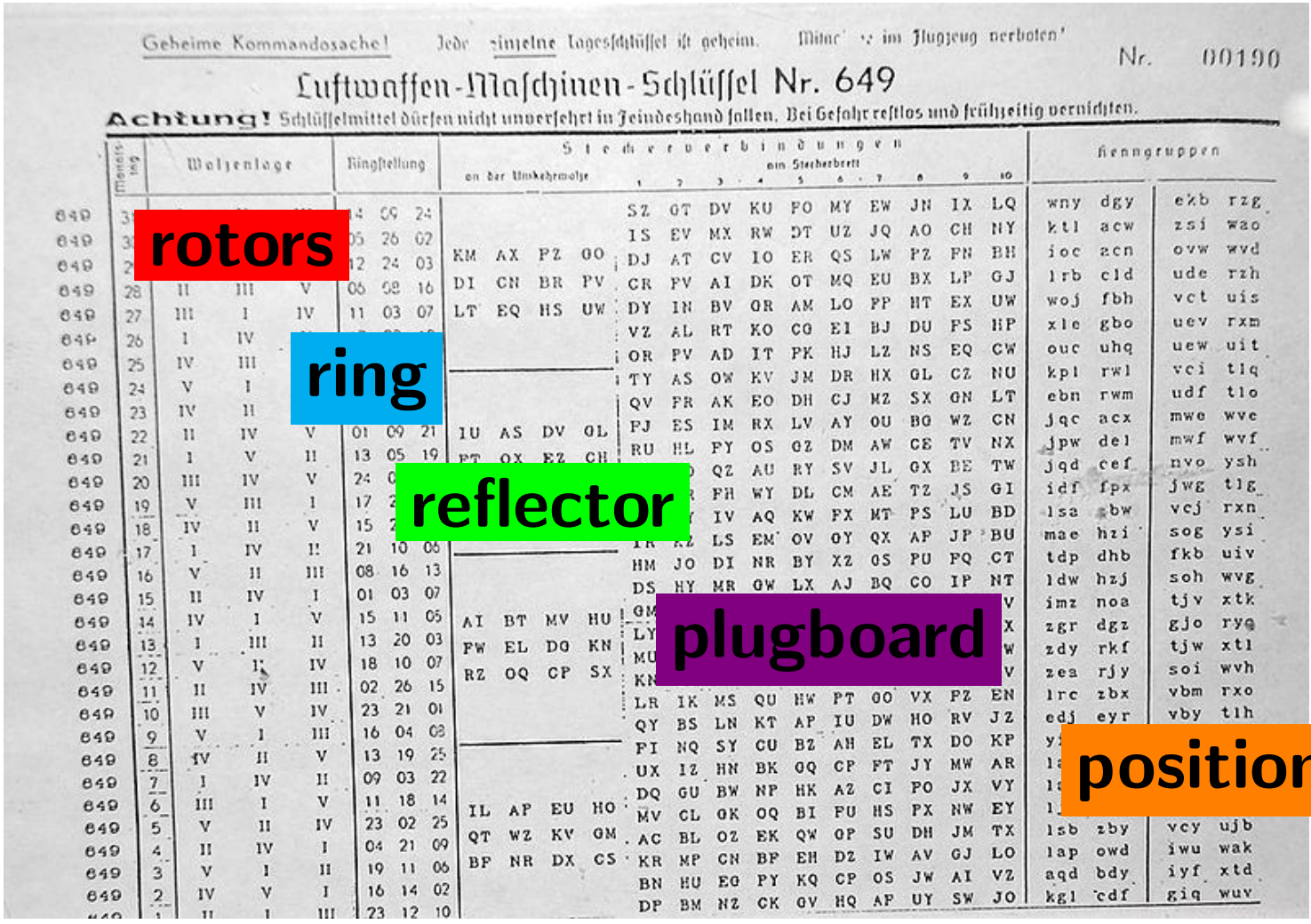
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion
789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
42 quintillion 76 quadrillion 184 trillion

