

5 Relevanz informatischer Entwicklung

Ver- und Entschlüsseln von Informationen

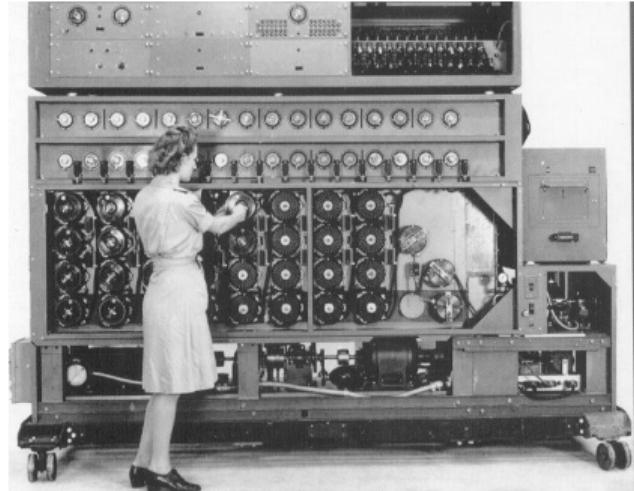
Marianne Maertens

Technische Universität Berlin

Wintersemester 2025/2026

Themen

- Wiederholung: Objektivität, Turing-Maschine
- Geschichte der Verschlüsselung
- Das RSA-Kryptosystem
 - Primzahltests
 - Teilerfremdheit
 - Erweiterter Euklidischer Algorithmus
 - Modularer Kehrwert
- Relevanz



Themen

- Wiederholung: Objektivität, Turing-Maschine
- Geschichte der Verschlüsselung
- Das RSA-Kryptosystem
 - Primzahltests
 - Teilerfremdheit
 - Erweiterter Euklidischer Algorithmus
 - Modularer Kehrwert
- Relevanz



Objektivität

klassische Wissenschaftstheorie:

- Objektivität verlangt, dass individuelle Biases durch methodische Verfahren so weit wie möglich kontrolliert werden, sodass Ergebnisse intersubjektiv prüfbar bleiben

Wissen(schaft) ist situiert (Situated knowledge, Haraway, 1988)

- Objektivität garantiert, dass wissenschaftliche Erkenntnisse universell gültig sind, unabhängig von historischen oder kulturellen Kontexten. (*falsch*)

Wissenschaft findet immer im historischen Kontext statt



Der Fall Alan Turing (ARTE, <https://www.youtube.com/watch?v=Rm9wvo2PSoI>)

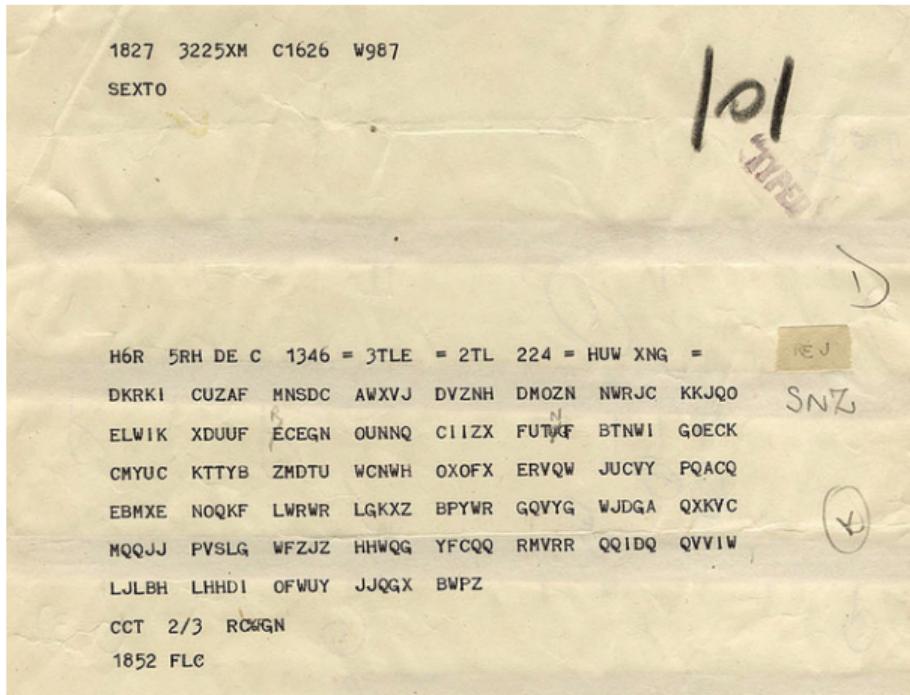
Enigma “knacken”

IRGENDEIN
TEXT →



→ DMZO NDJE
QQLI W

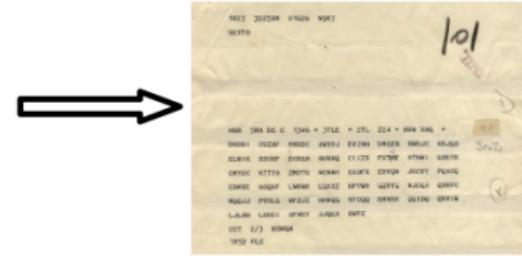
Enigma “knacken”



[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))

Enigma “knacken”

IRGENDEIN
TEXT →



Funktion verstehen durch Analyse des Aufbaus

Enigma “knacken”

?



MEB	SHN	DE	C	1245	=	376	224	=	HN	380	=
EINKE	OSZET	PHODC	AHEUJ	SZVHN	THDNE	SHHUC	KHEUP				
ELKHE	ZDHPF	PSDKE	WURQ	CLIXX	FUTRR	HTRH	GROK				
ORHAC	KTTFS	ZDHTV	WOMH	UFXPA	CEHPR	JHCHY	PENAS				
EDRHO	HADP	LHME	LOHIZ	OPTHR	WHTTA	RASH	GRPC				
MUGU	PTTLS	WEZZ	WMBB	THFQQ	THHHH	UDTIN	OFKIN				
LALHE	LBHBB	GWHT	HAJCH	UNFZ							
COT	E/F	HMKA									

tägliche Änderung der Konfiguration der Maschine

Enigma “knacken”

