Wie geheim ist eine Geheimschrift?

Dr. Felix Fontein

Institut für Mathematik
Universität Zürich

15. Januar 2014

Was wir heute behandeln

- Wo werden Geheimschriften verwendet?
- Wie funktionieren einfache Geheimschriften?
- Wie kann man solche Geheimschriften trotzdem lesen?
- Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?
- Und worauf basieren moderne Geheimschriften?

Was wir heute behandeln

- Wo werden Geheimschriften verwendet?
- Wie funktionieren einfache Geheimschriften?
- Wie kann man solche Geheimschriften trotzdem lesen?
- Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?
- Und worauf basieren moderne Geheimschriften?

Wo werden Geheimschriften verwendet?

- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet

Wo werden Geheimschriften verwendet?

- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet

Wo werden Geheimschriften verwendet?

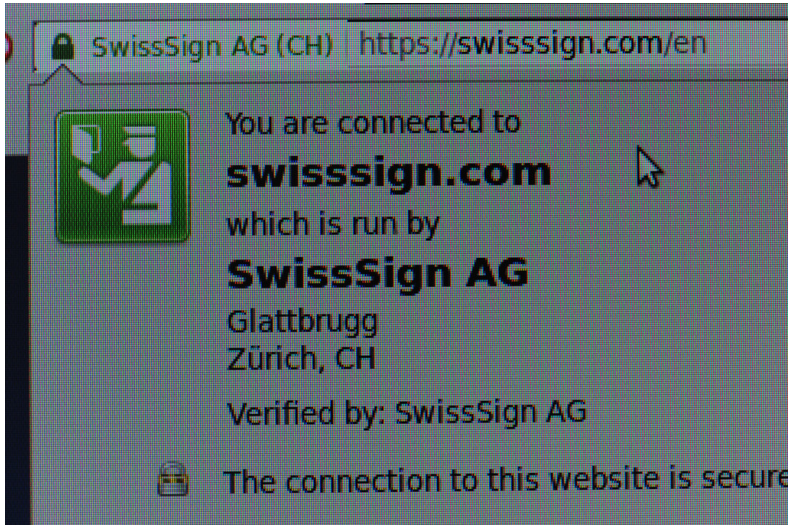
- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet

Wo werden Geheimschriften verwendet?

- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet

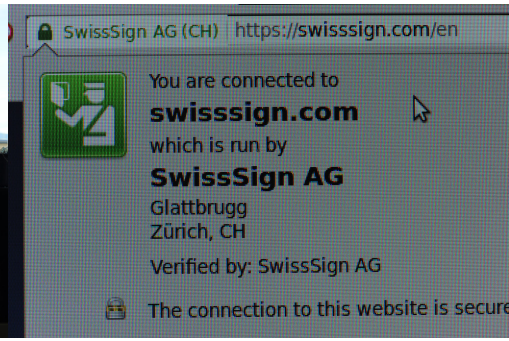
Wo werden Geheimschriften verwendet?

- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet



Wo werden Geheimschriften verwendet?

- Passwörter beim Computer
- Handy-Gespräche
- Fernsehen über Kabel
- Internet



Was wir heute behandeln

Wie funktionieren einfache Geheimschriften?

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

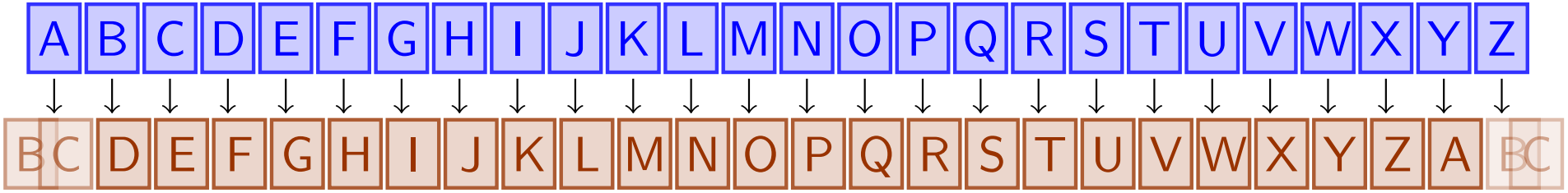
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Tp ibu Dbftbs tfjof Obdisjdiufo wfstufdlu:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:



Tp ikw Dofvbs tfjqf Qodksjdkwfq yfstwfdlw:

Verschiebung um einen Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
~~B~~ ~~C~~	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B C

Vr kdw Fdhvdu vhlqh Qdfkulfkwh yhuvwhfnw:

Verschiebung um drei Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Vr kdw Fdhvdu vhlqh Qdfkulfkwhq yhuvwhfnw:

Verschiebung um drei Buchstaben!

Caesar-Systeme

So hat Caesar seine Nachrichten versteckt:

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

Vr kdw Fdhvdu vhlqh Qdfkulfkwhq yhuvwhfnw:

Verschiebung um drei Buchstaben!

Und wie sicher ist das?

`Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:`

Und wie sicher ist das?

```
     Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:
+1   Ws lex Geiwev wimri Reglvmglxir zivwxigox:
```

Und wie sicher ist das?

	Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:
+1	Ws lex Geiwev wimri Reglvmglxir zivwxigox: ✗
+2	Xt mfy Hfjxfw xjnsj Sfhmwnhmyjs ajwxyjhpy: ✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗
+4	Zv	oha	Jhlzhy	zlpul	Uhjoypjoalu	clyzaljra:	✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗
+4	Zv	oha	Jhlzhy	zlpul	Uhjoypjoalu	clyzaljra:	✗
+5	Aw	pib	Kimaiz	amqvm	Vikpzqkpbmv	dmzabmksb:	✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗
+4	Zv	oha	Jhlzhy	zlpul	Uhjoypjoalu	clyzaljra:	✗
+5	Aw	pib	Kimaiz	amqvm	Vikpzqkpbmv	dmzabmksb:	✗
⋮	⋮						
⋮	⋮						

Und wie sicher ist das?

	Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:	
+1	Ws lex Geiwev wimri Reglvmglxir zivwxigox:	✗
+2	Xt mfy Hfjxfw xjnsj Sfhmwnhmyjs ajwxyjhpy:	✗
+3	Yu ngz Igkygx ykotk Tginxoinzkt bkxyzkiqz:	✗
+4	Zv oha Jhlzhy zlpul Uhjoypjoalu clyzaljra:	✗
+5	Aw pib Kimaiz amqvm Vikpzqkpbmv dmzabmksb:	✗
⋮	⋮	
⋮	⋮	
+19	Ok dwp Ywaown oaeja Jwydneydpaj ranopaygp:	✗

Und wie sicher ist das?

	Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:	
+1	Ws lex Geiwev wimri Reglvmglxir zivwxigox:	✗
+2	Xt mfy Hfjxfw xjnsj Sfhmwnhmyjs ajwxyjhpy:	✗
+3	Yu ngz Igkygx ykotk Tginxoinzkt bkxyzkiqz:	✗
+4	Zv oha Jhlzhy zlpul Uhjoypjoalu clyzaljra:	✗
+5	Aw pib Kimaiz amqvm Vikpzqkpbmv dmzabmksb:	✗
⋮	⋮	
⋮	⋮	
+19	Ok dwp Ywaown oaeja Jwydneydpaj ranopaygp:	✗
+20	Pl exq Zxbpxo pbfkb Kxzeofzeqbk sbopqbzhq:	✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗
+4	Zv	oha	Jhlzhy	zlpul	Uhjoypjoalu	clyzaljra:	✗
+5	Aw	pib	Kimaiz	amqvm	Vikpzqkpbmv	dmzabmksb:	✗
⋮	⋮						
⋮	⋮						
+19	Ok	dwp	Ywaown	oaeja	Jwydneydpaj	ranopaygp:	✗
+20	Pl	exq	Zxbpxo	pbfkb	Kxzeofzeqbk	sbopqbzhq:	✗
+21	Qm	fyr	Aycqyp	qcglc	Lyafpgafrcl	tcpqrcair:	✗

Und wie sicher ist das?