Second World War



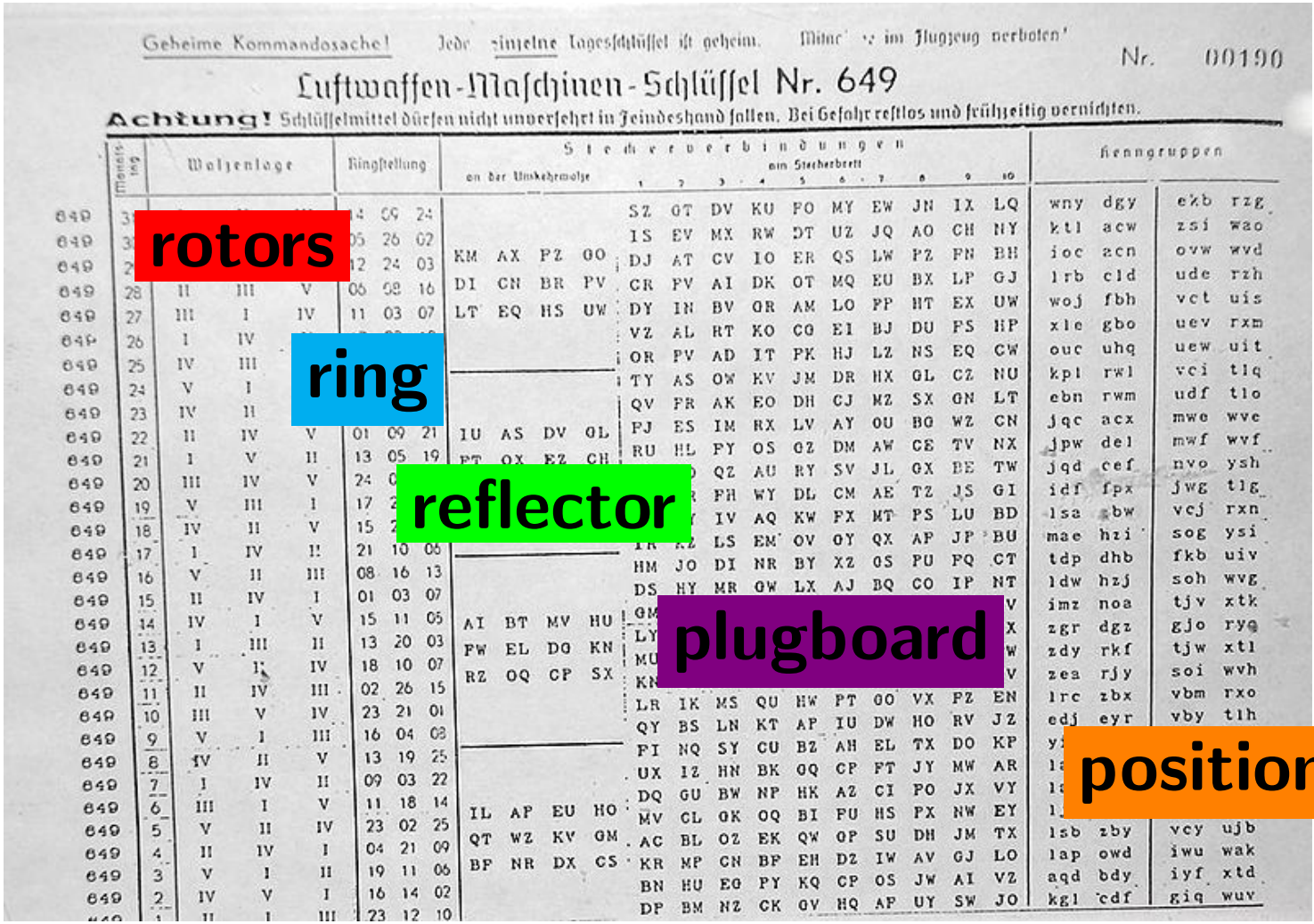
$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion
789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
42 quintillion 76 quadrillion 184 trillion 530 billion