Heeres-Stabs-Maschinenschlüssel Süd Nr. 70												Nr. 0027												
Datum	Walzenlage			Ringstellung			Steckerverbindungen						Kenngruppen											
	I	II	III	I	II	III	IV	V	VI	VII	VIII	VII	VIII	V	VII	VIII	V	VII	VIII	V	VII	VIII	V	VII
70. 31.	III	I	IV	16	03	24	HZ	YR	I	F	QT	JN	GC	AP	UX	BD	KS	VZW	WBH	NUF	REV			
70. 30.	V	IV	I	26	22	25	BL	AN	GO	IY	VE	MX	SW	QZ	PO	UK	FSE	FUG	RDQ	BDO				
70. 29.	III	IV	V	14	18	05	CV	WK	MS	UP	OJ	DZ	XA	LR	IY	HN	HY	FSG	WSA	WHR				
70. 28.	I	II	V	11	10	02	ZJ	BP	VK	UG	LW	QX	SA	MT	ED	YH	YOR	XOF	EXQ	POZ				
70. 27.	V	I	III	20	07	15	KZ	FD	UP	MG	XS	OC	WR	EB	YL	IA	IWC	AUQ	FV1	LUA				
70. 26.	II	V	IV	01	02	21	GS	VC	IL	HR	JN	XO	TO	HD	PF	EU	CLE	MYK	ESL	MQG				
70. 25.	I	V	II	07	08	19	BD	WN	CX	TI	KS	MO	UH	VF	ZJ	LG	PKW	MWN	BFW	VBL				
70. 24.	IV	II	I	17	19	08	GU	OE	XA	CI	MS	HY	JN	PF	KL	ZW	HLO	CHV	LQG	TUP				
70. 23.	II	V	III	13	24	07	XP	VB	ZM	HW	Q1	DS	LC	UG	PK	EO	XQH	PCU	SQL	GON				
70. 22.	III	II	I	18	16	01	Q1	HE	HP	MU	AR	YL	KO	GJ	XV	ZN	TAL	TUQ	SNJ	RER				
70. 21.	V	II	IV	23	09	26	VQ	IN	EB	PY	ZX	GH	HM	RL	CW	SK	JIB	YSE	BCE	IFB				
70. 20.	V	I	II	25	25	14	PV	EY	MN	US	KJ	IM	WD	XL	GT	BZ	EHO	KFG	QGD	KKT				
70. 19.	I	III	II	06	20	23	JE	FW	KK	OC	PQ	MU	US	DB	OY	VE	TAV	MQY	RUC	ENL				
70. 18.	I	IV	III	22	26	22	XK	ZS	QU	#A	TV	I	HD	YO	PR	ML	GMB	OUY	SLS	VDT				
70. 17.	III	I	II	24	21	18	JN	GP	CB	KS	WU	ZL	OJ	VR	DF	YH	WEJ	YRC	RRO	UNX				
70. 16.	V	IV	II	19	06	06	UQ	BO	EI	MO	HF	OT	WZ	CP	LA	SV	TRD	RTP	PTX	TJP				
70. 15.	III	V	IV	04	13	13	XV	KF	YS	PI	UE	LJ	AW	QH	CR	GZ	UYE	PJP	SLU	GMJ				
70. 14.	I	II	IV	09	11	17	EY	UR	IQ	ZK	CF	WN	LP	ON	HA	VS	UOD	BVI	HOO	UKV				
70. 13.	V	III	II	05	25	09	LY	XU	VN	OR	RC	PD	IA	EZ	GT	KQ	XSG	BSD	RGX	OPG				
70. 12.	I	V	IV	03	08	12	XW	KB	IZ	UN	DA	MP	LY	HJ	RV	QP	OKQ	UVF	UVL	SGB				
70. 11.	V	I	IV	10	02	20	DA	IG	SY	GI	GE	XW	MU	PZ	HQ	TJ	NPD	BYC	CAS	LQM				
70. 10.	II	IV	V	16	07	16	ZT	PD	MR	XT	BB	ES	IL	HO	QO	WJN	TMW	TER	RPM					
70. 9.	IV	II	III	26	09	11	ZU	PD	MR	XT	BB	AC	ES	IL	HO	QO	AJN	TMW	TER	RPM				
70. 8.	I	V	III	20	10	10	ZD	YQ	AK	IS	RB	WS	CU	FL	WW	NP	LED	XUS	WSA	BMC				
70. 7.	III	IV	I	01	19	24	AH	GM	OV	RP	BP	EJ	KC	SZ	UI	NQ	MCH	CWO	IWW	STS				
70. 6.	III	II	V	07	14	10	VN	AY	CM	ZG	XU	RT	LP	HS	IF	KQ	MDT	SXF	LXI	BPR				
70. 5.	II	III	IV	04	12	18	CA	YW	HO	SB	KP	ID	LT	VN	GZ	XW	YOK	FCS	FOR	XNN				
70. 4.	II	I	V	14	08	19	HD	PY	XW	PU	IQ	LK	WZ	JC	EO	RQ	XIL	SWB	OPV	LPP				
70. 3.	IV	V	II	25	07	14	OM	QS	BT	KJ	FY	VN	RZ	HA	IW	UO	EXQ	SEY	CCN	UPY				
70. 2.	II	I	III	06	23	03	KV	FA	NT	UW	ZD	CM	JR	LE	XI	PY	BJV	EAX	AFR	FOR				
70. 1.	IV	III	V	19	22	17	GZ	UD	TY	KN	PW	RH	EA	SC	QP	MO	IVM	YRW	VIM	URY				

[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))

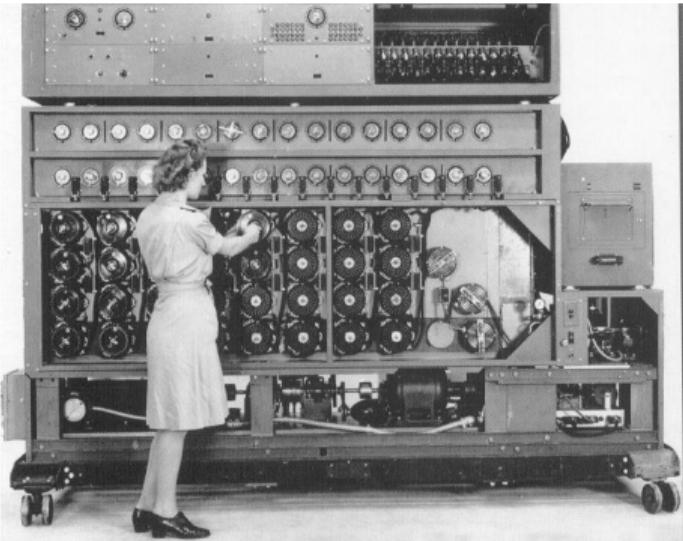
- Walzenlage (3 aus 5)

- Walzenstellung (26 Positionen, A-Z)

- Ringstellung (26)
- Steckerverbindungen
- ! Kombinatorik

Enigma “knacken”

Datum	Walzenlage		Ringstellung		Steckerverbindungen												Kenngruppen							
	III	I	IV	V	16	03	24	HZ	YR	JF	QT	JN	GC	AP	UX	BD	KS	vzw	wbh	nuf	rev	fze	fug	rdq
70	V	IV	I	26	22	25	BL	AN	GO	TY	VE	MX	SW	QZ	PO	UK	cle	myk	esl	maq	zce	gut	zce	zce
70	III	IV	V	14	18	05	CV	WK	MS	UP	OJ	DZ	XA	LR	YI	HN	hyv	fso	ska	whr	zce	zce	zce	zce
70	I	II	V	11	10	02	ZJ	BP	VK	UG	LW	QX	SA	MT	ED	YH	yor	xof	axq	ooz	zce	zce	zce	zce
70	V	I	III	20	07	15	KZ	FD	UP	MG	XG	OC	WR	EB	YL	IA	lwo	axq	fvi	luu	zce	zce	zce	zce
70	II	V	IV	01	02	21	GS	VC	IL	HR	JN	XO	TQ	HD	PF	EU	ole	myk	esl	maq	zce	zce	zce	zce
70	I	V	II	07	08	19	BD	WN	CX	TI	KS	MQ	UH	VF	JZ	LG	pkw	nwn	bfn	vbl	zce	zce	zce	zce
70	IV	II	I	17	19	08	GU	OE	XA	CI	MS	HY	JN	PF	KL	ZW	hlo	chv	lbg	tup	zce	zce	zce	zce
70	II	V	III	13	24	07	XP	VB	ZM	HW	Q1	DS	LC	UG	PK	EO	xqa	pca	sol	gen	zce	zce	zce	zce
70	III	II	I	18	16	01	Q1	HE	HP	MU	AR	YL	KO	GJ	XV	ZN	tal	tuq	mnj	rak	zce	zce	zce	zce
70	II	V	IV	23	09	26	VQ	IN	EB	PY	ZX	GJ	HM	RL	CW	SK	jlb	yse	bce	ifb	zce	zce	zce	zce
70	V	I	IV	25	25	14	PV	EY	MN	US	KJ	IM	WD	XL	GT	BZ	eho	kfg	oqd	kkt	zce	zce	zce	zce
70	III	I	III	06	20	23	JE	FW	KK	OC	PQ	MH	US	DB	OY	VE	tav	mqy	ruc	ens	zce	zce	zce	zce
70	I	IV	III	22	26	22	XK	ZS	QU	#A	TV	IS	HD	YO	PR	ML	gmb	oyx	zls	vdt	zce	zce	zce	zce
70	III	I	II	24	21	18	JN	GP	CB	KS	WU	ZL	OI	VR	DF	YH	wej	yro	rro	uhx	zce	zce	zce	zce
70	V	IV	II	19	06	06	UQ	BO	EI	MG	HF	OT	WZ	CP	LA	SV	trd	rtp	pix	tjp	zce	zce	zce	zce
70	III	V	IV	04	13	13	XV	KF	YS	PI	UE	LJ	AW	QH	CR	GZ	uye	ppj	eliu	gmj	zce	zce	zce	zce
70	I	II	IV	09	11	17	EY	UR	IQ	ZK	CF	WL	ON	HA	VS	uod	bvi	ho	ukv	zce	zce	zce	zce	
70	III	V	III	05	25	09	LY	XU	VN	OR	RC	PD	IA	EZ	GT	NQ	xsg	bsd	rgx	cpg	zce	zce	zce	zce
70	II	V	IV	03	02	12	XB	KB	IZ	UN	DA	MP	LY	HJ	RV	QP	okq	uvf	uvf	sgb	zce	zce	zce	zce
70	II	I	V	10	02	20	DA	IG	SY	GE	CE	XM	MU	PF	HQ	TJ	npd	byz	cas	lqm	zce	zce	zce	zce
70	III	II	IV	16	02	16	TD	PD	MR	JK	HL	WZ	WZ	WZ	WZ	WZ	zce	zce	zce	zce	zce	zce	zce	zce
70	IV	II	III	26	09	11	ZU	PD	MR	XT	BM	AC	BS	IL	HO	QO	ajh	lmw	ter	rsw	zce	zce	zce	zce
70	I	V	III	20	10	10	ZD	YQ	AK	II	RB	VS	CU	FL	WM	NP	lad	xuz	eva	hmc	zce	zce	zce	zce
70	III	IV	I	01	19	24	AH	GM	OV	RP	BP	EJ	XG	SZ	UI	NQ	mob	cwo	lmw	sts	zce	zce	zce	zce
70	III	V	II	07	14	10	VN	AY	CM	ZG	XU	RT	LP	HS	IF	KQ	mdt	xfx	lxz	bpr	zce	zce	zce	zce
70	II	III	IV	04	12	18	CA	YH	HO	SB	KP	ID	LT	VN	GZ	XH	yok	fcs	for	xxn	zce	zce	zce	zce
70	4.	I	V	14	08	19	HD	PY	XN	PU	IK	LW	WZ	JC	EO	RQ	xil	swb	opv	lpp	zce	zce	zce	zce
70	3.	IV	V	25	07	14	OM	QS	BT	KJ	FY	VN	RZ	HA	IW	UD	sqx	sey	coc	upy	zce	zce	zce	zce
70	2.	II	I	06	23	03	KV	FA	NT	UW	ZD	CM	JR	LE	XI	PY	bjv	eax	off	for	zce	zce	zce	zce
70	L	IV	III	19	22	17	GZ	UD	TY	KN	PW	RH	EA	SC	QP	MO	rvm	yrw	vim	ury	zce	zce	zce	zce