	Vr	kdw	Fdhvdu	vhlnh	Ndfkulfkvhq	yhuvwhfnw:	
+1	Ws	lex	Geiwev	wimri	Reglvmglxir	zivwxigox:	✗
+2	Xt	mfy	Hfjxfw	xjnsj	Sfhmwnhmyjs	ajwxyjhpy:	✗
+3	Yu	ngz	Igkygx	ykotk	Tginxoinzkt	bkxyzkiqz:	✗
+4	Zv	oha	Jhlzhy	zlpul	Uhjoypjoalu	clyzaljra:	✗
+5	Aw	pib	Kimaiz	amqvm	Vikpzqkpbmv	dmzabmksb:	✗
⋮	⋮						
⋮	⋮						
+19	Ok	dwp	Ywaown	oaeja	Jwydneydpaj	ranopaygp:	✗
+20	Pl	exq	Zxbpxo	pbfkb	Kxzeofzeqbk	sbopqbzhq:	✗
+21	Qm	fyr	Aycqyp	qcglc	Lyafpgafrcl	tcpqrcair:	✗
+22	Rn	gzs	Bzdrzq	rdhmd	Mzbgqhbgsdm	udqrsdbjs:	✗

Und wie sicher ist das?

	Vr kdw Fdhvdu vhlnh Ndfkulfkvhq yhuvwhfnw:	
+1	Ws lex Geiwev wimri Reglvmglxir zivwxigox:	✗
+2	Xt mfy Hfjxfw xjnsj Sfhmwnhmyjs ajwxyjhpy:	✗
+3	Yu ngz Igkygx ykotk Tginxoinzkt bkxyzkiqz:	✗
+4	Zv oha Jhlzhy zlpul Uhjoypjoalu clyzaljra:	✗
+5	Aw pib Kimaiz amqvm Vikpzqkpbmv dmzabmksb:	✗
⋮	⋮	
⋮	⋮	
+19	Ok dwp Ywaown oaeja Jwydneydpaj ranopaygp:	✗
+20	Pl exq Zxbpxo pbfkb Kxzeofzeqbk sbopqbzhq:	✗
+21	Qm fyr Aycqyp qcglc Lyafpgafrcl tcpqrcair:	✗
+22	Rn gzs Bzdrzq rdhmd Mzbgqhbgsdm udqrsdbjs:	✗
+23	So hat Caesar seine Nachrichten versteckt:	✓

Und wie sicher ist das?

Höchstens 25 mal probieren!

Und wie sicher ist das?

Höchstens 25 mal probieren!

$\longrightarrow$ nicht sehr sicher...

Substitutions-Systeme

Wie kann man das geschickter anstellen?

Substitutions-Systeme

Wie kann man das geschickter anstellen?

Idee: beliebige Buchstabenvertauschungen zulassen!

Substitutions-Systeme

Wie kann man das geschickter anstellen?

Idee: beliebige Buchstabenvertauschungen zulassen!

So ist das schon viel komplizierter:

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

Substitutions-Systeme

Wie kann man das geschickter anstellen?

Idee: beliebige Buchstabenvertauschungen zulassen!

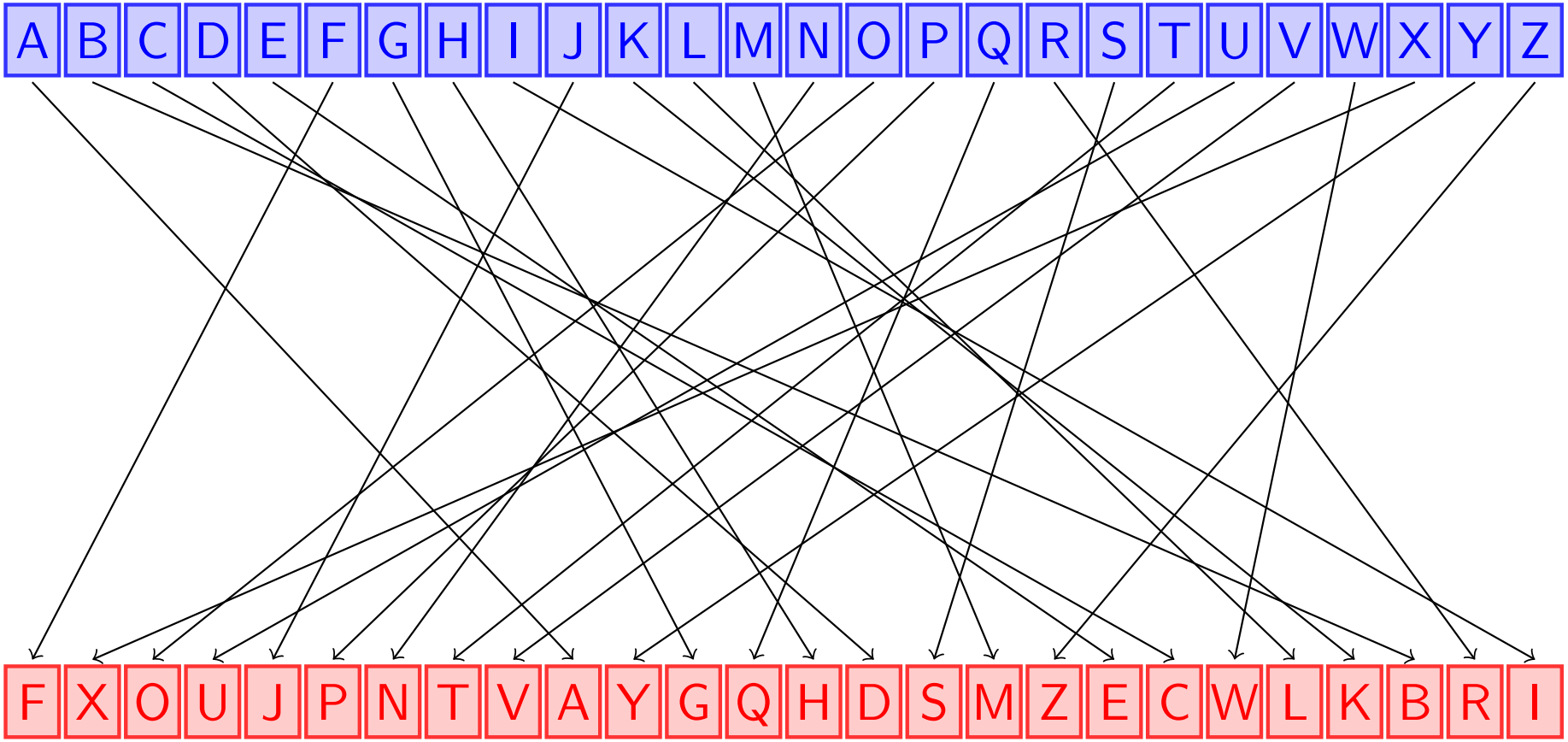
So ist das schon viel komplizierter:

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

Ed vec ufe eotdh lvjg ydqsgvivjzcjz:

Substitutions-Systeme

So ist das schon viel komplizierter:



Ed vec ufe eotdh lvjg ydqsgvivjzcjz:

Und wie sicher ist das?

Es gibt

$$\begin{aligned} 26! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots 24 \cdot 25 \cdot 26 \\ &= 403'291'461'126'605'635'584'000'000 \end{aligned}$$

Möglichkeiten! (403 Quadrillionen 291 Trilliarden 461 Trillionen 126 Billiarden 605 Billionen 635 Milliarden 584 Millionen)

Und wie sicher ist das?

Es gibt

$$\begin{aligned} 26! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots 24 \cdot 25 \cdot 26 \\ &= 403'291'461'126'605'635'584'000'000 \end{aligned}$$

Möglichkeiten! (403 Quadrillionen 291 Trilliarden 461 Trillionen 126 Billiarden 605 Billionen 635 Milliarden 584 Millionen)

Zum Vergleich: um einen Sechser im Lotto zu bekommen und die Superzahl richtig zu haben, muss man in etwa

$$139'838'160$$

mal Lotto spielen!

