

Cryptography during the two world wars, and wrap-up of classical ciphers.

Math 4440/5440.

First World War German Cipher: ADFGVX Cipher

	A	D	F	G	V	X		3	4	2	1
A	c	o	8	x	f	4		D	G	X	G
D	m	k	3	a	z	9		X	G	D	G
F	n	w	1	0	j	d		A	A	D	D
G	5	s	i	y	h	u		D	G	X	G
V	p	l	v	b	6	r		F	X	D	G
X	e	q	7	t	2	g		F	D	F	A

Plaintext: ATTACK AT DAWN

Step 1: DG XG XG DG AA DD DG XG FX DG FD FA

Ciphertext: GGDGGAXDDXDFDXADFFGGAGXD

Comments

	A	D	F	G	V	X	3	4	2	1
A	c	o	8	x	f	4	D	G	X	G
D	m	k	3	a	z	9	X	G	D	G
F	n	w	1	0	j	d	A	A	D	D
G	5	s	i	y	h	u	D	G	X	G
V	p	l	v	b	6	r	F	X	D	G
X	e	q	7	t	2	g	F	D	F	A

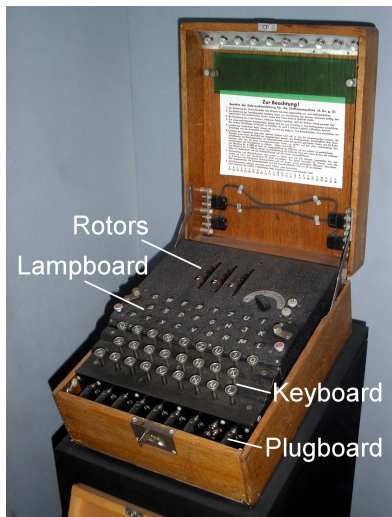
1. The thing on the left is a Polybius square; dates back to ancient greece.
2. It's purpose was coding theory: reduce the number of symbols in the alphabet from 26 to 5.
3. Long-distance signalling (e.g. holding up 1-5 firey torches) was less prone to error with a smaller alphabet.
4. Message length increases but error rate decreases.

Some clues to cryptanalysis (French broke it)

	A	D	F	G	V	X		3	4	2	1
A	c	o	8	x	f	4		D	G	X	G
D	m	k	3	a	z	9		X	G	D	G
F	n	w	1	0	j	d		A	A	D	D
G	5	s	i	y	h	u		D	G	X	G
V	p	l	v	b	6	r		F	X	D	G
X	e	q	7	t	2	g		F	D	F	A

1. Because the keylength (3421) is even here, the letters in one column are either all column headers or all row headers.
2. Column header D has a different frequency than row header D.
3. Use frequency analysis to identify the likely columns.
4. Pair columns (e.g. put 3 next to 4) and do frequency analysis on the digraphs (DG, XG etc.) to see if the pairing is correct.

Second World War



Wartime Enigma Machine

Second World War



Nr. 00190

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

Wagennummer	Wagenlage	Ringstellung	Stieleverbindungen										Klemmgruppen								
			an der Umkehrrolle				am Stichenrolle														
			1	2	3	4	5	6	7	8	9	10									
040	31	I V III	14	09	24			SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg
040	30	IV III II I	05	26	02			IS	EV	MX	KW	DT	UJ	ZQ	A0	CH	NY	ktl	acw	zsl	wao
040	29	III II I	12	24	03	KM	AX	PZ	GO									ioc	zcn	ovw	wvd
040	28	II III V	06	08	16	DI	CN	BR	PV									lrb	cid	ude	rzl
040	27	III I IV	11	03	07	LT	EQ	HS	UW									wof	fbh	vct	uis
040	26	I IV V	17	22	19			VZ	AL	RT	KO	CO	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
040	25	IV III I	08	25	12			OR	PV	AD	IT	PK	HJ	LZ	N5	EQ	CW	ouc	uhq	uew	uti
040	24	V I IV	05	18	14			TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwf	vei	tlq
040	23	IV II I	24	12	04			PJ	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwu	udf	tlö
040	22	II IV V	01	09	21			QJ	ES	IM	RX	LV	AD	OU	BO	WZ	CN	jgc	acx	mwe	wvc
040	21	I V II	11	03	19	PT	OX	EZ	CH									jpw	del	nwf	wvf
040	20	III IV V	24	01	10	MR	KN	BQ	PW									Jqd	cef	nvo	ysh
040	19	V III I	17	25	20			OP	HO	PZ	AU	RT	SV	JL	QX	BE	TV	jef	fpz	nwo	tlg
040	18	IV II V	15	23	26			DX	FR	QH	WY	DL	CM	AE	T2	JS	G1	isa	gbw	vcj	rxn
040	17	I IV II	21	06	16			EJ	OY	IV	AQ	KW	FX	MT	P5	LU	BD	mae	hzi	sog	ysi
040	16	V II III	08	16	13			IR	KZ	LS	EM	OY	QY	AX	JP	BU		tdp	dhb	fkp	uiv
040	15	II IV I	01	03	07			HM	JO	DI	NR	BT	XZ	OS	PU	PQ	CT	ldw	hzi	soh	wvg
040	14	IV I V	15	11	05	AI	BT	MV	HU									imz	noa	tjv	xtk
040	13	I III II	11	20	03	PW	EL	DO	KN									zgr	dgz	gjo	ryt
040	12	V I IV	18	10	07	RZ	OQ	CP	SX									zda	rkf	tjw	xtl
040	11	II IV III	02	26	15			MO	BP	CY	RZ	KX	AN	JT	DO	IL	PW	zds	rjy	soi	whh
040	10	III V IV	23	21	01			KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	1rc	zbx	vbm	rxo
040	9	V I III	16	04	08			LR	IK	MS	QO	HW	PT	OO	VX	PZ	EN	edj	eyr	vby	thi
040	8	IV II V	13	19	25			QY	B5	LN	KT	AP	IU	DO				yan	dha	eke	tti
040	7	I IV II	09	03	22			UX	I2	NN	BK	OQ	CP	FT	JY	MP	AR	lzd	dgb	zsj	wbi
040	6	III I V	11	18	14			DU	GU	BW	NP	HK	A2	C1	P0	JX	VY	lao	cft	zsk	wbj
040	5	V I IV	23	02	25	IL	AP	EU	HO									lju	edr	iye	waj
040	4	II IV I	04	21	09	QT	WZ	KV	GM									lzb	zby	vcy	obj
040	3	V I II	19	11	06	BP	NR	DX	CS									lap	owd	iwu	wak
040	2	IV V I	16	14	02			BN	HO	EO	PY	KQ	CP	OS	JW	AI	VZ	agc	bdy	iyf	xtd
040	1	V I III	22	12	10			DB	BM	N2	CK	OV	HQ	AP	UY	SW	JO	kgl	edf	giq	wuv

Second World War

Geheime Kommandosache!

Jede einzelne Lageschlüssel ist geheim.

Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unverändert in Feindeshand fallen. Bei Gefahr reiflos und frühzeitig vernichten.

