An Enigma Machine in Elm

bobkonf 2022 / **@arkh4m**

My name is Ju 🙇‍♂️

whoami

- I was born in 🇨🇳
- Grew up in 🇮🇹
- Live in 🇬🇧
- Find me at **@arkh4m**
- Work for no_red_ink

A super super super short history of cryptography

What is it

kryptos hidden / *graphia* writing

— Encode: turn *plain* text into *cypher* text.

— Decode: turn *cypher* text into *plain* text.

Caesar Cipher

Shift each letter by 3.

Caesar Cipher

Encode: shift by 3

ET TU BRUTUS

turns into

HW WX EUXWX

Caesar Cipher

Encode: shift by 3

ET TU BRUTUS

turns into

HW WX EUXWX

Decode: shift by -3

HW WX EUXWX

turns into

ET TU BRUTUS

Monoalphabetic substitution

Decide on a mapping between letters:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ZYXWVUTSRQPONMLKJIHGFEDCBA

Monoalphabetic substitution

Encode: lookup table

NEVER GONNA GIVE YOU UP

turns into

MVEVI TLMMZ TREV BLF FK

Monoalphabetic substitution

Encode: lookup table

NEVER GONNA GIVE YOU UP

turns into

MVEVI TLMMZ TREV BLF FK

Decode: reverse lookup

MVEVI TLMMZ TREV BLF FK

turns into

NEVER GONNA GIVE YOU UP

Any problems?

Spaces

- Spaces in cipher text give away too much.

  MVEVI TLMMZ TREV BLF FK

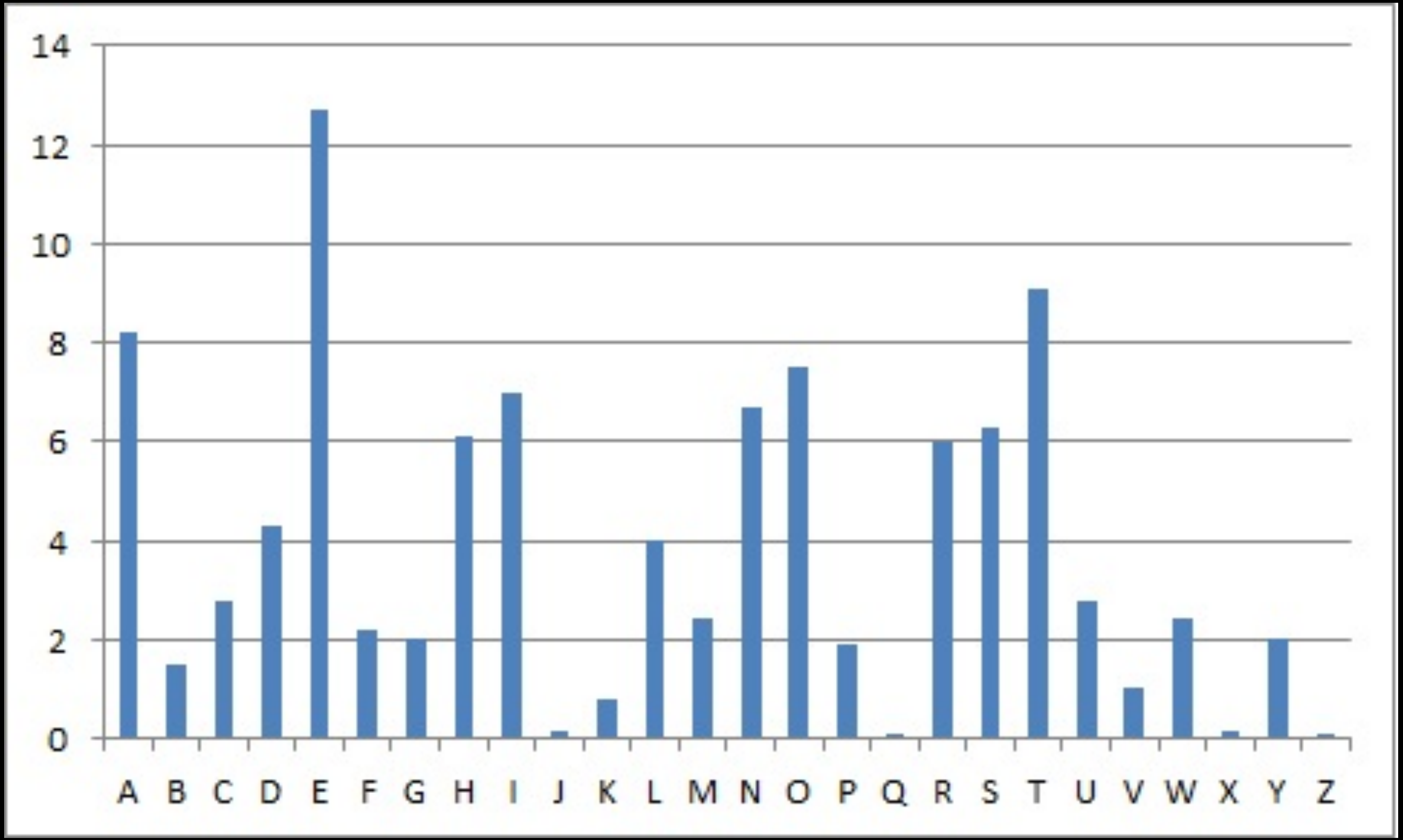
- Easy fix, just remove them!

