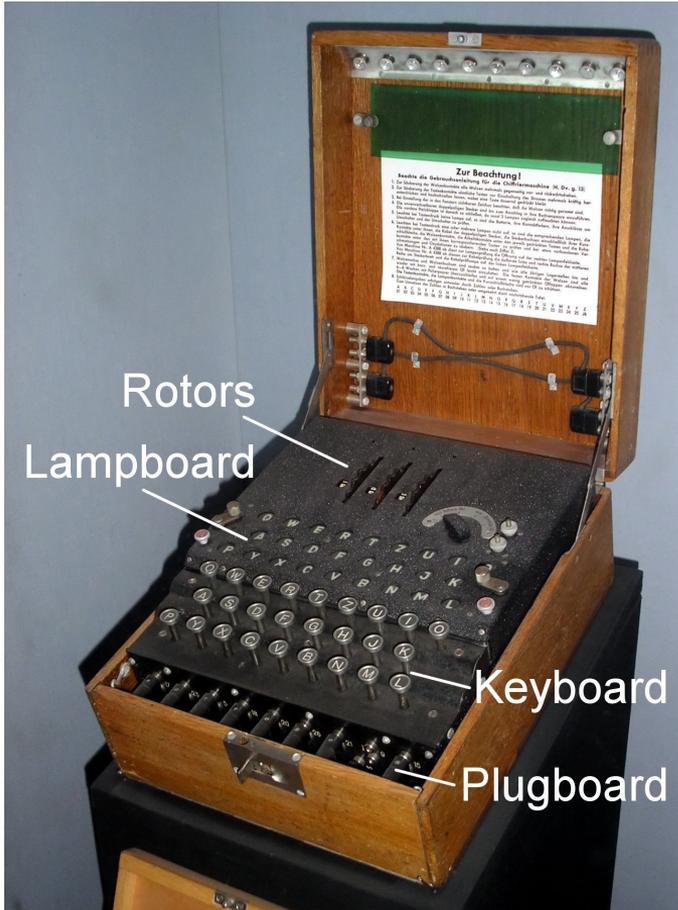


Enigma messages

Laura Sach

What is Enigma?



Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

Nr. 00014

Datum	Wahrselage	Ringstellung	Steckerverbindungen													Kenngruppen			
0 31	V II IV	17 09 02	KT	AJ	IV	UR	NY	HE	SD	XP	FE	CQ	afy	asy	zqk	bql			
0 30	I III V	22 12 10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	awz	omo	myj			
0 29	V IV II	04 01 25	WJ	VD	PO	MQ	FX	SR	NE	LG	UC	BK	ruj	kao	fqi	rwu			
0 28	II III IV	05 08 12	HR	TJ	LD	IO	ON	GX	QK	PE	WS	AP	ioy	kjv	yko	fxo			
0 27	I II III	10 20 15	AQ	ZK	MU	OH	ST	LN	XY	IJ	BP	VY	ggf	jus	lrs	glo			
0 26	II V I	18 09 06	DS	UL	SJ	OI	HN	FT	AK	YC	XQ	GB	orl	rht	kas	ego			
0 25	V IV III	26 07 18	WA	QD	XS	UY	LG	JJ	FB	HK	MT	CE	pfr	ljw	zgg	vgj			
0 24	III I IV	04 19 24	OH	XM	DJ	IL	VU	KG	QE	BT	FR	AS	nbt	pyd	eqo	wyu			
0 23	I IV V	11 17 01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	lmf			
0 22	IV I III	21 11 17	CV	LE	KN	UH	YJ	TI	KB	FE	PA	MO	jlw	vrh	vya	pbf			
0 21	I V II	06 21 10	JN	UX	TT	BG	DR	QC	KE	SP	HE	LA	sit	jlo	jcl	pvi			
0 20	V II III	07 18 04	SG	NW	SM	VY	XT	UR	OO	LB	AQ	HF	otx	gns	xeg	nvo			
0 19	IV V I	08 09 22	IT	YK	BL	RZ	VP	PN	JW	QO	MS	AE	lyx	jua	sju	nss			
0 18	I IV III	26 10 11	BU	TS	VE	JL	WX	AY	EG	ZM	ED	NF	ise	ysj	skw	znr			
0 17	III V I	11 22 16	GY	JN	SP	KI	LB	QD	UX	OW	HR	MA	xvd	kkb	pci	fug			
0 16	V I IV	04 09 24	QL	EY	BG	MN	EO	AW	TC	VK	FS	HF	afy	uah	tpn	npf			
0 15	II V III	08 20 14	JD	BM	XR	LG	FC	OP	SJ	YH	VK	EW	nfk	pvm	vus	opr			
0 14	IV I II	25 12 16	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MO	zgo	omz	pdf	xuq			
0 13	I V IV	07 18 05	IW	NB	XO	YS	AJ	MQ	VH	PT	UL	RH	zor	ocm	odl	ijs			
0 12	IV III II	19 05 21	ON	LG	IS	DO	SE	VE	TQ	KM	JP	AX	eqk	whq	avo	zpf			
0 11	V II I	09 20 14	BV	PF	GM	AJ	OU	VB	WS	NT	OK	EZ	hvm	lod	nco	yxx			
0 10	IV V III	21 08 03	IJ	XR	ZV	NT	GK	OU	EB	FL	MY	HD	bqd	ska	ggg	zss			
0 9	III I II	14 16 06	LN	IK	RS	DB	TX	GO	WY	EV	OP	RA	myh	noz	xrx	ess			
0 8	IV III I	09 18 14	SG	XU	WE	AF	LP	IY	SQ	DO	VJ	HT	qoc	keo	oon	kde			
0 7	II I V	18 15 24	EK	RO	JX	WV	HS	QP	BE	MU	TN	CA	fmo	mkh	lbe	tmq			
0 6	III II IV	25 01 17	DC	VG	OL	UA	EK	ZH	TX	FW	IM	RP	tlo	wbj	sre	kjd			
0 5	V III I	19 25 15	QF	DG	ZJ	NE	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd			
0 4	IV II V	26 04 08	MX	QO	HJ	TB	GA	KP	LZ	CS	WJ	NV	clc	idh	yoc	hwt			
0 3	V III II	01 09 23	EI	DY	FO	SJ	PN	LB	RR	GX	AH	CU	jty	bsy	kdh	asq			
0 2	I V III	10 07 02	SO	LA	VM	CT	PX	YB	HU	SD	RN	EL	uqn	nasx	jqk	psb			
0 1	IV I V	20 05 10	SX	KU	QP	VN	JO	TC	LA	WM	OB	ZP	aro	eej	fnz	szk			

Crown Copyright 2017

Image taken from
<https://projects.raspberrypi.org/en/projects/oc-tapi-brute-force-enigma>

How does Enigma work?