Und wie sicher ist das?

Es gibt

$$\begin{aligned} 26! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots 24 \cdot 25 \cdot 26 \\ &= 403'291'461'126'605'635'584'000'000 \end{aligned}$$

Möglichkeiten! (403 Quadrillionen 291 Trilliarden 461 Trillionen 126 Billiarden 605 Billionen 635 Milliarden 584 Millionen)

Zum Vergleich: um einen Sechser im Lotto zu bekommen und die Superzahl richtig zu haben, muss man in etwa

$$139'838'160$$

mal Lotto spielen!

Das sind 18 Dezimalstellen weniger!

Was wir heute behandeln

Wie kann man solche Geheimschriften trotzdem lesen?

Häufigkeitsanalyse

Vorsicht:

Ed vec ufe eotdh lvjg ydqsgvivjzcjz

Häufigkeitsanalyse

Vorsicht:

Ed vec ufe eotdh lvjg ydqsgvivjzcjz

Anders sortiert:

cc ddd eeee f gg h i jjj l o q s t u vvvv y zz

Manche Buchstaben kommen **öfter** vor als andere!

Häufigkeitsanalyse

- in der deutschen Sprache kommt **e** am häufigsten vor! (17.40%)
- danach folgen **n** (9.78%), **i** (7.55%), **s** (7.27%), **r** (7.00%) und **a** (6.51%)
- Buchstaben wie **p** (0.79%), **v** (0.67%), **j** (0.27%), **y** (0.04%), **x** (0.03%), **q** (0.02%) kommen selten vor

Häufigkeitsanalyse

- in der deutschen Sprache kommt **e** am häufigsten vor! (17.40%)
- danach folgen **n** (9.78%), **i** (7.55%), **s** (7.27%), **r** (7.00%) und **a** (6.51%)
- Buchstaben wie **p** (0.79%), **v** (0.67%), **j** (0.27%), **y** (0.04%), **x** (0.03%), **q** (0.02%) kommen selten vor

Ed vec ufe eotdh lvjg ydqsgvivjzcjz

cc ddd eeee f gg h i jjj l o q s t u vvvv y zz

e, **n**, **i**, **s**, **r**, **a** $\longleftrightarrow$ **d**, **e**, **j**, **v**?

Häufigkeitsanalyse

- in der deutschen Sprache kommt **e** am häufigsten vor! (17.40%)
- danach folgen **n** (9.78%), **i** (7.55%), **s** (7.27%), **r** (7.00%) und **a** (6.51%)
- Buchstaben wie **p** (0.79%), **v** (0.67%), **j** (0.27%), **y** (0.04%), **x** (0.03%), **q** (0.02%) kommen selten vor

Ed vec ufe eotdh lvjg ydqsgvivjzcjz

cc ddd eeee f gg h i jjj l o q s t u vvvv y zz

e, **n**, **i**, **s**, **r**, **a** $\longleftrightarrow$ **d**, **e**, **j**, **v**?

So ist das schon viel komplizierter

Häufigkeitsanalyse

A	B	C	D	E	F	G	H	I
5.54%	1.61%	2.60%	4.32%	14.81%	1.41%	2.56%	4.05%	6.43%

J	K	L	M	N	O	P	Q	R
0.23%	1.03%	2.93%	2.15%	8.33%	2.14%	0.25%	0.02%	5.96%

S	T	U	V	W	X	Y	Z	␣
6.19%	5.24%	3.70%	0.57%	1.61%	0.03%	0.03%	0.96%	15.30%

Wie kann man die Geheimschrift verbessern?

- Nicht einen Buchstaben auf einmal bearbeiten, sondern mehrere!

Wie kann man die Geheimschrift verbessern?

- Nicht einen Buchstaben auf einmal bearbeiten, sondern mehrere!

N	o	c	h	␣	v	i	e	l	␣	k	o	m	p	l	i	z	i	e	r	t	e	r	!

N o c h ␣ v i e	l ␣ k o m p l i	z i e r t e r !

Wie kann man die Geheimschrift verbessern?

- Nicht einen Buchstaben auf einmal bearbeiten, sondern mehrere!

N	o	c	h	␣	v	i	e	l	␣	k	o	m	p	l	i	z	i	e	r	t	e	r	!

N o c h ␣ v i e	l ␣ k o m p l i	z i e r t e r !

Bei 54 verschiedenen Zeichen (Buchstaben klein und gross, Leerzeichen, Ausrufezeichen) gibt es $54^8 = 72'301'961'339'136$ verschiedene Inhalte für die grossen Buchstabenpakete!

$$
\begin{aligned}
AAAAAAAA &\rightarrow BZKOPCIW \\
AAAAAAAB &\rightarrow AJBIZURE \\
AAAAAAAC &\rightarrow QLGKKXJT \\
&\vdots \\
AAAAAABA &\rightarrow WUIRKCKL \\
AAAAAABB &\rightarrow APGOFZST \\
&\vdots
\end{aligned}
$$

Wie kann man die Geheimschrift verbessern?

- Nicht einen Buchstaben auf einmal bearbeiten, sondern mehrere!

N	o	c	h	␣	v	i	e	l	␣	k	o	m	p	l	i	z	i	e	r	t	e	r	!

N o c h ␣ v i e	l ␣ k o m p l i	z i e r t e r !

Bei 54 verschiedenen Zeichen (Buchstaben klein und gross, Leerzeichen, Ausrufezeichen) gibt es $54^8 = 72'301'961'339'136$ verschiedene Inhalte für die grossen Buchstabenpakete!

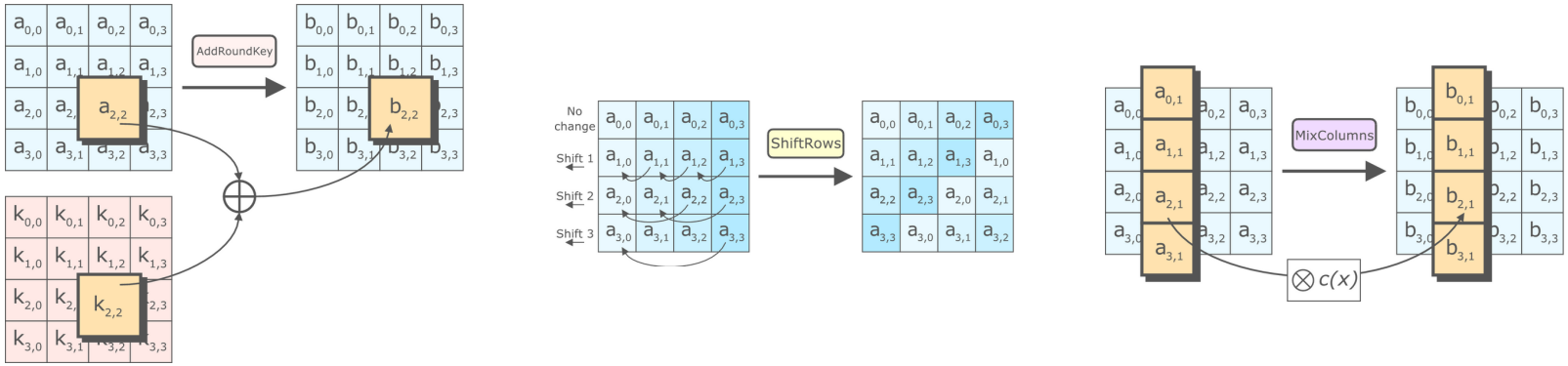
$$
\begin{aligned}
AAAAAAAA &\rightarrow BZKOPCIW \\
AAAAAAAB &\rightarrow AJBIZURE \\
AAAAAAAC &\rightarrow QLGKKXJT \\
&\vdots \\
AAAAAABA &\rightarrow WUIRKCKL \\
AAAAAABB &\rightarrow APGOFZST \\
&\vdots
\end{aligned}
$$

- Nicht bei jedem Buchstaben(-paket) die gleiche Vertauschung nehmen!