Second World War



$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million

Second World War

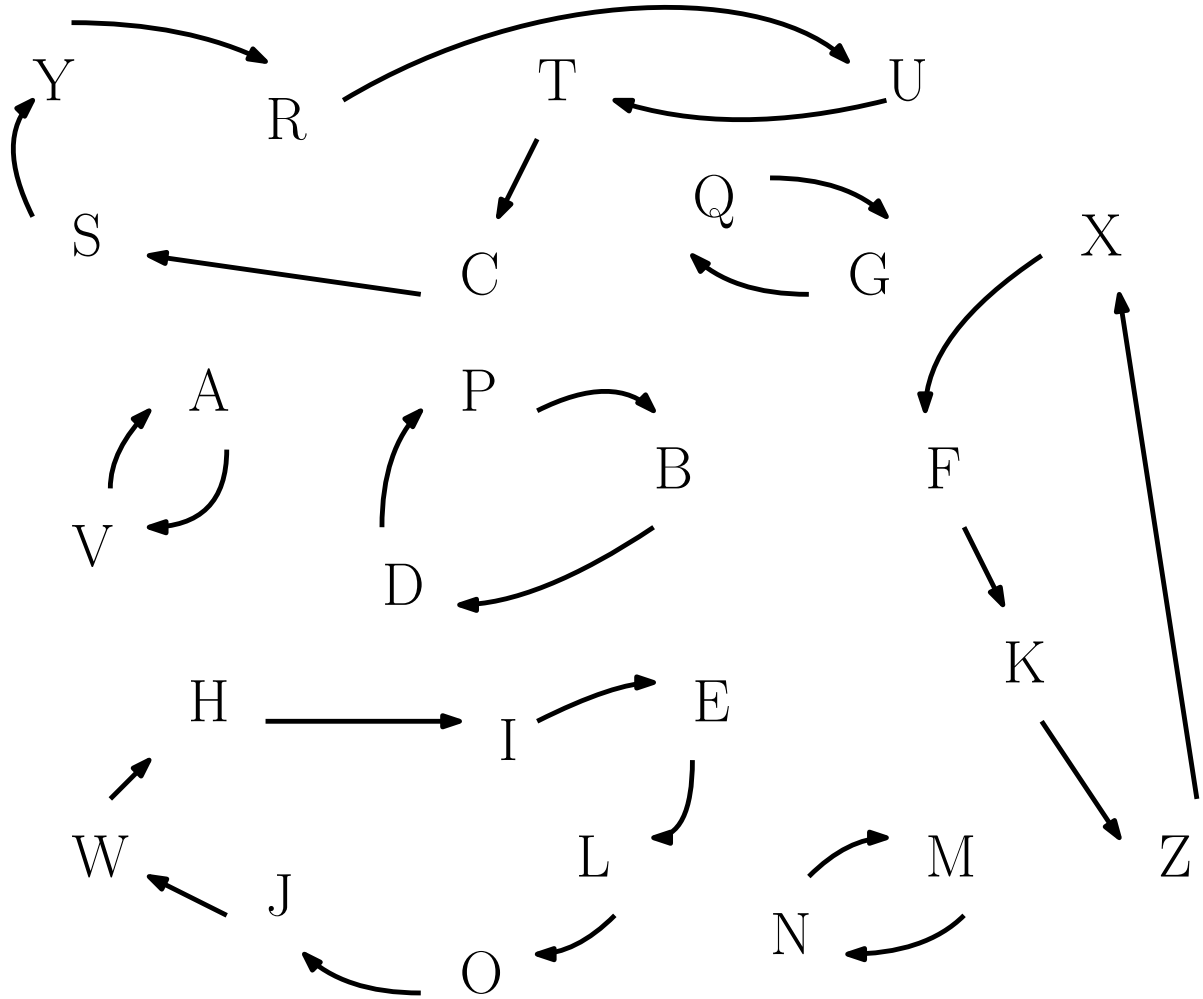


$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq$ 150 undecillion 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million

$\simeq 10^{38}$ keys

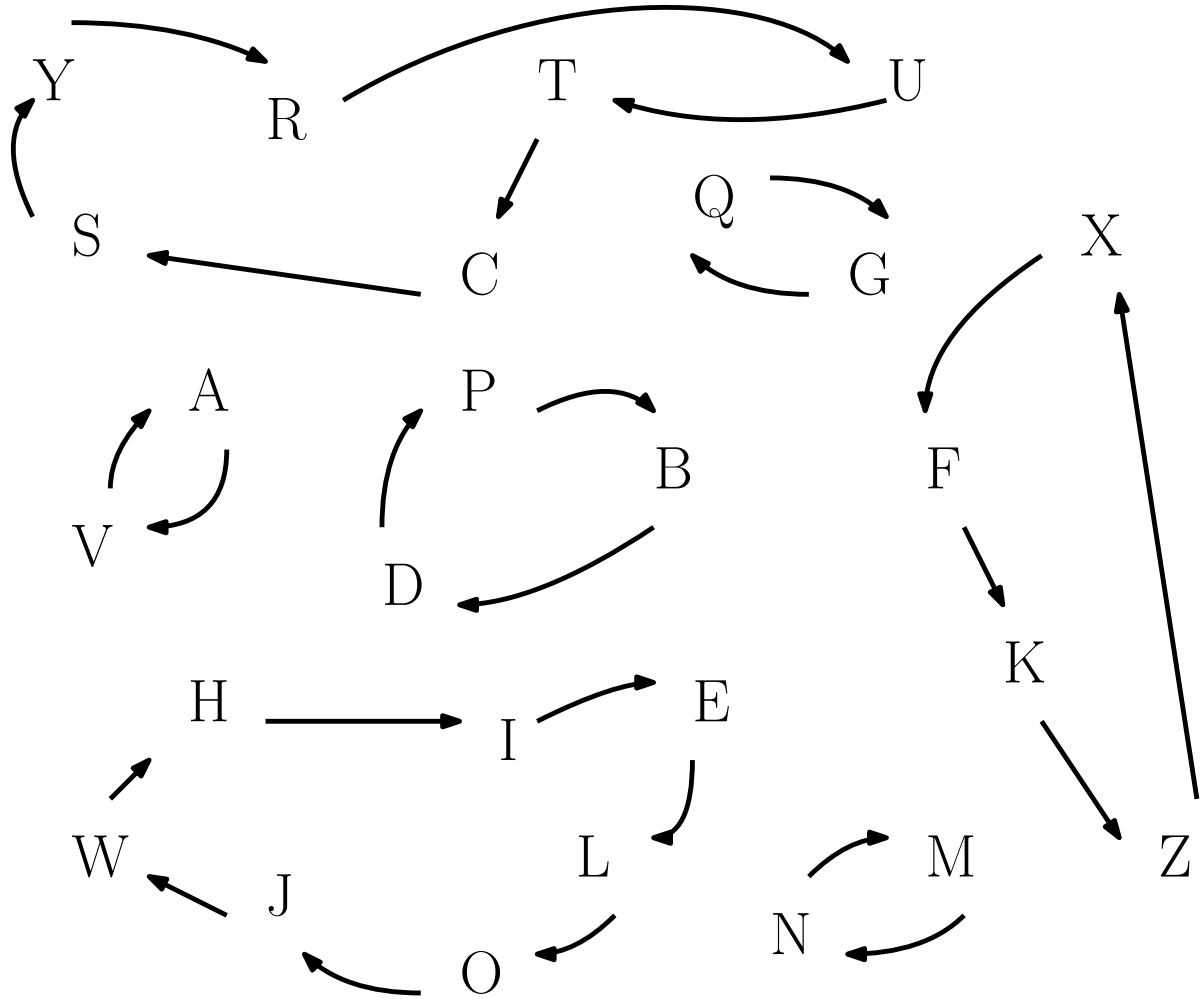
Second World War

A random permutation of the alphabet:



Second World War

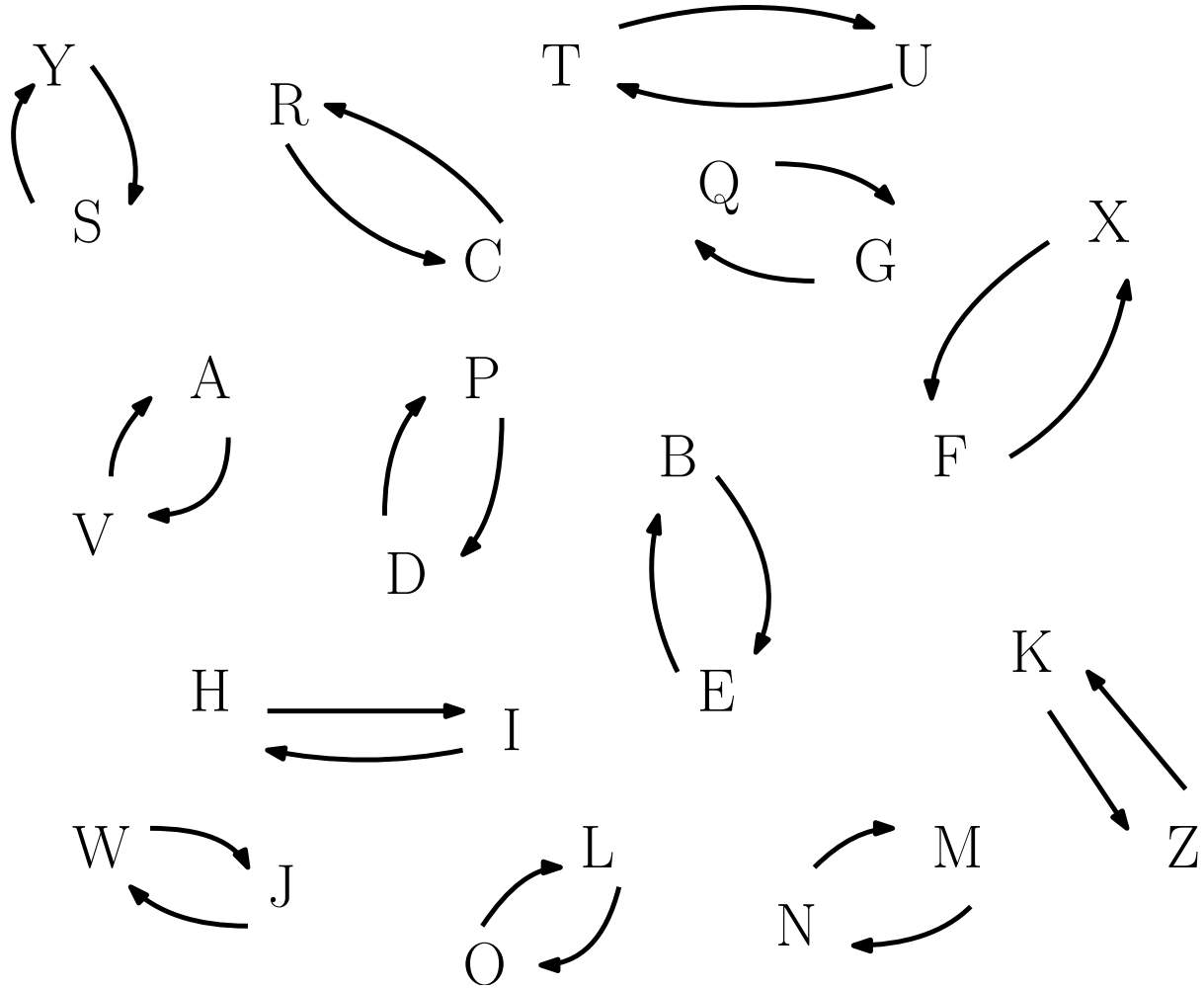
A random permutation of the alphabet:



Cycle structure: 6-2-2-3-4-7-2

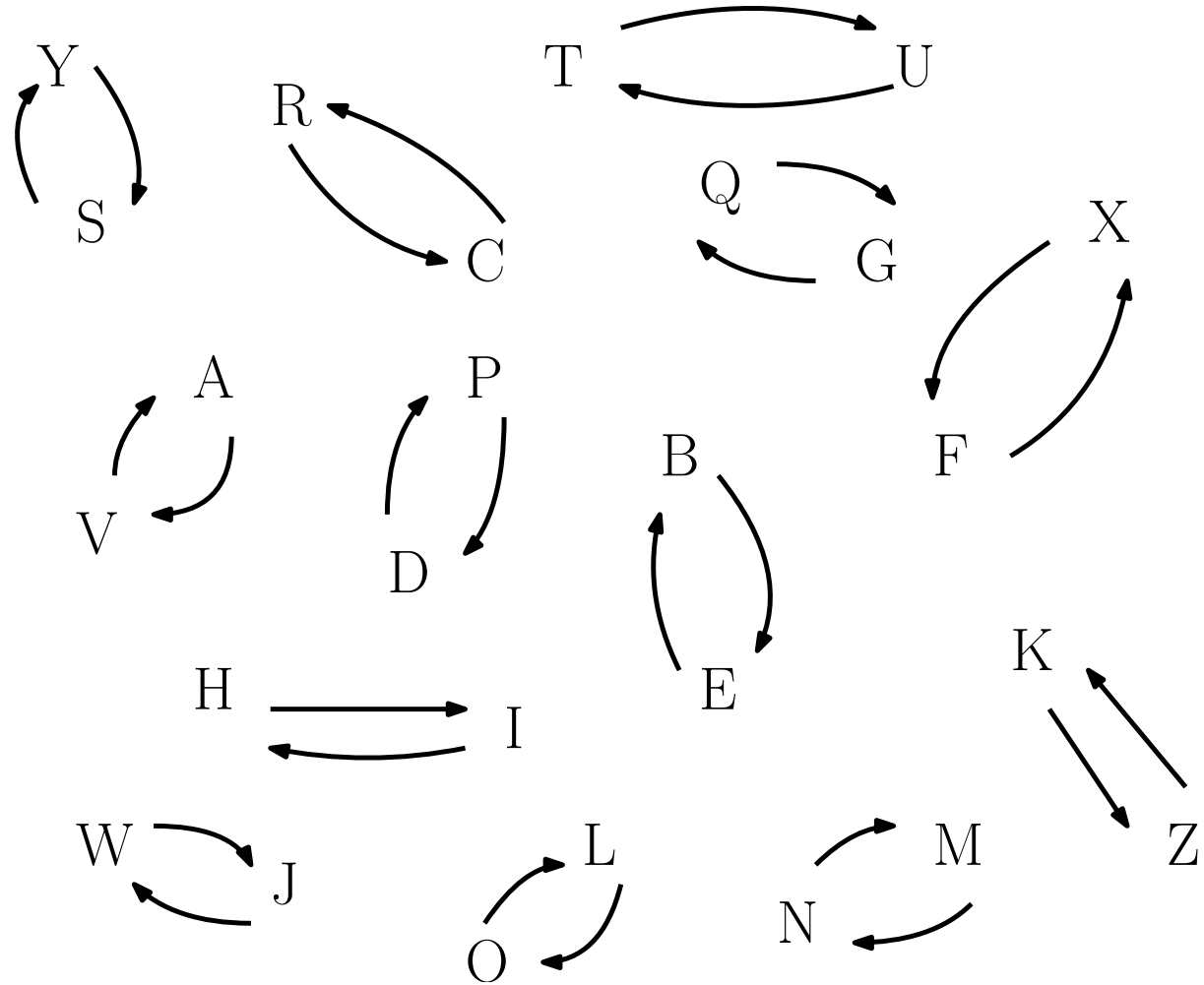
Second World War

An enigma permutation of the alphabet:



Second World War

An enigma permutation of the alphabet:



Cycle structure: 2-2-2-2-2-2-2-2-2-2-2-2-2-2

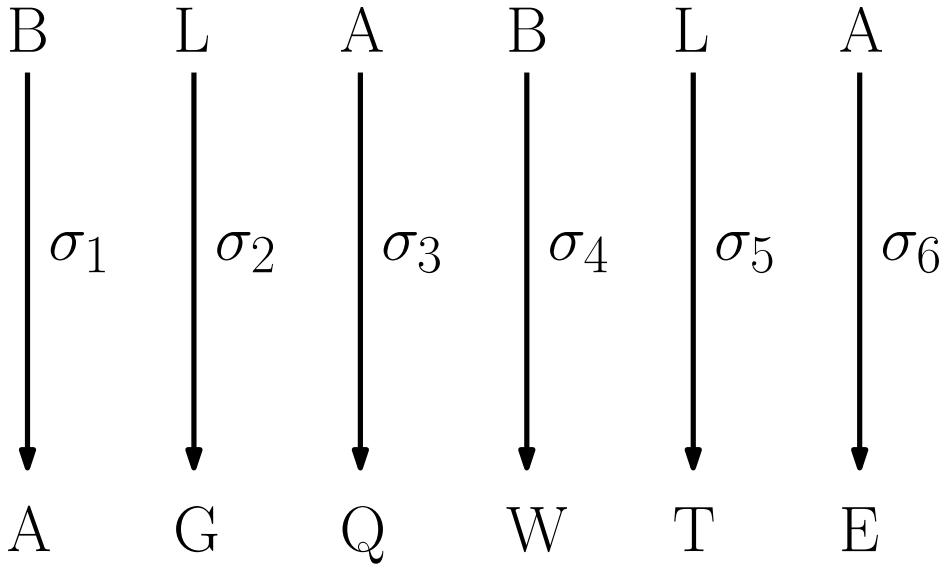
Don't use just one daily key!

1. If you use the same daily key on all messages that day, then one could try frequency analysis on all the first characters of all the messages. Then frequency analysis on all second characters, etc.
2. So, choose a random message key (rotor start positions, e.g. BLA) and send that using the daily key.
3. Then send the message in the message key.
4. BUT: radio is noisy, so send it twice (send BLABLA encrypted with daily key).