  NEVER GONNA GIVE YOU UP

  turns into

  MVEVITLMMZTREVBLFFK

Frequency analysis



No fix sry 🙀🙀🙀

Fast forward a 1000 years...

The Enigma Machine

Zur Beachtung!

Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13)

1. Zur Säuberung der Walzenkontakte alle Walzen mehrmals gegenseitig vor- und rückwärtsdrehen.
2. Zur Säuberung der Tastenkontakte sämtliche Tasten vor Einschaltung des Stromes mehrmals kräftig herunterdrücken und hochschnellen lassen, wobei eine Taste dauernd gedrückt bleibt.
3. Bei Einstellung der in den Fenstern sichtbaren Zeichen beachten, daß die Walzen richtig gerastet sind.
4. Die unverwechselbaren doppelpoligen Stecker sind bis zum Anschlag in ihre Buchsenpaare einzuführen. Die vordere Holzklappe ist danach zu schließen, da sonst 3 Lampen zugleich aufleuchten können.
5. Leuchtet bei Tastendruck keine Lampe auf, so sind die Batterie, ihre Kontaktfedern, ihre Anschlüsse am Umschalter und der Umschalter zu prüfen.
6. Leuchten bei Tastendruck eine oder mehrere Lampen nicht auf, so sind die entsprechenden Lampen, die Kontakte unter ihnen, die Kabel der doppelpoligen Stecker, die Steckerbuchsen einschließlich ihrer Kurzschlußbleche, die Walzenkontakte, die Arbeitskontakte unter den jeweils gedrückten Tasten und die Ruhekontakte unter den mit ihnen korrespondierenden Tasten zu prüfen und bei etwa vorhandenen Verschmutzungen und Oxydationen zu säubern (siehe auch Ziffer 2).
   Von Maschine Nr. A 4388 ab dient zur Lampenprüfung die Öffnung auf der rechten Lampenfeldseite.
   Von Maschine Nr. A 4388 ab dienen zur Kabelprüfung die äußerste linke und rechte Buchse der mittleren Reihe am Steckerbrett und die Kabelprüflampe auf der linken Lampenfeldseite.
7. Walzenachse und Walzenbuchsen sind sauber zu halten und wie alle übrigen Lagerstellen hin und wieder mit harz- und säurefreiem Öl leicht einzufetten. Die festen Kontakte der Walzen sind alle 6—8 Wochen mit Polierpapier überzuschleifen und mit einem wenig getränkten Öllappen abzureiben. Die Tastenkontakte, die Lampenkontakte und die Kurzschlußbleche sind vor Öl zu schützen.
8. Schlüsselangaben erfolgen entweder durch Zahlen oder Buchstaben.
   Zum Umsetzen der Zahlen in Buchstaben oder umgekehrt dient nachstehende Tafel:

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
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

The Enigma Machine

- Used from the 1920s
- Used by all Wehrmacht in WW2
- Mechanical with a battery
- Polyalphabetic cipher

