Von der Enigma zum elektronischen Personalausweis

Die Mathematik der Kryptographie

Ulrich Görtz

Science Pub Stuttgart, 14.3.2016

UNIVERSITÄT DUISBURG ESSEN

Essener Seminar für Algebraische Geometrie und Arithmetik

Science Pub Quiz

Frage

Welcher Wochentag ist in 699 Tagen?

Science Pub Quiz

Frage

Welcher Wochentag ist in 699 *Tagen?*

(A) Samstag

(B) Sonntag

(C) Montag

(D) Dienstag

Science Pub Quiz

Frage

Welcher Wochentag ist in 699 Tagen?

(B) Sonntag

(D) Dienstag

Science Pub Quiz

Frage

Welcher Wochentag ist in 699 Tagen?

(B) Sonntag

(D) Dienstag

Science Pub Quiz

Frage

Wie lange dauert es, auf einem handelsüblichen Computer eine Primzahl mit 1200 *Stellen zu finden?*

Science Pub Quiz

Frage

Wie lange dauert es, auf einem handelsüblichen Computer eine Primzahl mit 1200 *Stellen zu finden?*

(A) einige Mikrosekunden

(B) einige Sekunden

(C) einige Minuten

(D) einige Stunden

Science Pub Quiz

Frage

Wie lange dauert es, auf einem handelsüblichen Computer eine Primzahl mit 1200 Stellen zu finden?

(A) einige Mikrosekunden

(B) einige Sekunden

(C) einige Minuten

Science Pub Quiz

Frage

Wie lange dauert es, auf einem handelsüblichen Computer eine Primzahl mit 1200 Stellen zu finden?

(A) einige Mikrosekunden

(B) einige Sekunden

(C) einige Minuten

Science Pub Quiz

Frage

Wie lange dauert es in ungünstigen Fällen, auf einem handelsüblichen Computer die Primfaktorzerlegung einer Zahl mit 500 Stellen zu finden?

Science Pub Quiz

Frage

Wie lange dauert es in ungünstigen Fällen, auf einem handelsüblichen Computer die Primfaktorzerlegung einer Zahl mit 500 Stellen zu finden?

(A) einige Stunden

(B) einige Tage

(C) einige Jahre

(D) einige Tausend Jahre

Science Pub Quiz

Frage

Wie lange dauert es in ungünstigen Fällen, auf einem handelsüblichen Computer die Primfaktorzerlegung einer Zahl mit 500 Stellen zu finden?

(B) einige Tage

(D) einige Tausend Jahre

Science Pub Quiz

Frage

Wie lange dauert es in ungünstigen Fällen, auf einem handelsüblichen Computer die Primfaktorzerlegung einer Zahl mit 500 Stellen zu finden?

(B) einige Tage

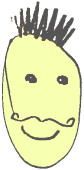
(D) einige Tausend Jahre

Grundlegendes Ziel

Übermittle eine Nachricht so, dass ein Außenstehender sie nicht entschlüsseln kann.

Grundlegendes Ziel

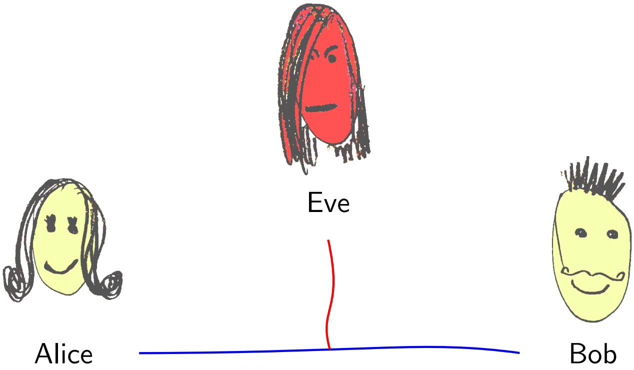
Übermittle eine Nachricht so, dass ein Außenstehender sie nicht entschlüsseln kann.

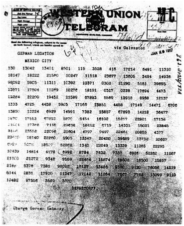


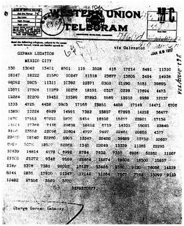
Alice Bob

Grundlegendes Ziel

Übermittle eine Nachricht so, dass ein Außenstehender sie nicht entschlüsseln kann.




WESTERN UNION
TELEGRAM
via Galveston
GERMAN LEGATION
MEXICO CITY
BERNSTORFF


WESTERN UNION
TELEGRAM

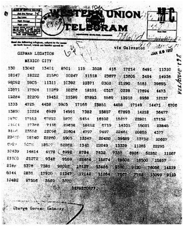
via Galveston
JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
[illegible] 17553 67893 5870 5454 16102 15217 22801 17138
[illegible] 17388 7446 23638 18222 6719 14331 15021 23845
[illegible] 23552 22096 21604 4797 9497 22464 20855 4377
[illegible] 18140 22260 5905 13347 20420 39689 13732 20667
[illegible] 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
[illegible] 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

