

# verschlüsselt entschlüsselt

– wie es geht  
und wie man es selber macht



30. Mai 2018

Prof. Dr. rer. nat. Peter Gerwinski  
Campus Velbert/Heiligenhaus  
Hochschule Bochum

Hochschule Bochum  
Bochum University  
of Applied Sciences



Campus  
Velbert/Heiligenhaus

DEUTSCHES SCHLOSS- UND BESCHLÄGEMUSEUM VELBERT



[www.museum.velbert.de](http://www.museum.velbert.de)

# verschlüsselt entschlüsselt

– wie es geht  
und wie man es selber macht

- Wie funktioniert die Enigma-Verschlüsselung?
- Wie konnte die Enigma-Verschlüsselung gebrochen werden?
  - Pause –
- Wie verschlüsselt man heute?



Hochschule Bochum  
Bochum University  
of Applied Sciences



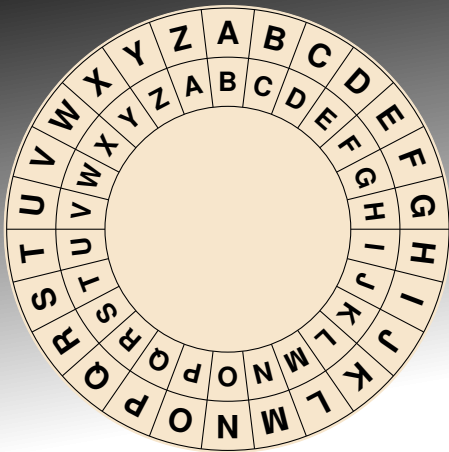
Campus  
Velbert/Heiligenhaus

DEUTSCHES SCHLOSS- UND BESCHLÄGEMUSEUM VELBERT



[www.museum.velbert.de](http://www.museum.velbert.de)

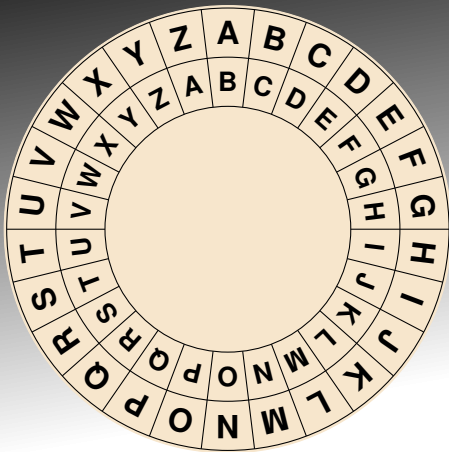
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Cäsar-Chiffre: Buchstaben verdrehen

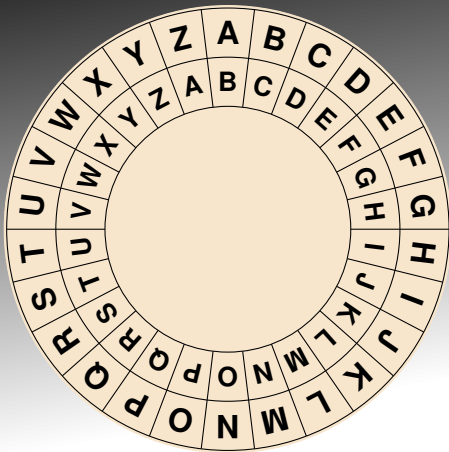
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen  
B

Cäsar-Chiffre: Buchstaben verdrehen

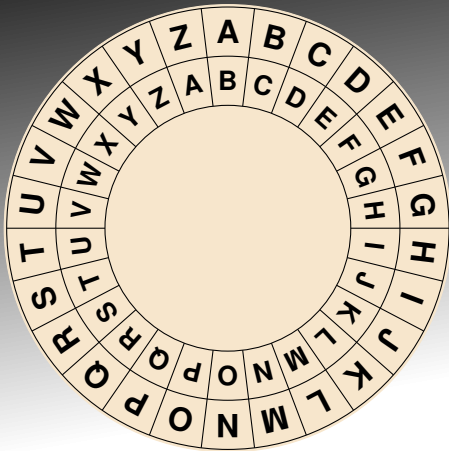
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen  
Bq

Cäsar-Chiffre: Buchstaben verdrehen

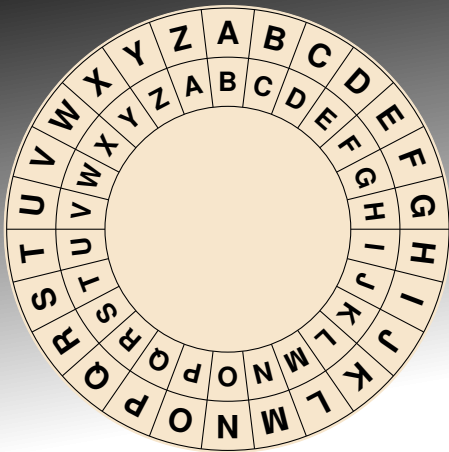
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen  
Bqg

Cäsar-Chiffre: Buchstaben verdrehen

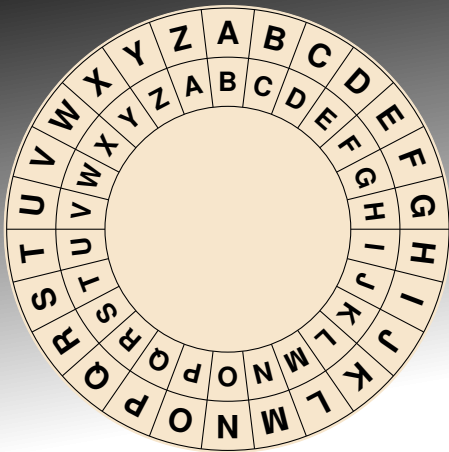
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen  
Bqgfmldvifo

Cäsar-Chiffre: Buchstaben verdrehen

# Wie funktioniert die Enigma-Verschlüsselung?

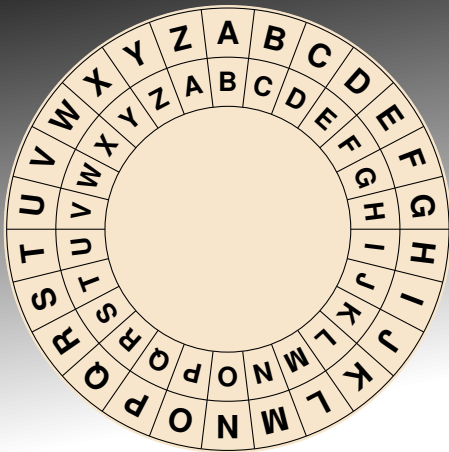


Bqgfmldvdi fo

Cäsar-Chiffre: Buchstaben verdrehen



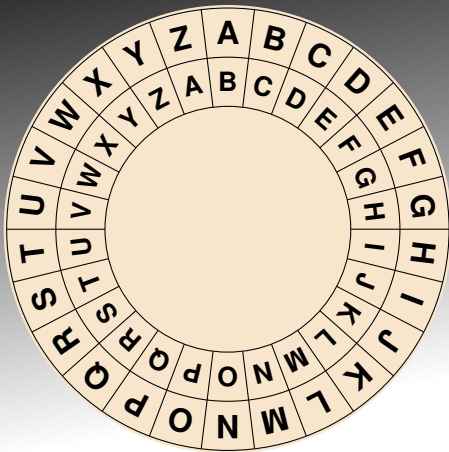
# Wie funktioniert die Enigma-Verschlüsselung?



Bqgfmldvifo  
A

Cäsar-Chiffre: Buchstaben verdrehen

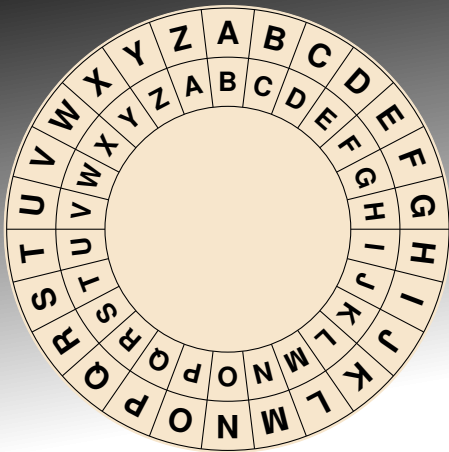
# Wie funktioniert die Enigma-Verschlüsselung?



Bqgfmldvifo  
Ap

Cäsar-Chiffre: Buchstaben verdrehen

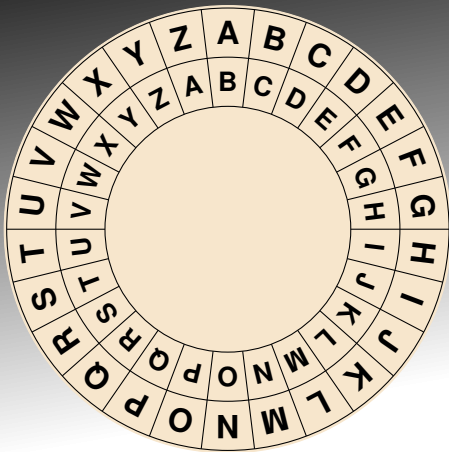
# Wie funktioniert die Enigma-Verschlüsselung?



Bqgfmldvifo  
Apf

Cäsar-Chiffre: Buchstaben verdrehen

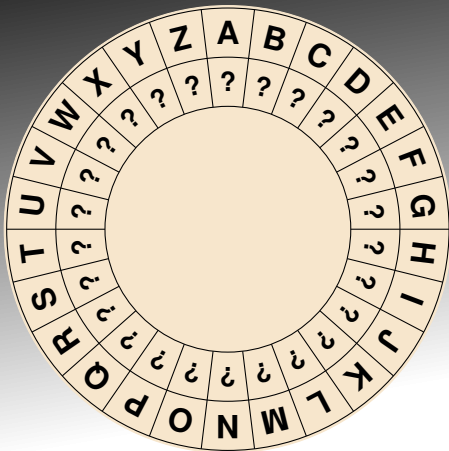
# Wie funktioniert die Enigma-Verschlüsselung?



Bqgfmldi fo  
Apfelkuchen

Cäsar-Chiffre: Buchstaben verdrehen

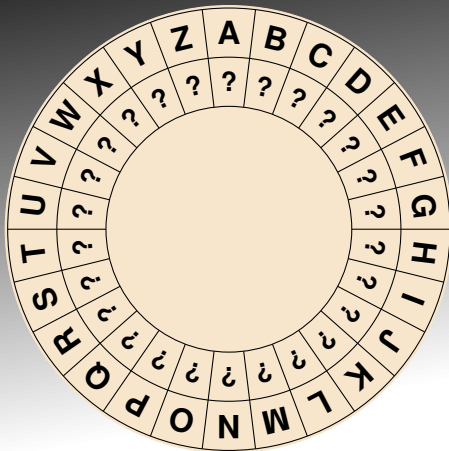
# Wie funktioniert die Enigma-Verschlüsselung?



Vwuhqj jhkhlp

Cäsar-Chiffre: Buchstaben verdrehen  
Verschlüsselung brechen: ???

# Wie funktioniert die Enigma-Verschlüsselung?



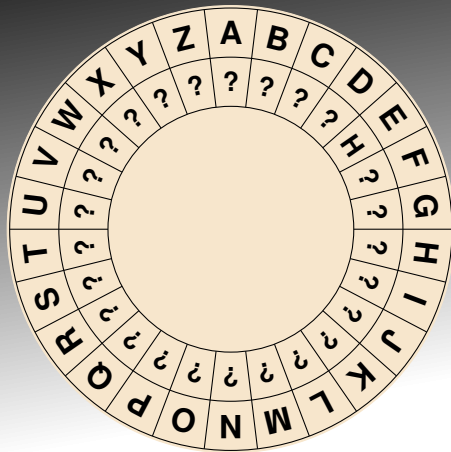
Vwu**h**qj j**h**k**h**lp

Cäsar-Chiffre: Buchstaben verdrehen

Verschlüsselung brechen:

**Regelmäßigkeit** der Sprache: Buchstabenhäufigkeit

# Wie funktioniert die Enigma-Verschlüsselung?



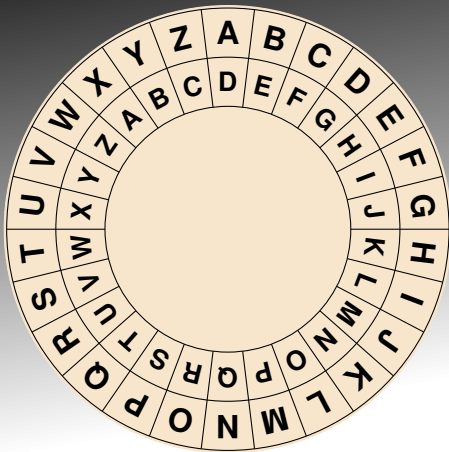
Vwu**h**qj j**h**khlp  
---**e**--- --**e**-**e**---

Cäsar-Chiffre: Buchstaben verdrehen

Verschlüsselung brechen:

**Regelmäßigkeit** der Sprache: Buchstabenhäufigkeit

# Wie funktioniert die Enigma-Verschlüsselung?



Vwu**h**qj j**h**khlp  
---**e**--- --**e**-**e**---

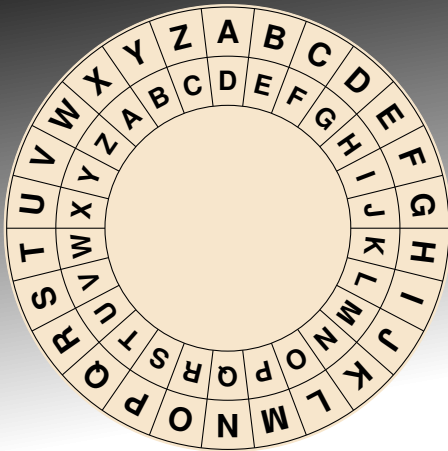
Cäsar-Chiffre: Buchstaben verdrehen

Verschlüsselung brechen:

**Regelmäßigkeit** der Sprache: Buchstabenhäufigkeit



# Wie funktioniert die Enigma-Verschlüsselung?



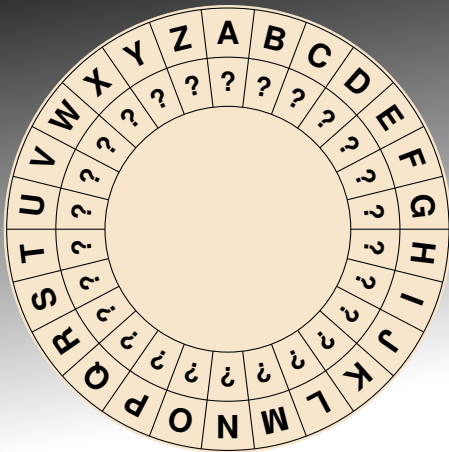
Vwu**h**qj j**h**khlp  
Stre**n**g ge**h**eim

Cäsar-Chiffre: Buchstaben verdrehen

Verschlüsselung brechen:

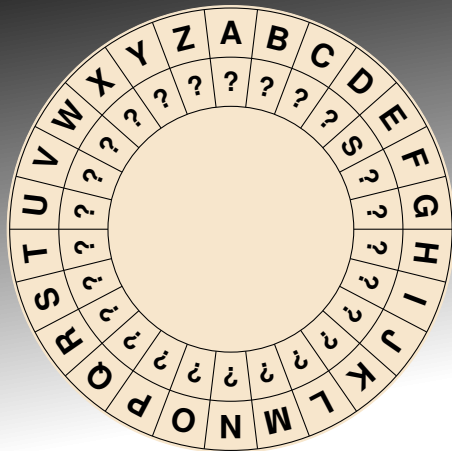
**Regelmäßigkeit** der Sprache: Buchstabenhäufigkeit

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsrsukfuz wsa  
Sfulkd

# Wie funktioniert die Enigma-Verschlüsselung?



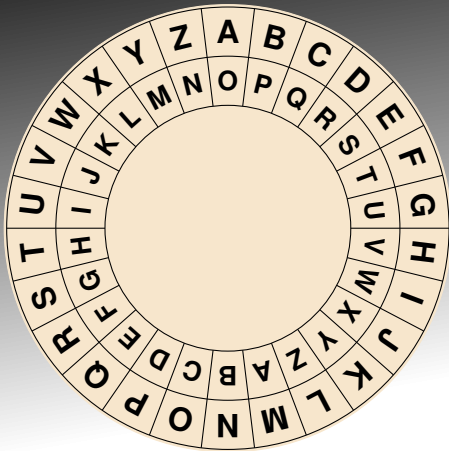
Wdz Lsrsukfuz wsa

Sfulkd

--- e-e-----e-

E-----

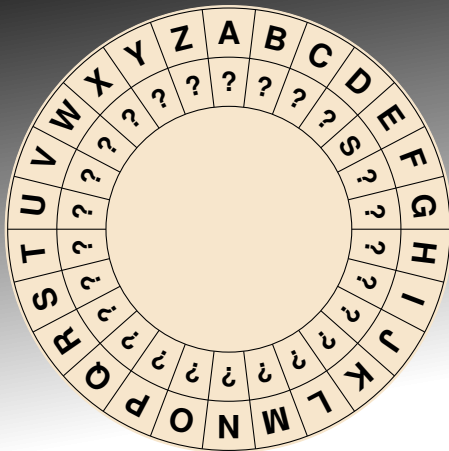
# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsrsukfuz wsa  
Sfulkd

Ipl Xedegwrgl iem  
Ergxwp

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsrsukfuz wsa

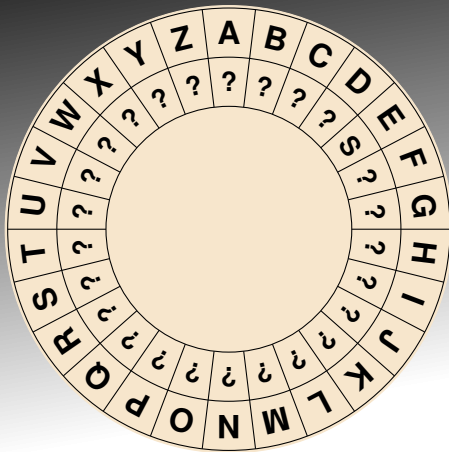
Sfulkd

Ipl Xedegwrgl iem

Ergxwp

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsrsukfuz wsa

Sfulkd

--- e-e --- e-

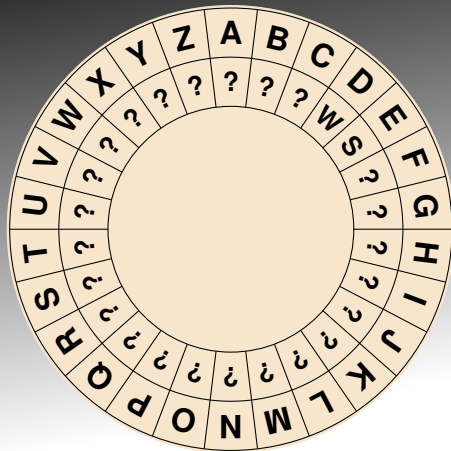
E-----

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln

Verschlüsselung brechen:

Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

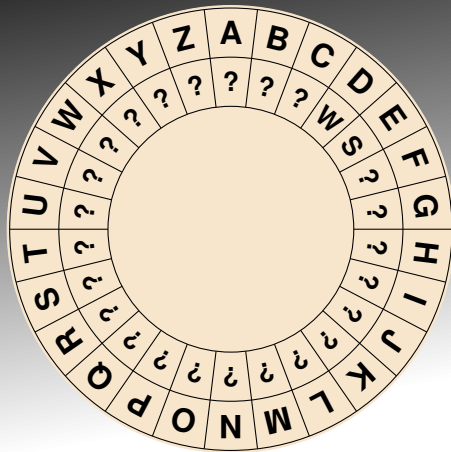
# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsrsukfuz wsa  
Sfulkd  
--- -e-e----- de-  
E-----

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln  
Verschlüsselung brechen:  
Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

# Wie funktioniert die Enigma-Verschlüsselung?

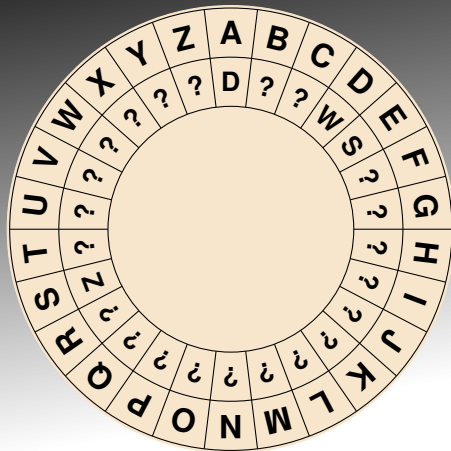


Wdz Lsr sukfuz wsa  
Sfulkd  
D-- -e-e----- de-  
E-----

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln  
Verschlüsselung brechen:  
Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache



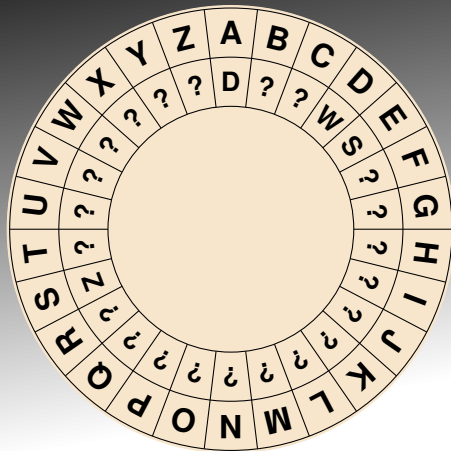
# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsr sukfuz wsa  
Sfulkd  
Das -e-e----- de-  
E-----

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln  
Verschlüsselung brechen:  
Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

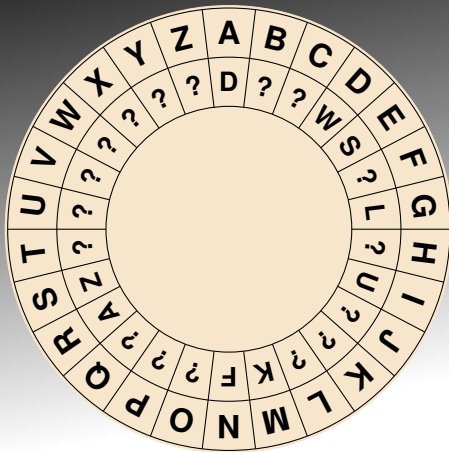
# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsr suk fuz wsa  
Sfulkd  
Das -e-e-----s de-  
E-----a

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln  
Verschlüsselung brechen:  
Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsr suk fuz wsa

Sfulkd

Das -e-e-----s der

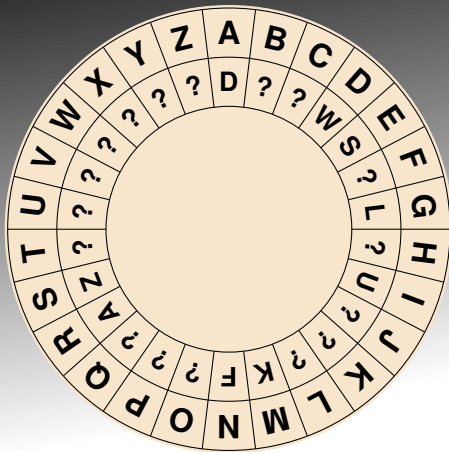
Enigma

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln

Verschlüsselung brechen:

Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsr suk fuz wsa

Sfulkd

Das -e-ei-nis der

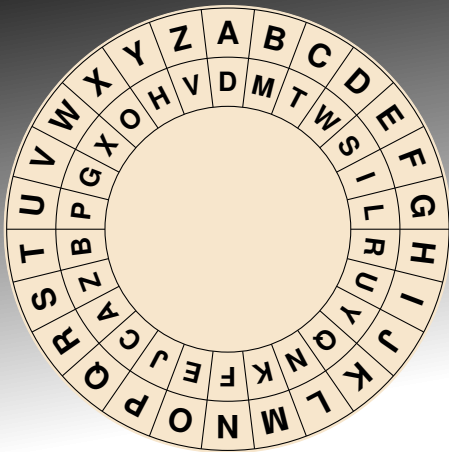
Enigma

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln

Verschlüsselung brechen:

Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

# Wie funktioniert die Enigma-Verschlüsselung?



Wdz Lsr<sup>s</sup>ukfuz wsa

Sfulkd

Das Gehe<sup>e</sup>imnis der

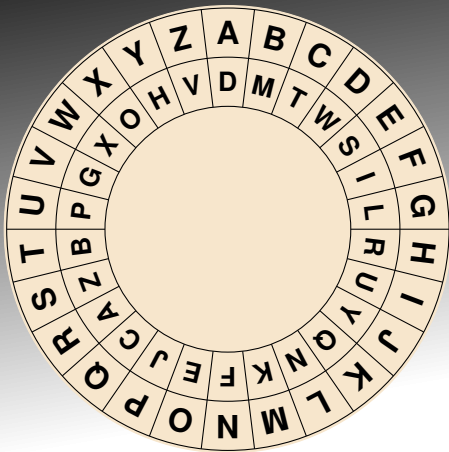
Enigma

Monoalphabetische Substitution: Buchstaben durcheinanderwürfeln

Verschlüsselung brechen:

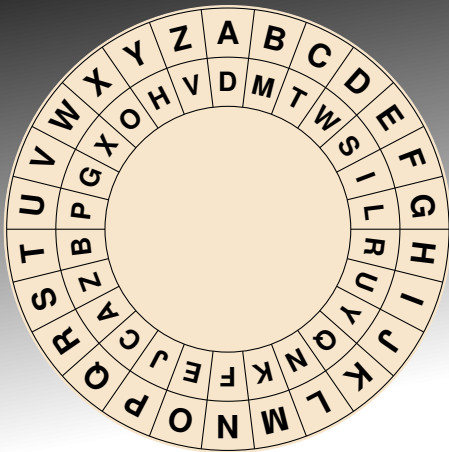
Buchstabenhäufigkeit und weitere **Regelmäßigkeiten** der Sprache

# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

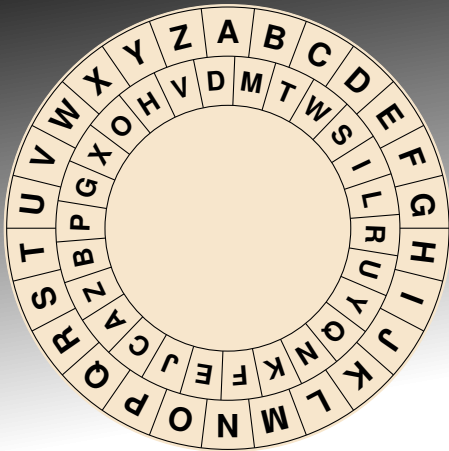
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

D

# Wie funktioniert die Enigma-Verschlüsselung?

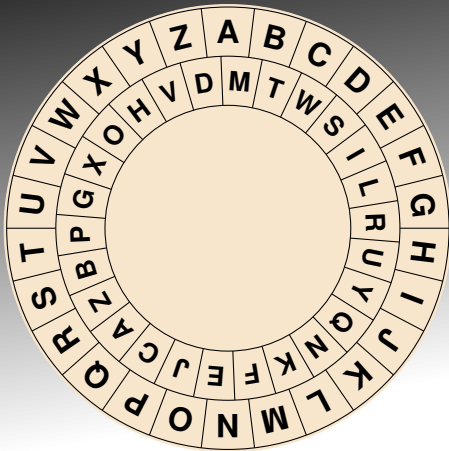


Apfelkuchen

D



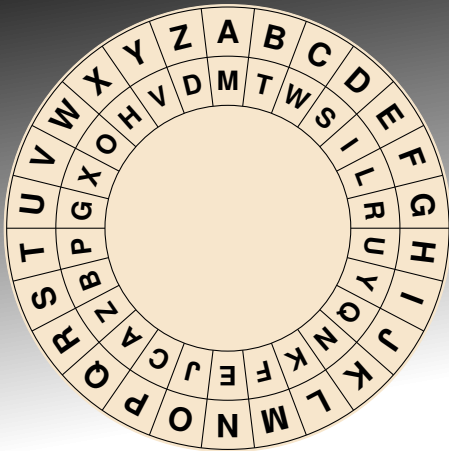
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

D

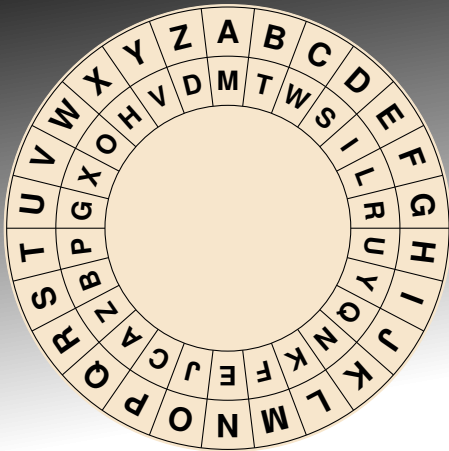
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

D

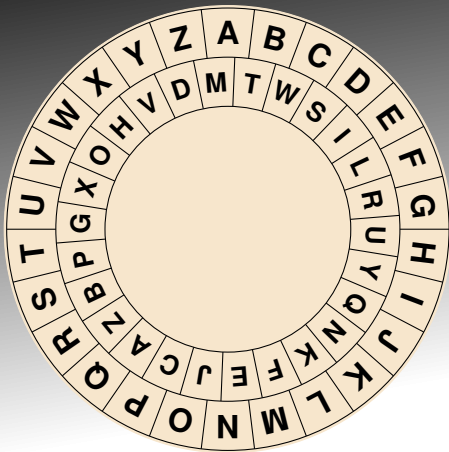
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dc

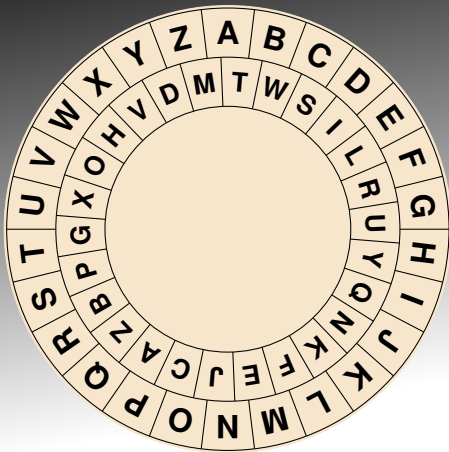
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dc

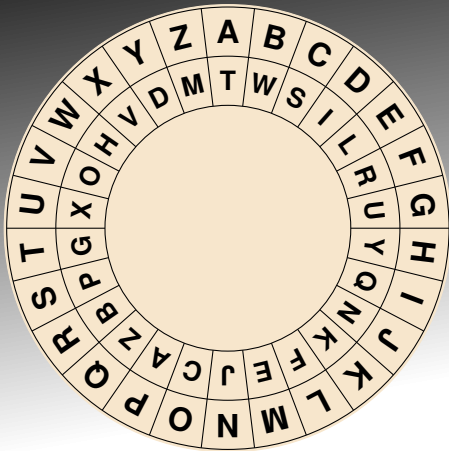
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dc

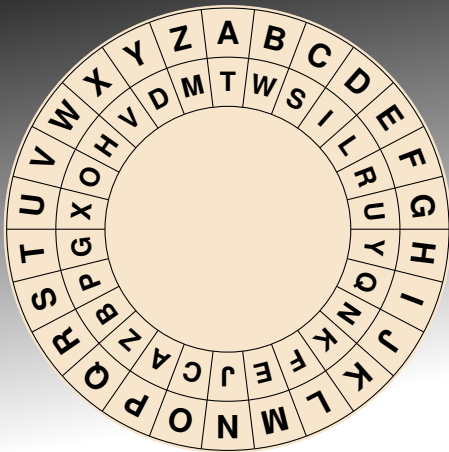
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dc