Platz Nr.	Wolkenlage	Ringstellung	Stichvererbinderungen										Kenngruppen				
			an der Umkehrstelle		am Stichenort												
			1	2	3	4	5	6	7	8	9	10					
649 31	I V III	14 09 24				SZ	OT	DV	KU	FO	MY	EW	JH	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	zsl wao
649 29	III II I	12 24 03	KM AX PZ OO			DJ	AT	CV	IO	ER	GS	LW	PZ	FN	BH	loc acn	oww vzh
649 28	II III V	06 58 16	DI CN BR PV			CK	PV	AI	DK	OT	MQ	EU	BX	LP	OJ	lrb cld	ude rzh
649 27	III I IV	11 03 07	LT EQ HS UW			DY	IN	BV	QR	AM	LO	PP	HT	EX	UW	woj fbb	vct uis
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
649 24	V I IV	05 18 14				TY	AS	OM	KV	JM	DR	HX	GL	CZ	NU	kpl rwi	vci tlg
649 23	IV II I	24 12 04				QV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn rwm	udf tlo
649 22	II IV V	01 09 21	IU AS DV OL			PJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jac acx	mwe wvc
649 21	I V II	13 05 19	PT OX EZ CH			RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpd del	mwf wvf
649 20	III IV V	24 01 10	MR KN BQ PW			DP	HO	QZ	AU	RY	SV	JL	OX	BE	TW	jcd cef	nvo ysh
649 19	V III I	17 25 20				OX	PR	FH	WY	DL	CM	AE	TZ	JS	G1	idf fpx	jwg tlg
649 18	IV II V	15 23 26				EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	isa gbw	vcj 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				HM	JO	DI	NR	BY	XZ	OS	PU	PQ	CT	tdp dnb	fkf uiv
649 15	II IV I	01 03 07				DS	HY	NR	OW	LX	AJ	BQ	CO	IP	NT	ldw hzj	soh wvg
649 14	IV I V	15 11 05	AI BT MV HU			OM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz noa	tjv xtk
649 13	I III II	13 20 03	PW EL DO KN			LY	AO	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgt	gjo ryg
649 12	V I IV	18 10 07	RZ OQ CP SX			MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	ady rki	tjw xtl
649 11	II IV III	02 26 15				KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	sea rly	soi wvh
649 10	III V IV	23 21 04				LR	IK	MS	QU	HW	PT	OO	VX	PE	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 tih
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	HM	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 AP EU HO			MV	GL	OK	OQ	BI	FU	HS	FX	NW	EY	lju edr	iyw waj
649 4	II IV I	04 21 09	QT WZ KV GM			AC	BL	OZ	EK	QV	OP	SH	JM	TX		lsb zby	vcy ujb
649 3	V I II	19 11 06	BP NR DX CS			KR	NP	CN	BF	EH	DZ	IW	AV	OJ	LO	lap owd	iwu wak
649 2	IV V I	16 14 02				BN	HU	EO	FY	KQ	CP	OS	JW	AI	VZ	aqd bdy	iyf xtd
649 1	II I III	23 12 10				DP	BM	NZ	CK	OY	GK	AP	UY	SW	JO	kgl cdf	giz wuv

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unverfehrt in Feindeshand fallen. Bei Gefahr reiflos und frühzeitig vernichten.

Platz Nr.	Wolkenlage	Ringstellung		Stecherverbindungen										Kerngruppen		
				an der Umkehrrolle	1	2	3	4	5	6	7	8	9	10		
649	30	4 09 24			SZ	OT	DV	KU	FO	MY	EW	JH	IX	LQ	wny dgy	ekb rzg
649	30	5 26 02			IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl acw	zsl wzo
649	30	12 24 03	KM AX PZ OO		DJ	AT	CV	IO	ER	GS	LW	PZ	PH	BH	loc zcn	oww vwd
649	28	06 58 16	DI CN BR PV		CR	PV	AI	DK	OT	MQ	EU	BX	LP	OJ	lrh cld	ude rzh
649	27	11 03 07	LT EQ HS UW		DY	IN	BV	QR	AM	LO	PP	HT	EX	UW	woj fbb	vct uis
649	26	17 22 19			VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle gbo	uev rxm
649	25	08 25 12			OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc uhq	uew uit
649	24	05 18 14			TY	AS	OM	KV	JM	DR	HX	GL	CZ	NU	kpl rwl	vci tlg
649	23	24 12 04			QV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn rwm	udf tlo
649	22	01 09 21	IU AS DV GL		PJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jac acx	mwe wve
649	21	13 05 19	PT OX EZ CH		RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpd del	mwf wvf
649	20	24 01 10	MR KN BQ PW		DP	HO	QZ	AU	RY	SV	JL	OX	BE	TW	jcd cef	nvo ysh
649	19	17 25 20			OX	PR	FH	WY	DL	CM	AE	TZ	JS	G1	ief fpx	jwg tlg
649	18	15 23 26			EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	isa gbw	vcj rxn
649	17	21 10 06			IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae hzi	sog ysi
649	16	08 16 13			HM	JO	DI	NR	BY	XZ	OS	PU	FQ	CT	tdp dhh	fkv uiv
649	15	01 03 07			DS	HY	NR	OW	LX	AJ	BQ	CO	IP	NT	ldw hza	soh wvg
649	14	15 11 05	AI BT MV HU		OM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz noa	tjv xtk
649	13	13 20 03	PW EL DO KM		LY	AO	KM	BR	IQ	JU	HV	SW	ET	CX	zgr dgi	gjo ryg
649	12	18 10 07	RZ OQ CP SX		MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	ady rki	tjw xtl
649	11	02 26 15			KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	sea rly	soi wvh
649	10	23 21 04			LR	IK	MS	QU	HW	PT	OO	VX	PE	EN	lrc zbx	vbm rxo
649	9	16 04 08			QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj eyr	vby tih
649	8	13 19 25			FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz dha	ekc tli
649	7	09 03 22			UX	IZ	HN	BK	OQ	CP	FT	JY	HM	AR	lan dgb	zsj wbi
649	6	11 18 14			DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao cft	zsk wbj
649	5	23 02 25	IL AP EU HO		MV	GL	OK	OQ	B1	FU	HS	FX	NW	EY	lju edr	iye waj
649	4	04 21 09	QT WZ KV GM		AC	BL	OZ	EK	QV	OP	SU	DH	JM	TX	lsb zby	vcy ujb
649	3	19 11 06	BP NR DX CS		KR	NP	CN	BF	EH	DZ	IW	AV	OJ	LO	lap owd	iwu wak
649	2	16 14 02			BN	HU	EO	FY	KQ	CP	OS	JW	AI	VZ	aqd bdy	iyf xtd
649	1	23 12 10			DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl cdf	giz wuv

5.4.3

Nr. 00190

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

$$5 \cdot 4 \cdot 3 \cdot 26^3$$

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unverfehrt in Feindeshand fallen. Bei Gefahr reiflos und frühzeitig vernichten.

Platzang.	Wolkenlage	Ringstellung	Stichvererbinderungen										Reihengruppen				
			an der Umkehrrolle		am Stecherbrett												
			1	2	3	4	5	6	7	8	9	10					
649	3												wny dgy	ekb rzg			
649	3												ktl acw	zsl wzo			
649	2												ioc zcn	oww vwd			
649	28	II	III	V	06	58	16	DI	CN	BR	PV		lrb cld	ude rzh			
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW		woj fbb	vct uis			
649	26	I	IV					VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP
649	25	IV	III					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW
649	24	V	I					TY	AS	OM	KV	JM	DR	HX	GL	CZ	NU
649	23	IV	II					QV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT
649	22	II	IV	V	01	09	21	IU	AS	DV	QL						
649	21	I	V	II	13	05	19	PT	OX	EZ	CH						
649	20	III	IV	V	24												
649	19	V	III	I	17												
649	18	IV	II	V	15												
649	17	I	IV	II	21	10	06										
649	16	V	II	III	08	16	13										
649	15	II	IV	I	01	03	07										
649	14	IV	I	V	15	11	05	AI	BT	MV	HU						
649	13	I	III	II	13	20	03	PW	EL	DO	KM						
649	12	V	I	IV	18	10	07	RZ	OQ	CP	SX						
649	11	II	IV	III	02	26	15										
649	10	III	V	IV	23	21	04										
649	9	V	I	III	16	04	08										
649	8	IV	II	V	13	19	25										
649	7	I	IV	II	09	03	22										
649	6	III	I	V	11	18	14	IL	AP	EU	HO						
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM						
649	4	II	IV	I	04	21	09	BP	NR	DX	CS						
649	3	V	I	II	19	11	06										
649	2	IV	V	I	16	14	02										
649	1	II	I	III	23	12	10	DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12})$$