[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))

- Turing-Bombe reduziert den effektiven Schlüsselraum
- Methode des wahrscheinlichen Wortes (crib)

Enigma “knacken”

Heeres-Stabs-Maschinenschlüssel Süd Nr. 70												Nr. 6022														
Datum	Walzenlage			Ringstellung			Steckerverbindungen						Kenngruppen													
	I	II	III	I	IV	V	16	03	24	HZ	YR	JF	QT	JN	GC	AP	UX	BD	KS	vzw	wbh	nuf	rev	fze	fug	rdq
70.	31.	III	I	IV	V	16	22	25	BL	AN	GO	TY	VE	MX	SW	QZ	PO	UK	hyv	fso	ska	whr	yor	xof	sqg	poz
70.	30.	III	IV	V	14	18	05	CV	WK	MS	UP	OJ	DZ	XA	LR	YI	HN	lwo	sqg	fvi	luu	cle	myk	esl	mag	
70.	29.	I	II	V	11	10	02	ZJ	BP	VK	UG	LW	QX	SA	MT	ED	YH	pkw	nwn	bff	vbl	hlo	chv	lgq	tup	
70.	28.	V	I	III	20	07	15	KZ	FD	UP	MG	XG	OC	WR	EB	YL	IA	xqa	pca	sol	gen	tal	tuq	mnj	rak	
70.	27.	II	V	IV	01	02	21	GS	VC	IL	HR	JN	XO	TQ	BD	PP	EU	jib	yss	bce	ifb	eho	kfg	oqd	kkt	
70.	26.	I	V	II	07	08	19	BD	WN	CX	TI	KS	MQ	UH	VF	JZ	LG	wje	oyc	sls	vdt	gmb	oyx	sls	vdt	
70.	25.	IV	II	I	17	19	08	GU	OE	XA	CI	MS	HY	JN	PF	KL	ZW	trd	rtp	pix	tjp	uwe	ppj	slu	gmj	
70.	24.	II	V	III	13	24	07	XP	ZB	ZM	HW	QI	DS	LC	UG	PK	EO	uod	bvi	hou	ukv	uog	uvf	uwl	sgb	
70.	23.	III	II	I	18	16	01	Q1	HE	HP	MU	AR	YL	KO	GJ	XV	ZN	xsg	bsd	rgx	cpg	okq	uvf	uwl	sgb	
70.	22.	V	II	IV	23	09	26	QV	IN	EB	PY	ZX	GJ	HM	RL	CW	SK	npd	byz	cse	lqm	zil	swb	opv	lpp	
70.	21.	V	I	IV	25	25	14	PV	EY	HN	US	KJ	IM	WD	XL	OT	BZ	ayn	lmw	ter	rpe	zil	swb	opv	lpp	
70.	20.	V	I	II	06	20	23	JZ	FW	XX	KC	PQ	MS	UD	GY	VE	tao	mqy	ruc	esl	ayn	lmw	ter	rpe		
70.	19.	I	III	II	22	26	22	XK	ZS	QU	KA	TV	IS	HD	YO	PR	ML	zod	oyc	sls	vdt	zod	oyc	sls	vdt	
70.	18.	I	IV	III	22	26	22	JN	GP	CB	KS	WU	ZL	OI	VR	DF	YH	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	17.	III	I	II	24	21	18	XK	GP	CB	KS	WU	ZL	OI	VR	DF	YH	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	16.	V	IV	II	19	06	06	UQ	BO	EI	MO	HP	OT	ZW	CP	LA	SV	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	15.	III	V	IV	04	13	13	XV	KF	YS	PI	UE	LJ	AW	QH	CR	GZ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	14.	I	II	IV	09	11	17	XY	UR	IQ	ZK	CF	WP	ON	HA	VS	trd	rtp	pix	tjp	trd	rtp	pix	tjp		
70.	13.	V	III	II	05	25	09	LY	XU	VN	OR	RC	PD	IA	EZ	GT	KQ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	12.	I	V	IV	03	02	12	XB	KB	IZ	UN	DA	MP	LY	RJ	RV	QP	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	11.	V	I	IV	16	02	20	DA	IG	SY	GE	XM	PZ	HQ	TJ	trd	rtp	pix	tjp	trd	rtp	pix	tjp			
70.	10.	II	V	IV	20	07	16	ZT	PD	IK	JI	WU	PD	IA	ED	GT	KQ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	9.	IV	II	III	26	09	11	ZU	PD	KR	XT	BM	AC	BS	IL	HO	QO	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	8.	I	V	III	20	10	10	ZD	YQ	AK	IE	RS	VS	CU	FL	WW	NP	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	7.	III	IV	I	01	19	24	AH	GM	OV	RP	BP	EJ	KC	SZ	UI	NQ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	6.	III	V	II	07	14	10	VN	AY	CM	ZG	ZU	XT	LT	HS	IF	KQ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	5.	III	III	IV	04	12	18	CA	YW	HO	SB	KP	ID	LT	VN	GZ	XB	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	4.	I	V	II	14	08	19	HD	PY	XU	PU	IQ	LK	WZ	JC	EO	RQ	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	3.	IV	V	II	25	07	14	QW	BT	KJ	FY	VN	RZ	HA	IW	UD	trd	rtp	pix	tjp	trd	rtp	pix	tjp		
70.	2.	V	I	III	06	23	03	KV	FA	NT	WD	ZD	CM	JR	LE	XI	PY	trd	rtp	pix	tjp	trd	rtp	pix	tjp	
70.	1.	IV	III	V	19	22	17	GZ	UD	TY	KN	PW	RH	EA	SC	QP	MO	trd	rtp	pix	tjp	trd	rtp	pix	tjp	

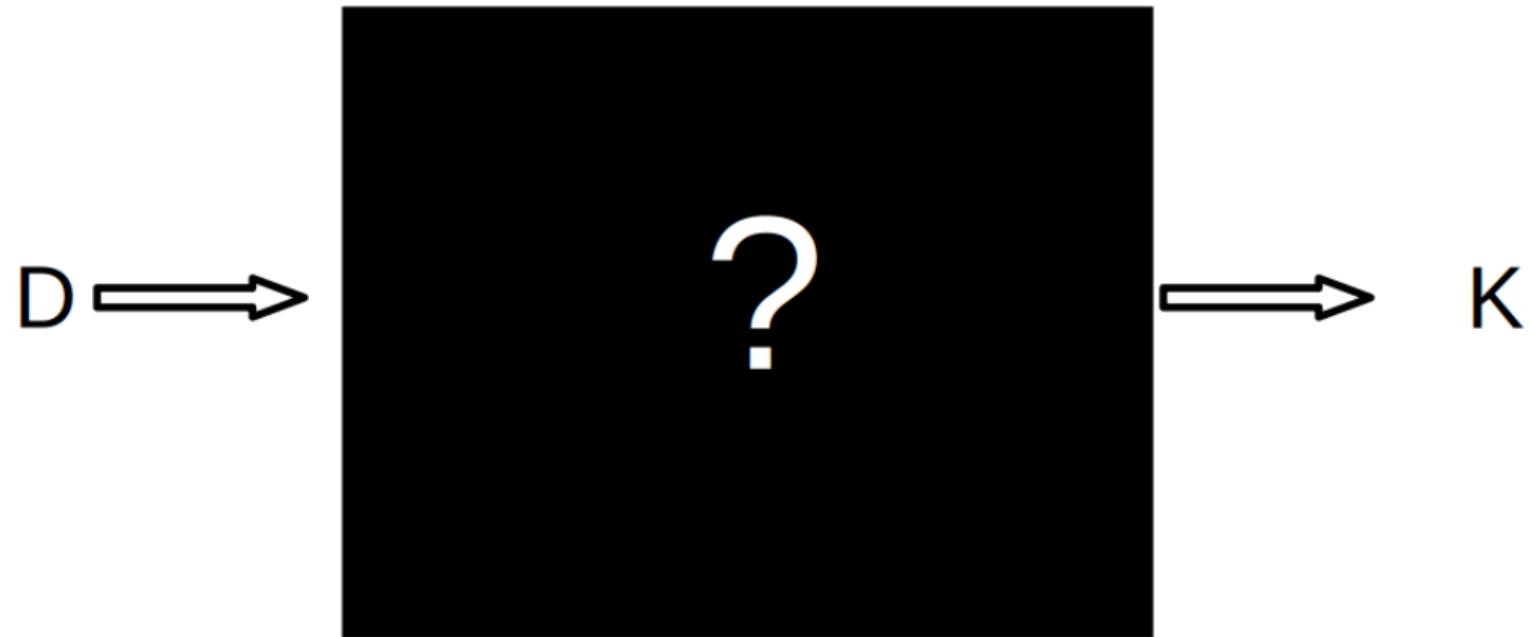
[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))

