A Whirlwind Tour of Cryptography

Katherine E. Stange, Math 4440/5440 First Day (August 26, 2024)

Ancient Cryptography

אבגדהוזחטיכלמנסעפצקרשת תשרקצפעסנמלכיטחזוהדגבא Atbash Cipher Jeremiah 25:26 "The king of Sheshach shall drink after them" $bb1 \rightarrow bb1$ בבל)

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

Ancient Cryptography



Ceasar Wheel

image: Subjectiveart, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

Last 500 years

Vigenère Cipher



"impossible of translation" - Scientific American, 1917

Example of a substitution cipher (replacing characters)

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

First World War



Plaintext: attack at dawn

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

Ciphertext: GGDGGAXDDXDFDXADFFGGAGXD

Includes an example of a **transposition cipher** (reordering characters)

Second World War



Wartime Enigma Machine

at left: public domain; at right: Bundesarchiv, Bild 1011-769-0229-10A / Borchert, Erich (Eric) / CC-BY-SA 3.0, CC BY-SA 3.0 DE https://creativecommons.org/licenses/by-sa/3.0/de/deed.en, via Wikimedia Commons

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 のへで

Second World War



Second World War

	Ac	h	tur	igr	LU] Schlü[[e	Imit	telo	ürfe	n nidi	tunt	uj1	ntin	Jeind	esha	nd fo	llen.	Bei	ie fah	r reft	los u	nd fr	ülyei	lig vern	iditen.		
	Tonals- 109	1	W e I	3 e n l a g	e .	Ring	ftellu	ng	en	ber Um	5 Achemic	l e Ișe	di v	r U 7	• • •	b i ii ein	ð u Stech	erbrett 6 -	е т 7		•	10	1	frenns	ruppe	n
05	21	1	1	v	111	14	20	24					SZ	0T	DV	KU	FO	МХ	EW	JN	11	LQ	wny	dgy	exp	TZE
10	20	1.	NY.	111	11	05	26	62					15	EV	MX	RW	DT	UZ	JQ	٨0	CH	NY	811	acw	zsi	24
20	30		111	n	1	12	24	03	KM	XA	PZ	00	DJ	AT	CV	10	ER	QS	LW	P2	FN	BH	ioc	acu	OVW	WV
10	29				v	05	0.0	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	NQ	EU	BX	LP	GJ	115	cld	ude	TZ
10	20			T	11	11	03	07	LT	EO	HS	UW	DY	11	BV	OR	MA	LO	PP	HT	EX	UW	woj	fbh	vet	ui.
10	21		1	11/	W	17	22	10					VZ	AL	RT	ко	co	E1	BJ	DU	FS	HP	xle	gbo	uev	L XI
412	20		111			08	25	12	100			1	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	ui
949	10		N.		iN	05	19	14		7			TY	AS	0%	κv	JM	DR	нх	0L	C2.	NU	k.pl	rwl	vci	tle
146	14					24	12	04					i qv	FR	AK	EO	DH	CJ	N2	SX	GN	LT	ebn	rwm	udf	tie
940	123			11	w	01	00	21	111	24	DV	01.	FJ	ES	IM	RX	LV	AY	0U	BO	WZ	CN	190	acx	mwe	ww
946	14			NV NV		13	05	10	10	~~		CN	RU	HL	FY	05	02	DM	A.M.	CE	TV	NX	jpw	del	mwi	wv.
010	12			IV	v	24	01	10	PT	0.1	5.6	C n	DP	10	QZ	UA	RY	SV	JL	OX	BE	TW	jqd	cef	nvo	yst
048	10		W	111	;	17	25	20	MR	KN	RÓ	PW	OX.	PR	FH	WY	DL	CM	AE	TZ	1,5	GI	idf	fpx	JWE	118
040		-	"IV		· v	15	23	26					EJ	OY	IV	AQ	K₩	FX	NT	PS	LU	BD	-152	*pw	VCJ	TXI
840	1.	2	-	IV	11	21	10	05	1	1200		-	IR	KZ	LS	EM.	٥٧	٥Y	QX	AP	JP	BU	mae	hzi	SOE	y 5 1
840	E	2	v	11	111	08	16	13					HM	10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	rob	
649		5	11	IV	1	01	03	07					DS	HY	MR	0.8	ΓX	٧J	BQ	co	IP	NT	Idw	nzj	tiv	rty
640		4	IV	1	v	15	11	05	AT	BT	MV	HU	I GM	JR	KS	IY	HZ.	PL	XA	BT	CQ	NV	1 mz	der	gio	rva
849		3	1	in	11	13	20	03	PW	FL.	DO	KN	LY	AG	KM	BR	IQ	10	NV	5.	DT NI	DW	2 GI	rkf	tiw	xti
645	, -	12	v	11	IV	18	10	07	1.0	00	CP	C Y	1 MU	BP	CY	RZ	KX	AN	JT	DG	TL DY	TW	Luy	riv	soi	wył
841		11	11	IV	111	02	26	15	RL	00	01	34	KN	UY	HR	PW	FM	80	52	Q1	DA D7	FN	line	Thx	ybm	rxo
841	2	10	111	v	1V	23	1 21	01					LR	18	MS	QU	1.0	TI	DW	10	BV	.1.2	edi	evr	vby	tih
841	9	9	v	1	111	10	04	03					QY	BS	LN	AT	NP D2	10	PL.	TY	no	KP	viz	dha	ekc	tli
84	9	8	1V	н	v	13	3 19	25		1.1.2.5			FI	NQ	51	CU BY	86	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi
84	9	7	1	1V	11	. 0	0	3 22	2				. UX	12		NP	HW	42	CT	PO	JX	VY	120	cft	zsk	wbj
64	9	6	in	I	v	1	1 18	3 1-	IL	AP	EU	но	: DQ	CL.	OK	00	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
64	9	5	v	11	IV	2	3 0	2 2	01	WZ	KV	GM	AC	BL.	07	EK	0¥	OP	SU	DH	JM	тх	150	zby	vcy	ujb
64	9	4	11	17	1	0	4 2	1 0	1 100	NB	DX	cs	· KB	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak
84	9	3	v	1	11	1	9 1	1 0	D Dr	in		1	BN	HU	EQ	PY	KQ	CP	os	JW	AI	V2	aqd	bdy.	iyf.	xtd
64	9	2	17	v	1	11	0 1	4 0					DP	BM	NZ	CK	ov	NQ	AP	UY	SW	JO	kg1	cdf	giq	wuv

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = のへで

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

- 1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
- 2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

- 1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
- 2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
- 3. A decryption method, that uses the secret key to transform the ciphertext into the plaintext.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

- 1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
- 2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
- 3. A decryption method, that uses the secret key to transform the ciphertext into the plaintext.

Problems: key distribution

system	key	encryption	decryption
Ceasar			
Vigenère			
ADFGVX			
Enigma			

◆□▶ ◆□▶ ◆目▶ ◆目▶ ▲□▶ ◆□◆

system	key	encryption	decryption
Ceasar	shift	shift	shift
		forward	backward
Vigenère			
ADFGVX			

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

Enigma

system	key	encryption	decryption
Ceasar	shift	shift	shift
		forward	backward
Vigenère	sequence	shift	shift
	of shifts	forward	backward
ADFGVX	square &	complicated!	complicated
	column order		backwards!
Enigma	machine	press key,	press key,
	setup	read light	read light

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

The keyspace is the set of all possible secret keys.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

The **keyspace** is the set of all possible secret keys. A **cryptanalyst** tries to break a cryptosystem.

The **keyspace** is the set of all possible secret keys. A **cryptanalyst** tries to break a cryptosystem. The first, most naïve method is **exhaustive search**: trying all possible keys.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

The **keyspace** is the set of all possible secret keys.

A cryptanalyst tries to break a cryptosystem.

The first, most naïve method is **exhaustive search**: trying all possible keys.

key	plaintext	key	plaintext
0	WFYDAKZLWPL	13	JSLQNXMYJCY
1	XGZEBLAMXQM	14	KTMROYNZKDZ
2	YHAFCMBNYRN	15	LUNSPZOALEA
3	ZIBGDNCOZSO	16	MVOTQAPBMFB
4	AJCHEODPATP	17	NWPURBQCNGC
5	BKDIFPEQBUQ	18	OXQVSCRDOHD
6	CLEJGQFRCVR	19	PYRWTDSEPIE
7	DMFKHRGSDWS	20	QZSXUETFQJF
8	ENGLISHTEXT	21	RATYVFUGRKG
9	FOHMJTIUFYU	22	SBUZWGVHSLH
10	GPINKUJVGZV	23	TCVAXHWITMI
11	HQJOLVKWHAW	24	UDWBYIXJUNJ
12	IRKPMWLXIBX	25	VEXCZJYKVOK

What's better than exhaustive search?

A X Y D L B A A X R is L O N G F E L L O W

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBDBWAC AIOA OZB

F Z O L W . — W S Z D O W D P U O Z B W Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Source: www.dailyrepublic.com

What's better than exhaustive search?

A X Y D L B A A X R is L O N G F E L L O W

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBDBWAC AIOA OZB

F Z O L W . — W S Z D O W D P U O Z B W Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Source: www.dailyrepublic.com

The number of possible keys: 26!

What's better than exhaustive search?

A X Y D L B A A X R is L O N G F E L L O W

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBDBWAC AIOA OZB

F Z O L W . — W S Z D O W D P U O Z B W Yesterday's Cryptoquote: ONCE YOU DECIDE TO TITILLATE INSTEAD OF ILLUMINATE, YOU'RE ON A SLIPPERY SLOPE. — BILL MOYERS