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

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

Platzang.	Wellenlage	Ringstellung	Stichverbindungen										Reihengruppen		
			an der Umkehrrolle	1	2	3	4	5	6	7	8	9	10		
649	III	V	4 09 24											wny dgy	ekb rzg
649	III	V	05 26 02											ktl acw	zsl wzo
649	III	V	12 24 03	KM AX PZ OO										ioc zcn	oww vwd
649	III	V	06 58 16	DI CN BR PV										lrb cld	ude rzh
649	III	V	11 03 07	LT EQ HS UW										woj fbb	vct uis
649	III	V	08 58 16											xle gbo	uev rxm
649	III	V	11 03 07											ouc uhq	uew uit
649	III	V	08 58 16											kpl rwl	vci tlg
649	III	V	11 03 07											ebn rwm	udf tlo
649	III	V	08 58 16											jac acx	mwe wve
649	III	V	11 03 07											jpw del	mwf wvf
649	III	V	08 58 16											jcd cef	nvo ysh
649	III	V	11 03 07											ief fpx	jwg tlg
649	III	V	08 58 16											isa bw	voj rxn
649	III	V	11 03 07											mae hzi	sog ysi
649	III	V	08 58 16											tdp dhh	fkv uiv
649	III	V	11 03 07											ldw hzi	soh wvg
649	III	V	08 58 16											imz noa	tjv xtk
649	III	V	11 03 07											zgr dgi	gjo ryg
649	III	V	08 58 16											tdj rkl	tjw xtl
649	III	V	11 03 07											sea riy	soi wvh
649	III	V	08 58 16											lrc zbx	vbm rxo
649	III	V	11 03 07											edj eyr	vby tih
649	III	V	08 58 16											yiz dha	ekc tli
649	III	V	11 03 07											lan dgb	zsj wbi
649	III	V	08 58 16											lao cft	zsk wbj
649	III	V	11 03 07											lju edr	iye waj
649	III	V	08 58 16											lsb zby	vcy ujb
649	III	V	11 03 07											lap owd	iwu wak
649	III	V	08 58 16											aqd bdy	iyf xtd
649	III	V	11 03 07											kgi cdf	giz wuv

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10})$$

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unverändert in Feindeshand fallen. Bei Gefahr sofort und frühzeitig vernichten.

Platz Nr.	Wellenlage	Ringstellung	Stichverbindungen								Heirgruppen							
			an der Umkehrrolle	1	2	3	4	5	6	7								
649	30	II	4 09 24	SZ	GT	DV	KU	FO	MY	EW	JN	LX	wny dgy	ekb rzg				
649	30	II	05 26 02	IS	EV	MX	RW	DZ	UZ	JO	AO	CH	lqy	ktl acw	zsl wzo			
649	30	II	12 24 03	DJ	AT	CV	IO	EH	QS	LW	PZ	PH	BH	loc acn	oww vwd			
649	28	II	06 58 16	DI	CN	BR	PV	GR	PV	AI	BK	OT	MQ	EU	BL	OJ	lrb cld	ude rzh
649	27	III	1 IV	DY	IN	BV	QR	AM	LO	PP	HT	EX	UW	woj fbb	vct uis			
649	26	I	IV	VZ	AL	RT	KO	CG	EL	BJ	DU	PS	HP	xle gbo	uev rxm			
649	25	IV	III	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc uhq	uew uit			
649	24	V	I	TY	AS	OW	KV	JM	DR	HX	OL	CZ	HU	kpl rwl	vci tlg			
649	23	IV	II	QV	FR	AK	EO	DH	CJ	MZ	SO	ON	LT	ebn rwm	udf tlo			
649	22	II	IV	PJ	ES	IM	RX	LV	AO	BX	WZ	GN	CH	jac acx	mwe wve			
649	21	I	V	RU	HL	PY	OS	GZ	DM	AW	CE	TE	NX	jpw del	mwf wvf			
649	20	III	IV	QZ	AO	QZ	AO	QZ	AO	QZ	AO	QZ	AO	jcd cef	nvo ysh			
649	19	V	III	PH	WT	DL	CM	AE	TZ	J5	G1			ief fpx	jwg tlg			
649	18	IV	II	IV	IV	IV	IV	IV	IV	IV	IV	IV	IV	isa gw	voj rxn			
649	17	I	IV	HM	JO	DI	NR	BY	XZ	OS	PU	FP	CT	mae hzi	sog ysi			
649	16	V	III	DS	HY	MR	OW	LX	AJ	BQ	CO	IP	NT	tdp dhh	fkv uiv			
649	15	II	IV	AI	BT	MV	HU	GM						imz noa	tjv xtk			
649	14	IV	I	FW	EL	DO	KN	MO						zgr dgi	gjo ryg			
649	13	I	III	RZ	OQ	CP	SX	KN						tjw xtl	tjw xtl			
649	12	V	II	LR	IK	MS	QO	HW	PT	OO	VX	PZ	EN	sea rly	soi wvh			
649	11	II	IV	QY	B5	LN	KT	AP	UD	WO	RV	KZ		lrc zbx	ybm rxo			
649	10	III	V	PI	NQ	SY	CU	BZ	AN	EL	TX	DO	JP	edj eyr	yby tih			
649	9	V	I	UX	I2	HN	BK	QO	CP	PT	JY	MW	AR					
649	8	IV	II	DU	GU	BW	NP	HK	A2	CI	PO	JX	VY					
649	7	I	IV	IL	AF	EU	HO	MV	CL	OK	QO	BI	PU	HS	FX	NW	EY	
649	6	III	I	QT	WZ	KV	GM	AC	BL	O2	EK	QW	OP	SU	DH	JN	TX	
649	5	V	II	BP	NR	DX	CS	KR	MP	CN	BP	EH	Z2	IN	AV	GJ	LO	
649	4	II	IV					BN	HU	EO	PY	KQ	CP	OS	JW	AI	VZ	
649	3	V	I					DP	BM	N2	CK	OQ	HV	AP	UY	SW	JO	
649	2	IV	V															
649	1	II	I															

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3$$

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Minder 2 im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

