> Es ist eine riesige Erleichterung, dass mein Gebiet, die Geschichte, keine solchen Preise besitzt. Meiner Ansicht nach, gerade nach der Lektüre von Elisabeth Crawfords Arbeit über die Geschichte der Nobelpreise [welche nicht für vorgegebene Probleme vergeben werden], ist ihr Effekt, etwaige Forschung und die Wertschätzung derselben zu verzerren und zu verengen.

Ein abschließender Gedanke

Wenn wie in der griechischen Antike eine Stiftung einen Preis für den „Klügsten von allen“ ausschriebe, würden wir dann alle als Resultat des Wettstreits klüger werden? Würde die Evolution damit einen Riesenschritt vorankommen?

Adresse des Autors
Prof. Dr. Philip J. Davis
Division of Applied Mathematics
Brown University
Providence, RI 02912, USA
Philip_Davis@brown.edu

Aus dem Amerikanischen von Folkmar Bornemann

Der schwierigste Code aller Zeiten ist geknackt

von Folkmar Bornemann

Nach seinem Buch über Fermats letzten Satz *gelang Simon Singh vor zwei Jahren mit* The Codebook *(dt. unter dem Titel* Geheime Botschaften*, Hanser, 2000) gleich der nächste Besteller. Er fügte diesem Buch eine Art Übungsaufgabe bei: zehn Geheimtexte aufsteigenden Schwierigkeitsgrades, genannt* The Cipher Challenge*, oder noch werbewirksamer, „der schwierigste Code aller Zeiten“. Singh stiftete 10.000 Pfund für die erste vollständige korrekte Lösung bis zum 1. Januar 2010.*

Fünf schwedische Informatiker[1] schafften es dann schon am 5. Oktober 2000. Für die Entschlüsselung des zehnten, schwierigsten Geheimtextes faktorisierten sie in 13 Tagen Laufzeit auf einer Workstation mit 4 Alpha-Prozessoren folgenden 512bit RSA-Modul (155 Dimalstellen):

$$\begin{aligned}&10742788291266565907178411279942116612663921794753294588877817210355464150980121879033832926235281090750672083504941996433143425558334401855808989426892463 = 12844205165381031491662259028977553198964984323915864368216177647043137765477 \cdot 8363918321876069378206508564497107619045200261997249855967291088123013944892 19\end{aligned}$$

Allein diese Leistung ist schon ein enormer Erfolg. Hierzu hatten sie die Implementierung des *General Number Field Sieve* weiterentwickelt, welche Monate zuvor am niederländischen CWI zur Rekordfaktorisierung von RSA-155 verwendet worden war. Der 38seitige, exzellente und spannende Bericht der Fünf findet sich im Internet unter `http://codebook.org` und beschreibt auch die Lösung der vorangehenden neun Geheimtexte (unter den Verschlüsselungsmethoden finden sich neben RSA und DES auch historisch interessante wie Playfair und eine 3-Rotor-Enigma).

Singh berichtet auf der Webseite der Cipher Challenge, dass sich Menschen aller Lebensbereiche und aller Alterstufen beteiligt hätten, von Anfängern und Schulkindern bis hin zu Mathematikern und Berufskryptographen, ja sogar ein Träger der Fields-Medaille sei dabei gewesen (`http://www.4thestate.co.uk/CipherChallenge`).

Lehrreich ist auch ein Blick auf die Berichterstattung in der Presse, etwa im *Tagesspiegel* (`http://www2.tagesspiegel.de/archiv/2001/01/13/ak-in-13184.html`): die Interpretationen müssen mit Vorsicht genossen werden, da etwa Schlüssellängen symmetrischer und asymmetrischer Verfahren umstandslos in einen Topf geworfen werden.

1 Gunnar Andersson, Lars Ivansson und Staffan Ulfberg promovierten letztes Jahr in Theoretischer Informatik am Royal Institute of Technology in Stockholm, Torbjörn Granlund besitzt eine Firma für Open-Source-Softwarelösungen, Fredrik Almgren arbeitet in einer Firma für mobile Internetlösungen.