Lauschen zwecklos!

Anna Pippich und Reinhard Racke

Universität Konstanz

WARUM GEHEIM?

- Kriegsstrategien

WARUM GEHEIM?

- Kriegsstrategien
- Zettel bei der Klassenarbeit

WARUM GEHEIM?

- Kriegsstrategien
- Zettel bei der Klassenarbeit
- Trainertaktik beim Fußballspiel

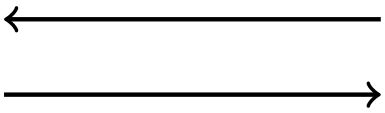
WARUM GEHEIM?

- Kriegsstrategien
- Zettel bei der Klassenarbeit
- Trainertaktik beim Fußballspiel
- Spionage: Entdeckung, Durchführung

WARUM GEHEIM?

- Kriegsstrategien
- Zettel bei der Klassenarbeit
- Trainertaktik beim Fußballspiel
- Spionage: Entdeckung, Durchführung
- ...

. . . SICHER KOMMUNIZIEREN!?



- Email
- Online-Banking
- Internetdienste
- . . .

VERBERGEN

- Spezialtinte wie etwa Zitronensaft

VERBERGEN

- Spezialtinte wie etwa Zitronensaft
- In einem Bild: kurze und lange Grashalme nach dem Morse-Alphabet

VERBERGEN

- Spezialtinte wie etwa Zitronensaft
- In einem Bild: kurze und lange Grashalme
  nach dem Morse-Alphabet
- In anderem Text: Beispiel „heute ist schulfrei“
  als jeweils dritten Buchstaben:

  bzhhrejuuevthfeloisvsgrtmjseecdvhyauokldgfhjrmvehbix

VERSCHLÜSSELN

KLARTEXT

Verschlüsseln →

← Entschlüsseln

GEHEIMTEXT

Eigentliche Nachricht, der Klartext, wird mittels eines Verfahrens, das einen Schlüssel benötigt, in einen Geheimtext übersetzt. Zum Entschlüsseln benötigt man den richtigen Schlüssel.

KEIN LATEIN, ABER GEHEIM!

Caesar

HEI 9IO NUK! OHL K1R

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

H			
E			
I			
9			

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

H	I		
E	O		
I	N		
9	U		

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

H	I	K	
E	O	!	
I	N	O	
9	U	H	

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

H	I	K	L
E	O	!	K
I	N	O	1
9	U	H	R

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUK! OHL K1R

H	I	K	L
E	O	!	K
I	N	O	1
9	U	H	R

HI KLEO! KINO 19 UHR

SENDEN DER GEHEIMBOTSCHAFT

Gutzufus und Stopdenbus

HEI 9IO NUKM AHL AUR

H	I	K	L
E	O	M	A
I	N	A	U
9	U	H	R

. . . EINE NACHRICHT VON CAESAR!

Kleopatra

HI KLEO MAINAU 9 UHR

???

SICHERHEIT

Verschlüsseln

KLARTEXT → GEHEIMTEXT

KLARTEXT ← GEHEIMTEXT

Entschlüsseln

SICHERHEIT HÄNGT VON SCHLÜSSEL AB!

KRYPTOLOGIE

Kryptographie: Die Wissenschaft von der Verschlüsselung einer Nachricht oder der Verschleierung ihres Inhalts.

Kryptoanalyse: Die Wissenschaft von der Erschließung des Klartextes aus dem Geheimtext ohne Kenntnis des Schlüssels.

Symmetrische Verschlüsselungsverfahren

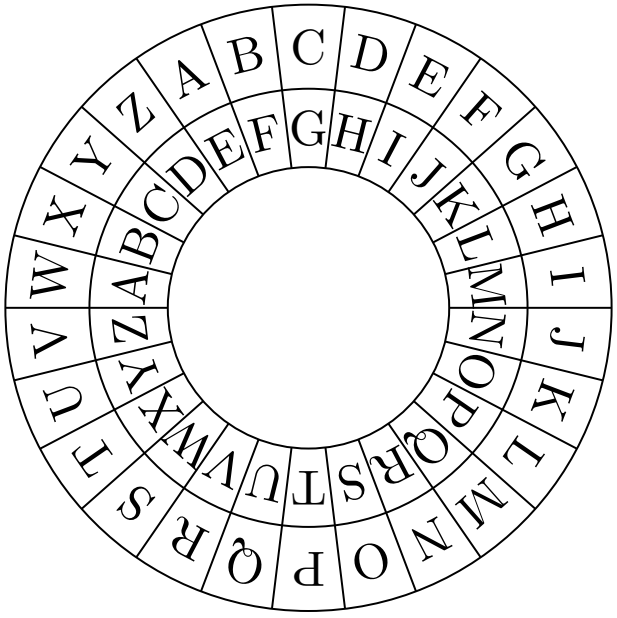
Bei symmetrischen Verschlüsselungsverfahren sind die Schlüssel zum Ver- und Entschlüsseln im Wesentlichen identisch.

z.B. Klartextbuchstaben nach einer eindeutig umkehrbaren Vorschrift durch Geheimtextbuchstaben ersetzen:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	...
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	

BEISPIEL: CAESAR-VERSCHIEBUNG

z.B. Caesar-Verschiebung um 4



Geheimtext:	K	I	L	I	M	Q	R	M	W

Klartext:	G	E	H	E	I	M	N	I	S

BUCHSTABENHÄUFIGKEITEN

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6,51%	n	9,78%
b	1,89%	o	2,51%
c	3,06%	p	0,79%
d	5,08%	q	0,02%
e	17,40%	r	7,00%
f	1,66%	s	7,27%
g	3,01%	t	6,15%
h	4,76%	u	4,35%
i	7,55%	v	0,67%
j	0,27%	w	1,89%
k	1,21%	x	0,03%
l	3,44%	y	0,04%
m	2,53%	z	1,13%

SICHERHEIT: CAESAR-VERSCHIEBUNG

- Caesar-Verschiebung einfaches, aber auch sehr unsicheres Verfahren (nur 25 verschiedene Schlüssel)

- Grundprinzip moderner Kryptographie:

> Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels, aber nicht von der Geheimhaltung des Verfahrens abhängen!

VIGENÈRE-VERSCHLÜSSELUNG

- Polyalphabetische Modifikation der Caesar-Verschiebung
- Zusätzliches Schlüsselwort bestimmt die Verschiebeanzahl nach Caesar

VIGENÈRE-VERSCHLÜSSELUNG

- Polyalphabetische Modifikation der Caesar-Verschiebung
- Zusätzliches Schlüsselwort bestimmt die Verschiebeanzahl nach Caesar
- Konvention: Buchstabe *A* entspricht keiner Verschiebung, Buchstabe *B* einer Verschiebung um 1, usw.

