Absolut geheim!

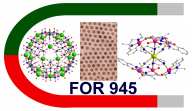
Jürgen Schnack

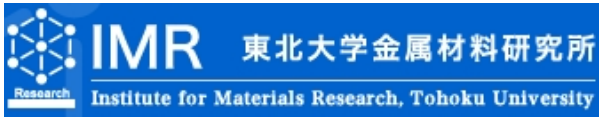
Fakultät für Physik – Universität Bielefeld

http://obelix.physik.uni-bielefeld.de/∼schnack/

Preisverleihung – Mathematikolympiade Kreis Gütersloh

Städtisches Gymnasium Gütersloh, 24. 01. 2017





Herzlichen

Glückwunsch

Ihr seid super!

Herzlichen Dank an Herrn Venz

und einen tollen Applaus!

Liebe Eltern (insbesondere die Väter),

auch wenn es Ihnen auf der Zunge liegt:

SIE DÜRFEN HEUTE

NICHT VORSAGEN!

Ich brauche Geld!

VIEL GELD!

Das Clay-Institut für Mathematik in den USA vergibt

1.000.000 $

für die Lösung eines Millenium-Problems!

Lösungen an Clay Mathematics Institute, 70 Main St, Suite 300, Peterborough, NH 03458, USA

1.000.000 $!!!

Die Milleniumsprobleme

- Beweis der Vermutung von Birch und Swinnerton-Dyer,
- Beweis der Vermutung von Hodge,
- Analyse von Existenz und Regularität von Lösungen des Anfangswertproblems der dreidimensionalen inkompressiblen Navier-Stokes-Gleichungen,
- Lösung des P-NP-Problems,
- Beweis der Poincaré-Vermutung
  (2002 gelöst von Grigori Jakowlewitsch Perelman),
- Beweis der Riemannschen Vermutung,
- strenge Begründung der quantisierten Yang-Mills-Theorie.

Ich hab das mal gegoogelt:
https://de.wikipedia.org/wiki/Millennium-Probleme

Wir schaffen das!

Ihr löst ein Problem!

Ich regel das mit dem Geld!

Für die Geldübergabe müssen wir

Nachrichten verschlüsseln

oder Signaturen erstellen.

Caesar-Verschlüsselung

Verschiebung der Buchstaben, z.B.

A $\Rightarrow$ E, B $\Rightarrow$ F, C $\Rightarrow$ G, . . . , Z $\Rightarrow$ D

HALLO $\Rightarrow$ LEPPT

Verschlüsseln eines Buchstabens b:

$$s = (b + k) \pmod{26}$$

Entschlüsseln eines Buchstabens s:

$$b = (s - k) \pmod{26}$$

(Zahlen 0, 1, . . . , 25 für die Buchstaben)

Modulo

$$a = b \pmod{n}$$

bedeutet, dass a und b bei Division durch n den gleichen Rest geben, z.B.

$$17 = 7 \pmod{10} \qquad \text{oder} \qquad 7 = 1 \pmod{6}\ .$$

Eigentlich ist $7 \cdot 1/7 = 1$, aber mit Modulo geht auch

$$7 \cdot 3 = 1 \pmod{10}\ .$$

Caesar-Verschlüsselung

Verschiebung der Buchstaben, z.B.

A $\Rightarrow$ E, B $\Rightarrow$ F, C $\Rightarrow$ G, . . . , Z $\Rightarrow$ D

HALLO $\Rightarrow$ LEPPT

Verschlüsseln eines Buchstabens b:

$s = (b + k) \pmod{26}$

Entschlüsseln eines Buchstabens s:

$b = (s - k) \pmod{26}$

(Zahlen 0, 1, . . . , 25 für die Buchstaben)

Problem: Man muss dem anderen mitteilen, wie man verschlüsselt hat, also z.B. $k = 4$.
Wer dies erfährt, kann alles entschlüsseln.

Es gibt Verfahren,

bei denen man aller Welt

den Schlüssel mitteilen kann!

(Und trotzdem kann man damit nicht entschlüsseln.)

RSA-Verfahren (Rivest, Shamir, Adleman)

- Wähle zufällig zwei etwa gleich große Primzahlen p und q.
- Berechne $N = p \cdot q$, genannt RSA-Modul.
- Berechne die Eulersche φ-Funktion von N: $\varphi(N) = (p-1) \cdot (q-1)$
- Wähle eine Zahl e mit $1 < e < \varphi(N)$, die zu $\varphi(N)$ teilerfremd ist.
  Oft $e = 2^{16} + 1 = 65537$.
- Berechne den Entschlüsselungsexponenten d, so dass gilt $e \cdot d = 1 \pmod{\varphi(N)}$.
  d wird multiplikatives Inverses von e bzgl. $\varphi(N)$ genannt.