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

Source: www.dailyrepublic.com

,	Acl	htu	i pn	Luf	tw	inf tel d	fer	1 - 17 11 nida	la∫	chi	ner art in	1-5 Jeind	(1) la	nd fo	llen.	Nr. Beil	64 iefah	49 1 reft	los 11	nd fr	ihsei	tig vern	iditen.		
Ĩ	nog	W o	lgenlog		Ring	ftellu	ng	en l	are Un	5 Achron	l e dyr	di e	e v 2	e'r 1	b i i	ð i Stech	erbrett 6 -	, y 1			10		henn	pruppe	n
20	21	1	v	111	14	2.9	24					SZ.	07	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	exp	rzg
30	20	137	111	11	05	26	62					15	EV	MX	RW	DT	UZ	JQ	٨0	CH	NY	k t l	acw	251	200
40	20	111	11	1	12	24	03	КМ	XA	PZ	00	DJ	TA	cv	10	ER	QS	LW	P2	FN	BH	ioc	acu	OVW	AA4
40	27	11		v	05	90	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.	EU	BX	\mathbf{P}	0 J	115	cld	ude	rzh
10	20	111	1	11/	11	03	07	1.7	EO	HS	UW	DY	IN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis
	21		11/	v	17	22	10	1				V2	AL	RT	KO	co	E1	BJ	DU	FS	HP	xle	gbo	uev	rxn
412	20	1			08	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
49	23	IV N		111	05	18	14		7.11.27			TY	AS	ow	κv	JM	DR	НΧ	GL	C2.	NU	k p l	rwl	vei	tiq
146	24				24	12	04					QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo
946	23	11	11	v	01	00	21	10		DV	01.	FJ	ES	IM	RX	LV	٨Y	00	BO	WZ	CN	100	acx	mwe	wvc
940	22	1	NV N		13	05	19	10	0.4	29	CN	RU	HL	FY	05	62	DM	¥.M	CE	TV	NX	Jpw	del	mwi	WVI.
040	21	in	11	v	24	01	10	1.1			DW	DF	10	QZ	ΑU	RY	sv	JL	0 X	BE	TW	jqd	cel	nvo	ysn +1a
640	10	v	111	1	17	25	20	MR	VII	by		OX.	PR	FH	WY	DL	CM	AE	72	15	GI	101	1.px	JWE	
040	19	TV	11	· v	15	23	26	1				EJ	OY	IV	AQ	КW	FX	NT	PS	ru	BD	158	*p*	vej	1 ×0
640	17	1	IV	1!	21	10	05	1	-			IR	KZ	LS	EM.	ov	OY	QX	AP	JP	80	mae	dbb	The	niv
649	1 16	v	11	111	08	16	13	1000				НМ	10	DI	NR	BY	XZ	05	PU	FQ	UT	top	bai	sob	WVP
649	15	11	IV	1	01	03	07					DS	HY	MR	0.8	LX	VJ	BG	00	11	MI	ima	nos	tiv	xtk
649	14	11	1	v	15	11	05	IAI	вт	MV	HU	1 OM	JR	KS	11	HZ.	PL	AA	DI	00	CT		dez	eio	rva
849	13	1	iII	11	13	20	03	FW	EL	DO	KN	LY	YO	KM	BR	10		12	na	II.	PW	zdy	rkf	tjw	xtl
649	12	V	1	IV	18	10	07	P7	00	CP	SX	I MU	Br	UD	RL DW	PH	10	57	07	DX	JV	203	riy	soi	wvh
049	11	11	IV.	111 -	02	26	15					KN	01	nn.	011	NW.	PT	00	VX	FZ	EN	Irc	zbx	vbm	TXO
849	10	III	v	17	23	21	01					LR	11	1.N	KT	AP	TU	DW	HO	RV	JZ	edj	eyr	vby	tlh
649	9	V	. 1	. 111	. 16	04	03	-				- 101	20	SY	CU	RZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli
649	8	VP.	П	۷	13	3 19	25					111	17	HN	BK	00	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi
849	9 7	1	17	п	. 0	0	3 Z					. DO	GU	BW	NP	HK	A2	CI	PO	JX	VY	120	cft	zsk	wbj
845	0 6	111	I	v	1	1 18	5 14	IL	AF	EU	HO	WV	GL	OK	00	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
641	9 5	S. V	11	IV	2	3 0	1 2	97	W2	KV	GN	. AC	BL	02	EK	QX	OP	SU	DH	JM	TX	150	zby	vcy	ujb
641	D A	11	17	1	10	4 2	0	BF	NE	DX	cs	KR	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak
64	9	3 V	1	1		× 1	0	51				BN	HU	EO	PY	KQ	CP	os	JW	IA	vz	aqd	bdy.	lyf.	xtd.
64	0	2 10	V		1.							DP	ВМ	NZ	CK	OV	HQ	AP	UY	SW	JO	kg1	cdf	819	wuv

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

1	010		Incolar		Eina	Balles				5	1 0	di e	e U	e r	611	1 0 1	1 11 (100	henny	enppe	n
	E	the state	ifening		rung	trante	"y	en l	ber Un	kehrma	olye		2	,		3	6	7		9	10				1000
0	31				14	00	24					SZ.	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exp	r z
0	2	ro	$+ \circ$	KC	05	26	62					15	EV	МΧ	RW	DT	UZ	10	V0	CH	NY	ktl	acw	2.51	22
0	2	U	ιU	13	2	24	03	KM	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	0VW	wv.
õ l	20	11	111	v	0.5	90	16	DI	CN	BR	PV	CR	FV	AI	DK	0T	N.Q.	EU	BX	LP	0 J	115	cld	ude	rz
0	20	111	1	11/	11	03	07	1.7	EO	HS	UW	DY	IN	вv	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	ui
	21		111/	v	17	22	10					V2	AL	RT	KO	co	E1	BJ	DU	FS	HP	xle	gbo	uev	r x
2	20	1			0.8	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	ui
10	25	1v V		111	05	18	14		7.11.27			TY	AS	ow	κv	JM	DR	НΧ	GL	C2	NU	k p l	rwl	vei	11
18	24	, v		11	24	12	02					iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	t1
19	23	IV.	11		01	00	21	1.0		DV	01	PJ	ES	IM	RX	LV	٨Y	00	BO	WZ	CN	JQC	acx	mwe	WV
40	22	n	IV N		112	05	10	10	AS		01	RU	HL	FY	05	02	DM	¥¥.	CE	TV	NX	Jpw	del	mwf	wv
50	21				2.	01	10	FT	0X	5.6	Un	DP	20	QZ	UA.	RY	sv	JL	οx	BE	TW	jqd	cef	nvo	ys
49	20	m	11	, Y	17	25	20	MR	KN	BQ	PW	l ox	PR	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	11
49	19				15	23	26					EJ	OY	IV	AQ	XW	FX	MT	PS	LU	BD	1 s a	₩pж	vej	TX
49	18	11	nr		21	10	06	1				IR	K.Z	LS	EM'	٥ν	ΟY	QX	AP	JP	, BA	mae	hzi	508	y 5
35	1.	1			0.0	16	13	-				НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	IKD	11
49	10				01	03	07					DS	HY	MR	0.14	ΓX	٨J	BQ	co	IP	NT	ldw	hzj	son	wv
90	15			i.	15	11	05	1.7				i OM	JR	KS	IY	H2	PL	AX	BT	CQ	NV	imz	noa	tjv	χt
950	144	1.14	in		13	20	03	N1	DI	pc v		LY	AG	KM	BR	IQ	JU	HV	SW	ET	cx	zgr	dgz	810	ry
940	1.3	-1		iv	18	10	07	PW	EL	Du	KN	MU	BP	CY	RZ	КX	AN	JT	DG	IL	PW	zdy	rki	tjw	xt
040	12	1 11	iv	111	02	26	15	RZ	00	CP	SX	; KN	UY	HR	PW	PN	во	EZ	QT	DX	JV	zea	134	501	
040	1-0	1	v	11	27	21	01					LR	IK	MS	QU	H¥	PT	00	VX	FZ	EN	Irc	20X	v Om	+1
840	1.0	W N		111	10	04	0					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	ed)	eyr	409	* 1
010	1 2	- rv	II.	· · · v	1 13	3 19	2	-	-			FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	912	dab	ari	wh
840	1.7		iv	ш	0	0	3 2	2				. UX	12	HN	BK	QQ	CP	FT	JI	MW	AR	lan	oft	75%	wb
840		- in	I	v	1	1 18	3 1.				1 10	. DQ	GU	BW	NP	HK	AZ	CI	PO	JA	FY	140	cdr	ive	wa.
645	2 1	V	11	IV	2	3 0	2 2	5 11	AP	EU	no	MV	CL	OK	QQ	BI	PU	115	P'A DH	IM	TY	Isb	zby	VCY	uji
645		i n	17	1	0	4 2	0	Q QT	W2	K.	GM	. AC	BL	02	EK	QX.	OP	50	DH	01	LO	130	owd	iwu	wa
849		v	1	11	1	9 1	1 0	5 BF	NB	DX	cs	KR	MP	CN	BP	EH	DZ	20	14	AT	¥2.	and	bdy	iyf	xt
641		V IV	٧	I	1	6 1	4 0	2				BN	HU	EO	PT	KQ	NO	10	IIY	SW	10	kel	cdf	giq	wu
				111	12	3 1	2 1	01				DP	89	512	U.K.	JY	114	415		2.0	100 C			and the second se	

 $5 \cdot 4 \cdot 3$

-	7CI	mu	ng!	5th[ti]]	elmit	ttel o	ucle	it iting	tune	S S	1 c	di r	1 0	e r	b i i	1 0 1	1 II (1 v 1		10 10			64004		0
1	6.41	U) o	lienlog	¢	Sing	gftellu	ng:	en t	er Um	Achtere	olye			, .		5 Steeb	erbrett 6				10	1200	nearry		
						10	21	-				\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exp	rzę
10	31				0	24	62					15	FV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	zsi	#20
48	3.	rO	LΟ	\mathbf{rs}	25	20	02	КИ	AX	PZ	00	DI	AT	CV	10	ER	0S.	LW	P2	FN	BH	ioc	acn	OVW	WVC
49	2				14		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	BX	LP	0J	1 rb	cld	ude	rzł
49	28	11	III	V	00	55	10	1.0	80	ue	1114	DY	TN	AV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis
49	27	m	1	IV	11	03	07	P.L	54	no	Un	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxt
148	26	1	IV .					1000				OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
940	25	IV	III	r	ır	۱C	r		-			TY	15	0×	KV.	JM	DR	HX	GL	C2.	NU	kp1	rw1	vci	tle
948	24	v	1		••	3	5					OV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tle
549	23	11	11									PI	23	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wve
649	22	11	10	V	01	64	21	10	AS	DV	0.P	RII	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wv:
849	21	1	v		13	05	19	FT	ox	EZ	CH	DP	20	07.	AU	BY	sv	JL	ox	BE	TW	jqd	cef	nvo	yst
649	20	111	10	v	24	UI	10	MR	KN	BQ	PW	OX	PR	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	t18
649	19	V	III	1	11/	20	20	1.1.				1.81	OY	IV	40	XW	FX	NT	PS	LU	BD	1 s a	"ab₩	vej	TXT
649	18	10	11	· · ·	15	23	20					TR	¥.Z	LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi
849	17.	1.1.	10	11	21	10	12		-			НМ	10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv
649	16	v	11	m	00	02	07					DS	HY	MR	0.	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	WVE
849	15	11			15		05					i OM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xth
649	14	1.10			1.3	10	01	N1	вт	MV	nu	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgz	610	ryq
649	13	1			1.0	10	07	PW	EL	DO	KN	MU	BP	CY	RZ	KΧ	AN	JT	DG	IL	PW	zdy	rkf	tjw	xti
699	112	· ·			10	2 26	15	RZ	00	CP	SX	KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	zea	rjy	501	wvn
049	11	1	11	111	12	2 21	0					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vom	TXO
844	1.10	1 m		111	1	6 00	0					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	voy	+14
040	1 4	- iv		· · v	12	3 19	2	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	y12	dna	exc	whi
0.59	10	- 1	11	11	0	9 03	2	2				. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	lan	ago	253	whi
010	1 1		11	v	1	1 18	3 1					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	120	cit	ive	was
840	1.6	- v	11	IV	2	3 0	2 2	5 IL	AP	EU	но	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1 Ju	car	VCV	uib
0.45		1 11	11	1	0	4 2	0	Q QT	W2	KV	. GW	. AC	BL	02	EK	QX	OP	50	DH	JM	TX	150	and	iwn	wak
041		· v	1	11	li	9 1	1 0	5 BF	NR	DX	CS	' KR	MP	CN	BF	EH	DZ	IW	AV	01	LO	and	bdy	ivf	xtd
- 11 4 5																									