VIGENÈRE-VERSCHLÜSSELUNG

- Polyalphabetische Modifikation der Caesar-Verschiebung
- Zusätzliches Schlüsselwort bestimmt die Verschiebeanzahl nach Caesar
- Konvention: Buchstabe *A* entspricht keiner Verschiebung, Buchstabe *B* einer Verschiebung um 1, usw.

Beispiel: zusätzliches Schlüsselwort „BUCH“

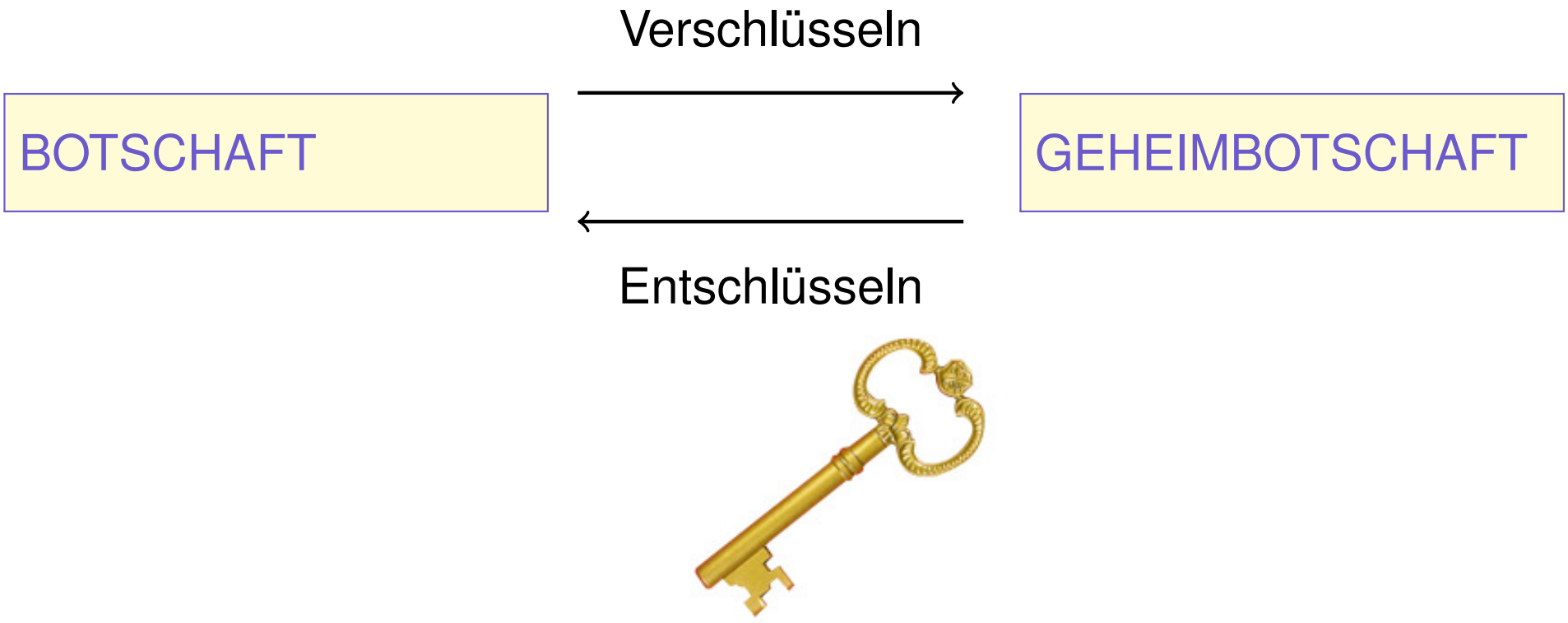
Alphabet wird für ersten zu verschlüsselnden Buchstaben um $1 = B$, dann um $20 = U$, $2 = C$, $7 = H$, dann wieder um 1, 20, 2, 7, usw. Stellen verschoben

Schlüssel:	B	U	C	H	B	U	C	H	B
Klartext:	G	E	H	E	I	M	N	I	S
Geheimtext:	H	Y	J	L	J	G	P	P	T

SICHERHEIT: VIGENÈRE-VERSCHLÜSSELUNG

- Verfahrens nur sicher, wenn das zusätzliche Schlüsselwort genauso lang ist, wie der Klartext, dieses aus einer Folge zufälliger, gleichverteilter Buchstaben besteht und jeweils nur einmal verwendet wird
- In der Praxis im Allgemeinen zu aufwendig!
- Variante eines polyalphabetischen Verschlüsselungsverfahrens: Enigma

ASYMMETRISCHES VERSCHLÜSSELN



- Verschlüsseln mit öffentlichem Schlüssel
- Entschlüsseln mit geheimen Schlüssel
- Aber: geheimer Schlüssel unmöglich aus öffentlichem Schlüssel abzuleiten!

FRAGE

Gibt es eine Verschlüsselungsfunktion so, dass

- das Verschlüsseln (mit öffentlichen Schlüssel) einfach möglich ist,

FRAGE

Gibt es eine Verschlüsselungsfunktion so, dass

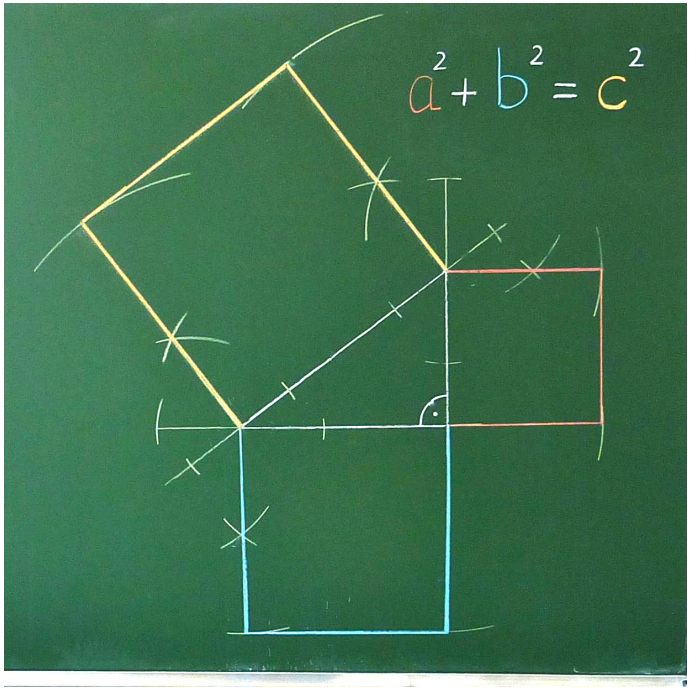
- das Verschlüsseln (mit öffentlichen Schlüssel) einfach möglich ist,
- das Entschlüsseln für einen Angreifer ohne Zusatzinformation unmöglich, d.h. in keiner adäquaten Zeit praktisch durchführbar ist,

FRAGE

Gibt es eine Verschlüsselungsfunktion so, dass

- das Verschlüsseln (mit öffentlichen Schlüssel) einfach möglich ist,
- das Entschlüsseln für einen Angreifer ohne Zusatzinformation unmöglich, d.h. in keiner adäquaten Zeit praktisch durchführbar ist,
- das Entschlüsseln für den Empfänger mit Hilfe des geheimen Schlüssels einfach möglich ist?