Was wird heute verwendet?

Advanced Encryption Standard (AES)

- Seit über 13 Jahren
- Arbeitet mit 16 bis 32 Zeichen auf einmal
- Bisher kein praktischer Ansatz zum Knacken

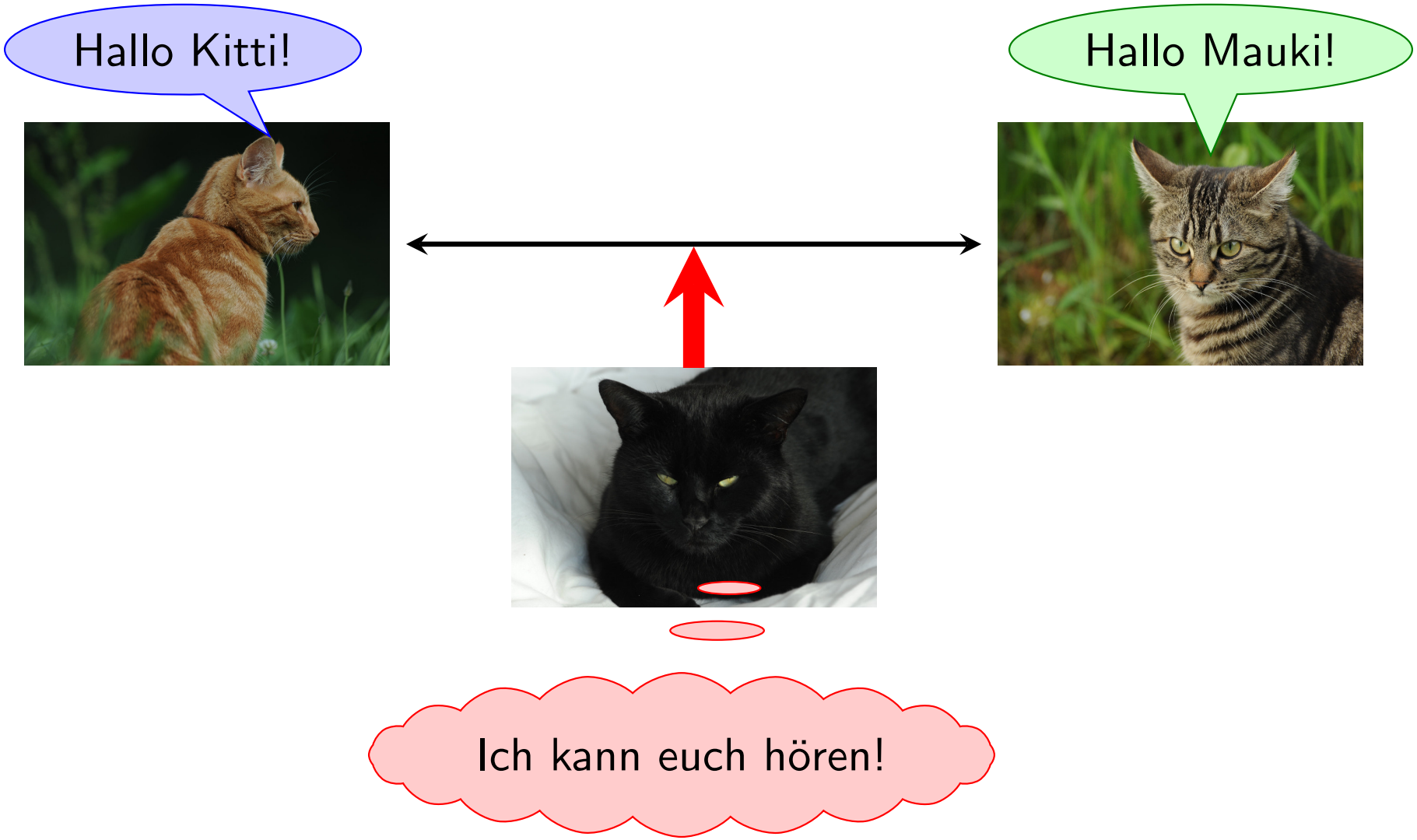


Was wir heute behandeln

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?



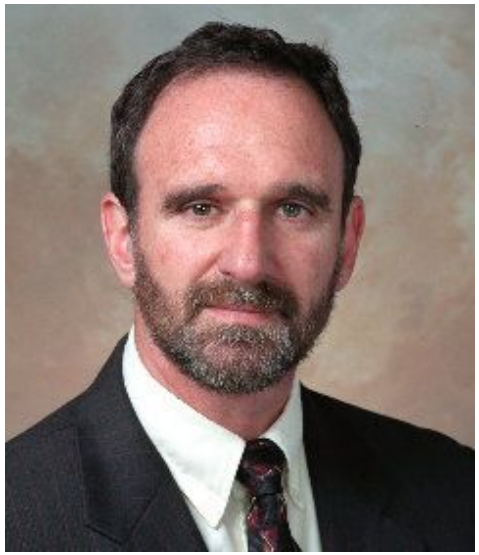
Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

1976: Diffie-Hellman-Schlüsselaustausch

Whitfield Diffie

CC-BY-2.0 © Mary Holzer
Quelle: Infosecpedia, Wikipedia

Martin Hellman



CC-BY-SA-3.0 © Martin Hellman
Quelle: Wikipedia

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

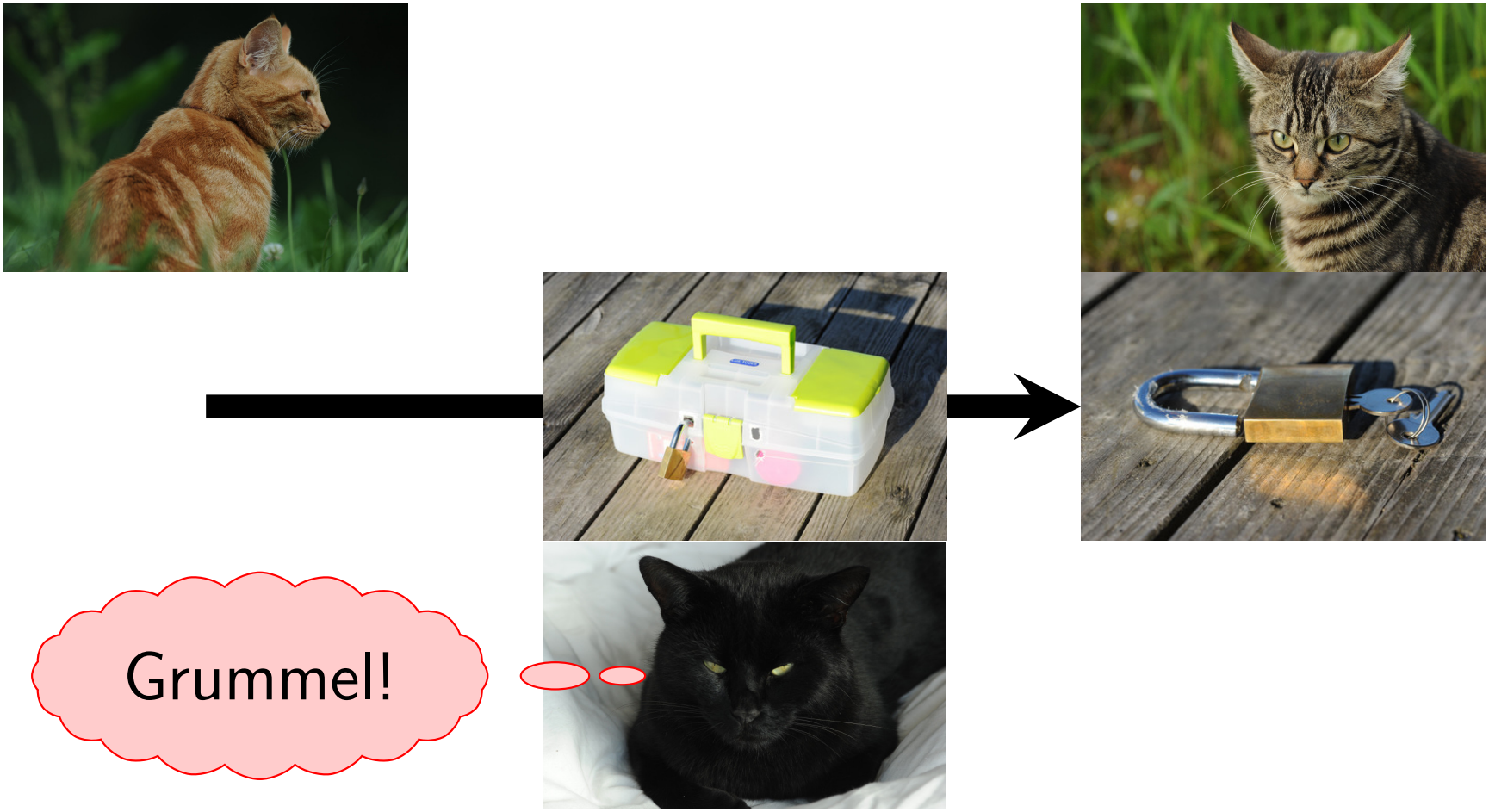
Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