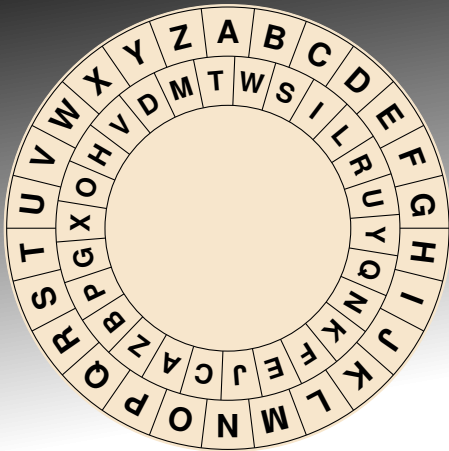
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcr

# Wie funktioniert die Enigma-Verschlüsselung?

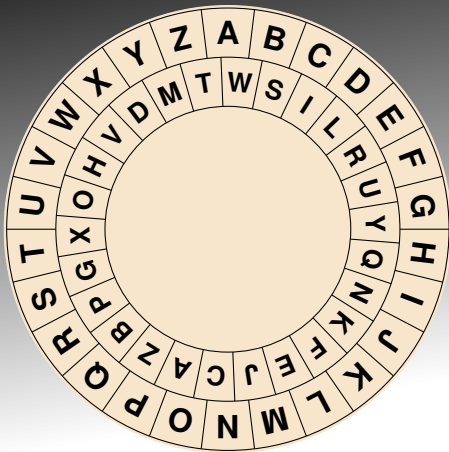


Apfelkuchen

Dcr



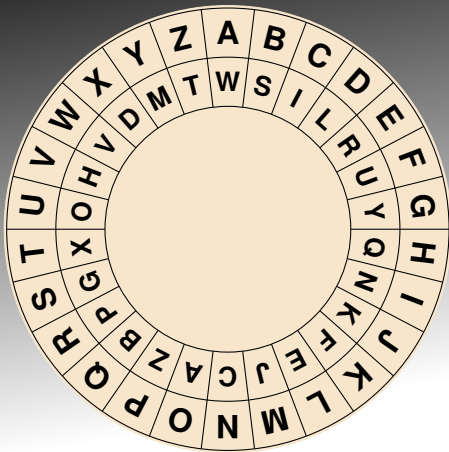
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcr

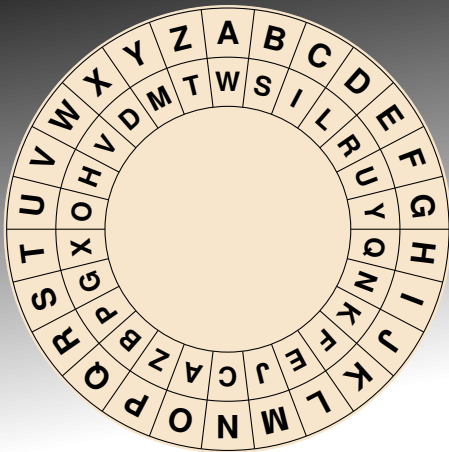
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcr

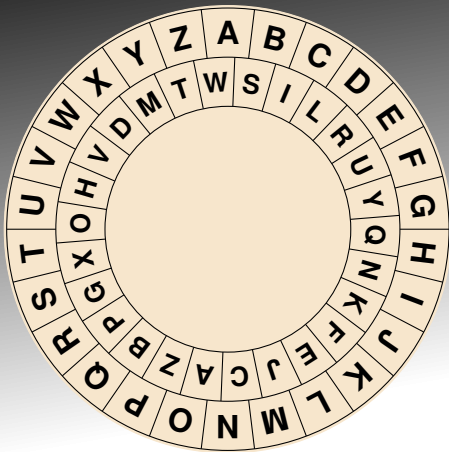
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrr

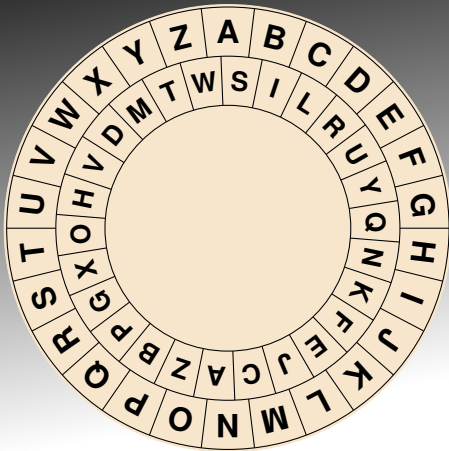
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrr

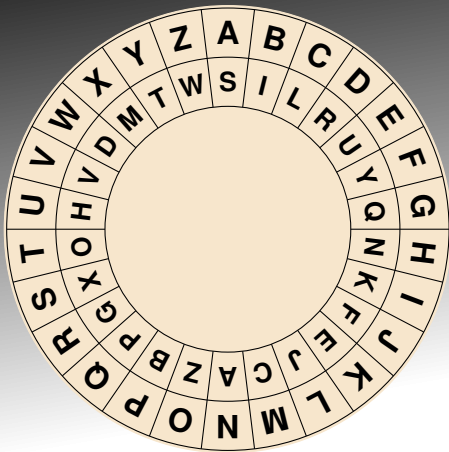
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrr

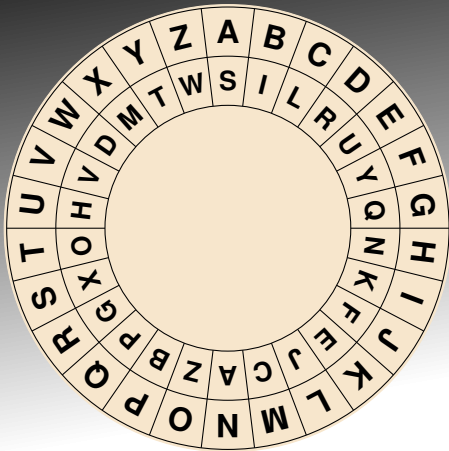
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrr

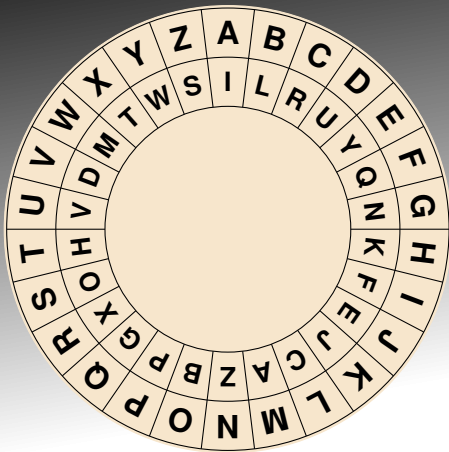
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrrj

# Wie funktioniert die Enigma-Verschlüsselung?

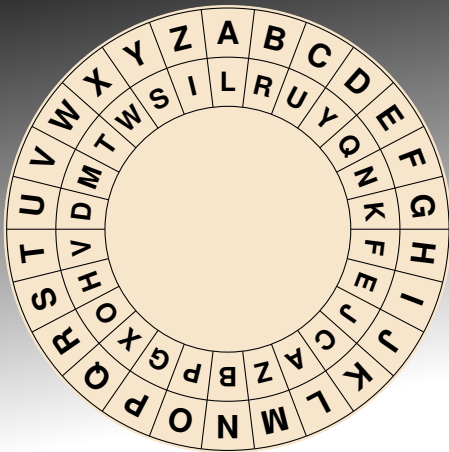


Apfelkuchen

Dcrrjj



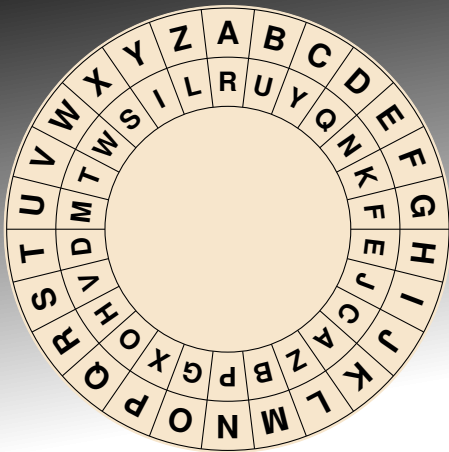
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrrjjd

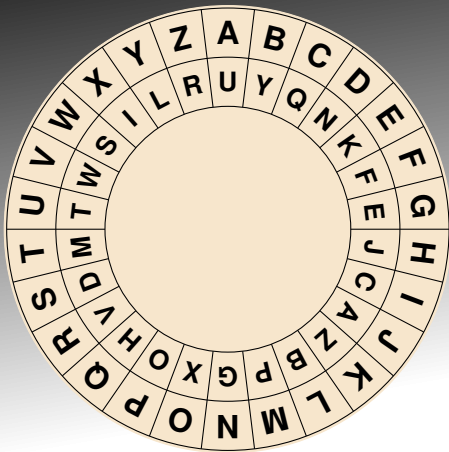
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrrjjdy

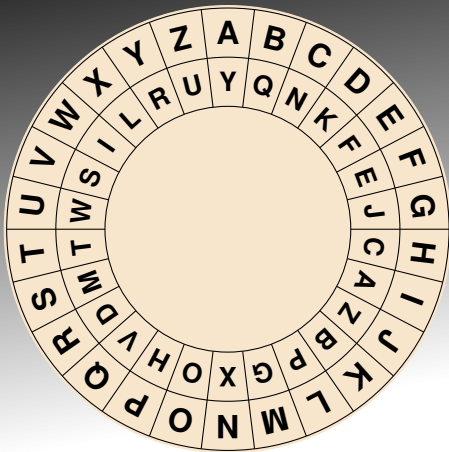
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrrjjdyj

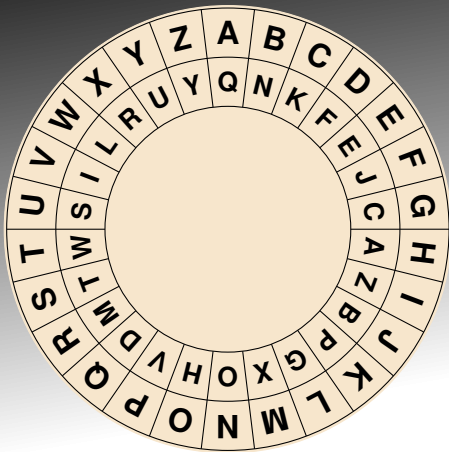
# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

Dcrrjjdyjf

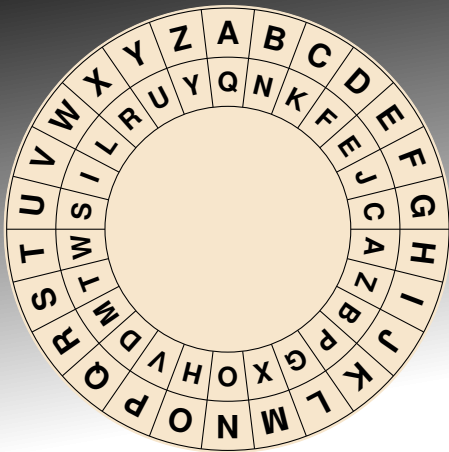
## Wie funktioniert die Enigma-Verschlüsselung?



# Apfelkuchen

Dcrrjjdyjfo

# Wie funktioniert die Enigma-Verschlüsselung?

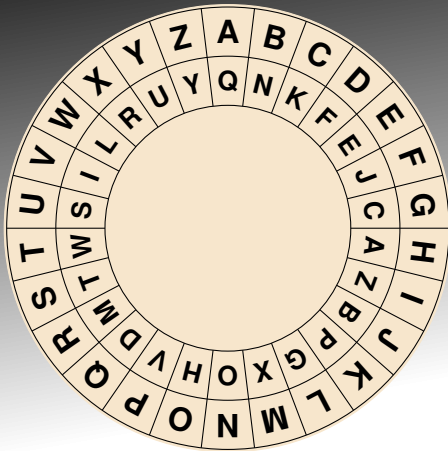


Apfelkuchen

Dcrrjjdyjfo

Rotierende Walze

# Wie funktioniert die Enigma-Verschlüsselung?



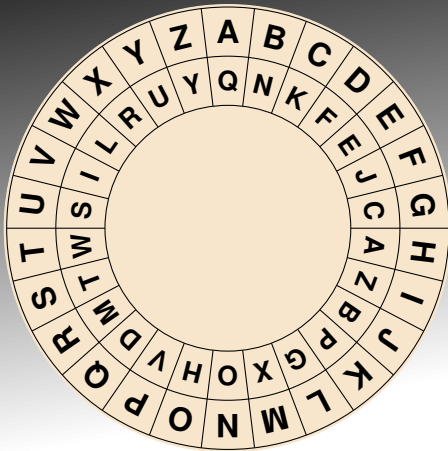
Apfelkuchen

Dcrrjjdyjfo

Rotierende Walze

wiederholt sich nach 1 Umdrehung → **Regelmäßigkeit**

# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

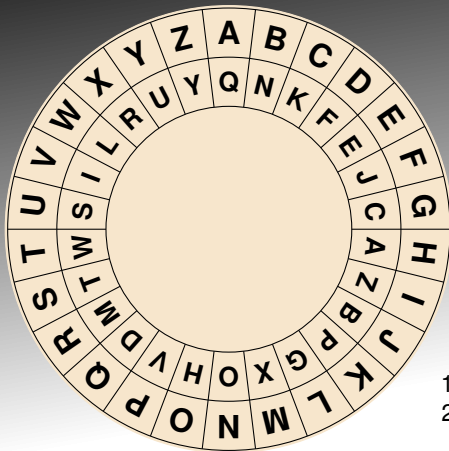
Dcrrjjdyjfo

Rotierende Walze

wiederholt sich nach 1 Umdrehung → ~~Regelmäßigkeit~~  
dann zweite Walze weiterdrehen → wieder unregelmäßig



# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

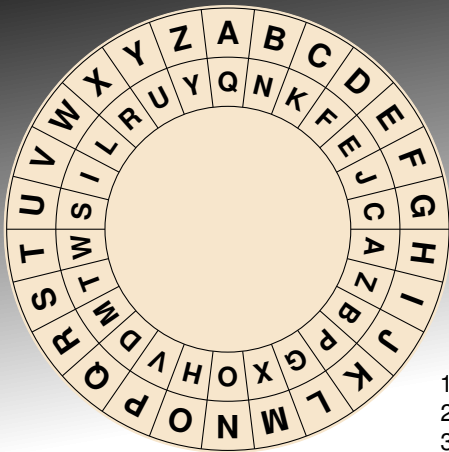
Dcrrjjdyjfo

1. Walze: DMTWSILRUYQNKFEJCAZBPGXOHV
2. Walze: HQZGPJTMOBLNCIFDYAWVEUSRXL

Rotierende Walze

wiederholt sich nach 1 Umdrehung → ~~Regelmäßigkeit~~  
dann zweite Walze weiterdrehen → wieder unregelmäßig

# Wie funktioniert die Enigma-Verschlüsselung?



Apfelkuchen

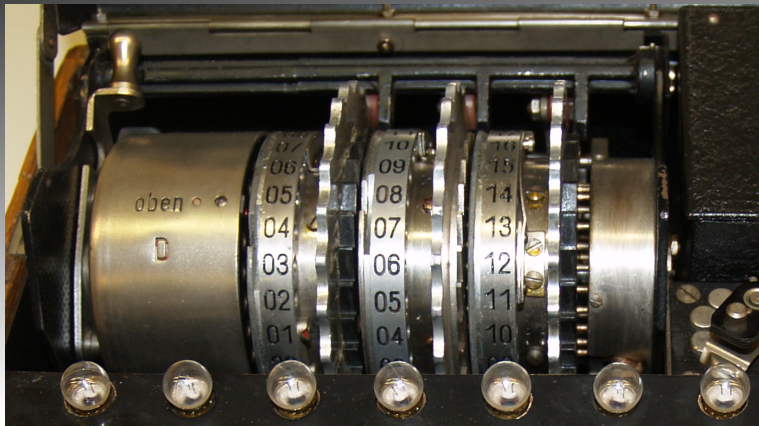
Dcrrjjdyjfo

1. Walze: DMTWSILRUYQNKFEJCAZBPGXOHV
2. Walze: HQZGPJTMOBLNCIFDYAWVEUSRXL
3. Walze: UQNTLSZFMREHDPLKIBVYGJCWGA

Rotierende Walze

wiederholt sich nach 1 Umdrehung → ~~Regelmäßigkeit~~  
dann zweite Walze weiterdrehen → wieder unregelmäßig

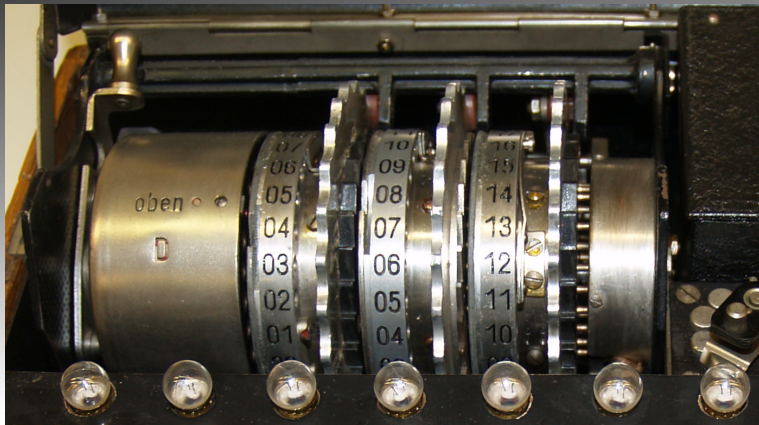
# Wie funktioniert die Enigma-Verschlüsselung?



Enigma: „Kilometerzähler“ aus 3 Walzen

→ wiederholt sich erst nach  $26 \cdot 26 \cdot 26 = 17\,576$  Buchstaben

# Wie funktioniert die Enigma-Verschlüsselung?

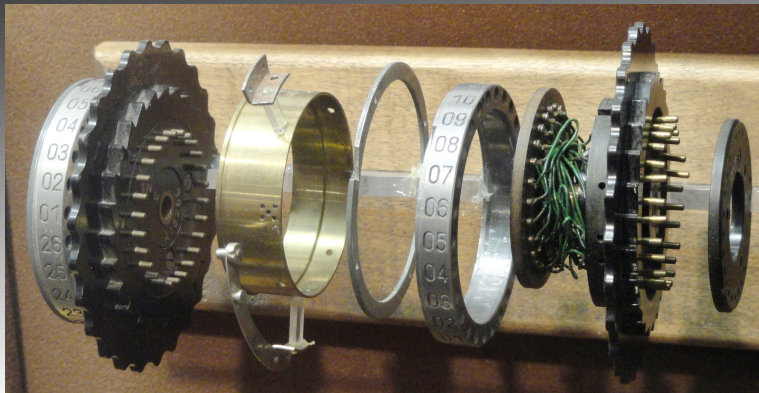


Enigma: „Kilometerzähler“ aus 3 Walzen

→ wiederholt sich erst nach  $26 \cdot 26 \cdot 26 = 17\,576$  Buchstaben

Nachrichten sind kürzer → keine **Regelmäßigkeit** erkennbar

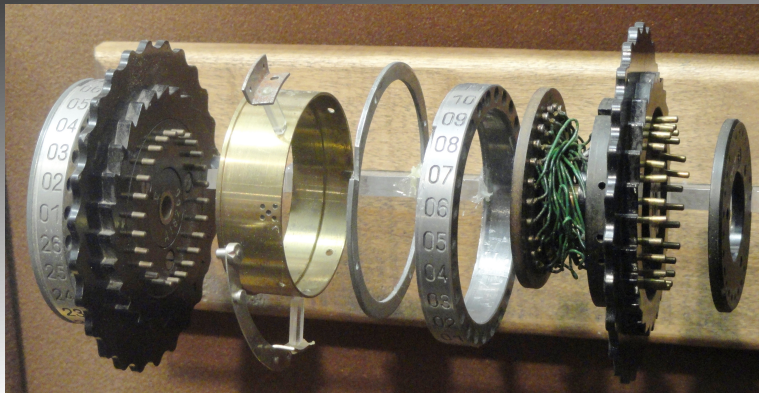
# Wie funktioniert die Enigma-Verschlüsselung?



Walzen im Inneren fest verdrahtet

→ schwer geheimzuhalten

# Wie funktioniert die Enigma-Verschlüsselung?

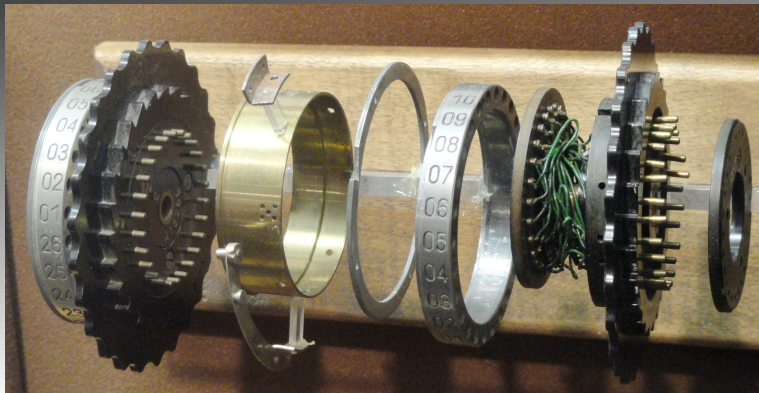


Walzen im Inneren fest verdrahtet

→ schwer geheimzuhalten

→ ... und das ist auch gar nicht nötig!

# Wie funktioniert die Enigma-Verschlüsselung?

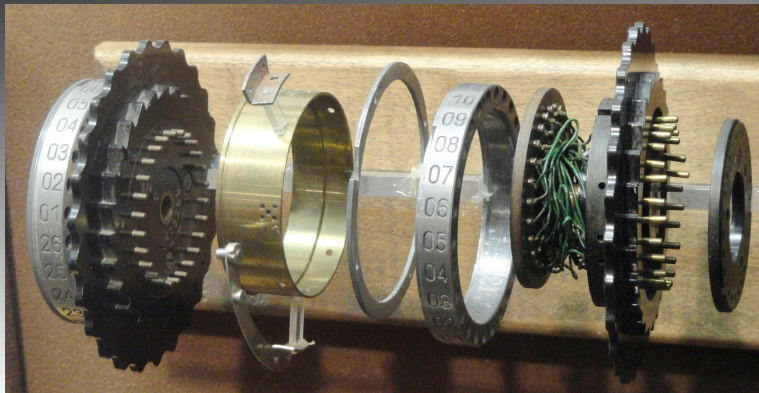


Walzen im Inneren fest verdrahtet

→ schwer geheimzuhalten

→ ... und das ist auch gar nicht nötig ... und darf es auch nicht sein!

# Wie funktioniert die Enigma-Verschlüsselung?

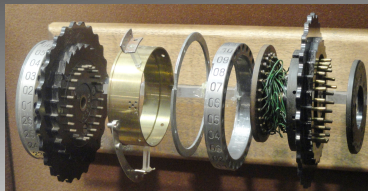
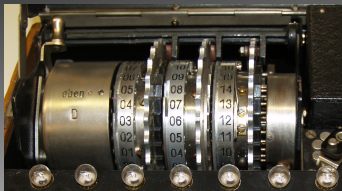


## Kerckhoffs-Prinzip:

schwer zu ändern     $\longrightarrow$     Verfahren     $\longrightarrow$     offenlegen!     $\longrightarrow$     **sicherer**  
leicht zu ändern     $\longrightarrow$     Schlüssel     $\longrightarrow$     geheim halten!



# Wie funktioniert die Enigma-Verschlüsselung?



- **Walzenlage**

3 von 5 Walzen auswählen, beliebig anordnen

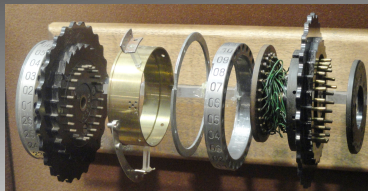
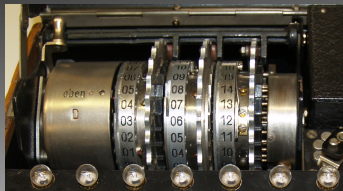
→  $5 \cdot 4 \cdot 3 = 60$  Möglichkeiten

- **Walzenstellung**

Anfangsstellungen der Walzen

→  $26 \cdot 26 \cdot 26 = 17\,576$  Möglichkeiten

# Wie funktioniert die Enigma-Verschlüsselung?

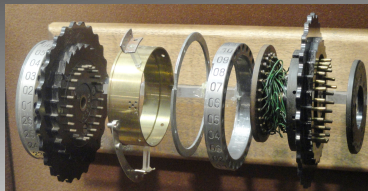
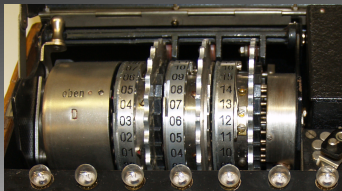


- **Walzenlage**  $\rightarrow 5 \cdot 4 \cdot 3 = 60$
- **Walzenstellung**  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$

Zusätzlich:

- **Ringstellung**  
Innenleben der Walzen verdrehen  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$  Möglichkeiten

# Wie funktioniert die Enigma-Verschlüsselung?

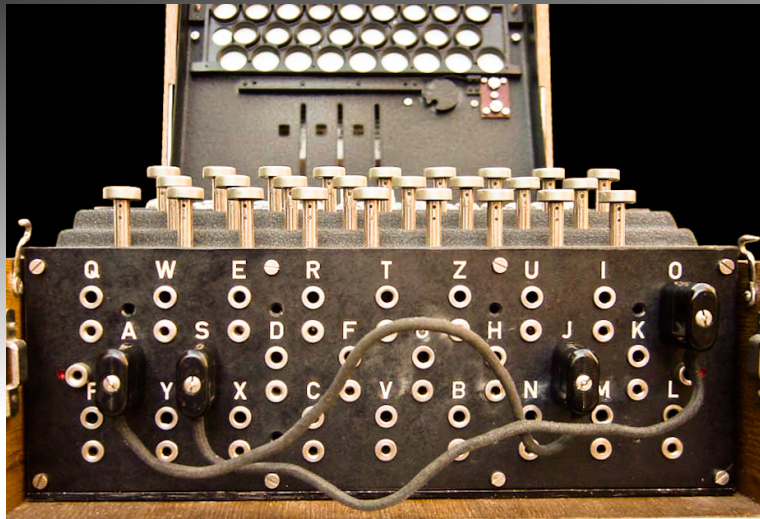


- **Walzenlage**  $\rightarrow 5 \cdot 4 \cdot 3 = 60$
- **Walzenstellung**  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$

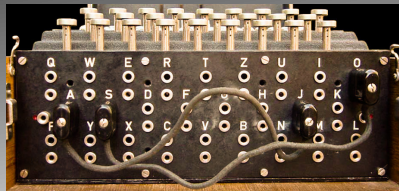
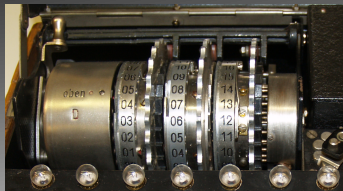
Zusätzlich:

- **Ringstellung**  
Innenleben der Walzen verdrehen  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$  Möglichkeiten
- **Steckerverbindungen**  
Buchstaben miteinander vertauschen, z. B. zehnmal

# Wie funktioniert die Enigma-Verschlüsselung?



# Wie funktioniert die Enigma-Verschlüsselung?



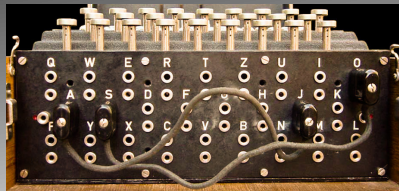
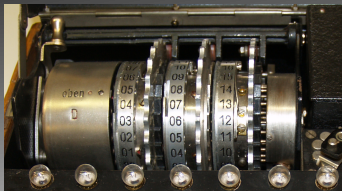
- **Walzenlage**  $\rightarrow 5 \cdot 4 \cdot 3 = 60$
- **Walzenstellung**  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$

Zusätzlich:

- **Ringstellung**  
Innenleben der Walzen verdrehen  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$  Möglichkeiten
- **Steckerverbindungen**  
Buchstaben miteinander vertauschen, z. B. zehnmal

$$\rightarrow \frac{26 \cdot 25}{2} \cdot \frac{24 \cdot 23}{2} \cdot \dots \cdot \frac{8 \cdot 7}{2} = 150\,738\,274\,937\,250 \quad \text{Möglichkeiten}$$

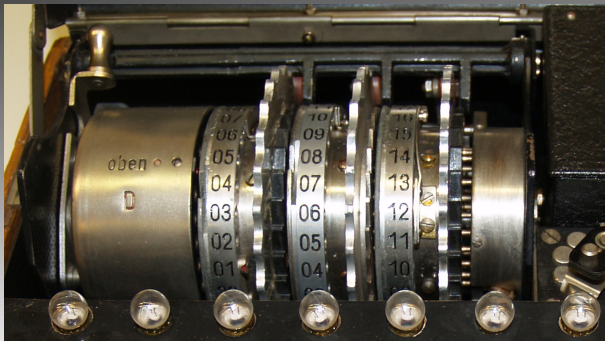
# Wie funktioniert die Enigma-Verschlüsselung?



- **Walzenlage**  $\rightarrow 5 \cdot 4 \cdot 3 = 60$
- **Walzenstellung**  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$
- **Ringstellung**  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,576$
- **Steckerverbindungen**  $\rightarrow 150\,738\,274\,937\,250$

$\rightarrow$  insgesamt  $60 \cdot 17\,576 \cdot 17\,576 \cdot 150\,738\,274\,937\,250$   
 $= 2\,793\,925\,870\,508\,516\,103\,360\,000$  verschiedene **Schlüssel**

# Wie funktioniert die Enigma-Verschlüsselung?



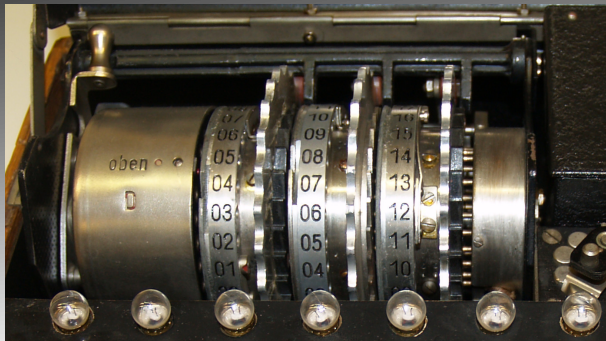
Zusätzlich: **Umkehrwalze**

Buchstaben durcheinanderwürfeln und zurück durch die Walzen schicken

→ A wird X  $\Leftrightarrow$  X wird A → einfacher zu bedienen

→ A wird niemals A, B wird niemals B, ... → noch sicherer

# Wie funktioniert die Enigma-Verschlüsselung?



Zusätzlich: **Umkehrwalze**

Buchstaben durcheinanderwürfeln und zurück durch die Walzen schicken

→ A wird X  $\Leftrightarrow$  X wird A → einfacher zu bedienen

→ A wird niemals A, B wird niemals B, ... → ~~noch sicherer~~

→ **Regelmäßigkeiten!**



# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- **Walzenlage**

$$5 \cdot 4 \cdot 3 = 60$$

- **Walzenstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Ringstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Steckerverbindungen**

$$150\,738\,274\,937\,250$$

→ **insgesamt**

$$2\,793\,925\,870\,508\,516\,103\,360\,000$$

Schlüssel durchprobieren

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- **Walzenlage**

$$5 \cdot 4 \cdot 3 = 60$$

- **Walzenstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Ringstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Steckerverbindungen**

$$150\,738\,274\,937\,250$$

—→ **insgesamt**

2 793 925 870 508 516 103 360 000

Schlüssel durchprobieren

—→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

Geheime Kommandosache!

