Die Welt der Primzahlen, I

Mathematik *Querbeet*

Prof. Dr. Stefan Wewers

Institut für Algebra und Zahlentheorie
Universität Ulm

18. Dezember 2020

Ein Quiz

1.Frage

Welcher Arbeitgeber beschäftigt die meisten Mathematiker ?

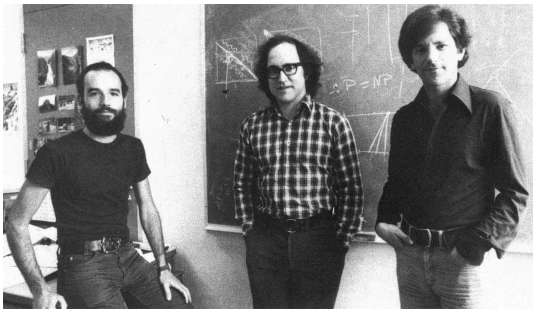
Die *NSA* (National Security Agency):

Ein Quiz

2.Frage

Was bedeutet **RSA** ?

RSA steht für **R***ivest,* **S***hamir und* **A***dleman*, den drei Entwicklern des gleichnamigen Kryptosystems:



Ein Quiz

3.Frage

Ist 3551 ein Primzahl ?

Primzahlen

Definition

Eine **Primzahl** ist eine natürliche Zahl $p > 1$, die nur durch 1 und durch sich selbst teilbar ist.

Es gibt unendlich viele Primzahlen:

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Jede natürliche Zahl $n > 1$ lässt sich auf eindeutige Weise als ein Produkt von Primzahlen schreiben,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

(mit $p_1 \leq p_2 \leq \ldots \leq p_r$).

Der Fundamentalsatz der Arithmetik

Theorem

Jede natürliche Zahl $n > 1$ lässt sich auf eindeutige Weise als ein Produkt von Primzahlen schreiben,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

(mit $p_1 \leq p_2 \leq \ldots \leq p_r$).

Beispiele:

$$60 = 2^2 \cdot 3 \cdot 5.$$

$$8001 = 3^2 \cdot 7 \cdot 127.$$

Die *Eindeutigkeitsaussage* im obigen Satz zeigt z.B.:

$$23 \nmid 8001.$$

Das Faktorisierungsproblem

Gegeben sei eine (möglicherweise sehr große) natürliche Zahl n. Gibt es eine effiziente Methode, die Primfaktorzerlegung von n zu bestimmen?

Probedivision:

1. Teste, für alle Primzahlen $p \leq \sqrt{n}$, ob $p \mid n$.
2. Falls es einen Primteiler $p \mid n$ gibt, ersetze n durch n/p und gehe zurück zu 1.
3. Sonst ist n eine Primzahl.

Das Faktorisierungsproblem

Angenommen, wir möchten die Zahl

$$n = 98949700653137365196479537425523417869 7$$

faktorisieren.
Für die Probedivision müssten wir ungefähr

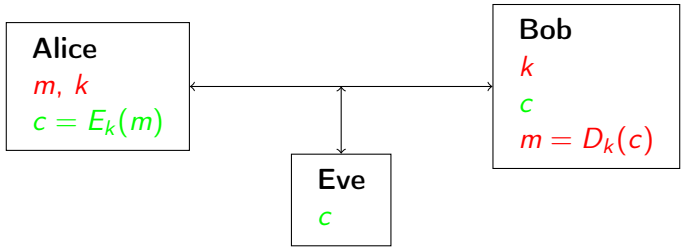
$$\frac{\sqrt{n}}{\log(\sqrt{n})} \approx 7 \cdot 10^{17}$$

Primzahlen p testen. Wenn jeder Test ungefähr $1\mu s$ dauert, bräuchten wir ca.

20000 Milliarden Jahre.

Symmetrische Verschlüsselungsverfahren

Ein einfaches Modell:



Dabei ist k der geheime *Schlüssel*, m der *Klartext*, und

$$c = E_k(m)$$

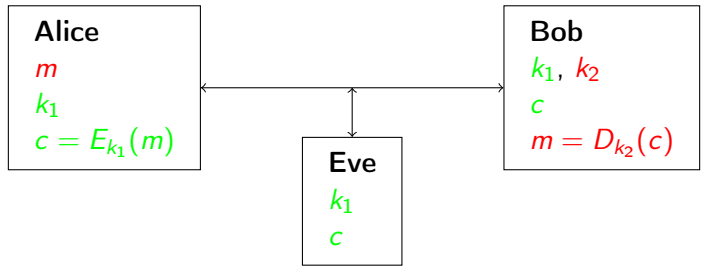
der *Geheimtext*.

Ver- und Entschlüsselung:

$$m \overset{E_k}{\longmapsto} c \overset{D_k}{\longmapsto} m.$$

Ein asymmetrisches Verschlüsselungsverfahren

Wir betrachten die übliche Modellsituation; diesmal möchte Alice eine Nachricht m an Bob schicken.



Die RSA-Verschlüsselung

- 1977 entwickelt von **R***ivest,* **S***hamir und* **A***dleman*
- 1983 patentiert; September 2000 ist das Patent erloschen
- Der private Schlüssel ist (N, e), wobei
  - $N = p \cdot q$ eine **RSA-Zahl** ist,
  - e teilerfremd zu N.
- Die Verschlüsselungsfunktion ist

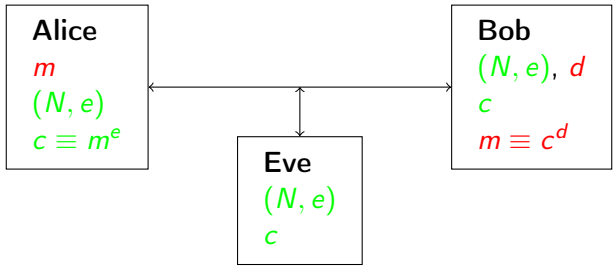
$$E_{(N,e)} : \; m \mapsto c := m^e \pmod{N}$$

- Der geheime Schlüssel ist ein d so dass für alle m gilt:

$$c^d = (m^e)^d = m^{ed} \equiv m \pmod{N}.$$

- Ein solches d kann nur berechnen, wer die Faktorisierung $N = p \cdot q$ kennt!

Das RSA-Verfahren



- Bob wählt p, q, e und berechnet $N = pq$ und d mit $ed \equiv 1 \pmod{(p-1)(q-1)}$
- Bob veröffentlicht (N, e)
- Alice berechnet $c \equiv m^e \pmod{N}$ und schickt c an Bob
- Bob berechnet $m \equiv c^d \pmod{N}$.

Der Faktorisierungsrekord

Im September 2020 konnte ein Team von Mathematikern und Informatikern eine 768-Bit RSA-Zahl faktorisieren ($\sim$ 231 Dezimalstellen).

Der verwendete Algorithmus ist das sogenannte *Zahlkörpersieb* .

Die Berechnung dauerte ungefähr 2700 Rechnerjahre.

Aktuell werden in der Regel RSA-Zahlen mit 2048 Bits verwendet ($\sim$ 617 Dezimalstellen).

Quantencomputer

RSA-Verschlüsselung mit 2048 Bits gilt momentan als sicher (für die nächsten 10 Jahre..).

Wegen erwartetem weiteren Fortschritt von Rechnerleistung und Algorithmen muss man von Zeit zu Zeit die Schlüssellänge erhöhen.

Aber: Auf einem hinreichend leistungsfähigem *Quantencomputer* wäre das Faktorisieren in „polynomialer" Zeit möglich, und die Sicherheit des RSA-Kryptosystems endgültig kompromittiert.