- Turing-Bombe reduziert den effektiven Schlüsselraum
- Methode des wahrscheinlichen Wortes (crib)
- involutorische Verschlüsselung ($U \rightarrow X$, $X \rightarrow U$)

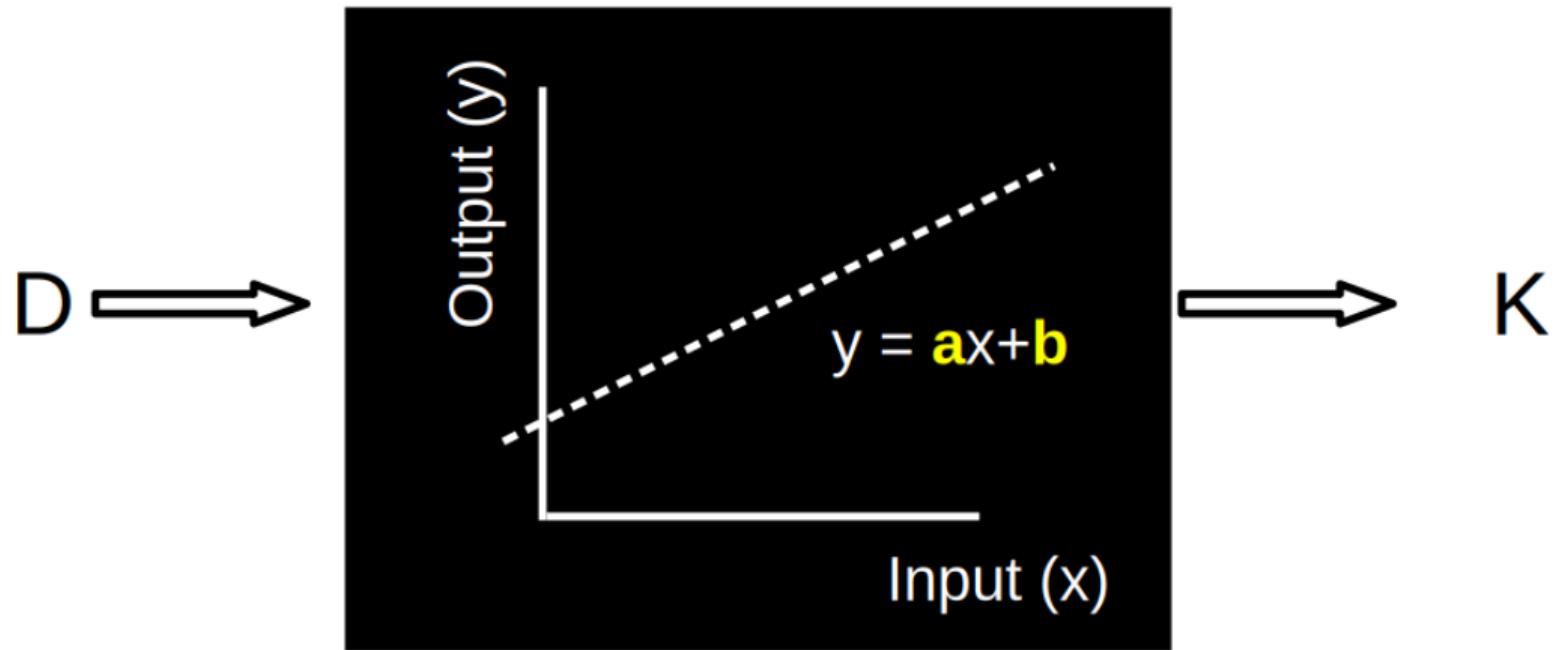
BHNCXSEQKOBIIODWFBTZGCYEHQQJEWOYNBDXHQBALHTSSDPWG

- 1 OBERKOMMANDODERWEHRMACHT
 - 2 OBERKOMMANDODERWEHRMACHT
 - 3 OBERKOMMANDODERWEHRMACHT
 - 4 OBERKOMMANDODERWEHRMACHT
 - 5 OBERKOMMANDODERWEHRMACHT
 - 6 OBERKOMMANDODERWEHRMACHT
 - 7 OBERKOMMANDODERWEHRMACHT
 - 8 OBERKOMMANDODERWEHRMACHT
 - 9 OBERKOMMANDODERWEHRMACHT
 - 10 OBERKOMMANDODERWEHRMACHT
 - 11 OBERKOMMANDODERWEHRMACHT
 - 12 OBERKOMMANDODERWEHRMACHT
 - 13 OBERKOMMANDODERWEHRMACHT
 - 14 OBERKOMMANDODERWEHRMACHT
 - 15 OBERKOMMANDODERWEHRMACHT
 - 16 OBERKOMMANDODERWEHRMACHT
 - 17 OBERKOMMANDODERWEHRMACHT
 - 18 OBERKOMMANDODERWEHRMACHT
 - 19 OBERKOMMANDODERWEHRMACHT
 - 20 OBERKOMMANDODERWEHRMACHT
 - 21 OBERKOMMANDODERWEHRMACHT
 - 22 OBERKOMMANDODERWEHRMACHT
 - 23 OBERKOMMANDODERWEHRMACHT
 - 24 OBERKOMMANDODERWEHRMACHT
 - 25 OBERKOMMANDODERWEHRMACHT
 - 26 OBERKOMMANDODERWEHRMACHT
 - 27 OBERKOMMANDODERWEHRMACHT
- BHNCXSEQKOBIIODWF

Lösung durch Algorithmen



Lösung durch Algorithmen



Geschichte der Kryptographie

Leseauftrag: Lesen Sie S. 6-12

1. Im Text wird Leibniz' Verschlüsselung mit Schlüsselwort beschrieben. Was ist eine Schwäche des Verfahrens?
2. Was ist eine monoalphabetische Verschlüsselung? Was ist die Schwäche dieser Verfahren?
3. Was ist der Unterschied zwischen einer Chiffre und einem Code?
4. Nach welchem Prinzip funktionierte die Enigma?
5. Nach welchem Prinzip funktionierte Leibniz' Machina Decipratoria?



1. Leibniz' Verfahren

- *kryptos* - verborgen, geheim
- Kryptographie, *graphein* - schreiben = Geheimschrift, Wissenschaft der Verschlüsselung von Informationen
- Kryptologie, *logos* - Wort, richtige Einsicht = Wissenschaft eines best. Fachgebietes

Guten Morgen mit Schlüsselwort BOXKAMPFJURY verschlüsseln.

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

GUTEN MORGEN

XYUOP CKFXOP

- fehleranfällig, leicht zu dechiffrieren

2. Monoalphabetische Verfahren

- verwenden 1 Zuordnung von Klartext- zu Chiffretextbuchstaben

Deutsch

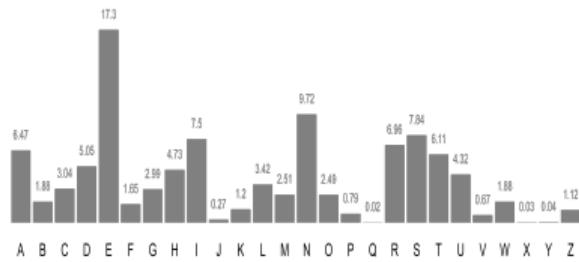
Englisch

Polnisch

2. Monoalphabetische Verfahren

- verwenden 1 Zuordnung von Klartext- zu Chiffretextbuchstaben
- Code knacken durch Häufigkeitsanalyse der Buchstaben

Deutsch
Relative Häufigkeit der Buchstaben in deutschsprachigen Texten (in %)