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

-stone	640	Wel	jenlag	e .	King	ftellur	ng			9	1 0	iti e	e v	e t	b i i en	i d i Stech	erbrett					1.5	henny	ruppe	n
E	1				-	-	-	en.	ue un		acse	1	2	,	*	5	6	7		17	10	VOV	dev	exb	TZP
3	1				4	69	24					S2	07	DV	KU	PO	MI	10	311	CN	NY	k 11	acw	7.51	720
3	8	1	TO	rs	05	26	<u>62</u>			-	-	15	EV	MX	RW	51	02	14	NO	DI	101	inc	200	0.YW	wyd
	8		LO		12	24	03	NR	AY.	r L	00	DJ	TA	CV	10	ER	62	PA	11	1.0	0.1	1 mb	eld	ude	726
	28	11	111	V	05	90	16	DI	CN	BR	PV.	CR	FV	AI	DK	OT	NQ	EU	DA	Dr.	1110		thh	vet	uis
1 :	27	111	1	1V	11	03	07	LT	EQ	HS	UW	DY	IN	BV	OR	MA	LO	rr	81	DE	UP	noj	rbo	ney	TTE
	26	1	11	- Charles		-						V2	AL	RT	KO	CO	EI	BJ	DU	13	CIM .		ubo	new	mit
	25	IV	111				-				1	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	out	unq	uc.	+ 1 /
2	24	v	1	r		19	2				1	TY	AS	0%	KV	JM	DR	нх	GL	CZ	no	x p i	1.41	ude	+11
e l	23	11	11			C	2					QV	FR	AK	EO	DH	61	MZ	21	UN	01	con		mwe	ww
0	22	11	1V	V	01	09	21	10	AS	DV	OL	FJ	ES	IM	RX	LV	V.V.	00	80	WL	UN	Jqc	del	mwf	wv
0	21	1	v	11	13	05	19	PT	ox	E2	CH	RU	HL	FT	05	62	DM	A	00	05	mw	1. Spr	cef	nyo	vs)
0	20	111	1V	v	24	C							- 2	QZ	YO	ET	SV	31	01	16	GI	san	for	SWE	111
8	19	v	111	1	17	- 2	r	ρt	16	יר	٠ †،		r 1	FH	WI	DL	CM	AL	16	10	nD	100	shw	vei	TXI
9	18	IV	11	v	15	1		U		~	-		- {	10	AQ	N.W.	FA OX	0.7	10	IP	BH	100	hzi	SOR	ysi
10	17	1	IV	1!	21	10	00					10		LS	EM	0V	72	05	201	FO	CT	tdp	dhb	fkb	ui
9	16	v	11	111	08	16	13					нм	10	DI	ON	DI	A 1	BO	00	TP	NT	ldw	hzi	soh	wv
19	15	11	IV	1	01	03	07	0.25				DS	11	VC	TY	N2	PL.	AY	BT	co	NV	imz	noa	tjv	x t l
19	14	11	1	v	15	11	05	AI	BT	MV	HU	GW	- 10	EN NU	np	10	.10	RV	SW	ET	cx	zer	dgz	gjo	rye
10	13	1		п	13	20	03	FW	EL	DO	KN	1	np.	CY	R7	KY.	AN	IT	DG	1L	PW	zdy	rkf	tjw	xtl
49	12	v	1	IV .	18	10	07	RZ	00	CP	SX	I MU	. 111	HR	PW	PM	BO	EZ	OT	DX	JV	202	rjy	soi	wvł
49	11	11	IV	111 -	02	26	15					TR	TK	MS	ou	HW	PT	00	VX	FZ	EN	Irc	zbx	vbm	TXC
49	10	III	v	17	23	21	01					OY	RS	LN	KT	AP	IU	DW	но	'RV	JZ	edj	eyr	vby	tib
49	9	V.	. 1		. 10	04	0					PT	NO	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli
149	8	VP.	П	v	13	3 19	2					inx	12	HN	BK	00	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi
949	17	1	IV	11	. 0	0 03	5 2	1				DO	GU	BW	NP	HK	A2	CI	PO	JX	٧Y	120	cft	zsk	wbj
149	6	111	I	v	11	1 12	5 1.	IL	AF	EU	но	· NV	GL	OK	00	BI	FU	HS	PX	NW	EY	1 ju	cdr	iye	waj
49	5	V	11	IV	2	3 04		01	W2	K	. GM	AC	BL	02	EK	Q¥	OP	SU	DH	JM	TX	150	zby	vcy	ujt
49	4	. 11	1V	1	10	a 21		BF	NE	D?	cs	· KB	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak
49	3	V	1	п	1.	y 11		2				BN	HU	EO	PY	KQ	CP	05	JW	IA	vz	aqd	bdy.	191	xte
340	12	IV	V		11	· ··	- 0	* I						110	OV	av	HO	AP.	IIY	SW	JO	13X	cdf	819	wus

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

▲□▶▲□▶★≣▶★≣▶ = ● のへで

1	100	W e	Izenla		Sin	pftellu	ing		Are the	5	1 0	ets e	e v	e 't	b i i en	i d i Stech	i n (1	henny	tubbe	n
	Ě		-					-				1	2				WY	FW	111	17	1.0	WOY	dgy	6%6	rz
9	31				4	59	24					34	01	DV NY	80	nr	117	10	10	CH	NY	ku	acw	251	54
8	30	rn	TO	rs	- 05	26	62	511	4.8	P7	00	15	LV	DI A	TO	20	00	1.4	P7	EN	BH	ioc	acn	OVW	WV
9	2				12	24	03	DT	00		PU	DJ	AT NW		DY	0T	NO	EU	RX	LP	0J	1 rb	cld	ude	rz
9	28	п	111	v	05	80	10	DI	GI	DR		- CR	T V	81	DR	1.1	1.0	pp	HT	EX	UW	woj	fbh	vet	uí
9	27	111	1	1V	11	03	07	LT	EQ	HS	UW	101	10	DT	VA	co	11	RI	DU	PS	HP	xle	gbo	uev	rx
9	26	1	IV										AD		1.0	PV	111	1.7	NS	EO	CW	ouc	uhq	uew	ui
10	25	IV	III		īr	۰ ۲	r					OR	14	AD	21	11	DR	HY	61.	C2.	NU	k p l	rwl	vci	t 1
19	24	V	1			• •	έ.					1 11	N.S		FO	DH	CI	W2	SX	ON	LT	ebn	rwm	udf	tl
9.9	23	11	11				-					QV	PC	TH	D Y	LV	AY	011	BO	WZ	CN	190	acx	mwe	wv
9.0	22	11	IV	v	01	09	21	10	AS	DV	OL	I PJ	b a	PY	05	07	DM	AW	CE	TV	NX	Jpw	del	mwf	**
50	21	1	v	11	13	05	19	FT	ОX	EZ	CH	1 KO	1.5	07	AU	RY	SV	JL	ox	BE	TW	jqd	cef	nvo	ys
49	20	111	10	v	24	4		_1	н.				. (FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	t1
49	19	V.	III	1	11/	1	r	eı	16	20		O	r i	IV	40	XW	FX	MT	PS	LU	BD	1 s a	"ab₩	vej	LX.
49	18	10	11	· ·	15	1	-							LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	SOE	y s
49	117	1.1.	10	11	21	10	12	-				НМ	10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	ui
49	16	V.	11	111	00	03	07					DS	HY	MR	0.	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wv
49	15	11			1.5		05					i GM									v	imz	noa	tjv	xt
950	1.5						0.01	N1	DI	DC 4		LY	n			T	n (n:	ירב	1	х	zgr	dgz	810	ry
Gree	15	-1- v	···· 12	IV	118	3 10	0 01	PW	EL	00	KN	MU	P			5.				-	w	zdy	rkf	tjw	xt
946		1 1	iv	111	10	2 2	5 15	RZ	00	CP	SX	KN	_			_					v	zea	rj y	501	
0 1 0			v	11	12	3 2	1 0					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	Irc	LOX	why	+1
840	1.	v v	i	111	1	6 0	4 0	3				QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	ed)	dba	ekc	11
840		T IV	П	v	11	3 1	9 2	-	1			FI	NQ	SY	CU	BZ	HA	SL	TX	DO	AP	y12	deh	251	wb
849		7 1	17	11	0	9 0	3 2	2				. UX	12	HN	BK	QQ	CP	PT	JI	NW TY	VY	120	oft	zsk	wb.
849		6 in	1	v	1	1 1	8 1	4		- 11	1 10	; DQ	GU	BW	NP	HK	AZ	ue	PU	NW	FY	1 1 1	cdr	iye	wa
649	2	5 V	11	IV	2	3 0	2 2	5 11			01	MV	CL	OK	QQ	51	01	112	DH	IM	TX	150	zby	vcy	uj
845		4 11	17	1	0	14 2	1 0	9 97	W 2	. KI	0 10	· . AC	BL	0z	EK DD	04	D7	19	AV	0.1	LO	lap	owd	iwu	wa
849	2	3 V	1	11	1	9 1	1 0	6 BF	NH	(D)	cs	KF	t MP	CN	BF	SH NO	CP	05	JW	AT	V2	agd	bdy	iyf	xt
845		2 1	v v	I	1	6 1	4 0	2				BI	e HQ	EO	11	44	U.C.				10	kel	'edf	rig	wu

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

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

1	amats-	W o	ljenlog		Ring	Itellu	ng	en i	ber Um	5 skihras	1 e	ets e		e 'r	b i i en	i d i	i ii (10	1.Sec.	henn) tuppe	n
		-	-				2.1					\$2	0T	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	625	rzg
2	31				C	24	62					15	FV	MX	RW	DT	UZ	JQ	٨0	CH	NY	k t l	acw	zsi	05%
14	30	rO	LO	\mathbf{rs}	25	20	02	КИ	AX	PZ	00	DI	AT	CV	10	ER	0S.	LW	P2.	FN	BH	ioc	acn	OVW	bvw
8	2				2		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	вх	LP	OJ	1 rb	cld	ude	rzh
19	28	11	m	v	00	30	10	1.0	80	ue	1114	DY	TN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis
18	27	III	1	11	11	05	0/	DT	54			V2	AL.	RT	KO	CO	E1	BJ	DU	FS	HP	xle	gbo	uev	rxm
49	26	1	IV									OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
49	25	IV	m	r	ın	10	r		-			TY	15	OX	KV.	JM	DR	HX	GL	C2.	NU	kp1	rwl	vci	tlq
49	24	v	1	8 -		3	5	1.2				OV	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo
49	23	114	11									PI	23	TM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc
40	22	11	10	v	01	64	21	10	A2	DV	0L	RII	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf
30	21	1	v		13	05	TA.	PT	ОX	EZ	CH	no		0Z	AU	RY	sv	JL	оx	BE	TW	jqd	cef	nvo	ysh
49	20	III	IV	v.	124	2		-1	н.	~ ~		~ .		FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig
49	19	V		1	17	1	r	еı	It	20	1	U	6	IV	AQ	XW	FX	NT	PS	LU	BD	1 s a	∦p.A	vej	rxn.
49	18	11	11		10	1.	- 04	_				1.0		LS	EM.	ov	OY	QX	AP	JP	, BA	mae	hzi '	SOE	ysi
149	11	1	10	1.	00	16	13					НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv
349	10	V.	11		00	02	07					DS	HY	MR	0W	LX	٨J	BQ	co	IP	NT	ldw	hzj	soh	wvg.
340	15	1		4	115	11	05					i GM									v	imz	noa	tjv	XTK
549	14	1.10			12	20	03	N1	вт	MV	nu	LY	n		10	T	ה	n:	יב	1	X	zgr	dgz	sio	ryg
940	13	-1- v	· · ·	IV	118	10	07	PW	EL	DO	KN	MU	P			-				~	w	zdy	rkf	tjw	xui
040		1 1	iv	111	02	28	15	RZ	00	CP	SX	KN							_	_	v	zea	rjy	501	
040		1	v	11	23	21	01					LR	IK	MS	QU	H¥	PT	00	VX	FZ	EN	Irc	LOX	vom	+115
840	1.	l v	1	111	16	0	03					QY	BS	LN	KT	AP	IU	DW	NO	RV	JZ	ed)	eyr	109	
010		- rv		· · · v	1 13	10	25	-	-			FI	NQ	SY	CU	BZ	HA	RP	TX	00	AP		-		Lin
840			11	11	09	0	3 22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	1	JO	51	LIO
840		in in	I	v	11	1	3 14				110	. DQ	GU	BW	NP	HK	A2	CI	P0	J X	FY				
840		- v		IV	23	0	2 2	IL	AP	EU	no	MV	CL	0 K	QQ	BI	FU	HS	PX	Pew .	EI	1ch	thy	YCY	uib
645		i n	17	1	0	: 2	0	QT	W2	K K	GW		BL	02	EK	QX.	OP	50	DH	01	LO	130	owd	iwu	wak
840	0	v	1	11	19	1	1 0	BF	NE	DX	cs	. KB	MP	CN	BP	EH	DZ	1.4	14		12	and	bdy	ivf	xtd
645	0	2 1	٧	I	10	5 1	4 0	2				BN	HO	EO	PT	KQ	NO	10	IIY	ew.	10	kel	cdf	giq	wuy