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

Maschinen-Nr.	Wellenlage	Ringstellung	S t e c h e r v e r b i n d u n g e n										Kenngruppen				
			an der Umschleudre										am Stecherbrett				
			1	2	3	4	5	6	7	8	9	10					
0490	3	I	4	05	24	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LY	wny dgy ekb rig	
0491	3	I	5	26	02	15	EV	MX	RW	DT	UZ	QJ	AO	CH	LQ	ktl acw zsi wzo	
0492	3	I	2	24	03	KM	AX	PZ	00	DJ	AT	CV	10	EH	QS	ioc acn ovw wwd	
0493	28	II	III	V	05	08	16	DI	CN	BR	PV	CR	PV	AI	DK	1rb cid ude rsh	
0494	27	III	I	IV	11	03	07	LT	EQ	H5	UW	DY	IN	BV	OR	woj fbh vcl uiz	
0495	26	I	IV					VZ	AL	RT	KO	CG	EL	BJ	DU	xie gbo uev ram	
0496	25	IV	III					OR	PV	AD	IT	PK	HL	LS	ES	ouc uho uew uit	
0497	24	V	I					TY	AS	OW	KV	JM	DR	HX	OL	kpl rwl vci tio	
0498	23	IV	II					QV	FR	AK	OE	DH	CJ	MZ	SO	ebn rwn udf tic	
0499	22	II	IV	V	01	09	21	IU	AS	DV	OL	FJ	ES	IM	RX	lqj acx mwe wvc	
0500	21	I	V	II	13	05	19	PT	OX	EZ	CH	RU	HL	PY	OS	jpw del mwf wvf	
0501	20	III	IV	V	24	00	01	QZ	AL	UV	AY	AW	SG	WZ	CN	jqd cef nvo ysh	
0502	19	V	III	I	17	02	04	FR	WT	DL	CM	AE	TZ	J5	G1	iefj spx jwg tig	
0503	18	IV	II	V	15	02	05	IV	AQ	KW	FX	MT	PS	LU	BD	isa gbw vej rxn	
0504	17	I	IV	II	21	10	08	FR	LS	EM	OV	OY	QX	AP	JP	mae hzi sog ysi	
0505	16	V	II	III	08	16	13	HM	JO	DI	NR	BY	XZ	OS	PU	tdp dhh fkb uiv	
0506	15	II	IV	I	01	03	07	DS	EY	MR	OW	LX	AJ	BQ	CO	ldw hzj soh wvg	
0507	14	IV	I	V	15	11	05	AI	BT	MV	HU	OM				imz noa tjo xtk	
0508	13	I	III	II	13	20	03	FW	EL	DO	KN	LY				xgr gdz gjo ryg	
0509	12	V	I	IV	18	10	07	RZ	OQ	CP	SX	KN				zdy rkj tjw xtl	
0510	11	II	IV	III	02	26	15									zea rfy soi wwh	
0511	10	III	V	IV	23	21	04	LR	IK	MS	QU	HW	PT	00	VX	lrc zbx ybm rxo	
0512	9	V	I	III	16	04	08	QY	B5	LN	KT	AP	IU	DH	RO	edj eyr vby tlh	
0513	8	IV	II	V	13	19	25	PI	NQ	SY	CU	BZ	AN	EL	TX		
0514	7	I	IV	II	09	03	22	UX	I2	HN	BK	QO	CF	PT	JY		
0515	6	III	I	V	11	18	14	DQ	GU	BW	NP	HK	A2	CI	PO		
0516	5	V	II	IV	23	02	25	IL	AF	EU	HO	MV	CL	OK	QO		
0517	4	II	IV	I	04	21	09	QT	WZ	KV	OM	AC	BL	O2	EK		
0518	3	V	I	II	19	11	06	BP	NR	DX	CS	KR	MP	CN	BP		
0519								BN	HU	EO	PY	KQ	CP	OS	JW	AI	agb bdy iyf xtd
0520	2	IV	V	I	16	14	02	DP	BM	N2	CK	OY	HQ	AP	UY	SW	kgf edf gix wuv

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq 150 \text{ undecillion}$$

Second World War

Geheime Kommandosache!

Jeder einzelne Lageschlüssel ist geheim.

Minder 2 im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

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

Maschinen-Nr.	Wellenlage	Ringstellung	S t e c h e r v e r b i n d u n g e n										Kenngruppen			
			an der Umschleifvorrichtung													
			am Stecherbrett													
			1	2	3	4	5	6	7	8	9	10				
0490	3	I	4	05	24	SZ	GT	DV	KU	FO	MY	EW	JN	LX	wny dgy	ekb rig
0491	3	I	5	26	02	15	EV	MX	RW	DT	UZ	QY	AO	CH	ktl acw	zsi wzo
0492	3	I	2	24	03	DJ	AT	CV	IO	EH	QS	LW	PZ	PH	ioc acn	ovw wwd
0493	28	II	III	V	05	08	16	DI	CN	BR	PV	CR	PV	AI	1rb cid	ude rsh
0494	27	III	I	IV	11	03	07	LT	EQ	H5	UW	DY	BN	OR	woj fbh	vcl uiz
0495	26	I	IV					VZ	AL	RT	GO	CG	EI	BJ	xie gho	uev ram
0496	25	IV	III					OR	PV	AD	IT	PK	HL	LS	ouc ubq	uew uit
0497	24	V	I					TY	AS	OW	KV	JM	DR	HX	klp rwl	vci tio
0498	23	IV	II					QV	FR	AK	EO	DH	CJ	MZ	ebn rwn	udf tlo
0499	22	II	IV	V	01	09	21	FJ	ES	IM	RX	LV	AY	SO	jac acx	mwe wvc
0500	21	I	V	II	13	05	19	RU	HL	PY	OS	GZ	DM	AW	jpw del	mwf wvf
0501	20	III	IV	V	24	00	01	QZ	AO	QV	UY	SV	JL	OE	jgd cef	nvo ysh
0502	19	V	III	I	17	02	06	FR	WT	DL	CM	AE	TZ	J5	ief fpx	jwg tlg
0503	18	IV	I	V	15	02	07	IV	AQ	KW	FX	MT	PS	LU	isa gbw	vcj rxn
0504	17	I	IV	II	21	10	08	FR	LS	EM	OV	OY	QX	AP	mae hzi	sog ysi
0505	16	V	II	III	08	16	13	HM	JO	DI	NR	BY	XZ	OS	tdp hzb	fkv uiv
0506	15	II	IV	I	01	03	07	DS	HY	MR	OW	LX	AJ	BQ	ldw hzj	soh wvg
0507	14	IV	I	V	15	11	05	AI	BT	MV	HU	OM			imz noa	tjv xtk
0508	13	I	III	II	13	20	03	FW	EL	DO	KN	LY			xgr gdz	gjo ryg
0509	12	V	I	IV	18	10	07	RZ	OQ	CP	SX	KN			zdy rkj	tjw xtl
0510	11	II	IV	III	02	26	15	LR	IK	MS	QU	HW	PT	OO	lrc zbx	ybm rxo
0511	10	III	V	IV	23	21	04	QY	B5	LN	KT	AP	UD	HO	edj eyr	vby tlh
0512	9	V	I	III	16	04	08	PI	NQ	SY	CU	BZ	AN	EL		
0513	8	IV	II	V	13	19	25	UX	I2	HN	BK	QO	CF	PT	1	
0514	7	I	IV	II	09	03	22	DQ	GU	BW	NP	HK	A2	CI	po jx	vy
0515	6	III	I	V	11	18	14	IL	AF	EU	HO					
0516	5	V	II	IV	23	02	25	MT	CL	OK	QO	BI	FU	HS	px dh	nm ey
0517	4	II	IV	I	04	21	09	QT	WZ	KV	OM	AC	BL	O2	ek qu	sp uh
0518	3	V	I	II	19	11	06	BP	NR	DX	CS	KR	MP	CN	BP	EH
0519	2	IV	V	I	16	14	02	BN	HU	EO	PY	KQ	CP	OS	JW	AI
0520	1	III	IV	II	23	12	10	DP	BM	N2	CK	OQ	HV	AP	UY	SW

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq 150 \text{ undecillion}$$

Nr. 00190

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

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

Second World War

[illegible]
$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150 \text{ undecillion}$$