Cryptanalysis of Enigma

Message key: BLA

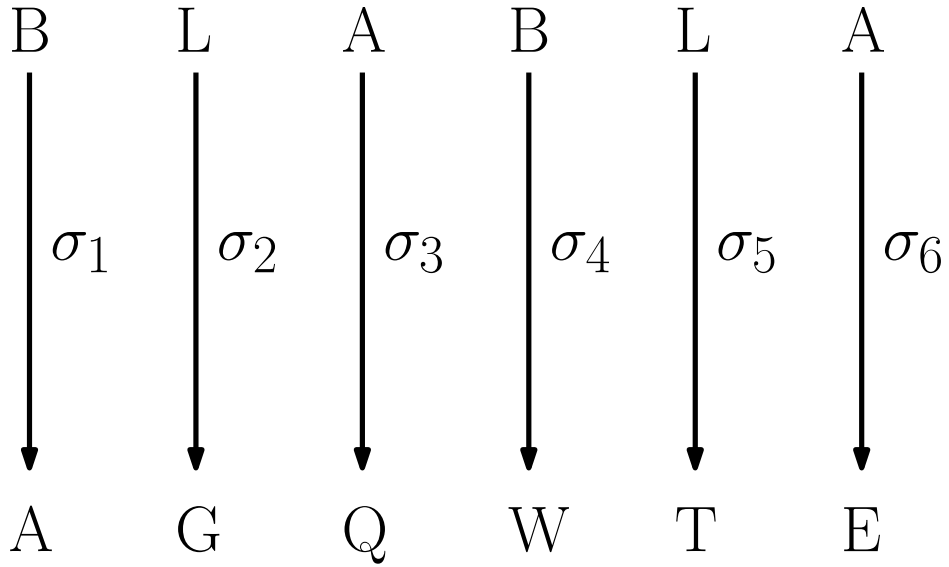
Encrypted message key (using daily key):



Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



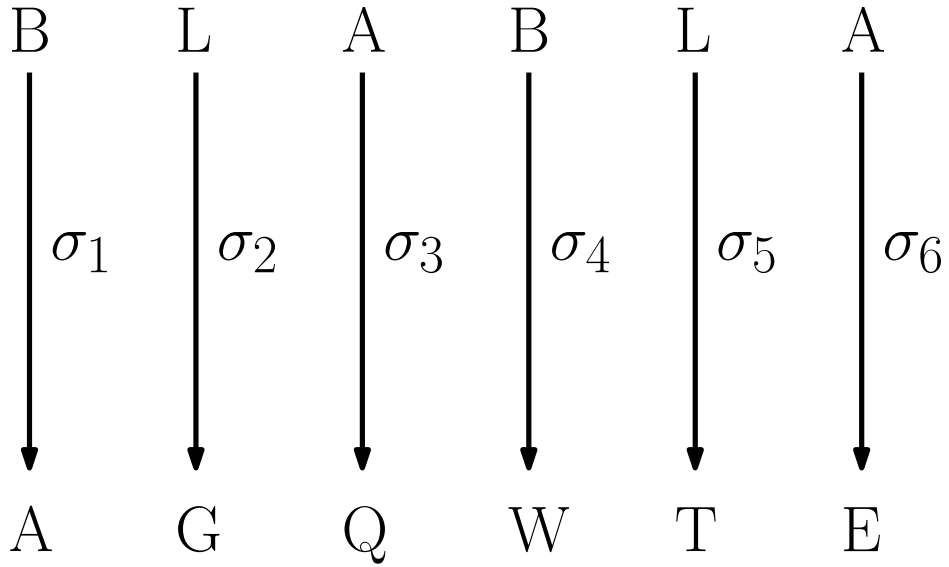
Learned information about $\sigma_4 \circ \sigma_1$:

$$A \to W$$

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

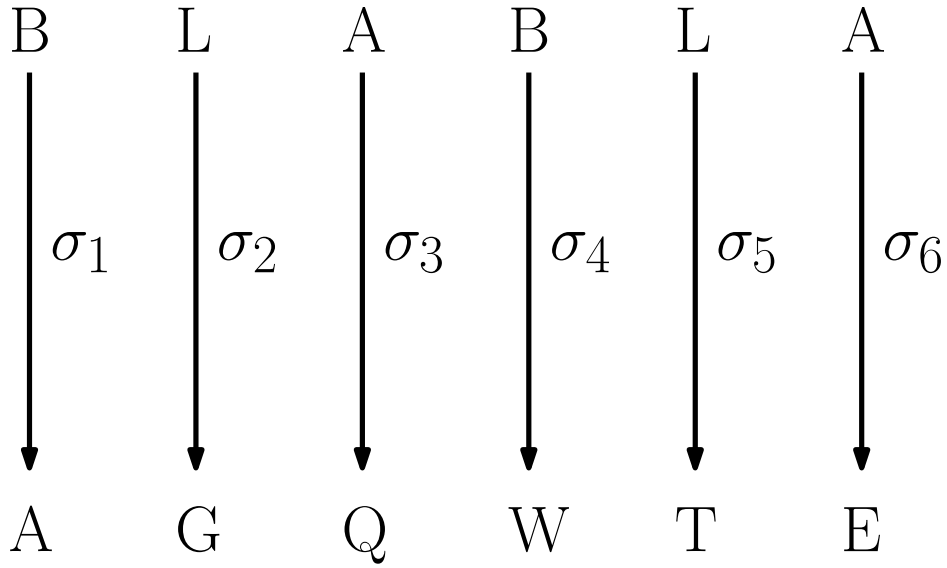
$$A \to W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