FRAGEN WIR DEN ZAHLENTHEORETIKER . . .



Plusminus

Wie kann man heutzutage sicher verschlüsseln?

MODULO-RECHNEN

Schreibweise:

$$a = b \bmod n,$$

wenn a und b nach Division durch n den gleichen Rest lassen.

z.B.:

$$9 + 7 = 4 \bmod 12$$

MODULO-RECHNEN

Schreibweise:

$$a = b \bmod n,$$

wenn a und b nach Division durch n den gleichen Rest lassen.

z.B.:

$$9 + 7 = 4 \bmod 12$$

Vorteile

- Menge der Reste endlich:

  $$r = 0, 1, \ldots, n - 1$$

  $\Longrightarrow$ Computer-tauglich
- Rechnen mit Resten wie gewohnt: Modulo-Rechnen

MODULO-RECHNEN

Schreibweise:

$$a = b \bmod n,$$

wenn a und b nach Division durch n den gleichen Rest lassen.

z.B.:

$$9 + 7 = 4 \bmod 12$$

Vorteile

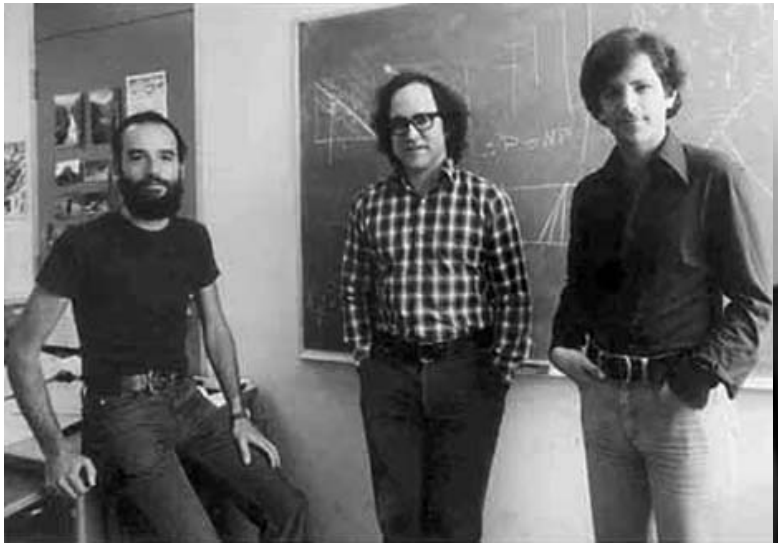
- Menge der Reste endlich:

  $$r = 0, 1, \ldots, n - 1$$

  $\Longrightarrow$ Computer-tauglich
- Rechnen mit Resten wie gewohnt: Modulo-Rechnen
- z.B.: $98^7 = 2^7 = 2^4 \cdot 2^3 = 16 \cdot 8 = 4 \cdot 8 = 32 = 8 \bmod 12$.

RSA-VERFAHREN

- erfunden 1977
- eines der ersten Public-Key Kryptosysteme
- benutzt asymmetrischen Schlüssel, d.h. Schlüssel zum Verschlüsseln ist öffentlich, Schlüssel zum Entschlüsseln bleibt geheim



Ron Rivest (1947–), Adi Shamir (1952–), Leonard Adleman (1945–)