789 decillion 931 nonillion 331 octillion

Nr. 00190

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

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

Second World War

Geheime Kommandosache! Jede einzelne Lageschlüssel ist geheim. Mithr. 2 im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Maschinen- Nr.	Wellenlage	Ringstellung	S t e c h e r v e r b i n d u n g e n										Kenngruppen			
			an der Umkleenachse	1	2	3	4	5	6	7	8	9	10			
049 3		4 05 24		SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny dgy	ekb rig	
049 3		05 26 02		15	EV	MX	RW	DT	UZ	JY	AO	CH	NY	ktl acw	zsi wzo	
049 2		02 24 03	KM AX PZ 00	DJ	AT	CV	10	ER	QS	LW	PZ	PH	BH	ioc acn	ovw wvd	
049 26	II III	06 08 16	DI CN BR PV	CR	PV	AI	DK	OT	HQ	EU	BL	PL	OJ	lrb cid	ude rzh	
049 27	III I	11 03 07	LT EQ H5 U0	DY	IN	BV	OR	AM	LO	PP	HT	EX	UW	woj fbh	vcl uis	
049 26	I IV			VZ	AL	RT	KO	CG	EI	BJ	DU	PS	HP	xle gbo	uev ram	
049 25	IV III			OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc uhq	uew uit	
049 24	V I			TY	AS	OW	KV	JN	DR	HX	OL	CZ	NU	kpl rwl	vci tio	
049 23	IV II			QV	FR	AK	EO	DH	CJ	MZ	SO	ON	LT	ebn rwn	udf tiq	
049 22	II IV	01 09 21	IU AS DV OL	FJ	ES	IM	RX	LV	AY	AO	BX	WZ	GN	jac acx	mwe wve	
049 21	I V	13 05 19	PT OX FZ CH	RU	HL	PY	OS	GZ	DM	AW	CE	TE	NX	jpw del	mwf wrf	
049 20	III IV	24 00 01		QZ	AO	UW	SV	JL	OE	DE	TW			jgd cef	nvo ysh	
049 19	V III	17 02 03		FR	WT	DL	CM	AE	TZ	J5	G1			ief fpx	jwg tig	
049 18	IV V	15 02 03		IV	AO	KW	FY	KT	PS	LP	BD			isa gbw	vej rxn	
049 17	I IV	21 10 06		LS	EM	OV	OY	QX	AF	JP	BU			mae hzi	sog ysi	
049 16	V II	08 16 13		HM	JO	DI	NR	BY	XZ	OS	PU	PQ	NT	tép dhh	fkf uiv	
049 15	II IV	01 03 07		DS	HY	MR	OW	LX	AJ	BQ	CO	IP	CT	ldw hzj	soh wvg	
049 14	IV I	15 11 05	AI BT MV HU	OM										imz noa	tjv xtk	
049 13	I III	13 20 03	FW EL DO KN	LY										zgr gda	gjo ryg	
049 12	V I	18 10 07	RZ OQ CP SX	KN										zdy rkj	tjw xtl	
049 11	II IV	02 26 15		LR	IK	MS	QU	HW	PT	OO	VX	PZ	EN	lrc zbx	ybm rxo	
049 10	III V	23 21 04		QY	B5	LN	KT	AF	IU	DW	HO	RV	JZ	edj eyr	vby tlh	
049 9	V I	16 04 08		PI	NQ	SY	CU	BZ	AN	EL	TX	DO	KP			
049 8	IV II	13 09 25		UX	IZ	HN	BK	QO	CF	PT	JY	MW	AR			
049 7	I IV	09 03 22		DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY			
049 6	III I	11 18 14		IL	AF	EU	HO	MV	CL	OK	QO	BI	FU	hps dxj	nw ey	
049 5	V II	23 02 25		QT	WZ	KV	GM	AC	BL	OZ	EK	QU	OS	PU	DH	TX
049 4	II IV	04 21 09	BP NR DX CS		KR	MP	CN	BP	EH	DZ	1N	AV	GJ	LO		
049 3	V I	19 11 06		BN	HU	EO	PY	KQ	CP	OS	JW	AI	VZ	agd bwy	iyf xtd	
049 2	IV V	16 14 02		DP	BM	NZ	CK	OV	HQ	AF	UY	SW	JO	kgl edf	giz wuv	

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150 \text{ undecillion}$$

789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion

Second World War

Geheime Kommandosache! Jede einzelne Lageschlüssel ist geheim. Mündlich im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Platz Nr.	Wolkenlage	Ringstellung	Stichvererbinderungen										Kerngruppen								
			an der Umkehrrolle		am Stecherbrett																
			1	2	3	4	5	6	7	8	9	10									
040	I	III	4	09	24			SZ	OT	DV	KU	FO	MY	EW	JH	IX	LQ	wny dgy	ekb rzg		
040	I	III	5	26	02			IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl acw	zsl wzo		
040	I	III	6	24	03			DJ	AT	CV	IO	ER	GS	LW	PZ	FN	BH	ioc acn	oww vwd		
040	II	III	V	06	58	16		DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU	BX	LP	OJ
040	II	III	IV	11	03	07		LT	EQ	HS	UW	DY	IN	BV	QR	AM	LO	PP	HT	EX	UW
040	II	III	IV	12	08	16						VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP
040	II	III	IV	13	08	16						OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW
040	II	III	IV	14	08	16						TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU
040	II	III	IV	15	08	16						QV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT
040	II	III	IV	16	08	16						PJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN
040	II	III	IV	17	08	16						RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX
040	II	III	IV	18	08	16															
040	II	III	IV	19	08	16															
040	II	III	IV	20	08	16															
040	II	III	IV	21	08	16															
040	II	III	IV	22	08	16															
040	II	III	IV	23	08	16															
040	II	III	IV	24	08	16															
040	II	III	IV	25	08	16															
040	II	III	IV	26	08	16															
040	II	III	IV	27	08	16															
040	II	III	IV	28	08	16															
040	II	III	IV	29	08	16															
040	II	III	IV	30	08	16															
040	II	III	IV	31	08	16															
040	II	III	IV	32	08	16															
040	II	III	IV	33	08	16															
040	II	III	IV	34	08	16															
040	II	III	IV	35	08	16															
040	II	III	IV	36	08	16															
040	II	III	IV	37	08	16															
040	II	III	IV	38	08	16															
040	II	III	IV	39	08	16															
040	II	III	IV	40	08	16															
040	II	III	IV	41	08	16															
040	II	III	IV	42	08	16															
040	II	III	IV	43	08	16															
040	II	III	IV	44	08	16															
040	II	III	IV	45	08	16															
040	II	III	IV	46	08	16															
040	II	III	IV	47	08	16															
040	II	III	IV	48	08	16															
040	II	III	IV	49	08	16															
040	II	III	IV	50	08	16															
040	II	III	IV	51	08	16															
040	II	III	IV	52	08	16															
040	II	III	IV	53	08	16															
040	II	III	IV	54	08	16															
040	II	III	IV	55	08	16															
040	II	III	IV	56	08	16															
040	II	III	IV	57	08	16															
040	II	III	IV	58	08	16															
040	II	III	IV	59	08	16															
040	II	III	IV	60	08	16															
040	II	III	IV	61	08	16															
040	II	III	IV	62	08	16															
040	II	III	IV	63	08	16															
040	II	III	IV	64	08	16															
040	II	III	IV	65	08	16															
040	II	III	IV	66	08	16															
040	II	III	IV	67	08	16															
040	II	III	IV	68	08	16															
040	II	III	IV	69	08	16															
040	II	III	IV	70	08	16															
040	II	III	IV	71	08	16															
040	II	III	IV	72	08	16															
040	II	III	IV	73	08	16															
040	II	III	IV	74	08	16															
040	II	III	IV	75	08	16															
040	II	III	IV	76	08	16															
040	II	III	IV	77	08	16															
040	II	III	IV	78	08	16															
040	II	III	IV	79	08	16															
040	II	III	IV	80	08	16															
040	II	III	IV	81	08	16															
040	II	III	IV	82	08	16															
040	II	III	IV	83	08	16															
040	II	III	IV	84	08	16															
040	II	III	IV	85	08	16															
040	II	III	IV	86	08	16															
040	II	III	IV	87	08	16															
040	II	III	IV	88	08	16															
040	II	III	IV	89	08	16															
040	II	III	IV	90	08	16															
040	II	III	IV	91	08	16															
040	II	III	IV	92	08	16															
040	II	III	IV	93	08	16</															

