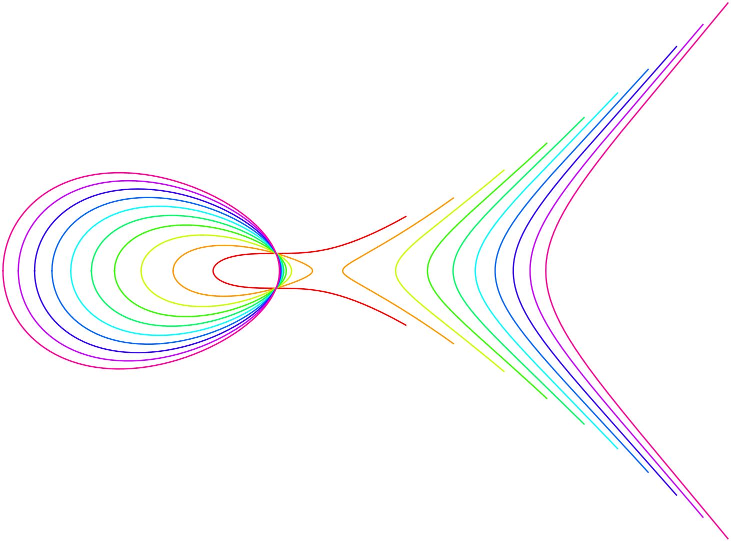
A Whirlwind Tour of Cryptography



Katherine E. Stange, Math 4440/5440 First Day (August 26, 2024)

Ancient Cryptography

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

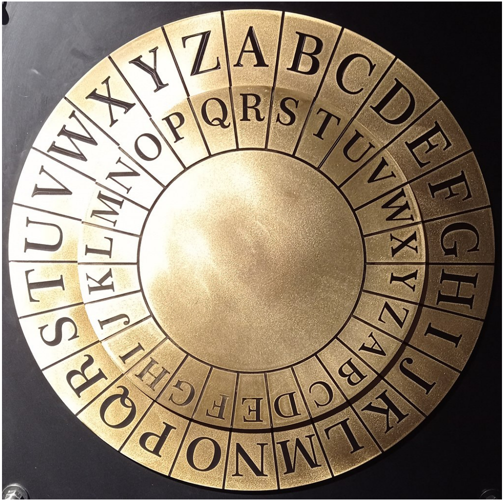
ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א

Atbash Cipher

Jeremiah 25:26 “The king of Sheshach shall drink after them”

(בבל *bbl* → ששך *ššk*)

Ancient Cryptography


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

Ceasar Wheel

image: Subjectiveart, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

Last 500 years

Vigenère Cipher

KEY	1	3	2	4	1	3	2	4	1	3	2	4
PLAINTEXT	A	T	T	A	C	K	A	T	D	A	W	N
CIPHERTEXT	B	W	V	E	D	N	C	X	E	D	Y	R

"impossible of translation" - Scientific American, 1917

Example of a **substitution cipher** (replacing characters)

First World War

	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

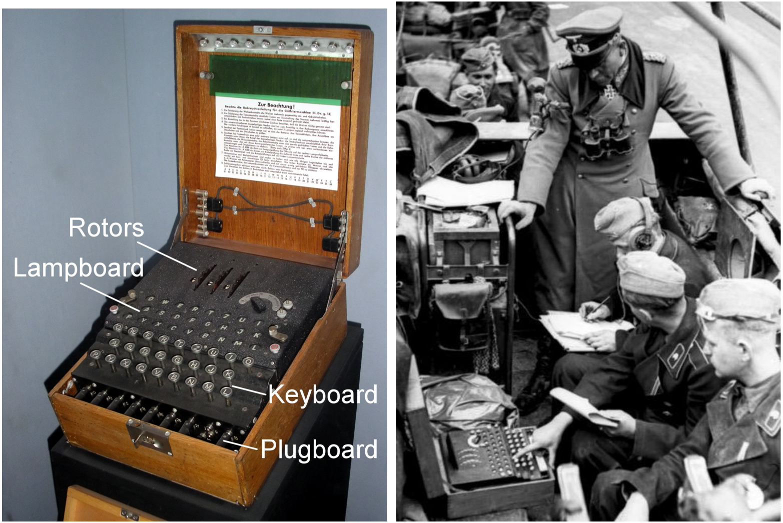
Plaintext: attack at dawn

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

Ciphertext: GGDGGAXDDXDFDXADFFGGAGXD

Includes an example of a **transposition cipher** (reordering characters)

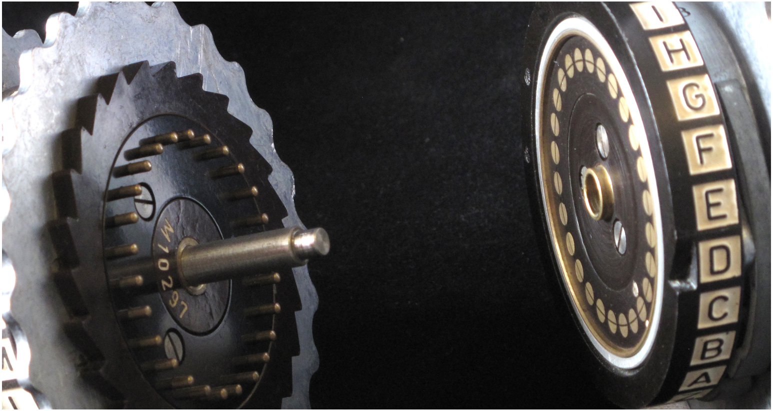
Second World War



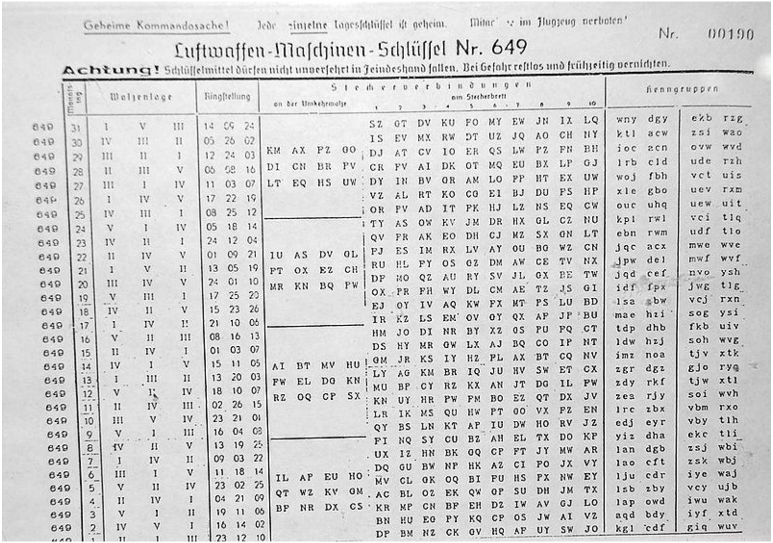
Wartime Enigma Machine

at left: public domain; at right: Bundesarchiv, Bild 101I-769-0229-10A / Borchert, Erich (Eric) / CC-BY-SA 3.0, CC BY-SA 3.0 DE https://creativecommons.org/licenses/by-sa/3.0/de/deed.en, via Wikimedia Commons

Second World War



Second World War



Geheime Kommandosache! Jeder 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.

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen											Kenngruppen			
								an der Umkehrwalze	am Steckerbrett 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	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	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	FV	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	HO	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	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26		EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]bw	vcj	rxn
649	17	I	IV	II	21	10	06		IR	KZ	LS	EM	OV	GY	QX	AF	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 DQ 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	FW	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	CF	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

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
3. A **decryption method**, that uses the **secret key** to transform the **ciphertext** into the **plaintext**.