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

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 のへで

1	5100	We	lienlag		Ring	Itellu	ng		ar the	5	1 0	ets e	e v	e r	b i i ei	n d 1 n Steet	i n (9 4 1				1	henny	tubbe	n	
1	È				10000							1	2) . DV	4 VII	5	MY	FW	IN	12	LO	wny	dgy	exb	rzg	
0	31		• -		4	54	24					36	E.I.	MY	P.W.	57	112	10	40	CH	NY	ktl	acw	251	05%	
8	30	rn	ТО	rs	22	26	02	811	6.X	P2	00	15	10	CV	10	50	05	LW	P2.	FN	BH	ioc	acn	OVW	bvw	
8	2	. <u> </u>			12	24	03	DT	0.11	-	PU	0.0	nu		DY	OT	NO	EU	BX	LP	OJ	115	cld	ude	rzh	
9	28	11	ш	v	05	80	10	DI	Git	DR	1.1	- CR	T V	A1	DR	11	1.0	pp	HT	EX	UW	woj	fbh	vet	uis	
9	27	ш	1	11	11	03	07	LT	EQ	HS	UW	. D1	10	DV	vo.	00	11	RI	DU	PS	HP	xle	gbo	uev	rxm	
9	26	1	IV .										AL		1.0	PV	111	1.7	NS	EO	CW	ouc	uhq	uew	uit	
10	25	IV	111	r	in		r					OR	10	AD	11	11	DR	HY	61.	C7.	NU	kpl	rwl	vci	tig	
19	24	v	1			Ę	5					1 01	20	1.8	FO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	11	11									D1	23	TM	RY	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
10	22	11	IV	V	01	09	21	10	AS	DV	OL	PIL	HI.	FY	05	02	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
50	21	1	v	11	13	05	19	FT	0X	E2	CH	1 KO	1.5	07	AU	RY	SV	JL	ox	BE	TW	jqd	cef	nvo	ysh	
49	20	111	1V	v	24	9		_ 1	Π.					FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig	
49	19	V	111	1	17	3	r	en	16	20	Т	OI	r ;	TV		XX	FX	MT	PS	LU	BD	1 5 8	sbw	vej	rxn_	
49	18	IV	11	· · ·	15	1.					· · ·			LS	EM	ov	OY	QX.	AP	JP	BU	mae	hzi '	sog	ysi.	
49	17	1.1.	IV	12	21	10	00					нм	10	DI	NR	BY	X.2	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
49	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg	
49	15	11	. IV .	1	101	05	01	1				i gu				-					v	imz	noa	tjv	xtk	
149	14	1.1V	1		15	:0	03	VI	вт	MV	но	LY	n			m l	h	n:	י ב	1	х	zgr	dgz	ots	ryq	
949	13	-1		IV	18	10	07	PW	EL	DO	KN	MU	P			5				u	w	zdy	rkf	tjw	xtl	
999	12		1	11	02	26	15	RZ	00	CP	SX	KN									v	202	rjy	501	wvh	
940	11		W	11	22	21	01					LR	IK	MS	QU	H¥	PT	00	VX	FZ	EN	Irc	ZDX	vom	110	
840	1.10	1 W	1	111	16	04	1 03					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	409	ern	
010	14	- rv		· · v	13	15	25	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	y				1
0.49	1.0		IV	11	09	0	3 22					. UX	12	HN	BK	00	CP	FT	JY	MW	AR			5		I
840		- in	1	v	11	18	8 14	1				. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VI					r.
840		- v		IV	2	0	2 25	IL	AP	EO	NO	MV	CL	OK	00	BI	FU	HS	PX.	ILW.	LI	1 ch	* b #	VCV	uib	
840		1 11	11	1	0	2	1 05	QT	W2	K.	GN	. AC	BL	02	EK	QX.	OP	50	DH	SM CI	1.0	100	owd	iwu	wak	
840		v	1	11	19	1	1 00	BF	NB	DX	CS	KR	MP	CN	BF	EH	DZ	WL	AV	0.1	10	and	bdy	ivf	xtd	
-	30			1	1.	. 1	1 6					BN	HU	EO	PY	KQ	CP	05	JW	vr.		e.d.a		1.0		

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

1	10.0	Wal	jenlag	c	Ring	tellur	19	en è	er Un	5 Achros	1 e	its e		e t	b i i	1 0 1 Stech	erbrett				10	1300	frenns	tuppe	n	
	E		-			e c.	2.1				-	\$7	OT	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exb	rzg	
10	31	-			1	26	62					15	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	zsi	05%	
18	3	r U	LO	$\mathbf{r}\mathbf{s}$		20	02	КМ	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	OVW	wwd	
18	4		121	11	14	00		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	OJ	1 rb	cld	ude	rzh	
48	28	11	m		00	03	07	1.0	80	NS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vct	uis	
49	27	m	1	IV	11	03			54		0.	V2	AL.	RT	KO	co	E1	BJ	DU	FS	HP	xle	gbo	uev	rxm	
49	26	1	1.		•							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
49	25	IV	m	r	ın		5	-	-			TY	AS	ow	KV	JM	DR	НΧ	GL	C2.	NU	k p l	rwl	vci	tiq	
48	24	V	1	•		3'						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
140	23	IV	II		1.01					DW		PJ	ES	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
940	22	11	10	V	01	64	21	10	AP	DV	0L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
839	21	1	v		13	US	- PY	FT	оx	E2	CH	1 110		OZ	AU	RY	sv	JL	οx	BE	TW	jqd	cef	nvo	ysh	
849	20	111	IV	v.	124	2		_ f	Ι,	~~		~.		FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
649	19	V	m	1	17	1	r	-	It	20	ЛL.	UI	6	IV	AQ	XW	FX	NT	PS	LU	BD	1 s a	#pm	vej	rxn.	
649	18	IV	11		10	10	0.4	_			_	1.0		LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi.	
849	11.	1	14	11	00	16	13					НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
849	10	N N	II	1	01	03	07					DS_	HY	MR	0 W	LΧ	٨J	BQ	co	IP	NT	ldw	hzj	soh	wvg.	
849	15				15	11	05					I GM									v	imz	noa	tjv	XTR	
650	144	1.1			12	20	03	N1	DI	be a		LY	n			T	n (2	יר	1	X	zgr	dgz	810	ryg	
049	13	1		IV	118	10	07	PW	EL	DO	KN	MU	P			5.				ų,	w	zdy	rkf	tjw	xel	
040	12	1 11	iv	111	02	26	15	RZ	00	CP	SX	KN				_				_	v	zea	rj y	501		
040	110	1	v	11	23	21	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	Irc	LOX	why	tib	
840	1.0	v	i	111	16	04	60					QY	BS	LN	KT	AP	IU	DW	no	NV	JZ	ed)	eyr	109		
840	1 8	Try'	11	v	13	19	25	-				FI	NQ	SY	CU	BZ	HA	SL	TX	DO	AP		20		tion	-
840	17		11	11	09	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR		JU	51	uО	
840	16	- in	I	v	11	18	14	1			NC	. DQ	GU	BW	NP	HK	A2	CI	PO	JX	FY					
840	15	V	11	IV	23	02	25	1 IL	Ar	EU	ne	MV	CL	OK	QQ	BI	PU	115	11	111	my	leb	thy	VCV	uib	
645		1 ii	11	1	0	21	09	QT	W2	K4	GN	. AC	BL	02	EK	QX.	OP	50	DH	01	LO	130	owd	iwu	wak	
0.41	3	V V	1	11	19	11	00	BF	NB	DX	CS	· KR	MP	CN	BP	EH	DZ	20	14	AT	¥2.	and	bdy	iyf	xtd	
011		and the second s			100 B	1000200						BN	- 5413	£0	- 1' T	- 69	UP	03				TRACTOR OF STREET, STR	CONTRACTOR OF	Entran Subsc		

 $5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12!2^{12}) \cdot 26! / (10!6!2^{10}) \cdot 26^3 \simeq 150$ undecillion 789 decillion

~	Act	ntu	ngi	5djtu[]	Imitt	clòi	ir fes	nid	tunt	erjel	irt in	Jeind	esha	nd fr	llen.	Beit	Sefah	t reft	105 11	nd fr	ühzeit	lig vern	iditen.			
Teners-	641	We	ljenlog	¢	Ring]	tellur	19	en è	ier Un	5 Achron	l e ije	di e	e v 7	e r ,	b i i	1 0 1 5141	erbrett 6	7			10	1.500	henny	pruppe	n	
0 1	1					c.c	2:1					\$2	07	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	exp	rzg.	
01	2			-	6	26	62					15	EV	MX	RW	DT	UZ	JQ	٨0	CH	NY	k t l	acw	251	¥30	
2	3.		LU	rs.		20	02	КМ	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	OVW	wvd	
8	4				04	00		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	0 J	1 rb	cld	ude	rzh	
8	28	11	m		00	03	07	1.0	80	HS	IIV	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vet	uis	
8	27	m	1	IV	11	03			1.4		0.	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxn	
16	26	1	IV .	8								OR	PV	AD	TT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
10	25	IV	m	r	ın	0	5	-	-			TY	45	ow	KV	JM	DR	НΧ	GL	C2.	NU	kp1	rwl	vci	tiq	
18	24	V	1			Έ						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
19	23	11	11									PI	ES	TM	RX	LV	AY	ou	BO	WZ	CN	190	acx	mwe	wvc	
10	22	11	IV	v	01	64	21	10	AP	DV	0 L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
40	21	1	v		13	05	- PY	FT	оx	E2	CH	110		OZ	AU	RY	sv	JL	0 X	BE	TW	jqd	cef	nvo	ysh	
49	20	111	10	v	24	9		_ 1					- 1	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tlg_	
49	19	V	111	1	17	1	r	-	16	20	Ш	OI	1	IV	49	XW	FX	NT	PS	LU	BD	1 5 8	#p#	vej	rxn.	
49	18	IV	11	· ·	15	1.								LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	SOE	ysi.	
49	17.	1	10	11	21	10	12					НМ	10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
49	16	v	11	m	00	10	07					DS	HY	MR	0W	LX	ΛJ	BQ	co	IP	NT	1 dw	hzj	soh	WVE.	
149	15	11	. IV .	1	101	05	01		-			i gu				-					v	imz	noa	tjv	xtk	
149	14	1.10	1		15	:0	03	IA	вт	MV	но	LY	n		110	r	h	h 5	יו ב	-	х	zgr	dgz	ots	ryg	
949	13	1		III	110	10	07	FW	EL	DO	KN	MU	μ		u 3					U	W	zdy	rkf	tjw	xtl	
999	112	· ·	1	1.	102	26	15	RZ	00	CP	SX	KN									v	203	rjy	501	wvn	
949	11	1	IV.	111	1 22	20	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
899	1.10	1 m	, v	11	16	04	63					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	498	CIN .	
940	19	1		· · w	1 13	10	25					FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У	-			
849	8	- 11	II IV	11	00	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	1.		SII		ľ
940	17	1 10	14	v	1 11	18	14	1				. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1				1
049	1.0		11	IV	23	02	25	IL	AP	EU	нс	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1.		NON	nth	
049	12	1	11	1	04	21	09	QT	W2	KV	GN	. AC	BL	02	EK	Q.X	OP	50	DH	JM	TX	150	and	iwn	wak	
840	1 2	· v	1	11	19	11	05	BF	NB	DX	CS	· KR	MP	CN	BF	EH	DZ	IW	AV	01	LO	and	hdy	ivf	xtd	
640	12	11	v	I	16	14	: 02					BN	HU	EO	PY	KQ	CP	05	3.4	AL	10	kel	cdf	gig	wuy	
- 10		-			1	20062	2.00	100				np	214	217	CK	0.4	10	AF.	UI	37	~ 0			and the second second		