ASCII-CODE

American Standard Code for Information Interchange

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100				

ASCII-CODE

American Standard Code for Information Interchange

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100				

- HI
  72,73
- HI KLEO! KINO 20 UHR
  72, 73, 75, 76, 69, 79, 33, 75, 73, 78, 79, 50, 48, 85, 72, 82

RSA-VERFAHREN

ÖFFENTLICH

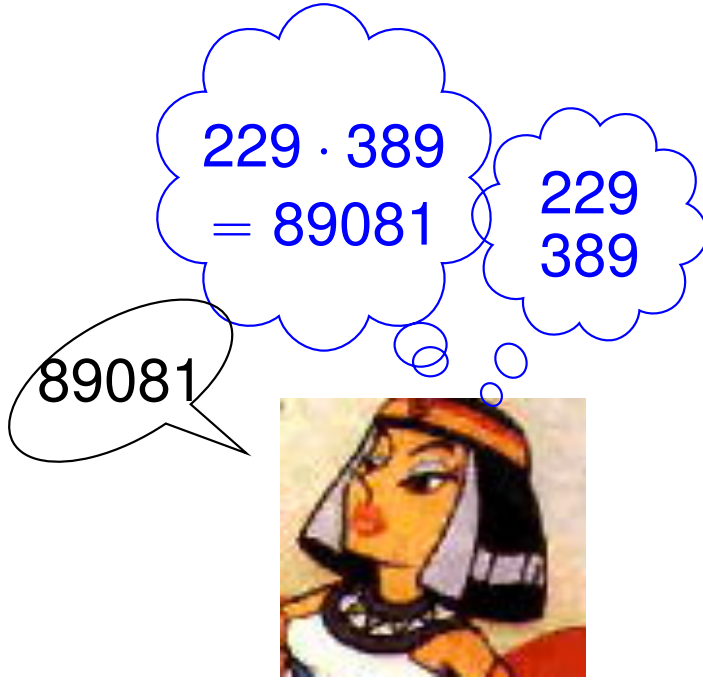
RSA-VERFAHREN

ÖFFENTLICH

RSA-VERFAHREN

ÖFFENTLICH

$m = 89081$

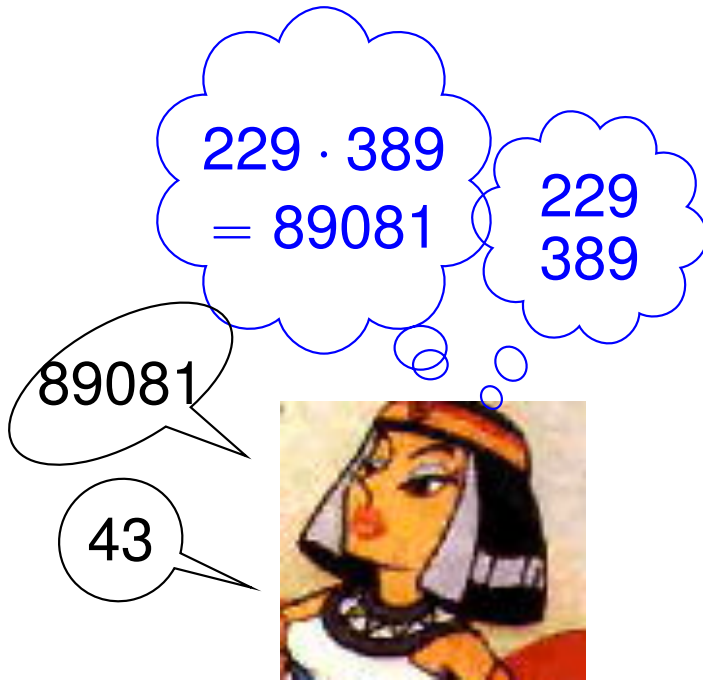


RSA-VERFAHREN

ÖFFENTLICH

$$m = 89081$$

$$k = 43$$

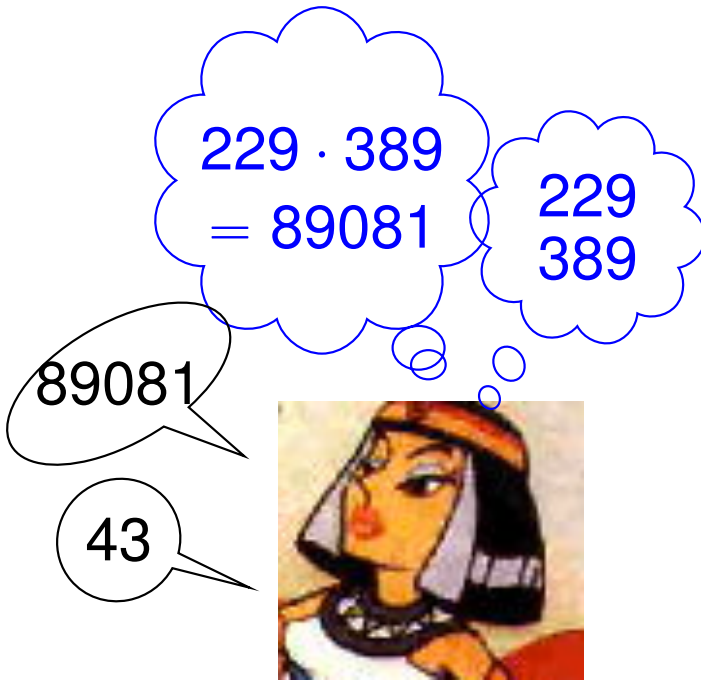


RSA-VERFAHREN

ÖFFENTLICH

$$m = 89081$$

$$k = 43$$

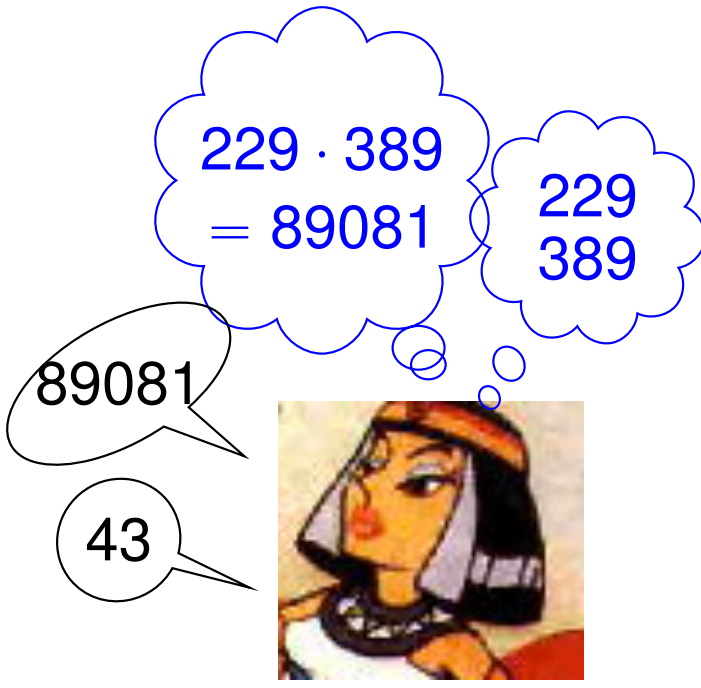


RSA-VERFAHREN

ÖFFENTLICH

$m = 89081$

$k = 43$



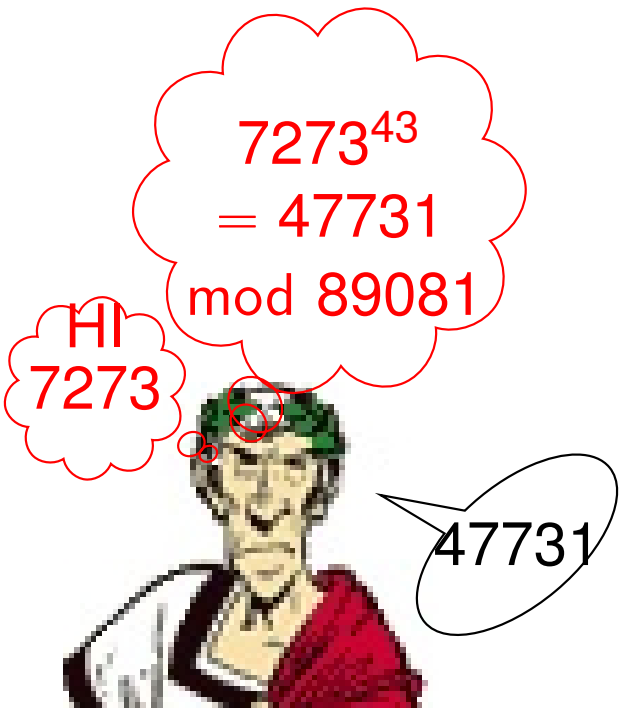
RSA-VERFAHREN

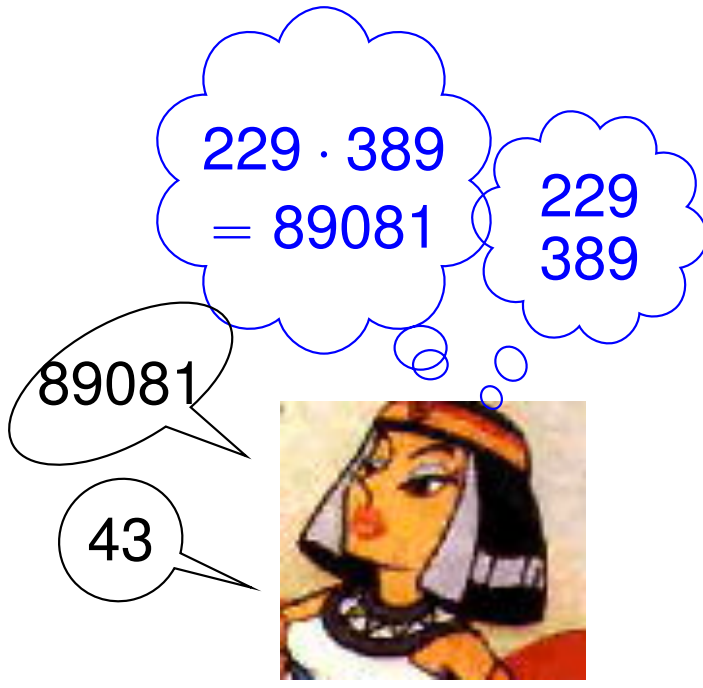
ÖFFENTLICH

$m = 89081$

$k = 43$

Nachricht: 47731