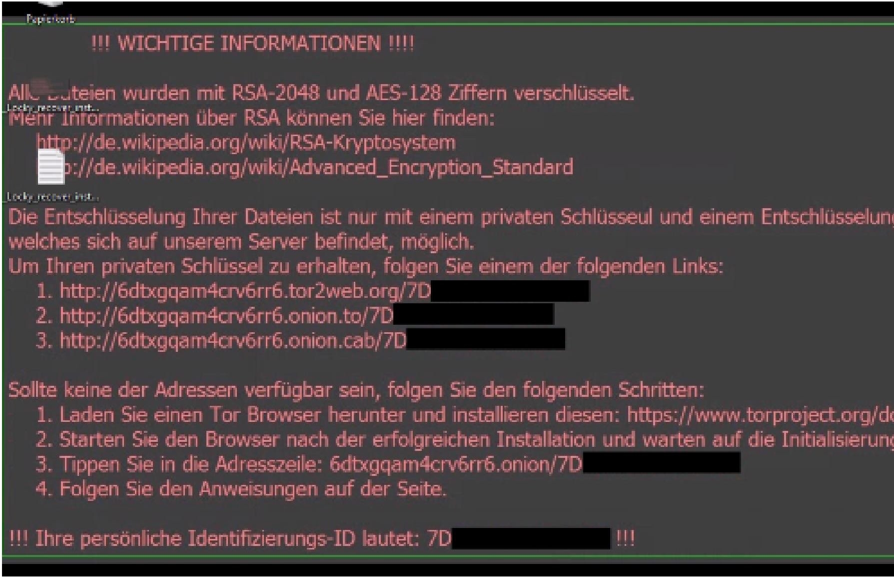
BERNSTORFF.

Charge German Embassy.



Bilder: Wikipedia. Zimmermann-Telegramm: Gemeinfrei; Enigma: CC BY-SA Benutzer: JochenF u.a.; Personalausweis: Gemeinfrei.

Locky


Papierkorb
!!! WICHTIGE INFORMATIONEN !!!!
Alle Dateien wurden mit RSA-2048 und AES-128 Ziffern verschlüsselt.
Locky_recover_inst...
Mehr Informationen über RSA können Sie hier finden:
http://de.wikipedia.org/wiki/RSA-Kryptosystem
p://de.wikipedia.org/wiki/Advanced_Encryption_Standard
Locky_recover_inst...
Die Entschlüsselung Ihrer Dateien ist nur mit einem privaten Schlüsseul und einem Entschlüsselun
welches sich auf unserem Server befindet, möglich.
Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:
1. http://6dtxgqam4crv6rr6.tor2web.org/7D[redacted]
2. http://6dtxgqam4crv6rr6.onion.to/7D[redacted]
3. http://6dtxgqam4crv6rr6.onion.cab/7D[redacted]
Sollte keine der Adressen verfügbar sein, folgen Sie den folgenden Schritten:
1. Laden Sie einen Tor Browser herunter und installieren diesen: https://www.torproject.org/d
2. Starten Sie den Browser nach der erfolgreichen Installation und warten auf die Initialisierun
3. Tippen Sie in die Adresszeile: 6dtxgqam4crv6rr6.onion/7D[redacted]
4. Folgen Sie den Anweisungen auf der Seite.
!!! Ihre persönliche Identifizierungs-ID lautet: 7D[redacted] !!!

Monoalphabetische Verschlüsselung: Jeder Buchstabe wird durch einen anderen Buchstaben ersetzt, und zwar immer durch denselben.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	$\ldots$
F	R	Z	E	G	A	U	B	C	K	O	S	D	X	I	$\ldots$

Monoalphabetische Verschlüsselung: Jeder Buchstabe wird durch einen anderen Buchstaben ersetzt, und zwar immer durch denselben.

$$\begin{array}{cccccccccccccccc} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & \dots \\ F & R & Z & E & G & A & U & B & C & K & O & S & D & X & I & \dots \end{array}$$

Leicht zu knacken durch "Häufigkeitsanalyse".

Monoalphabetische Verschlüsselung: Jeder Buchstabe wird durch einen anderen Buchstaben ersetzt, und zwar immer durch denselben.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	$\dots$
F	R	Z	E	G	A	U	B	C	K	O	S	D	X	I	$\dots$

Leicht zu knacken durch "Häufigkeitsanalyse".

Moderne Verfahren (computerbasiert): DES, AES. Dazu wird ein gemeinsamer "Schlüssel" vereinbart.

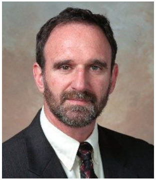
Public-Key-Kryptographie

Seit Mitte der 1970er Jahre wurden mehrere Verfahren erfunden, bei denen kein vorheriger Schlüsseltausch notwendig ist.

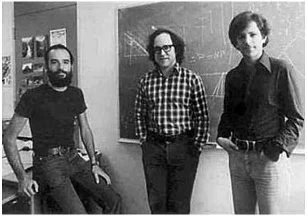
Public-Key-Kryptographie

Seit Mitte der 1970er Jahre wurden mehrere Verfahren erfunden, bei denen kein vorheriger Schlüsseltausch notwendig ist.

W. Diffie



M. Hellman



R. Rivest, A. Shamir, L. Adleman

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Sind p_1, p_2 große Primzahlen, so lässt sich das Produkt $N = p_1 p_2$ leicht berechnen ("schriftliche Multiplikation").

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Sind p_1, p_2 große Primzahlen, so lässt sich das Produkt $N = p_1 p_2$ leicht berechnen ("schriftliche Multiplikation").

Ist nur n bekannt, so sind die Primfaktoren p_1 und p_2 bestimmt ("eindeutige Primfaktorzerlegung"), aber in der Regel nicht leicht zu finden.