 $5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24!/(12!2^{12}) \cdot 26!/(10!6!2^{10}) \cdot 26^3 \simeq 150$ undecillion 789 decillion 931 nonillion

1				Saladi			1			6	1.0	di e				1 0 1	1 11 9	V 1				1				
1	1010	W a	lienlag	c	Ring]	tellun	9	en è	er Um	kehrme	ise					Stech	erbrett	,		•	10	1 Same	nenne	hentba		
							1					\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	6%9	rzg	
1	31				2.1	24	2					15	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	251	#20	
8	3	r U	LO	\mathbf{rs}		20	02	КИ	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	4			11	04	0.0		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	GJ	1 rb	cld	ude	rzh	
8	28	11	m		00	03	02	1.0	80	HS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vct	uis	
8	27	m	1	IV	11	03			1.4		0.	17	41.	RT	KO	co	El	BJ	DU	FS	HP	xle	gbo	uev	rxn	
6	26	1	IV .		•							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
9	25	IV	m	r	ın		5	-	-			TY	45	0%	KV	JM	DR	НΧ	GL	C2.	NU	k.p.l	rwl	vci	tlq	
18	24	V	1			3'						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
19	23	IV	II		0.01					nu		PJ	ES	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
10	22	11	IV	v	101	05	10	10	AD	Dv	0 D	RU	HL	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
50	21	1			13	05	191	PT	OX.	Е2	CH	1		QZ	AU	RY	sv	JL	ΟX	BE	TW	jqd	cef	nvo	ysh	
49	20	m	11	, Y	17	2		~f			+	~		FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19				15	1	r e	21	It	20	ıL	UI	1	IV	AQ	XW	FX	MT	PS	LU	BD	1 5 8	₩pж	vej	rxn.	
49	18	11	n		21	10	05	_				10		LS	EM'	٥ν	OY	QX	AP	JP	BU	mae	hzi	SOE	y51	
46	1.	·	11	111	08.	16	13					НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	IKD	UIV	
19	10		IV	1	01	03	07					DS	HY	MR	0 W	ΓX	٨J	BQ	CO	IP	NT	ldw	hzj	son	wvg.	
40	12	111		v	15	11	05		DT	WV	нп	I GM									v	imz	noa	tjv	X CK	
140	112		in	ii ii	13	20	03			Da	N.M	LY	n			5	n	٦2	٦r	· 🖊	X	zgr	agz	810	1.9%	
10	112	1- v	1	IV	118	10	07	PW	EL	Du	R.M.	MU	P		-	5.				~	w	zdy	TKI	cjw coi	wyh	
140	11	1 11	IV	111	02	26	15	RZ	00	OP	21	KN									U.V.	202	139	whm	TTO	
940	110	III	v	11	23	21	01					LR	IK	MS	QU	HW	PT	00	VX	FZ	EN 12	irc	20X	vbv	tih	
849	10	v	1	111	16	04	60					QY	BS	LN	KT	AP	10	DW	no	no	VP	euj	67.			
649	8	1 IV	Ш	٧	13	19	25	-	11.25		100	FI	NQ	SY	00	82	AH	55	TY	NW	AR	1.	20	Cit	tio	
849	17	1	1V	11	09	03	22					. UX	12	HN	BK	90	UP .2	CT	20	TY	VY	1	JU	51	ιU	
849	16	in	I	v	11	18	14	11.	AP	EU	но	; DQ	60	BW	NP	nK nT	PIL	HS	PY	NW	EY	1				
845	5	V	11	IV	23	02	25	100		EV	01	MV	CL	UK OZ	DQ PV	DI	02	SU	DH	JM	TX	150	zby	vcy	ujb	
841	4	11	1V	1	04	21	09	QT DO		DY	0.	. AC	BL	CN	BP	FH	DZ	TW	AV	OJ	LO	lap	owd	iwu	wak	
849	3	V	1	11	19	11	05	BF	NR	DX	1	RH DN	ME	FO	PY	KO	CP	os	JW	AI	V2	aqd	bdy.	iyf	xtd.	
	1000	AND INCOME.			1	100 C 100 C 100 C	- 60					- 00		- 40							- 0.02 gen					

 $5\cdot 4\cdot 3\cdot 26^3\cdot 24!/(12!2^{12})\cdot 26!/(10!6!2^{10})\cdot 26^3\simeq 150$ undecillion 789 decillion 931 nonillion 331 octillion

1				Saladi			1			6	1.0	di e				1 0 1	1 11 9	V 1				1				
1	1010	W a	lienlag	c	Ring]	tellun	9	en è	er Um	kehrme	ise					Stech	erbrett	,		•	10	1 Same	nenne	hentba		
							1					\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	6%9	rzg	
1	31				2.1	24	2					15	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	251	#20	
8	3	r U	LO	\mathbf{rs}		20	02	КИ	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	4			11	04	0.0		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	GJ	1 rb	cld	ude	rzh	
8	28	11	m		00	03	02	1.0	80	HS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vct	uis	
8	27	m	1	IV	11	03			1.4		0.	17	41.	RT	KO	co	El	BJ	DU	FS	HP	xle	gbo	uev	rxn	
6	26	1	IV .		•							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
9	25	IV	m	r	ın		5	-	-			TY	45	0%	KV	JM	DR	НΧ	GL	C2.	NU	k.p.l	rwl	vci	tlq	
18	24	V	1			3'						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
19	23	IV	II		0.01					nu		PJ	ES	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
10	22	11	IV	v	101	05	10	10	AD	Dv	0 D	RU	HL	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
50	21	1			13	05	191	PT	OX.	Е2	CH	1		QZ	AU	RY	sv	JL	ΟX	BE	TW	jqd	cef	nvo	ysh	
49	20	m	11	, Y	17	2		~f			+	~		FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19				15	1	r e	21	It	20	ıL	UI	1	IV	AQ	XW	FX	MT	PS	LU	BD	1 5 8	₩pж	vej	rxn.	
49	18	11	n		21	10	05	_				10		LS	EM'	٥ν	OY	QX	AP	JP	BU	mae	hzi	SOE	y51	
46	1.	·	11	111	08.	16	13					НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	IKD	UIV	
19	10		IV	1	01	03	07					DS	HY	MR	0 W	ΓX	٨J	BQ	CO	IP	NT	ldw	hzj	son	wvg.	
40	12	111		v	15	11	05		DT	WV	нп	I GM									v	imz	noa	tjv	X CK	
140	112		in	ii ii	13	20	03			Da	N.M	LY	n			5	n	٦2	٦r	· 🖊	X	zgr	agz	810	1.9%	
10	112	1- v	1	IV	118	10	07	PW	EL	Du	R.M.	MU	P		-	5.				~	w	zdy	TKI	cjw coi	wyh	
140	11	1 11	IV	111	02	26	15	RZ	00	OP	21	KN									U.V.	202	139	whm	TTO	
940	110	III	v	11	23	21	01					LR	IK	MS	QU	HW	PT	00	VX	FZ	EN 12	irc	20X	vbv	tih	
849	10	v	1	111	16	04	60					QY	BS	LN	KT	AP	10	DW	no	no	VP	euj	67.			
649	8	1 IV	Ш	٧	13	19	25	-	11.11		100	FI	NQ	SY	00	82	AH	55	TY	NW	AR	1.	20	Cit	tio	
849	17	1	1V	11	09	03	22					. UX	12	HN	BK	90	UP	CT	20	TY	VY	1	JU	51	ιU	
849	16	in	I	v	11	18	14	11.	AP	EU	но	; DQ	60	BW	NP	nK nT	PIL	HS	PY	NW	EY	1				
845	5	V	11	IV	23	02	25	100		EV	01	MV	CL	UK OZ	DQ PV	DI	02	SIL	DH	JM	TX	150	zby	vcy	ujb	
841	4	11	1V	1	04	21	09	QT DO		DY	0	. AC	BL	CN	BP	FH	DZ	TW	AV	OJ	LO	lap	owd	iwu	wak	
849	3	V	1	11	19	11	05	BF	NR	DX	1	RH DN	ME	FO	PY	KO	CP	os	JW	AI	V2	aqd	bdy.	iyf	xtd.	
	1000	AND INCOME.			1	100 C 100 C 100 C	- 60					- 00		- 40							- 0.02 gen					

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

	6.41	Wal	jenlag		Fingl	tellu	19		or the	5	1 0	ets e	e v	e t	b i i en	i d i	erbrett					1300	henng	ruppei	1	
in the							1					1 0.7	7	DV.	KU	FO	MY	EW	JN	13	LQ	wny	dgy	exb	rzg	
21	31		• • •		4	04	24					16	FU	MY	RW	DT	UZ	JO	40	CH	NY	k t l	acw	zsi	05%	
6	30	r O	ГО	\mathbf{rs}	22	20	02	KM.	AX	PZ	00	D.1	17	CV	10	FR	os	LW	P2	FN	BH	ioc	acn	OVW	bvw	
9	2			_	12	24	05	DI	CN	np	PU	CP	PH	AT	DK	OT	NO	EU	BX	LP	OJ	1 rb	cld	ude	rzh	
9	28	11	111	V	05	96	10					DY	1.1	BV	OR	AN.	1.0	PP	HT	EX	UW	woj	fbh	vet	uis	
8	27	111	1	IV	11	03	0/	P.L.	24	na	0.	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm	
6	26	1	IV .									0.0	DU	AD	IT	PY	HI	1.2	NS	EQ	CW	ouc	uhq	uew	uit	
9	25	IV	ш	r	in		r					. ev	10	OV	ww.	11	DR	нх	QL.	CZ.	NU	kpl	rw1	vci	tlq	
8	24	v	1			Ę						1 01	20	1.8	FO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
9	23	14	11									D1	23	TM	RY	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
0	22	11	14	V	01	69	21	10	AS	DV	OL	PIL	HI.	FY	05	02	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
9	21	1	v	11	13	05	19	FT	OX	EZ	CH	I NO		07.	AU	RY	SV	JL	ox	BE	TW	jqd	cef	nvo	ysh	
0	20	111	1V	v	24	4		_ 1					- 1	FH	WY	DL	CM	AE	22	15	GI	idf	fpx	JWE	tig	
18	19	V	III	1	17	1	r	-11	IE	20		OI	- i	TV	40	XX	FX	NT	PS	LU	BD	153	sb₩	vej	rxn.	
18	18	11	n	v	15	1.					· ·			LS	EM'	ov	OY	QX	AP	JP	BU	mae	hzi '	SOE	ysi.	
10	17	1	10	11	21	10				-		нм	.10	DI	NR	BY	X.2	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
19	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
49	15	11	. 10	1	101	05	01					i gu				-					v	imz	noa	tjv	xtk	
49	14	. 1V	1		15	:0	03	IA	вт	MV	но	LY	n		110	r	ה	n :	א ב	1	х	zgr	dgz	ots	ryg	12
49	13	1		IV	18	10	07	PW	EL	DO	KN	MU	P			5				u	w	zdy	rkf	tjw	xtl	
919	12		1	111	02	26	15	RZ	00	CP	SX	KN									v	202	rjy	501	wvh	
10	11	1	W	11	23	21	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	ZDX	vom	+15	
HP	1.10	1 m	,	111	116	04	63					'QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	409	ern	
940	19	1 m		v	1 13	19	75	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	y				
940	1.0		11	11	09	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	1		SI		
940	1:	1	1	v	111	18	14	1				. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY					
040	6	- v	11	IV	23	0	25	IL	AP	EU	HO	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1 ab	a bu	VCV	nib	
140	12	1 1	11	1	04	21	05	QT	WZ	KW	GN	. AC	BL	02	EK	QX	OP	50	DH	JM	TX	150	owd	iwu	wak	
1.10	1 2	· .	1	11	19	11	00	BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	WI	AV	0.1	10	and	bdy	ivf	xtd	
940	100														- 0.9	~ ~ ~ ~		- 151						the second se		