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
3. A **decryption method**, that uses the **secret key** to transform the **ciphertext** into the **plaintext**.

Problems: key distribution

Symmetric Key Cryptography

system	key	encryption	decryption
Ceasar			
Vigenère			
ADFGVX			
Enigma			

Symmetric Key Cryptography

system	key	encryption	decryption
Ceasar	shift	shift forward	shift backward
Vigenère			
ADFGVX			
Enigma			

Symmetric Key Cryptography

system	key	encryption	decryption
Ceasar	shift	shift forward	shift backward
Vigenère	sequence of shifts	shift forward	shift backward
ADFGVX	square & column order	complicated!	complicated backwards!
Enigma	machine setup	press key, read light	press key, read light

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.

A **cryptanalyst** tries to break a cryptosystem.

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.
A **cryptanalyst** tries to break a cryptosystem.
The first, most naïve method is **exhaustive search**: trying all possible keys.

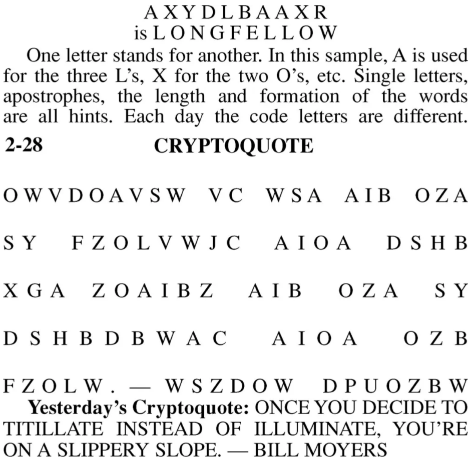
Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.
A **cryptanalyst** tries to break a cryptosystem.
The first, most naïve method is **exhaustive search**: trying all possible keys.

key	plaintext
0	WFYDAKZLWPL
1	XGZEBLAMXQM
2	YHAFCMBNYRN
3	ZIBGDNCOZSO
4	AJCHEODPATP
5	BKDIFPEQBUQ
6	CLEJGQFRCVR
7	DMFKHRGSDWS
8	ENGLISHTEXT
9	FOHMJTIUFYU
10	GPINKUJVGZV
11	HQJOLVKWHAW
12	IRKPMWLXIBX

key	plaintext
13	JSLQNXMYJCY
14	KTMROYNZKDZ
15	LUNSPZOALEA
16	MVOTQAPBMFB
17	NWPURBQCNGC
18	OXQVSCRDOHD
19	PYRWTDSEPIE
20	QZSXUETFQJF
21	RATYVFUGRKG
22	SBUZWGVHSLH
23	TCVAXHWITMI
24	UDWBYIXJUNJ
25	VEXCZJYKVOK

What's better than exhaustive search?



AXYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

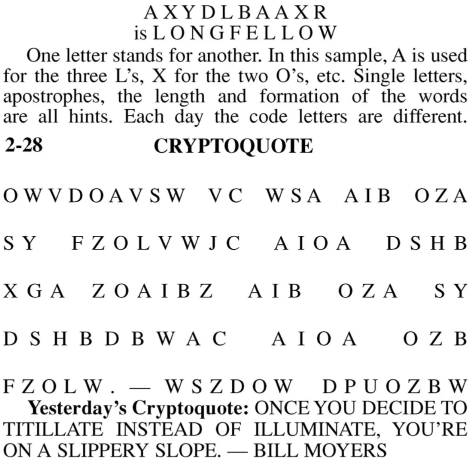
2-28 **CRYPTOQUOTE**

OWVDOAVSW VC WSA AIB OZA
SY FZOLVWJC AIOA DSHB
XGA ZOAIBZ AIB OZA SY
DSHBDBWAC AIOA OZB
FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

Source: *www.dailyrepublic.com*

What's better than exhaustive search?



AXYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 **CRYPTOQUOTE**

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBDBWAC AIOA OZB

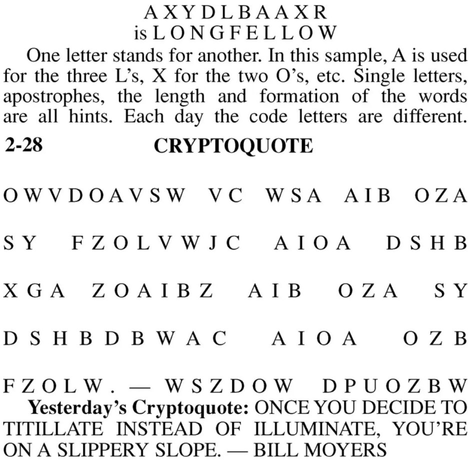
FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

Source: *www.dailyrepublic.com*

The number of possible keys: 26!

What's better than exhaustive search?



AXYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 **CRYPTOQUOTE**

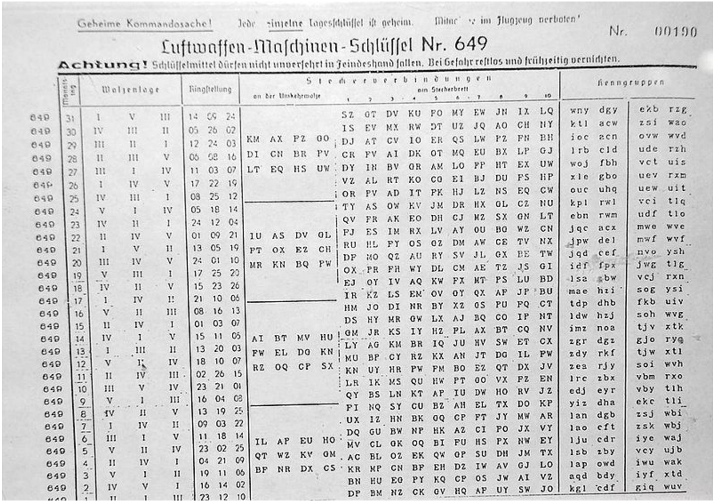
OWVDOAVSW VC WSA AIB OZA
SY FZOLVWJC AIOA DSHB
XGA ZOAIBZ AIB OZA SY
DSHBDBWAC AIOA OZB
FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

Source: *www.dailyrepublic.com*

The number of possible keys: 26!
$> 400,000,000,000,000,000,000,000,000 = 4 \times 10^{26}$.