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Beispiel

$$257 \cdot 379 =$$

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Beispiel

$$257 \cdot 379 = 97403$$

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

Beispiel

$$257 \cdot 379 = 97403$$

Beispiel

$$95567 =$$

Grundprinzip: Mathematische Einbahnstraßen

Es gibt mathematische Rechnungen, die leicht durchzuführen, aber schwer umzukehren sind:

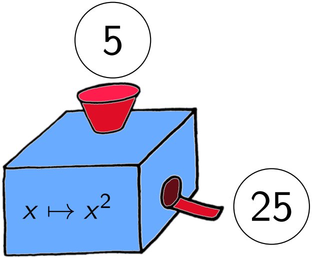
Beispiel

$$257 \cdot 379 = 97403$$

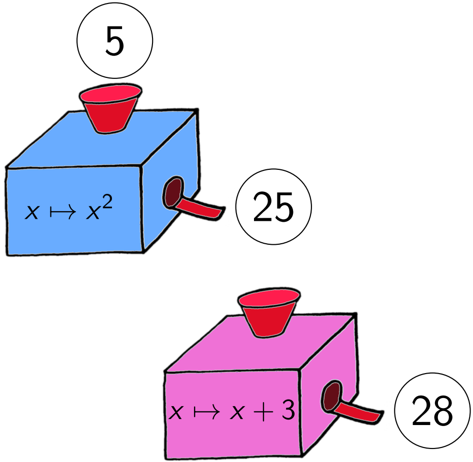
Beispiel

$$95567 = 227 \cdot 421$$

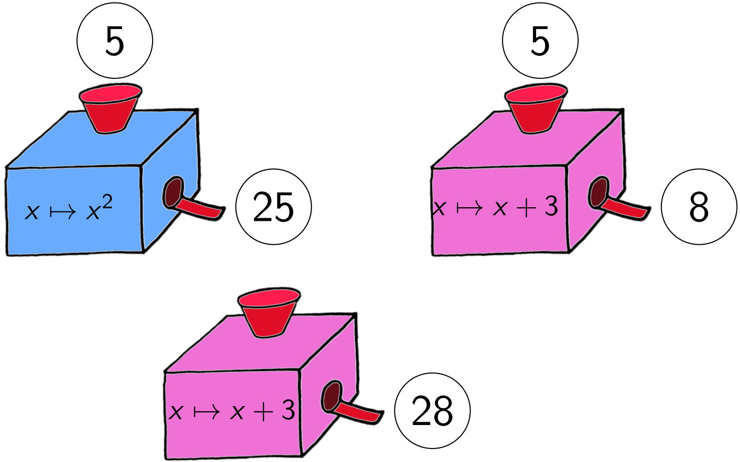
Vertauschbare Maschinen



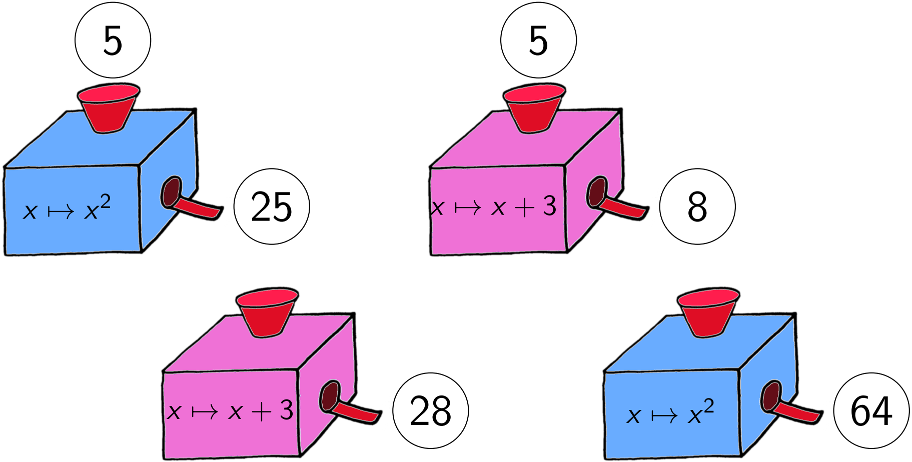
Vertauschbare Maschinen



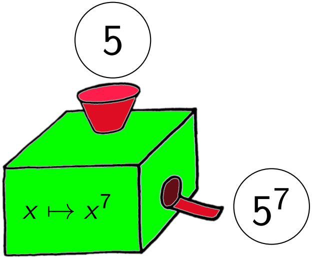
Vertauschbare Maschinen



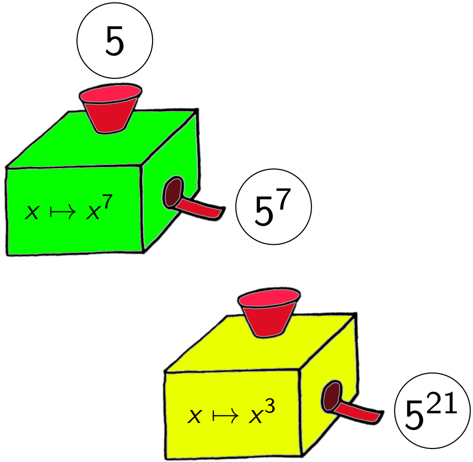
Vertauschbare Maschinen



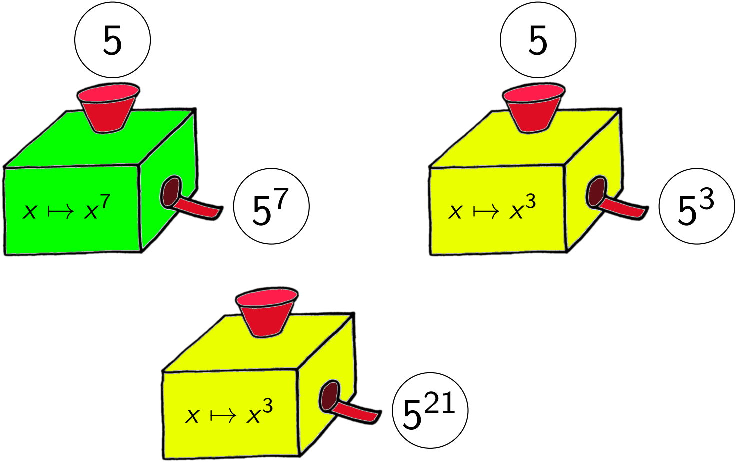
Vertauschbare Maschinen



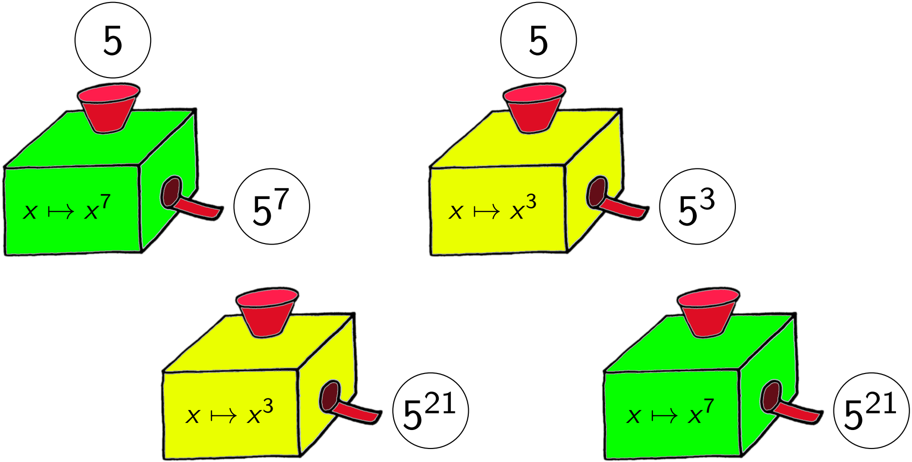
Vertauschbare Maschinen



Vertauschbare Maschinen



Vertauschbare Maschinen



Diffie-Hellman-Schlüsseltausch

Öffentliche Daten: x, die “Bauart” der Maschinen.

Diffie-Hellman-Schlüsseltausch

Alice

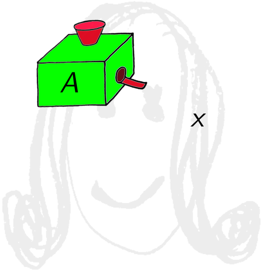
Bob

Eve

Diffie-Hellman-Schlüsseltausch

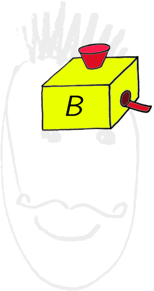
Alice

Bob



x

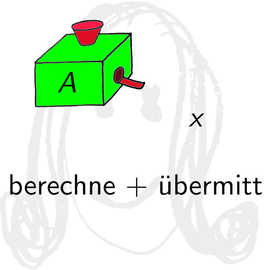
x

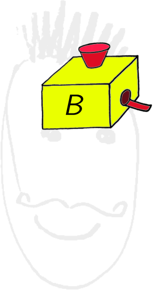


Eve: x

Diffie-Hellman-Schlüsseltausch

Alice **Bob**





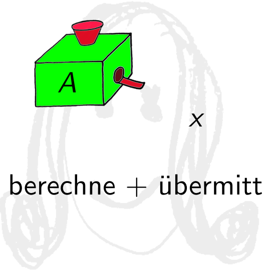
x x

berechne $+$ übermittle $A(x)$

Eve: x

Diffie-Hellman-Schlüsseltausch

Alice

