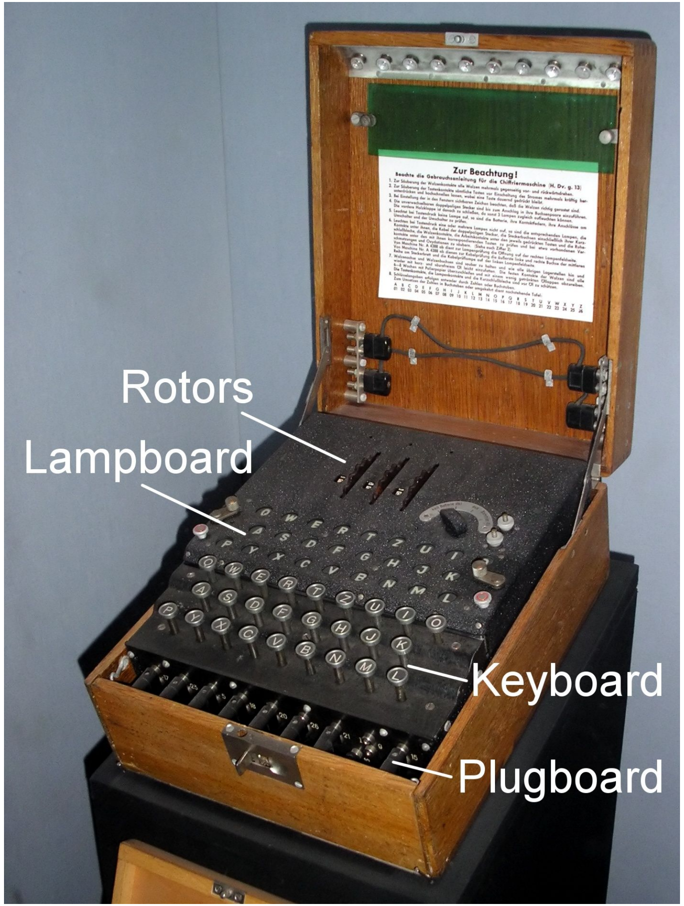
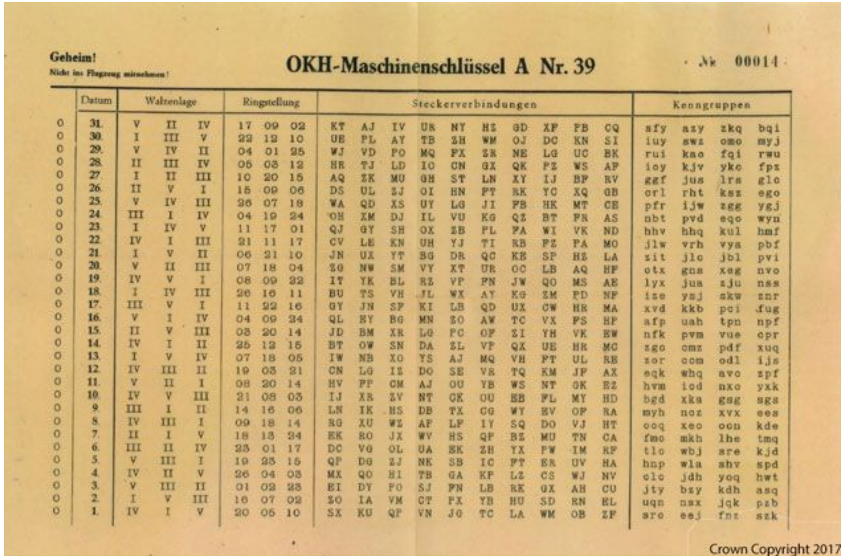
RASPBERRY JAM Cotswold

Enigma messages

Laura Sach

What is Enigma?