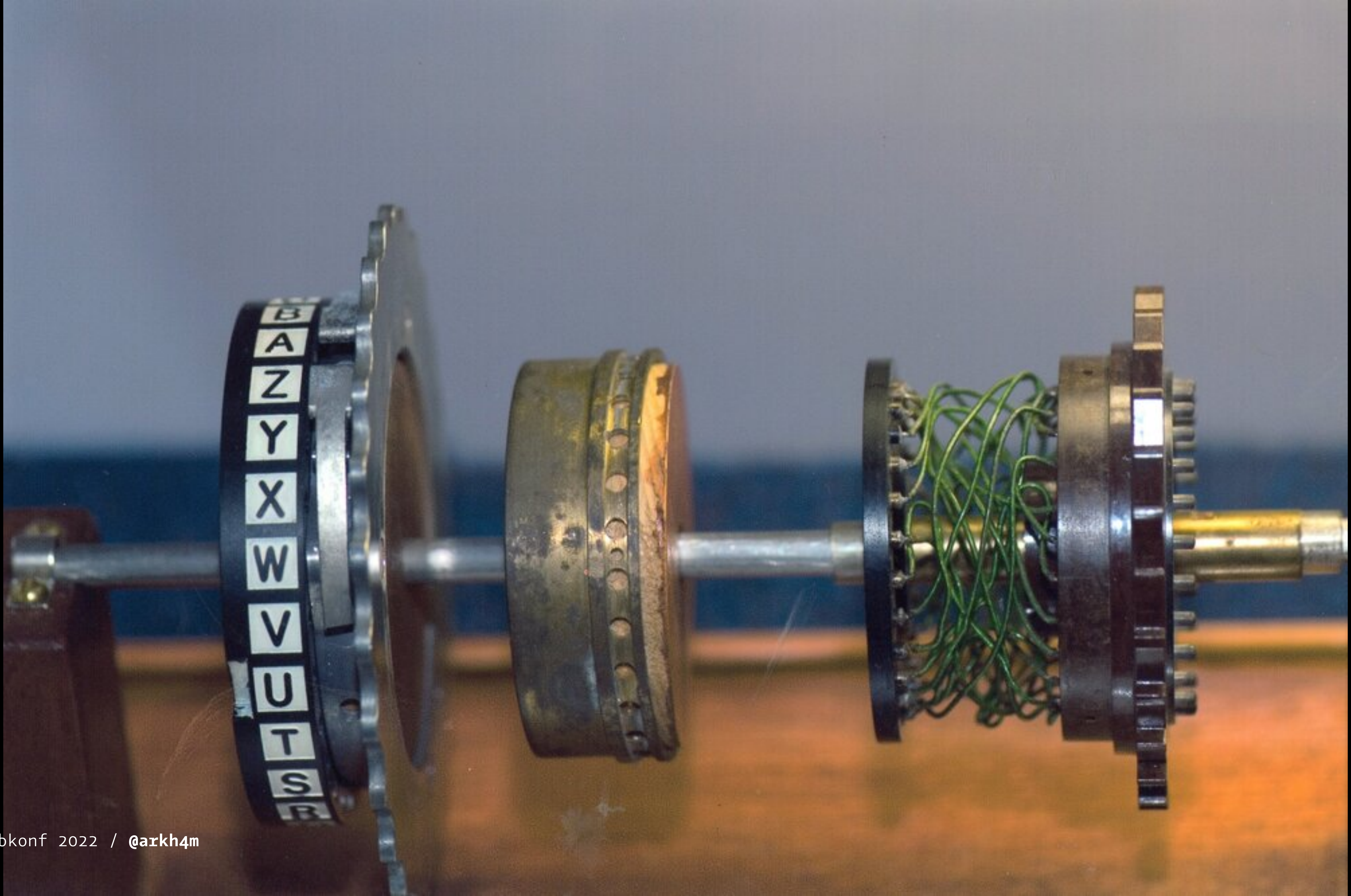
Zur Beachtung!
Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13)
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