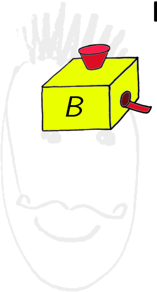


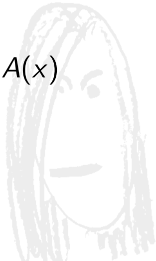
x

berechne + übermittle $A(x)$

$x,\ A(x)$

Bob

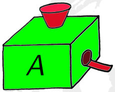




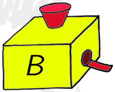
Eve: $x,\ A(x)$

Diffie-Hellman-Schlüsseltausch

Alice



Bob



x

$x,\ A(x)$

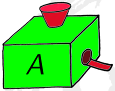
berechne + übermittle $A(x)$

berechne + übermittle $B(x)$

Eve: $x,\ A(x)$

Diffie-Hellman-Schlüsseltausch

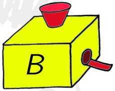
Alice



x, $B(x)$

berechne + übermittle $A(x)$

Bob



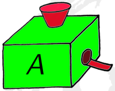
x, $A(x)$

berechne + übermittle $B(x)$

Eve: x, $A(x)$, $B(x)$

Diffie-Hellman-Schlüsseltausch

Alice

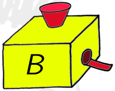


x, $B(x)$, $A(B(x))$

berechne + übermittle $A(x)$

berechne $A(B(x))$

Bob



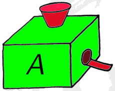
x, $A(x)$

berechne + übermittle $B(x)$

Eve: x, $A(x)$, $B(x)$

Diffie-Hellman-Schlüsseltausch

Alice

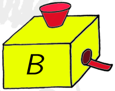


x, $B(x)$, $A(B(x))$

berechne + übermittle $A(x)$

berechne $A(B(x))$

Bob



x, $A(x)$, $B(A(x))$

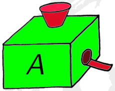
berechne + übermittle $B(x)$

berechne $B(A(x))$

Eve: x, $A(x)$, $B(x)$

Diffie-Hellman-Schlüsseltausch

Alice

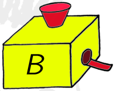


x, $B(x)$, $A(B(x))$

berechne + übermittle $A(x)$

berechne $A(B(x))$

Bob



x, $A(x)$, $B(A(x))$

berechne + übermittle $B(x)$

berechne $B(A(x))$

Eve: x, $A(x)$, $B(x)$

Diffie-Hellman-Schlüsseltausch

Ergebnis:

Alice kennt $A(B(x))$, Bob kennt $B(A(x))$,

Eve kennt $x,\ A(x),\ B(x)$.