Beispiel:
$p = 11$, $q = 13$, dann $N = p \cdot q = 143$.
$\varphi(N) = (p-1) \cdot (q-1) = 120$.
Wählen $e = 23$.
Berechnen d (zu Hause) zu $d = 47$.

Verschlüsseln und Entschlüsseln

- Verschlüsseln von Nachrichten m:

  $c = m^e \pmod N$ ergibt Geheimtext c.

  m muss kleiner als N sein.

- Unser Beispiel: 7 verschlüsselt ergibt $7^{23} \pmod{143} = 2$

- Entschlüsseln von Nachrichten c:

  $m = c^d \pmod N$ ergibt den Ausgangstext m.

- Unser Beispiel: 2 entschlüsselt ergibt $2^{47} \pmod{143} = 7$

Zum Verschlüsseln braucht man nur e und N, die Zahlen kann man aller Welt geben. Das ist der öffentliche Schlüsssel.

Zum Entschlüsseln braucht man d und N, die Zahl d gibt man niemandem! Zusammen mit N ist das der private Schlüsssel.

Warum kann man diese Verschlüsselung nur sehr schwer knacken?

Primfaktorzerlegung

- N ist öffentlich und war $N = p \cdot q$.
- Wir bräuchten doch nur N in p und q zu zerlegen, dann sind wir fertig und können den Code knacken!!!
- Los geht's!
- Was waren noch einmal Primzahlen?

Primfaktorzerlegung

- N ist öffentlich und war $N = p \cdot q$.
- Wir bräuchten doch nur N in p und q zu zerlegen, dann sind wir fertig und können den Code knacken!!!
- Los geht's!
- Was waren noch einmal Primzahlen?
- Was ist eine Primfaktorzerlegung?

Primfaktorzerlegung

- N ist öffentlich und war $N = p \cdot q$.
- Wir bräuchten doch nur N in p und q zu zerlegen, dann sind wir fertig und können den Code knacken!!!
- Los geht's!
- Was waren noch einmal Primzahlen?
- Was ist eine Primfaktorzerlegung?
- Wie würdet Ihr die Primfaktorzerlegung einer Zahl N durchführen?

$\rightarrow$ Mathematica Notebooks

Einwegfunktionen

- Das Produkt zweier Zahlen zu bilden, ist viel einfacher, als umgekehrt heraus zu finden, aus welchen Faktoren eine Zahl aufgebaut ist!
- Solche Funktionen heißen Einwegfunktionen.
- Anderes Beispiel: Telefonbuch
- Einen Schlüssel aus zwei Primzahlen zu bauen, ist also viel, viel einfacher, als diesen Schlüssel zu knacken.

Toll, diese Einwegfunktionen!

. . . , aber . . .

Gibt es diese Einwegfunktionen überhaupt?

Vielleicht sind wir auch einfach

nur zu doof?

Der Aufwand für Einwegfunktionen

ist in die einfache Richtung ein Polynom der Größe,

ist in die schwere Richtung kein Polynom der Größe

(sondern schlimmer, z.B. exponentiell).

Wenn Ihr die Existenz von Einwegfunktionen beweisen könnt, habt Ihr auch das P-NP-Milleniumsproblem gelöst!

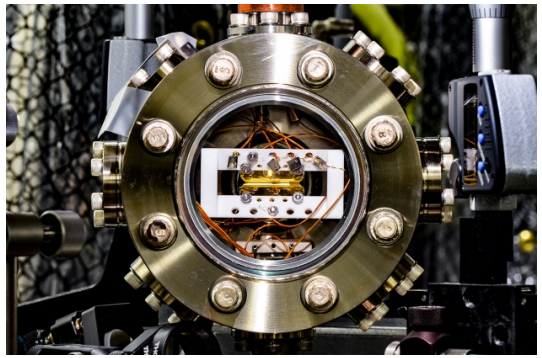
1.000.000 $!!!

Unterschied zwischen Mathematikern und Physikern:

Mathematiker suchen den Beweis,

Physiker bauen die
Entschlüsselungsmaschine,
den Quantencomputer.

Quantencomputer



Klassischer Computer bearbeitet einen Zustand, z.B. (01101001)

Quantencomputer bearbeitet alle Zustände gleichzeitig, also z.B.

(00000001)+(00000010)+(00000011)+(00000100)+...

Primfaktorzerlegung durch Shor-Algorithmus

Die Möglichkeiten des Quantencomputers wachsen exponentiell mit der Zahl der Qubits, beim klassischen Computer nur linear mit der Zahl der cores.

Tolle Leute bei Google
oder Microsoft
und auch in Europa
arbeiten an Quantencomputern.

Ihr könnt dabei sein!

Denn Ihr mögt Mathematik!

Damit könnt Ihr Vieles studieren, z.B.

Physik!

Vielen Dank für Eure Aufmerksamkeit