Polyalphabetic

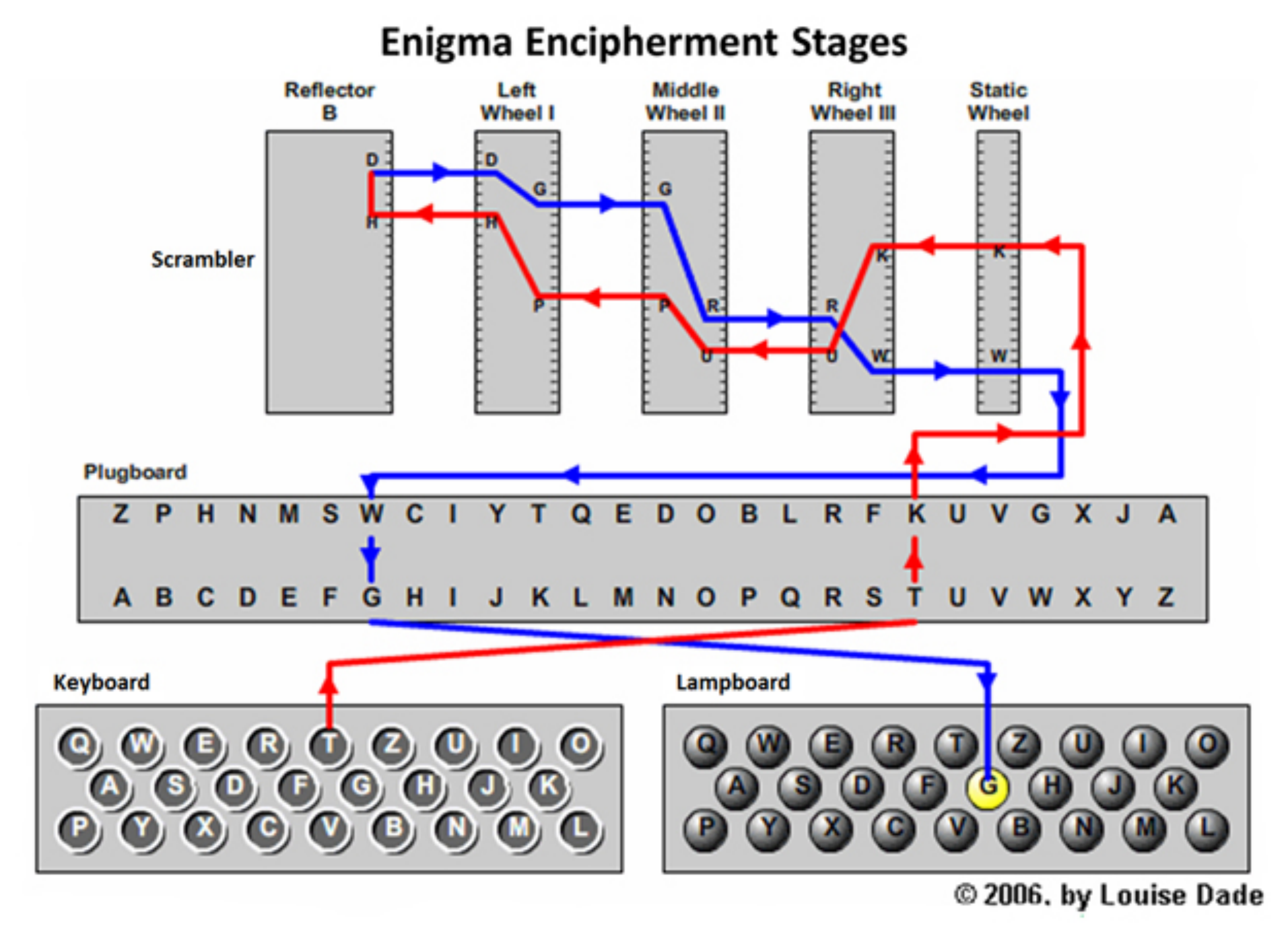
The cipher changes at every keypress! How?

Zur Beachtung!
Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13)