Diffie-Hellman-Schlüsseltausch

Ergebnis:

Alice kennt $A(B(x))$, Bob kennt $B(A(x))$,

Eve kennt $x,\ A(x),\ B(x)$.

- Falls $A(B(x)) = B(A(x))$, so kann dieser Wert nun als Schlüssel benutzt werden.
- Sicherheit: Es darf nicht (leicht) möglich sein, aus x, $A(x)$ und $B(x)$ auf A oder B (und damit $A(B(x))$) zurückzuschließen.

Erster Versuch . . .

Sei x eine Zahl, zum Beispiel $x = 5$.

Erster Versuch . . .

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Erster Versuch ...

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Bob wählt eine Zahl B, zum Beispiel $B = 7$ und benutzt als $B(x)$ den Wert $x^B = 5^7$.

Erster Versuch ...

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Bob wählt eine Zahl B, zum Beispiel $B = 7$ und benutzt als $B(x)$ den Wert $x^B = 5^7$.

Der gemeinsame Schlüssel ist
$(x^A)^B = (x^B)^A = 5^{21} = 476837158203125$

Erster Versuch . . .

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Bob wählt eine Zahl B, zum Beispiel $B = 7$ und benutzt als $B(x)$ den Wert $x^B = 5^7$.

Der gemeinsame Schlüssel ist
$(x^A)^B = (x^B)^A = 5^{21} = 476837158203125$

Ungeeignet, denn

- leicht umkehrbar, und
- es treten zu große Zahlen auf.

Erster Versuch ...

Sei x eine Zahl, zum Beispiel $x = 5$.

Alice wählt eine Zahl A, zum Beispiel $A = 3$ und benutzt als $A(x)$ den Wert $x^A = 5^3$.

Bob wählt eine Zahl B, zum Beispiel $B = 7$ und benutzt als $B(x)$ den Wert $x^B = 5^7$.

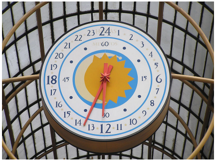
Der gemeinsame Schlüssel ist
$(x^A)^B = (x^B)^A = 5^{21} = 476837158203125$

Ungeeignet, denn

- leicht umkehrbar, und
- es treten zu große Zahlen auf.

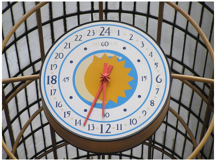
$$3 = \log_5(5^3)$$

Beispiele für das Rechnen mit Resten



Uhrzeit.
Wie viel Uhr ist es in 25 Stunden? . . . in 100 Stunden? . . . in 1000 Stunden?

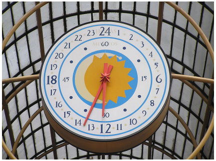
Beispiele für das Rechnen mit Resten



Uhrzeit.
Wie viel Uhr ist es in 25 Stunden? ... in 100 Stunden? ... in 1000 Stunden?

Wochentag. Welcher Wochentag ist heute in 1000 Tagen?

Beispiele für das Rechnen mit Resten



Uhrzeit.
Wie viel Uhr ist es in 25 Stunden? . . . in 100 Stunden? . . . in 1000 Stunden?

Wochentag. Welcher Wochentag ist heute in 1000 Tagen?

Teilbarkeit durch 9. Ist 123456789 durch 9 teilbar?

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5$,

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5, \qquad 64 \mod 17 = 13,$

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5, \qquad 64 \mod 17 = 13, \qquad -4 \mod 17 = 13.$

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5, \qquad 64 \mod 17 = 13, \qquad -4 \mod 17 = 13.$

Beispiel

$$\begin{aligned} 5^7 \mod 17 &= 5 \cdot (5^2)^3 \mod 17 = 5 \cdot (25)^3 \mod 17 \\ &= 5 \cdot 8^3 \mod 17 = 5 \cdot 8 \cdot 64 \mod 17 \\ &= 40 \cdot (-4) \mod 17 = -24 \mod 17 = 10 \end{aligned}$$

Schreibweise

Definition

Seien x, n ganze Zahlen. Wir schreiben $x \mod n$ für den Rest, den x bei Division durch n lässt.

Beispiel

$36 \mod 31 = 5, \qquad 64 \mod 17 = 13, \qquad -4 \mod 17 = 13.$

Beispiel

$$\begin{aligned} 5^7 \mod 17 &= 5 \cdot (5^2)^3 \mod 17 = 5 \cdot (25)^3 \mod 17 \\ &= 5 \cdot 8^3 \mod 17 = 5 \cdot 8 \cdot 64 \mod 17 \\ &= 40 \cdot (-4) \mod 17 = -24 \mod 17 = 10 \end{aligned}$$

Zum Vergleich: $5^7 = 78125$.

Eine praktikable Version des Schlüsseltauschs

Öffentlich: (große Prim-)Zahl p, eine Zahl x, $1 < x < p$.

Eine praktikable Version des Schlüsseltauschs

Öffentlich: (große Prim-)Zahl p, eine Zahl x, $1 < x < p$.