Jede einzelne Tageschlüssel ist geheim.

Mitarbeiter 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	Wellenlage			Ringstellung	S t e c h e r v e r b i n d u n g e n										Kenngruppen			
					an der Umkehrmarke													
					nim Streicherblatt													
					1	2	3	4	5	6	7	8	9	10				
649	31	I	V	III	14 09 24	KM AX PZ GO DI CN BR PV LT EQ HS UW	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny dgy	ekb rze
649	30	IV	III	II	05 26 02		IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	kti acw	zsi wao
649	29	III	II	I	12 24 03		DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc acn	ovw vwd
649	28	II	III	V	06 08 16		CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrp cld	ude rzh
649	27	III	I	IV	11 03 07		DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj fbb	vct uis
649	26	I	IV	V	17 22 19	IU AS DV GL PT OX EZ CH MR KN BQ PW	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 tlg
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		PJ	ES	IM	RX	LV	AY	OU	BO	WZ	CN	jqc acx	mwe wve
649	21	I	V	II	13 05 19	AI BT MV HU FW EL DG KN RZ OQ CP SX	RU	HL	PY	OS	GZ	DM	AW	GE	TV	NX	jpw del	mwf wvf
649	20	III	IV	V	24 01 10		DP	MO	QZ	AU	RY	SV	JL	OX	BE	TW	jqd cef	nvo ysh
649	19	V	III	I	17 25 20		OX	PR	PH	WY	DL	CM	AE	TZ	J5	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	vcl rxn
649	17	I	IV	II	21 10 06		IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae hzi	sog ysi
649	16	V	II	III	08 16 13	IL AF EU HO QT WZ KV OM BF NR DX CS	HM	JO	DI	NR	BY	XZ	OS	PU	PQ	CT	tdp ddb	fkg uiv
649	15	II	IV	I	01 03 07		DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw hzj	sch wvg
649	14	IV	I	V	15 11 05		GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz noa	tjv xtk
649	13	I	III	II	13 20 03		LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgz	tjo ryg
649	12	V	I	IV	18 10 07		MU	BP	CY	RZ	KX	AN	TI	DG	IL	PW	zdy rkf	tjw xtl
649	11	II	IV	III	02 26 15	IL AF EU HO QT WZ KV OM BF NR DX CS	KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	zea rjy	soi wvh
649	10	III	V	IV	23 21 01		LR	IK	MS	QU	HW	PT	OO	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 AF EU HO QT WZ KV OM BF NR DX CS	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao cft	zsk wbj
649	5	V	II	IV	23 02 25		MV	CL	OK	OQ	BI	PU	HS	PX	NW	EY	lju cdr	iye waj
649	4	II	IV	I	04 21 09		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	EO	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	

Geheime Kommandosache!

Jede einzelne Tageschlüssel ist geheim.

Mitarbeiter im Flugzeug verboten!

Nr. 00190

## Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Mess- tag	Walzenlage				Ringstellung	S t e c k e r v e r b i n d u n g e n										Kenngruppen						
						an der Umkehrmole		am Streichenbrett														
								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	ekb	rzg
649	30	IV	III	II	05	26 02			IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	kti	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
649	28	II	III	V	06	08 16	DI	CN	BR	PV			CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ
649	27	III	I	IV	11	03 07	LT	EQ	HS	UW			DY	IN	BV	GR	AM	LO	PP	HT	EX	UW
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

Walzenlage, Ringstellung, Steckerverbindungen: täglich festgelegt

649	22	II	IV	V	01	09 21	IO	AS	DV	UL			RU	HL	PY	OS	GZ	DM	AW	GE	TV	NX	jpw	del	mwf	wvf
649	21	I	V	II	13	05 19	PT	OX	EZ	CH			DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	Jqd	cef	nvo	ysh
649	20	III	IV	V	24	01 10	MR	KN	BQ	PW			EX	PR	PH	WY	DL	CM	AE	TZ	J5	GI	idf	fpz	jwg	tlg
649	19	V	III	I	17	25 20			OJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD					lsa	gbw	vcj	rxn
649	18	IV	II	V	15	23 26			EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD					mae	hzi	sog	ysi
649	17	I	IV	II	21	10 06			IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU					tdp	dhb	fkg	uiv
649	16	V	II	III	08	16 13			HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT					ldw	hzj	sch	wvg
649	15	II	IV	I	01	03 07			DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT					imz	noa	tjv	xtk
649	14	IV	I	V	15	11 05	AI	BT	MV	HU			GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV				
649	13	I	III	II	13	20 03	PW	EL	DG	KN			LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgz	tjw	ryg
649	12	V	I	IV	18	10 07	RZ	OQ	CP	SX			MU	BP	CY	RZ	KX	AN	TI	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	OO	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			DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY					lao	cft	zsk	wbj
649	5	V	II	IV	23	02 25	IL	AF	EU	HO			MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
649	4	II	IV	I	04	21 09	QT	WZ	KV	OM			AC	BL	OZ	EK	QW	OP	SO	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	EO	PY	KQ	CP	OS	JW	AI	VZ					aqd	bdy	iyf	xta
649	1	II	I	III	23	12 10			DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO					kgl	cdf	giq	wuv

Geheime Kommandosache!

Jede einzelne Tageschlüssel ist geheim.

Mitarbeiter im Flugzeug verboten!

Nr. 00190

## Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Mess- tag	Walzenlage				Ringstellung	Steckerverbindungen										Kerngruppen							
						an der Umkehrmole	am Sticherbrett																
										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	ekb rzg	
649	30	IV	III	II	05	26	02			IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi wao	
649	29	III	II	I	12	24	03	KM	AX	PZ	GO			DJ	AT	CV	IO	ER	QS	LW	PZ	FN BH	
649	28	II	III	V	06	08	16	DI	CN	BR	PV			CR	FV	AI	DK	OT	MQ	EU	BX	LP GJ	
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW			DY	IN	BV	GR	AM	LO	PP	HT	EX UW	
649	26	I	IV	V	17	22	19							VZ	AL	RT	KO	CG	EI	BJ	DU	FS HP	
649	25	IV	III	I	08	25	12							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ CW	

Walzenlage, Ringstellung, Steckerverbindungen: täglich festgelegt

649	22	II	IV	V	01	09	21	IO	AS	DV	UL			RU	HL	PY	OS	GZ	DM	AW	GE	TV	NX	jpw del	mwf wvf
649	21	I	V	II	13	05	19	PT	OX	EZ	CH			MU	HL	PY	OS	GZ	DM	AW	GE	TV	NX	jpw del	mwf wvf
649	20	III	IV	V	24	01	10	UP	KN	BO	PW			DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jpd cef	nvo ysh
649	19	V																							
649	18	IV																							
649	17	I	IV	I	21	10	00							HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	tdp ddb	fkf uiv
649	16	V	II	III	08	16	13							DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw hzj	sch wvg
649	15	II	IV	I	01	03	07							GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz noa	tjv xtk
649	14	IV	I	V	15	11	05	AI	BT	MV	HU			LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgz	tjw ryg
649	13	I	III	II	13	20	03	PW	EL	DG	KN			LU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	zdy rkf	tdjv xtl
649	12	V	I	IV	18	10	07	RZ	OQ	CP	SX			KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV	zea rjy	soi wvh
649	11	II	IV	III	02	26	15							LR	IK	MS	QU	HW	PT	OO	VX	PZ	EN	lrc zbx	vbm rxh
649	10	III	V	IV	23	21	01							QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj eyr	vby tlh
649	9	V	I	III	16	04	08							FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz dha	ekc tli
649	8	IV	II	V	13	19	25							UX	IZ	HN	BK	OQ	CP	FT	JY	MW	AR	lan dgb	zsj wbi
649	7	I	IV	II	09	03	22							DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao cft	zsk wbj
649	6	III	I	V	11	18	14	IL	AF	EU	HO			MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	lju cdr	iye waj
649	5	V	II	IV	23	02	25	QT	WZ	KV	OM			AC	BL	OZ	EK	QW	OP	SO	DH	JM	TX	lsb zby	vcy ujb
649	4	II	IV	I	04	21	09	BF	NR	DX	CS			BR	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap owd	iwu wak
649	3	V	I	II	19	11	06							KN	HU	EO	PY	KQ	CP	OS	JW	AI	VZ	aqd bdy	iyf xtd
649	2	IV	V	I	16	14	02							DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl cdf	giq wuv
649	1	II	I	III	23	12	10																		

Walzenstellung: für jeden Spruch neu, mitschicken

## Wie konnte die Enigma-Verschlüsselung gebrochen werden?

Catharina Koonen-Andersson

Joh. "Christa" Lagerlöf 1848-96

Elin v. den Baryen 1877-96

Nr. 00150

Eufonia-Majchinen - Schijfel Nr. 649

Achtung! Die Majchinen dürfen nicht umgewandelt in andere Modelle werden. Bei jeder dieser Majchinen sind folgende umzusetzen:

		Wahlregeln	Ausführung	an der Maschine	an der Maschine	Kannengrößen
649	30	I	V	III	14 25 24	55 11 WV 48 128
649	30	II	III	II	15 20 20	15 11 WV 48 128
649	30	III	II	I	15 20 20	15 11 WV 48 128
649	30	IV	I	IV	15 20 20	15 11 WV 48 128
649	30	V	I	IV	15 20 20	15 11 WV 48 128
649	30	VI	I	IV	15 20 20	15 11 WV 48 128
649	30	VII	I	IV	15 20 20	15 11 WV 48 128
649	30	VIII	I	IV	15 20 20	15 11 WV 48 128
649	30	IX	I	IV	15 20 20	15 11 WV 48 128
649	30	X	I	IV	15 20 20	15 11 WV 48 128
649	30	XI	I	IV	15 20 20	15 11 WV 48 128
649	30	XII	I	IV	15 20 20	15 11 WV 48 128
649	30	XIII	I	IV	15 20 20	15 11 WV 48 128
649	30	XIV	I	IV	15 20 20	15 11 WV 48 128
649	30	XV	I	IV	15 20 20	15 11 WV 48 128
649	30	XVI	I	IV	15 20 20	15 11 WV 48 128
649	30	XVII	I	IV	15 20 20	15 11 WV 48 128
649	30	XVIII	I	IV	15 20 20	15 11 WV 48 128
649	30	XIX	I	IV	15 20 20	15 11 WV 48 128
649	30	XX	I	IV	15 20 20	15 11 WV 48 128
649	30	XXI	I	IV	15 20 20	15 11 WV 48 128
649	30	XXII	I	IV	15 20 20	15 11 WV 48 128
649	30	XXIII	I	IV	15 20 20	15 11 WV 48 128
649	30	XXIV	I	IV	15 20 20	15 11 WV 48 128
649	30	XXV	I	IV	15 20 20	15 11 WV 48 128
649	30	XXVI	I	IV	15 20 20	15 11 WV 48 128
649	30	XXVII	I	IV	15 20 20	15 11 WV 48 128
649	30	XXVIII	I	IV	15 20 20	15 11 WV 48 128
649	30	XXIX	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649	30	XL	I	IV	15 20 20	15 11 WV 48 128
649						

## Walzenlage, Ringstellung und Steckerverbindungen festgelegt

## Walzenstellung mitschicken

- Funkverbindung störanfällig  
→ zweimal senden
- zur Sicherheit: verschlüsseln
- ? erst verschlüsseln, dann verdoppeln?
- ? erst verdoppeln, dann verschlüsseln?

## Wie konnte die Enigma-Verschlüsselung gebrochen werden?

[illegible]

## Walzenlage, Ringstellung und Steckerverbindungen festgelegt

## Walzenstellung mitschicken

- Funkverbindung störanfällig  
→ zweimal senden
- zur Sicherheit: verschlüsseln
- ? ~~erst verschlüsseln, dann verdoppeln?~~

! erst verdoppeln, dann verschlüsseln

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

Gebühren-Kennzeichenschein Nr. 00190

Ich, Ernst Kersch, habe einmal (einmalig & getrennt) hier (in Bayern) verkauft

**Luftwaffen-Maschinen-Schlüssel Nr. 649**

**Achtung!** Jeder Empfänger dieses Briefes wird verpflichtet in Betreff des Verkaufs des Luftwaffen-Schlüssels die folgenden Vorschriften zu befolgen:

T	Wortstellung	Ausgangslage	an die Buchstaben													an die Zahlen													Buchstaben
			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	
040	1	V	10	14	05	24																							
040	10	IV	III	I	05	20	40																						
040	20	III	I	I	02	25	40																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						
040	20	III	II	V	05	22	10																						



# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

Gebühren-Kennzeichenschein Nr. 00190

Ich, Ernst Kerschbaum, habe einmal (einmalig & selten) hier (in Bayern) geboren.

**Luftwaffen-Maschinen-Schlüssel Nr. 649**

**Achtung!** Jede falsche Buchstabe wird verwandelt in einen anderen Buchstaben. Die Tabelle enthält die Zuordnung.

Wortstellung	Abbildung	an die Buchstaben	an Buchstaben	Zuordnung
040 1	V	04	04	24
040 2	V	04	04	24
040 3	V	04	04	24
040 4	V	04	04	24
040 5	V	04	04	24
040 6	V	04	04	24
040 7	V	04	04	24
040 8	V	04	04	24
040 9	V	04	04	24
040 10	V	04	04	24
040 11	V	04	04	24
040 12	V	04	04	24
040 13	V	04	04	24
040 14	V	04	04	24
040 15	V	04	04	24
040 16	V	04	04	24
040 17	V	04	04	24
040 18	V	04	04	24
040 19	V	04	04	24
040 20	V	04	04	24
040 21	V	04	04	24
040 22	V	04	04	24
040 23	V	04	04	24
040 24	V	04	04	24
040 25	V	04	04	24
040 26	V	04	04	24
040 27	V	04	04	24
040 28	V	04	04	24
040 29	V	04	04	24
040 30	V	04	04	24
040 31	V	04	04	24
040 32	V	04	04	24
040 33	V	04	04	24
040 34	V	04	04	24
040 35	V	04	04	24
040 36	V	04	04	24
040 37	V	04	04	24
040 38	V	04	04	24
040 39	V	04	04	24
040 40	V	04	04	24
040 41	V	04	04	24
040 42	V	04	04	24
040 43	V	04	04	24
040 44	V	04	04	24
040 45	V	04	04	24
040 46	V	04	04	24
040 47	V	04	04	24
040 48	V	04	04	24
040 49	V	04	04	24
040 50	V	04	04	24
040 51	V	04	04	24
040 52	V	04	04	24
040 53	V	04	04	24
040 54	V	04	04	24
040 55	V	04	04	24
040 56	V	04	04	24
040 57	V	04	04	24
040 58	V	04	04	24
040 59	V	04	04	24
040 60	V	04	04	24
040 61	V	04	04	24
040 62	V	04	04	24
040 63	V	04	04	24
040 64	V	04	04	24
040 65	V	04	04	24
040 66	V	04	04	24
040 67	V	04	04	24
040 68	V	04	04	24
040 69	V	04	04	24
040 70	V	04	04	24
040 71	V	04	04	24
040 72	V	04	04	24
040 73	V	04	04	24
040 74	V	04	04	24
040 75	V	04	04	24
040 76	V	04	04	24
040 77	V	04	04	24
040 78	V	04	04	24
040 79	V	04	04	24
040 80	V	04	04	24
040 81	V	04	04	24
040 82	V	04	04	24
040 83	V	04	04	24
040 84	V	04	04	24
040 85	V	04	04	24
040 86	V	04	04	24
040 87	V	04	04	24
040 88	V	04	04	24
040 89	V	04	04	24
040 90	V	04	04	24
040 91	V	04	04	24
040 92	V	04	04	24
040 93	V	04	04	24
040 94	V	04	04	24
040 95	V	04	04	24
040 96	V	04	04	24
040 97	V	04	04	24
040 98	V	04	04	24
040 99	V	04	04	24
040 100	V	04	04	24

Walzenlage, Ringstellung und Steckerverbindungen festgelegt

Walzenstellung mitschicken

- Funkverbindung störanfällig  
→ zweimal senden
- zur Sicherheit: verschlüsseln  
~~? erst verschlüsseln, dann verdoppeln?~~

! erst verdoppeln, dann verschlüsseln

→ zwei verschiedene Verschlüsselungen **derselben** drei Buchstaben  
außerdem: A wird X ⇔ X wird A → einfacher zu bedienen

Regelmäßigkeiten

## Wie konnte die Enigma-Verschlüsselung gebrochen werden?

Catharina Kornemannsdatter

Sole christa laus (1848) 6 phoen

Einer u im Bappten nehm?

Nr. 00150

Lufthafen-Mathiesen - Schiffler Nr. 649

Achtung: Schiffler'sche Dichte ist unvollständig in Buchstabenfolge. Die Buchstaben sind in Schiffler'scher Dichte

		Wahrzeichen	Buchstaben	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihenfolge	in der Reihen
--	--	-------------	------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	--------------------	---------------

## Walzenlage, Ringstellung und Steckerverbindungen festgelegt

## Walzenstellung mitschicken

- Funkverbindung störanfällig  
→ zweimal senden
- zur Sicherheit: verschlüsseln

~~? erst verschlüsseln, dann verdoppeln?~~

! erst verdoppeln, dann verschlüsseln

→ zwei verschiedene Verschlüsselungen **derselben** drei Buchstaben  
außerdem: A wird X  $\Leftrightarrow$  X wird A → einfacher zu bedienen

## Regelmäßigkeiten

→ Verdrahtung unbekannter Walzen berechnen

→ Walzenlage und Walzenstellung durchprobieren, ohne Ringstellung und Steckerverbindungen kennen zu müssen

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- **Walzenlage**

$$5 \cdot 4 \cdot 3 = 60$$

- **Walzenstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Ringstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Steckerverbindungen**

$$150\,738\,274\,937\,250$$

—→ **insgesamt**

2 793 925 870 508 516 103 360 000

Schlüssel durchprobieren

—→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- **Walzenlage**

$$5 \cdot 4 \cdot 3 = 60$$

- **Walzenstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Ringstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Steckerverbindungen**

~~150 738 274 937 250~~

—→ **insgesamt**

2 793 925 870 508 516 103 360 000

Schlüssel durchprobieren

—→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- **Walzenlage**

$$5 \cdot 4 \cdot 3 = 60$$

- **Walzenstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Ringstellung**

$$26 \cdot 26 \cdot 26 = 17\,576$$

- **Steckerverbindungen**

~~150 738 274 937 250~~

→ **insgesamt**

~~2 793 925 870 508 516 103 360 000~~

**18 534 946 560** Schlüssel durchprobieren

→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- Walzenlage

$$5 \cdot 4 \cdot 3 = 60$$

- Walzenstellung

$$26 \cdot 26 \cdot 26 = 17\,576$$

- Ringstellung

~~$$26 \cdot 26 \cdot 26 = 17\,576$$~~

- Steckerverbindungen

~~$$150\,738\,274\,937\,250$$~~

→ insgesamt

~~$$2\,793\,925\,870\,508\,516\,103\,360\,000$$~~  
$$1\,054\,560 \text{ Schlüssel durchprobieren}$$

→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

- Walzenlage

$$5 \cdot 4 \cdot 3 = 60$$

- Walzenstellung

$$26 \cdot 25 \cdot 26 = 16\,900$$

- Ringstellung

~~$$26 \cdot 26 \cdot 26 = 17\,576$$~~

- Steckerverbindungen

~~$$150\,738\,274\,937\,250$$~~

→ insgesamt

~~$$2\,793\,925\,870\,508\,516\,103\,360\,000$$~~  
$$1\,014\,000 \text{ Schlüssel durchprobieren}$$

→ stattdessen:

**Regelmäßigkeiten** ausnutzen!



Marian Rejewski (1905–1980)

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

1939/40: Wegfall der Spruchschlüsselverdopplung  
Gibt es weitere Regelmäßigkeiten?



# Wie konnte die Enigma-Verschlüsselung gebrochen werden?

1939/40: Wegfall der Spruchschlüsselverdopplung  
Gibt es weitere Regelmäßigkeiten?

A wird niemals A, B wird niemals B, ...  
→ noch sicherer

# Wie konnte die Enigma-Verschlüsselung gebrochen werden?



Alan Turing (1912–1954)

1939/40: Wegfall der Spruchschlüsselverdopplung  
Gibt es weitere Regelmäßigkeiten?

A wird niemals A, B wird niemals B, ...

→ ~~noch sicherer~~

→ **Regelmäßigkeit!**

BHNCXSEQKOBIIODWFBTZGCEYHQJJEWYOYNBDXHQBALHTSSDPGW

1 OBERKOMMANDODERWEHRMA**C**H**T**

2 OBERKOMMANDODERWEHRMA**C**H**T**

3 OBERKOMMANDO**D**ERWEHRMA**C**H**T**

4 OBERKOMMANDODERWEHRMA**C**H**T**

5 OBE**R**KOMMAN**D**ODERWEHRMA**C**H**T**

6 OBERKOMMANDODERWEHRMA**C**H**T**

7 OBERKOMMANDODERWEHRMA**C**H**T**

8 OBERKOMMANDODERWE**H**HRMA**C**H**T**

9 OBERK**O**MMANDODERWEHRMA**C**H**T**

10 OBE**R**KOMMANDODERWEHRMA**C**H**T**

11 OBERKOMMANDOD**E**RWEHRMA**C**H**T**

12 OBERKOMMANDODERWEHRMA**C**H**T**

13 OBERKOMMANDODERWE**H**HRMA**C**H**T**

14 OBERKOMMANDODERWEHRMA**C**H**T**

15 OBERKOMMANDODERWEHRMA**C**H**T**

16 OBERKOMMANDOD**E**RWEHRMA**C**H**T**

17 OBE**R**KOMMANDODERWEHRMA**C**H**T**

18 OBERKOMMANDODERWEHRMA**C**H**T**

19 OBERKOMMANDODERWEHRMA**C**H**T**

20 OBERKOMMANDO**D**ERWEHRMA**C**H**T**

21 OBERKOMMANDODERWEHRMA**C**H**T**

22 OBE**R**KOMMANDODERWEHRMA**C**H**T**

23 OBERKOMMANDO**D**ERWEHRMA**C**H**T**

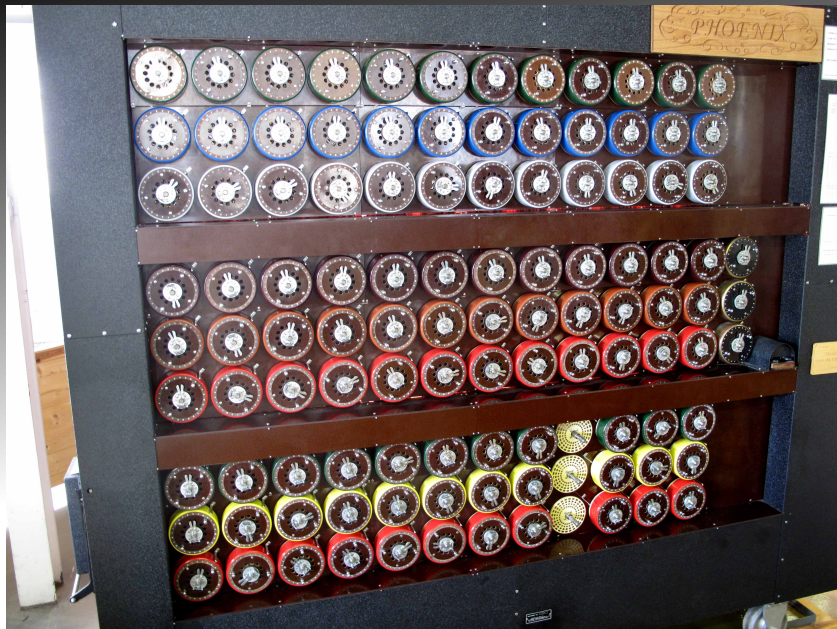
24 OBERKOMMAN**D**ODERWEHRMA**C**H**T**

25 OBERKOMMAN**D**ODERWE**H**HRMA**C**H**T**

26 OBERK**O**MMANDODERWEHRMA**C**H**T**

27 OBE**R**KOMMANDODERWEHRMA**C**H**T**

BHNCXSEQKOBIIODWFBTZGCEYHQJJEWYOYNBDXHQBALHTSSDPGW



# Wie konnte die Enigma-Verschlüsselung gebrochen werden?



Alan Turing (1912–1954)



Turing-Bombe (Nachbau)

- alle 1 014 000 Schlüssels durchprobieren
- Rechenzeit: 10 h
- 60 Turing-Bomben gleichzeitig: 10 min

# verschlüsselt entschlüsselt

– wie es geht  
und wie man es selber macht



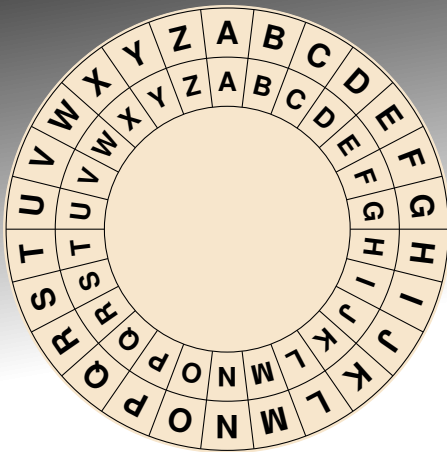
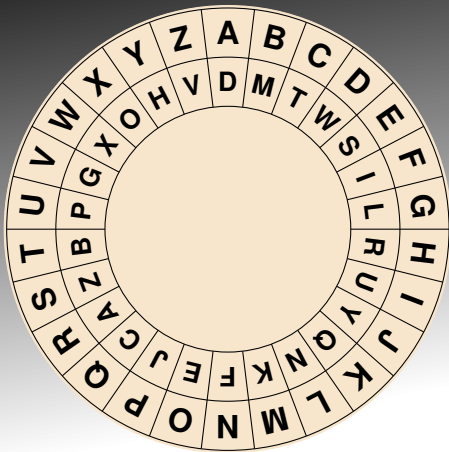
Hochschule Bochum  
Bochum University  
of Applied Sciences



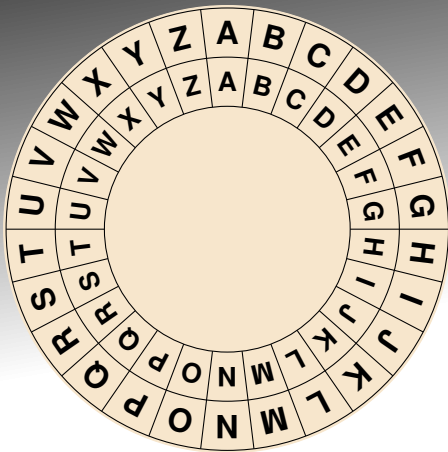
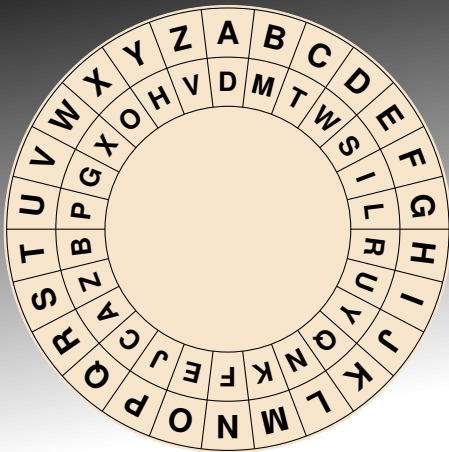
Campus  
Velbert/Heiligenhaus

- ✓ Wie funktioniert die Enigma-Verschlüsselung?
- ✓ Wie konnte die Enigma-Verschlüsselung gebrochen werden?
  - Pause –
- Wie verschlüsselt man heute?

# Wie verschlüsselt man heute?



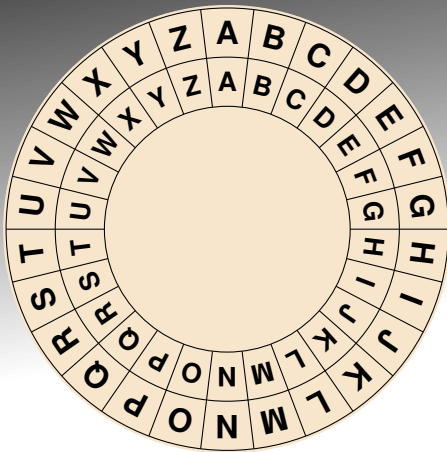
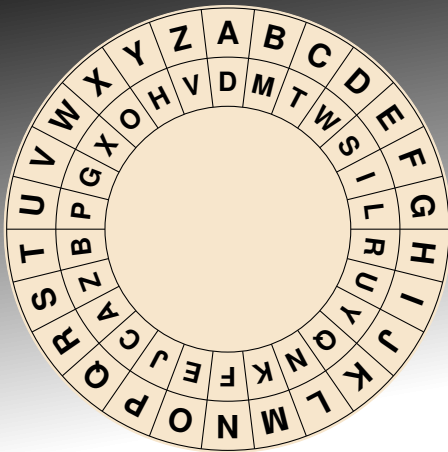
# Wie verschlüsselt man heute?



Computer

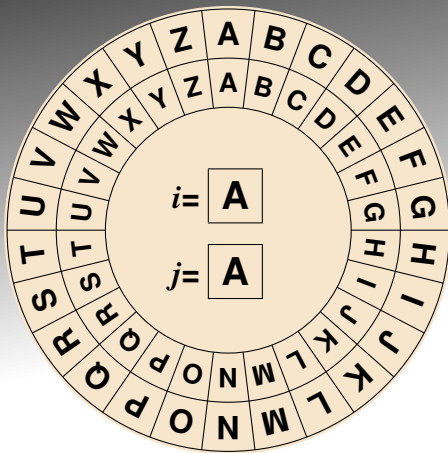
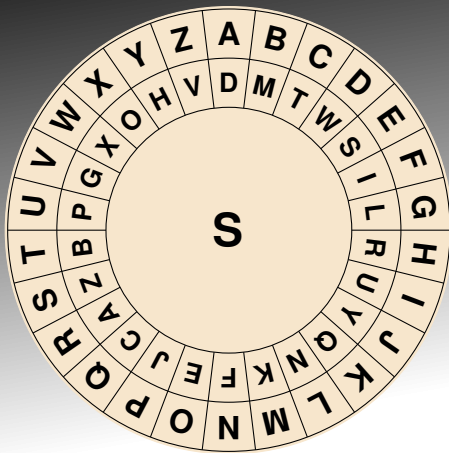


# Wie verschlüsselt man heute?



- Computer:
- rechnet extrem schnell
  - kann „Walze“ auch „umverdrahten“
  - behält immer den Überblick

# Wie verschlüsselt man heute?

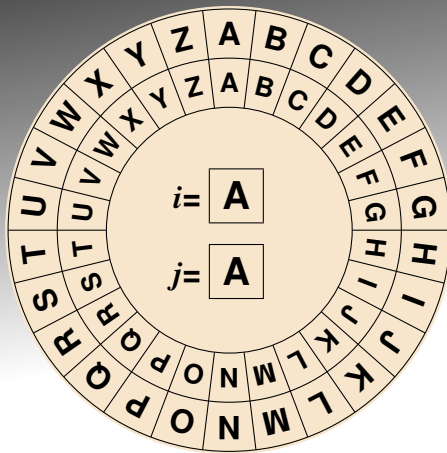
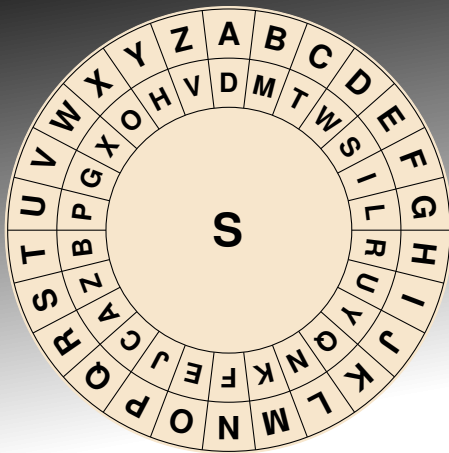


## RC4

- 2 Zähler:  $i$  und  $j$
- Hauptwalze  $S$
- Hilfswalze: Zähler „erhöhen“

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?