Nur Glühlampen mit 12 mm Durchmesser verwenden.
QWERTZUIO
ASDFGHJK
PYXCVBNML
A

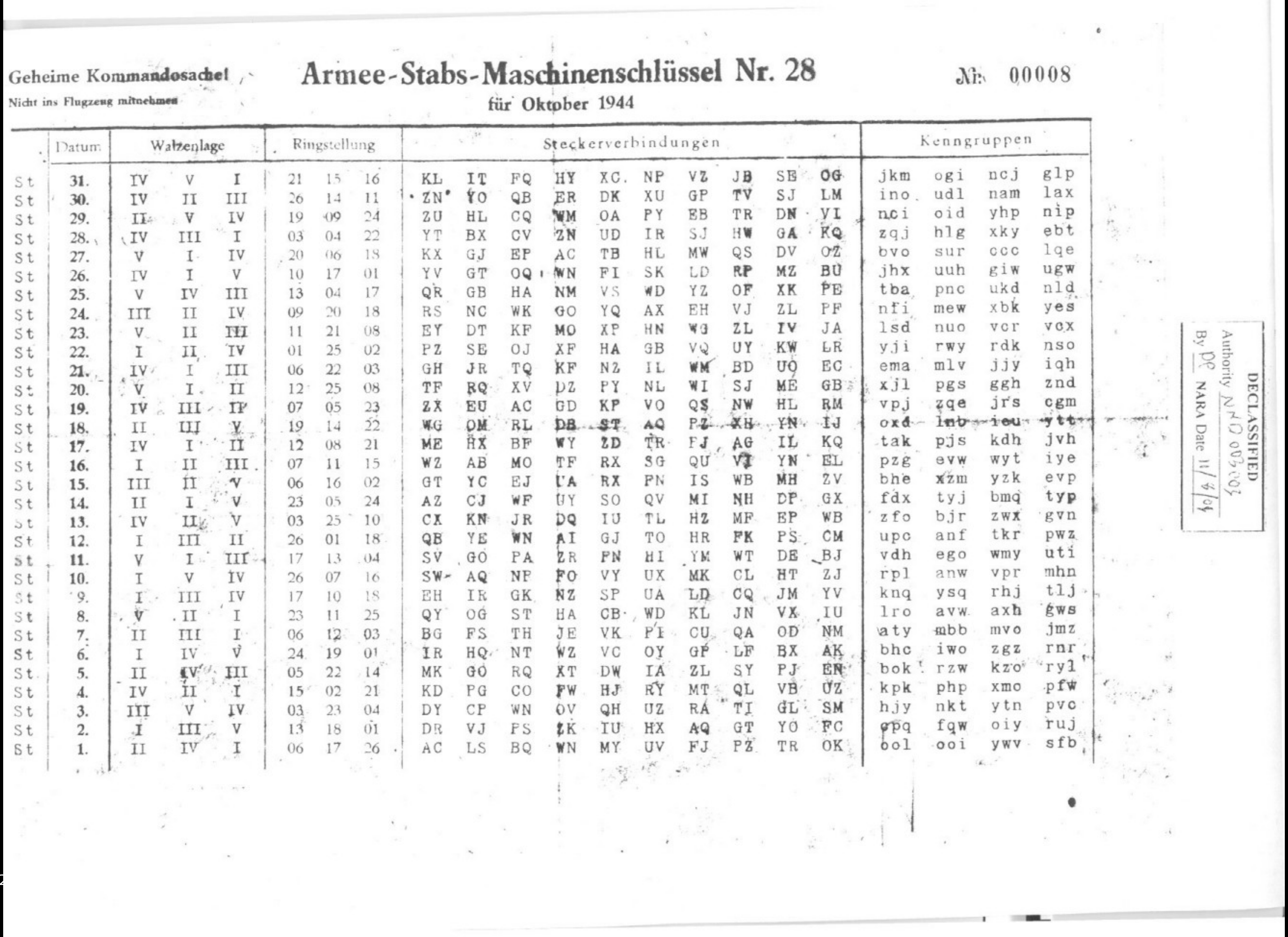

B
A
Z
Y
X
W
V
U
T
S
R

Journey of a letter



Enigma
Machine
Q
W
E
R
T
Z
A
S
D
F
G
H
P
Y
X
C
V
B
ENIGMA

How to use the Enigma Machine