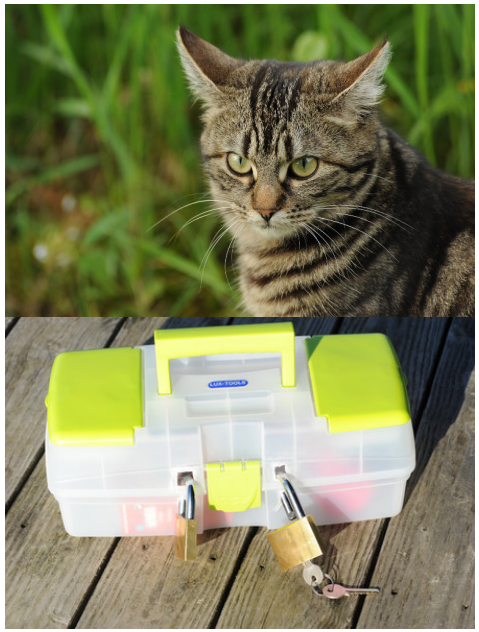
Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

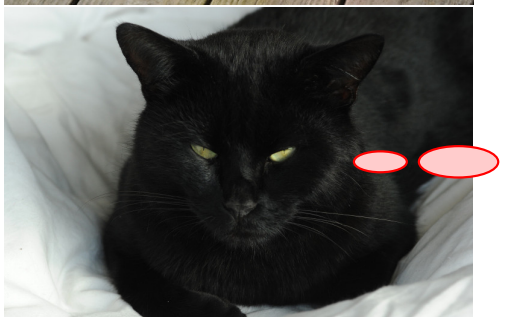
Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



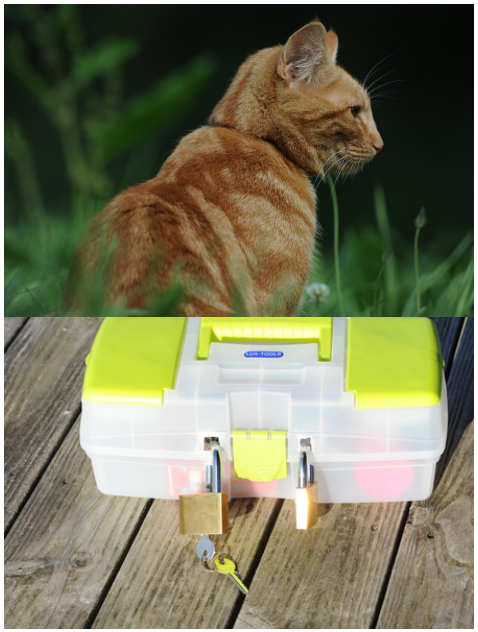
Grummel!

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

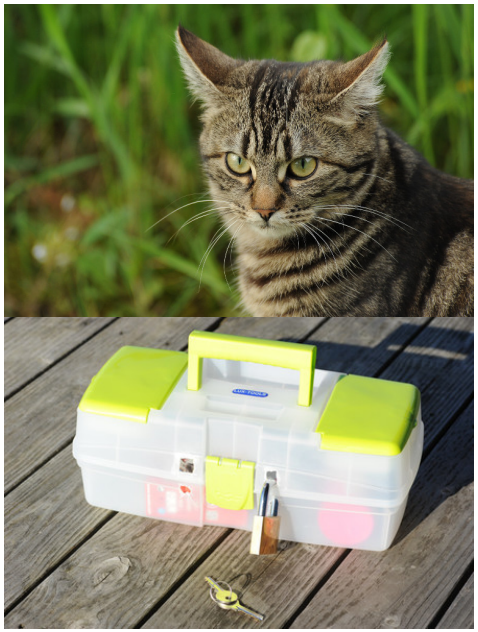
Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

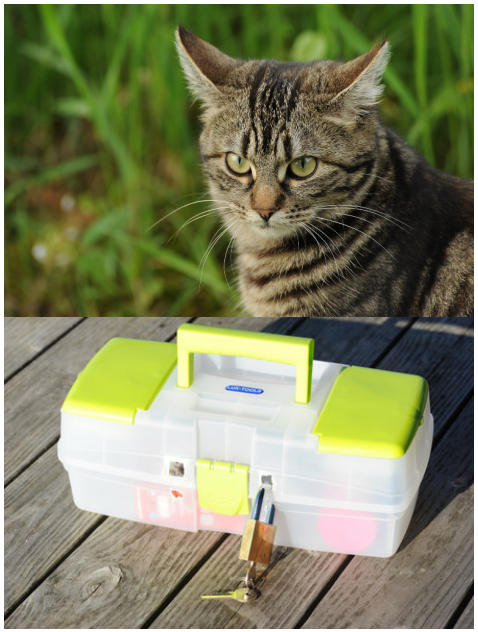
Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



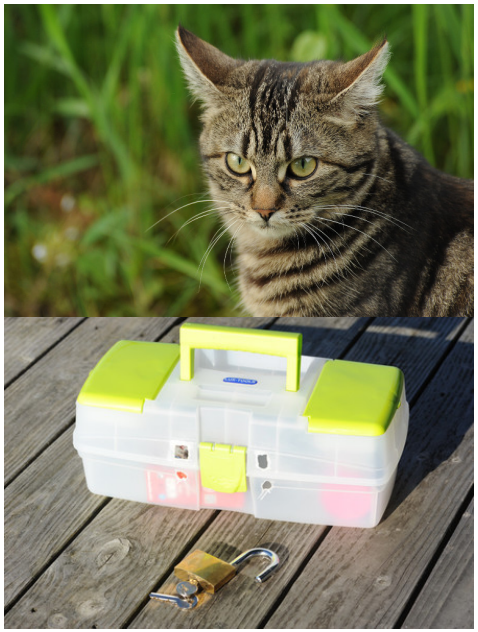
Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:



Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Vereinfachter Austausch:

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Was kann schiefgehen?

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Was kann schiefgehen?

- Die schwarze Katze bricht die Kiste auf!

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Was kann schiefgehen?

- Die schwarze Katze bricht die Kiste auf!

- Ist Kitti wirklich Kitti?
- Und ist Mauki wirklich Mauki?

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

Was kann schiefgehen?

- Die schwarze Katze bricht die Kiste auf!

