# Geheime Botschaften und Primzahlen

**VON BJÖRN UND SÖREN CHRISTENSEN**

In der vergangenen Woche ging es hier um Primzahlen, also um die Zahlen größer als 1, die nur durch 1 und sich selbst teilbar sind. Die ersten Primzahlen sind 2,3,5,7,11,13,17. In dieser Woche erklären wir, welche Rolle nun gerade diese Zahlen – und insbesondere große Primzahlen – für die Verschlüsselung von Nachrichten spielen.

Beginnen wir aber erst einmal mit Anna. Sie bekommt gerne Briefe von ihren Bekannten, möchte aber nicht, dass ihre neugierigen Geschwister diese zu Gesicht bekommen. Eine Möglichkeit für Anna wäre, einen riesigen Vorrat an identischen Vorhängeschlössern zu kaufen. Diese Vorhängeschlösser gibt sie geöffnet an jeden, der Interesse hat, ihr vielleicht einmal zu schreiben, behält aber den Schlüssel für sich. Schreibt Ben ihr also einen Brief, dann legt er diesen – so die Verabredung – in eine kleine feste Schachtel, verschließt diese, indem er das Vorhängeschloss zudrückt, und gibt die Schachtel bei Anna ab. Jetzt bekommt weder er selbst noch ein anderer diese wieder auf – außer Anna natürlich. Sie hat ja den Schlüssel. Wenn wir von Gewaltanwendung einmal absehen, hätten ihre neugierigen Geschwister keine Chance, das Schloss zu öffnen, es sei denn, sie fertigen unzählige mögliche Nachbauten des Schlüssels an, bis einer passt – ein offenkundig zu aufwendiges Unterfangen.

***ANNAS SYSTEM*** scheint also einigermaßen sicher zu sein, ist aber natürlich nicht praktikabel. Das Prinzip lässt sich aber auf moderne Verschlüsselungsverfahren mittels Computer übertragen – und dort kommen dann Primzahlen ins Spiel. Anna benutzt dafür zwei große Primzahlen, sagen wir 3673 und 4327. Diese entsprechen gerade ihrem Schlüssel, den sie an niemanden weitergibt, die nun aber ihr Computer multipliziert: 3673 x 4327 = 15893071. Das Ergebnis ist das offene Schloss, das sie jedem Interessierten überlässt. Bens Computer kann nun seine Nachricht mit Hilfe der Zahl 15893071 nach einem vorgegebenen Verfahren verschlüsseln. Diese Verschlüsselung lässt sich dann nur mittels der beiden Ursprungs-Primzahlen 3673 und 4327 rückgängig machen, die aber nur Anna besitzt. Auch wenn Bens Nachricht also von den Geschwistern abgefangen wird, können sie damit nichts anfangen – solange sie nicht herausfinden, dass 15893071 aus den Primzahlen 3673 und 4327 zusammengesetzt ist.

In diesem Fall könnte ein Computer das Problem noch bewältigen. Wenn Anna aber wirklich große Primzahlen nimmt, hat auch der größte Computer keine Chance mehr, da für das Zerlegen einer Zahl in ihre Primfaktoren auf der ganzen Welt kein wirklich schneller Algorithmus bekannt ist. Große Primzahlen helfen also in unserer modernen Kommunikation sichere Verschlüsselungen zu ermöglichen. ●

**Wie ein Sicherheitsschloss** *können Primzahlen Computer sichern.*

ADOBESTOCK



Schleswig-Holstein Journal, die Wochenendbeilage der Tageszeitungen im s:hz, 20.01.2018