Geheime Kommandosache!

Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

№ 00008

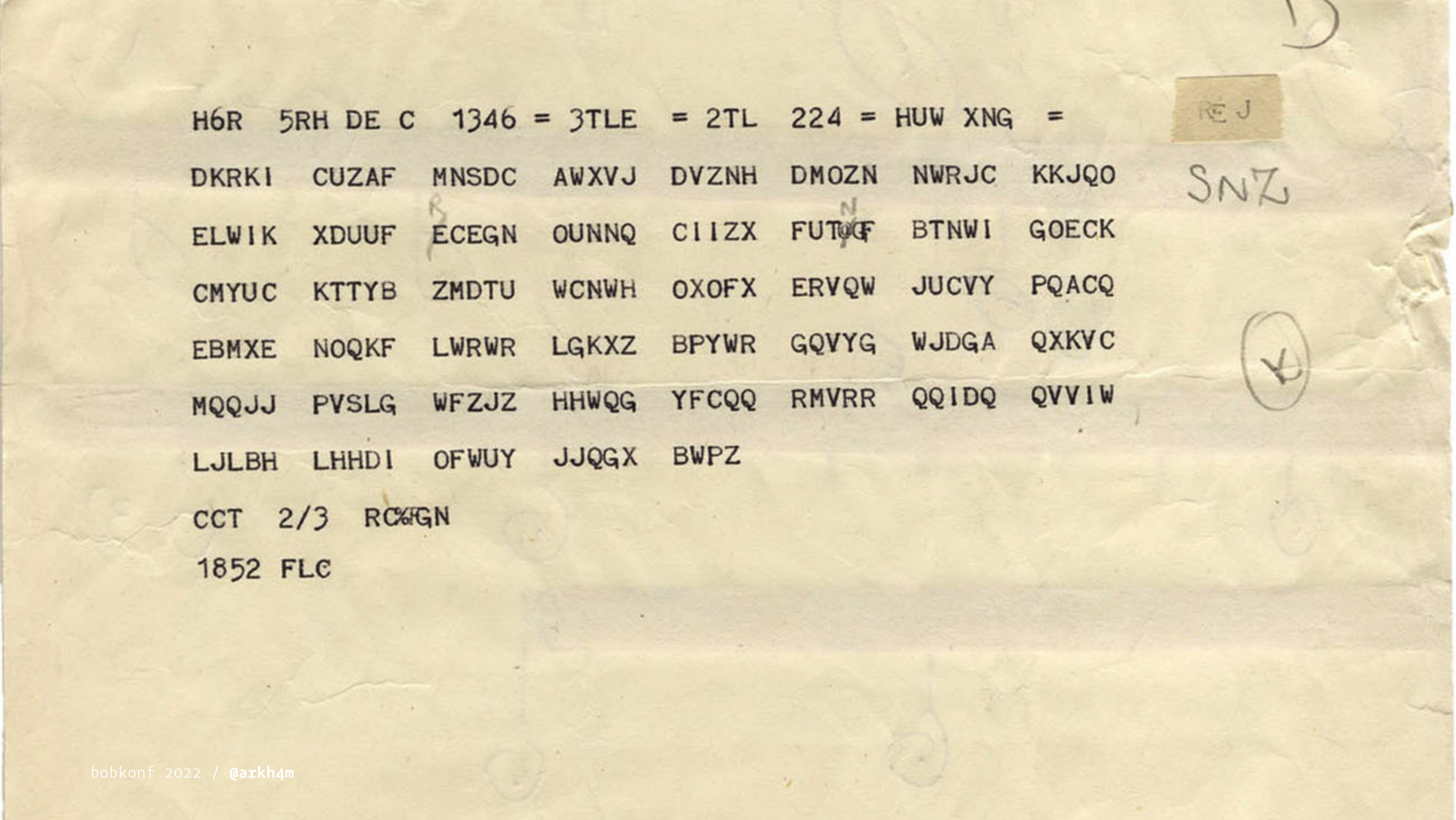
	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III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