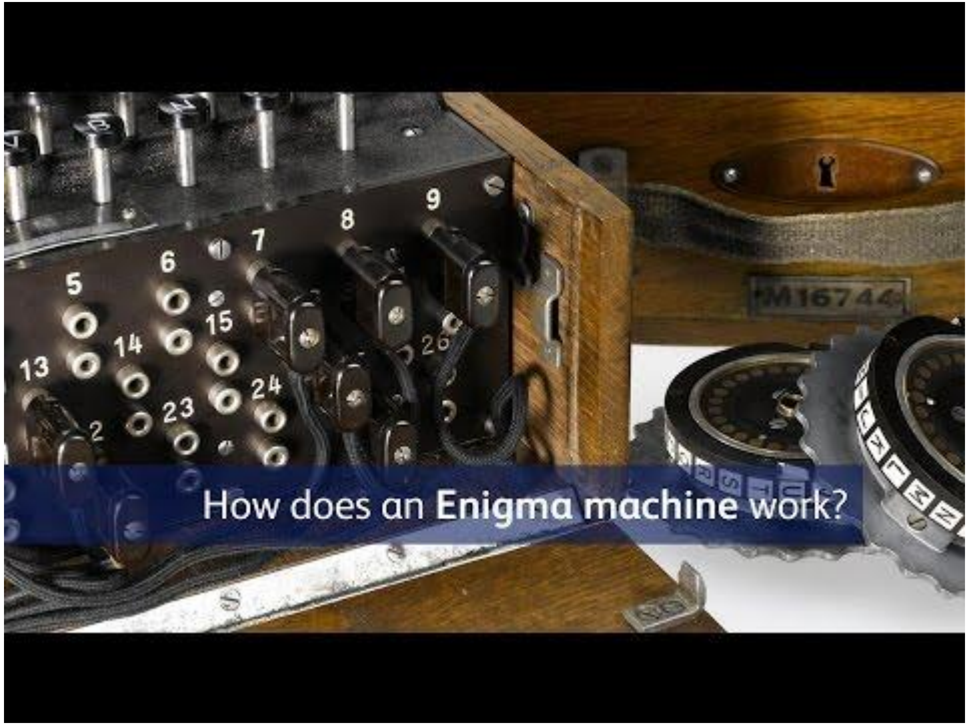
Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39 · № 00014 ·