Second World War

Geheime Kommandosache! Jede einzelne Lageschlüssel ist geheim. Mündlich im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Platz Nr.	Wolkenlage	Ringstellung	Stichvererbinderungen										Kenngruppen	
			an der Umkehrrolle		am Stecherbrett									
			1	2	3	4	5	6	7	8	9	10		
649	III	IV	4	09	24								wny dgy	ekb rzg
649	III	IV	5	26	02								ktl acw	zsl wzo
649	III	IV	12	24	03	KM	AX	PZ	OO				ioc zcn	oww vwd
649	III	IV	06	58	16	DI	CN	BR	PV				lrb cld	ude rzh
649	III	IV	1	IV	11	03	07	LT	EQ	HS	UW		woj fbb	vct uis
649	III	IV	2	IV	11	03	07						xle gbo	uev rxm
649	III	IV	25	IV	III								ouc uhq	uew uit
649	III	IV	24	V	I								kpl rwl	vci tlg
649	III	IV	23	IV	II								ebn rwm	udf tlo
649	III	IV	22	II	IV	V	01	09	21				jac acx	mwe wve
649	III	IV	21	I	V	II	13	05	19				jpw del	mwf wvf
649	III	IV	20	III	IV	V	24						jcd cef	nvo ysh
649	III	IV	19	V	III	I	17						ief fpx	jwg tlg
649	III	IV	18	IV	II	V	15						isa bw	vcj rxn
649	III	IV	17	I	IV	II	21	10	06				mae hzi	sog ysi
649	III	IV	16	V	III	II	08	16	13				tdp dhh	fkv uiv
649	III	IV	15	II	IV	I	01	03	07				ldw hzj	soh wvg
649	III	IV	14	IV	I	V	15	11	05				imz noa	tjv xtk
649	III	IV	13	I	III	II	13	20	03				zgr dgt	gjo ryg
649	III	IV	12	V	I	IV	18	10	07				tjw rkl	tjw xtl
649	III	IV	11	II	IV	III	02	26	15				sea rly	soi wvh
649	III	IV	10	III	V	IV	23	21	04				lrc zbx	ybm rxo
649	III	IV	9	V	I	III	16	04	08				edj eyr	yby tih
649	III	IV	8	IV	II	V	13	19	25					
649	III	IV	7	I	IV	II	09	03	22					
649	III	IV	6	III	I	V	11	18	14					
649	III	IV	5	V	II	IV	23	02	25					
649	III	IV	4	II	IV	I	04	21	09					
649	III	IV	3	V	I	II	19	11	06					
649	III	IV	2	IV	V	I	16	14	02					
649	III	IV	1	II	I	III	23	12	10					

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion

Nr. 00190

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

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

Second World War

Geheime Kommandosache! Jede einzelne Lageschlüssel ist geheim. Mündlich im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Platz Nr.	Wolkenlage	Ringstellung	Stichvererbinderungen										Reihennummern	
			an der Umkehrrolle		am Stecherbrett									
			1	2	3	4	5	6	7	8	9	10		
040	III	IV	4	09	24								wny dgy	ekb rzg
040	III	IV	5	26	02								ktl acw	zsl wzo
040	III	IV	12	24	03	KM	AX	PZ	OO				ioc zcn	oww vwd
040	III	IV	06	58	16	DI	CN	BR	PV				lrb cld	ude rzh
040	III	IV	1	IV	11	03	07	LT	EQ	HS	UW		woj fbb	vct uis
040	III	IV	26	1	IV								xle gbo	uev rxm
040	III	IV	25	IV	III								ouc uhq	uew uit
040	III	IV	24	V	I								kpl rwl	vci tlg
040	III	IV	23	IV	II								ebn rwm	udf tlo
040	III	IV	22	II	IV	V	01	09	21				jac acx	mwe wve
040	III	IV	21	I	V	II	13	05	19				ljd del	mwf wvf
040	III	IV	20	III	IV	V	24						jqd cef	nvo ysh
040	III	IV	19	V	III	I	17						ief fpx	jwg tlg
040	III	IV	18	IV	II	V	15						isa bw	vcj rxn
040	III	IV	17	I	IV	II	21	10	06				mae hzi	sog ysi
040	III	IV	16	V	II	III	08	16	13				tdp dhh	fkv uiv
040	III	IV	15	II	IV	I	01	03	07				ldw hzj	soh wvg
040	III	IV	14	IV	I	V	15	11	05				imz noa	tjv xtk
040	III	IV	13	I	III	II	13	20	03				zgr dgt	gjo ryg
040	III	IV	12	V	I	IV	18	10	07				tdw rkl	tjw xtl
040	III	IV	11	II	IV	III	02	26	15				sea rly	soi wvh
040	III	IV	10	III	V	IV	23	21	04				lrc zbx	ybm rxo
040	III	IV	9	V	I	III	16	04	08				edj eyr	yby tih
040	III	IV	8	IV	II	V	13	19	25					
040	III	IV	7	I	IV	II	09	03	22					
040	III	IV	6	III	I	V	11	18	14					
040	III	IV	5	V	II	IV	23	02	25					
040	III	IV	4	II	IV	I	04	21	09					
040	III	IV	3	V	I	II	19	11	06					
040	III	IV	2	IV	V	I	16	14	02					
040	III	IV	1	II	I	III	23	12	10					

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion

Second World War

Geheime Kommandosache! Jede einzelne Lageschlüssel ist geheim. Mündlich im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen - Schlüssel Nr. 649