The enigma keyspace



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

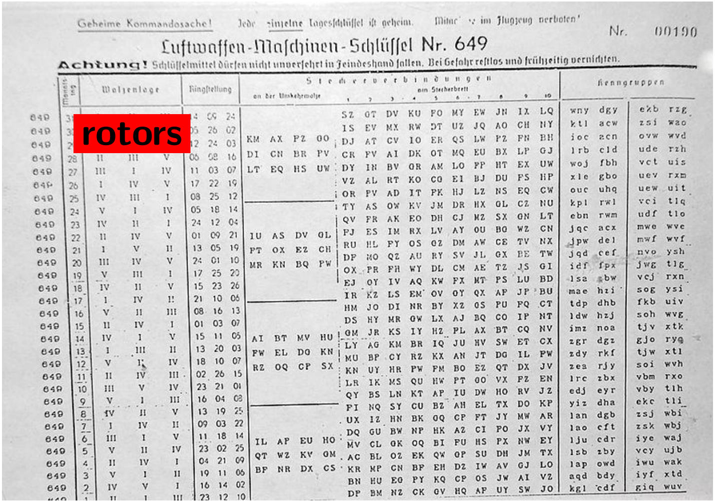
Nr. 00190

Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen											Kenngruppen			
								an der Umkehrwalze	am Steckerbrett													
									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	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	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	FV	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	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve
649	21	I	V	II	13	05	19	FT 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	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26		EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	zbw	vcj	rxn
649	17	I	IV	II	21	10	06		IR	KZ	LS	EM	OV	GY	QX	AF	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	FW	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		DQ	GU	BW	NP	HK	AZ	CI	FO	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	FY	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

The enigma keyspace



Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitna[illegible] im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maſchinen-Schlüſſel Nr. 649

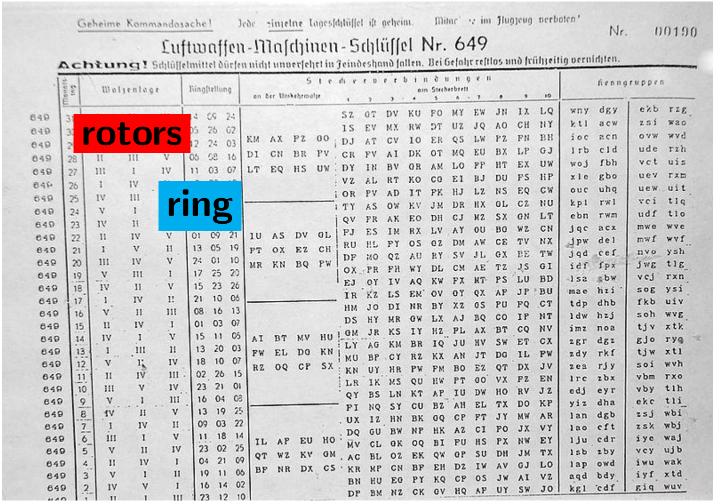
Achtung! Schlüſſelmittel dürfen nicht unverſehrt in Feindeshand fallen. Bei Gefahr reſtlos und frühzeitig vernichten.

	Monats-tag	Walzenlage			Ringſtellung			Steckerverbindungen											Kenngruppen			
								an der Umkehrwalze	am Steckerbrett													
									1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24		SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM AX PZ OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	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	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26		EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]bw	vcj	rxn
649	17	I	IV	II	21	10	06		IR	KZ	LS	EM	OV	GY	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	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	OP	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

rotors

$5 \cdot 4 \cdot 3$

The enigma keyspace



rotors
ring

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

Nr. 00190

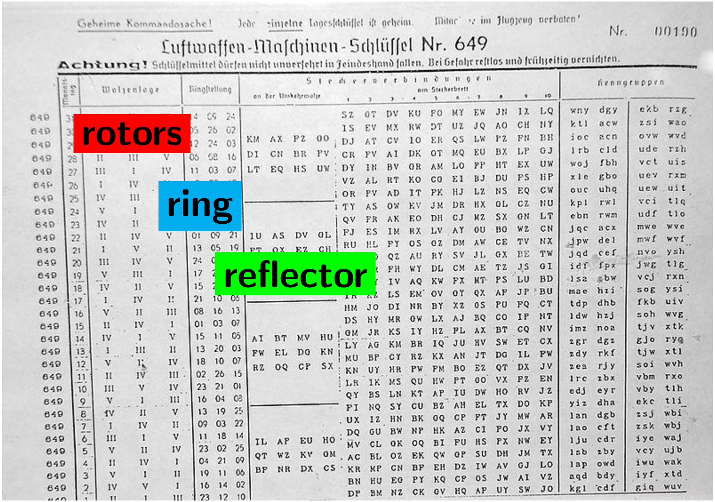
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen an der Umkehrwalze	am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31				4	09	24		SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30				5	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29				12	24	03	KM AX PZ OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	OR	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	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	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	GY	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 DO 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		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
649	1	II	I	III	23	12	10		DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv

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

The enigma keyspace



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.

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett 1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	[illegible]	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	[illegible]	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	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	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					IR	KE	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	DO	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	FW	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					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
649	1	II	I	III	23	12	10					DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv

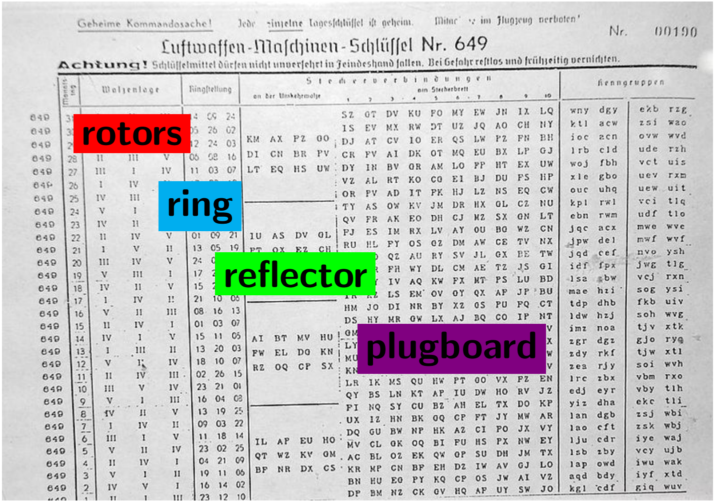
rotors

ring

reflector

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

The enigma keyspace



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.

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	PO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CO	EI	BJ	DU	PS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	BO	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]bw	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	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	PQ	CT	tdp	dhb	fkb	uiv
649	15	II	IV	I	01	03	07					DS	HY	MR	OW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg
649	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	OQ	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	OK	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	OP	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

rotors

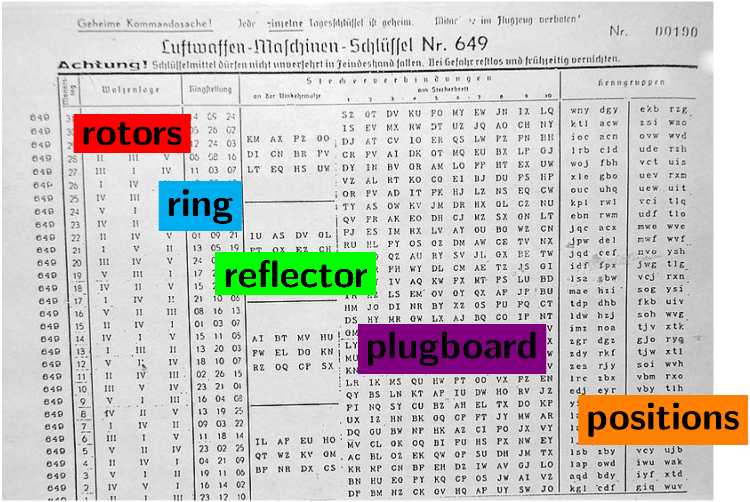
ring

reflector

plugboard

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

The enigma keyspace



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

Nr. 00190

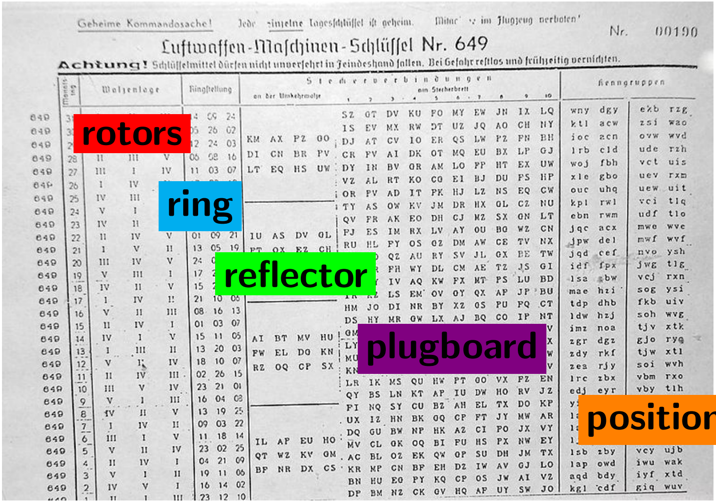
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

