

## Die Geschichte einer wundersamen Entdeckung

*Es klingt wie ein Märchen: Was Generationen von Experten nicht erreichten, gelingt einer norddeutschen Schülerin im Spiel – mit dauerhaften Konsequenzen für die bestehende Internet-Architektur.*

Das Produkt zweier Primzahlen, wenn sie groß genug sind, ergibt ein kaum beherrschbares Zahlenmonster. Hat man große Primzahlen zur Verfügung, (dafür gibt es Tests), lässt sich das Monster aber leicht bestimmen. Hat man aber nur das Monster und will die enthaltenen Faktoren berechnen, sollte man auf Jahrmillionen des Ausprobierens vorbereitet sein. Auch leistungsfähige Computer sind damit zunächst überfordert. Erst in jüngster Zeit wurden Algorithmen entwickelt, mit denen das für Monster von 200 und mehr Ziffern nach jahrelangen Operationen im Rechnerverbund gelang. Doch diese Erfolge wissenschaftlicher Spezialisten blieben Einzelfälle. Nur Quantencomputer, (die es noch nicht gibt), so die gängige Meinung, könnten solche Jobs in überschaubarer Zeit erledigen.

An dem Punkt der Entwicklung kommt ein schräger, frecher Text ins Spiel, der eine Gitterstruktur beschreibt, die mit den Primzahlen zusammenhängt. Diese Struktur macht es möglich, Primfaktoren quasi auf Knopfdruck *auszulesen*, schneller vermutlich, als ein Quantenrechner könnte.

Und jetzt der Clou. Das Thema, so technisch es klingen mag, ist gut versteckt in der unterhaltsamen, stellenweise zum Schreien komischen Rahmenhandlung eines modernen Märchens. Die Entdeckung der Struktur gelingt dort der Schülerin *Anne Senft*, und das passt genau ins Bild. Obwohl lange unauffindbar, erweist sich der Zusammenhang nach getaner Arbeit als unanständig simpel. Wie immer! Neugierde und Spieltrieb genügten, ihn aufzudecken. Es sind halbe Kinder, die den Schatz finden, und wer den unbeschwerten Aktionen dieser Helden folgt, wird im Vorübergehen, fast spielerisch davon erfahren. Man liest ein wenig, und ohne es recht zu merken, hat man was gelernt. Die Lektüre erfordert keinerlei Vorkenntnisse, nur das Vorwort richtet sich an fachlich vorbelastete *Mitleser*: IT-Leute, Entwickler, Forscher.

Denn während *normale* Leser einfach Spaß haben, müssen die reagieren: Die Primzahlen bilden einen neuralgischen Punkt der bestehenden Internet-Architektur. Als User haben wir täglich damit zu tun, ohne es zu merken: Bei Transaktionen, Authentifizierungen und Verschlüsselungen. Denn was geschieht?

Vereinfacht lässt sich sagen, dass das öffentlich einsehbare Produkt zweier Primzahlen als Monstergelände zur Verschlüsselung von Daten dient. Zum Entschlüsseln braucht man die enthaltenen Faktoren, die tendenziell unauffindbar bzw. nur den Berechtigten zugänglich sind. Die entsprechenden Prozesse laufen unbemerkt im Hintergrund. Wer in der Lage wäre, öffentliche Schlüssel schnell in ihre Bestandteile zu zerlegen, hätte sehr starke Argumente für neue, bessere Verfahren.

Nach der Publikation dieser märchenhaft anmutenden Geschichte entsteht eine völlig neue Situation. Was wie ein Schulstreich daherkommt, erweist sich als tickende Bombe. Die Jagd auf kryptische Daten ist eröffnet, der Druck auf Forscher und Entwickler steigt. Schwer zu sagen, was

dabei erstaunlicher ist, die Entdeckung an sich oder die Art, wie *Anne* und ihre Freunde damit umgehen.

Für die ist es ein Heidenspaß, den großen Spezialisten ein Lichtlein aufzusetzen und unbefangen mit mathematischen Ungenauigkeiten zu spielen. Werden nun Fachexperten auch mal etwas beitragen? Oder müssen wir warten, bis Kinder sich der entstandenen Probleme annehmen?

Titel: Als Anne Senft berühmt zu werden drohte, Autor: Thomas Bokelmann, Verlag: tredition.  
In 3 Formaten überall im Handel: Hardcover, Paperback und e-Book, weitere Infos hier:  
<https://tredition.de/publish-books/?books/ID90144/Als-Anne-Senft-beruehmt-zu-werden-drohte>

(Ende der Pressemitteilung, März 2017)