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

	act	ntu	ng!	Lu Schläff	ftw	nf tel d	fer	1 - 17 1 nida	la∫ tunt	dji	191 rt in	1 - S Jeind	(h)	Ü[]1 .nd fo	llen.	Nr. Beit	6. Sefah	treft	los 11	nd fr	ühzeil	lig vern	iditen.			
Tante	6 vi	W o	lzenlog		Ring	Itellu	ng	en l	are Um	5 kehrme	1 0	di e		e'r	b i i	1 0 1 51ert	arbrett			•	10	1.500	henny	ruppe	n	
0						r.c	2.1					SZ.	07	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	6%9	rzg.	
	2			-	1	26	62					15	EV	MX	RW	DT	UZ	JQ	٨0	CH	NY	k t l	acw	251	20	
2	3.		LO	rs		20	02	КМ	XA	PZ	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acn	OVW	MAG	
8	4		111		14	00		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	0 J	1 rb	cld	ude	rzh	
8	28	11	m		00	03	07	1.0	50	HS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vct	uis	
8	27	m	1	IV	11	03	0/		1.4			V2	AL.	RT	KO	CO	E1	BJ	DU	FS	HP	xle	gbo	uev	rxm	
9	26	1	IV .		•							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit.	
10	25	IV	m	r	In		5		-			TY	AS	0%	KV	JM	DR	НΧ	GL	C2.	NU	k p l	rwl	vci	tlq	
18	24	V	1			'8	5					iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
19	23	IV	11		1.01	- 00	- 11			DW		PJ	ES	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
10	22	11	IV		101	05	10	10	AD	Dv	0 D	RU	HL	FY	05	C2	DM	AW	CΕ	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v		13	05	19	PT	оx	62	CH			QZ	AU	RY	sv	JL	0 X	BE	TW	jqd	cef	nvo	ysh	
49	20	m	IV	÷	12	2		_ 1		~		~.	- R	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19	v		1	17	1	r	- 1	It	20		UI	6	IV	AQ	XW	FX	NT	PS	LU	BD	1 s a	#pm	vej	rxn.	
49	18	11			21	1.	- 04	_				1.0		LS	EM'	٥٧	θY	QX	AP	JP	, BA	mae	hzi	SOE	y51	
49	11.	- 1-	14	1.	00	16	13		-	1944		НМ	JO	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
49	10		II	1	00	03	07					DS_	HY	MR	0 W	LX	٨J	BQ	CO	IP	NT	ldw	hzj	soh	wvg.	
40	15	11		. N	15	11	05					1 OM									v	imz	noa	tjv	XTK	
950	14	1.1			12	20	03	N1	DI	DC 4		LY	n			T	n (2	יר	1	х	zgr	dgz	810	ryg	
940	13	1- 1.		IV	118	10	07	PW	EL	DO	KN	MU	P			-				-	w	zdy	rkf	tjw	xel	
140	1×	1 11	iv	111	02	26	15	RZ	00	CP	SX	KN									v	zea	rjy	501		
010	110	1 III	v	11	23	21	01					LR	IK	MS	QU	H¥	PT	00	VX	FZ	EN	Irc	208	why	tib	
0.40	1.10	1 W	1	111	16	04	03					QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	ed)	eyr	109		
010	1 0	1 rv		· · · v	1 13	1 19	25	-	-			FI	NQ	SY	CU	BZ	HA	EL	TX	DO	AP					
840	17	1 1	11	11	09	0	3 22					. UX	12	HN	BK	QQ	CP	FT	JI	NW	AR		JU	51		
849	16	1 in	I	v	11	18	3 14	1			10	. DQ	GU	BW	NP	HK	A2	CI	PO	JA	FY					
649	15	V	11	IV	23	3 0	2 2	IL	AP	20	01	MV	CL	OK	QQ	BI	PU	115	T Å	IM	TY	1sb	zby	YCY	ujb	
649	4	1 11	1V	1	0	: 2	0	QT	#2	KV	OR OF	. AC	BL	02	EK	QX.	D7	30	AV	0.1	LO	lap	owd	iwu	wak	
649	3	v	1	11	19	2 1	1 0	BF	NR	DX	cs	KR	MP	CN	BF	5H	CP	05	14	AT	¥2.	and	bdy	iyf	xtd	
640	12	IV	٧	I	10	5 1.	4 0	2				BN	HO	EO	£1	AV	NO	10	117	SW	10	kel	cdf	giq	wuv	

 $5\cdot 4\cdot 3\cdot 26^3\cdot 24!/(12!2^{12})\cdot 26!/(10!6!2^{10})\cdot 26^3\simeq 150$ undecillion 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion 42 quintillion
2	act	ntu	ngl	Lu Schlöff	ftw elmitt	n†	ic fer	1 - 1 1 a nida	(a)	d)11	ner Int in	1-5 Jeind	(1) li	11]]1 .nd fo	llen.	Nr. Beil	64 iefah	t reft	los 11	nd fr	ühzeit	ig vern	iditen.			
inter in	6 vi	We	ljenlog	e	Ring	tellu	19	en l	ar Un	5 Ashros	t e lyr	di e		e . r	b i i	i d i Stech	erbrett				10	1.500	henng	tubbe	n	
0	-	NOTOP II III II IV II IV IV III V I IV II II IV IV III V I IV II V I II V					2.1					\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exb	rzg.	
2	31				C .	21	62					15	FV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	zsi	05%	
8	30	r O	LΟ	\mathbf{rs}	10	20	02	КМ	AX	PZ	00	DI	AT	CV	10	ER	0S	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	2				14		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	BX	LP	0J	1 rb	cld	ude	rzh	
9	28	11	III	V	00	30	10	1.0	80	ue	1114	DY	TN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis	
19	27	111	1	IV	11	03	07	PL.	D.A	no	Un	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm	
99	26	1	IV .									OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
10	25	11	m	r	in	0	r		-			TY	15	0×	KV.	JM	DR	нх	GL	C2.	NU	kp1	rw1	vci	tlq	
49	24	v	1			E						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	14	11									PI	23	TM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
40	22	11	10	V	01	09	21	10	A2	Dv	0 L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v		13	05	19	PT	OX	E2	CH	I NO		07.	AU	BY	sv	JL	ox	BE	TW	jqd	cef	nvo	ysh	
49	20	111	1V	v	24	2		_ 1	Ξ.		ж.		- 6	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19	V	III	1	11/	1	r	aı	16	20		OI	1	IV	40	XW	FX	NT	PS	LU	BD	1 s a	#bw	vej	rxn.	
49	18	IV	n	· · ·	15	1.					· · ·			LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi.	
49	17	. 1.	10	11	21	10	00			-		нм	.10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
149	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
349	15	11	. IV .		101	05	07	1				i gu									v	imz	noa	tjv	xtk	
349	14	11	1		15	:0	03	VI	вт	MV	но	LY	n		110	r	٦/	n :	יו ב	-	х	zgr	dgz	sjo	ryg	
349	13			II	13	10	07	FW	EL	DO	KN	MU	μ		ч,	51	31			u	W	zdy	rkf	tjw	xti	
649	12	. v	1	11	10	26	15	RZ	00	CP	SX	KN									v	zea	rjy	soi	wvh	
049	11	1	IV	111	1 22	20	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
999	1.10	1 m	v,	11	16	04	63					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	v6y	CIN	
0-19	19	1		· · · w	1 13	10	25	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У	-	-		
849	8	- 1	II IV	11	00	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	11		SI)r
049	17		14	v	111	18	14					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1				
049	1.0		11	IV	23	0	25	IL	AP	EU	но	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1.		NON	nth	
049	2	1 .	11	1	04	21	05	QT	W2	KV	GN	. AC	BL	02	EK	QX	OP	SU	DH	JM	TX	150	209	iwn	wak	
840	1 2	· v	1	11	19	1	00	BF	NE	DX	CS	· KR	MP	CN	BF	EH	DZ	IW	AV	01	LO	and	hdy	ivf	xtd	
040		11	v	I	110	1.	: 03	2				BN	HU	EO	PY	KQ	CP	US	JW	AL	10	kel	odf	rio	wuy	

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

2	act	ntu	ngl	Lu Schlöff	ftw elmitt	n†	ic fer	1 - 1 1 a nida	(a)	d)11	ner Int in	1-5 Jeind	(1) li	11]]1 .nd fo	llen.	Nr. Beil	64 iefah	t reft	los 11	nd fr	ühzeit	ig vern	iditen.			
inter in	6 vi	We	ljenlog	e	Ring	tellu	19	en l	ar Un	5 Ashros	t e lyr	di e		e . r	b i i	i d i Stech	erbrett				10	1.500	henng	tubbe	n	
0	-	NOTOP II III II IV II IV IV III V I IV II II IV IV III V I IV II V I II V					2.1					\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exb	rzg.	
2	31				C .	21	62					15	FV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	zsi	05%	
8	30	r O	LΟ	\mathbf{rs}	10	20	02	КМ	AX	PZ	00	DI	AT	CV	10	ER	0S	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	2				14		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	BX	LP	0J	1 rb	cld	ude	rzh	
9	28	11	III	V	00	30	10	1.0	80	ue	1114	DY	TN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis	
19	27	III	1	IV	11	03	07	PL.	D.A	no	Un	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm	
99	26	1	IV .									OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
10	25	11	m	r	in	0	r		-			TY	15	0×	KV.	JM	DR	HX	GL	C2.	NU	kp1	rw1	vci	tlq	
49	24	v	1			E						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	14	11									PI	23	TM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
40	22	11	10	V	01	09	21	10	A2	Dv	0 L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v		13	05	19	PT	OX	E2	CH	I NO		07.	AU	BY	sv	JL	ox	BE	TW	jqd	cef	nvo	ysh	
49	20	111	1V	v	24	2		_ 1	Ξ.		ж.			FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19	V	III	1	11/	1	r	aı	16	20		OI	1	IV	40	XW	FX	NT	PS	LU	BD	1 s a	#bw	vej	rxn.	
49	18	IV	n	· · ·	15	1.					· · ·			LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi.	
49	17	. 1.	10	11	21	10	00			-		нм	.10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
149	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
349	15	11	. IV .		101	05	07	1				i gu									v	imz	noa	tjv	xtk	
349	14	11	1		15	:0	03	VI	вт	MV	но	LY	n		110	r	٦/	n :	יו ב	-	х	zgr	dgz	sjo	ryg	
349	13			II	13	10	07	FW	EL	DO	KN	MU	μ		ч ;	51	31			u	W	zdy	rkf	tjw	xti	
649	12	. v	1	11	10	26	15	RZ	00	CP	SX	KN									v	zea	rjy	soi	wvh	
049	11	1	IV	111	1 22	20	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
999	1.10	1 m	v,	11	16	04	63					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	v6y	UIN	
0-19	19	1		· · · w	1 13	10	25	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У	-	-		
849	8	- 1	II IV	11	00	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	11		SI)r
049	17		14	v	111	18	14					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1				
049	1.0		11	IV	23	0	25	IL	AP	EU	но	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1.		NON	nth	
049	2	1 .	11	1	04	21	05	QT	W2	KV	GN	. AC	BL	02	EK	QX	OP	SU	DH	JM	TX	150	209	iwn	wak	
840	1 2	· v	1	11	19	1	00	BF	NE	DX	CS	· KR	MP	CN	BF	EH	DZ	IW	AV	01	LO	and	hdy	ivf	xtd	
040		11	v	I	110	1.	: 03	2				BN	HU	EO	PY	KQ	CP	US	JW	AL	10	kel	odf	rio	wuy	