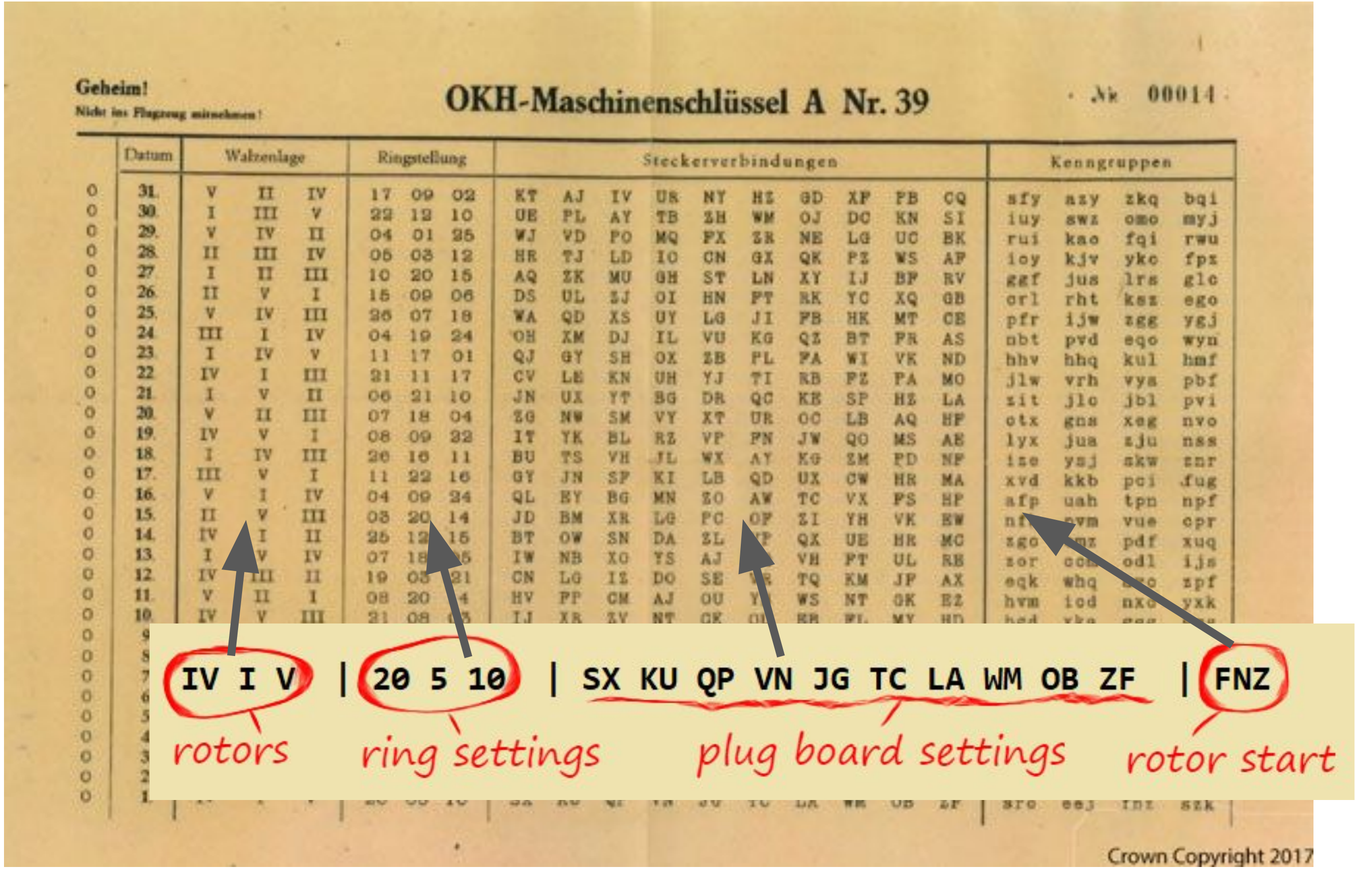
Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	ykc	fpz
27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
26.	II	V	I	15	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	FB	HK	MT	CE	pfr	ijw	zgg	ygj
24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	PR	AS	nbt	pvd	eqo	wyn
23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vya	pbf
21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	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	FN	JW	QO	MS	AE	lyx	jua	zju	nss
18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	PS	HP	afp	uah	tpn	npf
15.	II	V	III	03	20	14	JD	BM	XR	LG	FC	OF	ZI	YH	VK	EW	nfk	pvm	vue	cpr
14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgo	cmz	pdf	xuq
13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	RB	zor	ccm	odl	ijs
12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JF	AX	eqk	whq	avo	zpf
11.	V	II	I	08	20	14	HV	PF	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	iod	nxc	yxk
10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xka	gsg	sgs
9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	EV	OP	RA	myh	noz	xvx	ees
8.	IV	III	I	09	18	14	RG	XU	WZ	AF	LF	IY	SQ	DO	VJ	HT	ooq	xeo	oon	kde
7.	II	I	V	18	13	24	EK	RO	JX	WY	HS	QP	BZ	MU	TN	CA	fmo	mkh	lhe	tmq
6.	III	II	IV	23	01	17	DC	VG	OL	UA	EK	ZH	YX	PW	IM	KF	tlo	wbj	sre	kjd
5.	V	III	I	19	23	15	QP	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd
4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KP	LZ	CS	WJ	NV	clc	jdh	yoq	hwt
3.	V	III	II	01	02	23	EI	DY	FO	SJ	FN	LB	RK	GX	AH	CU	jty	bzy	kdh	asq
2.	I	V	III	16	07	02	ZO	IA	VM	CT	PX	YB	HU	SD	RN	EL	uqn	nsx	jqk	pzb
1.	IV	I	V	20	05	10	SX	KU	QF	VN	JG	TC	LA	WM	OB	ZF	sro	eej	fnz	szk

Image taken from
https://projects.raspberrypi.org/en/projects/octapi-brute-force-enigma

How does Enigma work?