Englisch

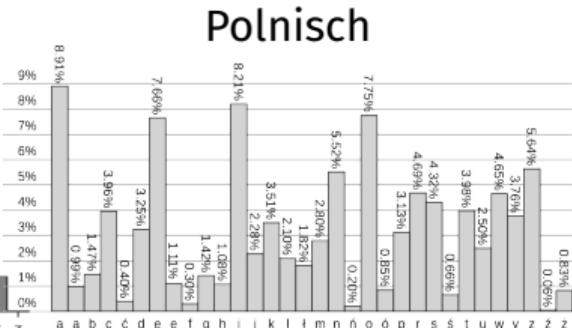
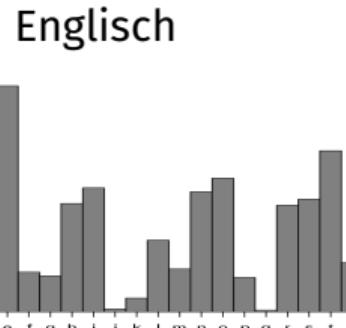
Polnisch

2. Monoalphabetische Verfahren

- verwenden 1 Zuordnung von Klartext- zu Chiffertextbuchstaben
 - Code knacken durch Häufigkeitsanalyse der Buchstaben



Quelle: Wikipedia



3. Chiffre vs. Code

Code: Zuordnung einer bedeutungsvollen Einheit zu einer anderen (kleiner)

Chiffre: Austausch von Buchstaben

Accessory,	Cannot sail by steamer you name. Will cable when steamer and date of departure are fixed.
Accidental,	Cannot say when shall be able to leave _____
Acclimate,	Cannot you start before _____
Accordion,	Cannot you start so as to reach here _____
Accosted,	Can you send me letter of introduction to _____
Accountant,	Come at once. Do not delay.
Accretion,	Care of _____
Accumulate,	Care of E. A. Adams & Co., Boston.
Accurate,	Care of Baring Bros. & Co., Liverpool.
Accursed,	Care of Baring Bros. & Co., London.
Accusing,	Care of Brown Brothers & Co., Boston.
Accustom,	Care of Brown Brothers & Co., New York.
Acerbity,	Care of Brown, Shipley & Co., Liverpool.
	Care of Brown, Shipley & Co., London.

https:

//de.khanacademy.org/computing/
computer-science/cryptography/
ciphers/a/ciphers-vs-codes

3. Chiffre vs. Code

Code: Zuordnung einer bedeutungsvollen Einheit zu einer anderen (kleiner)

Chiffre: Austausch von Buchstaben

Caesar-Chiffre als Beispiel für Substitutionschiffre

Geheim: ABEYX DHFFM SN LITXM KNXVDSNZ

Accessory,	Cannot sail by steamer you name. Will cable when steamer and date of departure are fixed.
Accidental,	Cannot say when shall be able to leave _____
Acclimate,	Cannot you start before _____
Accordion,	Cannot you start so as to reach here _____
Accosted,	Can you send me letter of introduction to _____
Accountant,	Come at once. Do not delay.
Accretion,	Care of _____
Accumulate,	Care of E. A. Adams & Co., Boston.
Accurate,	Care of Baring Bros. & Co., Liverpool.
Accursed,	Care of Baring Bros. & Co., London.
Accusation,	Care of Brown Brothers & Co., Boston.
Accusing,	Care of Brown Brothers & Co., New York.
Accustom,	Care of Brown, Shipley & Co., Liverpool.
Acerbity,	Care of Brown, Shipley & Co., London.

https:

//de.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes

3. Chiffre vs. Code

Code: Zuordnung einer bedeutungsvollen Einheit zu einer anderen (kleiner)

Chiffre: Austausch von Buchstaben

Caesar-Chiffre als Beispiel für Substitutionschiffre

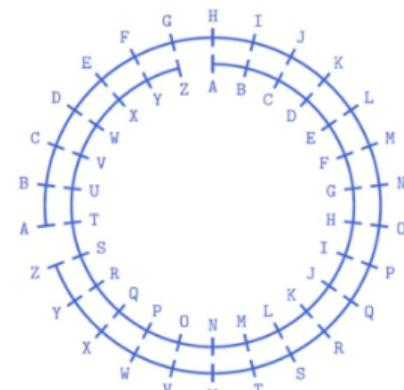
Geheim: ABEYX DHFFM SN LITXM KNXVDSNZ

Klar: HILFE KOMMT ZU SPAET RUECKZUG

Schlüssel: Scheibe um k Schritte drehen z.B. 7

Accessory,	Cannot sail by steamer you name. Will cable when steamer and date of departure are fixed.
Accidental,	Cannot say when shall be able to leave _____
Acclimate,	Cannot you start before _____
Accordion,	Cannot you start so as to reach here _____
Accosted,	Can you send me letter of introduction to _____
Accountant,	Come at once. Do not delay.
Accretion,	Care of _____
Accumulate,	Care of E. A. Adams & Co., Boston.
Accurate,	Care of Baring Bros. & Co., Liverpool.
Accursed,	Care of Baring Bros. & Co., London.
Accusation,	Care of Brown Brothers & Co., Boston.
Accusing,	Care of Brown Brothers & Co., New York.
Accustom,	Care of Brown, Shipley & Co., Liverpool.
Acerbity,	Care of Brown, Shipley & Co., London.

<https://de.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes>



3. Chiffre vs. Code

Code: Zuordnung einer bedeutungsvollen Einheit zu einer anderen (kleiner)

Chiffre: Austausch von Buchstaben

Caesar-Chiffre als Beispiel für Substitutionschiffre

Geheim: ABEYX DHFFM SN LITXM KNXVDSNZ

Klar: HILFE KOMMT ZU SPAET RUECKZUG

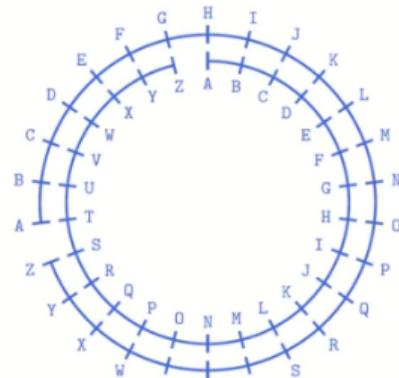
Schlüssel: Scheibe um k Schritte drehen z.B. 7

→ Modulare Arithmetik (kleine Anzahl an Schlüsseln)

- Buchstaben → Zahlen von 0-25
- Verschlüsseln: $c = m + k \bmod 26$,
- Entschlüsseln: $m = c - k \bmod 26$

Accessory,	Cannot sail by steamer you name. Will cable when steamer and date of departure are fixed.
Accidental,	Cannot say when shall be able to leave _____
Acclimate,	Cannot you start before _____
Accordion,	Cannot you start so as to reach here _____
Accosted,	Can you send me letter of introduction to _____
Accountant,	Come at once. Do not delay.
Accretion,	Care of _____
Accumulate,	Care of E. A. Adams & Co., Boston.
Accurate,	Care of Baring Bros. & Co., Liverpool.
Accursed,	Care of Baring Bros. & Co., London.
Accusation,	Care of Brown Brothers & Co., Boston.
Accusing,	Care of Brown Brothers & Co., New York.
Accustom,	Care of Brown, Shipley & Co., Liverpool.
Acerbity,	Care of Brown, Shipley & Co., London.

<https://de.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes>



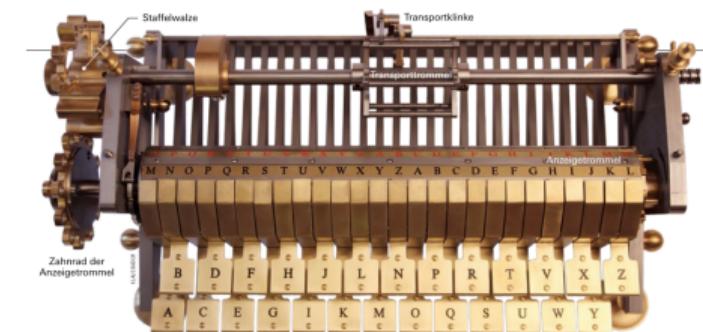
4.+5. Polyalphabetische Verfahren

Substitutionsverfahren mit mehr als einem Alphabet

Enigma



Machina deciphratoria



- Änderung des Alphabets in vorhersagbarer Art und Weise

- Änderung des Alphabets in irregulärer Art und Weise durch mechanische Staffelwalze

Polyalphabetische Substitutionsverfahren: One-Time-Pad

Vergrößerung der Schlüsselmenge durch Schlüssel“wörter”

Klartext	BBBBB	$A \rightarrow C, B \rightarrow D$
Schlüssel	CHIFFRE	
Chiffrat		

Polyalphabetische Substitutionsverfahren: One-Time-Pad

Vergrößerung der Schlüsselmenge durch Schlüssel“wörter”

Klartext	BBBBB	$A \rightarrow C, B \rightarrow D$
Schlüssel	C H IFFRE	
Chiffrat	D	

Polyalphabetische Substitutionsverfahren: One-Time-Pad

Vergrößerung der Schlüsselmenge durch Schlüssel“wörter”