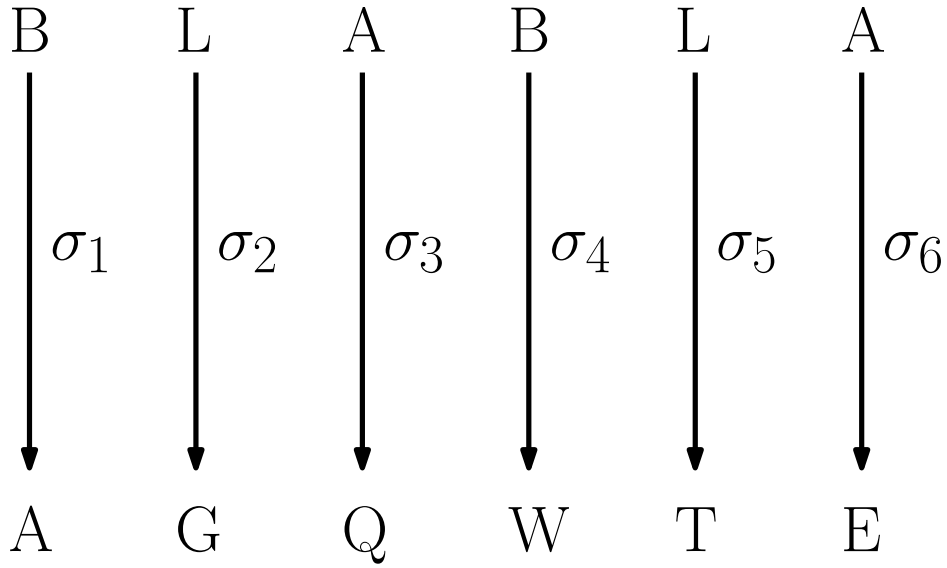
$$A \to W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.
2. This depends only on daily key rotor positions (not plugboard).

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

$$A \to W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.
2. This depends only on daily key rotor positions (not plugboard).
3. Use a lookup table to determine rotor positions!

Cryptanalysis of Enigma

Bletchley Park Bombe replica (Antoine Taveneaux)

Classical cryptography terminology

Substitution cipher. A cipher that acts on letters of the plaintext one-by-one according to a permutation of the alphabet.

Examples:

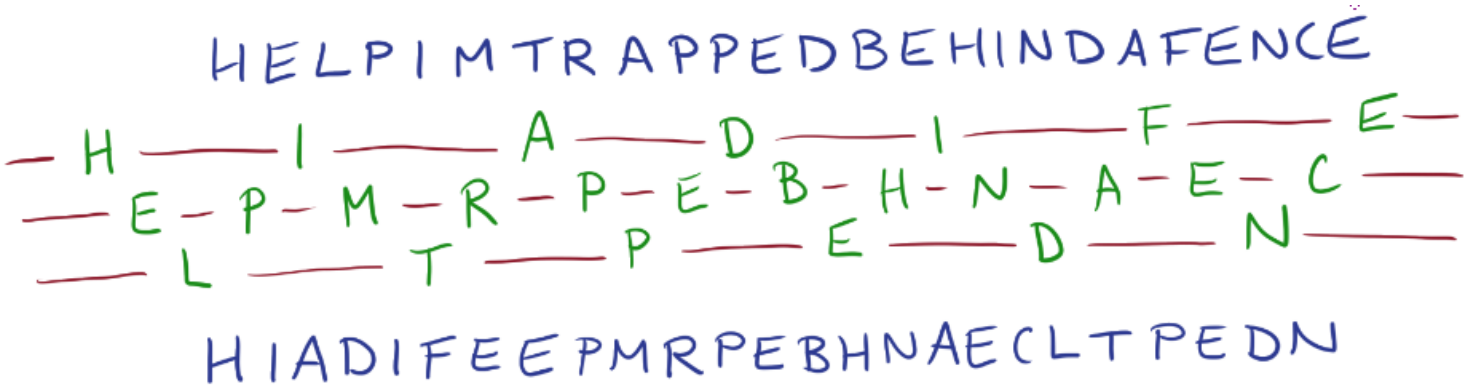
1. Caesar cipher
2. Affine cipher
3. Newspaper Cryptogram puzzles

Classical cryptography terminology

Transposition cipher. A cipher that acts on the plaintext by reordering its letters.

Examples:

1. Second half of ADFGXV cipher
2. RailFence Cipher



Classical cryptography terminology

Fractionating cipher. A cipher that replaces each plaintext character with several ciphertext characters.

Examples:

1. Polybius square (first half of ADFGXV cipher)

Classical cryptography terminology

Polyalphabetic cipher. A substitution cipher that uses a changing substitution key for each character.

Examples:

1. Vigenere cipher.
2. Enigma machine.

Classical cryptography terminology

Block cipher. A cipher that encrypts block-by-block instead of character-by-character.

Examples:

1. Hill cipher.

Classical cryptography terminology

Diffusion. A property of a cipher, namely that changing one character of plaintext results in many characters of ciphertext changing, and vice versa.

The idea: Prevents frequency analysis, because statistics of the plaintext "diffuse" to statistics of the ciphertext.