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

Platz Nr.	Wolkenlage	Ringstellung	Stichverbindungen										Reihenfolgen	
			an der Umkehrrolle		am Stecherblatt									
			1	2	3	4	5	6	7	8	9	10		
049	III	IV	4	09	24								wny dgy	ekb rzg
049	III	IV	5	26	02								ktl acw	zsl wzo
049	III	IV	6	24	03	KM	AX	PZ	OO				ioc acn	oww vwd
049	III	IV	7	06	58	DI	CN	BR	PV				lrh cld	ude rzh
049	III	IV	8	11	03	LT	EQ	HS	UW				woj fbb	vct uis
049	III	IV	9	06	58								xle gbo	uev rxm
049	III	IV	10	06	58								ouc uhq	uew uit
049	III	IV	11	06	58								kpl rwl	vci tlg
049	III	IV	12	06	58								ebn rwm	udf tlo
049	III	IV	13	06	58								jac acx	mwe wve
049	III	IV	14	06	58								jpw del	mwf wvf
049	III	IV	15	06	58								jqd cef	nvo ysh
049	III	IV	16	06	58								ief fpx	jwg tlg
049	III	IV	17	06	58								isa gbw	voj rxn
049	III	IV	18	06	58								mae hzi	sog ysi
049	III	IV	19	06	58								tdp dhh	fkv uiv
049	III	IV	20	06	58								ldw hzj	soh wvg
049	III	IV	21	06	58								imz noa	tjv xtk
049	III	IV	22	06	58								zgr dgt	gjo ryg
049	III	IV	23	06	58								tjw xkl	tjw xtl
049	III	IV	24	06	58								sea rly	soi wvh
049	III	IV	25	06	58								lrc zbx	ybm rxo
049	III	IV	26	06	58								edj eyr	yby tih
049	III	IV	27	06	58									
049	III	IV	28	06	58									
049	III	IV	29	06	58									
049	III	IV	30	06	58									
049	III	IV	31	06	58									
049	III	IV	32	06	58									
049	III	IV	33	06	58									
049	III	IV	34	06	58									
049	III	IV	35	06	58									
049	III	IV	36	06	58									
049	III	IV	37	06	58									
049	III	IV	38	06	58									
049	III	IV	39	06	58									
049	III	IV	40	06	58									
049	III	IV	41	06	58									
049	III	IV	42	06	58									
049	III	IV	43	06	58									
049	III	IV	44	06	58									
049	III	IV	45	06	58									
049	III	IV	46	06	58									
049	III	IV	47	06	58									
049	III	IV	48	06	58									
049	III	IV	49	06	58									
049	III	IV	50	06	58									
049	III	IV	51	06	58									
049	III	IV	52	06	58									
049	III	IV	53	06	58									
049	III	IV	54	06	58									
049	III	IV	55	06	58									
049	III	IV	56	06	58									
049	III	IV	57	06	58									
049	III	IV	58	06	58									
049	III	IV	59	06	58									
049	III	IV	60	06	58									
049	III	IV	61	06	58									
049	III	IV	62	06	58									
049	III	IV	63	06	58									
049	III	IV	64	06	58									
049	III	IV	65	06	58									
049	III	IV	66	06	58									
049	III	IV	67	06	58									
049	III	IV	68	06	58									
049	III	IV	69	06	58									
049	III	IV	70	06	58									
049	III	IV	71	06	58									
049	III	IV	72	06	58									
049	III	IV	73	06	58									
049	III	IV	74	06	58									
049	III	IV	75	06	58									
049	III	IV	76	06	58									
049	III	IV	77	06	58									
049	III	IV	78	06	58									
049	III	IV	79	06	58									
049	III	IV	80	06	58									
049	III	IV	81	06	58									
049	III	IV	82	06	58									
049	III	IV	83	06	58									
049	III	IV	84	06	58									
049	III	IV	85	06	58									
049	III	IV	86	06	58									
049	III	IV	87	06	58									
049	III	IV	88	06	58									
049	III	IV	89	06	58									
049	III	IV	90	06	58									
049	III	IV	91	06	58									
049	III	IV	92	06	58									
049	III	IV	93	06	58									
049	III	IV	94	06	58									
049	III	IV	95	06	58									
049	III	IV	96	06	58									
049	III	IV	97	06	58									
049	III	IV	98	06	58									
049	III	IV	99	06	58									
049	III	IV	100	06	58									

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million

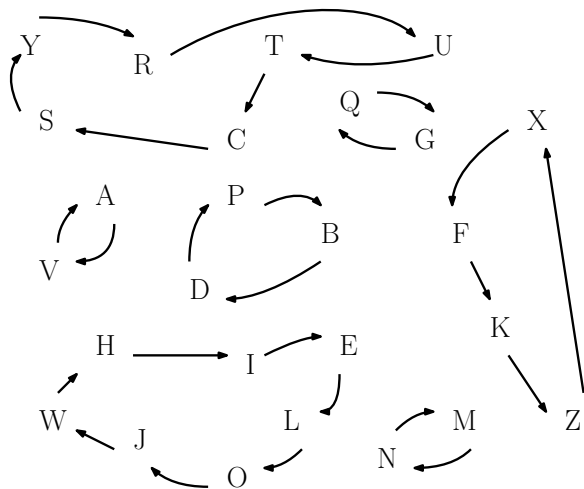
Nr. 00190

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

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \simeq 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million
 $\simeq 10^{38}$ keys

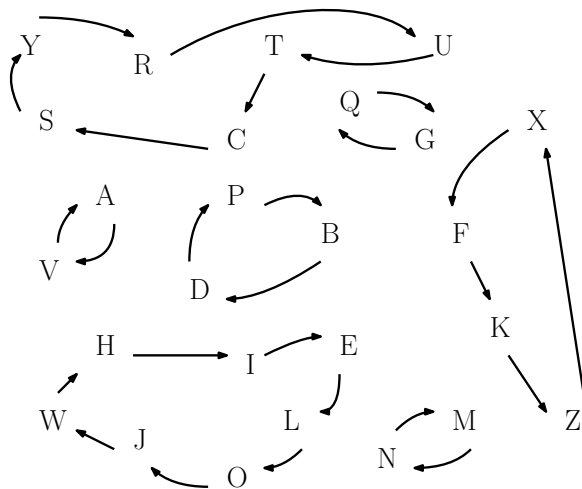
Second World War

A random permutation of the alphabet:



Second World War

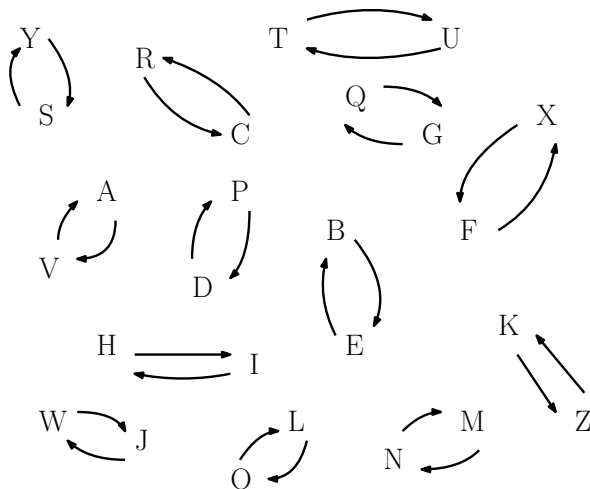
A random permutation of the alphabet:



Cycle structure: 6-2-2-3-4-7-2

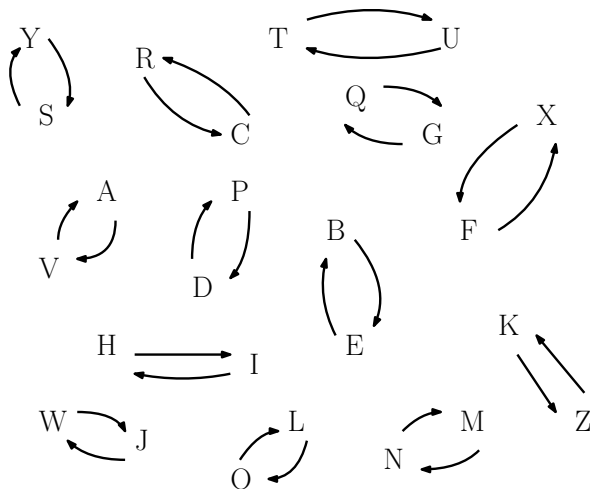
Second World War

An enigma permutation of the alphabet:



Second World War

An enigma permutation of the alphabet:



Cycle structure: 2-2-2-2-2-2-2-2-2-2-2-2

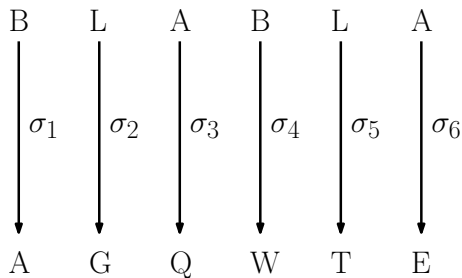
Don't use just one daily key!

1. If you use the same daily key on all messages that day, then one could try frequency analysis on all the first characters of all the messages. Then frequency analysis on all second characters, etc.
2. So, choose a random message key (rotor start positions, e.g. BLA) and send that using the daily key.
3. Then send the message in the message key.
4. BUT: radio is noisy, so send it twice (send BLABLA encrypted with daily key).