Alice

wählt eine Zahl $1 < A < p$ und schickt Bob die Zahl $x^A \mod p$.

Bob

wählt eine Zahl $1 < B < p$ und schickt Alice die Zahl $x^B \mod p$.

Eine praktikable Version des Schlüsseltauschs

Öffentlich: (große Prim-)Zahl p, eine Zahl x, $1 < x < p$.

Alice

wählt eine Zahl $1 < A < p$ und schickt Bob die Zahl $x^A \mod p$.

Bob

wählt eine Zahl $1 < B < p$ und schickt Alice die Zahl $x^B \mod p$.

Alice und Bob können $x^{AB} = (x^B)^A = (x^A)^B \mod p$ berechnen und als gemeinsamen Schlüssel berechnen.

Schlüsseltausch, Beispiel

Öffentlich: (große Prim-)Zahl $p = 17$, eine Zahl $x = 5$, $1 < x < p$.

Schlüsseltausch, Beispiel

Öffentlich: (große Prim-)Zahl $p = 17$, eine Zahl $x = 5$, $1 < x < p$.

Alice

wählt die Zahl $A = 3$ und schickt Bob die Zahl $5^3 \mod 17 = 6$.

Bob

wählt die Zahl $B = 7$ und schickt Alice
die Zahl $5^7 \mod 17 = 10$.

Schlüsseltausch, Beispiel

Öffentlich: (große Prim-)Zahl $p = 17$, eine Zahl $x = 5$, $1 < x < p$.

Alice

wählt die Zahl $A = 3$ und schickt Bob die Zahl $5^3 \mod 17 = 6$.

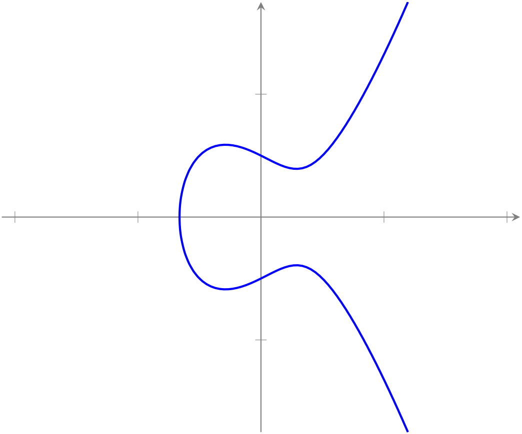
Bob

wählt die Zahl $B = 7$ und schickt Alice
die Zahl $5^7 \mod 17 = 10$.

Alice und Bob können $5^{21} \mod 17 = 10^3 \mod 17 = 14$
berechnen und als gemeinsamen Schlüssel verwenden.

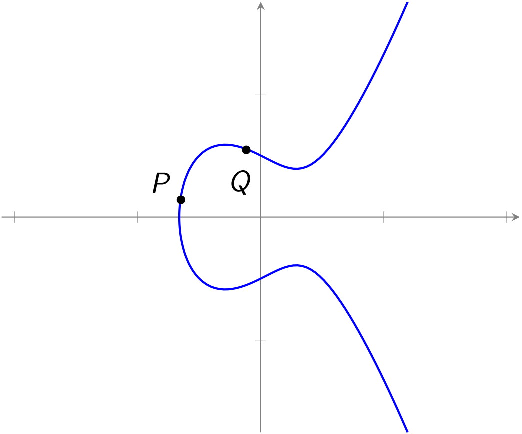
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



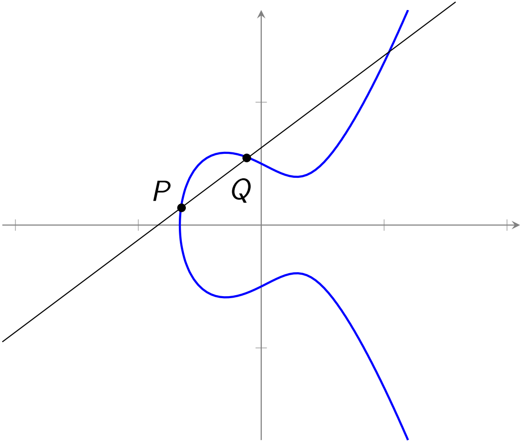
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



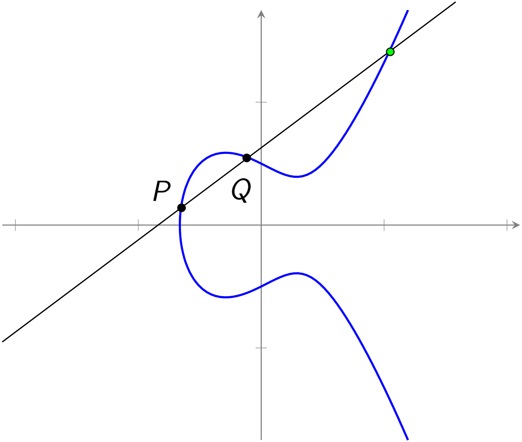
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



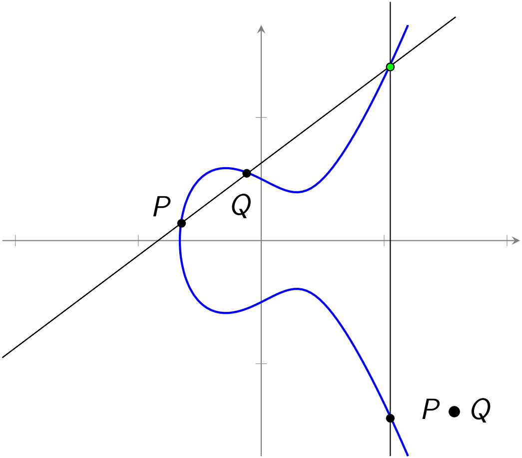
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