Monatstag | Walzenlage | Ringſtellung | Steckerverbindungen an der Umkehrwalze | am Steckerbrett 1 2 3 4 5 6 7 8 9 10 | Kenngruppen

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandosache! Jeder einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten! Nr. 00190

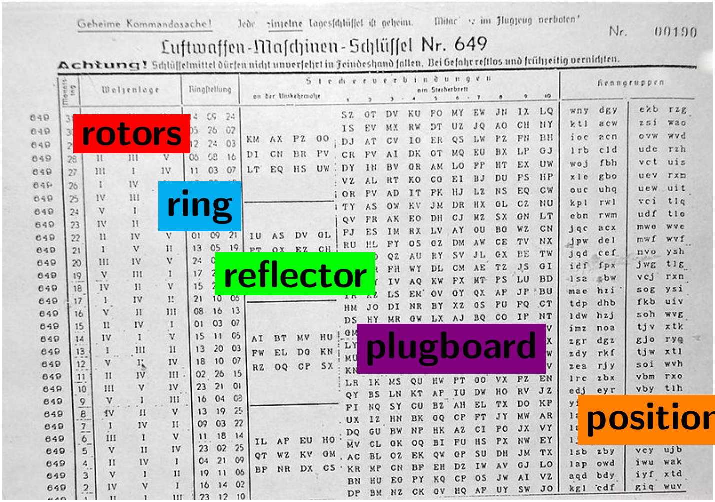
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen an der Umkehrwalze	am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24		SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM AX PZ GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]		VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]		OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]		TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]		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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]		[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]		[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06		[illegible]	[illegible]	LS	EM	OV	GY	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW EL DG KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ OQ CP SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15		KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22		UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14		DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL AP EU HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
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

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

The enigma keyspace



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.

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen											Kenngruppen			
								an der Umkehrwalze	am Steckerbrett													
									1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	14	09	24		SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM AX PZ OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI CN BR PV	CR	FV	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	[illegible]	[illegible]	[illegible]	[illegible]		VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]		OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]		TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]		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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]		[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]		[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06		[illegible]	[illegible]	LS	EN	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW EL DO KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ OQ CP SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15		KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22		UX	IZ	HN	BK	GQ	CF	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14	IL AP EU HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	QT WZ KV GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
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	AF	UY	SW	JO	kgl	cdf	giq	wuv

rotors

ring

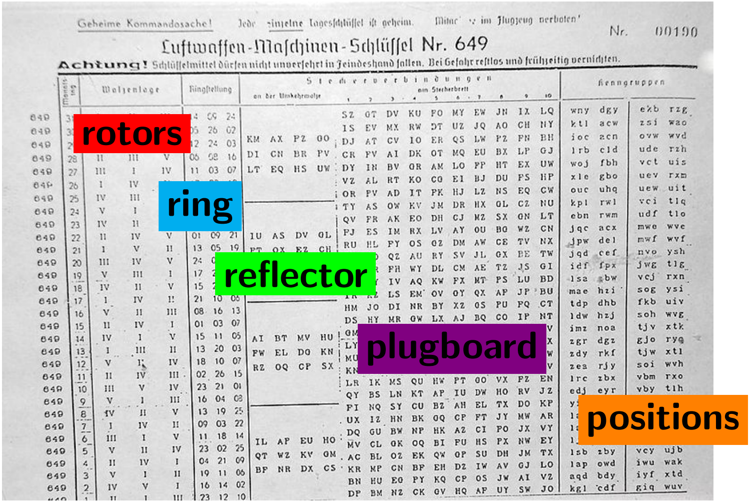
reflector

plugboard

positions

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten! Nr. 00190

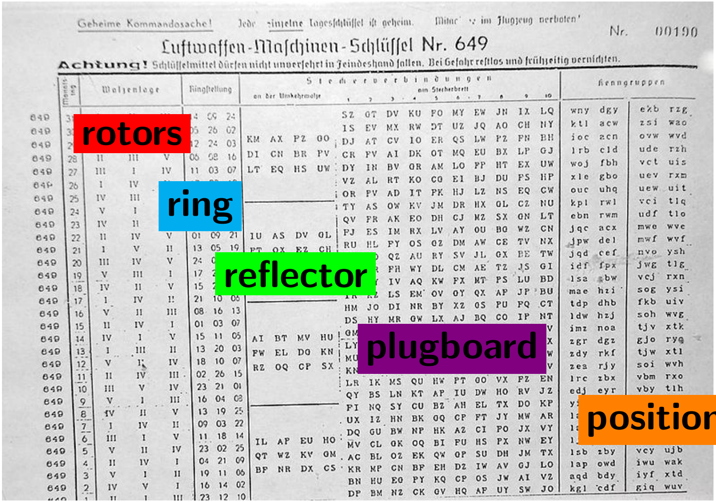
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monats-tag	Walzenlage			Ringſtellung			Steckerverbindungen an der Umkehrwalze				am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	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	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	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	fkb	uiv
649	15	II	IV	I	01	03	07					DS	HY	MR	OW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg
649	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	I	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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

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

The enigma keyspace



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.

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett 1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	joc	acn	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	OR	AM	LO	FP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DG	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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