Klartext	BBBBB	$A \rightarrow C, B \rightarrow D$
Schlüssel	CHIFFRE	$A \rightarrow H, B \rightarrow I$
Chiffrat	DI	

Polyalphabetische Substitutionsverfahren: One-Time-Pad

Vergrößerung der Schlüsselmenge durch Schlüssel“wörter”

Klartext	BBBBB	A → C, B → D
Schlüssel	CHIFFRE	A → H, B → I
Chiffrat	DI	

- Schlüssel muss mindestens gleich lang sein wie Klarnachricht
- Sicherheit, wenn:
 - Schlüssel *zufällig* gewählte Buchstabenfolge ist
 - pro Nachricht ein anderer Schlüssel verwendet wird - *One-Time-Pad (OTP)*

Polyalphabetische Substitutionsverfahren: One-Time-Pad

Vergrößerung der Schlüsselmenge durch Schlüssel“wörter”

Klartext	BBBBB	A → C, B → D
Schlüssel	CHIFFRE	A → H, B → I
Chiffrat	DI	

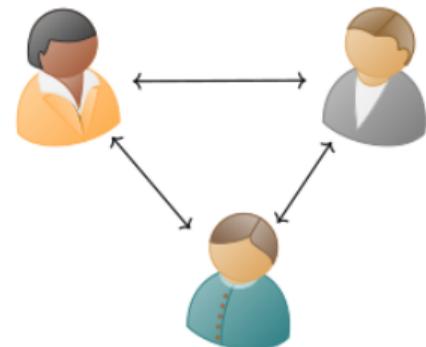
- Schlüssel muss mindestens gleich lang sein wie Klarnachricht
- Sicherheit, wenn:
 - Schlüssel *zufällig* gewählte Buchstabenfolge ist
 - pro Nachricht ein anderer Schlüssel verwendet wird - *One-Time-Pad (OTP)*
- symmetrisches Verschlüsselungsverfahren

Symmetrische Verschlüsselung

- Sender und Empfänger benutzen **denselben** Schlüssel

Probleme:

1. verschiedene Partner - verschiedene Schlüssel
z.B. für 12 Personen, die untereinander
kommunizieren, bräuchte man ?? Schlüssel
2. große Menge an Schlüsselmaterial (One-Time)
3. Schlüssel muss übertragen werden



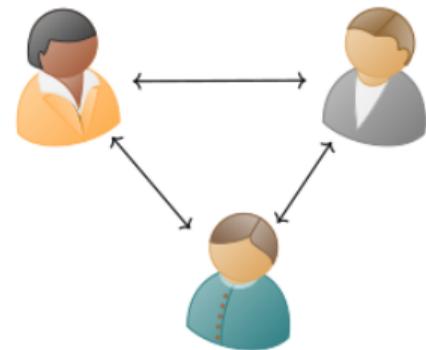
<https://ctan.org/pkg/tikzpeople>

Symmetrische Verschlüsselung

- Sender und Empfänger benutzen **denselben** Schlüssel

Probleme:

1. verschiedene Partner - verschiedene Schlüssel
z.B. für 12 Personen, die untereinander
kommunizieren, bräuchte man $(n^2 - n)/2 = 66$
Schlüssel
2. große Menge an Schlüsselmaterial (One-Time)
3. Schlüssel muss übertragen werden



<https://ctan.org/pkg/tikzpeople>

Anwendung: RSA-Kryptosystem

- 1977 **Rivest, Shamir, Adleman**
- asymmetrische Verschlüsselung
- 2002 Turing-Award



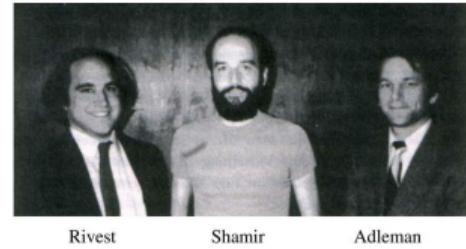
Rivest

Shamir

Adleman

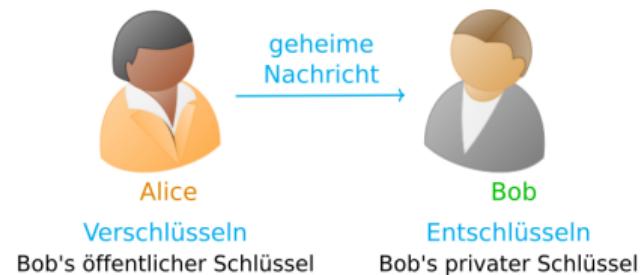
Anwendung: RSA-Kryptosystem

- 1977 **Rivest, Shamir, Adleman**
- asymmetrische Verschlüsselung
- 2002 Turing-Award



Grundidee: ein sich ergänzendes **Schlüsselpaar**

1. **öffentlicher** Schlüssel (public key) - dient zum Verschlüsseln der Nachricht
 2. **privater** Schlüssel (private key) - dient zum Entschlüsseln
- **Verschlüsseln** kann jede mit dem public key
 - **Entschlüsseln** kann nur Inhaber des privaten Schlüssels



RSA-Kryptosystem

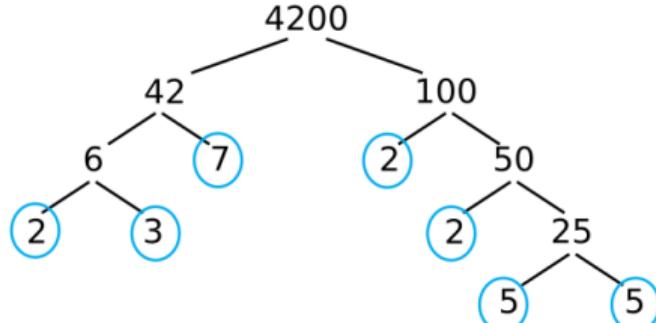
- beruht auf mathematischen Funktionen, die in einer Richtung einfach aber in der anderen Richtung (Umkehrfunktion) schwer zu berechnen sind -
Einwegfunktion (one-way function)
- Faktorisierung großer Zahl, d.h. Zerlegen in Primfaktoren, schwierig
- Multiplikation einer großen Zahl durch Multiplikation von Primzahlen einfach

RSA-Kryptosystem

- beruht auf mathematischen Funktionen, die in einer Richtung einfach aber in der anderen Richtung (Umkehrfunktion) schwer zu berechnen sind -
Einwegfunktion (one-way function)
- Faktorisierung großer Zahl, d.h. Zerlegen in Primfaktoren, schwierig
- Multiplikation einer großen Zahl durch Multiplikation von Primzahlen einfach
- manche Einwegfunktionen, sind **Falltürfunktionen** (trapdoor one-way function) - mit Hilfe einer Zusatzinformation sind sie auch rückwärts leicht zu berechnen

Einschub: Primfaktorzerlegung

- Primzahl ist eine ganze Zahl, $x \in \mathbb{N} > 1$, die nur durch sich selbst und durch 1 **teilbar** ist
- jede natürliche Zahl n lässt sich als Produkt aus Primzahlen darstellen - Primfaktorzerlegung
- bisher kein effizientes Faktorisierungsverfahren bekannt, mit dem man eine beliebige (große) Zahl in Primfaktoren zerlegen könnte (**Einwegfunktion**)



$$4200 = 2 * 2 * 2 * 3 * 5 * 5 * 7$$

Einschub: Euklidischer Algorithmus

$$ggT(5, 48) = 1$$

$$48 = 9 * 5 + 3$$

$$5 = 1 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

Einschub: Euklidischer Algorithmus

$$\text{ggT}(5, 48) = 1 \quad 48 = 9 * 5 + 3$$

$$5 = 1 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)

Einschub: Euklidischer Algorithmus

$$\text{ggT}(5, 48) = 1 \quad 48 = 9 * 5 + 3$$

$$5 = 1 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$\text{ggT}(5, 48) = 1 \quad 48 = 9 * 5 + 3$$

$$5 = 1 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$\begin{array}{l} ggT(5, 48) = 1 \\ \quad 48 = 9 * 5 + 3 \\ \quad \quad 5 = 1 * 3 + 2 \\ \quad \quad \quad 3 = 1 * 2 + 1 \\ \quad \quad \quad \quad 2 = 2 * 1 + 0 \end{array} \quad \begin{array}{l} = 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5 \\ = 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5 \\ \quad 1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3 \end{array}$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$\begin{array}{lll} ggT(5, 48) = 1 & 48 = 9 * 5 + 3 & = 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5 \\ & 5 = 1 * 3 + 2 & = 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5 \\ & 3 = 1 * 2 + 1 & 1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3 \\ & 2 = 2 * 1 + 0 & \end{array}$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

$$-19 * 5 + 2 * 48 = 1$$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$\begin{array}{l} ggT(5, 48) = 1 \\ \quad 48 = 9 * 5 + 3 \\ \quad \quad 5 = 1 * 3 + 2 \\ \quad \quad \quad 3 = 1 * 2 + 1 \\ \quad \quad \quad \quad 2 = 2 * 1 + 0 \end{array} \quad \begin{array}{l} = 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5 \\ = 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5 \\ \quad 1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3 \end{array}$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

$$-19 * 5 + 2 * 48 = 1$$

$$-19 * 5 \equiv 1 \pmod{48}$$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$\begin{array}{l} ggT(5, 48) = 1 \\ \quad 48 = 9 * 5 + 3 \\ \quad \quad 5 = 1 * 3 + 2 \\ \quad \quad \quad 3 = 1 * 2 + 1 \\ \quad \quad \quad \quad 2 = 2 * 1 + 0 \end{array} \quad \begin{array}{l} = 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5 \\ = 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5 \\ \quad 1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3 \end{array}$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

$$-19 * 5 + 2 * 48 = 1$$

$$-19 * 5 \equiv 1 \pmod{48}$$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