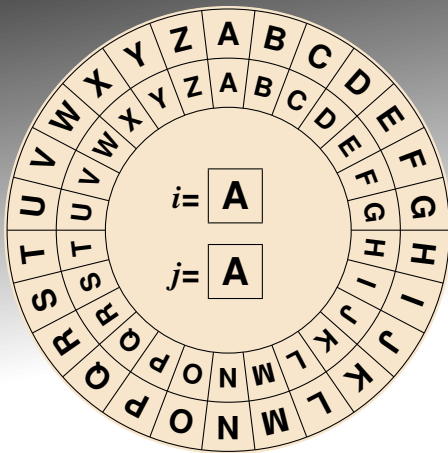
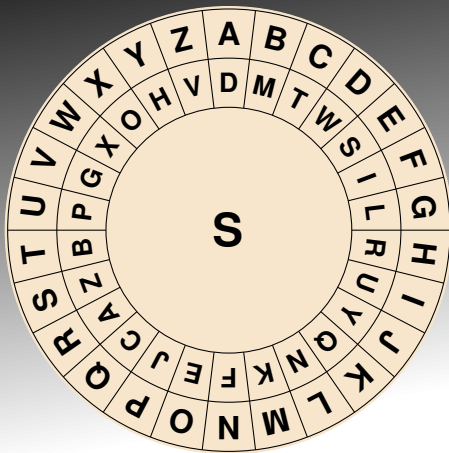


RC4

- Beispiel: erhöhe B um G

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?

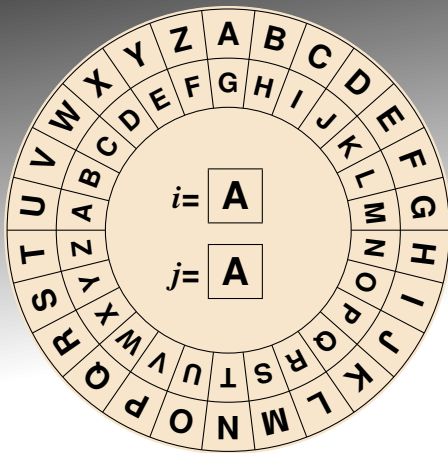
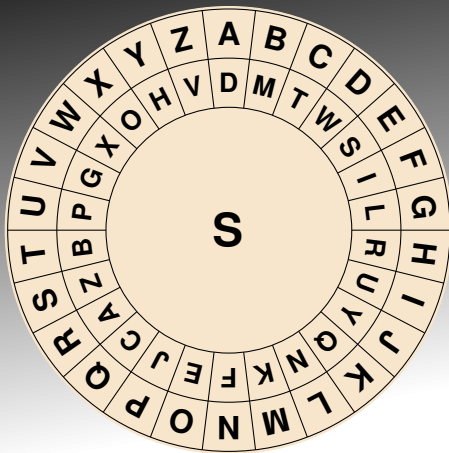


## RC4

- Beispiel: erhöhe B um G
- Hilfswalze auf G stellen

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?

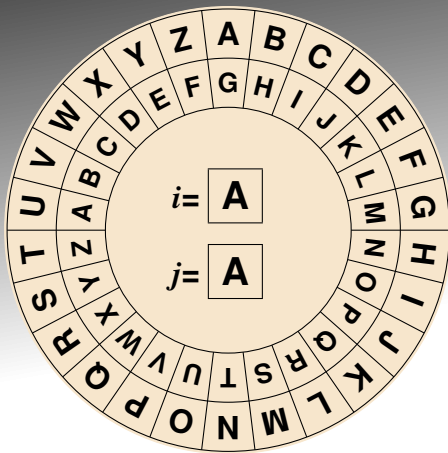
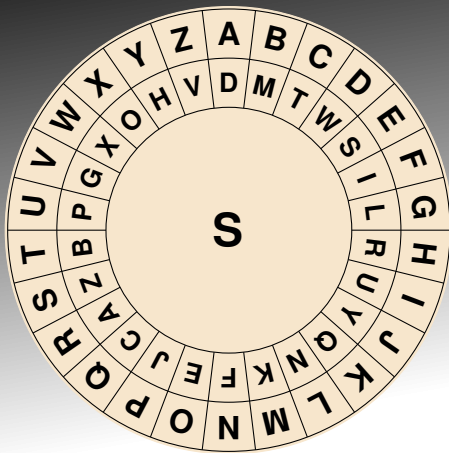


## RC4

- Beispiel: erhöhe B um G
- Hilfswalze auf G stellen

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?

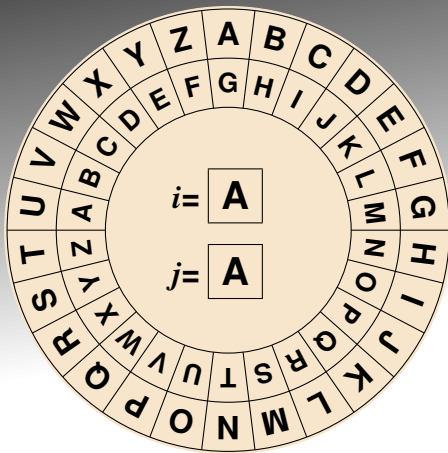
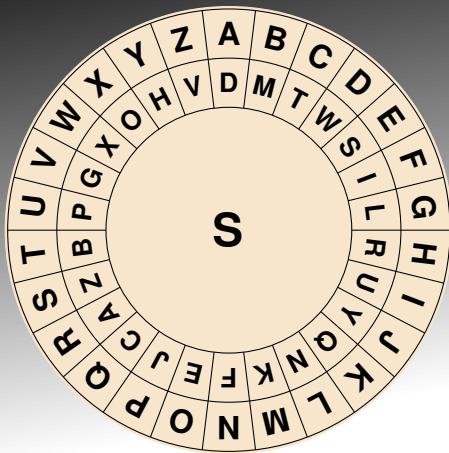


## RC4

- Beispiel: erhöhe B um G
- Hilfswalze auf G stellen
- B „verschlüsseln“

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?

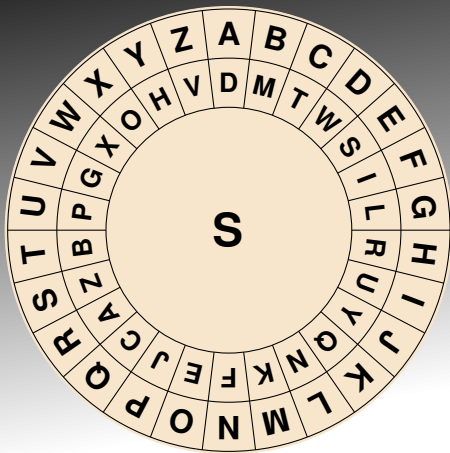


## RC4

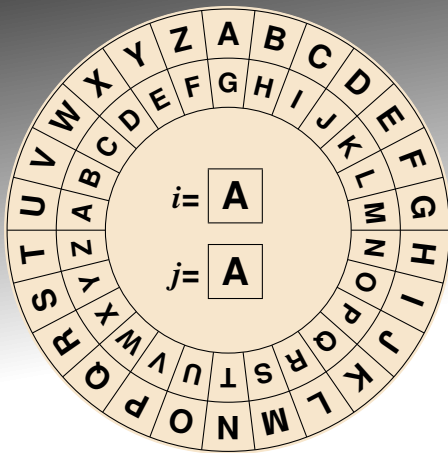
- Beispiel: erhöhe B um G
- Hilfswalze auf G stellen
- B „verschlüsseln“  $\rightarrow$  H

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

# Wie verschlüsselt man heute?



RC4

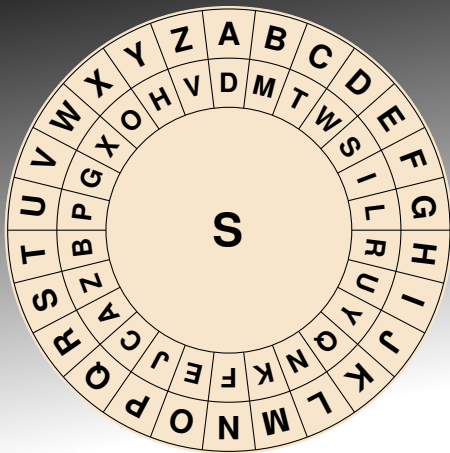


Enigma

-----

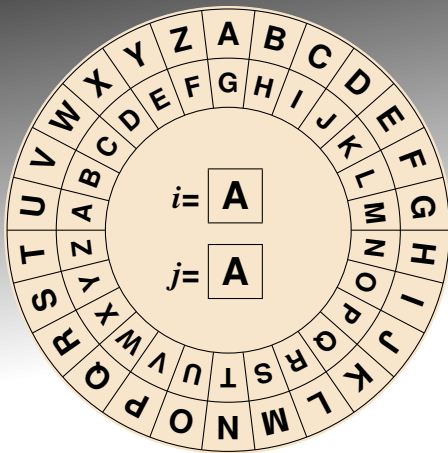


# Wie verschlüsselt man heute?



RC4

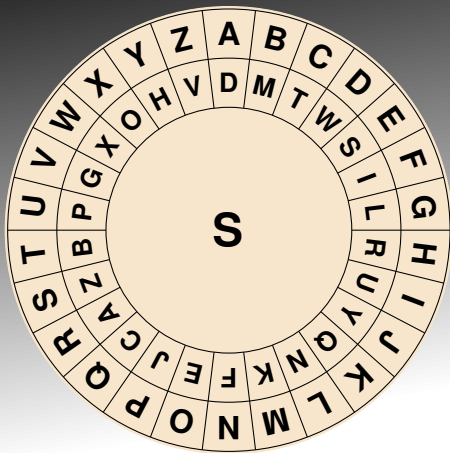
- Erhöhe  $i$



Enigma

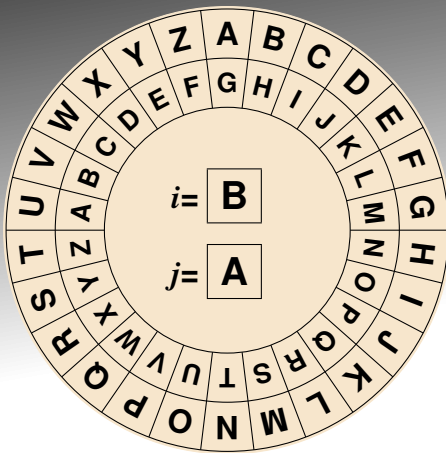
-----

# Wie verschlüsselt man heute?



RC4

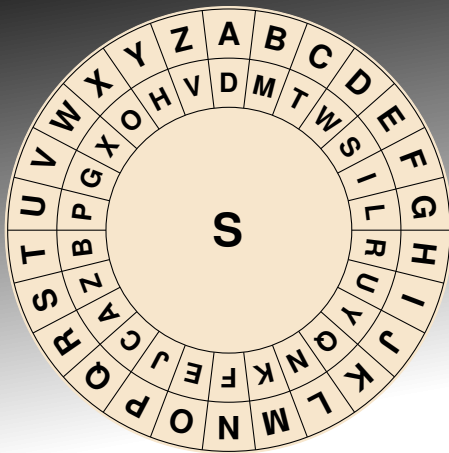
- Erhöhe  $i$



Enigma

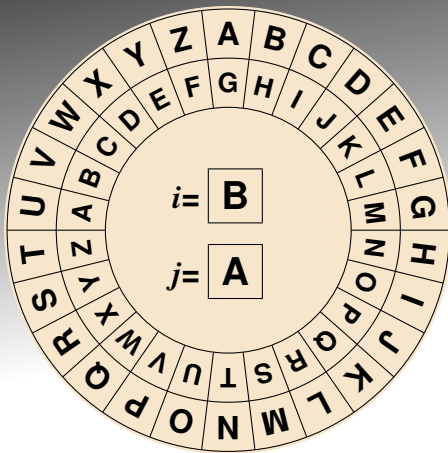
-----

# Wie verschlüsselt man heute?



RC4

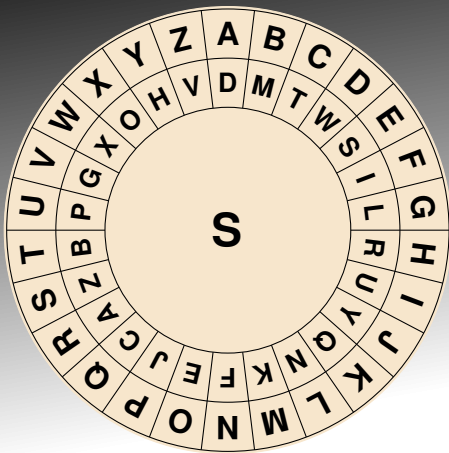
- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$



Enigma

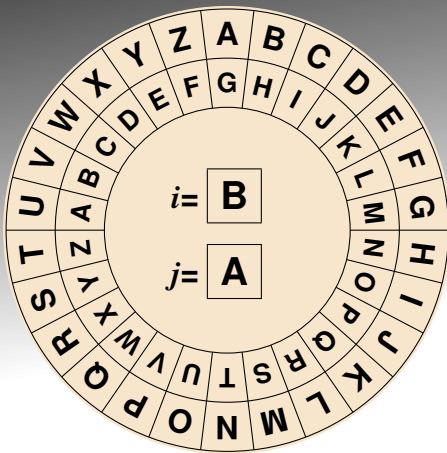
-----

# Wie verschlüsselt man heute?



RC4

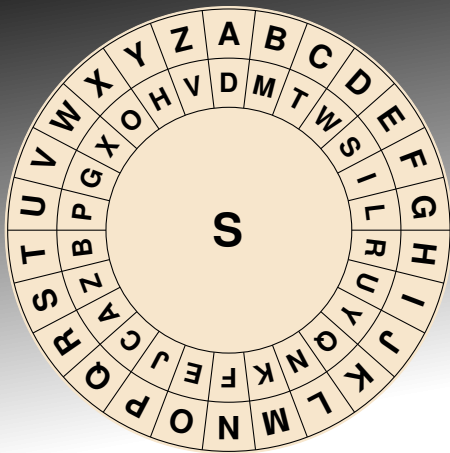
- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = M$



Enigma

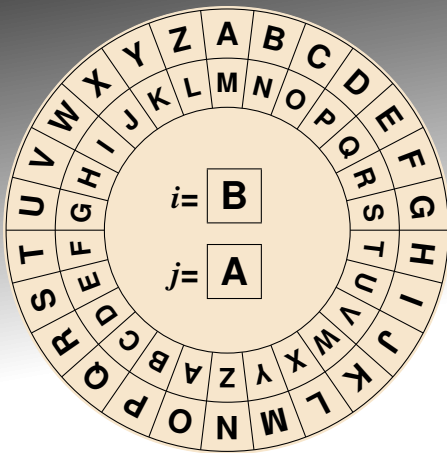
-----

# Wie verschlüsselt man heute?



RC4

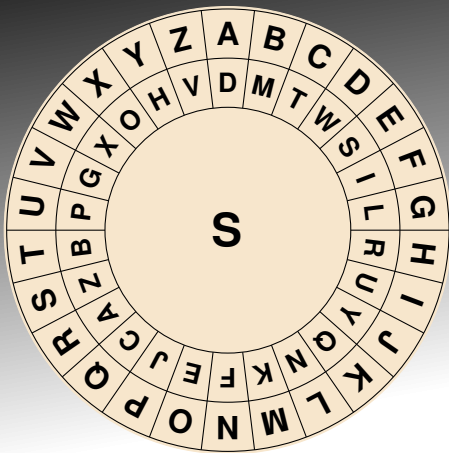
- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = M$



Enigma

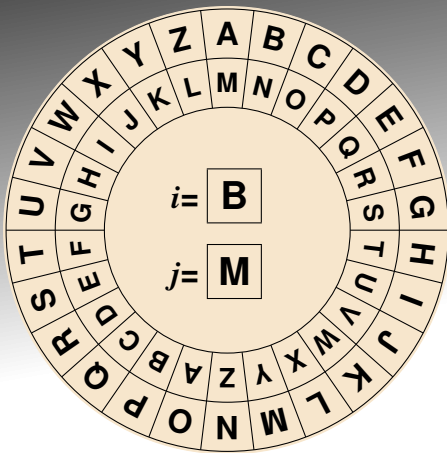
-----

# Wie verschlüsselt man heute?



RC4

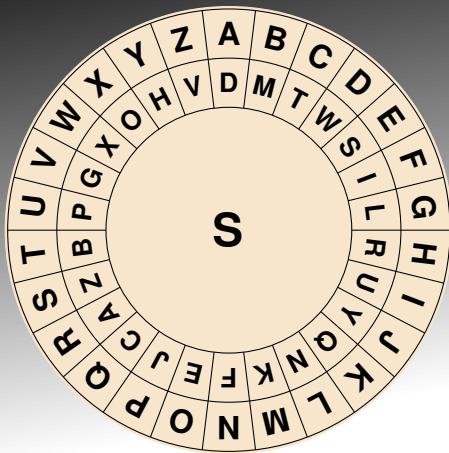
- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = M$



Enigma

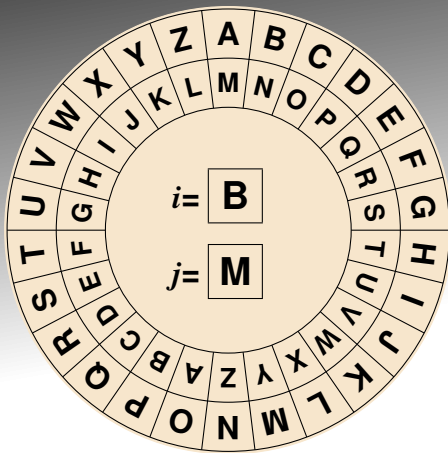
-----

# Wie verschlüsselt man heute?



RC4

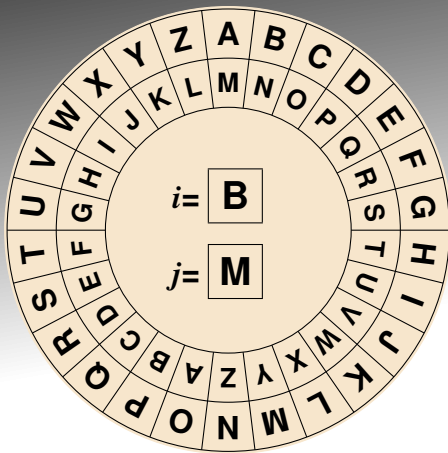
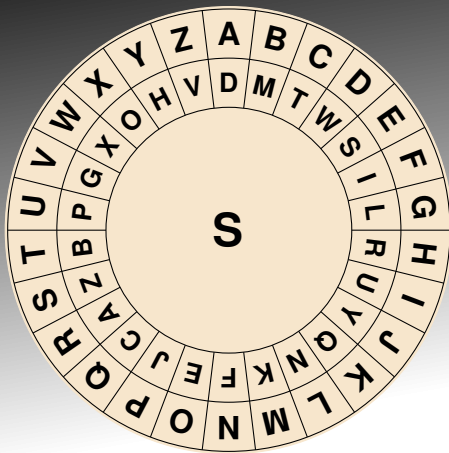
- Erhöhe  $j$  um  $S[i] = M$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

-----

# Wie verschlüsselt man heute?



RC4

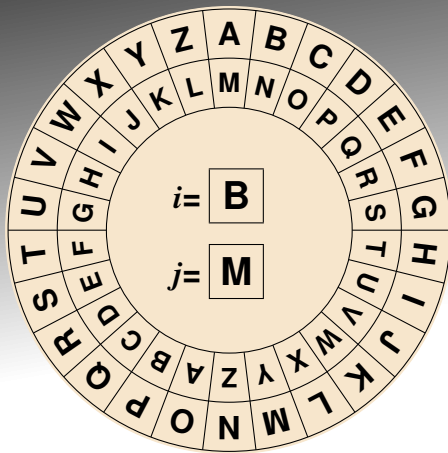
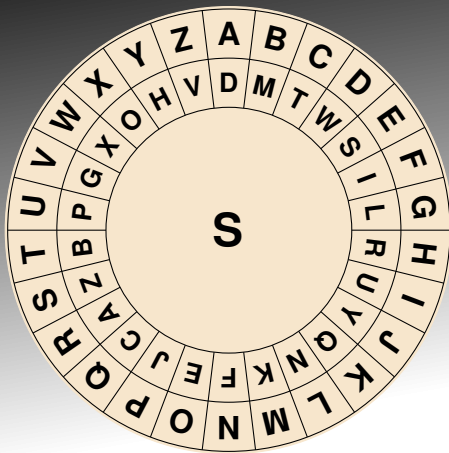
- Erhöhe  $j$  um  $S[i] = M$
- berechne  $S[j] = K$ , erhöht um  $S[i] = M$

Enigma

-----



# Wie verschlüsselt man heute?



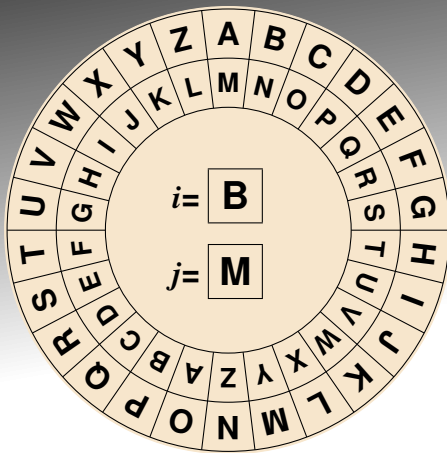
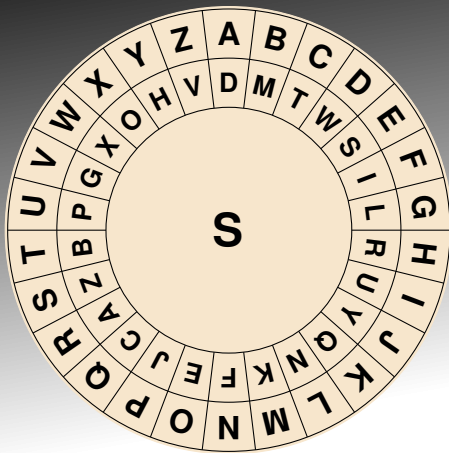
RC4

- Erhöhe  $j$  um  $S[i] = M$
- berechne  $S[j] = K$ , erhöht um  $S[i] = M$   
Ergebnis: W

Enigma

-----

# Wie verschlüsselt man heute?



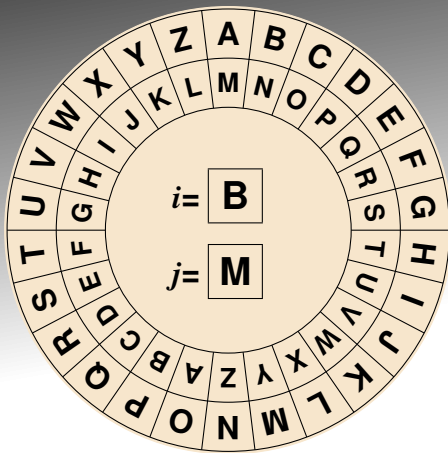
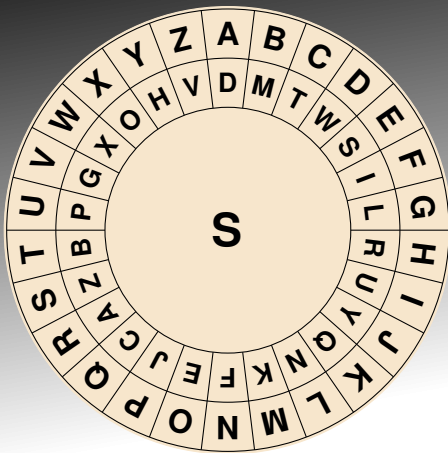
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = M$   
Ergebnis: W
- verschlüssele mit  $S[W]$

Enigma

-----

# Wie verschlüsselt man heute?



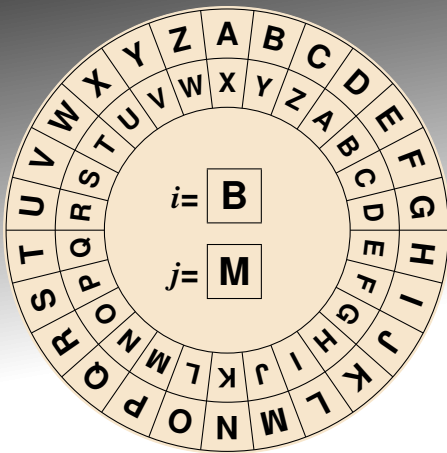
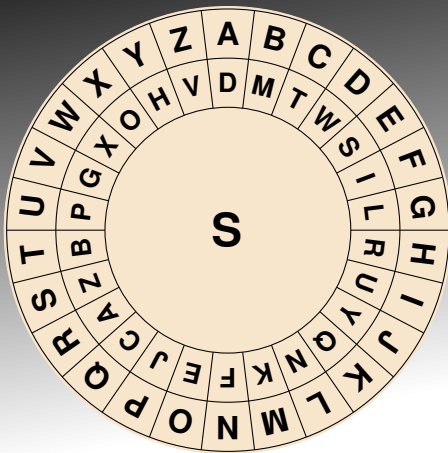
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = M$   
Ergebnis: W
- verschlüsse mit  $S[W] = X$

Enigma

-----

# Wie verschlüsselt man heute?



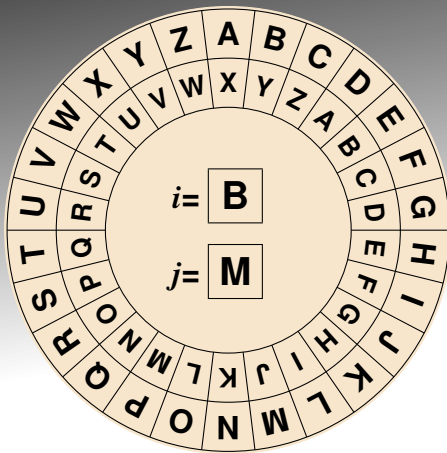
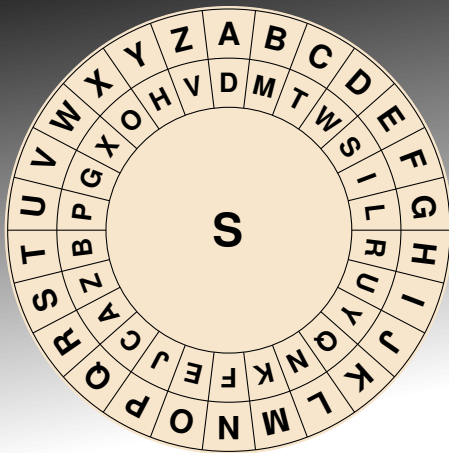
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = M$   
Ergebnis: W
- verschlüsse mit  $S[W] = X$

Enigma

-----

# Wie verschlüsselt man heute?



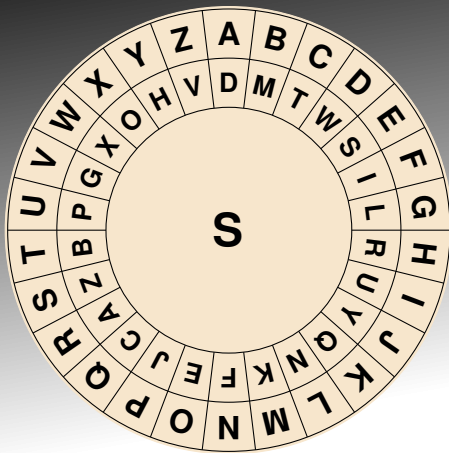
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = M$   
Ergebnis: W
- verschlüsse mit  $S[W] = X$

Enigma

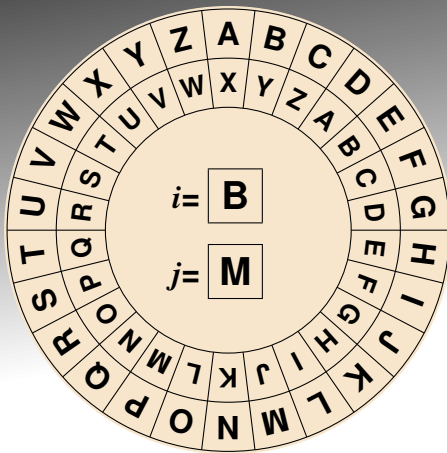
B-----

# Wie verschlüsselt man heute?



RC4

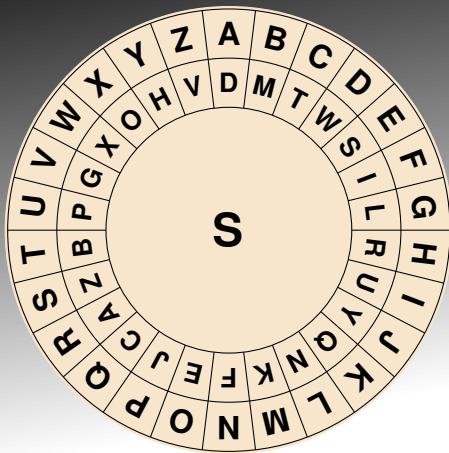
- verschlüssele mit  $S[W] = X$
- vertausche  $S[i]$  mit  $S[j]$



Enigma

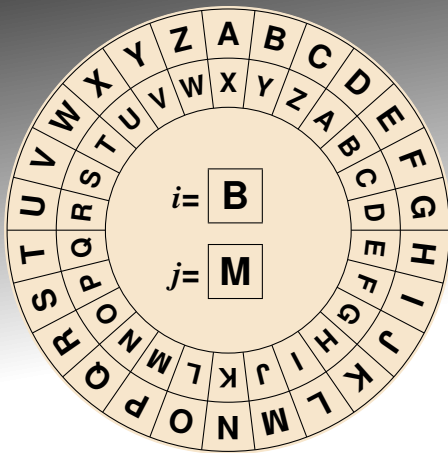
B-----

# Wie verschlüsselt man heute?



RC4

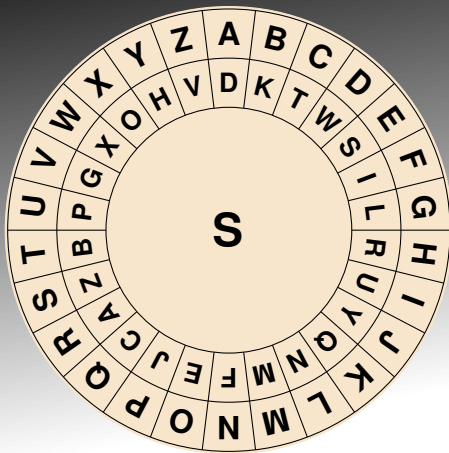
- verschlüssele mit  $S[W] = X$
- vertausche  $S[i] = M$  mit  $S[j] = K$