rotors

ring

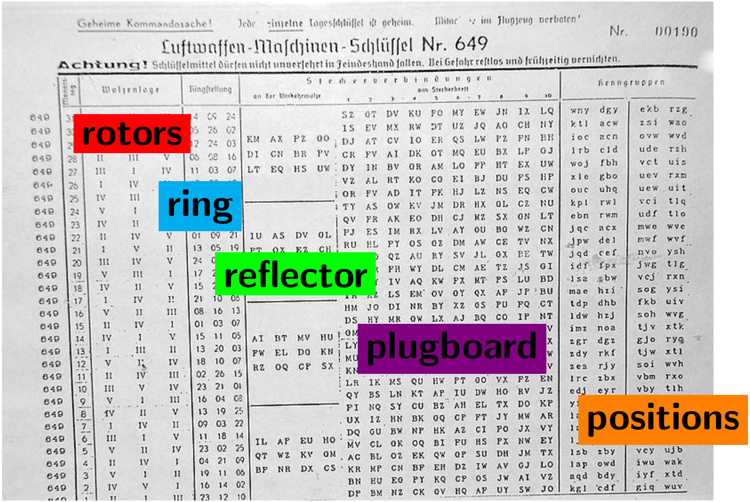
reflector

plugboard

positions

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

The enigma keyspace



rotors
ring
reflector
plugboard
positions

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

Nr. 00190

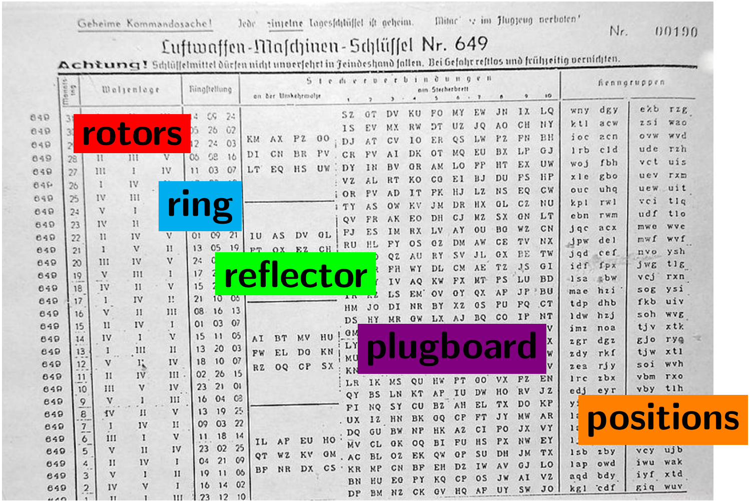
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31				14	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	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	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV									VZ	AL	RT	KO	CO	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	FJ	ES	IM	RX	LV	AY	OU	BO	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	0							QZ	AU	RY	SV	JL	GX	BE	TW		jqd	cef	nvo	ysh
649	19	V	III	I	17	2							FH	WY	DL	CM	AE	TZ	JS	GI		idf	fpx	jwg	tlg
649	18	IV	II	V	15	2							IV	AQ	KW	FX	MT	PS	LU	BD		lsa	bw	vcj	rxn
649	17	I	IV	II	21	10	06					IR	KZ	LS	EN	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									V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY									X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU									W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN									V	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	yi			
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	la			
649	6	III	I	V	11	18	14	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	ls			
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lj			
649	4	II	IV	I	04	21	09	BF	NR	DX	CS	AC	BL	OZ	EK	QW	OP	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

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

The enigma keyspace



rotors
ring
reflector
plugboard
positions

Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten! Nr. 00190

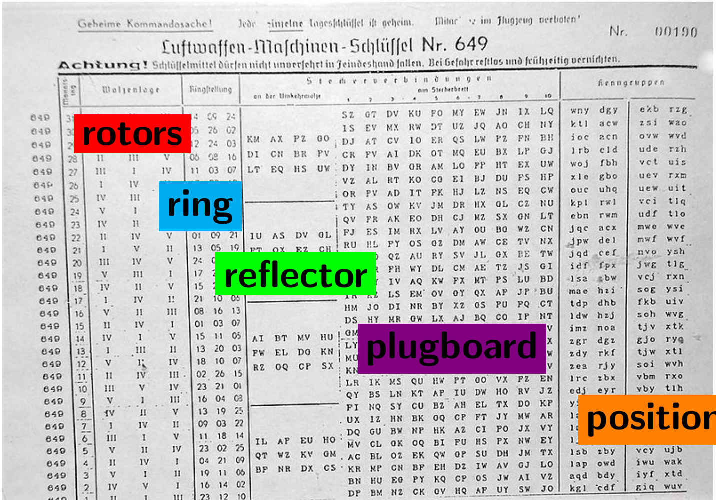
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	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	PF	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06					IR	[illegible]	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	PQ	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DQ	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	BF	NR	DX	CS	AC	BL	OZ	EK	QW	OP	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	AF	UY	SW	JO	kgl	cdf	giq	wuv

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten! Nr. 00190

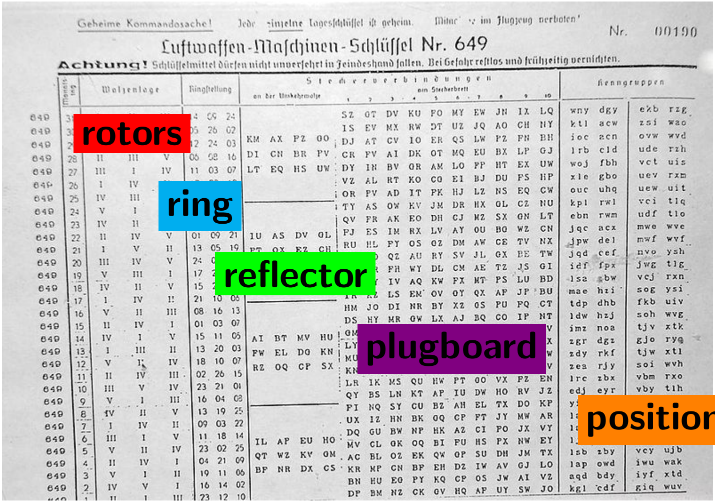
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	[illegible]	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CO	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	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	fkb	uiv
649	15	II	IV	I	01	03	07					DS	HY	MR	OW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg
649	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	OQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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
[illegible]	1	II	I	III	23	12	10					DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandosache!   Jede einzelne Tagesſchlüſſel iſt geheim.   Mitnahme im Flugzeug verboten!   Nr. 00190

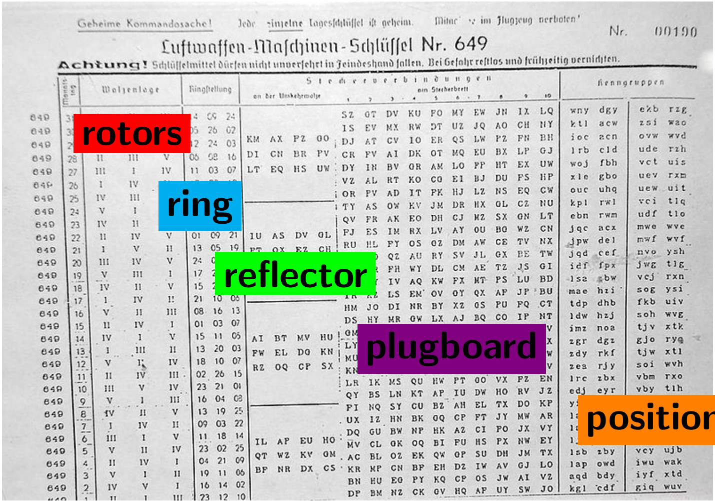
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	BO	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	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	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	X	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	W	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	V	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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

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

The enigma keyspace



Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten! Nr. 00190

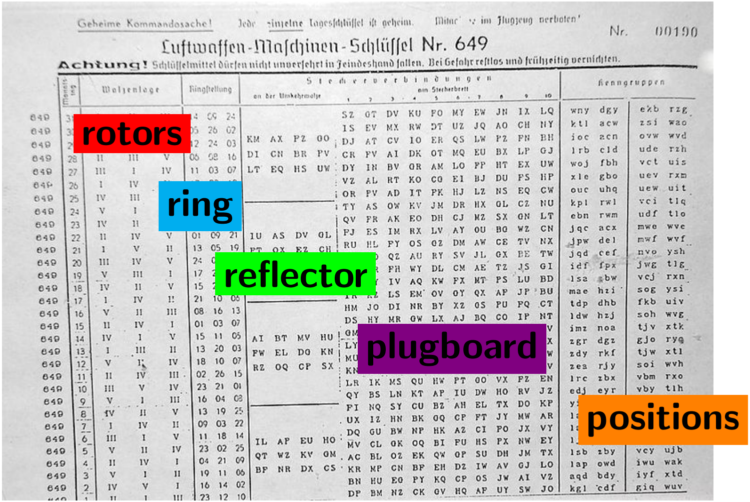
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	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	FV	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CO	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandosache! Jede einzelne Tagesſchlüſſel iſt geheim. Mitna[illegible] im Flugzeug verboten! Nr. 00190