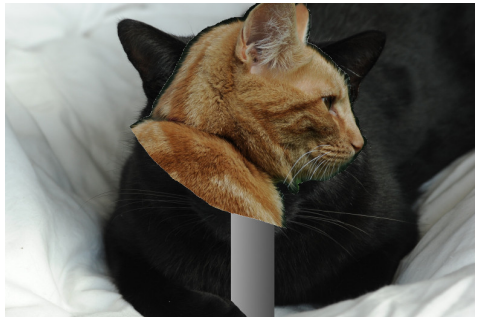
- Ist Kitti wirklich Kitti?
- Und ist Mauki wirklich Mauki?

Wie können sich zwei Personen auf eine Geheimschrift einigen, wenn eine dritte Person dabei ist?

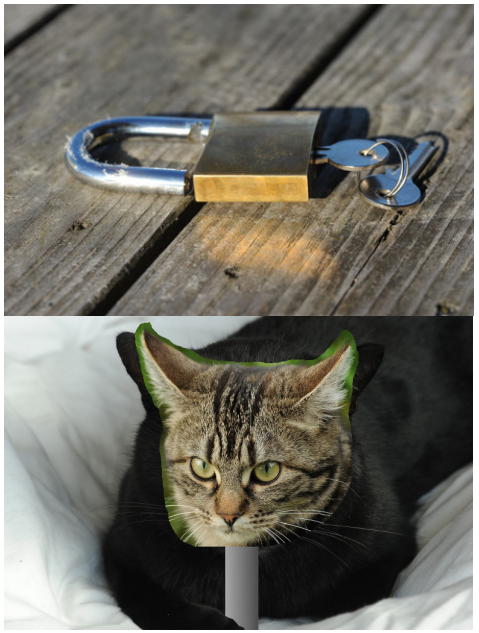
Was kann schiefgehen?

- Die schwarze Katze bricht die Kiste auf!

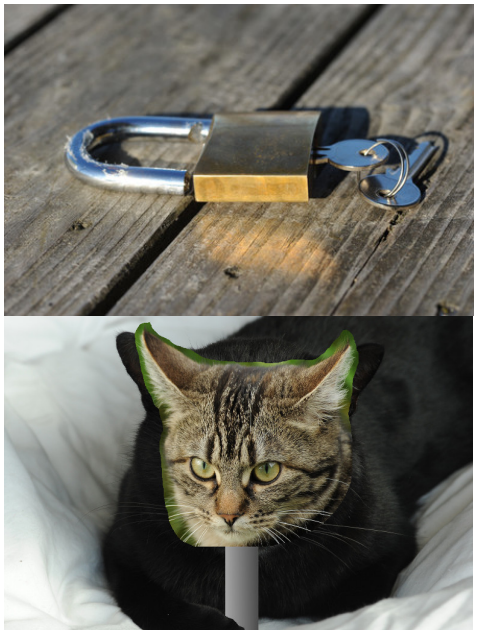
- Ist Kitti wirklich Kitti?
- Und ist Mauki wirklich Mauki?



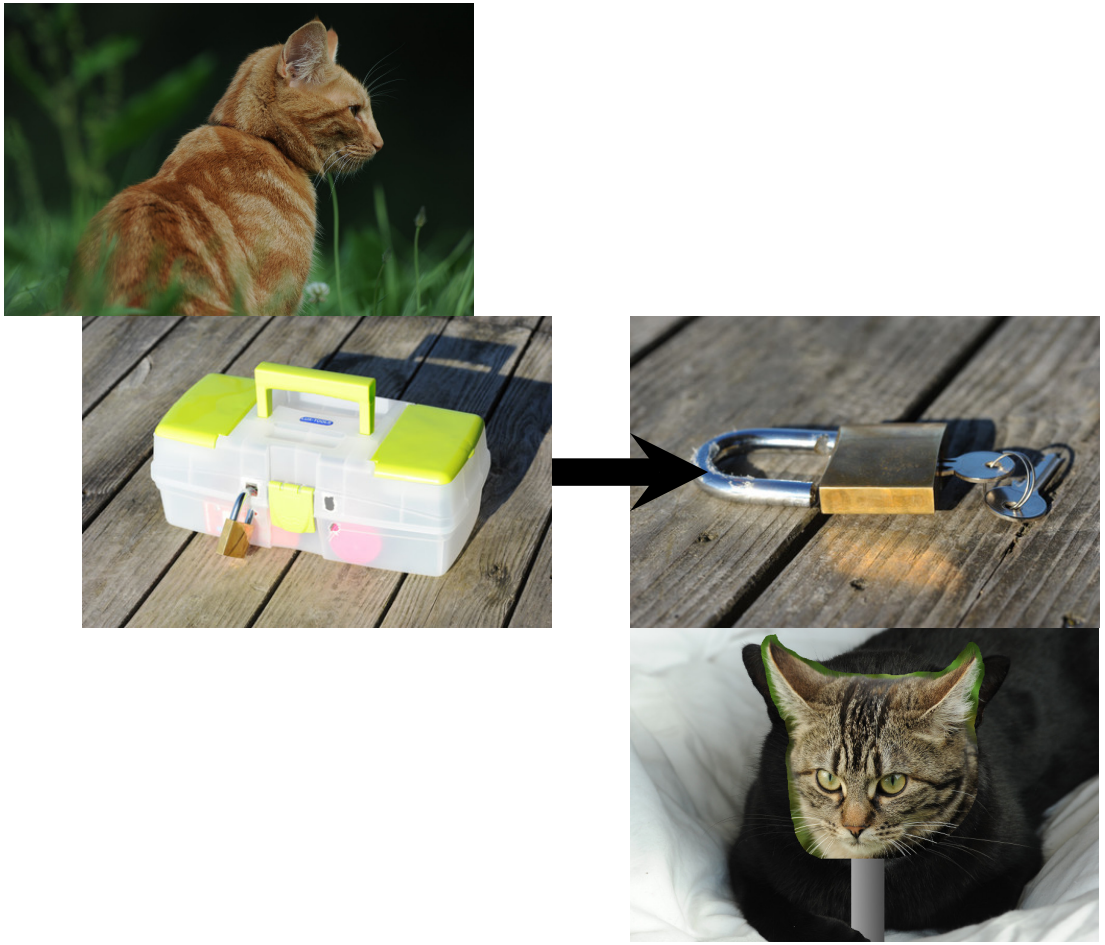
Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

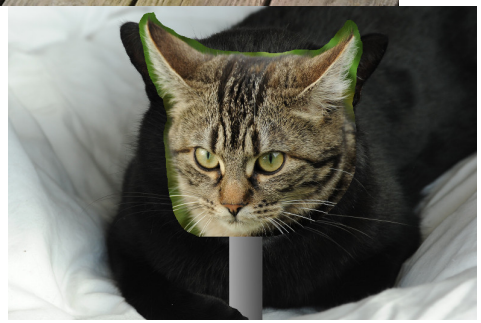


Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



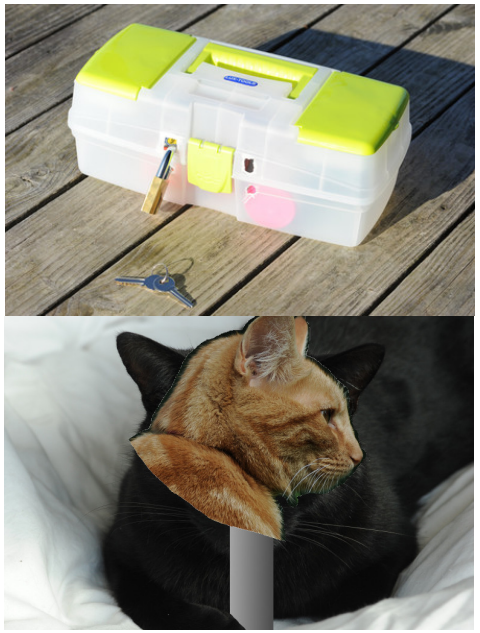
Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