Enigma

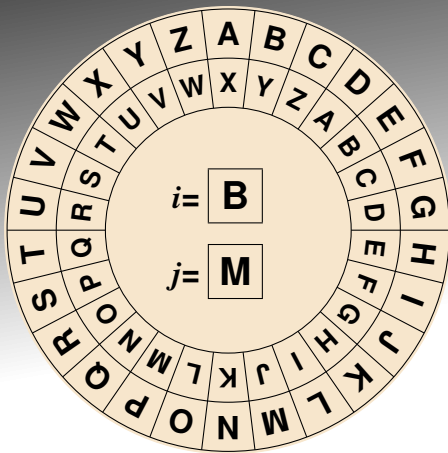
B-----

# Wie verschlüsselt man heute?



RC4

- verschlüssele mit  $S[W] = X$
- vertausche  $S[i] = M$  mit  $S[j] = K$

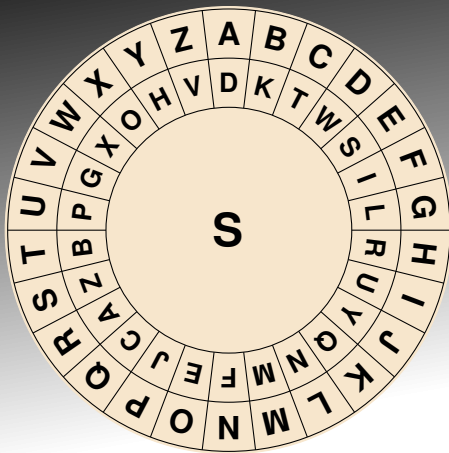


Enigma

B-----

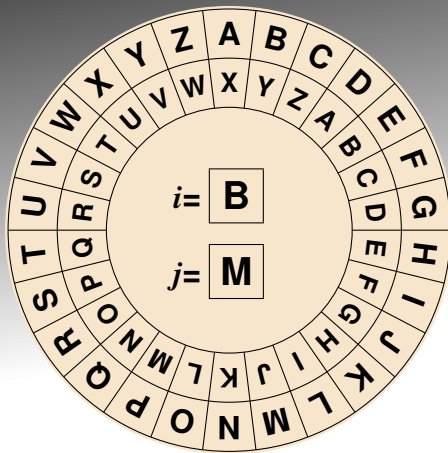


# Wie verschlüsselt man heute?



RC4

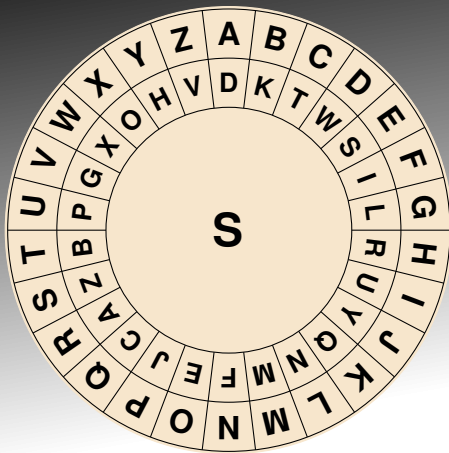
- vertausche  $S[i] = M$  mit  $S[j] = K$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

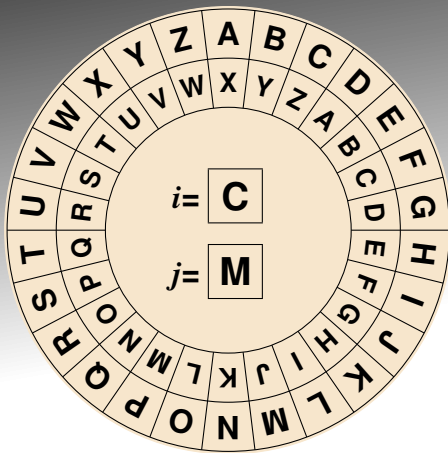
B-----

# Wie verschlüsselt man heute?



RC4

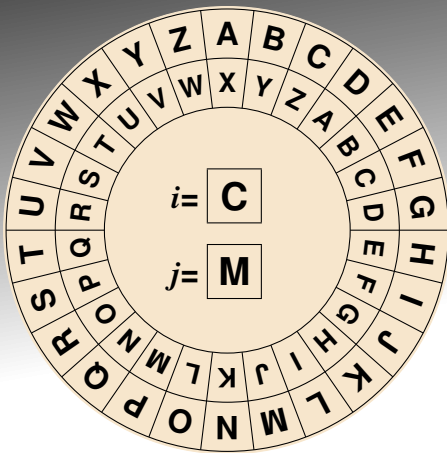
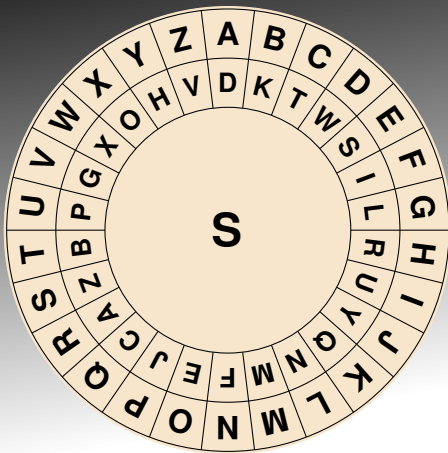
- vertausche  $S[i] = M$  mit  $S[j] = K$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

B-----

## Wie verschlüsselt man heute?



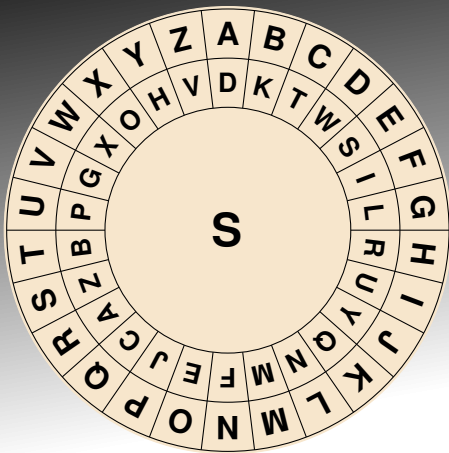
# RC4

- Nächster Buchstabe. Erhöhe  $i$
- Erhöhe  $j$  um  $\mathbf{S}[i]$

# Enigma

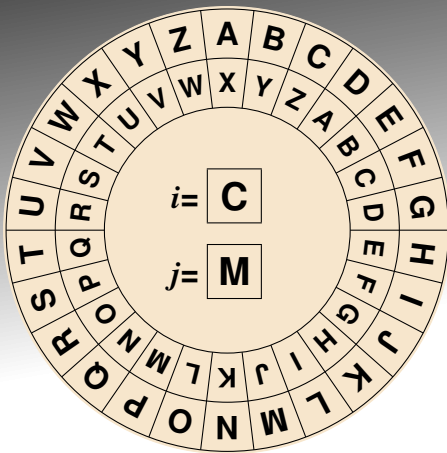
**B-----**

# Wie verschlüsselt man heute?



RC4

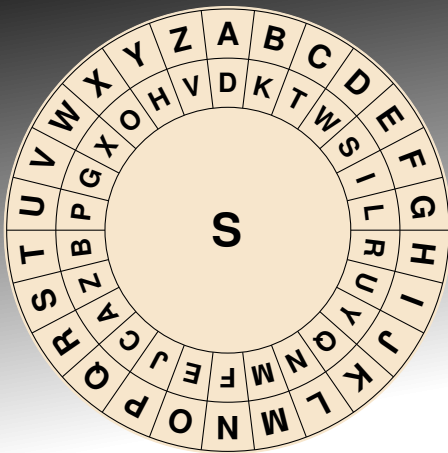
- Nächster Buchstabe. Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

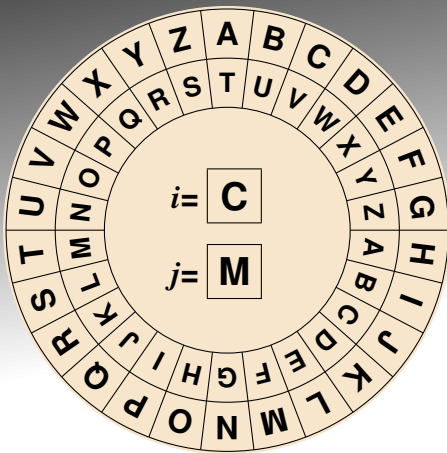
B-----

# Wie verschlüsselt man heute?



RC4

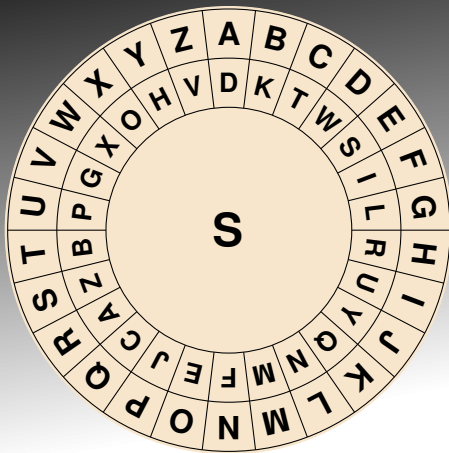
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

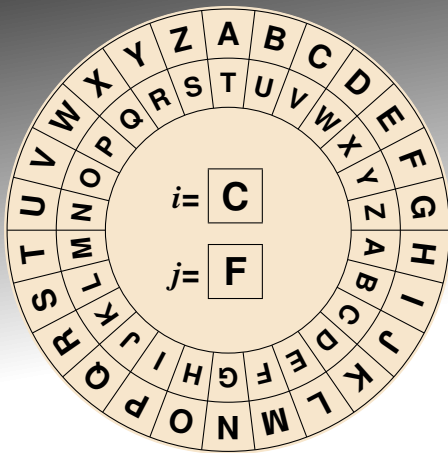
B-----

# Wie verschlüsselt man heute?



RC4

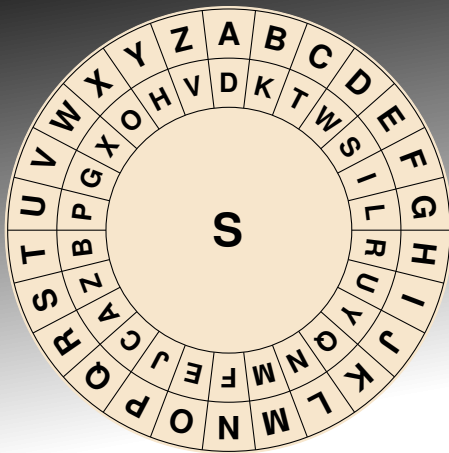
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

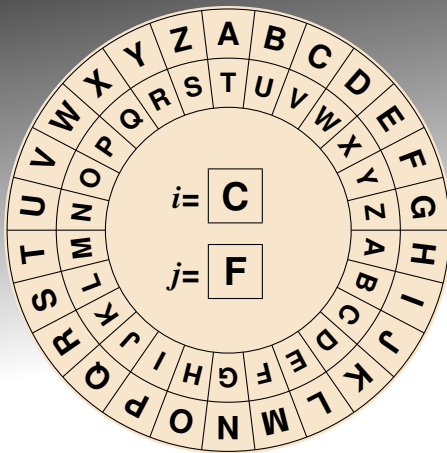
B-----

# Wie verschlüsselt man heute?



RC4

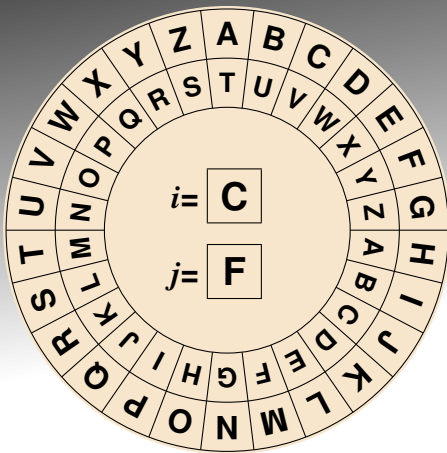
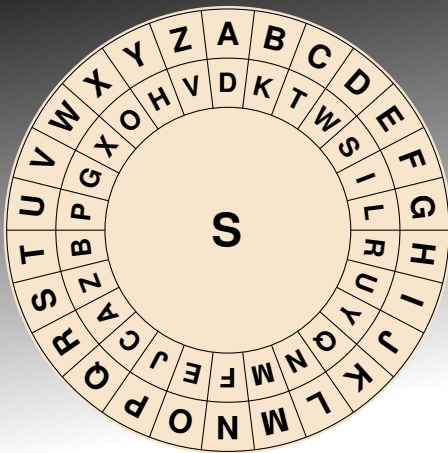
- Erhöhe  $j$  um  $S[i] = T$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

B-----

# Wie verschlüsselt man heute?



RC4

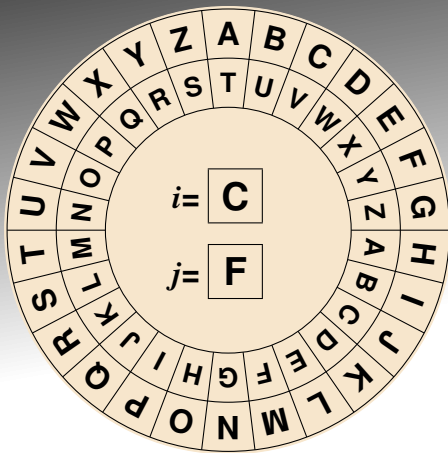
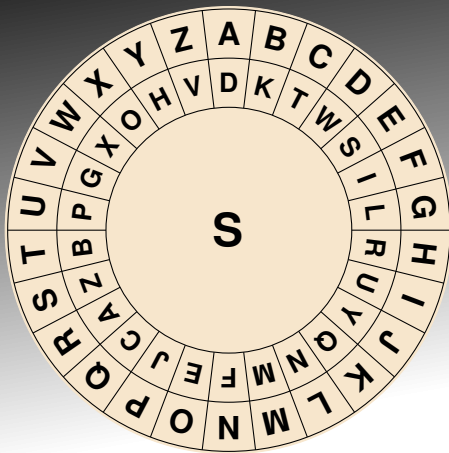
- Erhöhe  $j$  um  $S[i] = T$
- berechne  $S[j] = I$ , erhöht um  $S[i] = T$

Enigma

B-----



# Wie verschlüsselt man heute?



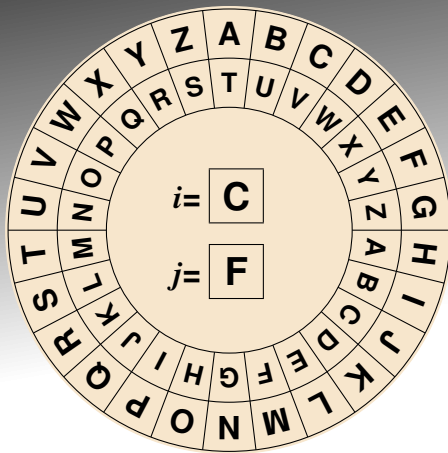
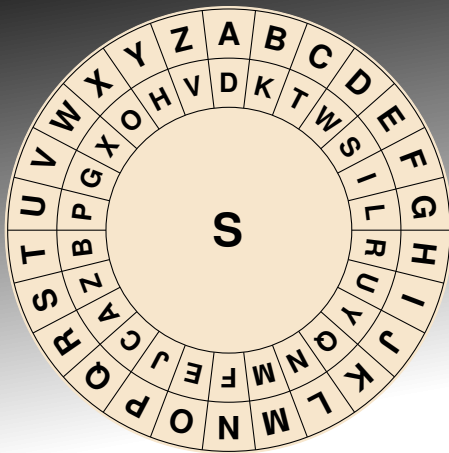
RC4

- Erhöhe  $j$  um  $S[i] = T$
  - berechne  $S[j] = I$ , erhöht um  $S[i] = T$
- Ergebnis: B

Enigma

B-----

# Wie verschlüsselt man heute?



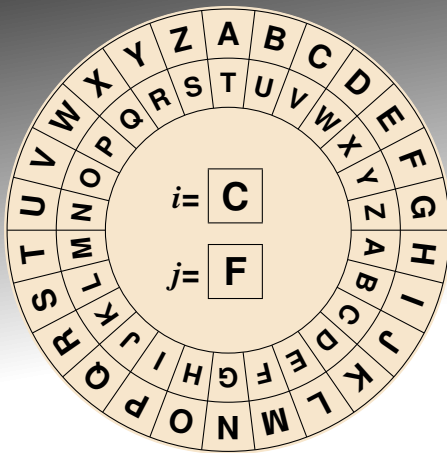
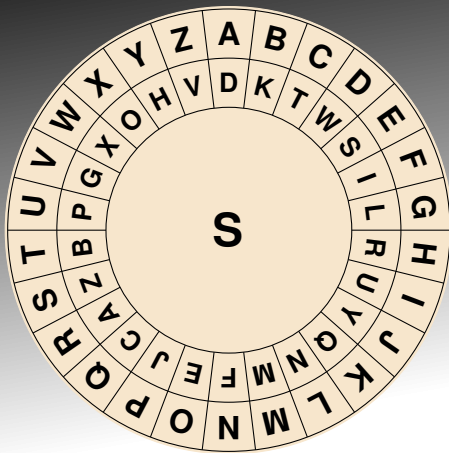
RC4

- berechne  $S[j] = I$ , erhöht um  $S[i] = T$   
Ergebnis: B
- verschlüssele mit  $S[B]$

Enigma

B-----

# Wie verschlüsselt man heute?



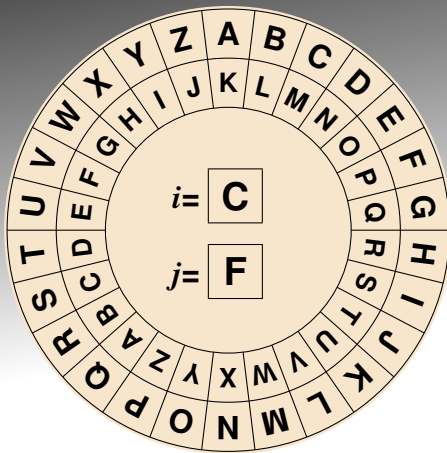
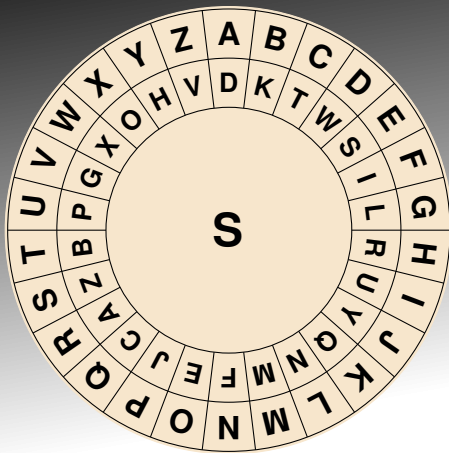
RC4

- berechne  $S[j] = I$ , erhöht um  $S[i] = T$   
Ergebnis: B
- verschlüsse mit  $S[B] = K$

Enigma

B-----

# Wie verschlüsselt man heute?



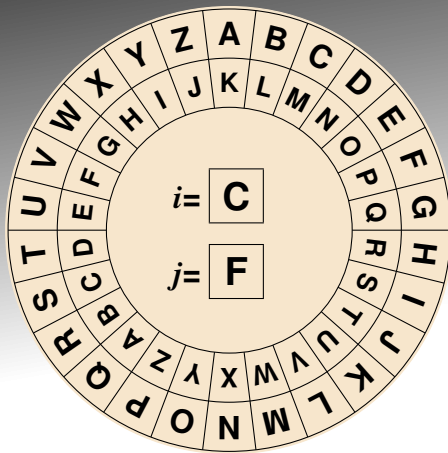
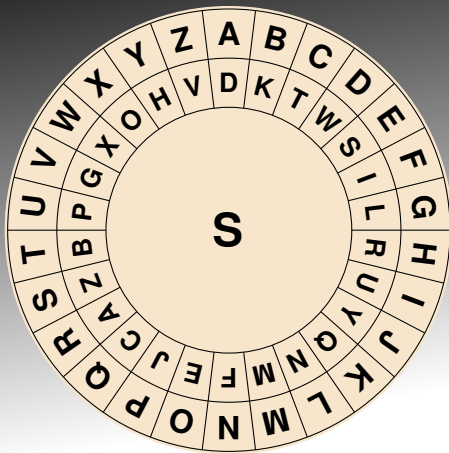
RC4

- berechne  $S[j] = I$ , erhöht um  $S[i] = T$   
Ergebnis: B
- verschlüsse mit  $S[B] = K$

Enigma

B-----

# Wie verschlüsselt man heute?



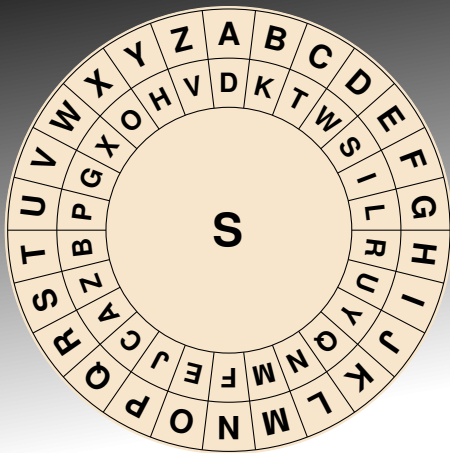
RC4

- berechne  $S[j] = I$ , erhöht um  $S[i] = T$   
Ergebnis: B
- verschlüsse mit  $S[B] = K$

Enigma

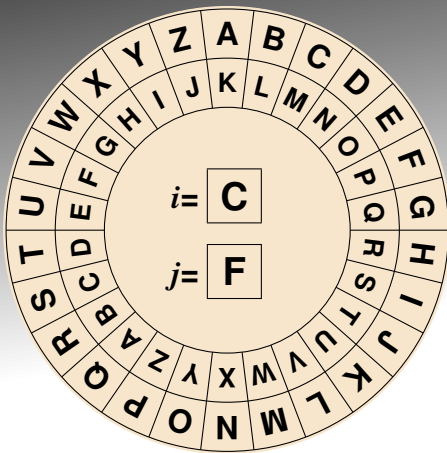
Bx----

# Wie verschlüsselt man heute?



RC4

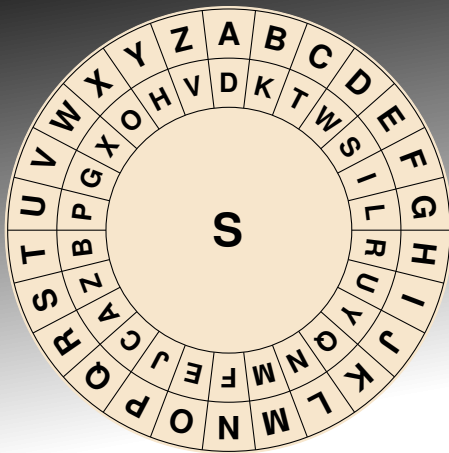
- verschlüssele mit  $S[B] = K$
- vertausche  $S[i]$  mit  $S[j]$



Enigma

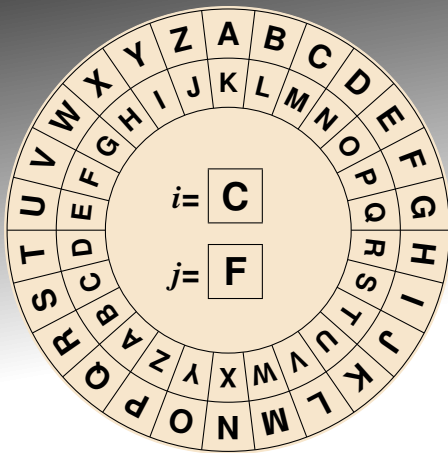
Bx----

# Wie verschlüsselt man heute?



RC4

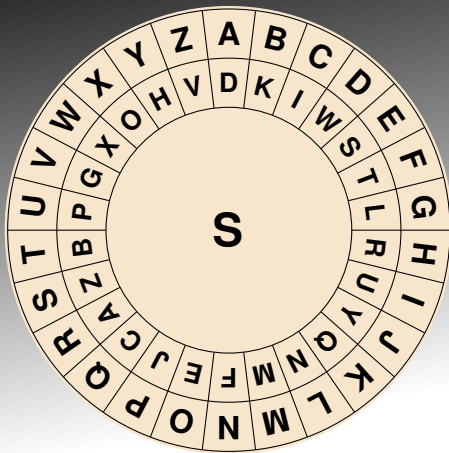
- verschlüssele mit  $S[B] = K$
- vertausche  $S[i] = T$  mit  $S[j] = I$



Enigma

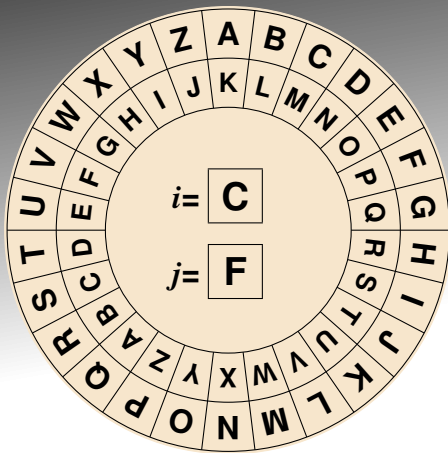
Bx----

# Wie verschlüsselt man heute?



RC4

- verschlüssele mit  $S[B] = K$
- vertausche  $S[i] = T$  mit  $S[j] = I$

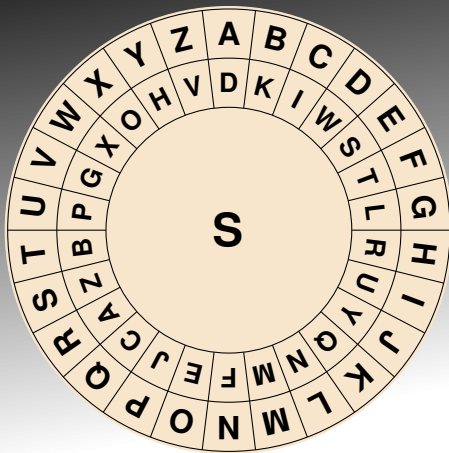


Enigma

Bx----

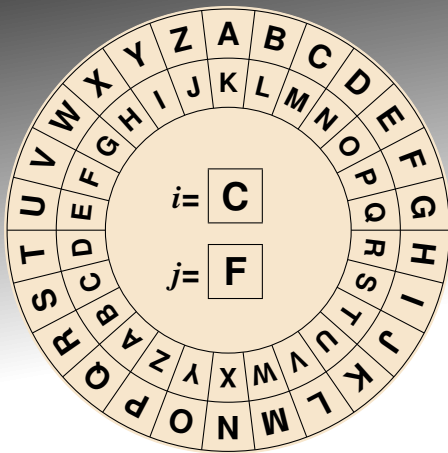


# Wie verschlüsselt man heute?



RC4

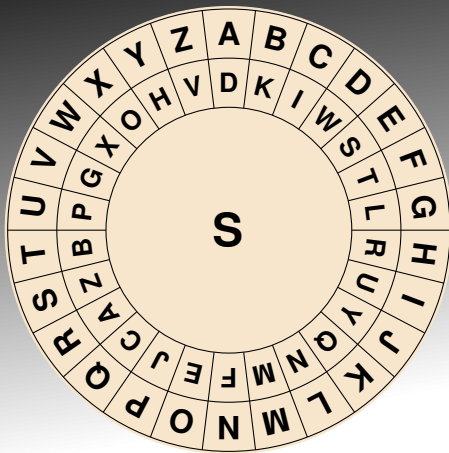
- vertausche  $S[i] = T$  mit  $S[j] = I$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

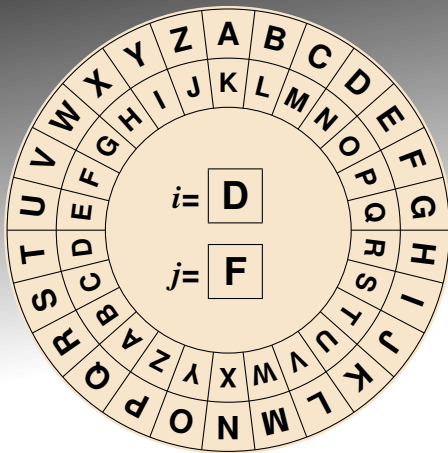
Bx----

# Wie verschlüsselt man heute?



RC4

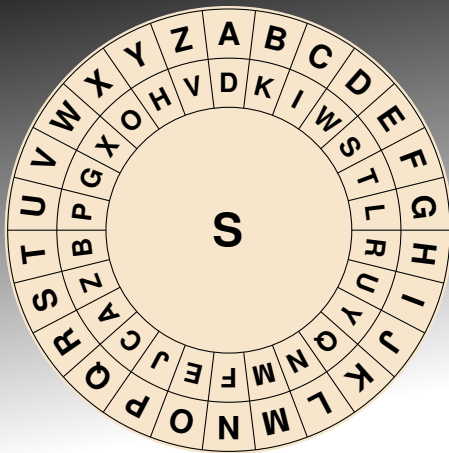
- vertausche  $S[i] = T$  mit  $S[j] = I$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

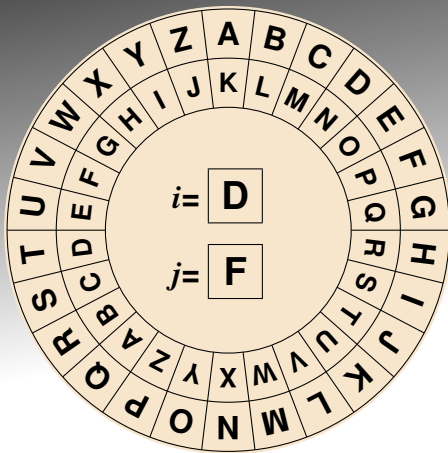
Bx----

# Wie verschlüsselt man heute?



RC4

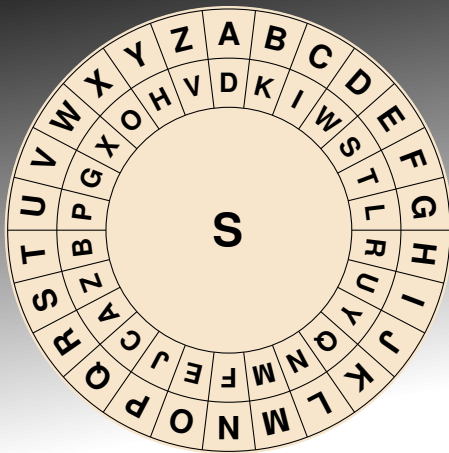
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$