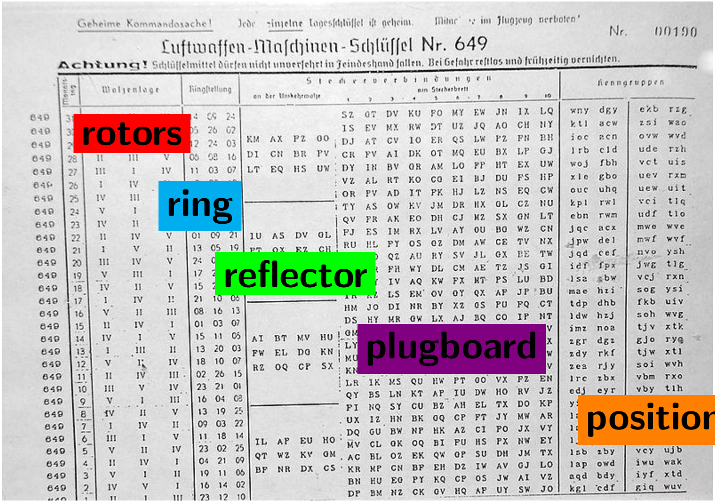
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett 1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	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	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	ET	OX	EZ	CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	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	PQ	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	BF	NR	DX	CS	AC	BL	OZ	EK	QW	OP	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

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

The enigma keyspace


rotors
ring
reflector
plugboard
positions

Geheime Kommandoſache!   Jede einzelne Tagesſchlüſſel iſt geheim.   Mitnahme im Flugzeug verboten!   Nr. 00190

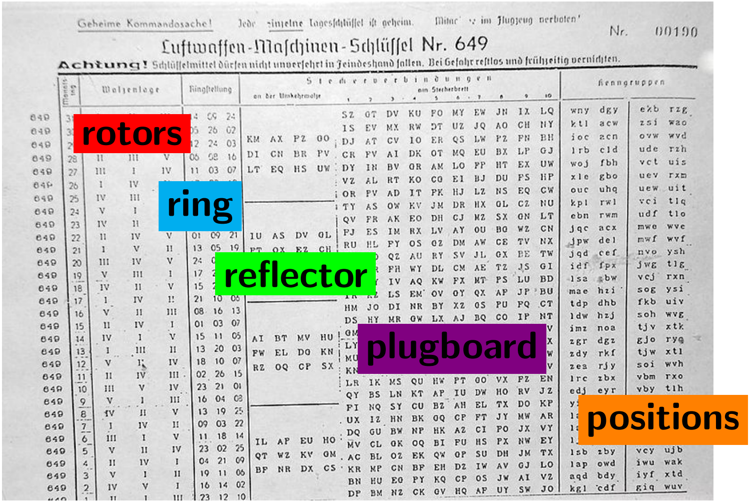
Luftwaffen-Maſchinen-Schlüſſel Nr. 649

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

	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen an der Umkehrwalze				am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	30	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	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	QR	AM	LO	FP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
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

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

The enigma keyspace



rotors
ring
reflector
plugboard
positions

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.

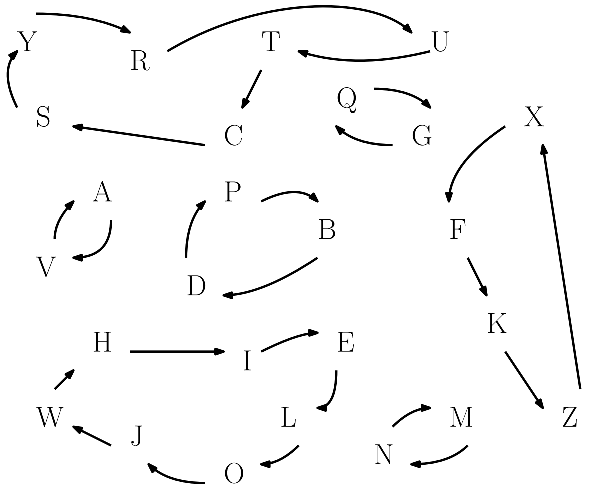
	Monatstag	Walzenlage			Ringſtellung			Steckerverbindungen														Kenngruppen			
								an der Umkehrwalze				am Steckerbrett													
												1	2	3	4	5	6	7	8	9	10				
649	31	[illegible]	[illegible]	[illegible]	[illegible]	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ezb	rzg
649	[illegible]	[illegible]	[illegible]	[illegible]	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	[illegible]	[illegible]	[illegible]	[illegible]	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	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	OR	AM	LO	FP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	[illegible]	[illegible]	[illegible]	[illegible]					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	[illegible]	[illegible]	[illegible]	[illegible]					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	[illegible]	[illegible]	[illegible]	[illegible]					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	[illegible]	[illegible]	[illegible]	[illegible]					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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	[illegible]	[illegible]					[illegible]	[illegible]	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	[illegible]	[illegible]					[illegible]	[illegible]	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
649	17	I	IV	II	21	10	06					[illegible]	[illegible]	LS	EN	OV	GY	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	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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	imz	noa	tjv	xtk
649	13	I	III	II	13	20	03	FW	EL	DO	KN	LY	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zgr	dgz	gjo	ryq
649	12	V	II	IV	18	10	07	RZ	OQ	CP	SX	MU	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	zdy	rkf	tjw	xtl
649	11	II	IV	III	02	26	15					KN	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	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	[illegible]	[illegible]	[illegible]	[illegible]
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	GQ	CP	FT	JY	MW	AR	[illegible]	[illegible]	[illegible]	[illegible]
649	6	III	I	V	11	18	14					DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	[illegible]	[illegible]	[illegible]	[illegible]
649	5	V	II	IV	23	02	25	IL	AP	EU	HO	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	[illegible]	[illegible]	[illegible]	[illegible]
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	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

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

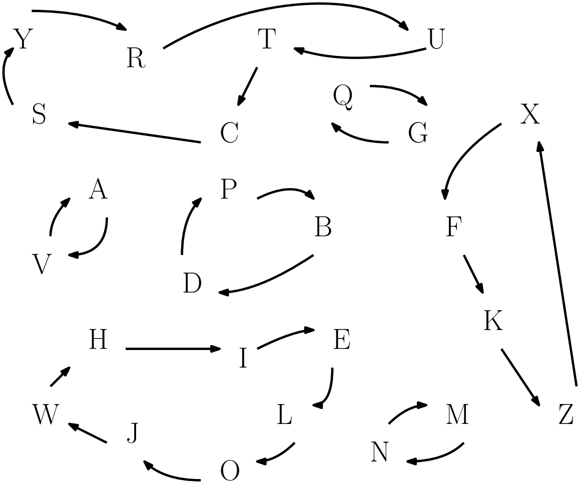
Cryptanalysis of enigma

A random permutation of the alphabet:



Cryptanalysis of enigma

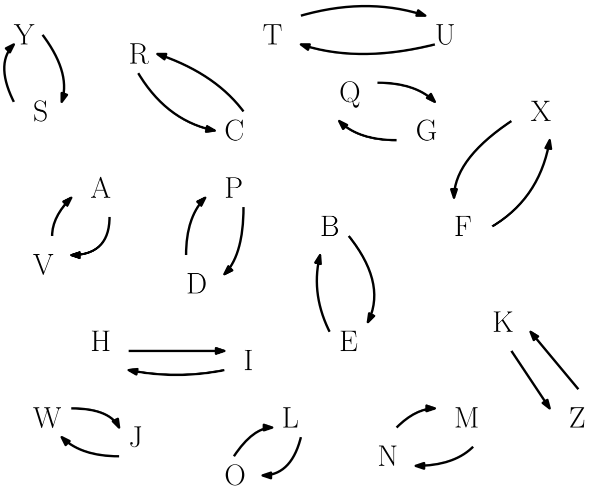
A random permutation of the alphabet:



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

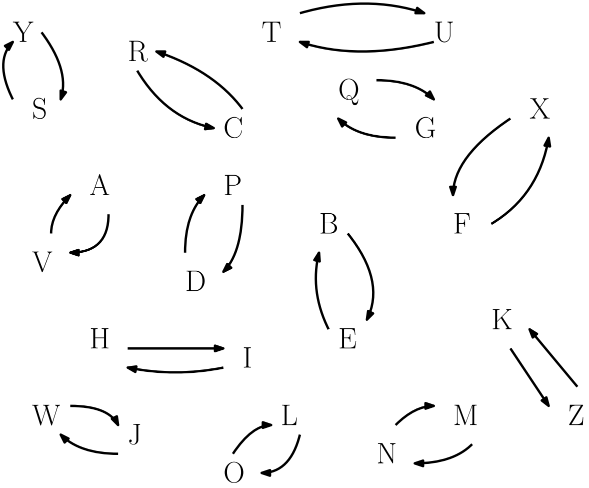
Cryptanalysis of enigma

An enigma permutation of the alphabet:



Cryptanalysis of enigma

An enigma permutation of the alphabet:



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

Cryptanalysis of enigma

Message key: BLA

Encrypted message key (using daily key):

$$\begin{tikzcd}
B \arrow[d, "\sigma_1"] & L \arrow[d, "\sigma_2"] & A \arrow[d, "\sigma_3"] & B \arrow[d, "\sigma_4"] & L \arrow[d, "\sigma_5"] & A \arrow[d, "\sigma_6"] \\
A & G & Q & W & T & E
\end{tikzcd}$$

Cryptanalysis of enigma

Message key: BLA

Encrypted message key (using daily key):

$$\begin{tikzcd}
B \arrow[d, "\sigma_1"] & L \arrow[d, "\sigma_2"] & A \arrow[d, "\sigma_3"] & B \arrow[d, "\sigma_4"] & L \arrow[d, "\sigma_5"] & A \arrow[d, "\sigma_6"] \\
A & G & Q & W & T & E
\end{tikzcd}$$

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

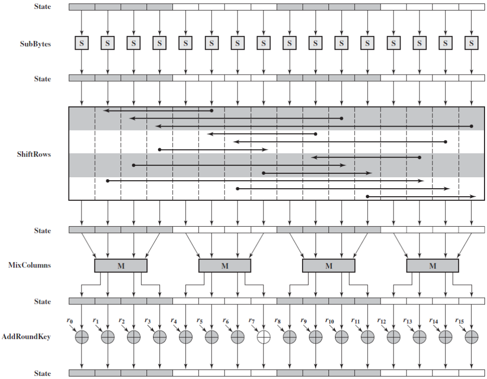
$$A \to W$$

Cryptanalysis of enigma

Bletchley Park Bombe replica

Antoine Taveneaux, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0, via Wikimedia Commons

Advent of Computers: AES (Advanced Encryption Standard)



Jeongysu, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0, via Wikimedia Commons

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

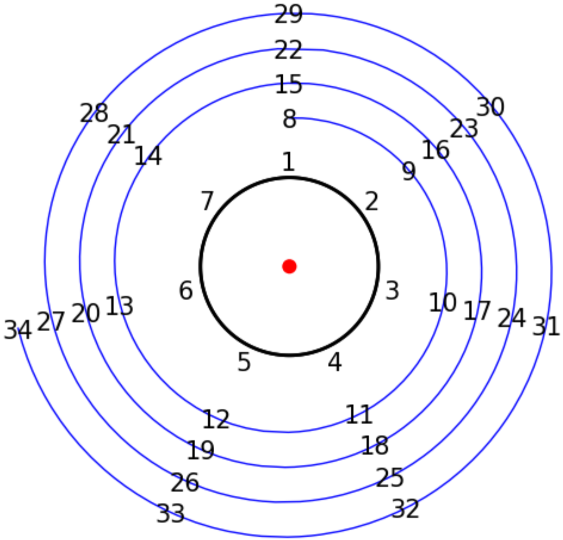
A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

How is this even possible?!

The door to modern cryptography: modular arithmetic



Diffie-Hellman Key Exchange

Setup: p (modulus), g

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice	Bob

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice	Bob
Secret: a	Secret: b

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice		Bob
Secret: a		Secret: b
g^a	$\longrightarrow$	g^a

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice		Bob
Secret: a		Secret: b
g^a	$\longrightarrow$	g^a
g^b	$\longleftarrow$	g^b

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice		Bob
Secret: a		Secret: b
g^a	$\longrightarrow$	g^a
g^b	$\longleftarrow$	g^b
Compute: $(g^b)^a \equiv g^{ab}$		Compute: $(g^a)^b \equiv g^{ab}$

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice		Bob
Secret: a		Secret: b
g^a	$\longrightarrow$	g^a
g^b	$\longleftarrow$	g^b
Compute: $(g^b)^a \equiv g^{ab}$		Compute: $(g^a)^b \equiv g^{ab}$

An eavesdropper Eve can see g^a and g^b and must compute g^{ab}.

Hard Cryptographic Problems

A **hard cryptographic problem** is:

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- **encryption** is easy (i.e. fast) using no secret info

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- **encryption** is easy (i.e. fast) using no secret info
- **decryption** is easy **for the intended recipient** (who has extra secret info)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- **encryption** is easy (i.e. fast) using no secret info
- **decryption** is easy **for the intended recipient** (who has extra secret info)
- **decryption** is infeasible (i.e. too slow) **for anyone else** (who does not have the extra info)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- a mathematical problem (e.g. factoring)
- which is **believed** to be **computationally intensive** to solve,
- and upon which we can build a **public-key cryptographic protocol** such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- **encryption** is easy (i.e. fast) using no secret info
- **decryption** is easy **for the intended recipient** (who has extra secret info)
- **decryption** is infeasible (i.e. too slow) **for anyone else** (who does not have the extra info)

For example, to decrypt a message meant for someone else, it may require factoring a number so big, that it is expected to take longer than the length of time before the sun dies.

Warning

We don't actually know they are hard!

Hard Cryptographic Problems

The **Computational Diffie-Hellman Problem**:
Given $g^a, g^b \pmod{p}$, compute g^{ab}.

- Typical algorithms take around $\sqrt{p}$ time.
- Human record: p of 795 bits using 3100 core-years
- Standard internet security: 1024 bits
- Logjam attack: 512 bits attacked in the wild
- (Why did Logjam work? Big swaths of the internet were using the **same prime**!)

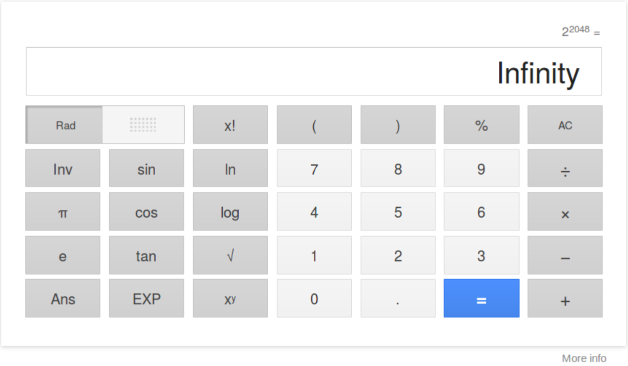
RSA: Rivest-Shamir-Adelman

The **Factoring Problem**:
Given an integer $n = pq$ for p and q prime, find p and q.

