"Eine Million Dollar ...

... für die Sicherheit Ihrer Kreditkarte?"

von Prof. Dr. Ehrhard Behrends und Prof. Dr. Peter Gritzmann

Natürlich achten Sie darauf, dass sich kein anderer Ihrer Kreditkarte bemächtigt, und natürlich steht Ihre vierstellige Geheimnummer nicht auf einem Zettel im Portemonnaie. Doppelte Sicherheit! Wenn jemandem Ihre Kreditkarte in die Hände fällt, muss er unter allen (prinzipiell) möglichen 10 000 Geheimnummern die richtige herausfinden. Die Wahrscheinlichkeit, dass er sie gleich im ersten Versuch rät, ist also 0,0001; bei drei Versuchen immer noch 0,0003, und nach drei Fehlversuchen wird die Karte eingezogen.

Bei Transaktionen am Geldautomaten oder über das Internet werden alle Informationen über "öffentliche" Datenleitungen übermittelt, aber natürlich kodiert, die 16 Stellen Ihrer Kreditkatennummer und die 4 Stellen Ihrer Geheimnummer. Ist das eigentlich sicher? Jedenfalls so sicher wie die verwendeten Geheimcodes.

Moderne Verfahren der Kryptographie beruhen darauf, dass es ungeheuer schwer ist, große natürliche Zahlen in ihre Teiler zu zerlegen. Nehmen Sie Ihre Lieblingszahl oder irgendeine andere; nennen wir sie *n*. Natürlich ist *n* durch 1 und *n* teilbar, das sind ihre trivialen Teiler, aber gibt es auch andere Teiler, und welche sind das? Probieren Sie es mit 187 einmal aus! Stimmt: 187 = 17 x 11. Bei 758 717 wird es schon mühsamer. Das nahe liegendste Verfahren zu überprüfen, ob eine Zahl *n* eine Primzahl oder eine zusammengesetzte Zahl ist, und welches ihre "nicht trivialen" Teiler sind, ist systematisch durch alle Teiler-Kandidaten, d.h. durch alle Zahlen von 2 bis *n*-1 zu dividieren. Geht das nie ohne Rest auf, so ist *n* eine Primzahl. Andernfalls hat man zwei Teiler gefunden. Wenn unsere Zahl *n* nun etwa 100-stellig ist, so müssten mit diesem Verfahren etwa

1.000.000.000.000.000.000.000.000.000

000.000.000.000.000.000.000.000.000

000.000.000.000.000.000.000.000

000.000.000.000.000.000.000

Divisionen durchgeführt werden, und das schaffen selbst die besten zur Verfügung stehenden Computer in ein paar Milliarden Jahren nicht. Man kann das Verfahren wesentlich verbessern

(natürlich braucht man nur Kandidaten bis zur Wurzel aus n zu probieren, und davon auch nicht alle...), aber ein richtig effizienter Algorithmus zur Zerlegung einer Zahl in ihre Teiler ist nicht bekannt. Tatsächlich ist auf das Faktorisieren einer speziellen 174-stelligen Zahl immerhin ein Preis von 10 000 Dollar ausgesetzt, und wenn Sie eine 617-stellige Zahl zerlegen können, erhalten Sie von RSA Security sogar 200 000 Dollar. (Der Weltrekord im Faktorisierungswettbewerb steht übrigens bei einer 155-stelligen Zahl; sie wurde mit Hilfe von 292 Rechnern in insgesamt 7,4 Monaten "geknackt".)

Vielleicht gibt es aber gar kein effizientes Verfahren? Wenn Sie das beweisen könnten, waren Sie sogar um 1000 000 Dollar reicher. Dann hätten Sie nämlich eines der sieben Milleniums-Probleme des amerikanischen Clay-Instituts gelöst, in "kryptisch-mathematischer" Notation: $P \neq NP$. Hinter diesem Kürzel verbirgt sich eine der spannendsten Fragestellungen der Wissenschaft, und sie berührt die prinzipiellen Grenzen unserer intellektuellen Möglichkeiten.

Der Buchstabe P steht dabei für die Klasse von "algorithmisch effizient" lösbaren Entscheidungsproblemen, Fragen also, deren Antworten "ja" oder "nein" algorithmisch "schnell" gefunden werden können. Um dieses mit der nötigen Präzision definieren zu können, muss man abstrakt festlegen, was ein Computer ist und kann, was ein Problem ist, wie eine konkrete Aufgabe des Problems für den Computer spezifiziert wird, und was es heißt, dass ein Problem "schnell" oder "effizient" lösbar ist. Ein ganz einfaches Problem aus P ist die Frage, ob eine gegebene Zahl durch 2 teilbar ist. Jeder weiß natürlich, dass eine Zahl durch 2 teilbar ist, wenn ihre letzte Ziffer durch 2 teilbar ist. Nachdem die Zahl eingelesen wurde, ignoriert der Algorithmus also alle Ziffern bis auf die letzte, und stellt lediglich fest, ob diese 0, 2, 4, 6 oder 8 ist. Fertig.