Cryptanalysis of Enigma

Message key: BLA

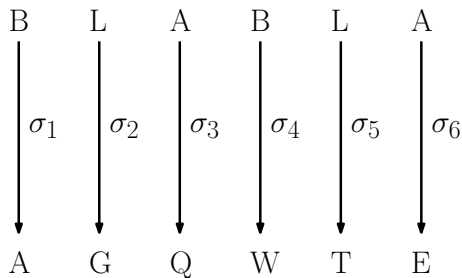
Encrypted message key (using daily key):



Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



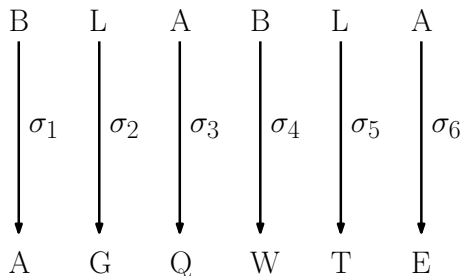
Learned information about $\sigma_4 \circ \sigma_1$:

$$A \rightarrow W$$

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

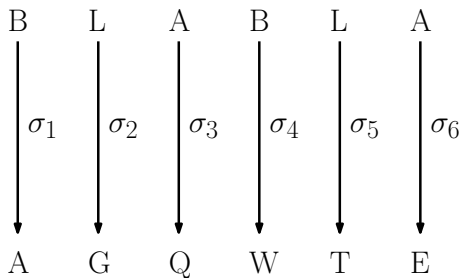
$$A \rightarrow W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

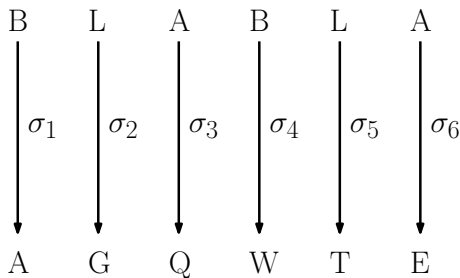
$$A \rightarrow W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.
2. This depends only on daily key rotor positions (not plugboard).

Cryptanalysis of Enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

$$A \rightarrow W$$

1. Collect these bits of info to discern cycle structure of $\sigma_4 \circ \sigma_1$.
2. This depends only on daily key rotor positions (not plugboard).
3. Use a lookup table to determine rotor positions!

Cryptanalysis of Enigma



Bletchley Park Bombe replica (Antoine Taveneaux)

Classical cryptography terminology

Substitution cipher. A cipher that acts on letters of the plaintext one-by-one according to a permutation of the alphabet.

Examples:

1. Caesar cipher
2. Affine cipher
3. Newspaper Cryptogram puzzles

Classical cryptography terminology

Transposition cipher. A cipher that acts on the plaintext by reordering its letters.

Examples:

1. Second half of ADFGVX cipher
2. RailFence Cipher

HELPI MTRAPPED BEHIND A FENCE

—	H	—	I	—	A	—	D	—	I	—	F	—	E	—
—	E	—	P	—	M	—	R	—	P	—	E	—	B	—
—	L	—	T	—	P	—	E	—	D	—	N	—		—

H I A D I F E E P M R P E B H N A E C L T P E D N

Classical cryptography terminology

Fractionating cipher. A cipher that replaces each plaintext character with several ciphertext characters.

Examples:

1. Polybius square (first half of ADFGVX cipher)

Classical cryptography terminology

Polyalphabetic cipher. A substitution cipher that uses a changing substitution key for each character.

Examples:

1. Vigenere cipher.
2. Enigma machine.

Classical cryptography terminology

Block cipher. A cipher that encrypts block-by-block instead of character-by-character.

Examples:

1. Hill cipher.

Classical cryptography terminology

Diffusion. A property of a cipher, namely that changing one character of plaintext results in many characters of ciphertext changing, and vice versa.

The idea: Prevents frequency analysis, because statistics of the plaintext "diffuse" to statistics of the ciphertext.

Examples:

1. Block ciphers satisfy diffusion (more if bigger blocks).
2. Vigenere cipher does not satisfy diffusion.

Classical cryptography terminology

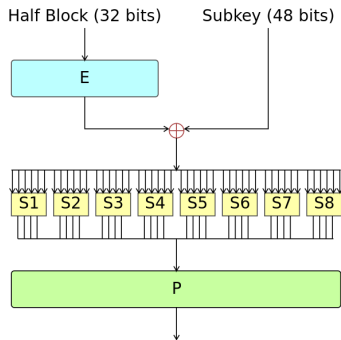
Confusion. A property of a cipher, namely that changing the key only slightly will result in the ciphertext changing a lot.

The idea: Prevents cryptanalysing the key one piece at a time, since each character of ciphertext depends on many parts of the key.

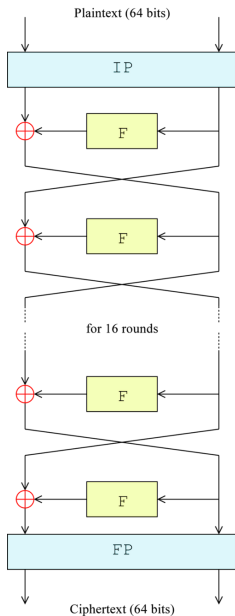
Examples:

1. Enigma has a fair bit of confusion. (A different rotor position on one rotor for example will change everything.)
2. Vigenere cipher does not satisfy confusion. (Each ciphertext character depends on only one character of the key.)

Advent of Computers: DES (Data Encryption Standard)



14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



Important points about DES (Data Encryption Standard)

Important points about DES (Data Encryption Standard)

1. Block cipher

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
 - ▶ send a DES key with public key cryptography then use DES

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
 - ▶ send a DES key with public key cryptography then use DES
7. Used 1975-2000
 - ▶ in 1999: broken in 22 hours, 15 minutes (distributed)
 - ▶ now you can buy a fancy computer and do it in 15 days

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
 - ▶ send a DES key with public key cryptography then use DES
7. Used 1975-2000
 - ▶ in 1999: broken in 22 hours, 15 minutes (distributed)
 - ▶ now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
 - ▶ Triple DES is an alternative where you do DES three times.

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
 - ▶ send a DES key with public key cryptography then use DES
7. Used 1975-2000
 - ▶ in 1999: broken in 22 hours, 15 minutes (distributed)
 - ▶ now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
 - ▶ Triple DES is an alternative where you do DES three times.
9. Carefully designed to maximize diffusion, avoid differential cryptanalysis (NSA controversy) etc.

Important points about DES (Data Encryption Standard)

1. Block cipher
2. Runs on binary bits (natural for a computer)
3. Components: permuting digits, expansion, XOR, S-boxes
 - ▶ Very classical cipher ideas
 - ▶ Very efficient to implement on computers
4. Reversible (if you use keys in opposite order, decryption is the same process as encryption)
5. Cryptanalysis: Exhaustive search, differential cryptanalysis, linear cryptanalysis
6. Symmetric-key cryptography; used in tandem with public-key cryptography
 - ▶ send a DES key with public key cryptography then use DES
7. Used 1975-2000
 - ▶ in 1999: broken in 22 hours, 15 minutes (distributed)
 - ▶ now you can buy a fancy computer and do it in 15 days
8. AES/Rijndael replaced it; similar block cipher, bigger and better.
 - ▶ Triple DES is an alternative where you do DES three times.
9. Carefully designed to maximize diffusion, avoid differential cryptanalysis (NSA controversy) etc.
10. Mathematically speaking, the culmination of classical cryptography and the beginning of modern academic cryptography.