- Human record: $n \sim 2^{829}$.
- Standard internet security: $n \sim 2^{2048}$.

How big is 2^{2048}?

How big is 2^{2048}?



2^{2048} =

Infinity

How big is 2^{2048}?

Estimate each quantity as a power of two (and put them in order!)

- The number of atoms in the universe.
- The number of cells in a human body.
- The number of insects per human on earth.
- The number of seconds until the sun dies.

How big is 2^{2048}?

How big is 2^{2048}?

- The number of insects per human on earth: $2^{28} \sim 200$ million.

How big is 2^{2048}?

- The number of insects per human on earth: $2^{28} \sim 200$ million.
- The number of cells in a human body: $2^{45} \sim 37.2$ trillion.

How big is 2^{2048}?

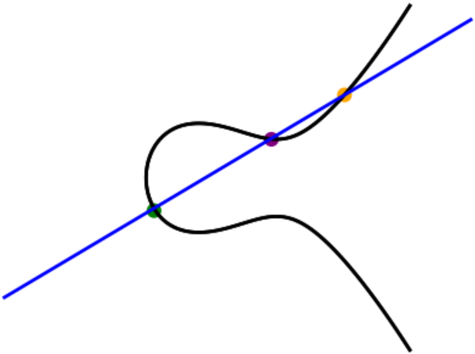
- The number of insects per human on earth: $2^{28} \sim 200$ million.
- The number of cells in a human body: $2^{45} \sim 37.2$ trillion.
- The number of seconds until the sun dies: $2^{57} \sim 7.5$ billion years.

How big is 2^{2048}?

- The number of insects per human on earth: $2^{28} \sim 200$ million.
- The number of cells in a human body: $2^{45} \sim 37.2$ trillion.
- The number of seconds until the sun dies: $2^{57} \sim 7.5$ billion years.
- The number of atoms in the universe: $2^{266} \sim 10^{80} \sim 100$ quadrillion vigintillion.

More modern cryptography: Elliptic Curve Cryptography

Do your computations with a crazy group called an



elliptic curve.

The Quantum Age

- When will we have quantum computers?

The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.

The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.
- What can they do?

The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.
- What can they do?
  - They can factor and solve discrete logarithm too quickly: break all of current cryptography.

The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.
- What can they do?
  - They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- What are we doing about it?

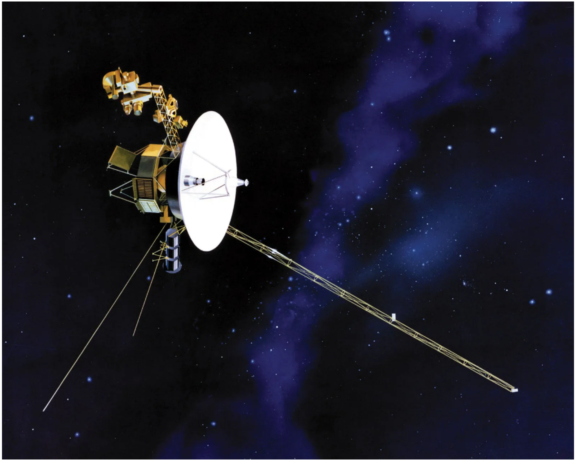
The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.
- What can they do?
  - They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- What are we doing about it?
  - NIST is standarizing new protols based on new hard problems that are believed to be quantum-safe.

The Quantum Age

- When will we have quantum computers?
  - The unit of measure is decades.
- What can they do?
  - They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- What are we doing about it?
  - NIST is standarizing new protols based on new hard problems that are believed to be quantum-safe.

We will study **quantum cryptography**, **quantum algorithms** and **post-quantum cryptography**.



Bonus: Whirlwind tour of coding theory

Image: the editors of encyclopedia britannica, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

Coding Theory

- What is coding theory for? (What problem are we solving?)

Coding Theory

- What is coding theory for? (What problem are we solving?)
    - Real-life **channels** (radio, cell phone, copper wires) are **noisy**.

Coding Theory

- What is coding theory for? (What problem are we solving?)
  - Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
  - We want to send messages in such a way that errors won't prevent understanding.

Coding Theory

- What is coding theory for? (What problem are we solving?)
  - Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
  - We want to send messages in such a way that errors won't prevent understanding.
  - Usually we model a channel as something that randomly flips bits of our binary message (**errors**).

Coding Theory

- What is coding theory for? (What problem are we solving?)
  - Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
  - We want to send messages in such a way that errors won't prevent understanding.
  - Usually we model a channel as something that randomly flips bits of our binary message (**errors**).
  - Nothing to do with secrecy.

Coding Theory

- What is coding theory?

Coding Theory

- What is coding theory?
    - We change our message (**encoding**) so that it is error resistant.

Coding Theory

- What is coding theory?
  - We change our message (**encoding**) so that it is error resistant.
  - We send **codewords** instead of plaintext symbols.

Coding Theory

- What is coding theory?
  - We change our message (**encoding**) so that it is error resistant.
  - We send **codewords** instead of plaintext symbols.
  - Example: ‘Victor’ instead of ‘V’ (radio) or ‘000’ instead of ‘0’ (a repeat code)

Coding Theory

- What is coding theory?
  - We change our message (**encoding**) so that it is error resistant.
  - We send **codewords** instead of plaintext symbols.
  - Example: ‘Victor’ instead of ‘V’ (radio) or ‘000’ instead of ‘0’ (a repeat code)
  - The receiver must **decode**

Coding Theory

- What makes a good code?

Coding Theory

- What makes a good code?
  - Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. ‘010’ is probably ‘0’ not ‘1’)

Coding Theory

- What makes a good code?
  - Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. ‘010’ is probably ‘0’ not ‘1’)
  - Strong **efficiency**: not too much space inflation (codewords are longer than the symbols they represent)
- What math goes into it?

Coding Theory

- What makes a good code?
  - Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. ‘010’ is probably ‘0’ not ‘1’)
  - Strong **efficiency**: not too much space inflation (codewords are longer than the symbols they represent)
- What math goes into it?
  - Finite fields, linear algebra

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
  - Paradigms, history and application
  - Modular arithmetic & discrete logarithm
  - Euclidean algorithm, primality testing & factoring
  - Finite fields & elliptic curve cryptography
  - Coding theory & lattice-based cryptography
  - Quantum aspects

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
  - Paradigms, history and application
  - Modular arithmetic & discrete logarithm
  - Euclidean algorithm, primality testing & factoring
  - Finite fields & elliptic curve cryptography
  - Coding theory & lattice-based cryptography
  - Quantum aspects
- Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
  - Paradigms, history and application
  - Modular arithmetic & discrete logarithm
  - Euclidean algorithm, primality testing & factoring
  - Finite fields & elliptic curve cryptography
  - Coding theory & lattice-based cryptography
  - Quantum aspects
- Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
  - Paradigms, history and application
  - Modular arithmetic & discrete logarithm
  - Euclidean algorithm, primality testing & factoring
  - Finite fields & elliptic curve cryptography
  - Coding theory & lattice-based cryptography
  - Quantum aspects
- Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord
- contingency plan: last-minute modality change

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
  - Paradigms, history and application
  - Modular arithmetic & discrete logarithm
  - Euclidean algorithm, primality testing & factoring
  - Finite fields & elliptic curve cryptography
  - Coding theory & lattice-based cryptography
  - Quantum aspects
- Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord
- contingency plan: last-minute modality change
- recording class