Einschub: Erweiterter Euklidischer Algorithmus

$$ggT(5, 48) = 1$$

$$48 = 9 * 5 + 3$$

$$= 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5$$

$$5 = 1 * 3 + 2$$

$$= 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5$$

$$3 = 1 * 2 + 1$$

$$1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3$$

$$2 = 2 * 1 + 0$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

$$-19 * 5 + 2 * 48 = 1$$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

$$-19 * 5 \equiv 1 \pmod{48}$$

$$+ 5 * 48$$

Einschub: Erweiterter Euklidischer Algorithmus

$$\text{ggT}(5, 48) = 1$$

$$48 = 9 * 5 + 3$$

$$= 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5$$

$$5 = 1 * 3 + 2$$

$$= 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5$$

$$3 = 1 * 2 + 1$$

$$1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3$$

$$2 = 2 * 1 + 0$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

$$-19 * 5 + 2 * 48 = 1$$

$$-19 * 5 \equiv 1 \pmod{48}$$

$$+ 5 * 48$$

$$29 * 5 = 1 \pmod{48}$$

Einschub: Erweiterter Euklidischer Algorithmus

$$\begin{array}{l} ggT(5, 48) = 1 \\ \quad 48 = 9 * 5 + 3 \\ \quad \quad 5 = 1 * 3 + 2 \\ \quad \quad \quad 3 = 1 * 2 + 1 \\ \quad \quad \quad \quad 2 = 2 * 1 + 0 \end{array} \quad \begin{array}{l} = 2 * (48 - 9 * 5) - 1 * 5 = 2 * 48 - 19 * 5 \\ = 3 - 1 * (5 - 1 * 3) = 2 * 3 - 1 * 5 \\ \quad 1 = 3 - 1 * 2 \quad 2 = 5 - 1 * 3 \end{array}$$

- gesucht: Kehrwert (Inverse) von 5 modulo 48 = 29
- Kehrwert von a modulo m ist positive Zahl $b < m$, die folgende Gleichung erfüllt:
 $b * a \equiv 1 \pmod{m}$ (Bsp: $b * 5 \equiv 1 \pmod{48}$)
- wenn a und m teilerfremd sind, gibt es einen modularen Kehrwert, \Rightarrow Erweiterter Euklidischer Algorithmus um ihn zu berechnen \Rightarrow Euklid. Alg. rückwärts: $1 = k_1 * 5 + k_2 * 48$

Probieren: $a = 3, m = 7, b * 3 \equiv 1 \pmod{7}$

b	0	1	2	3	4	5	$6(m-1)$
$b * 3$	0	3	6	9	12	15	18
$b * 3 // 7$	0	0	0	1	1	2	2
$b * 3 \pmod{7}$	0	3	6	2	5	1	4

$$\begin{array}{l} -19 * 5 + 2 * 48 = 1 \\ -19 * 5 \equiv 1 \pmod{48} \\ 29 * 5 = 1 \pmod{48} \end{array} \quad + 5 * 48$$

Übung

Bestimme die modulare Inverse von 5 modulo 24!

Übung

Bestimme die modulare Inverse von 5 modulo 24!

1. Testen auf Teilerfremdheit
2. falls ja, $\text{ggT}(5, 24) = 1$ darstellen als gewichtete Summe der beiden Zahlen
3. umformen in $b * 5 \equiv 1 \pmod{24}$

Übung

Bestimme die modulare Inverse von 5 modulo 24!

1. Testen auf Teilerfremdheit
2. falls ja, $\text{ggT}(5, 24) = 1$ darstellen als gewichtete Summe der beiden Zahlen
3. umformen in $b * 5 \equiv 1 \pmod{24}$

Euklid. Algorithmus $\text{ggT}(5, 24)$

$$24 = 4 * 5 + 4$$

$$5 = 1 * 4 + 1$$

$$4 = 4 * 1 + 0$$

Erweiterter Euklid. Algorithmus

$$1 = 5 - 1 * 4$$

$$4 = 24 - 4 * 5$$

$$1 = 5 - 1 * (24 - 4 * 5)$$

$$1 = 5 * 5 - 1 * 24 = 25 - 24$$

Umformen

$$1 = 5 * 5 - 1 * 24 \rightarrow 5 * 5 = 1 + 1 * 24$$

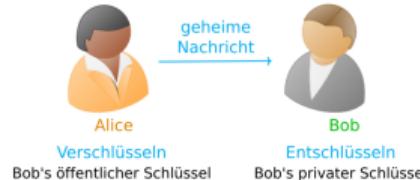
$$5 * 5 \equiv 1 \pmod{24}$$

RSA-Kryptosystem

Senderin (Alice) verschlüsselt Nachricht **N** mit public key (**e, n**) des Empfängers (Bob). Empfänger entschlüsselt den Geheimtext **C** mit private key (**d, n**).

Prinzip: Einwegfunktion (**One-way function**)

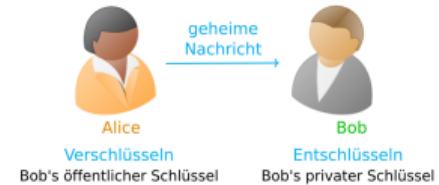
- leicht: $C = N^e \text{ mod } n$
 - prakt. unmöglich: Umkehrfunktion, Inverse von $N^e \text{ mod } n$
- nur möglich durch Kenntnis einer Hintertür (**trapdoor function**) d



Erzeugen des Schlüsselpaars: public and private

besteht aus drei Zahlen e , d und n

- n - RSA-Modul
- e, d - Ver- (*encrypt*) und Entschlüsselungsexponent (*decrypt*)
- (e,n) - public key, (d,n) - private key



Erzeugen des Schlüsselpaars: public and private

besteht aus drei Zahlen e , d und n

- n - RSA-Modul
- e, d - Ver- (*encrypt*) und Entschlüsselungsexponent (*decrypt*)
- (e,n) - public key, (d,n) - private key

1. wähle 2 Primzahlen p und q
2. berechne den RSA-Modul n als $n = p * q$
3. berechne $\phi(n) = (p - 1) * (q - 1)$



```
from sympy import prime  
p, q = prime(50), prime(54)  
n = p * q  
phi = (p-1) * (q-1)
```

```
print(p, q, n, phi)
```

```
229 251 57479 57000
```

Erzeugen des Schlüsselpaars: public and private

besteht aus drei Zahlen e , d und n

- n - RSA-Modul
- e, d - Ver- (*encrypt*) und Entschlüsselungsexponent (*decrypt*)
- (e,n) - public key, (d,n) - private key



1. wähle 2 Primzahlen p und q
2. berechne den RSA-Modul n als $n = p * q$
3. berechne $\phi(n) = (p - 1) * (q - 1)$
4. ermittle Zahl e , die teilerfremd zu $\phi(n)$ und $< \phi(n)$

```
from sympy import prime
p, q = prime(50), prime(54)
n = p * q
phi = (p-1) * (q-1)
```

```
print(p, q, n, phi)
```

```
229 251 57479 57000
```

```
from sympy import factorint
print(factorint(phi))
```

```
{2: 3, 3: 1, 5: 3, 19: 1}
```

```
e = 7 * 11
```

Erzeugen des Schlüsselpaars: public and private

besteht aus drei Zahlen e , d und n

- n - RSA-Modul
- e, d - Ver- (*encrypt*) und Entschlüsselungsexponent (*decrypt*)
- (e,n) - public key, (d,n) - private key



1. wähle 2 Primzahlen p und q
2. berechne den RSA-Modul n als $n = p * q$
3. berechne $\phi(n) = (p - 1) * (q - 1)$
4. ermittle Zahl e , die teilerfremd zu $\phi(n)$ und $< \phi(n)$
5. berechne d als Kehrwert von e modulo $\phi(n)$

```
from sympy import prime
p, q = prime(50), prime(54)
n = p * q
phi = (p-1) * (q-1)
```

```
print(p, q, n, phi)
```

```
229 251 57479 57000
```

```
from sympy import factorint
print(factorint(phi))
```

```
{2: 3, 3: 1, 5: 3, 19: 1}
```

```
e = 7 * 11
```

```
from sympy import mod_inverse
d = mod_inverse(e, phi)
print(d)
```

RSA-Kryptosystem

Senderin (Alice) verschlüsselt Klartext **N** mit public key (**e, n**) des Empfängers (Bob). Empfänger entschlüsselt den Geheimtext **C** mit private key (**d, n**).