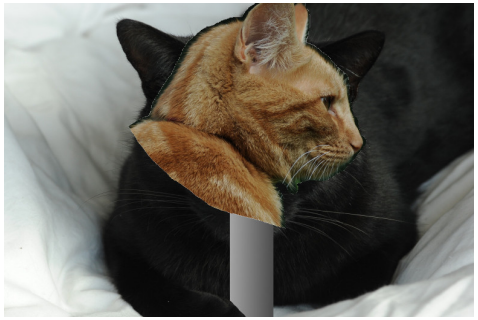
Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

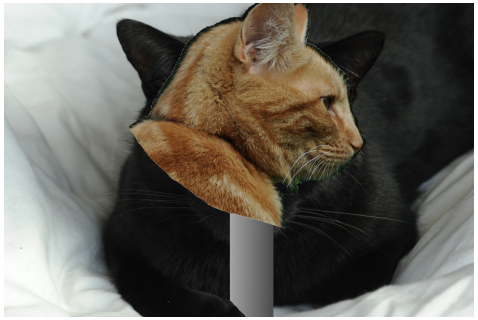


Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

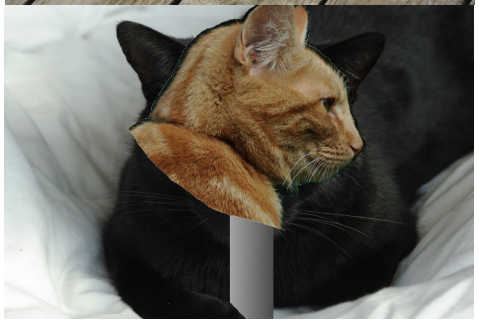
Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?



Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Ist Kitti wirklich Kitti? Und ist Mauki wirklich Mauki?

Was wir heute behandeln

Worauf basieren moderne Geheimschriften?

Moderne Kryptographie

... basiert z.B. auf der Schwierigkeit der Primfaktorzerlegung:

Einfach:

$$7 \cdot 13 = 91$$

Schwierig:

$$91 = ? \cdot ?$$

Moderne Kryptographie

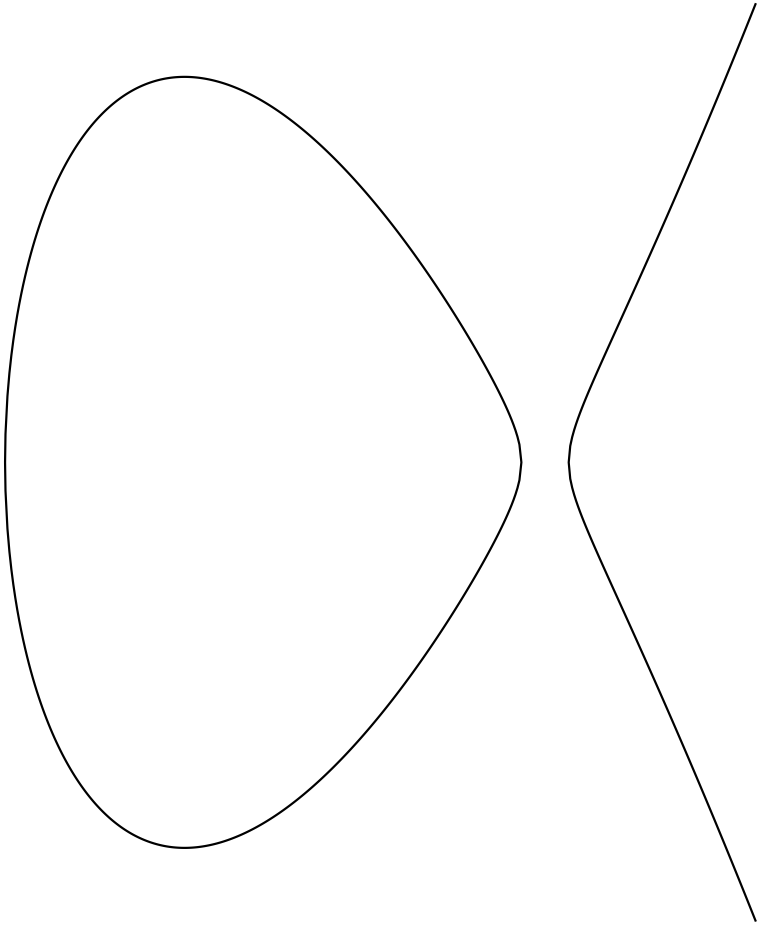
... basiert z.B. auf der Schwierigkeit der Primfaktorzerlegung:

```
843909269053189866936462039774305437477980443002358409691215680259217015429540
859919668456572519546489103100139671946391418403972866830909474935017344000640
049333014502324792586579106172804930824483360429355968708766507349129256049 3
755605646457455987231026092246466243109962365431843218994792552588895754283 13
350616941366347039547072726554243696138000476056961965561699990742741248615 66
864213192786617211771777700044505393730225689985403934179801803437997906499 79
868315097412907814923337791402964878208199691524567966193051102578468231449 50
608505156820978704752196867620605937987753425952418990021355878139828567778 84
825504319537047975156044027118128770411670132084782637383212793738123044856 51
021366935117354062590292011454550057828388637070344840848745727192687864107 04
008910836774920859135440214795673734439683464815763258070572365607153498759 06
377659125406822332723105330187326712682341643283373133039158351438641986235 41
517112534015351034839913940559057213885080032094681138949726322312000425808 94
727867947558749649186111660936158758266431390684347021047185964061179932405 86
096243323782747888126418867072941586164004172516403183964554975461688354357 99
086613093123296838038660283519573664383985590639337588256094985904103482238 93
```

Produkt von zwei grossen Primzahlen mit 1233 Dezimalstellen!

Moderne Kryptographie

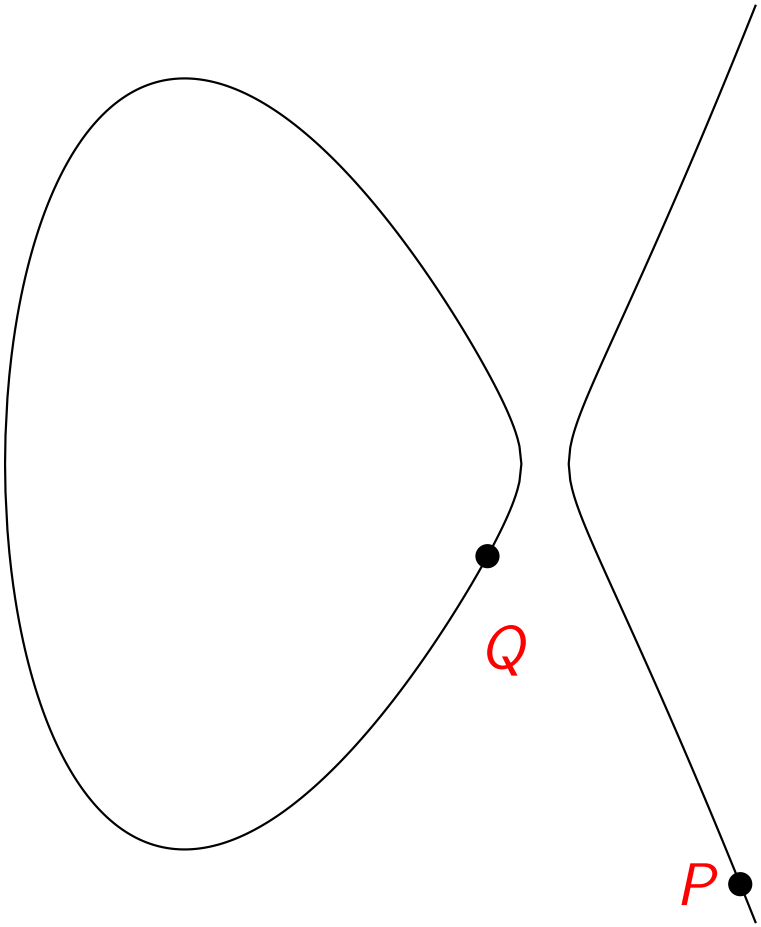
... basiert z.B. auf elliptischen Kurven: $y^2 = x^3 + Ax + B$



Hier kann man Punkte „addieren“!