DECLASSIFIED
Authority NND 003007
By DC NARA Date 11/4/04

bobkonf 2

How to encipher a message

- Open the codebook
- Pick the rotors with the right settings
- Set the plugboard
- Set the rotor positions randomly (write this down)
- Choose a three letter message key and encode it twice (write it down)
- Set the rotors positions to the message key and encrypt the message
- Send in plaintext the initial random positions, the six letter encoded message key and the encrypted message



D

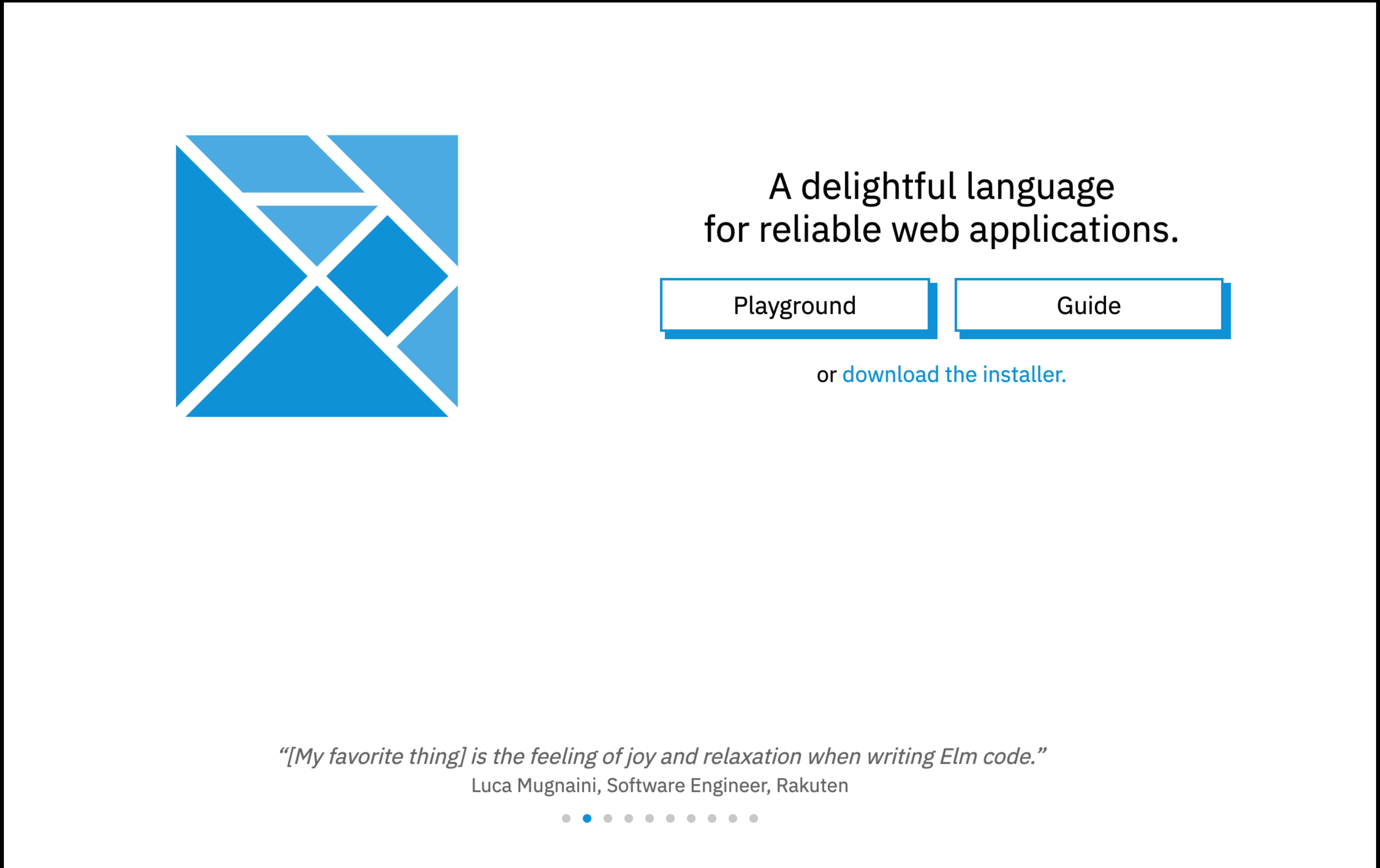
REJ

```
H6R  5RH DE C  1346 = 3TLE  = 2TL  224 = HUW XNG  =

DKRKI  CUZAF  MNSDC  AWXVJ  DVZNH  DMOZN  NWRJC  KKJQO      SNZ
              R                    N
ELWIK  XDUUF  ECEGN  OUNNQ  CIIZX  FUTQF  BTNWI  GOECK

CMYUC  KTTYB  ZMDTU  WCNWH  OXOFX  ERVQW  JUCVY  PQACQ

EBMXE  NOQKF  LWRWR  LGKXZ  BPYWR  GQVYG  WJDGA  QXKVC      K

MQQJJ  PVSLG  WFZJZ  HHWQG  YFCQQ  RMVRR  QQIDQ  QVVIW

LJLBH  LHHDI  OFWUY  JJQGX  BWPZ

CCT  2/3  RC%GN

1852 FLC
```