Das Problem "Gegeben sei eine natürliche Zahl *n*, ist *n* zusammengesetzt?" ist ebenfalls ein Entscheidungsproblem - nennen wir es ZUSAMMENGESETZTE ZAHL. Es ist nicht so klar - und war bis vor kurzem ungeklärt - ob dieses Problem ebenfalls algorithmisch effizient lösbar ist. Hingegen ist völlig klar, wie wir Sie davon überzeugen können, dass 758 717 eine zusammengesetzte Zahl ist, einfach, indem wir Ihnen die Teiler 761 und 997 angeben. Durch einfache Multiplikation können Sie sich leicht überzeugen, dass wir die Wahrheit gesagt haben: 758 717 = 761 x 997. Diese Eigenschaft eines Problems, eine Lösung zu besitzen, die - wenn man sie einmal hat - leicht überprüft werden kann, ist die definierende Eigenschaft der Klasse NP. Was für ZUSAMMENGESETZTE ZAHL gilt, gilt auch für die Geheimnummer Ihrer Kreditkarte. Wenn ein Taschendieb Ihre Kreditkarte und einen Zettel mit einer vierstelligen Zahl erbeutet, kann er leicht überprüfen, ob diese Nummer die zur Karte passende Geheimzahl ist. Er braucht sie einfach nur am Geldautomaten auszuprobieren.

Die Aussage "P gleich NP", bedeutet also: Wenn ich stets, d.h. für jede konkrete Aufgabe eines jeden Problems, von einer möglichen Lösung - wie auch immer ich an sie gelangt bin - leicht überprüfen kann, ob sie meine Aufgabe wirklich löst, dann kann ich stets sogar Lösungen effizient berechnen. ZUSAMMENGESETZTE ZAHL ist in NP, weil man für drei Zahlen *n*, *q* und *r* leicht überprüfen kann, ob $n = q \times r$ ist. Ist aber ZUSAMMENGESETZTE ZAHL auch in P? Die Antwort ist "ja", ZUSAMMENGESETZTE ZAHL kann effizient gelöst werden, aber das weiß man erst seit 2002. Sind unsere Geheimcodes also jetzt unsicher? Die überraschende Antwort: Das wissen wir nicht. Zwar lässt sich jetzt effizient feststellen, ob eine gegebene Zahl eine Primzahl ist oder nicht. Aber eine zusammengesetzte Zahl zu zerlegen, also ihre Teiler zu finden, das ist etwas ganz anderes. Formal ist das Problem "Gegeben sei eine zusammengesetzte Zahl *n*, gebe zwei "nicht triviale" Teiler an!" zwar kein Entscheidungsproblem, aber mit einem Trick kann man es auf ein

solches zurückführen, das in NP liegt. Aber ob dieses Problem - nennen wir es FAKTORISIERUNG - zu P gehört, weiß niemand.

Was könnte also passieren? Es könnte sein, dass es gelingt zu zeigen, dass P=NP gilt, und dann könnten alle gängigen Kryptographiesysteme effizient geknackt werden. Die praktischen Auswirkungen sind kaum vorstellbar! Es könnte aber auch sein, dass es Ihnen gelingt zu zeigen, dass FAKTORISIERUNG nicht in P liegt. Dann kann man prinzipiell immer sicherere Geheimcodes konstruieren und wäre den "Entschlüsselern" immer einen Schritt voraus. Und natürlich hätten Sie auch eine Million Dollar verdient, und das völlig zu Recht!

Unter den Problemen aus NP gibt es schwierigste, nämlich solche, die bereits P = NP erzwingen, wenn es für sie einen effizienten Algorithmus gibt; sie heißen NP-vollständig. Es ist nicht bekannt, ob FAKTORISIERUNG hierzu gehört. Das Problem des Handlungsreisenden (Traveling Salesman Problem), eine gegebene Zahl von "Städten" auf kürzest möglichem Weg zu besuchen, ist aber NP-vollständig, ebenfalls das Spiel Minesweeper und ferner eine große Anzahl von sehr praktischen Problemen aus der Industrie, der Wirtschaft, der Medizin, der Archäologie, der Biologie etc. (Mehr zu diesem Thema finden Sie hier.)

Professor Dr. Ehrhard Behrends,
FU Berlin.

Professor Dr. Peter Gritzmann,
TU München.