Settings sheet



Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39 · № 00014 ·

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
O	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
O	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
O	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
O	28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	ykc	fpx
O	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
O	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	FT	RK	YC	XQ	GB	orl	rht	ksz	ego
O	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
O	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	PR	AS	nbt	pvd	eqo	wyn
O	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
O	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vys	pbf
O	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	jlo	jbl	pvi
O	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	otx	gns	xeg	nvo
O	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jua	zju	nss
O	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
O	17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
O	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	PS	HP	afp	uah	tpn	npf
O	15.	II	V	III	03	20	14	JD	BM	XR	LG	PC	OF	ZI	YH	VK	EW	[illegible]	pvm	vue	cpr
O	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	[illegible]	QX	UE	HR	MC	zgo	[illegible]	pdf	xuq
O	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	[illegible]	VH	FT	UL	RB	zor	ccm	odl	ijs
O	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JP	AX	eqk	whq	[illegible]	zpf
O	11.	V	II	I	08	20	[illegible]	HV	FP	CM	AJ	OU	[illegible]	WS	NT	GK	EZ	hvm	iod	nxc	yxk
O	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	[illegible]	[illegible]	[illegible]	MY	HD	[illegible]	[illegible]	[illegible]	[illegible]
O	9.																				
O	8.																				
O	7.																				
O	6.																				
O	5.																				
O	4.																				
O	3.																				
O	2.																				
O	1.																				

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

Decrypt a message

```
GON XXLXYFQNZIK
```

```
LJE OIVGWVHOVHKAU
```

Encrypt a message

If you encrypt...

```
BFR RASPBERRYPI
```

...you should get

```
GON XXLXYFQNZIK
```

Decrypt this message

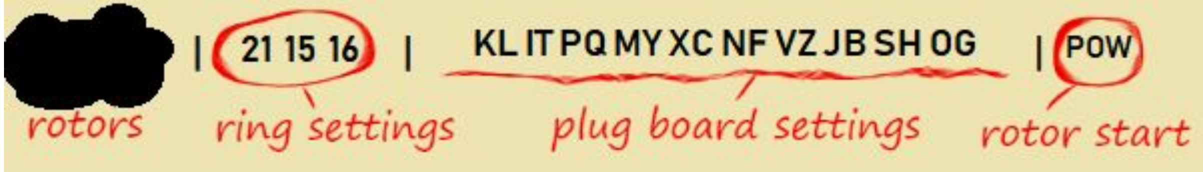
```
GED
```

```
HYZFQOOVVBBKBWPDZLSL
```

Uh oh...

You need to know the settings!