How to decipher a message

- Open the codebook
- Pick the rotors with the right settings
- Set the plugboard
- Set the rotor positions to the three letter plaintext message
- Decode the six letters to get the message key repeated twice
- Set the rotors to the message key and decrypt the message

Elm!



A delightful language
for reliable web applications.

or download the installer.

“[My favorite thing] is the feeling of joy and relaxation when writing Elm code.”
Luca Mugnaini, Software Engineer, Rakuten

Elm

- Statically typed
- Pure
- Compiles to JS
- Fun (hehe)

Code dive 🤿

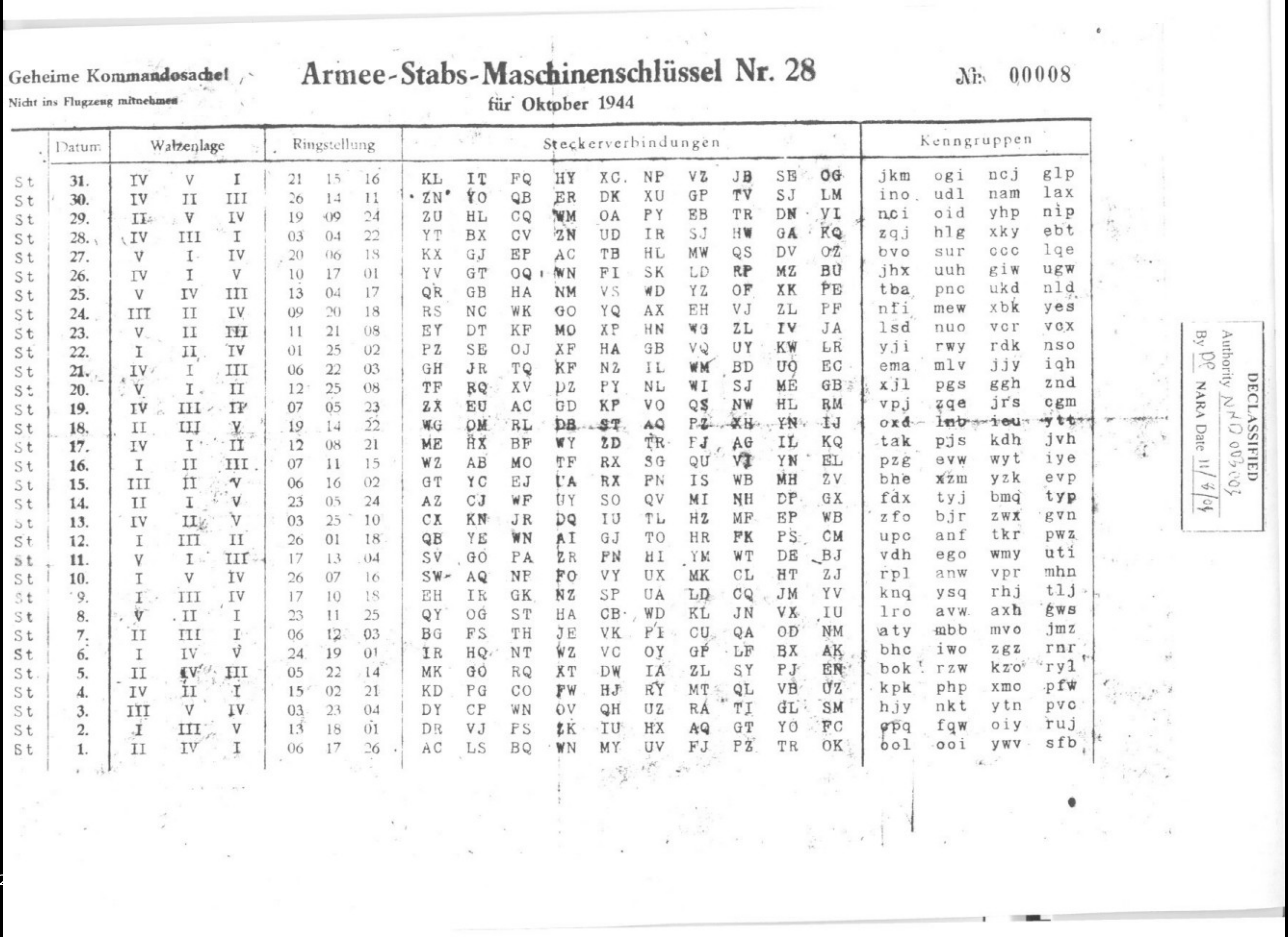
Rotor: encoding

```
encode : Char -> Enigma -> ( Char, Enigma )
encode input enigma =
    let
        ({ leftRotor, middleRotor, rightRotor } as stepped) =
            step enigma
    in
    ( input
        |> Plugboard.swap enigma.plugboard
        |> Rotor.toRotorOffset
        |> Rotor.forward rightRotor
        |> Rotor.forward middleRotor
        |> Rotor.forward leftRotor
        |> Reflector.reflect enigma.reflector
        |> Rotor.backward leftRotor
        |> Rotor.backward middleRotor
        |> Rotor.backward rightRotor
        |> Rotor.fromRotorOffset
        |> Plugboard.swap enigma.plugboard
    , stepped
    )
```

Rotor: stepping

```
step : Enigma -> Enigma
step ({ leftRotor, middleRotor, rightRotor } as info) =
    case ( Rotor.atNotch middleRotor , Rotor.atNotch rightRotor) of
        ( True, _ ) ->
            { info
                | middleRotor = Rotor.turn middleRotor
                , leftRotor = Rotor.turn leftRotor
                , rightRotor = Rotor.turn rightRotor
            }

        ( _, True ) ->
            { info
                | middleRotor = Rotor.turn middleRotor
                , rightRotor = Rotor.turn rightRotor
            }

        _ ->
            { info | rightRotor = Rotor.turn rightRotor }
```

Let's try it out!



Geheime Kommandosache!

Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

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

DECLASSIFIED
Authority NND 003003
By DP NARA Date 11/4/04

- Today is the 11th
- Rotors: V I III
- Settings: 17 13 04
- Plugboard: SV GO PA ZR FN HI YM WT DE BJ
- Random starting position: 5 12 13
- Message key: MIC
- Message: KEINE BESONDEREN EREIGNISSE

Resources

- How did the Enigma Machine work?
  https://www.youtube.com/watch?v=ybkkiGtJmkM
- Enigma, Historical Lessons in Cryptography
  https://jgandrews.com/posts/the-enigma-machine
- Working principle of the Enigma
  https://cryptomuseum.com/crypto/enigma/working.htm
- A better Elm implementation
  https://simonhauck.github.io/Enigma-Elm
- Enigma Machine Emulator
  https://www.101computing.net/enigma-machine-emulator
- Cipher Machines and Cryptology
  https://www.ciphermachinesandcryptology.com
- The German cipher machine Enigma
  https://www.matematiksider.dk/enigma_eng.html
- 3D printed Enigma machine
  https://www.youtube.com/watch?v=RP10yP5WgSM

Thank you!

- @arkh4m
- https://enigma.juliu.is
- https://github.com/arkham/enigma-in-elm
- https://donate.unhcr.org/int/en/ukraine-emergency