GEHEIME ENTSCHLÜSSELUNGS-ZAHL

$p := 229$, $q := 389$ (geheim)

$m = p \cdot q = 89081$ (öffentlich)

$k = 43$ (öffentlich)

Kleopatra rechnet:

GEHEIME ENTSCHLÜSSELUNGS-ZAHL

$p := 229$, $q := 389$ (geheim)

$m = p \cdot q = 89081$ (öffentlich)

$k = 43$ (öffentlich)

Kleopatra rechnet:

(1) $(p-1) \cdot (q-1) = 228 \cdot 388 = 88464$ (geheim!)

GEHEIME ENTSCHLÜSSELUNGS-ZAHL

$p := 229$, $q := 389$ (geheim)

$m = p \cdot q = 89081$ (öffentlich)

$k = 43$ (öffentlich)

Kleopatra rechnet:

(1) $(p-1) \cdot (q-1) = 228 \cdot 388 = 88464$ (geheim!)

(2) Bestimme x mit $43 \cdot x = 1 \bmod 88464$!

GEHEIME ENTSCHLÜSSELUNGS-ZAHL

$p := 229$, $q := 389$ (geheim)

$m = p \cdot q = 89081$ (öffentlich)

$k = 43$ (öffentlich)

Kleopatra rechnet:

(1) $(p-1) \cdot (q-1) = 228 \cdot 388 = 88464$ (geheim!)

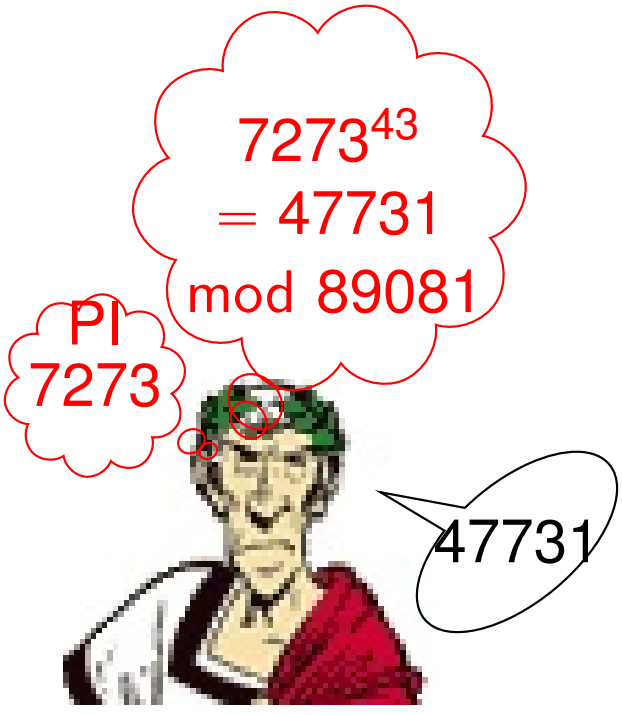
(2) Bestimme x mit $43 \cdot x = 1 \bmod 88464$!

- Ergebnis:

$$x = 67891$$

(geheime!) Entschlüsselungs-Zahl!