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

・ロト・四ト・モート ヨー うへの

2	act	ntu	ngl	Lu Schlöff	ftw elmitt	n†	ic fer	1 - 1 1 a nida	(a)	d)11	ner Int in	1-5 Jeind	(1) li	11]]1 .nd fo	llen.	Nr. Beil	64 iefah	t reft	los 11	nd fr	ühzeit	ig vern	iditen.			
inter in	6 vi	We	ljenlog	e	Ring	tellu	19	en l	ar Un	5 Ashros	t e lyr	di e		e . r	b i i	i d i Stech	erbrett				10	1.500	henng	tubbe	n	
0	-	NOTOP II III II IV II IV IV III V I IV II II IV IV III V I IV II V I II V					2.1					\$2	07	DV	KU	FO	MY	EW	JN	11	LQ	wny	dgy	exb	rzg.	
2	31				C .	21	62					15	FV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	zsi	05%	
8	30	r O	LΟ	\mathbf{rs}	10	20	02	КМ	AX	PZ	00	DI	AT	CV	10	ER	0S	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	2				14		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	BX	LP	0J	1 rb	cld	ude	rzh	
9	28	11	III	V	00	30	10	1.0	80	ue	1114	DY	TN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis	
19	27	111	1	IV	11	03	07	PL.	D.A	no	Un	117	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm	
99	26	1	IV .									OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
10	25	11	m	r	in	0	r		-			TY	15	0×	RV.	JM	DR	нх	GL	C2.	NU	kp1	rw1	vci	tlq	
49	24	v	1			E						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	14	11									PI	23	TM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
40	22	11	10	V	01	09	21	10	A2	Dv	0 L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v		13	05	19	PT	OX	E2	CH	I NO		07.	AU	BY	sv	JL	ox	BE	TW	jqd	cef	nvo	ysh	
49	20	111	1V	v	24	2		_ 1	Ξ.		ж.			FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig_	
49	19	V	III	1	11/	1	r	aı	16	20		OI	1	IV	40	XW	FX	NT	PS	LU	BD	1 s a	#bw	vej	rxn.	
49	18	IV	n	· · ·	15	1.					· · ·			LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi.	
49	17	. 1.	10	11	21	10	00			-		нм	.10	DI	NR	BY	XZ	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
149	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
349	15	11	. IV .		101	05	07	1				i gu									v	imz	noa	tjv	xtk	
349	14	11	1		15	:0	03	VI	вт	MV	но	LY	n		110	r	٦/	n :	יו ב	-	х	zgr	dgz	sjo	ryg	
349	13			II	13	10	07	FW	EL	DO	KN	MU	μ		ч ;	51	31			u	W	zdy	rkf	tjw	xti	
649	12	. v	1	11	10	26	15	RZ	00	CP	SX	KN									v	zea	rjy	soi	wvh	
049	11	1	IV	111	1 22	20	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
999	1.10	1 m	v,	11	16	04	63					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	v6y	UIN	
0-19	19	1		· · · w	1 13	10	25	-				FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У	-	-		
849	8	- 1	II IV	11	00	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	11		SI)r
049	17		14	v	111	18	14					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1				
049	1.0	- w	11	IV	23	0	25	IL	AP	EU	но	MV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1.		NON	nth	
049	2	1	11	1	04	21	05	QT	W2	KV	GN	. AC	BL	02	EK	QX	OP	SU	DH	JM	TX	150	209	iwn	wak	
840	1 2	· v	1	11	19	1	00	BF	NE	DX	CS	· KR	MP	CN	BF	EH	DZ	IW	AV	01	LO	and	hdy	ivf	xtd	
040		IN	v	I	110	1.	: 03	2				BN	HU	EO	PY	KQ	CP	US	JW	AL	10	kel	odf	rio	wuy	

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

	act	LUII htung! Shilillel Waljenlage				nff el di	en	a nidi]מ∫ ניוונ	dji1	191 rt in	1 - 5 Jeind	ch li	11]]1 nd fo	llen.	Nr. Beil	6. Sefah	treft	los 11	nd fri	ihseit	lig vern	iditen.			
1	6 vi	We	ljenlag	e	Ring	tellur	19	en i	ber Um	5 hibine	1 0	ets e	e v	e r	b i i	1 0 1 Stech	arbrett				10	1300	henng	ruppe	n	
	-					. c	2.1					\$2	07	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	exb	rzg.	
2	31				1	24	2					15	FV	MX	RW	DT	UZ	JQ	AO	CH	NY	k t l	acw	251	820 8	
R.	30	r O	LΟ	\mathbf{rs}	25	20	02	КМ	AX	PZ	00	D.I.	AT	CV	10	ER	0S.	LW	P2	FN	BH	ioc	acn	OVW	bvw	
8	2				2		03	DI	CN	RR	PV	CR	PV	AT	DK	OT	NO	EU	BX	LP	OJ	1 rb	cld	ude	rzh	
B	28	11	III		00	03	07	1.0	50	NS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vet	uis	
18	27	m	1	IV	11	03	0/	DT	14			W7	41.	RT	KO	co	EI	BJ	DU	FS	HP	xle	gbo	uev	rxn	
49	26	1	IV .									OP	PV	AD	IT.	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit	
10	25	11	III	r	ın	0	r		-			TY	15	0×	KV.	JM	DR	нх	GL	C2.	NU	kp1	rw1	vci	tlq	
49	24	v	1			E						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	14	11									PI	23	TN	RY	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
40	22	11	11	V	01	69	21	10	AS	DV	OL	PII	HI.	FY	05	02	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v	11	13	05	19	FT	OX	E2	CH	i no		07	AD.	RY	SV	JL	ox	BE	TW	jqd	cef	nvo	ysh	
49	20	111	10	v	24	9		_ 1	1				- 6	FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig	
49	19	V	111	1	11/	1	r	-11	IE	20		Or	- i	TV	40	X.W	FX	NT	PS	LU	BD	153	sb₩	vej	rxn_	
949	18	10	n	· •	15	1					· ·			LS	EM'	ov	OY	QX	AP	JP	BU	mae	hzi '	SOE	ysi.	
349	17	1	IV	12	21	10	00					нм	.10	DI	NR	BY	X.2	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
349	16	V	11	m	08	10	13	1.5				DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
349	15	11	IV.	1	101	05	0/				-	1.01				-					v	imz	noa	tjv	xtk	
349	14	11	1	v	15	11	03	VI	BT	MV	HU	LY	n	1.		r l	h		ע ב	-	х	zgr	dgz	gjo	ryg	
349	13			II	13	10	07	FW	EL	DO	KN	MU	μ		ч ;	51				u	W	zdy	rkf	tjw	xti	
649	112	· ·	15	10	10	26	16	RZ	00	CP	SX	KN									v	202	rjy	soi	wvn	
649	11	1 11	IV	III	1 22	20	01					LR	IK	MS	QU	H¥	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
649	10	III	v.	11	123	04	02					'QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	vby	tin	
649	19	V		· · · w	1 13	10	25	-			-	FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У	-	-		2
849	8	1 10	II IV	v II	100	03	22					. UX	12	HN	BK	QQ	CF	FT	JY	MW	AR	11		SI	ПО	ſ
049	17		14	II V	111	18	14					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1:				1
049	0	- m	1	IV	23	02	25	IL	AP	EU	но	NV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1		NON	nth	
049	12	1 1	11	1	04	21	05	QT	WZ	KV	GN	. AC	BL	02	EK	QX	OP	SU	DH	JM	TX	150	209	iwn	wak	
840	1 2	· v	1	11	19	11	00	BF	NR	DX	CS	' KR	MP	CN	BF	EH	DZ	IW	AV	0J	10	and	hdy	ivf	xtd	
010		IN	v	I	110	14	: 03	2				BN	HU	EO	PY	KQ	CP	US	JW	AL	10	kel	odf	rio	wuy	

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

-	ct	ntur	ign	Lu Schlüff	ftw elmitt	aff el di	en	Π ι nidi	la]	clju erjeb	1er rt in	1-5 Jeind	(1) li	11]]1 nd fo	llen.	Nr. Beil	64 Sefah	19	los 11	nd fr	ühzeit	lig vern	iditen.			
Tene 15-	6 vi	Wei	¢	Ring	tellur	19	en è	ier Um	5 kahrao	1 0	di e		e e .	b i i	i d i Stech	i n g erbrett	7		•	10	1300	henng	ruppe	n		
0	2.				14	2.9	2:1					SZ.	07	DV	KU	FO	мү	EW	JN	11	LQ	wny	dgy	exp	rzg.	
01	2				1	26	62					15	EV	MX	RW	DT	UZ	JQ	٨0	CH	NY	k t l	acw	251	20	
8	3.		LU	15	12	20	02	КМ	XA	P2	00	DJ	TA	CV	10	ER	QS	LW	P2	FN	BH	ioc	acu	OVW	ww.d	
8	4				04	00		DI	CN	BR	PV	CR	FV	AI	DK	OT	N.Q.M	EU	BX	LP	0 J	1 rb	cld	ude	rzh	
18	28	11	m		00	03	07	1.0	80	HS	IN	DY	IN	BV	OR	AM	LO	PP	НТ	EX	UW	woj	fbh	vct	uis	
18	27	m	1	IV	11	03			DA			V2	AL.	RT	KO	co	E1	BJ	DU	FS	HP	xle	gbo	uev	rxm	
16	26	1	IV .		•							OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit.	
49	25	IV	m	r	in	0	r		-			TY	15	0×	KV.	JM	DR	НΧ	GL	C2.	NU	k p l	rwl	vci	tlq	
49	24	v	1			E						iov	FR	AK	EO	DH	CJ	MZ	SX	ON	LT	ebn	rwm	udf	tlo	
49	23	14	11									PI	23	IM	RX	LV	AY	ou	BO	WZ	CN	jąc	acx	mwe	wvc	
40	22	11	IV	V	01	64	21	10	A2	DV	0 L	RI	HL.	FY	05	C2	DM	AW	CE	TV	NX	Jpw	del	mwf	wvf	
30	21	1	v		13	05	- PY	FT	OX.	E2	CH	110		07.	AU	RY	sv	JL	0 X	BE	TW	jqd	cef	nvo	ysh	
49	20	111	1V	v	24	9		_ 1	Ι.		ж.			FH	WY	DL	CM	AE	72	15	GI	idf	fpx	JWE	tig	
49	19	V	111	1	11/	1	r	-	IE	20		OI	1	IV	40	XW	FX	NT	PS	LU	BD	1 s a	"b₩	vej	rxn.	
949	18	IV	11	· · ·	15	1.					· · ·			LS	EM.	ov	OY	QX	AP	JP	BU	mae	hzi '	sog	ysi.	
349	17	1	10	11	21	10	00			-		нм	.10	DI	NR	BY	X.2	05	PU	FQ	CT	tdp	dhb	fkb	uiv	
149	16	v	11	m	08	10	13					DS	HY	MR	OW	LX	٨J	BQ	co	IP	NT	1 dw	hzj	soh	wvg.	
349	15	11	. IV .	1	101	05	01					i gu									v	imz	noa	tjv	xtk	
549	14	11	1	•	15		03	IA	вт	MV	HU	LY	1	1.		r l	~ (2	ע ב	-	х	zgr	dgz	ots	ryg	
649	13			n	13	20	07	FW	EL	DO	KN	MU	P		и ;	5		50		U	W	zdy	rkf	tjw	xtl	
649	112	· · ·	15	IV	10	26	16	RZ	00	CP	SX	KN									v	202	rjy	soi	wyh	
049	11	1 11	IV	111	1 22	20	01					LR	IK	MS	QU	Н₩	PT	00	VX	FZ	EN	lrc	zbx	vbm	TXO	
649	1.10	III	v	11	123	04	02					' QY	BS	LN	KT	AP	IU	DW	но	RV	JZ	edj	eyr	vby	tih	
649	19	V.		· · · ·	. 12	10	- 25				-	FI	NQ	SY	CU	BZ	HA	EL	TX	DO	KP	У		•		
849	8	11	n		100	03	22					. UX	12	HN	BK	QQ	CP	FT	JY	MW	AR	11		SI		T
049	17		10	II V	111	18	14					. DQ	GU	BW	NP	HK	A2	CI	PO	JX	VY	1:				
049	10	- m	1	11/	23	02	25	IL	AP	EU	но	NV	CL	OK	QQ	BI	FU	HS	PX	NW	EY	1	COLUMN 1			
649	1 2	1	11	14	04	21	09	QT	WZ	KV	GN	. AC	BL	02	EK	Q¥	OP	SU	DH	JM	TX	150	209	vey	wak	
049	1 4	- "	14		1.0		04	BF	NR	DX	CS	· KR	MP	CN	BF	EH	D2	IW	AV	OJ	LO	Inp	bwo	1.40	v t d	
040	1 2	1 1/																								