Brute force attack



[redacted] | 21 15 16 | KL IT PQ MY XC NF VZ JB SH OG | POW

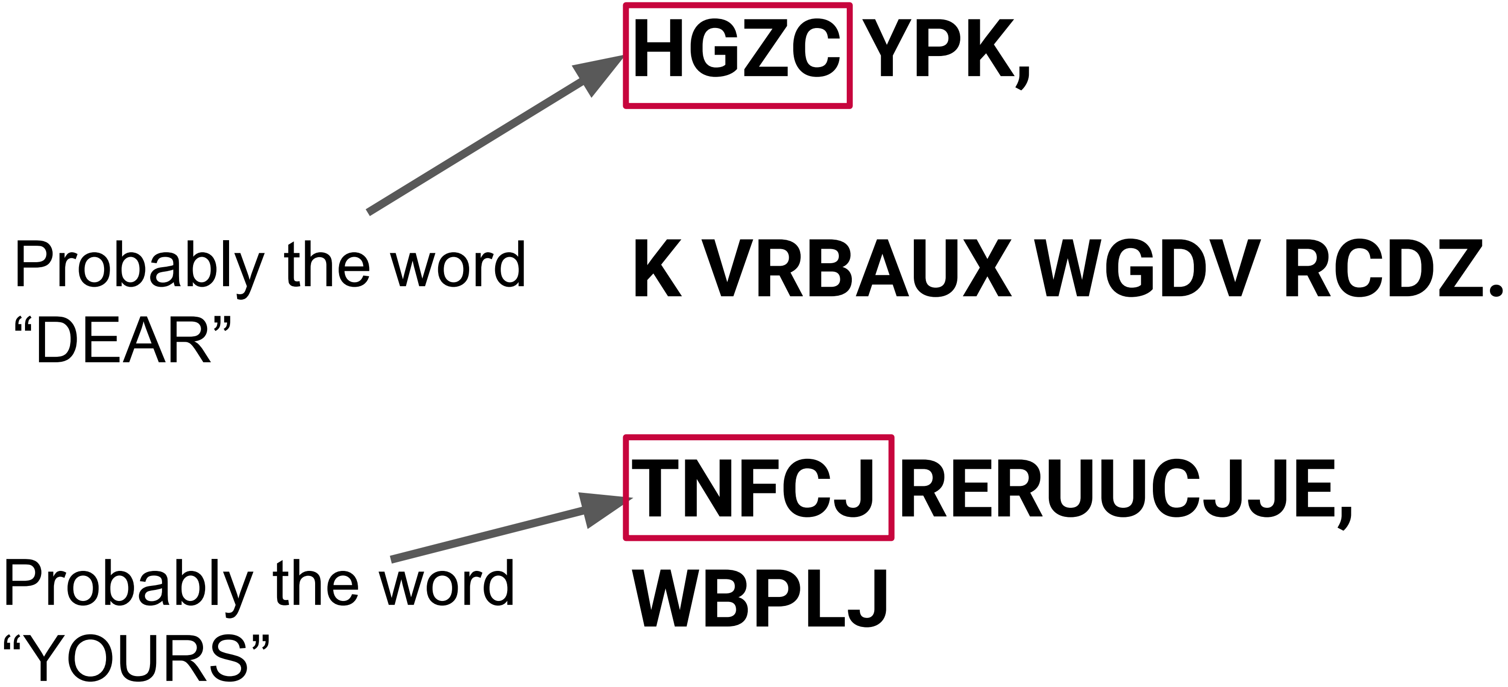
rotors
ring settings
plug board settings
rotor start

?? 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,

K VRBAUX WGDV RCDZ.

TNFCJ RERUUCJJE,

WBPLJ

Probably the word “DEAR”

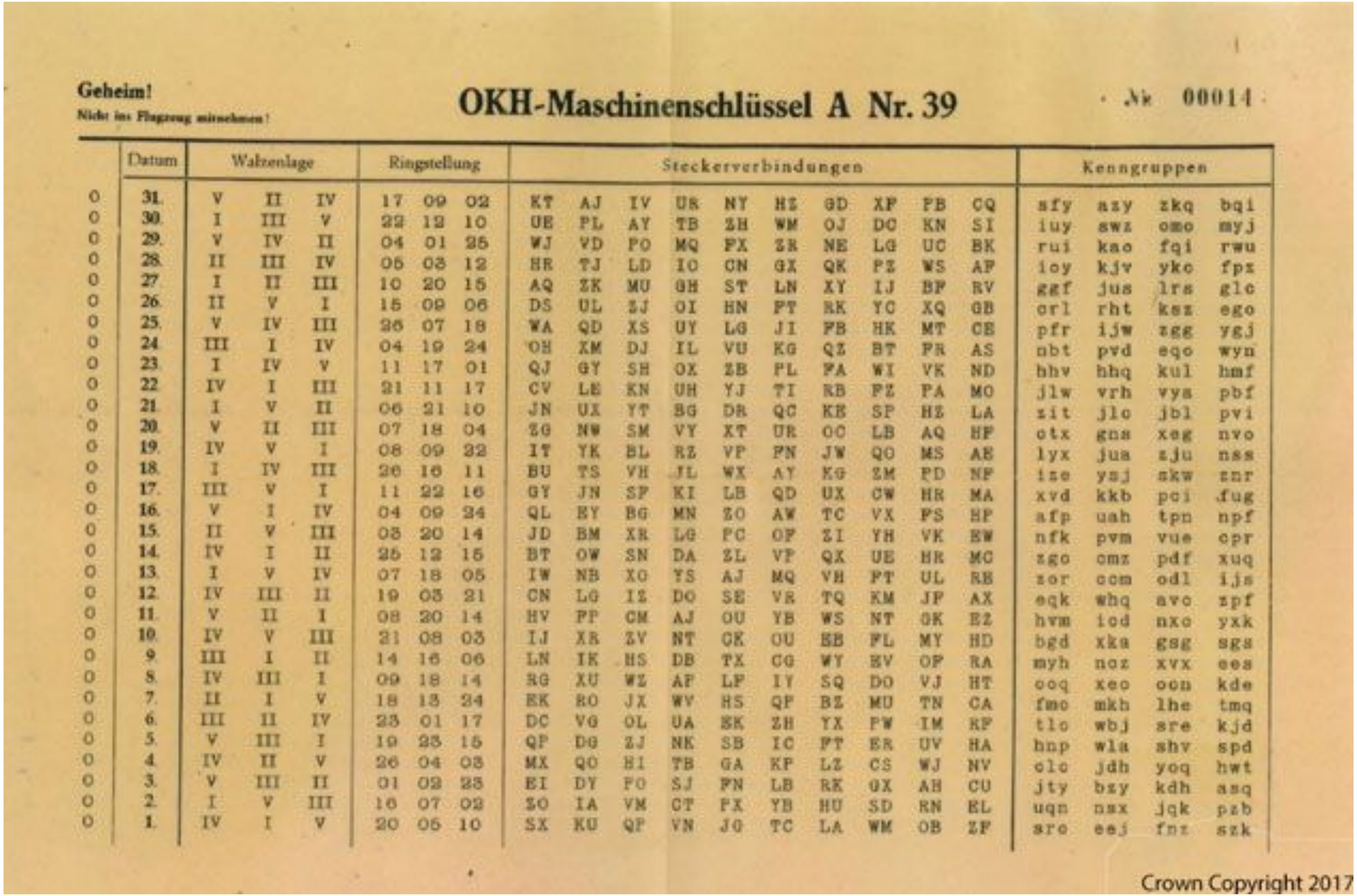
Probably the word “YOURS”