RSA-VERFAHREN

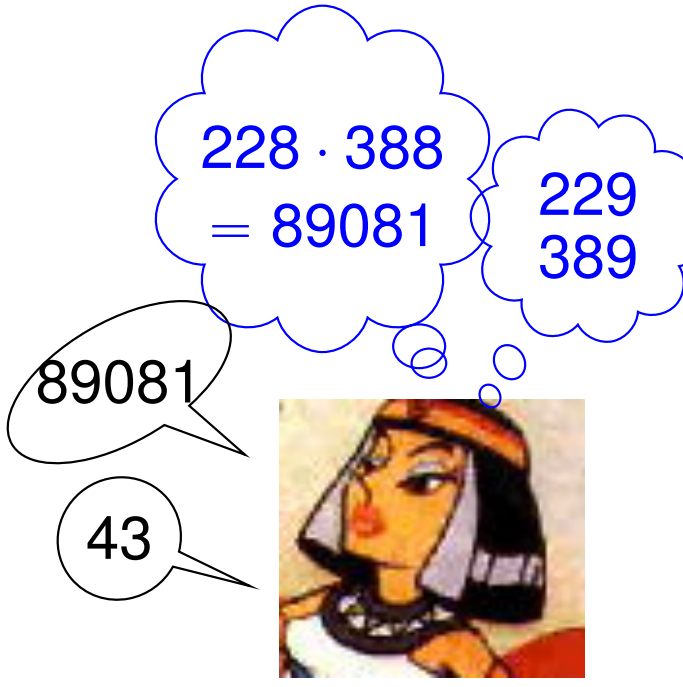


ÖFFENTLICH

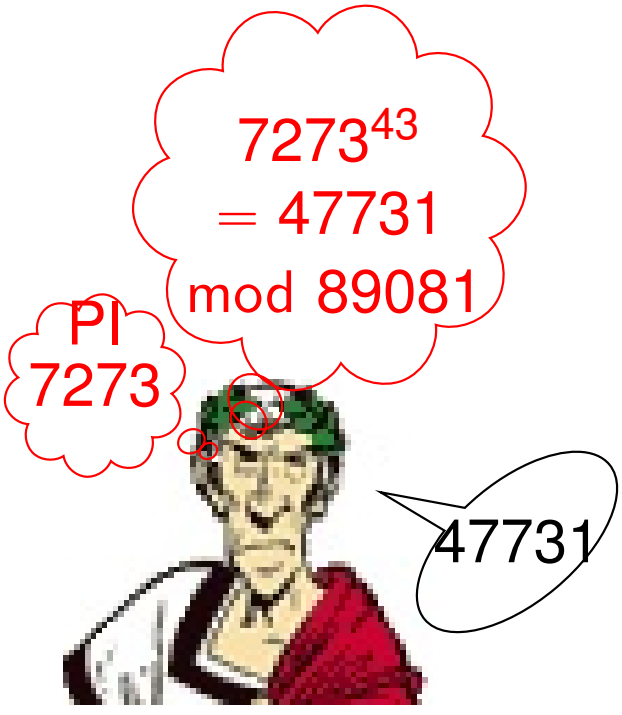
$m = 89081$

$k = 43$

Nachricht: 47731



RSA-VERFAHREN

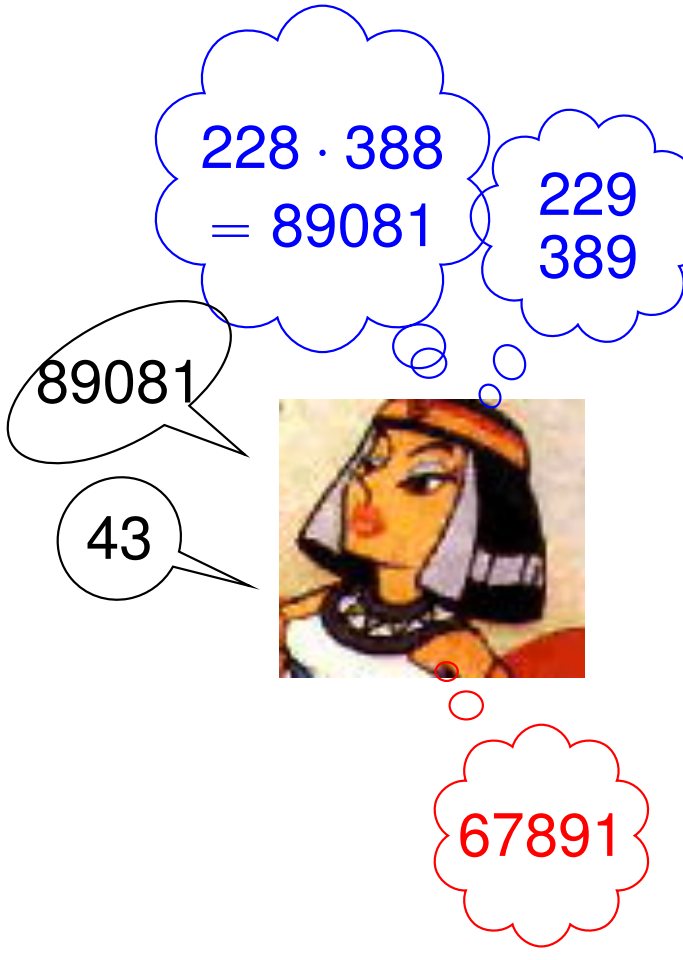


ÖFFENTLICH

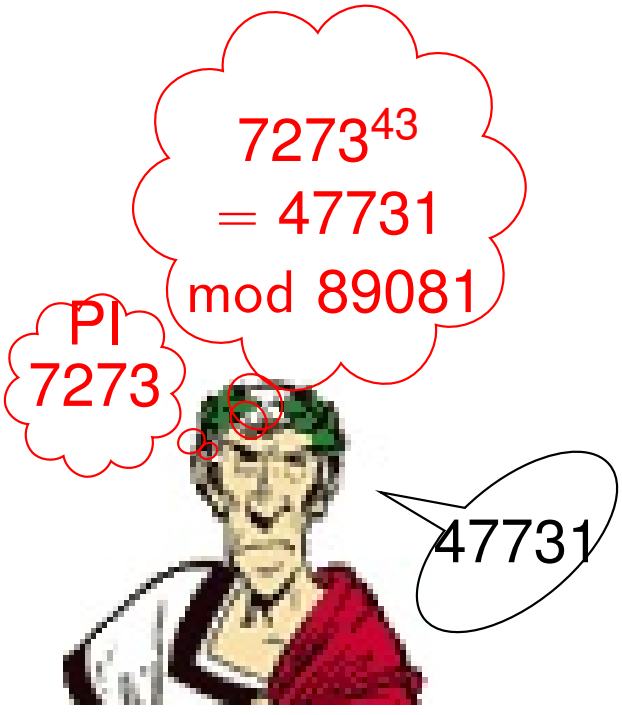
$m = 89081$

$k = 43$

Nachricht: 47731



RSA-VERFAHREN

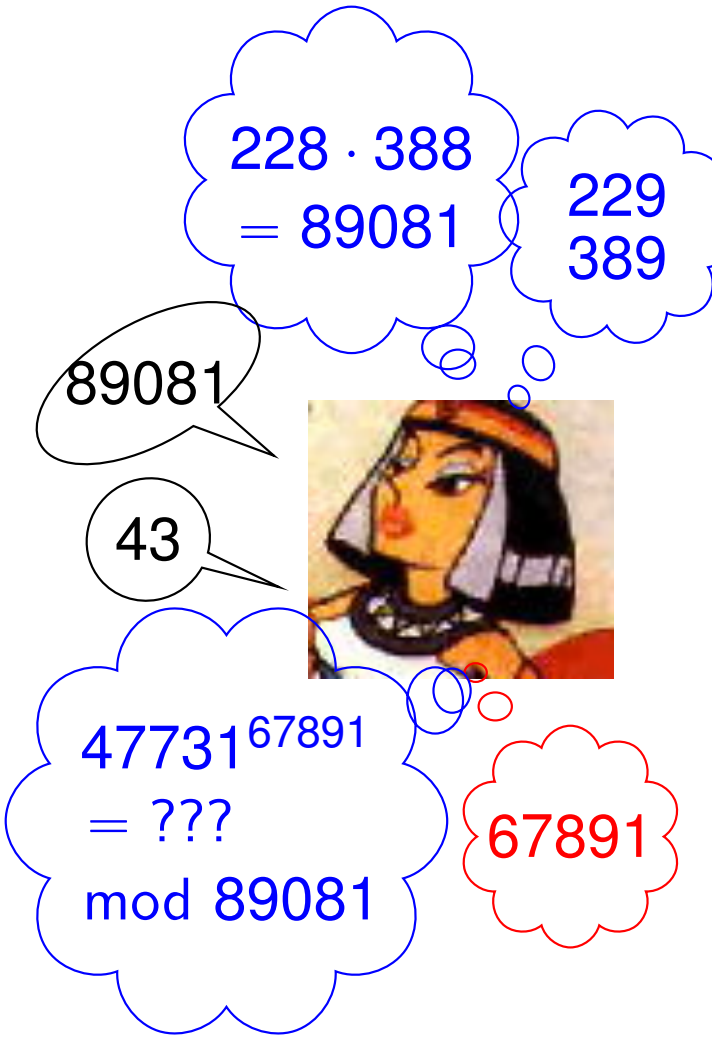


ÖFFENTLICH

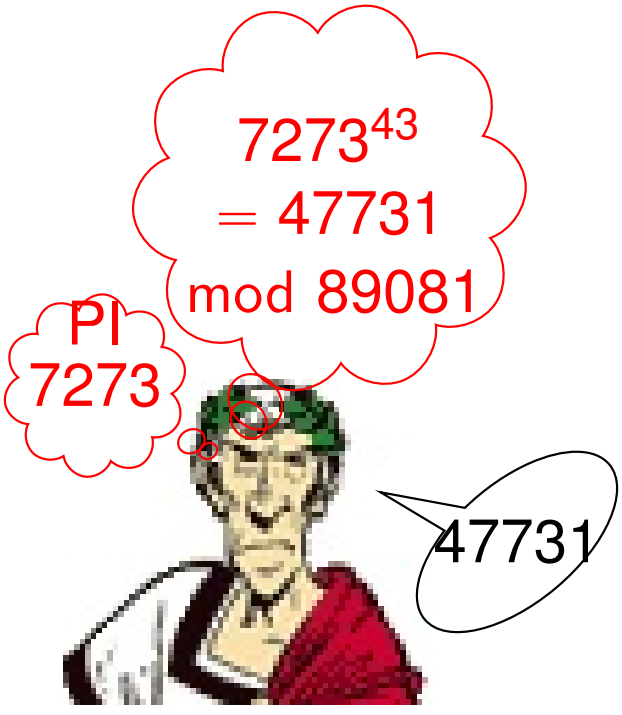
$m = 89081$

$k = 43$

Nachricht: 47731



RSA-VERFAHREN

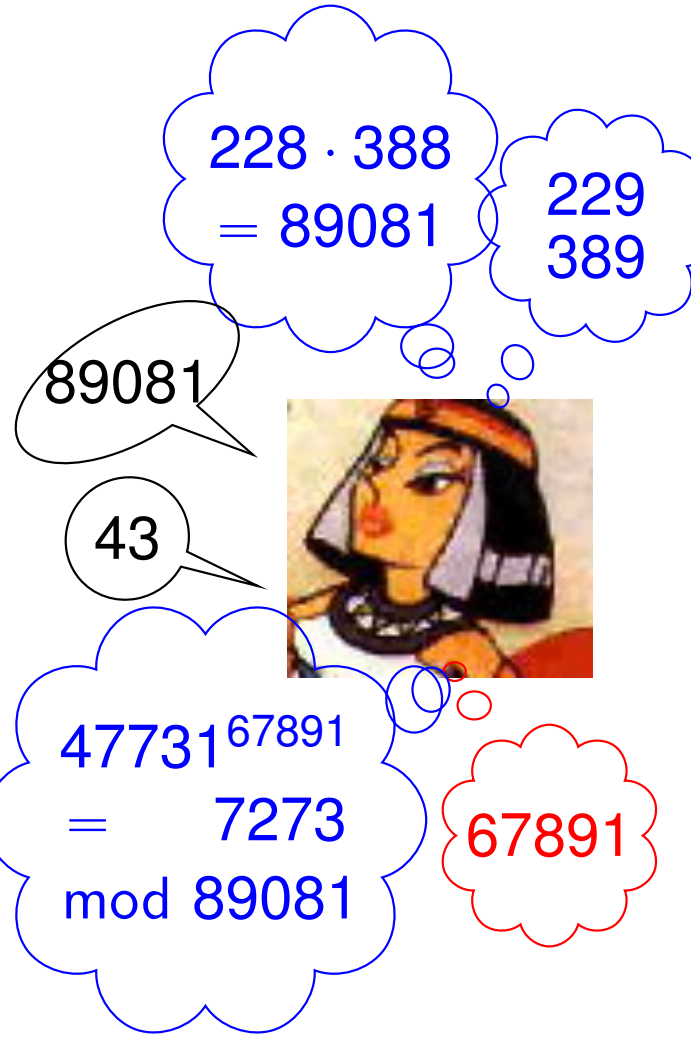


ÖFFENTLICH

$m = 89081$

$k = 43$

Nachricht: 47731



SICHERHEIT: RSA

- Öffentlicher Schlüssel zum Verschlüsseln: $(m = 89081, k = 43)$
- Geheimer Schlüssel zum Entschlüsseln: $x = 67891$
  Brauche $(p-1)\cdot(q-1)$ zum Berechnen von x, d.h. die Primfaktoren p und q von m!

SICHERHEIT: RSA

- Öffentlicher Schlüssel zum Verschlüsseln: $(m = 89081, k = 43)$
- Geheimer Schlüssel zum Entschlüsseln: $x = 67891$
  Brauche $(p-1)\cdot(q-1)$ zum Berechnen von x, d.h. die Primfaktoren p und q von m!

Heutzutage(!) sehr schwierig/unmöglich (für Computer):

- m ist das Produkt zweier großer Primfaktoren p, q (heutzutage 300-stellig)
- Primfaktoren von m bestimmen: p, q ?

SICHERHEIT: RSA

- Öffentlicher Schlüssel zum Verschlüsseln: $(m = 89081, k = 43)$
- Geheimer Schlüssel zum Entschlüsseln: $x = 67891$
  Brauche $(p-1)\cdot(q-1)$ zum Berechnen von x, d.h. die Primfaktoren p und q von m!

Heutzutage(!) sehr schwierig/unmöglich (für Computer):

- m ist das Produkt zweier großer Primfaktoren p, q (heutzutage 300-stellig)
- Primfaktoren von m bestimmen: p, q ?