Settings sheet

Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

Nr. 00014

Datum	Wahnenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	V II IV	17 09 02	KT AJ IV UR NY HI GD XF PB CQ	sfy azy zkq bqi
30.	I III V	22 12 10	UE PL AY TB SH WM OJ DC KN SI	iuy swz omo myj
29.	V IV II	04 01 26	WJ VD PO MQ PX ZR NE LG UC BK	rui kao fqi rwu
28.	II III IV	06 03 12	HR TJ LD IO ON GX QK PZ WS AP	ioy kjv ykc fpx
27.	I II III	10 20 15	AQ ZK MU GH ST LN XY IJ BP RV	ggf jus lrs glc
26.	II V I	16 09 06	DS UL ZJ OI HN PT RK YC XQ GB	orl rht ksz ego
25.	V IV III	26 07 18	WA QD XS UY LG JI PB HR MT CE	pfr ijw zgg ysj
24.	III I IV	04 19 24	OH XM DJ IL VU KG QZ BT PR AS	nbt pvd eqo wyu
23.	I IV V	11 17 01	QJ GY SH OX ZB PL PA WI VK ND	hhv hhq kul hmf
22.	IV I III	21 11 17	CV LE KN UH YJ TI RB PZ PA MO	jlw vrh vya pbf
21.	I V II	06 21 10	JN UI YF BG DR QC KE SF HE LA	sit jlc jbl pvi
20.	V II III	07 18 04	ZG NW SM VY XT UR OC LB AQ HF	otx gns xeg nvo
19.	IV V I	08 09 22	IT YK BL RZ VP PN JW QO MS AE	lyx jua sju nss
18.	I IV III	20 16 11	BU TS VH JL WX AY KG ZM PD NF	ise ysj skw enr
17.	III V I	11 22 16	GY JN SP KI LB QD UX OW HR MA	xvd kkb pci jug
16.	V I IV	04 09 24	QL BY BG MN ZO AW TC VX PS HP	afp uah tpn npf
15.	II V III	08 20 14	JD BM XR LG PC OF ZI YH VK BW	nf qvm vue opr
14.	IV I II	25 12 15	BT OW SN DA ZL PF QX UE HR MC	zgo qmr pdf xuq
13.	I V IV	07 18 05	IW NB XO YS AJ ZR VH PT UL RB	zor ccm odl ijs
12.	IV III II	19 05 21	ON LG IS DO SE YR TQ KM JP AX	eqk whq lro zpf
11.	V II I	08 20 14	HV PF CM AJ OU YL WS NT OK EZ	hvm iod nku ykk
10.	IV V III	21 08 03	TJ XR ZV NT OK QK UR HR WL MY UN	had vba zgg

IV I V		20 5 10		SX KU QP VN JG TC LA WM OB ZF		FNZ
rotors		ring settings		plug board settings		rotor start

Crown Copyright 2017

Decrypt a message

GON XXLXYFQNZIK

LJE OIVGWVHVKAU

Encrypt a message

If you encrypt...

BFR RASPBERRYPI

...you should get

GON XXLXYFQNZIK

Decrypt this message

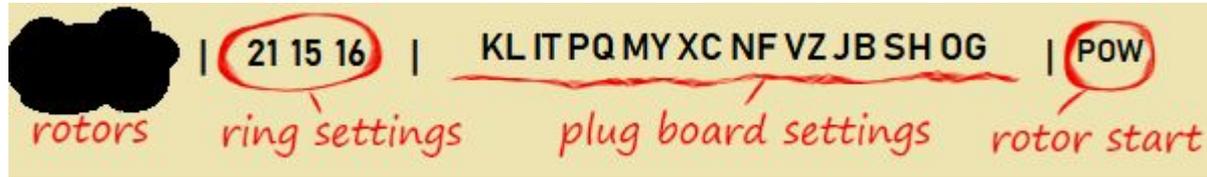
GED

HYZFQOOVVBBKBWPDZLSL

Uh oh...

You need to know the settings!

Brute force attack



?? rotors chosen

?? message key

Is it I I I? Is it I I II? Is it I I III?

Is it I I IV? Is it I I V? Is it I II I?

Is it I II II? etc...

Crib text

HGZC YPK,

Probably the word
“DEAR”

K VRBAUX WGDV RCDZ.

TNFCJ RERUUCJJE,

Probably the word
“YOURS”

WBPLJ

Crib text

Crib text: WEATHER

Cipher text: VZTLMPU

VZTLMPUSLKTEXYWZWKXDOTT

Geheim!

Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

Nr. 00014

	Datum	Walzenlage	Ringstellung	Steckerverbindungen																Kenngruppen			
0	31.	V II IV	17 09 02	KT	AJ	IV	UR	NY	HS	GD	XP	PB	CQ	sfy	azy	zkq	bqi						
0	30.	I III V	22 12 10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj						
0	29.	V IV II	04 01 26	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu						
0	28.	II III IV	06 03 12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AP	ioy	kjv	ykc	fpz						
0	27.	I II III	10 20 16	AQ	ZK	MU	GH	ST	LN	XY	IJ	BP	RV	gaf	jus	lrs	glc						
0	26.	II V I	16 09 06	DS	UL	ZJ	OI	HN	PT	RK	YC	XQ	GB	orl	rht	ksz	ego						
0	25.	V IV III	26 07 18	WA	QD	XS	UY	LG	JI	PB	HK	MT	CE	pfr	ijw	zgg	ysj						
0	24.	III I IV	04 19 24	OH	XM	DJ	IL	VU	KG	QZ	BT	FR	AS	nbt	pvd	eqo	wyu						
0	23.	I IV V	11 17 01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf						
0	22.	IV I III	21 11 17	CV	LE	KN	UH	YJ	TI	KB	PZ	PA	MO	jlw	vrh	vys	pbf						
0	21.	I V II	06 21 10	JN	UX	YT	BG	DR	QC	KE	SP	HS	LA	zit	jlo	jbl	pvi						
0	20.	V II III	07 18 04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	otx	gns	xeg	nvo						
0	19.	IV V I	08 09 22	IT	YK	BL	RZ	VP	PN	JW	QO	MS	AE	lyx	jua	sju	nss						
0	18.	I IV III	26 16 11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ise	ysj	skw	znr						
0	17.	III V I	11 22 16	GY	JN	SP	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	jag						
0	16.	V I IV	04 09 24	QL	EY	BG	MN	ZO	AW	TC	VX	PS	HP	afp	uab	tpn	npf						
0	15.	II V III	08 20 14	JD	BM	XR	LG	FC	OF	ZI	YH	VK	EW	nfk	pvm	vue	opr						
0	14.	IV I II	26 12 16	BT	OW	SN	DA	ZL	VF	QX	UE	HR	MC	zgo	cmz	pdf	xuq						
0	13.	I V IV	07 18 06	IW	NB	XG	YS	AJ	MQ	VH	PT	UL	RE	zor	ccm	odl	ijs						
0	12.	IV III II	19 03 21	CN	LG	IE	DO	SE	VR	TQ	KM	JP	AX	eqk	whq	avo	zpf						
0	11.	V II I	08 20 14	HV	PP	CM	AJ	OU	YB	WS	NT	OK	EZ	hvm	iod	nxc	yxx						
0	10.	IV V III	21 08 03	IJ	XR	ZV	NT	OK	OU	SB	FL	MY	HD	bgd	xka	gsg	sga						
0	9.	III I II	14 16 06	LN	IK	HS	DB	TX	CG	WY	EV	OP	RA	myh	noz	vxv	ees						
0	8.	IV III I	09 18 14	RG	XU	WE	AF	LP	IY	SQ	DO	VJ	HT	ooq	xec	ocn	kde						
0	7.	II I V	18 13 24	EK	RO	JX	WY	HS	QP	BZ	MU	TN	CA	fmo	mkb	lhe	tmq						
0	6.	III II IV	23 01 17	DC	VG	OL	UA	SK	ZH	YX	PW	IM	KP	tlo	wbj	sre	kjd						
0	5.	V III I	19 23 16	QP	DG	ZJ	NK	SB	IC	PT	ER	UV	HA	hnp	wla	shv	spd						
0	4.	IV II V	26 04 08	MX	QO	H1	TB	GA	KP	LZ	CS	WJ	NY	clo	jdh	yoq	hwt						
0	3.	V III II	01 02 28	EI	DY	FO	SJ	PN	LB	RK	GX	AH	CU	jty	bsy	kdh	asq						
0	2.	I V III	16 07 02	ZO	IA	VM	CT	FX	YB	HU	SD	RN	EL	uqn	nax	jqk	pzb						
0	1.	IV I V	20 06 10	SX	KU	QP	VN	JG	TC	LA	WM	OB	ZF	sre	eej	fnz	szk						

License

This workshop is based on a resource at

<https://projects.raspberrypi.org/en/projects/octapi-brute-force-enigma>

OctaPi: brute-force Enigma by [GCHQ](#) and the Raspberry Pi Foundation is licensed under a Creative Commons Attribution 4.0 International Licence.

Code, scripts and images [Crown Copyright](#)

License: [Apache 2](#)