Crib text

Crib text: WEATHER

Cipher text: VZTLMPU

```
VZTLMPUSLKTEXYWZWKXDOTT
```



Geheim!

Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

№ 00014

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
O	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
O	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
O	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
O	28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	ykc	fpz
O	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
O	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	PT	RK	YC	XQ	GB	orl	rht	ksz	ego
O	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
O	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	FR	AS	nbt	pvd	eqo	wyn
O	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
O	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vys	pbf
O	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	jlo	jbl	pvi
O	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	otx	gns	xeg	nvo
O	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jua	zju	nss
O	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
O	17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
O	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	FS	HP	afp	uah	tpn	npf
O	15.	II	V	III	03	20	14	JD	BM	XR	LG	PC	OF	ZI	YH	VK	EW	nfk	pvm	vue	cpr
O	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgo	cmz	pdf	xuq
O	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	RB	zor	ccm	odl	ijs
O	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JP	AX	eqk	whq	avc	zpf
O	11.	V	II	I	08	20	14	HV	PP	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	icd	nxc	yxk
O	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xks	gsg	sgs
O	9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	EV	OP	RA	myh	noz	xvx	ees
O	8.	IV	III	I	09	18	14	RG	XU	WZ	AF	LF	IY	SQ	DO	VJ	HT	ooq	xeo	ocn	kde
O	7.	II	I	V	18	13	24	EK	RO	JX	WV	HS	QP	BZ	MU	TN	CA	fmo	mkh	lhe	tmq
O	6.	III	II	IV	23	01	17	DC	VG	OL	UA	EK	ZH	YX	PW	IM	KF	tlo	wbj	sre	kjd
O	5.	V	III	I	19	23	15	QP	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd
O	4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KP	LZ	CS	WJ	NV	clc	jdh	yoq	hwt
O	3.	V	III	II	01	02	23	EI	DY	FO	SJ	FN	LB	RK	GX	AH	CU	jty	bzy	kdh	asq
O	2.	I	V	III	16	07	02	ZO	IA	VM	CT	PX	YB	HU	SD	RN	EL	uqn	nsx	jqk	pzb
O	1.	IV	I	V	20	05	10	SX	KU	QP	VN	JG	TC	LA	WM	OB	ZF	sro	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