Examples:

1. Block ciphers satisfy diffusion (more if bigger blocks).
2. Vigenere cipher does not satisfy diffusion.

Classical cryptography terminology

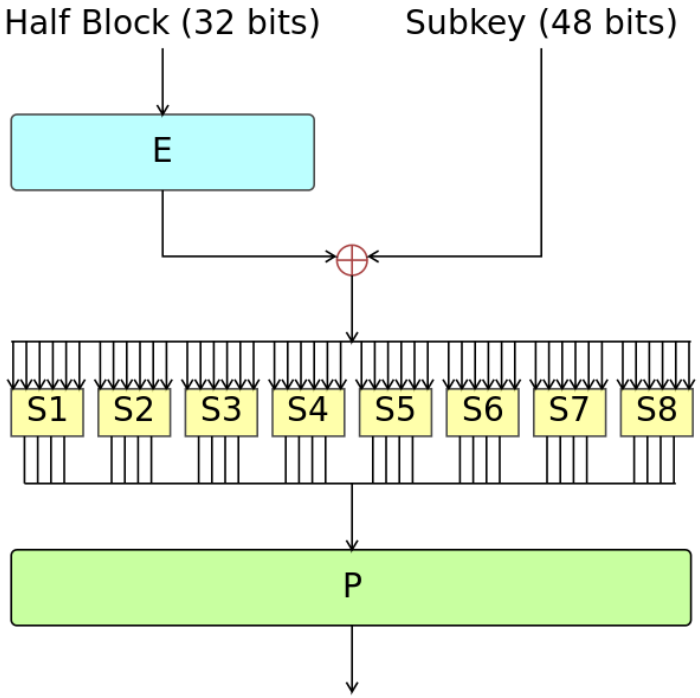
Confusion. A property of a cipher, namely that changing they key only slightly will result in the ciphertext changing a lot.

The idea: Prevents cryptanalysing the key one piece at a time, since each character of ciphertext depends on many parts of the key.

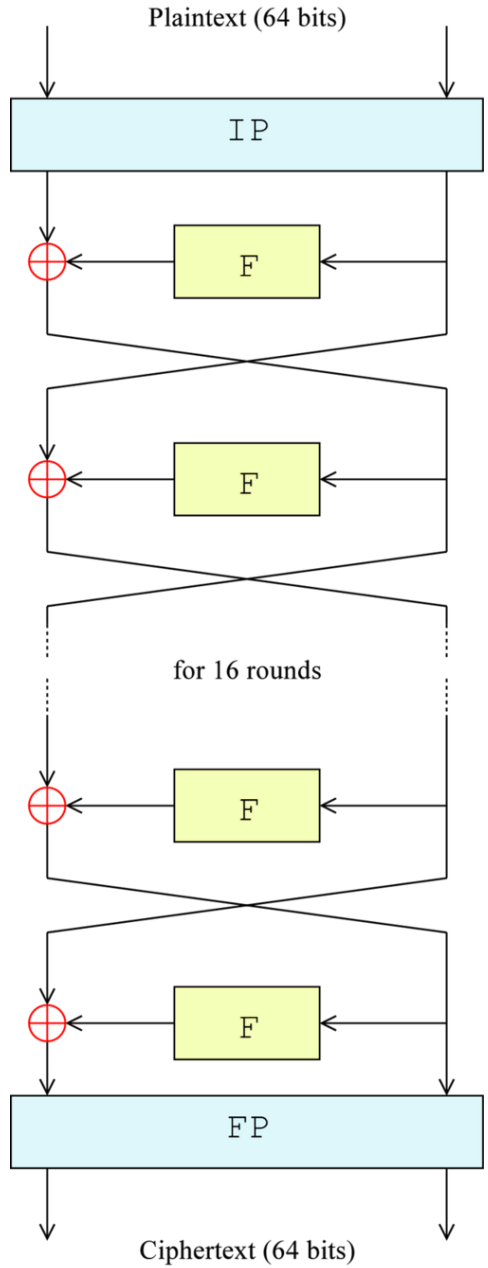
Examples:

1. Enigma has a fair bit of confusion. (A different rotor position on one rotor for example will change everything.)
2. Vigenere cipher does not satisfy confusion. (Each ciphertext character depends on only one character of the key.)

Advent of Computers: DES (Data Encryption Standard)



14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



Important points about DES (Data Encryption Standard)

Important points about DES (Data Encryption Standard)

1. Block cipher

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
   - send a DES key with public key cryptography then use DES

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
   - send a DES key with public key cryptography then use DES
7. Used 1975-2000
   - in 1999: broken in 22 hours, 15 minutes (distributed)
   - now you can buy a fancy computer and do it in 15 days

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
   - send a DES key with public key cryptography then use DES
7. Used 1975-2000
   - in 1999: broken in 22 hours, 15 minutes (distributed)
   - now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
   - Triple DES is an alternative where you do DES three times.

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
   - send a DES key with public key cryptography then use DES
7. Used 1975-2000
   - in 1999: broken in 22 hours, 15 minutes (distributed)
   - now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
   - Triple DES is an alternative where you do DES three times.
9. Carefully designed to maximize diffusion, avoid differential cryptanalysis (NSA controversy) etc.

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
   - Very classical cipher ideas
   - Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
   - send a DES key with public key cryptography then use DES
7. Used 1975-2000
   - in 1999: broken in 22 hours, 15 minutes (distributed)
   - now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
   - Triple DES is an alternative where you do DES three times.
9. Carefully designed to maximize diffusion, avoid differential cryptanalysis (NSA controversy) etc.
10. Mathematically speaking, the culmination of classical cryptography and the beginning of modern academic cryptography.