Prinzip: Einwegfunktion (**One-way function**)

- leicht: $C = N^e \bmod n$
- prakt. unmöglich: Umkehrfunktion, Inverse von $N^e \bmod n$
→ nur möglich durch Kenntnis einer Hintertür (**trapdoor function**) d

Verschlüsseln: $C = N^e \bmod n$

RSA-Kryptosystem

Senderin (Alice) verschlüsselt Klartext **N** mit public key (**e, n**) des Empfängers (Bob). Empfänger entschlüsselt den Geheimtext **C** mit private key (**d, n**).

Prinzip: Einwegfunktion (**One-way function**)

- leicht: $C = N^e \bmod n$
- prakt. unmöglich: Umkehrfunktion, Inverse von $N^e \bmod n$
→ nur möglich durch Kenntnis einer Hintertür (**trapdoor function**) d

Verschlüsseln: $C = N^e \bmod n$

$$n = p * q \text{ (geheim)}$$

$$\phi(n) = (p - 1) * (q - 1)$$

RSA-Kryptosystem

Senderin (Alice) verschlüsselt Klartext **N** mit public key (**e, n**) des Empfängers (Bob). Empfänger entschlüsselt den Geheimtext **C** mit private key (**d, n**).

Prinzip: Einwegfunktion (**One-way function**)

- leicht: $C = N^e \bmod n$
- prakt. unmöglich: Umkehrfunktion, Inverse von $N^e \bmod n$
→ nur möglich durch Kenntnis einer Hintertür (**trapdoor function**) d

Verschlüsseln: $C = N^e \bmod n$

$$n = p * q \text{ (geheim)}$$

$$\phi(n) = (p - 1) * (q - 1)$$

$$\text{für } e \text{ gilt: } \text{ggT}(e, \phi(n)) = 1$$

RSA-Kryptosystem

Senderin (Alice) verschlüsselt Klartext **N** mit public key (**e, n**) des Empfängers (Bob). Empfänger entschlüsselt den Geheimtext **C** mit private key (**d, n**).

Prinzip: Einwegfunktion (**One-way function**)

- leicht: $C = N^e \bmod n$
- prakt. unmöglich: Umkehrfunktion, Inverse von $N^e \bmod n$
→ nur möglich durch Kenntnis einer Hintertür (**trapdoor function**) d

Verschlüsseln: $C = N^e \bmod n$

$$n = p * q \text{ (geheim)}$$

$$\phi(n) = (p - 1) * (q - 1)$$

$$\text{für } e \text{ gilt: } \text{ggT}(e, \phi(n)) = 1$$

Entschlüsseln: $(N^e)^d \bmod n$

wenn $\bmod n$ gerechnet wird

Ein Durchlauf durch RSA

Verschlüsselung E (encryption) von
Nachricht N mit **öffentlichen** Schlüssel
($n = p * q, e$) des **Empfängers**

$$C = N^e \mod n$$

Ein Durchlauf durch RSA

Verschlüsselung E (encryption) von Nachricht N mit **öffentlichen** Schlüssel $(n = p * q, e)$ des **Empfängers**

$$C = N^e \mod n$$

Bob's öffentlicher Schlüssel ist **(187,7)**, also $n = 187$ und $e = 7$. Alice will Nachricht $N = 76$ an **Bob** schicken. Sie verschlüsselt:

$$E(76) = 76^7 \mod 187 = 32$$

Ein Durchlauf durch RSA

Verschlüsselung E (encryption) von Nachricht N mit **öffentlichen** Schlüssel $(n = p * q, e)$ des **Empfängers**

$$C = N^e \mod n$$

Entschlüsselung D (decryption) von C mit dem aus (n, e) berechneten **privaten** Schlüssel d des **Empfängers**

$$\begin{aligned} D(C) &= C^d \mod n = (N^e)^d \mod n \\ &= N \end{aligned}$$

Bob's öffentlicher Schlüssel ist **(187,7)**, also $n = 187$ und $e = 7$. Alice will Nachricht $N = 76$ an **Bob** schicken. Sie verschlüsselt:

$$E(76) = 76^7 \mod 187 = 32$$

Ein Durchlauf durch RSA

Verschlüsselung E (encryption) von Nachricht N mit **öffentlichen** Schlüssel $(n = p * q, e)$ des **Empfängers**

$$C = N^e \mod n$$

Entschlüsselung D (decryption) von C mit dem aus (n, e) berechneten **privaten** Schlüssel d des **Empfängers**

$$\begin{aligned} D(C) &= C^d \mod n = (N^e)^d \mod n \\ &= N \end{aligned}$$

Bob's öffentlicher Schlüssel ist **(187,7)**, also $n = 187$ und $e = 7$. Alice will Nachricht $N = 76$ an **Bob** schicken. Sie verschlüsselt:

$$E(76) = 76^7 \mod 187 = 32$$

Bob's **privater** Schlüssel ist $d = 23$. **Bob** entschlüsselt die verschlüsselte Nachricht $C = 32$ mit:

$$D(32) = 32^{23} \mod 187 = 76$$

Kann man den Code “knacken”?

- kennt man p und q , dann kann man sofort n und $\phi(n) = (p - 1) * (q - 1)$ berechnen

Kann man den Code “knacken”?

- kennt man p und q , dann kann man sofort n und $\phi(n) = (p - 1) * (q - 1)$ berechnen
- da e öffentlich ist, kann man dann auch d als Kehrwert von e berechnen

Kann man den Code “knacken”?

- kennt man p und q , dann kann man sofort n und $\phi(n) = (p - 1) * (q - 1)$ berechnen
- da e öffentlich ist, kann man dann auch d als Kehrwert von e berechnen

Die Sicherheit des Verfahrens beruht auf “Erfahrung”

Kann man den Code “knacken”?

- kennt man p und q , dann kann man sofort n und $\phi(n) = (p - 1) * (q - 1)$ berechnen
- da e öffentlich ist, kann man dann auch d als Kehrwert von e berechnen

Die Sicherheit des Verfahrens beruht auf “Erfahrung”

- Ist n groß genug, so ist es *schwer* (nicht schnell genug), n in Primfaktoren zu zerlegen (Primfaktorzerlegung ist one-way Funktion)

Relevanz von Forschung im Spannungsfeld von:

- hoher Informationswert (Quellen, präzise Dokumentation, überprüfbar, nachvollziehbar, ...)
- Erkenntnisse erweitern Wissen im Fachgebiet
- Erkenntnisse sind von praktischem Nutzen
- Konsequenzen technischer Entwicklung (Technikfolgenabschätzung, Dual Use)
- Kontext technischer Entwicklung (Objektivität?)
- Verteilungsgerechtigkeit
- Sicherheit
- Privatsphäre und Anonymität
- ...

Computerethik ist Teilgebiet der Technikethik

<https://de.wikipedia.org/wiki/Computerethik>

Sie befinden sich hier: Technische Universität Berlin » Über die TU Berlin » Organisation » Rechtliches » Richtlinien / Leitlinien » Zivilklausel

Zivilklausel der TU Berlin

Die TU Berlin hat auf der Sitzung des Akademischen Senats vom 29. Mai 1991 beschlossen, aus Verantwortung und aufgrund der Rolle der Hochschule vor und im Zweiten Weltkrieg, insbesondere in der Rüstungsforschung, die alliierten Bestimmungen fortzuführen und keine rüstungsrelevante Forschung durchzuführen.

Hierzu beschloss der Akademische Senat im Wortlaut:

"Der Akademische Senat (AS) begrüßt die Diskussion innerhalb der Universität, die darauf abzielt, rüstungsrelevante Forschung auch nach Wegfall der alliierten Bestimmungen an der TU Berlin zu verhindern. Die Mitglieder des AS sind sich darüber einig, dass an der TU Berlin keine Rüstungsforschung durchgeführt werden soll. Weiterhin ist sich der AS auch im Klaren darüber, dass wissenschaftliche Ergebnisse nicht davor geschützt werden können, für militärische Zwecke von Dritten missbraucht zu werden."

Quellen

Haraway, D. (1988). Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective, *Feminist Studies*, 14(3), 575-599.

Weitz E. (2018). Konkrete Mathematik (nicht nur) für Informatiker. Das RSA-Kryptosystem (Kapitel 10). Heidelberg: Springer.

<https://www.youtube.com/watch?v=mDRMzBLI3U4>