Enigma

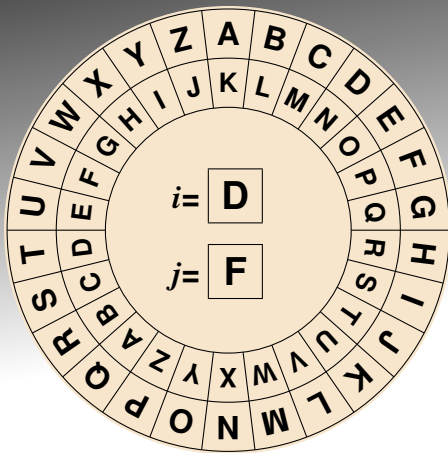
Bx----

# Wie verschlüsselt man heute?



RC4

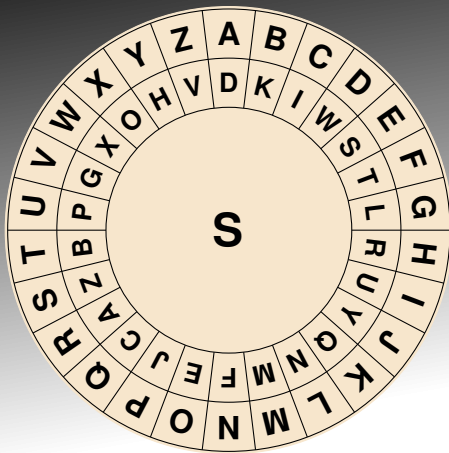
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = W$



Enigma

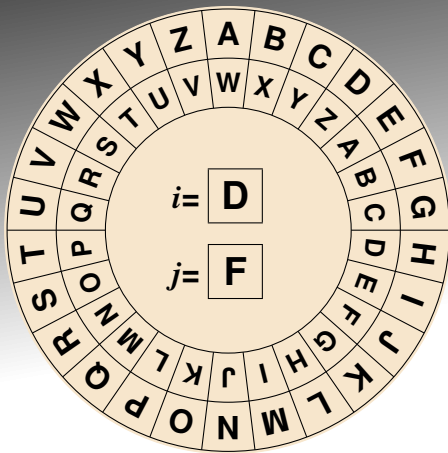
Bx----

# Wie verschlüsselt man heute?



RC4

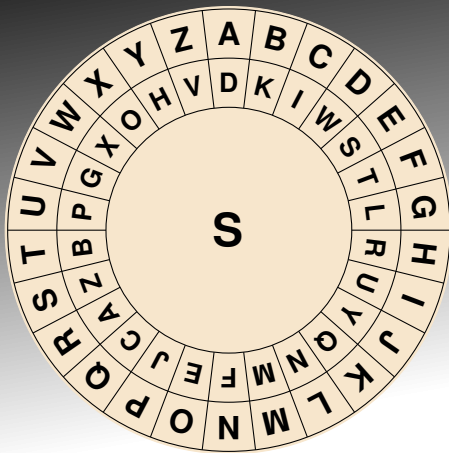
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = W$



Enigma

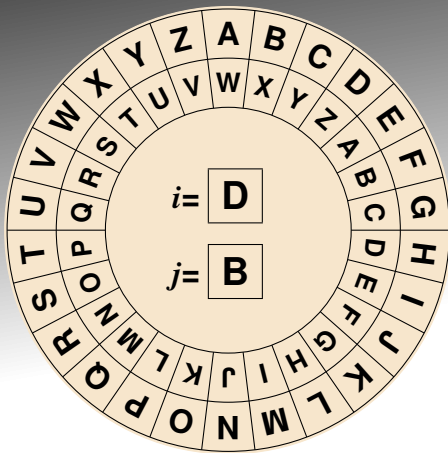
Bx----

# Wie verschlüsselt man heute?



RC4

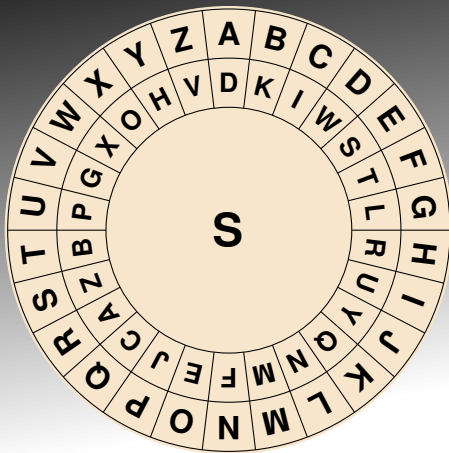
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = W$



Enigma

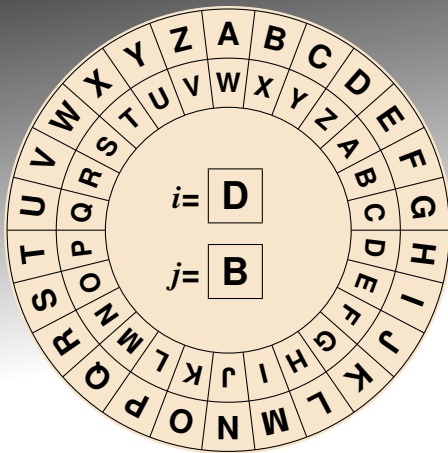
Bx----

# Wie verschlüsselt man heute?



RC4

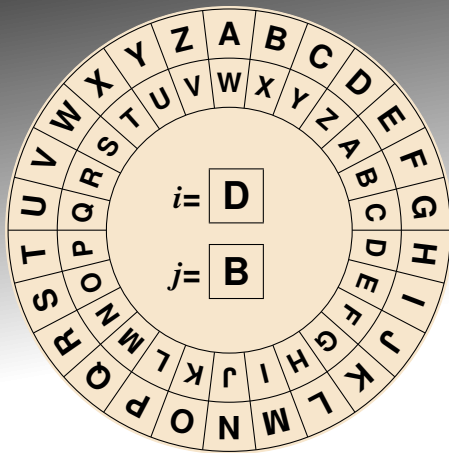
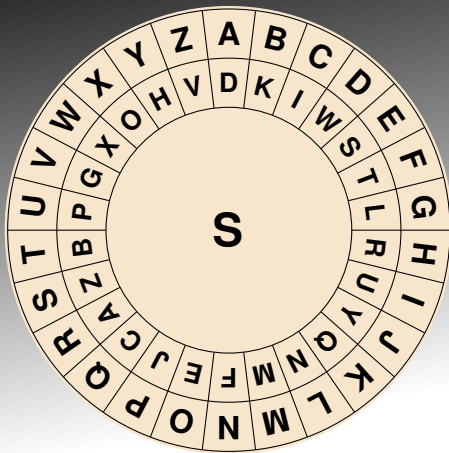
- Erhöhe  $j$  um  $S[i] = W$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

Bx----

# Wie verschlüsselt man heute?



RC4

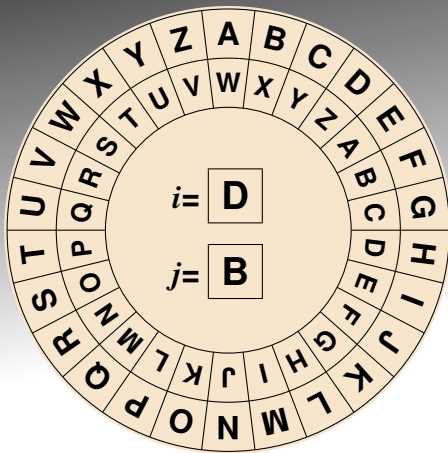
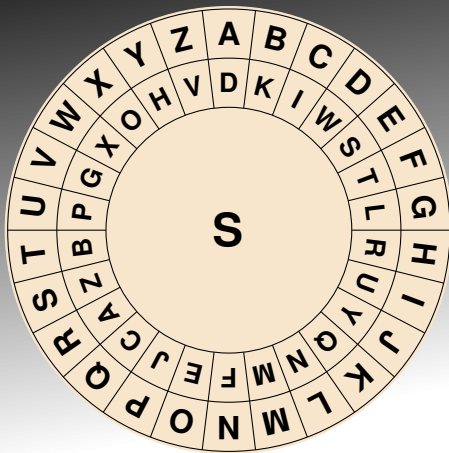
- Erhöhe  $j$  um  $S[i] = W$
- berechne  $S[j] = K$ , erhöht um  $S[i] = W$

Enigma

Bx----



# Wie verschlüsselt man heute?



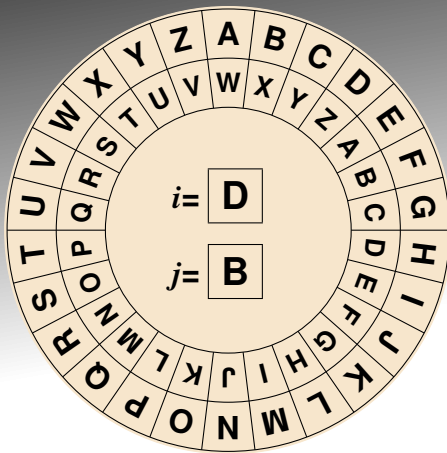
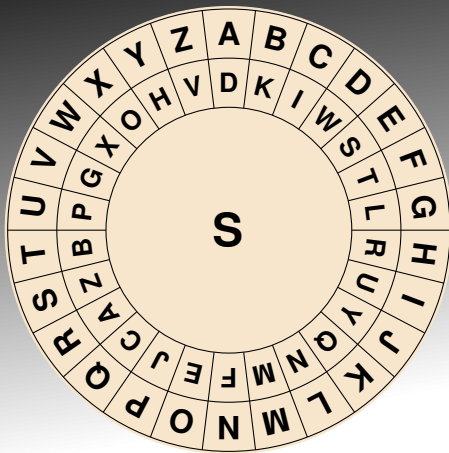
RC4

- Erhöhe  $j$  um  $S[i] = W$
- berechne  $S[j] = K$ , erhöht um  $S[i] = W$   
Ergebnis: G

Enigma

Bx----

# Wie verschlüsselt man heute?



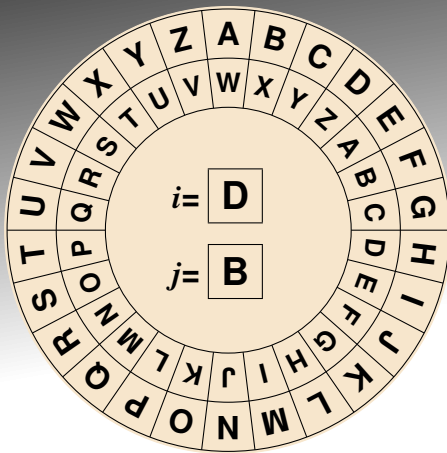
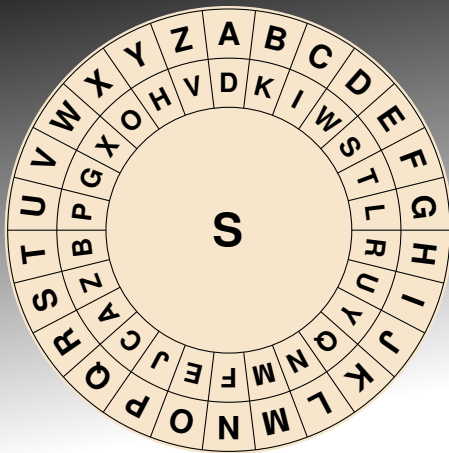
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = W$   
Ergebnis: G
- verschlüssele mit  $S[G]$

Enigma

Bx----

# Wie verschlüsselt man heute?



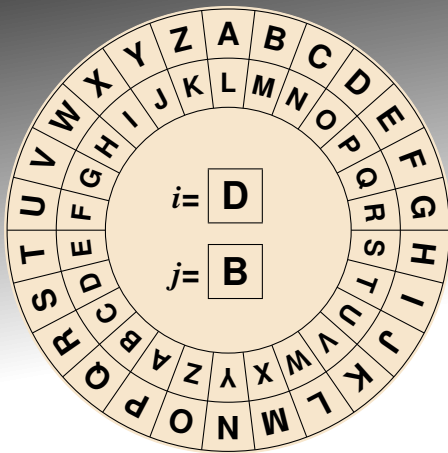
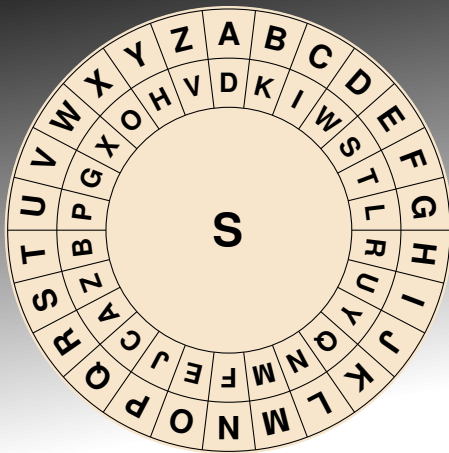
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = W$   
Ergebnis: G
- verschlüsse mit  $S[G] = L$

Enigma

Bx----

# Wie verschlüsselt man heute?



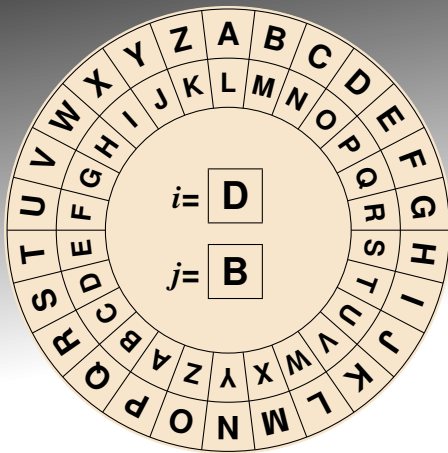
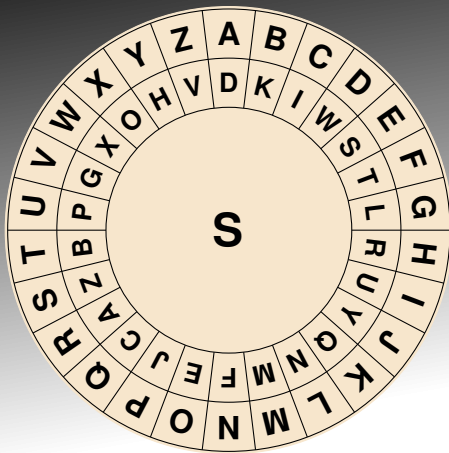
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = W$   
Ergebnis: G
- verschlüsse mit  $S[G] = L$

Enigma

Bx----

# Wie verschlüsselt man heute?



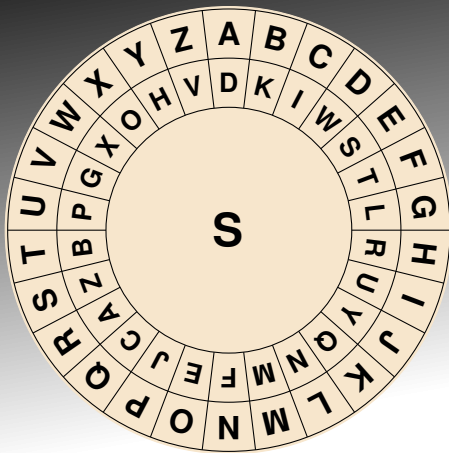
RC4

- berechne  $S[j] = K$ , erhöht um  $S[i] = W$   
Ergebnis: G
- verschlüsse mit  $S[G] = L$

Enigma

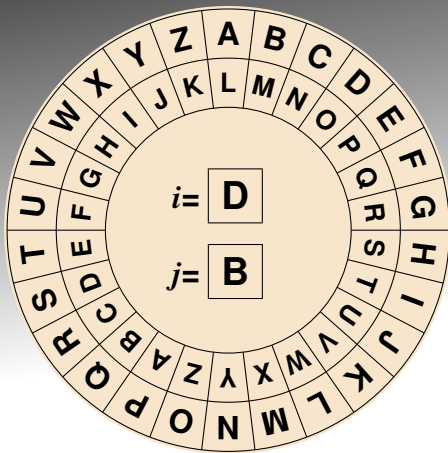
Bxt---

# Wie verschlüsselt man heute?



RC4

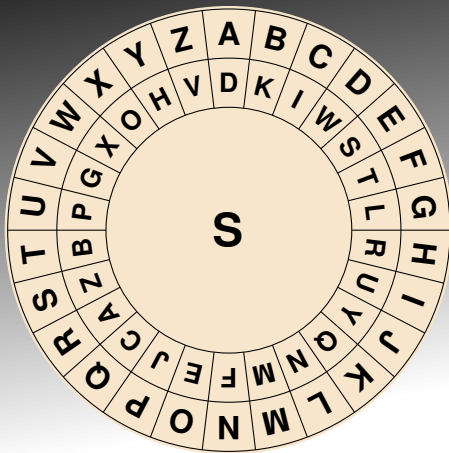
- verschlüssele mit  $S[G] = L$
- vertausche  $S[i]$  mit  $S[j]$



Enigma

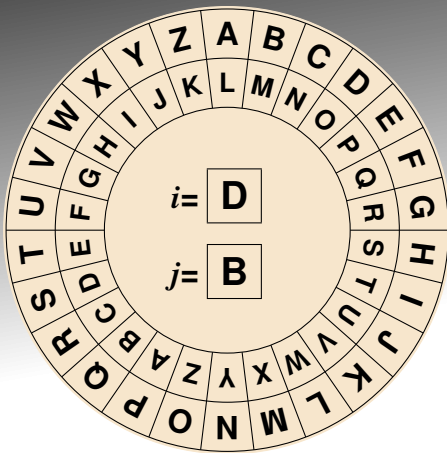
Bxt---

# Wie verschlüsselt man heute?



RC4

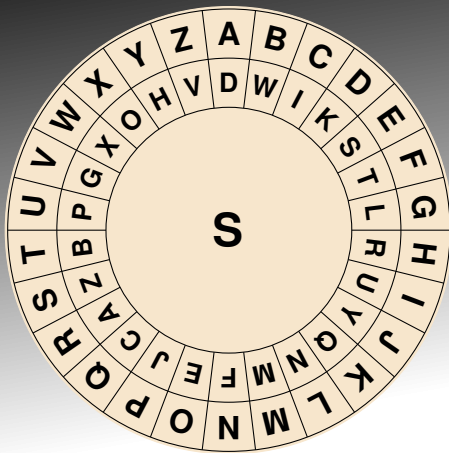
- verschlüssele mit  $S[G] = L$
- vertausche  $S[i] = W$  mit  $S[j] = K$



Enigma

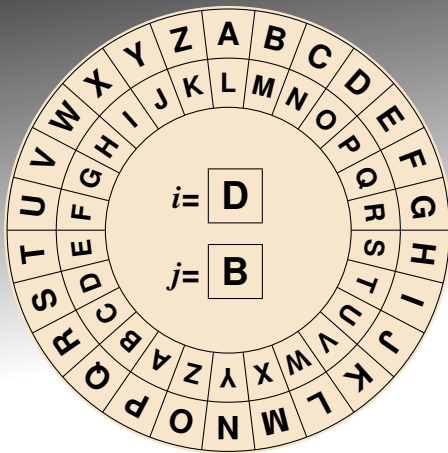
Bxt---

# Wie verschlüsselt man heute?



RC4

- verschlüssele mit  $S[G] = L$
- vertausche  $S[i] = W$  mit  $S[j] = K$

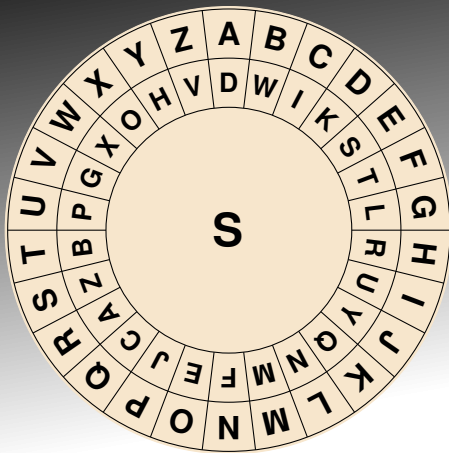


Enigma

Bxt---

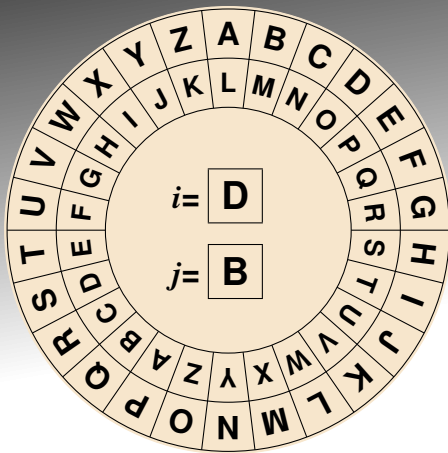


# Wie verschlüsselt man heute?



RC4

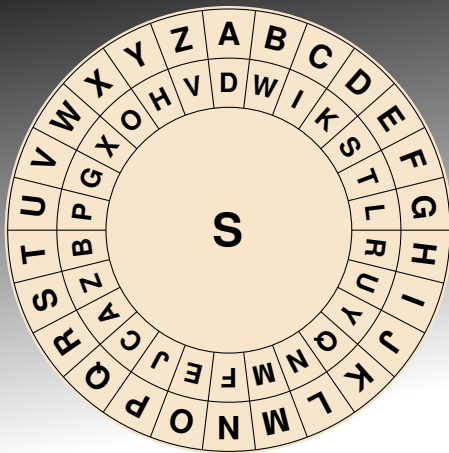
- vertausche  $S[i] = W$  mit  $S[j] = K$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

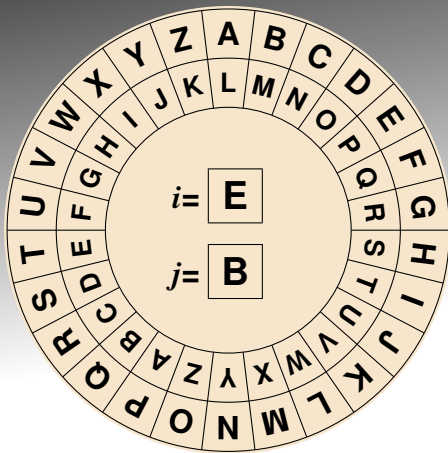
Bxt---

# Wie verschlüsselt man heute?



RC4

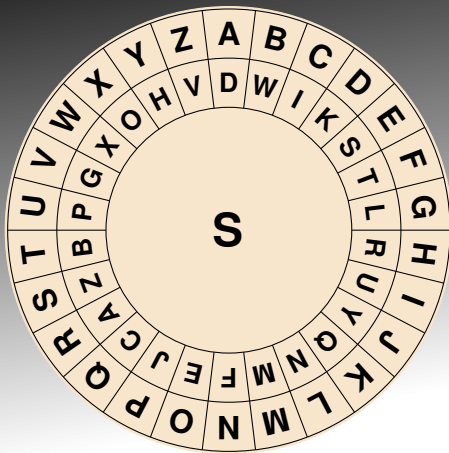
- vertausche  $S[i] = W$  mit  $S[j] = K$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

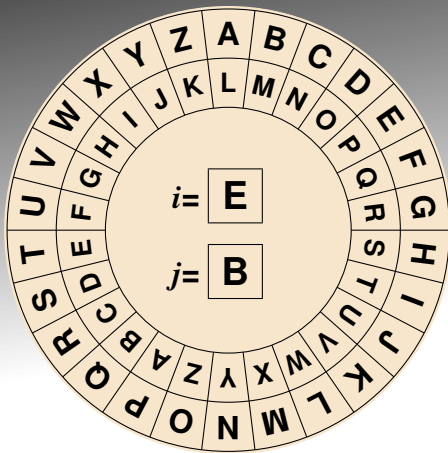
Bxt---

# Wie verschlüsselt man heute?



RC4

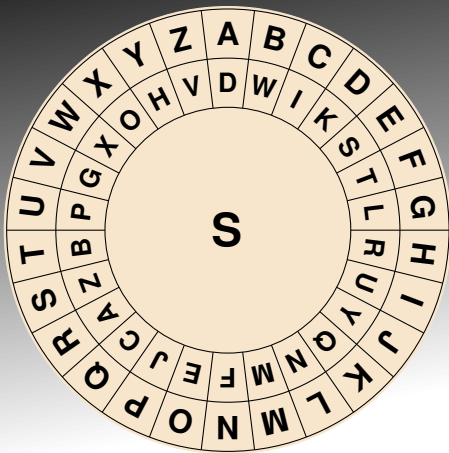
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$



Enigma

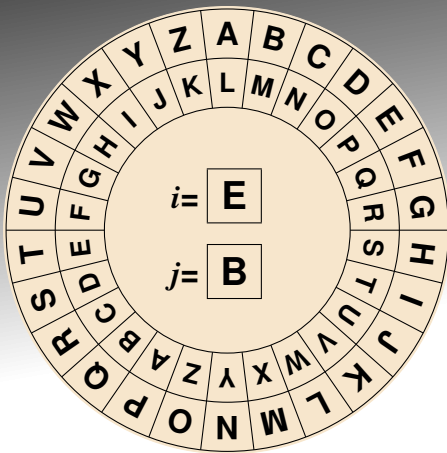
Bxt---

# Wie verschlüsselt man heute?



RC4

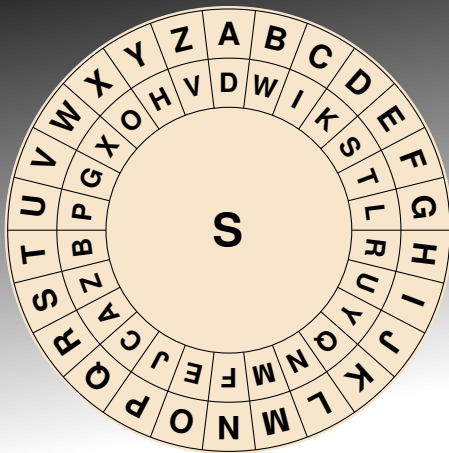
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = S$



Enigma

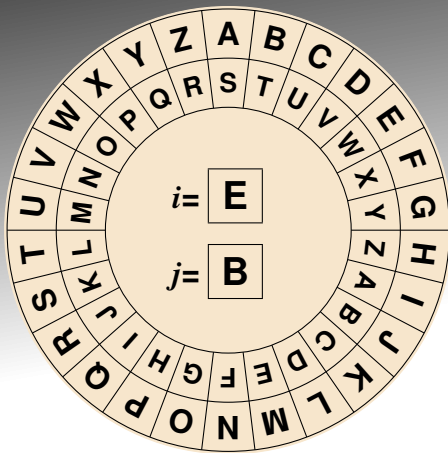
Bxt---

# Wie verschlüsselt man heute?



RC4

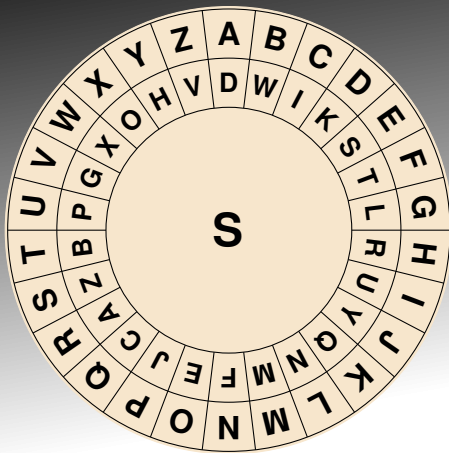
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = S$



Enigma

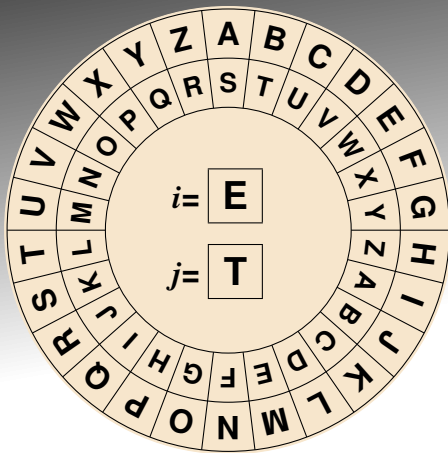
Bxt---

## Wie verschlüsselt man heute?



# RC4

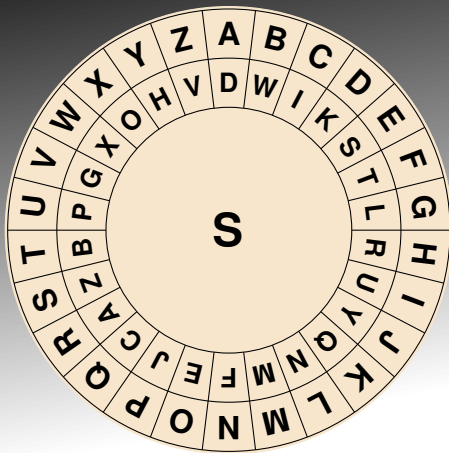
- Nächster Buchstabe. Erhöhe  $i$
- Erhöhe  $j$  um  $\mathbf{S}[i] = \mathbf{S}[j]$



# Enigma

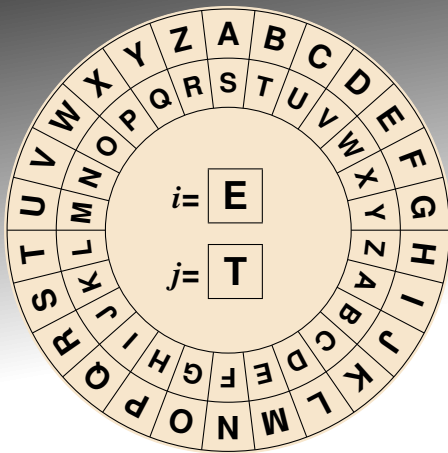
**Bxt---**

# Wie verschlüsselt man heute?



RC4

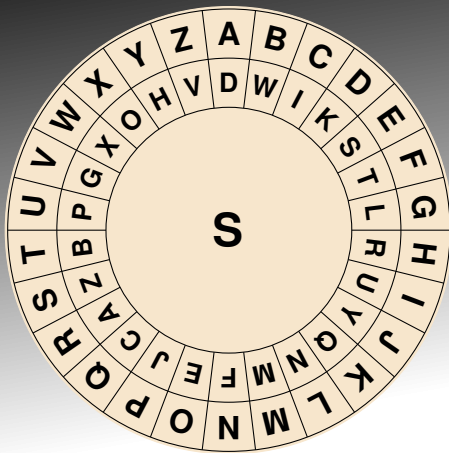
- Erhöhe  $j$  um  $S[i] = S$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

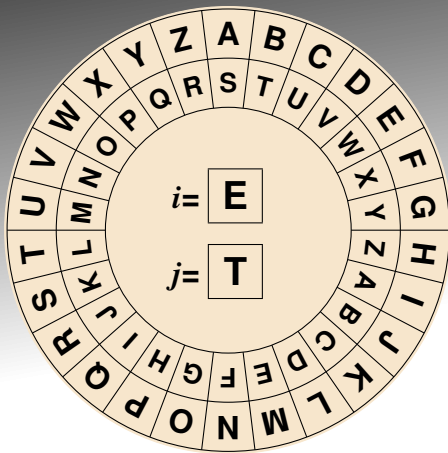
Bxt---

# Wie verschlüsselt man heute?



RC4

- Erhöhe  $j$  um  $S[i] = S$
- berechne  $S[j] = B$ , erhöht um  $S[i] = S$

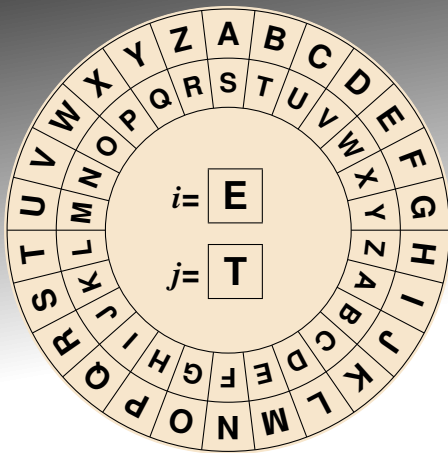
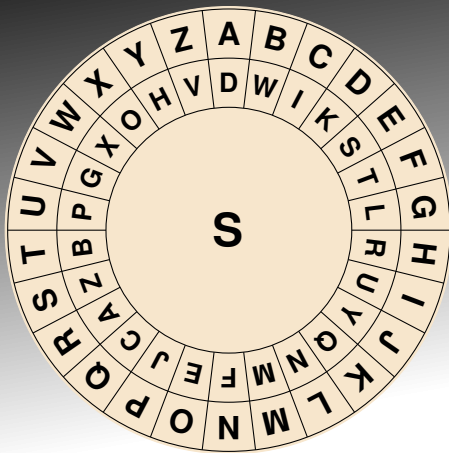