Moderne Kryptographie

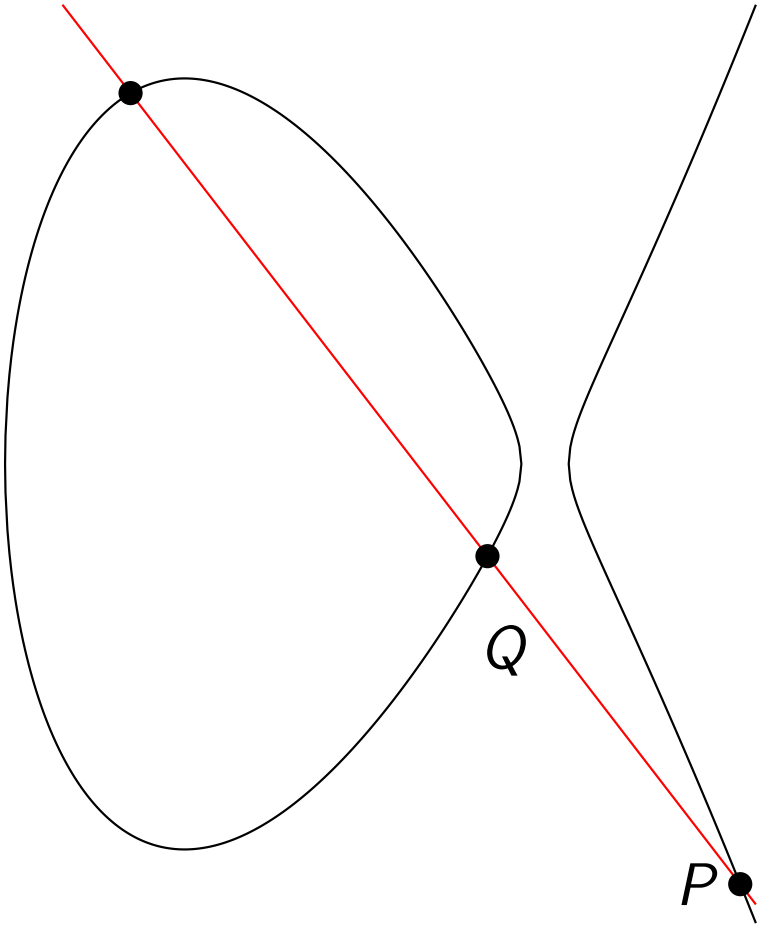
... basiert z.B. auf elliptischen Kurven: $y^2 = x^3 + Ax + B$



Hier kann man Punkte „addieren“!

Moderne Kryptographie

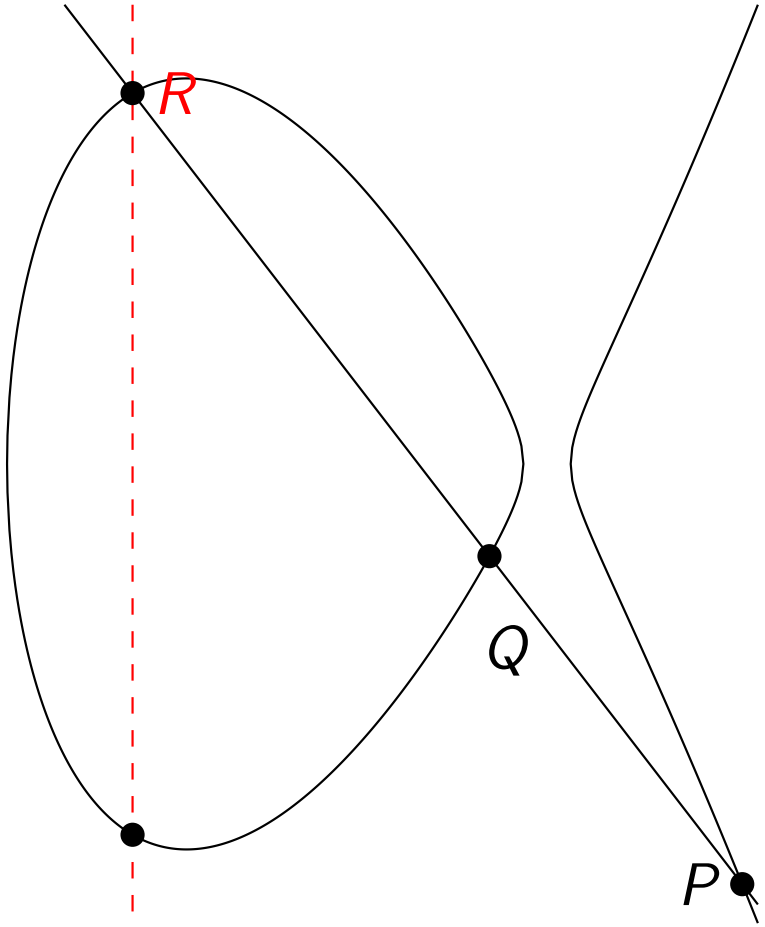
... basiert z.B. auf elliptischen Kurven: $y^2 = x^3 + Ax + B$



Hier kann man Punkte „addieren“!

Moderne Kryptographie

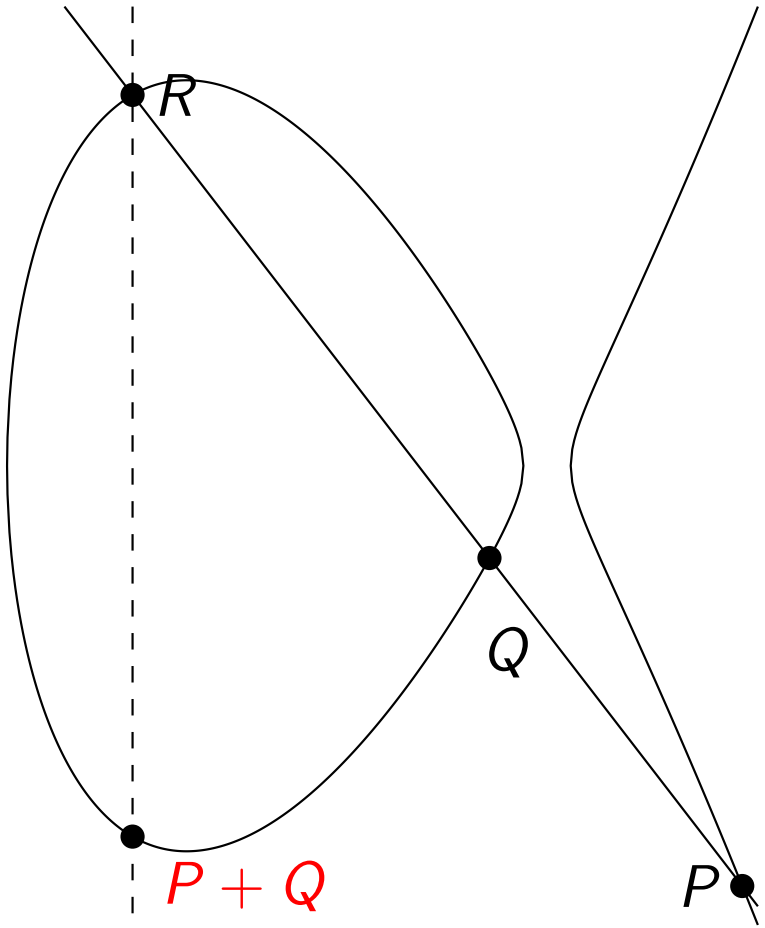
... basiert z.B. auf elliptischen Kurven: $y^2 = x^3 + Ax + B$



Hier kann man Punkte „addieren“!

Moderne Kryptographie

... basiert z.B. auf elliptischen Kurven: $y^2 = x^3 + Ax + B$



Hier kann man Punkte „addieren“!

?