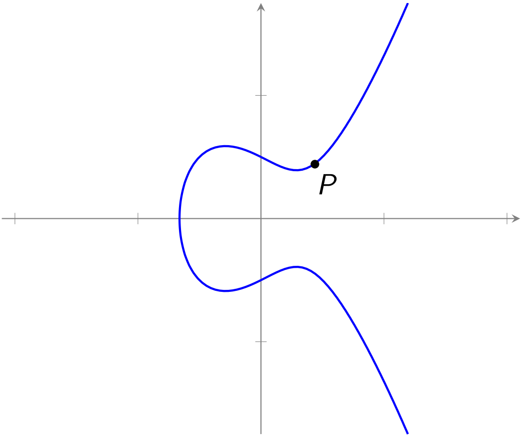
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



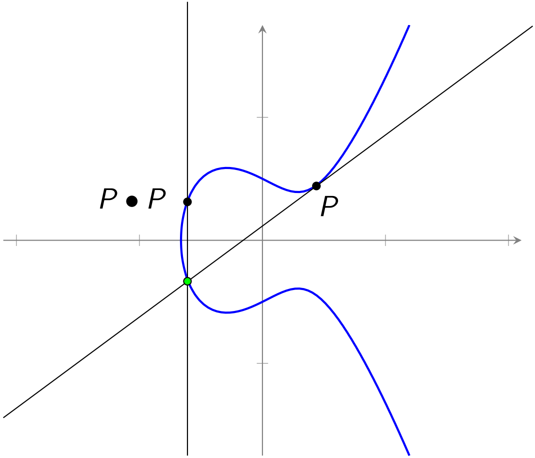
Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



Kryptographie mit elliptischen Kurven

$$y^2 = x^3 - x + 1$$



Diffie-Hellman-Schlüsseltausch mit Elliptischen Kurven

Öffentlich

Wähle eine elliptische Kurve und einen Punkt P darauf.

Diffie-Hellman-Schlüsseltausch mit Elliptischen Kurven

Öffentlich

Wähle eine elliptische Kurve und einen Punkt P darauf.

Alice

wählt eine Zahl A, berechnet $P^A = P \bullet \cdots \bullet P$ und schickt dies an Bob.

Bob

wählt eine Zahl B, berechnet $P^B = P \bullet \cdots \bullet P$ und schickt dies an Alice.

Diffie-Hellman-Schlüsseltausch mit Elliptischen Kurven

Öffentlich

Wähle eine elliptische Kurve und einen Punkt P darauf.

Alice

wählt eine Zahl A, berechnet $P^A = P \bullet \cdots \bullet P$ und schickt dies an Bob.

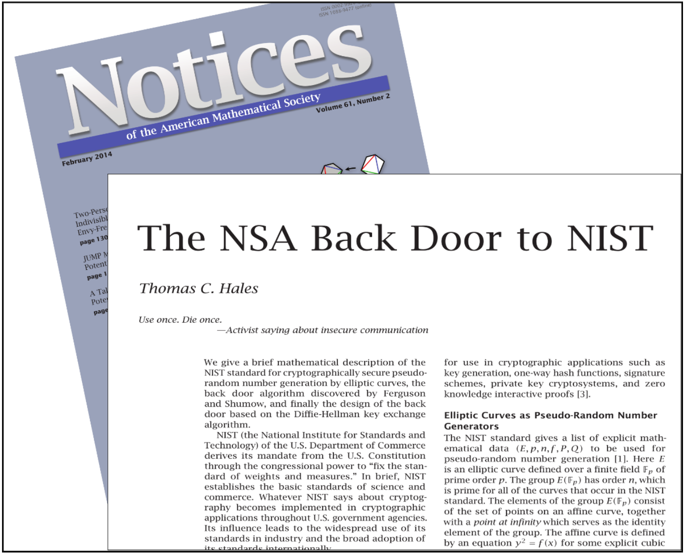
Bob

wählt eine Zahl B, berechnet $P^B = P \bullet \cdots \bullet P$ und schickt dies an Alice.

Gemeinsamer Schlüssel

die erste Koordinate des Punktes $(P^A)^B = (P^B)^A$.

Wie wählt man eine geeignete elliptische Kurve?



The NSA Back Door to NIST

Thomas C. Hales

Use once. Die once.
—*Activist saying about insecure communication*

We give a brief mathematical description of the NIST standard for cryptographically secure pseudo-random number generation by elliptic curves, the back door algorithm discovered by Ferguson and Shumow, and finally the design of the back door based on the Diffie-Hellman key exchange algorithm.

NIST (the National Institute for Standards and Technology) of the U.S. Department of Commerce derives its mandate from the U.S. Constitution through the congressional power to "fix the standard of weights and measures." In brief, NIST establishes the basic standards of science and commerce. Whatever NIST says about cryptography becomes implemented in cryptographic applications throughout U.S. government agencies. Its influence leads to the widespread use of its standards in industry and the broad adoption of its standards internationally.

for use in cryptographic applications such as key generation, one-way hash functions, signature schemes, private key cryptosystems, and zero knowledge interactive proofs [3].