Die Sicherheit von RSA beruht auf Faktorisierungsproblem!

EIN REALISTISCHERES BEISPIEL

Empfänger B (Kleopatra) wählt die Primzahlen

$$p = 153249554086588885835834702715030918361873935752883763 3,$$

$$q = 153249554086588885835834702715030918361897446794836651 3,$$

berechnet (geheim)

$$(p-1)(q-1) = 234854258277383322788948059678933702737604357590890678840660716359774775359774775655274689263398074873348682847417958 4$$

und gibt folgenden öffentlichen Schlüssel bekannt:

$$k = 43$$

$$m = p \cdot q = 234854258277383322788948059678933702737604357590890679147159824532952547326944094693459911597120065395138372 9$$

EIN REALISTISCHERES BEISPIEL

Absender A (Caesar) transkribiert seine Nachricht mit ASCII-CODE als

$$a = 72737576697933757378795048857282$$

und übermittelt die verschlüsselte Nachricht

$$b = a^{43} = 26813938939096546944108886368459521627439793755540819218258228214554234381355214245969232791647169454219670 7 \bmod m$$

Empfänger B bestimmt geheimen Schlüssel

$$x = 491555424301499977930356403979163563869404469376282816178127080753016972301737721714088993920962359448084$$

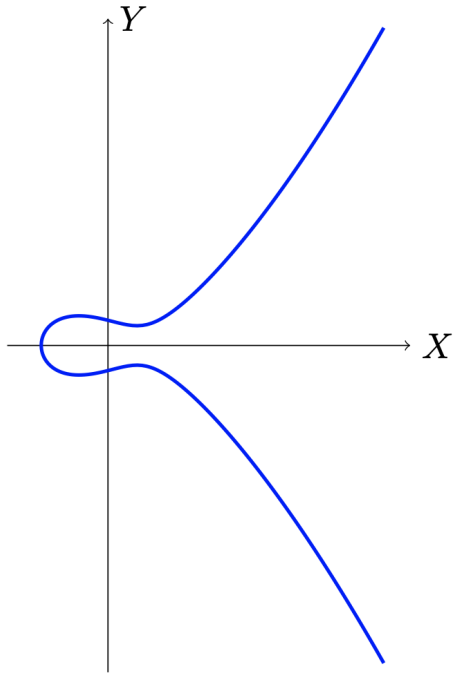
Empfänger B entschlüsselt die Nachricht, indem er $b^x \bmod m$ bestimmt, und erhält

$$b^x = a = 72737576697933757378795048857282 \bmod m$$

. . . IN ZUKUNFT?

Heutzutage:

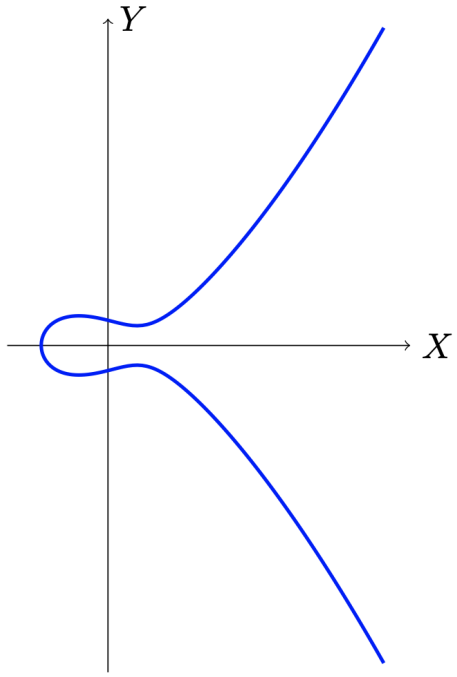
- Meist asymmetrische Verschlüsselungs-verfahren, die elliptische Kurven verwenden
- Sicherheit beruht auf Analogon des Faktorisierungsproblems
- Größere Sicherheit bei weniger Speicherbedarf!



. . . IN ZUKUNFT?

Heutzutage:

- Meist asymmetrische Verschlüsselungs-verfahren, die elliptische Kurven verwenden
- Sicherheit beruht auf Analogon des Faktorisierungsproblems
- Größere Sicherheit bei weniger Speicherbedarf!



In Zukunft: . . . Post-Quantum-Kryptographie!?

VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

ENTSCHLÜSSELUNG FUNKTIONIERT

Wir wissen

(1) $7273^{43} = 47731 \mod 89081$

(2) $43 \cdot 67891 = 88464 \cdot 33 + 1$

ENTSCHLÜSSELUNG FUNKTIONIERT

Wir wissen

(1) $7273^{43} = 47731 \mod 89081$

(2) $43 \cdot 67891 = 88464 \cdot 33 + 1$

Wir rechnen

$$47731^{67891} \underset{(1)}{=} 7273^{43 \cdot 67891} \underset{(2)}{=} 7273^{88464 \cdot 33 + 1} \mod 89081$$

ENTSCHLÜSSELUNG FUNKTIONIERT

Wir wissen

(1) $7273^{43} = 47731 \mod 89081$

(2) $43 \cdot 67891 = 88464 \cdot 33 + 1$

Wir rechnen

$$47731^{67891} \underset{(1)}{=} 7273^{43 \cdot 67891} \underset{(2)}{=} 7273^{88464 \cdot 33 + 1} \mod 89081$$

Zwischenschritt (Satz von Euler für $p = 229$, $q = 389$)

$$7273^{88464 \cdot 33} = (7273^{33})^{88464} = (7273^{33})^{(p-1)(q-1)} = 1 \mod 89081$$

ENTSCHLÜSSELUNG FUNKTIONIERT

Wir wissen

(1) $7273^{43} = 47731 \mod 89081$

(2) $43 \cdot 67891 = 88464 \cdot 33 + 1$

Wir rechnen

$$47731^{67891} \underset{(1)}{=} 7273^{43 \cdot 67891} \underset{(2)}{=} 7273^{88464 \cdot 33 + 1} \mod 89081$$

Zwischenschritt (Satz von Euler für $p = 229$, $q = 389$)

$$7273^{88464 \cdot 33} = (7273^{33})^{88464} = (7273^{33})^{(p-1)(q-1)} = 1 \mod 89081$$

Damit insgesamt

$$\begin{aligned} 47731^{67891} &= 7273^{88464 \cdot 33 + 1} = 7273^{88464 \cdot 33} \cdot 7273 = 1 \cdot 7273 \\ &= 7273 \mod 89081 \end{aligned}$$