Enigma

Bxt---



## Wie verschlüsselt man heute?



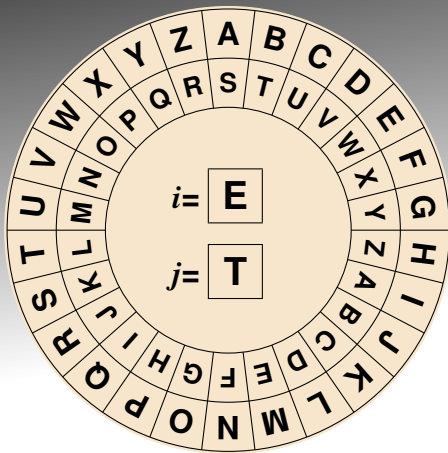
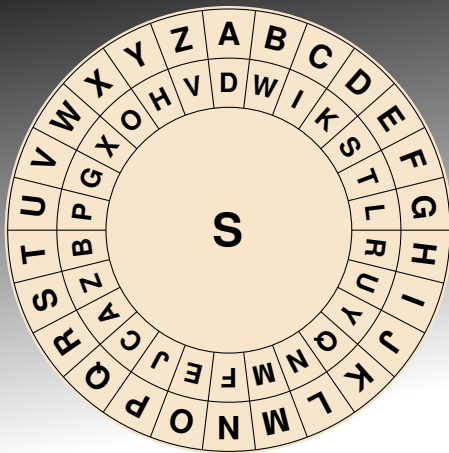
# RC4

- Erhöhe  $j$  um  $\mathbf{S}[i] = S$
  - berechne  $\mathbf{S}[j] = B$ , erhöht um  $\mathbf{S}[i] = S$
- Ergebnis: T

# Enigma

**Bxt---**

# Wie verschlüsselt man heute?



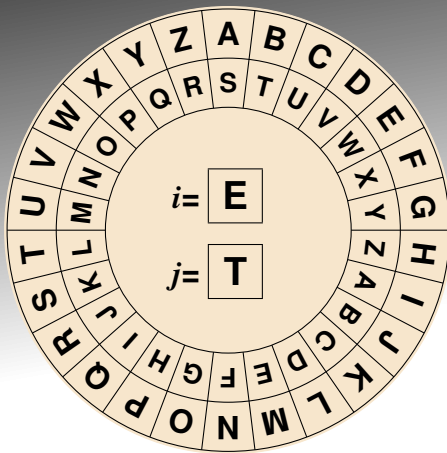
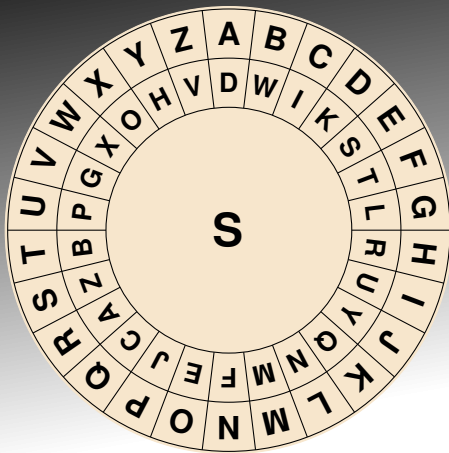
RC4

- berechne  $S[j] = B$ , erhöht um  $S[i] = S$   
Ergebnis: T
- verschlüssele mit  $S[T]$

Enigma

Bxt---

# Wie verschlüsselt man heute?



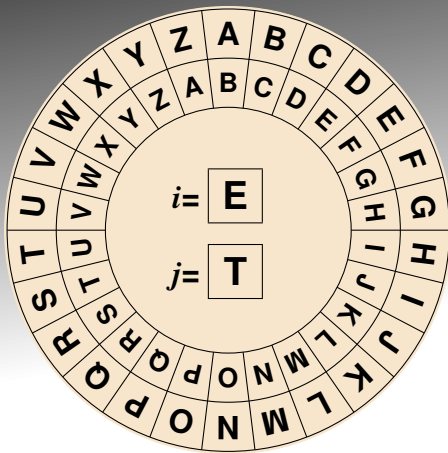
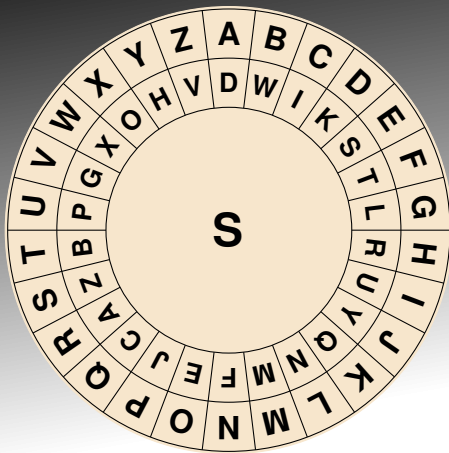
RC4

- berechne  $S[j] = B$ , erhöht um  $S[i] = S$   
Ergebnis: T
- verschlüsse mit  $S[T] = B$

Enigma

Bxt---

# Wie verschlüsselt man heute?



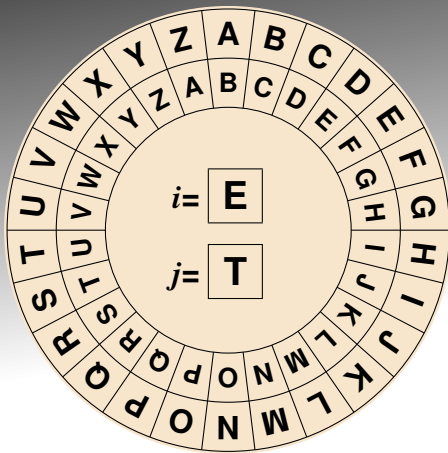
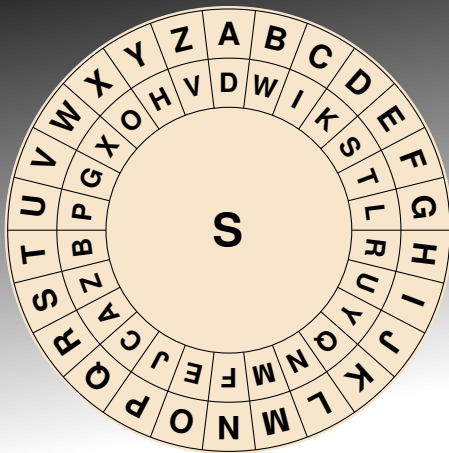
RC4

- berechne  $S[j] = B$ , erhöht um  $S[i] = S$   
Ergebnis: T
- verschlüsse mit  $S[T] = B$

Enigma

Bxt---

# Wie verschlüsselt man heute?



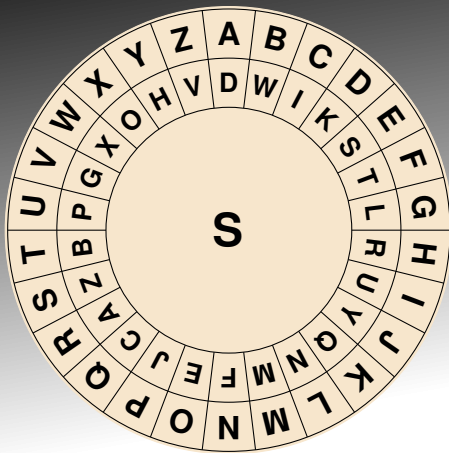
RC4

- berechne  $S[j] = B$ , erhöht um  $S[i] = S$   
Ergebnis: T
- verschlüsse mit  $S[T] = B$

Enigma

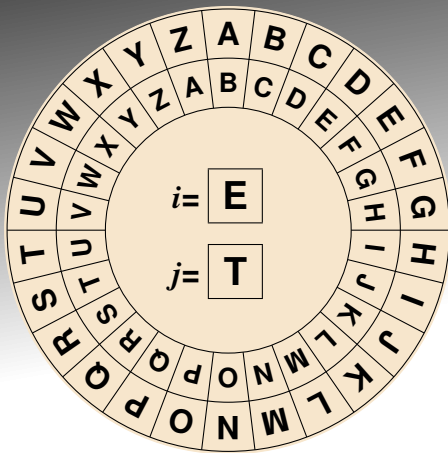
Bxth--

# Wie verschlüsselt man heute?



RC4

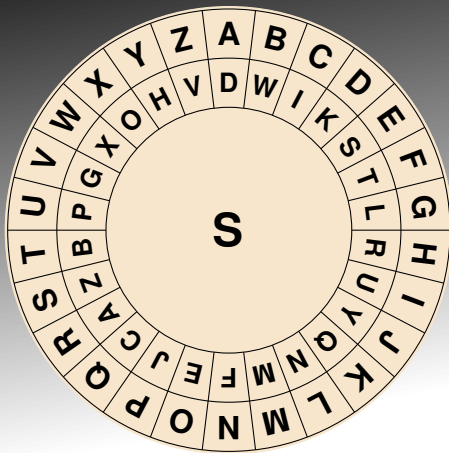
- verschlüssele mit  $S[T] = B$
- vertausche  $S[i]$  mit  $S[j]$



Enigma

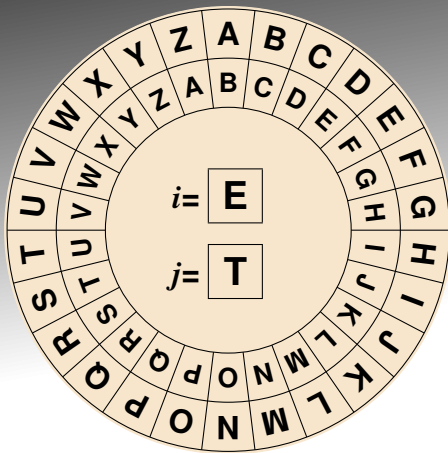
Bxth--

# Wie verschlüsselt man heute?



RC4

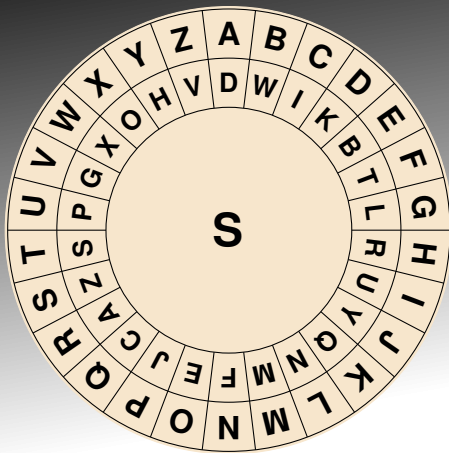
- verschlüssele mit  $S[T] = B$
- vertausche  $S[i] = S$  mit  $S[j] = B$



Enigma

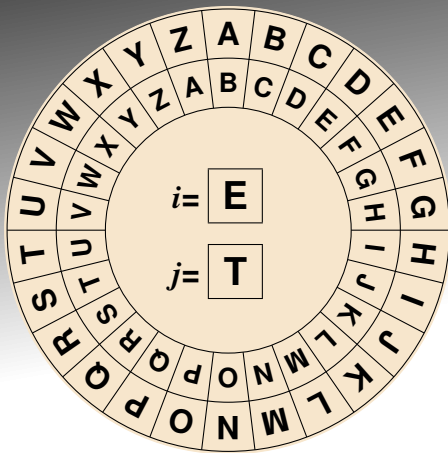
Bxth--

# Wie verschlüsselt man heute?



RC4

- verschlüssele mit  $S[T] = B$
- vertausche  $S[i] = S$  mit  $S[j] = B$

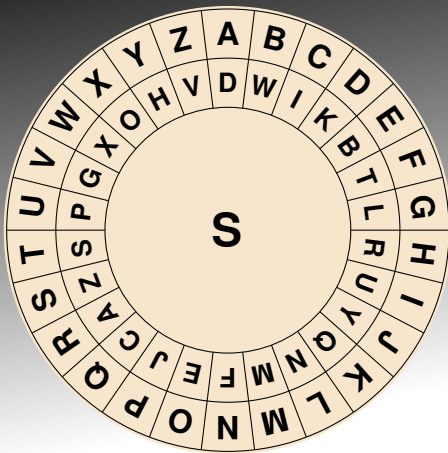


Enigma

Bxth--

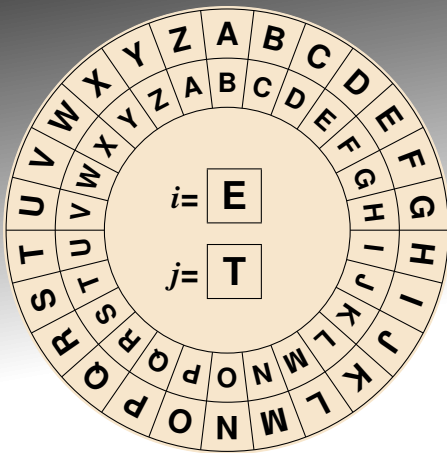


# Wie verschlüsselt man heute?



RC4

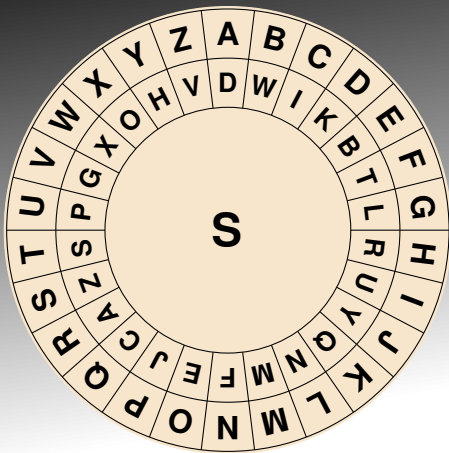
- vertausche  $S[i] = S$  mit  $S[j] = B$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

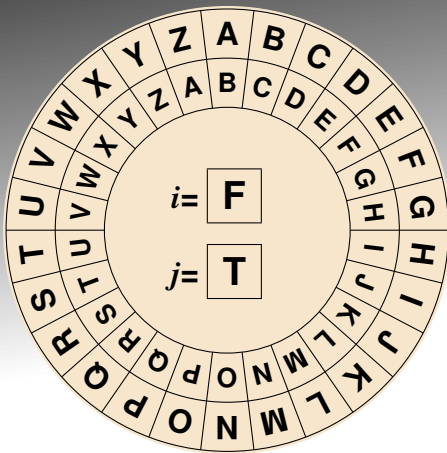
Bxth--

# Wie verschlüsselt man heute?



RC4

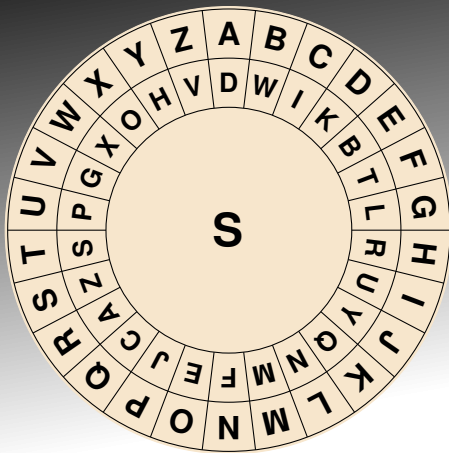
- vertausche  $S[i] = S$  mit  $S[j] = B$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

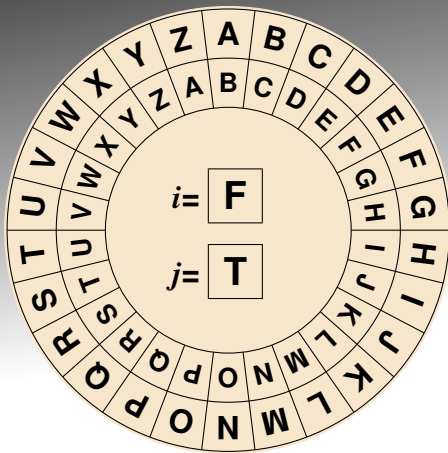
Bxth--

# Wie verschlüsselt man heute?



RC4

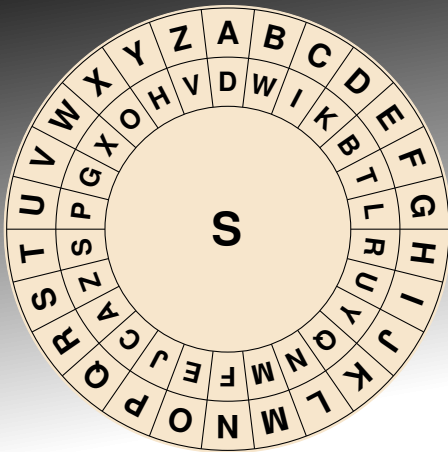
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$



Enigma

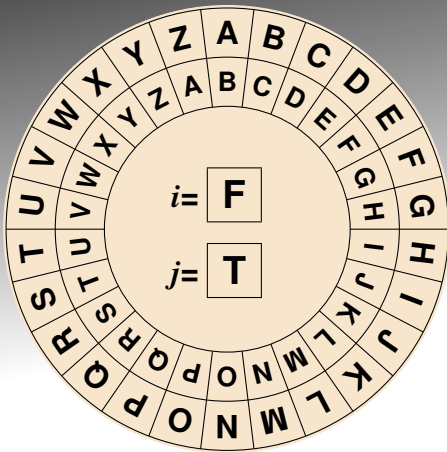
Bxth--

# Wie verschlüsselt man heute?



RC4

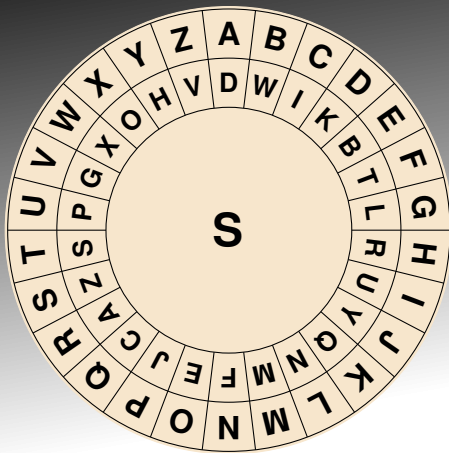
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

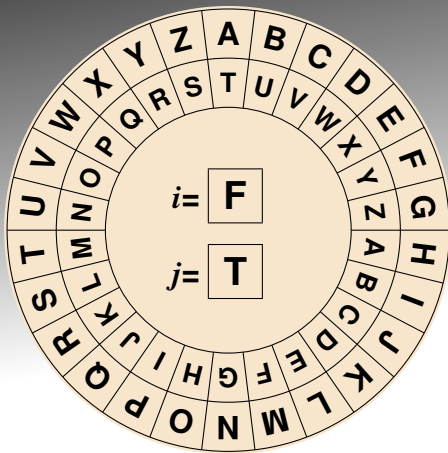
Bxth--

# Wie verschlüsselt man heute?



RC4

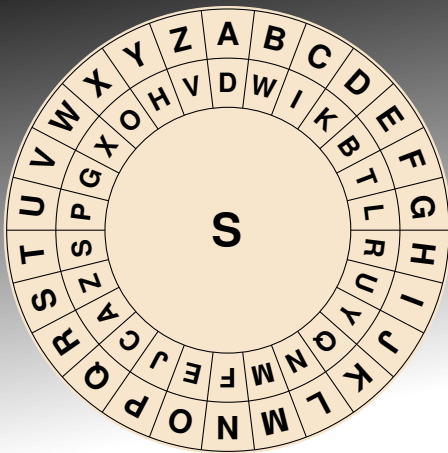
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

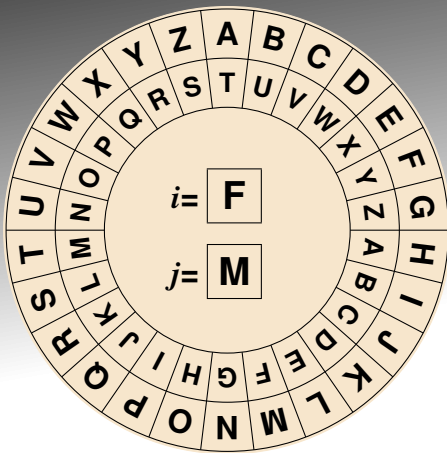
Bxth--

# Wie verschlüsselt man heute?



RC4

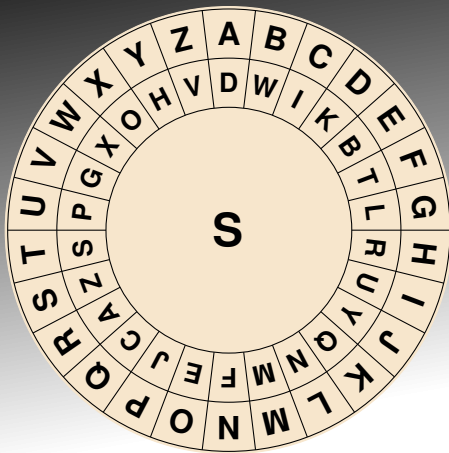
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = T$



Enigma

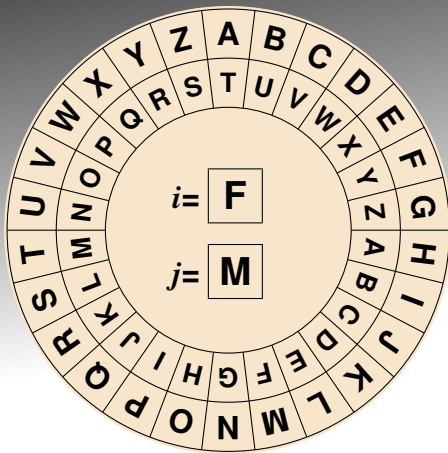
Bxth--

# Wie verschlüsselt man heute?



RC4

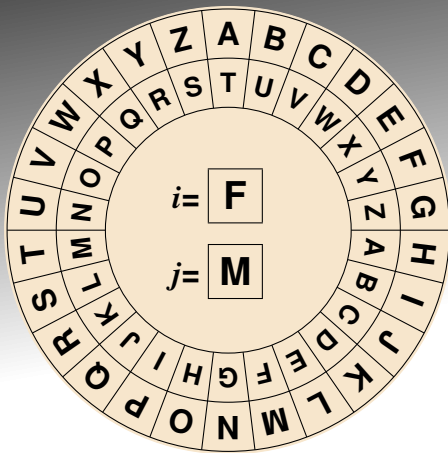
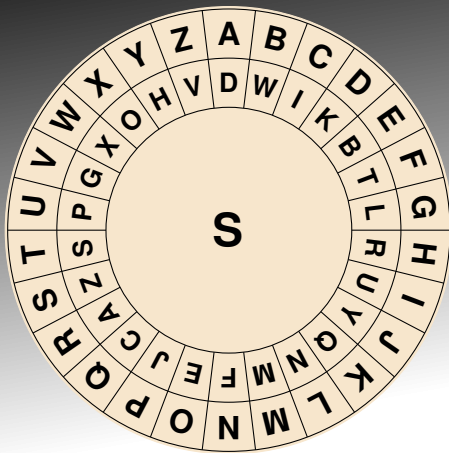
- Erhöhe  $j$  um  $S[i] = T$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

Bxth--

# Wie verschlüsselt man heute?



RC4

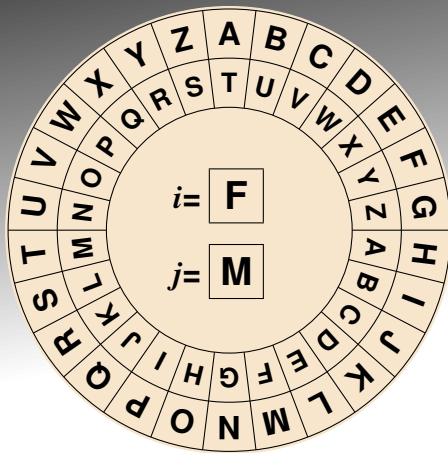
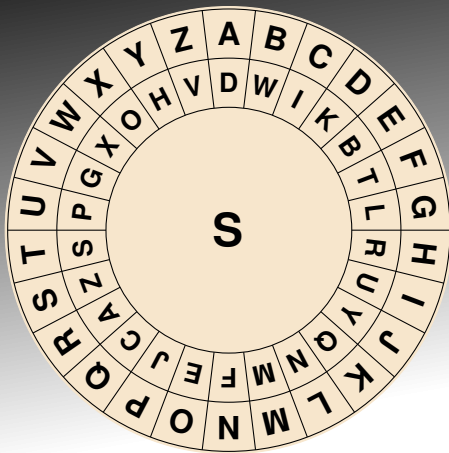
- Erhöhe  $j$  um  $S[i] = T$
- berechne  $S[j] = M$ , erhöht um  $S[i] = T$

Enigma

Bxth--



# Wie verschlüsselt man heute?



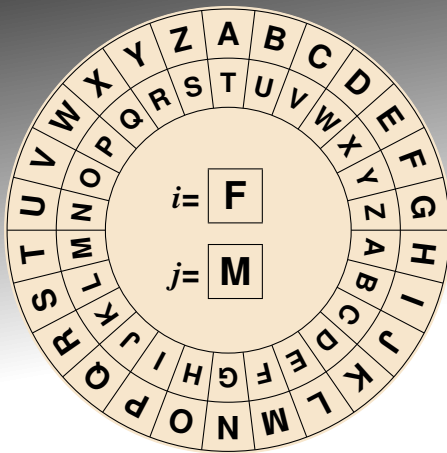
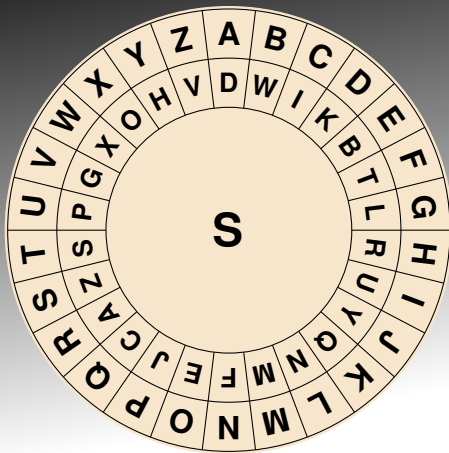
RC4

- Erhöhe  $j$  um  $S[i] = T$
  - berechne  $S[j] = M$ , erhöht um  $S[i] = T$
- Ergebnis: F

Enigma

Bxth--

# Wie verschlüsselt man heute?



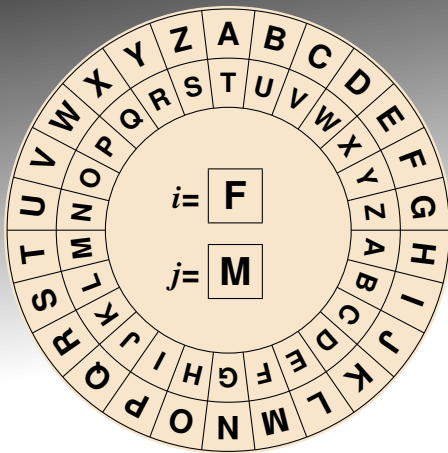
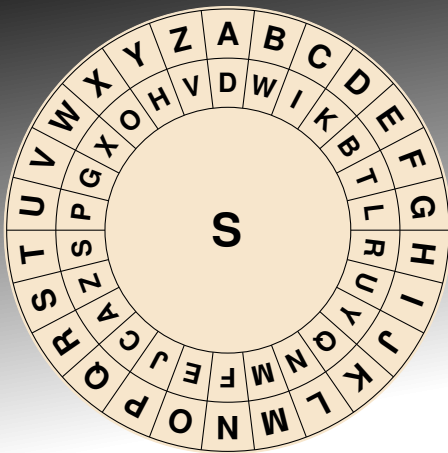
RC4

- berechne  $S[j] = M$ , erhöht um  $S[i] = T$   
Ergebnis: F
- verschlüssele mit  $S[F]$

Enigma

Bxth--

# Wie verschlüsselt man heute?



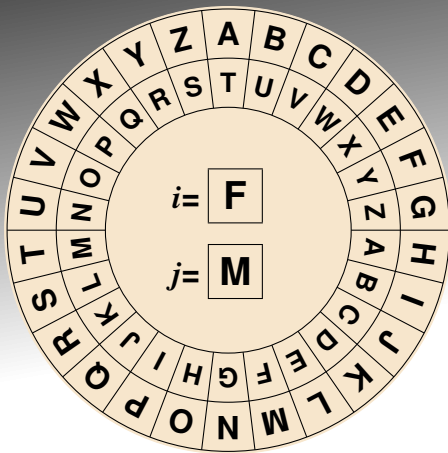
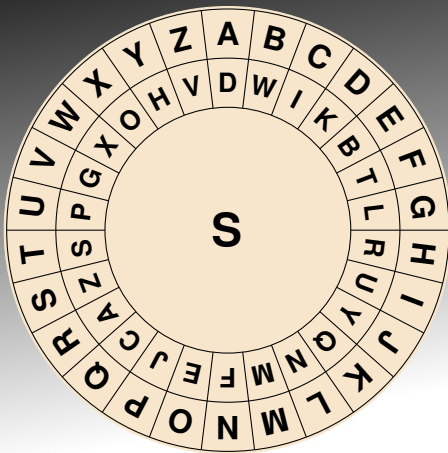
RC4

- berechne  $S[j] = M$ , erhöht um  $S[i] = T$   
Ergebnis: F
- verschlüsse mit  $S[F] = T$

Enigma

Bxth--

# Wie verschlüsselt man heute?



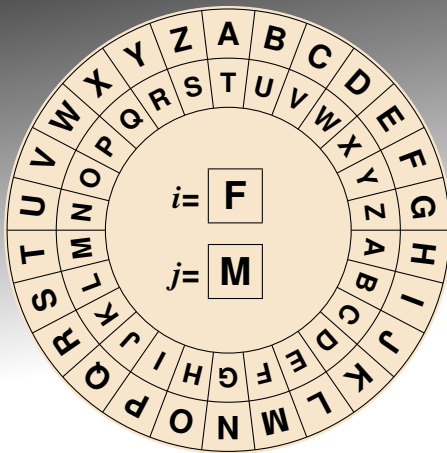
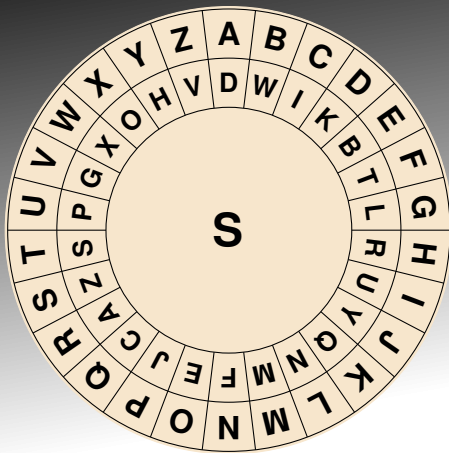
RC4