A random permutation of the alphabet:



◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

A random permutation of the alphabet:



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

э

An enigma permutation of the alphabet:



▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 のへで

An enigma permutation of the alphabet:



э

Message key: BLA Encrypted message key (using daily key):

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

Message key: BLA Encrypted message key (using daily key):

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

$$A \rightarrow W$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●



Bletchley Park Bombe replica Antoine Taveneaux, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0, via_Wikimedia Commons

Advent of Computers: AES (Advanced Encryption Standard)



Jeongysu, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0, via Wikimedia Commons

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

How is this even possible?!

The door to modern cryptography: modular arithmetic



Setup: p (modulus), g



Setup: p (modulus), g

Alice

Bob

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @





Setup: p (modulus), g



▲□▶ ▲□▶ ▲ □▶ ▲ □▶ □ のへぐ

Setup: p (modulus), g



▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 のへで

Setup: p (modulus), g



▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

Setup: p (modulus), g



An eavesdropper Eve can see g^a and g^b and must compute g^{ab} .

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

A hard cryptographic problem is:

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

- A hard cryptographic problem is:
 - ► a mathematical problem (e.g. factoring)

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

- A hard cryptographic problem is:
 - a mathematical problem (e.g. factoring)
 - which is believed to be computationally intensive to solve,

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

- A hard cryptographic problem is:
 - a mathematical problem (e.g. factoring)
 - which is believed to be computationally intensive to solve,

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

and upon which we can build a public-key cryptographic protocol such as encryption,

- A hard cryptographic problem is:
 - ► a mathematical problem (e.g. factoring)
 - which is believed to be computationally intensive to solve,
 - and upon which we can build a public-key cryptographic protocol such as encryption,
 - whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

A hard cryptographic problem is:

- a mathematical problem (e.g. factoring)
- which is believed to be computationally intensive to solve,
- and upon which we can build a public-key cryptographic protocol such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for public-key encryption is that

A hard cryptographic problem is:

- a mathematical problem (e.g. factoring)
- which is believed to be computationally intensive to solve,
- and upon which we can build a public-key cryptographic protocol such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

encryption is easy (i.e. fast) using no secret info

- A hard cryptographic problem is:
 - a mathematical problem (e.g. factoring)
 - which is believed to be computationally intensive to solve,
 - and upon which we can build a public-key cryptographic protocol such as encryption,
 - whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.
- The idea for public-key encryption is that
 - encryption is easy (i.e. fast) using no secret info
 - decryption is easy for the intended recipient (who has extra secret info)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

- A hard cryptographic problem is:
 - a mathematical problem (e.g. factoring)
 - which is believed to be computationally intensive to solve,
 - and upon which we can build a public-key cryptographic protocol such as encryption,
 - whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.
- The idea for public-key encryption is that
 - encryption is easy (i.e. fast) using no secret info
 - decryption is easy for the intended recipient (who has extra secret info)
 - decryption is infeasible (i.e. too slow) for anyone else (who does not have the extra info)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

A hard cryptographic problem is:

- a mathematical problem (e.g. factoring)
- which is believed to be computationally intensive to solve,
- and upon which we can build a public-key cryptographic protocol such as encryption,
- whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for public-key encryption is that

- encryption is easy (i.e. fast) using no secret info
- decryption is easy for the intended recipient (who has extra secret info)
- decryption is infeasible (i.e. too slow) for anyone else (who does not have the extra info)

For example, to decrypt a message meant for someone else, it may require factoring a number so big, that it is expected to take longer than the length of time before the sun dies.



We don't actually know they are hard!



The **Computational Diffie-Hellman Problem**: Given $g^a, g^b \pmod{p}$, compute g^{ab} .

- Typical algorithms take around \sqrt{p} time.
- Human record: p of 795 bits using 3100 core-years
- Standard internet security: 1024 bits
- Logjam attack: 512 bits attacked in the wild
- (Why did Logjam work? Big swaths of the internet were using the same prime!)
RSA: Rivest-Shamir-Adelman

The Factoring Problem:

Given an integer n = pq for p and q prime, find p and q.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

- Human record: $n \sim 2^{829}$.
- Standard internet security: $n \sim 2^{2048}$.

How big is 2^{2048} ?

How big is 2^{2048} ?

					2 ²⁰⁴		
						Infinity	
Rad		x!	()	%	AC	
Inv	sin	In	7	8	9	÷	
π	COS	log	4	5	6	×	
е	tan	1	1	2	3	-	
Ans	EXP	ХУ	0		=	+	

More info

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

Estimate each quantity as a power of two (and put them in order!)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

- The number of atoms in the universe.
- The number of cells in a human body.
- The number of insects per human on earth.
- The number of seconds until the sun dies.

How big is 2^{2048} ?

• The number of insects per human on earth: $2^{28} \sim 200$ million.

(ロ)、(型)、(E)、(E)、(E)、(O)へ(C)

The number of insects per human on earth: 2²⁸ ~ 200 million.
The number of cells in a human body: 2⁴⁵ ~ 37.2 trillion.

How big is 2^{2048} ?

The number of insects per human on earth: 2²⁸ ~ 200 million.
The number of cells in a human body: 2⁴⁵ ~ 37.2 trillion.
The number of seconds until the sun dies: 2⁵⁷ ~ 7.5 billion years.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

- The number of insects per human on earth: $2^{28} \sim 200$ million.
- The number of cells in a human body: $2^{45} \sim 37.2$ trillion.
- The number of seconds until the sun dies: 2⁵⁷ ~ 7.5 billion years.
- ▶ The number of atoms in the universe: $2^{266} \sim 10^{80} \sim 100$ quadrillion vigintillion.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

More modern cryptography: Elliptic Curve Cryptography

Do your computations with a crazy group called an



elliptic curve.

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

When will we have quantum computers?

(ロ)、(型)、(E)、(E)、(E)、(O)へ(C)

When will we have quantum computers?

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @

The unit of measure is decades.

When will we have quantum computers?

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

The unit of measure is decades.

► What can they do?

When will we have quantum computers?

The unit of measure is decades.

- What can they do?
 - They can factor and solve discrete logarithm too quickly: break all of current cryptography.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

When will we have quantum computers?

The unit of measure is decades.

- What can they do?
 - They can factor and solve discrete logarithm too quickly: break all of current cryptography.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

What are we doing about it?

When will we have quantum computers?

The unit of measure is decades.

- What can they do?
 - They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- What are we doing about it?
 - NIST is standarizing new protols based on new hard problems that are believed to be quantum-safe.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

When will we have quantum computers?

The unit of measure is decades.

- What can they do?
 - They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- What are we doing about it?
 - NIST is standarizing new protols based on new hard problems that are believed to be quantum-safe.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

We will study **quantum cryptography**, **quantum algorithms** and **post-quantum cryptography**.



Bonus: Whirlwind tour of coding theory

Image: the editors of encyclopedia britannica, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

イロト イヨト イヨト イヨト

What is coding theory for? (What problem are we solving?)

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

What is coding theory for? (What problem are we solving?)
Real-life channels (radio, cell phone, copper wires) are noisy.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

- What is coding theory for? (What problem are we solving?)
 - Real-life **channels** (radio, cell phone, copper wires) are **noisy**.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

We want to send messages in such a way that errors won't prevent understanding.

- What is coding theory for? (What problem are we solving?)
 - Real-life channels (radio, cell phone, copper wires) are noisy.
 - We want to send messages in such a way that errors won't prevent understanding.
 - Usually we model a channel as something that randomly flips bits of our binary message (errors).

- What is coding theory for? (What problem are we solving?)
 - Real-life channels (radio, cell phone, copper wires) are noisy.
 - We want to send messages in such a way that errors won't prevent understanding.
 - Usually we model a channel as something that randomly flips bits of our binary message (errors).

Nothing to do with secrecy.





What is coding theory?

We change our message (encoding) so that it is error resistant.

What is coding theory?

We change our message (encoding) so that it is error resistant.

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

We send codewords instead of plaintext symbols.

- What is coding theory?
 - We change our message (encoding) so that it is error resistant.
 - We send codewords instead of plaintext symbols.
 - Example: 'Victor' instead of 'V' (radio) or '000' instead of '0' (a repeat code)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

- What is coding theory?
 - We change our message (encoding) so that it is error resistant.
 - We send codewords instead of plaintext symbols.
 - Example: 'Victor' instead of 'V' (radio) or '000' instead of '0' (a repeat code)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

The receiver must decode





What makes a good code?

Strong error correction: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

What makes a good code?

Strong error correction: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

- Strong efficiency: not too much space inflation (codewords are longer than the symbols they represent)
- What math goes into it?

What makes a good code?

Strong error correction: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')

- Strong efficiency: not too much space inflation (codewords are longer than the symbols they represent)
- What math goes into it?
 - Finite fields, linear algebra

About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.

- Course modules:
 - Paradigms, history and application
 - Modular arithmetic & discrete logarithm
 - Euclidean algorithm, primality testing & factoring
 - Finite fields & elliptic curve cryptography
 - Coding theory & lattice-based cryptography
 - Quantum aspects

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
 - Paradigms, history and application
 - Modular arithmetic & discrete logarithm
 - Euclidean algorithm, primality testing & factoring
 - Finite fields & elliptic curve cryptography
 - Coding theory & lattice-based cryptography
 - Quantum aspects
- Course style: Daily assignments, regular quizzes, poster project, self-evaluation

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
 - Paradigms, history and application
 - Modular arithmetic & discrete logarithm
 - Euclidean algorithm, primality testing & factoring
 - Finite fields & elliptic curve cryptography
 - Coding theory & lattice-based cryptography
 - Quantum aspects
- Course style: Daily assignments, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
 - Paradigms, history and application
 - Modular arithmetic & discrete logarithm
 - Euclidean algorithm, primality testing & factoring
 - Finite fields & elliptic curve cryptography
 - Coding theory & lattice-based cryptography
 - Quantum aspects
- Course style: Daily assignments, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord
- contingency plan: last-minute modality change

Your semester ahead

- About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- Course modules:
 - Paradigms, history and application
 - Modular arithmetic & discrete logarithm
 - Euclidean algorithm, primality testing & factoring
 - Finite fields & elliptic curve cryptography
 - Coding theory & lattice-based cryptography
 - Quantum aspects
- Course style: Daily assignments, regular quizzes, poster project, self-evaluation
- https://crypto.katestange.net (linked in canvas) / discord
- contingency plan: last-minute modality change
- recording class