Elliptic Curves as Pseudo-Random Number Generators

The NIST standard gives a list of explicit mathematical data (E, p, n, f, P, Q) to be used for pseudo-random number generation [1]. Here E is an elliptic curve defined over a finite field $\mathbb{F}_p$ of prime order p. The group $E(\mathbb{F}_p)$ has order n, which is prime for all of the curves that occur in the NIST standard. The elements of the group $E(\mathbb{F}_p)$ consist of the set of points on an affine curve, together with a *point at infinity* which serves as the identity element of the group. The affine curve is defined by an equation $y^2 = f(x)$ for some explicit cubic

Quellen/Weiterführende Lektüre

S. Singh, *Geheime Botschaften*, dtv 2001.

http://de.wikipedia.org/wiki/Kryptographie

T. Körner, *The pleasures of counting*, Cambridge University Press, 1996.

J. Buchmann, *Einführung in die Kryptographie*, Springer-Verlag, 2010.

D. R. Stinson, *Cryptography – Theory and Practice*, CRC Press, 1995.

Prinzip der Public-Key-Kryptographie

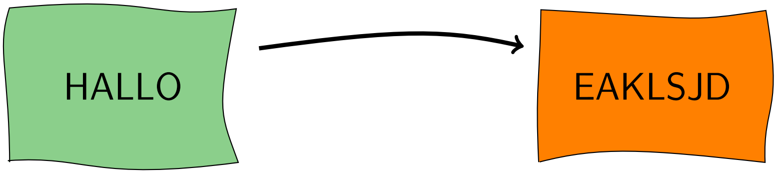
Wir suchen eine “Maschine” (einen Algorithmus), die

(1) aus einem gegebenen Klartext schnell einen “verschlüsselten” Text berechnen kann,

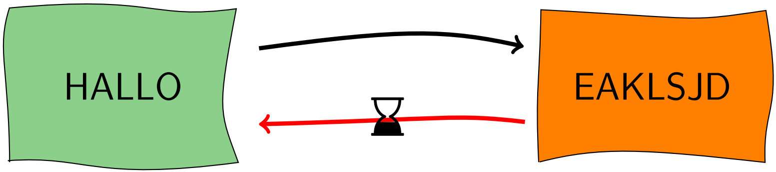
(2) so dass sich aus dem verschlüsselten Text der Klartext *unter Zuhilfename zusätzlicher Informationen, die für (1) nicht benötigt werden,* schnell berechnen lässt,

(3) aber sich der Klartext ohne diese zusätzlichen Informationen nur mit erheblichem Aufwand aus dem verschlüsselten Text berechnen lässt.

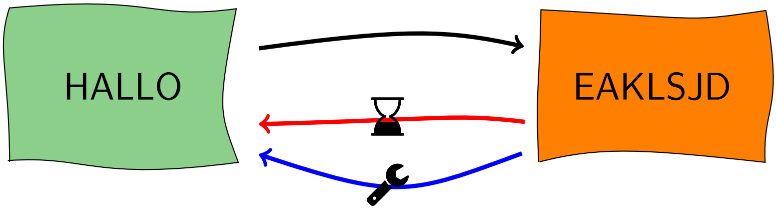
Prinzip der Public-Key-Kryptographie



Prinzip der Public-Key-Kryptographie



Prinzip der Public-Key-Kryptographie



Verschlüsselung mit RSA

Wähle große Primzahlen $p \neq q$, $N = pq$,
e teilerfremd zu $(p-1)(q-1)$.
Berechne f so dass $ef \equiv 1 \mod (p-1)(q-1)$.

Verschlüsselung mit RSA

Wähle große Primzahlen $p \neq q$, $N = pq$,
e teilerfremd zu $(p-1)(q-1)$.
Berechne f so dass $ef \equiv 1 \mod (p-1)(q-1)$.

K Klartext (als Zahl $< N$), C verschlüsselter Text.

Verschlüsselung

$C := K^e \mod N$

Verschlüsselung mit RSA

Wähle große Primzahlen $p \neq q$, $N = pq$,
e teilerfremd zu $(p-1)(q-1)$.
Berechne f so dass $ef \equiv 1 \mod (p-1)(q-1)$.

K Klartext (als Zahl $< N$), C verschlüsselter Text.

Verschlüsselung

$C := K^e \mod N$

Entschlüsselung

$$\text{Berechne } C^f = K^{ef} \equiv K \mod N.$$

Der Satz von Euler

Satz

Seien p, q verschiedene Primzahlen.
Sei $N = pq$, $d \in \mathbb{Z}$ mit

$$d \equiv 1 \mod (p-1)(q-1).$$

Dann gilt $a^d \equiv a \mod N$.

Beispiel

$p = 5,\ q = 7,\ N = 35,\ d = 25,\ a = 3.$

$$3^{25} = 27^8 \cdot 3 \equiv (-8)^8 \cdot 3 \equiv (-6)^4 \cdot 3 \equiv 36^2 \cdot 3 \equiv 3 \mod 35$$

Entschlüsselung ohne Schlüssel?

Die einzige offensichtliche Möglichkeit, aus N, e und C wieder K zu berechnen, ist mit Hilfe von f. Aber f lässt sich nur dann aus e berechnen, wenn p und q bekannt sind.

Das Problem ist also, die Zahl N in ihre Primfaktoren zu zerlegen.

Entschlüsselung ohne Schlüssel?

Die einzige offensichtliche Möglichkeit, aus N, e und C wieder K zu berechnen, ist mit Hilfe von f. Aber f lässt sich nur dann aus e berechnen, wenn p und q bekannt sind.

Das Problem ist also, die Zahl N in ihre Primfaktoren zu zerlegen.

Dafür ist —bei entsprechender Größe von p und q— kein schnelles Verfahren bekannt. Primzahlen der entsprechenden Größe zu finden, ist vergleichsweise leicht. Eine übliche Größe für wichtige geheime Nachrichten wäre heutzutage, Primzahlen p und q mit ungefähr 300 Stellen zu verwenden.