- berechne  $S[j] = M$ , erhöht um  $S[i] = T$   
Ergebnis: F
- verschlüsse mit  $S[F] = T$

Enigma

Bxth--

# Wie verschlüsselt man heute?

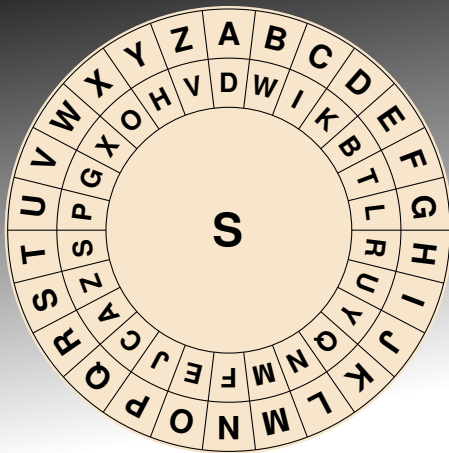


RC4

- berechne  $S[j] = M$ , erhöht um  $S[i] = T$   
Ergebnis: F
- verschlüsse mit  $S[F] = T$

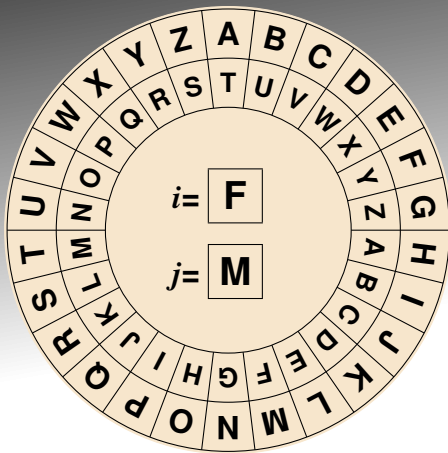
Enigma  
Bxthf-

# Wie verschlüsselt man heute?



RC4

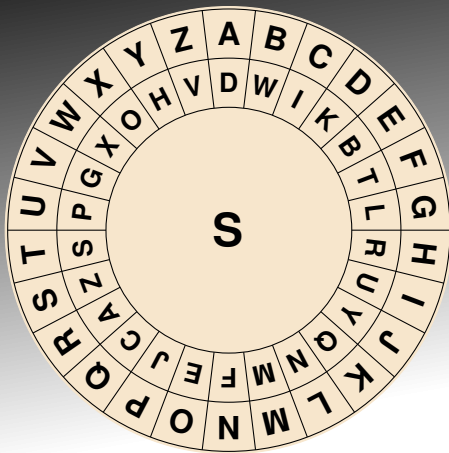
- verschlüssele mit  $S[F] = T$
- vertausche  $S[i]$  mit  $S[j]$



Enigma

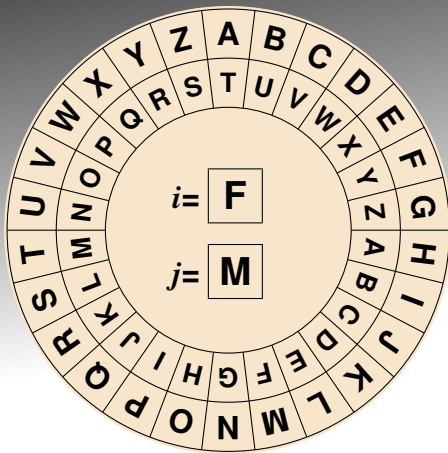
Bxthf-

# Wie verschlüsselt man heute?



RC4

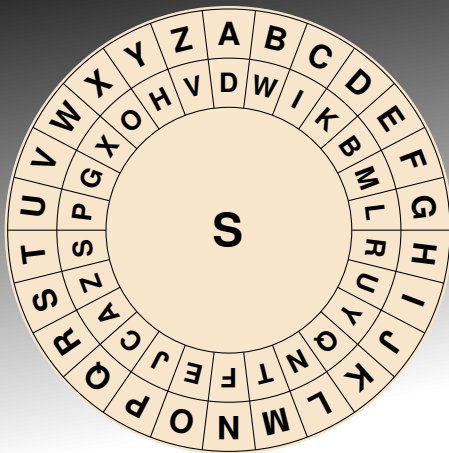
- verschlüssele mit  $S[F] = T$
- vertausche  $S[i] = T$  mit  $S[j] = M$



Enigma

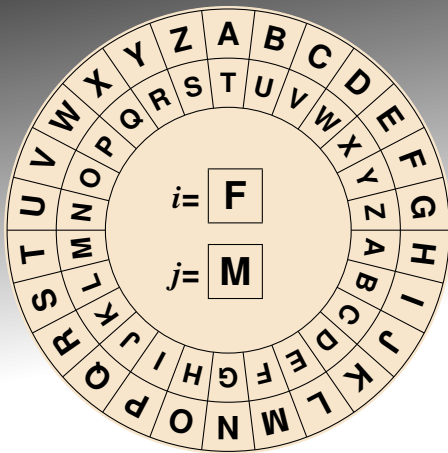
Bxthf-

# Wie verschlüsselt man heute?



RC4

- verschlüssele mit  $S[F] = T$
- vertausche  $S[i] = T$  mit  $S[j] = M$

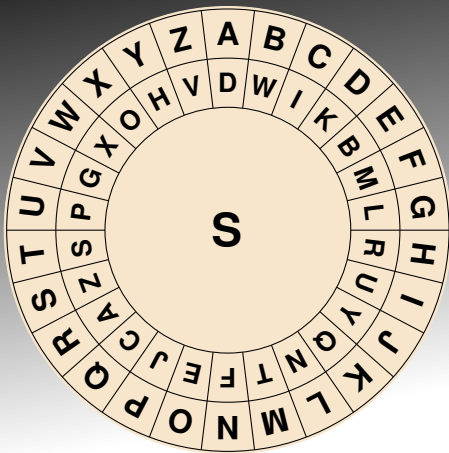


Enigma

Bxthf-

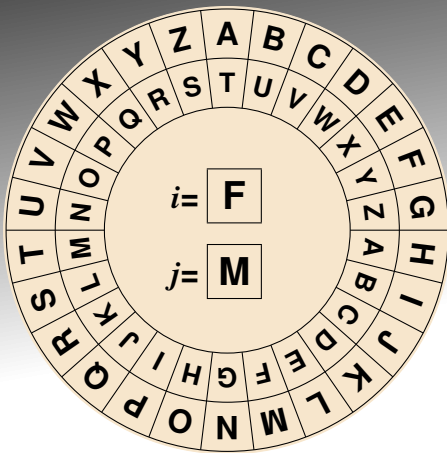


# Wie verschlüsselt man heute?



RC4

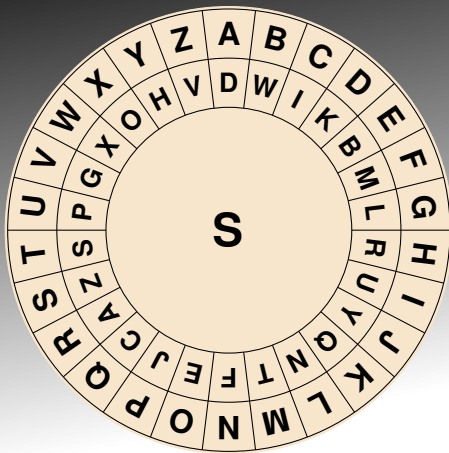
- vertausche  $S[i] = T$  mit  $S[j] = M$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

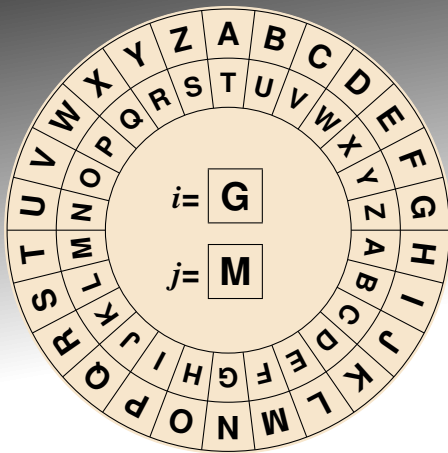
Bxthf-

# Wie verschlüsselt man heute?



RC4

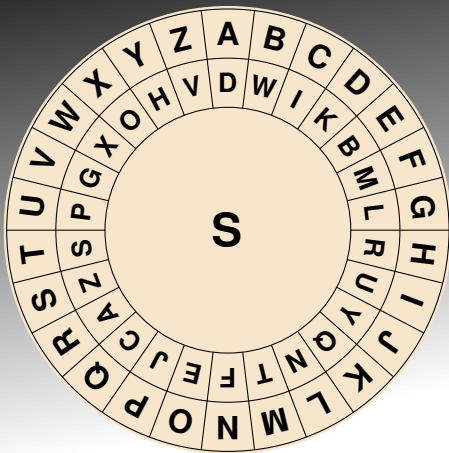
- vertausche  $S[i] = T$  mit  $S[j] = M$
- Nächster Buchstabe.  
Erhöhe  $i$



Enigma

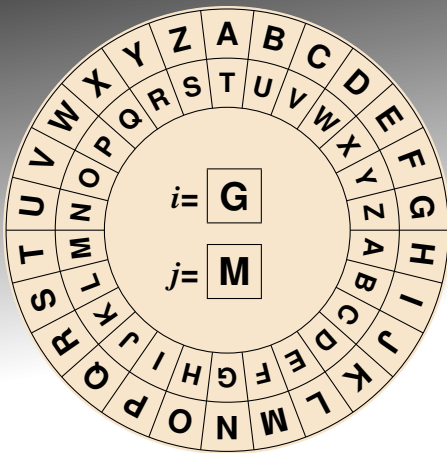
Bxthf-

# Wie verschlüsselt man heute?



RC4

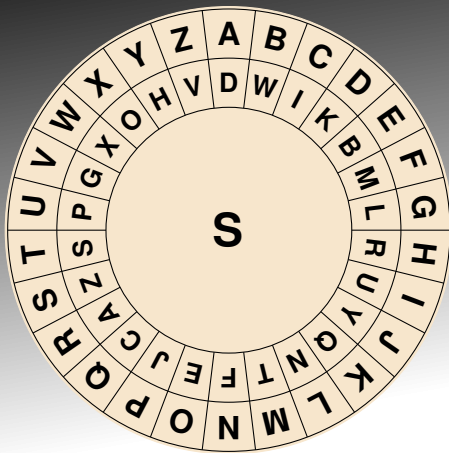
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$



Enigma

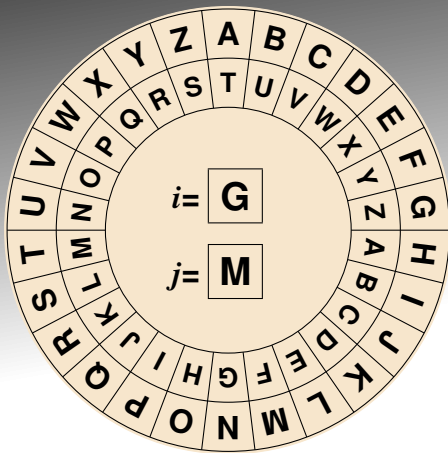
Bxthf-

# Wie verschlüsselt man heute?



RC4

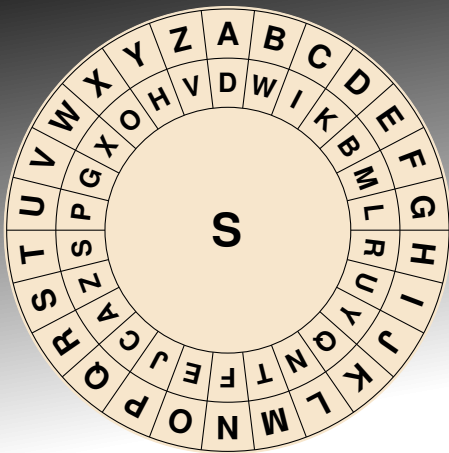
- Nächster Buchstabe.  
Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = L$



Enigma

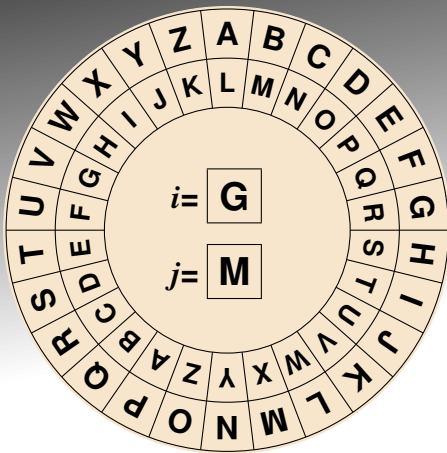
Bxthf-

# Wie verschlüsselt man heute?



RC4

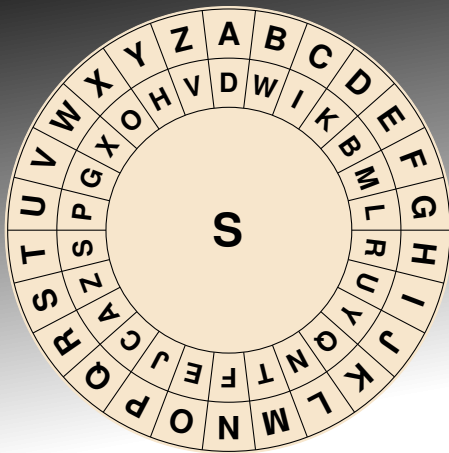
- Nächster Buchstabe. Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = L$



Enigma

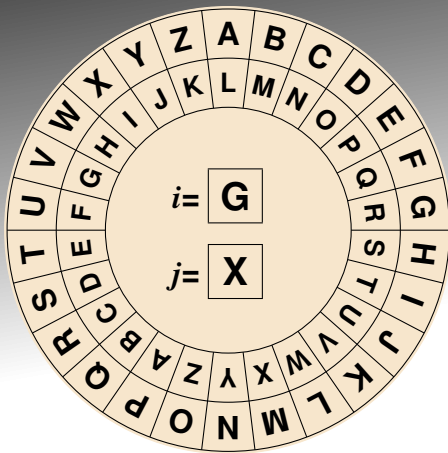
Bxthf-

# Wie verschlüsselt man heute?



RC4

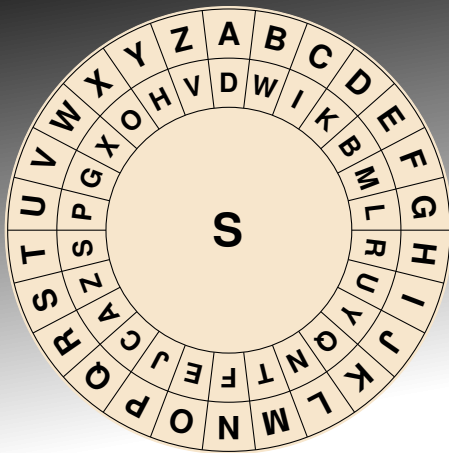
- Nächster Buchstabe. Erhöhe  $i$
- Erhöhe  $j$  um  $S[i] = L$



Enigma

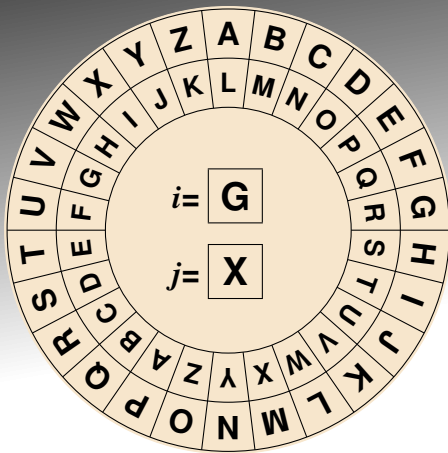
Bxthf-

# Wie verschlüsselt man heute?



RC4

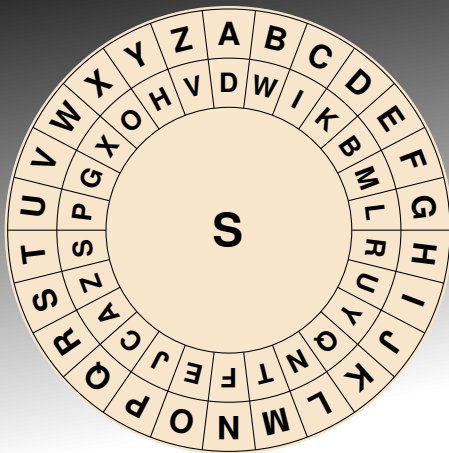
- Erhöhe  $j$  um  $S[i] = L$
- berechne  $S[j]$ , erhöht um  $S[i]$



Enigma

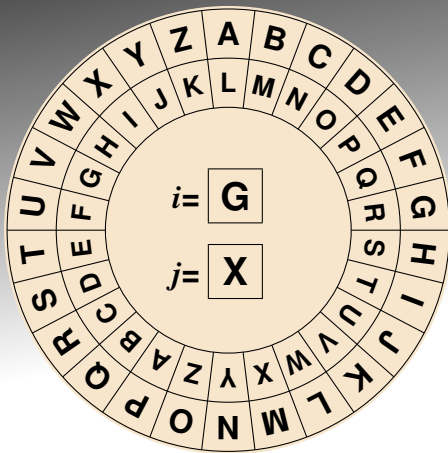
Bxthf-

# Wie verschlüsselt man heute?



RC4

- Erhöhe  $j$  um  $S[i] = L$
- berechne  $S[j] = O$ , erhöht um  $S[i] = L$

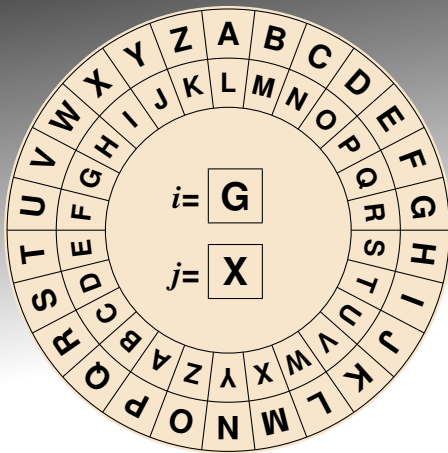
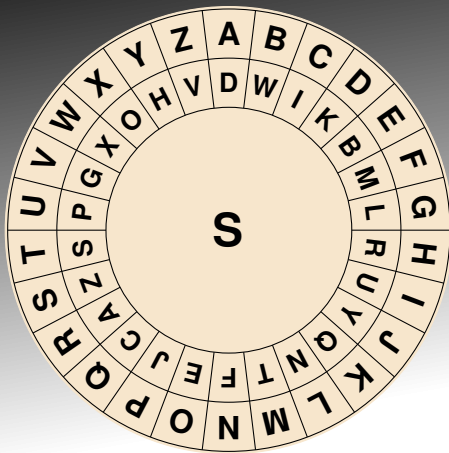


Enigma

Bxthf-



# Wie verschlüsselt man heute?



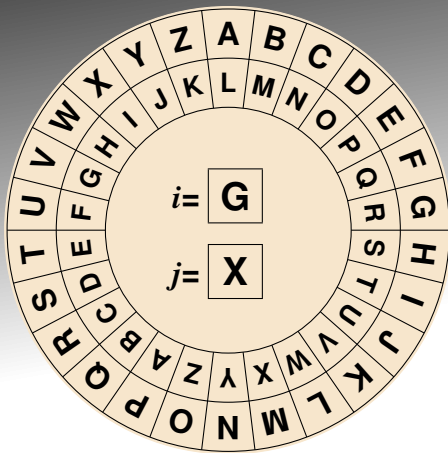
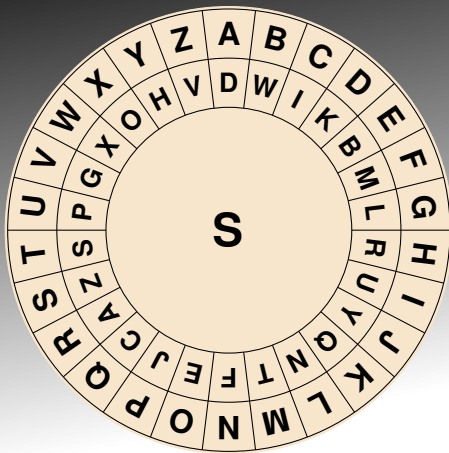
RC4

- Erhöhe  $j$  um  $S[i] = L$
- berechne  $S[j] = O$ , erhöht um  $S[i] = L$   
Ergebnis: Z

Enigma

Bxthf-

# Wie verschlüsselt man heute?

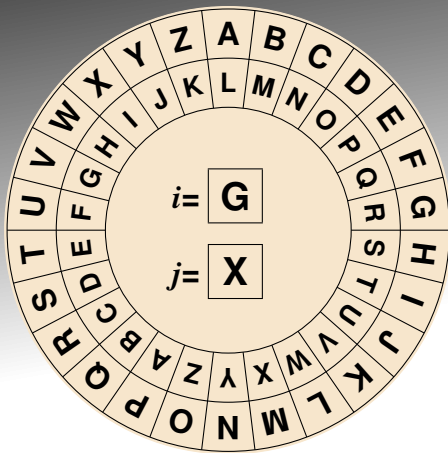
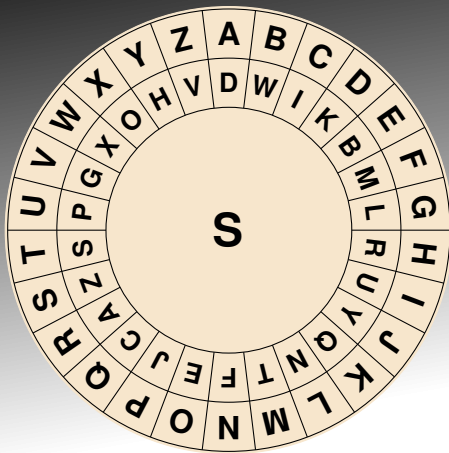


RC4

- berechne  $S[j] = O$ , erhöht um  $S[i] = L$   
Ergebnis: Z
- verschlüssele mit  $S[Z]$

Enigma  
Bxthf-

# Wie verschlüsselt man heute?



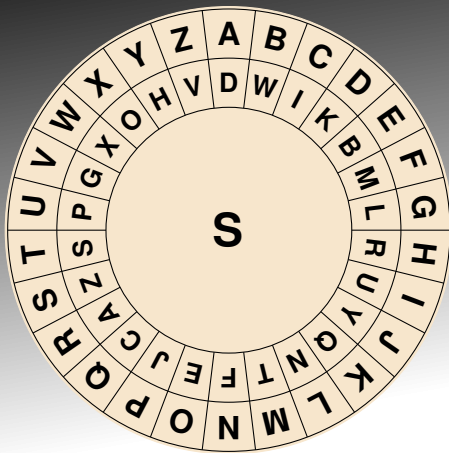
RC4

- berechne  $S[j] = O$ , erhöht um  $S[i] = L$   
Ergebnis: Z
- verschlüsse mit  $S[Z] = V$

Enigma

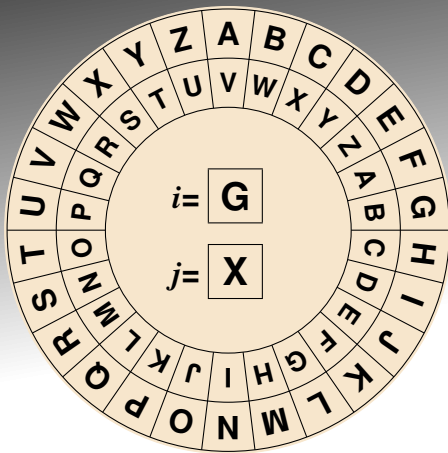
Bxthf-

# Wie verschlüsselt man heute?



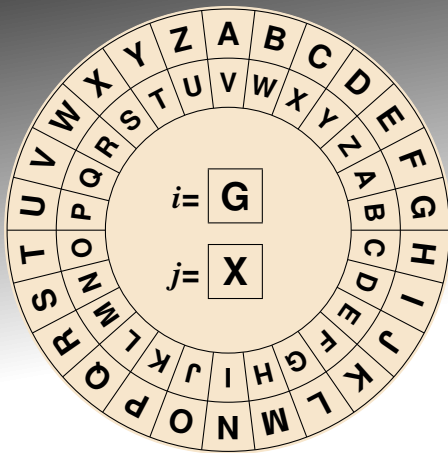
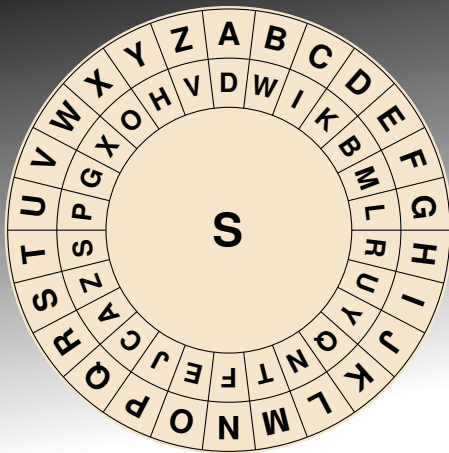
RC4

- berechne  $S[j] = O$ , erhöht um  $S[i] = L$   
Ergebnis:  $Z$
- verschlüsse mit  $S[Z] = V$



Enigma  
Bxthf-

## Wie verschlüsselt man heute?



# RC4

- berechne  $\mathbf{S}[j] = \mathbf{O}$ , erhöht um  $\mathbf{S}[i] = \mathbf{L}$   
Ergebnis:  $\mathbf{Z}$
- verschlüssele mit  $\mathbf{S}[\mathbf{Z}] = \mathbf{V}$

Enigma  
Bxthfv

# Wie verschlüsselt man heute?

## RC4

- Erhöhe  $i$
- Erhöhe  $j$  um  $S[i]$
- berechne  $S[j]$ , erhöht um  $S[i]$   
Ergebnis:  $k$
- verschlüssele mit  $S[k]$
- vertausche  $S[i]$  mit  $S[j]$
- Nächster Buchstabe.

- sehr einfach
- bis 2015: Verschlüsselung von Webseiten, WLAN, Fernwartung
- nicht mehr als sicher eingestuft

# Wie verschlüsselt man heute?

## Verschlüsselungsverfahren:

Enigma	DES	RC4	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

# Wie verschlüsselt man heute?

## Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...



# Wie verschlüsselt man heute?

## Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

### **Problem:**

Schlüssel sicher übertragen

# Wie verschlüsselt man heute?

## Symmetrische Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

**Problem:** gleicher Schlüssel zum Verschlüsseln und zum Entschlüsseln  
Schlüssel sicher übertragen

# Wie verschlüsselt man heute?

## Symmetrische Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

**Problem:** gleicher Schlüssel zum Verschlüsseln und zum Entschlüsseln  
Schlüssel sicher übertragen

**Lösung:** verschiedene Schlüssel zum Verschlüsseln und zum Entschlüsseln

# Wie verschlüsselt man heute?

## Symmetrische Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

**Problem:** gleicher Schlüssel zum Verschlüsseln und zum Entschlüsseln  
Schlüssel sicher übertragen

**Lösung:** verschiedene Schlüssel zum Verschlüsseln und zum Entschlüsseln  
öffentlich geheim

# Wie verschlüsselt man heute?

## Symmetrische Verschlüsselungsverfahren:

<del>Enigma</del>	<del>DES</del>	<del>RC4</del>	AES	3DES
IDEA	Blowfish	Twofish	CAST5	...

**Problem:** gleicher Schlüssel zum Verschlüsseln und zum Entschlüsseln  
Schlüssel sicher übertragen

**Lösung:** verschiedene Schlüssel zum Verschlüsseln und zum Entschlüsseln  
öffentlich geheim

```
graph TD; A[Schlüsselpaar] --> B[öffentlich]; A --> C[geheim];
```

Schlüsselpaar

## Asymmetrische Verschlüsselungsverfahren:

RSA	El-Gamal	cv25519	...
-----	----------	---------	-----

# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

PGP

GnuPG

K-9 Mail

...



# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

PGP

GnuPG

K-9 Mail

...

# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

PGP

GnuPG

K-9 Mail

...

GnuPG-Unterstützung für E-Mail-Programme:

Evolution      mutt      KMail  
Claws Mail      Thunderbird mit Enigmail  
Eudora mit EudoraGPG      Gpg4win  
GPGMail      ...

# Wie verschlüsselt man heute?

## Software für Verschlüsselung

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

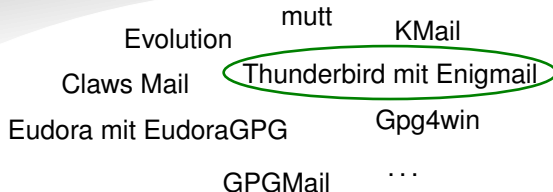
PGP

GnuPG

K-9 Mail

...

GnuPG-Unterstützung für E-Mail-Programme:



# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Anleitung

- E-Mail-Programm installieren  
(z. B. Thunderbird)
- Unterstützung für Verschlüsselung installieren  
(z. B. Enigmail)
- Schlüsselpaar erzeugen
- eigenen öffentlichen Schlüssel weitergeben  
→ verschlüsselter Empfang möglich
- andere öffentliche Schlüssel importieren  
→ verschlüsselter Versand möglich
- Für maximale Sicherheit:  
Schlüssel-Fingerprints abgleichen,  
Schlüssel gegenseitig zertifizieren

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln



# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln

Gegenmaßnahmen:

- HTML abschalten!

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EFail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln

Gegenmaßnahmen:

- HTML abschalten!
- Updates für E-Mail-Programme

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EMail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln

Gegenmaßnahmen:

- HTML abschalten!
- Updates für E-Mail-Programme

→ Die eigentliche Verschlüsselung ist sicher.  
Sicherheitslücken in E-Mail-Programmen im Rahmen des „Üblichen“

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EMail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln

Gegenmaßnahmen:

- HTML abschalten!
- Updates für E-Mail-Programme

→ Die eigentliche Verschlüsselung ist sicher.  
Sicherheitslücken in E-Mail-Programmen im Rahmen des „Üblichen“

→ Keine Panik!

# Wie verschlüsselt man heute?

## Software für Verschlüsselung: Die EMail-Sicherheitslücke

2 Standards:

- S/MIME – zentral geregelt
- OpenPGP – dezentral

Beide sind betroffen!

OpenPGP weniger.

Gefahren:

- „Man kann auch Malware verschlüsselt versenden.“
- konkret: E-Mail-Programm dazu bringen, Nachrichten für Dritte zu entschlüsseln

Gegenmaßnahmen:

- HTML abschalten!
- Updates für E-Mail-Programme

- Die eigentliche Verschlüsselung ist sicher.  
Sicherheitslücken in E-Mail-Programmen im Rahmen des „Üblichen“
- Keine Panik – aber auch kein Leichtsinn!

# verschlüsselt entschlüsselt

– wie es geht  
und wie man es selber macht

- ✓ Wie funktioniert die Enigma-Verschlüsselung?
- ✓ Wie konnte die Enigma-Verschlüsselung gebrochen werden?
- ✓ Wie verschlüsselt man heute?



Hochschule Bochum  
Bochum University  
of Applied Sciences



Campus  
Velbert/Heiligenhaus

DEUTSCHES SCHLOSS- UND BESCHLÄGEMUSEUM VELBERT   
[www.museum.velbert.de](http://www.museum.velbert.de)