Sicherheit ohne Grenzen

Vertraulichkeit und Authentizität mit mathematischen Methoden

Von Albrecht Beutelspacher

Durch grell aufgemachte Berichte über Hacker und Viren ist auch einer breiten Öffentlichkeit inzwischen drastisch vor Augen geführt worden, daß Computer nicht a priori sicher sind. Das ist ein Problem, das wir nicht als internes Problem der Rechenzentren abtun können; denn es betrifft uns alle: Computer steuern Fabriken und Kraftwerke, Computer berechnen unsere Lohn- und Gehaltsauszüge, und spätestens hier wird jeder hellhörig und möchte sicher gehen, daß sein Gehalt richtig berechnet wurde. Auch im täglichen Leben spielt Datensicherheit eine große Rolle, und zwar insbesondere im Zahlungsverkehr: Wir wollen sicher sein, daß bei den Geldausgabeautomaten oder beim Bezahlen mit „electronic cash" an der Tankstelle kein Mißbrauch möglich ist; und wir wollen sicher sein, daß jeder Geldschein, den wir erhalten, ein gültiges Zahlungsmittel ist. Diese bunte Palette von Beispielen macht klar, daß Datensicherheit ein wichtiges und umfassendes Gebiet ist. Daher ist es kein Wunder, daß sich die Wissenschaft von der Sicherheit der Daten, nämlich die Kryptologie, in den letzten Jahren zu einem neuen zentralen Forschungsgebiet entwickelt hat.

Das Ziel der Kryptologie ist, Mechanismen zu entwickeln, welche die oben geschilderten Bedrohungen wirkungslos machen. Die von der Kryptologie eingesetzten Methoden stammen aus der Technik, der Informatik, überraschenderweise aber zu einem guten und entscheidenden Teil aus der Mathematik, und was noch überraschender ist, aus Teilen der Mathematik, die man früher – sei es verächtlich, sei es stolz – als „reine Mathematik" bezeichnet hat.

Die Kryptologie hat zwei Hauptziele. Das erste besteht darin, die Vertraulichkeit von Daten zu gewährleisten. Dies ist ein klassisches und altes Gebiet, das vor allem von militärischen Interessen gefördert wurde. Schon C. Julius Caesar hat vor rund 2000 Jahren gewisse Texte chiffriert, und zwar so, daß er jeden Buchstaben des Alphabets durch einen anderen ersetzt hat. Genauer gesagt hat er eine Zahl k – den Schlüssel – gewählt und dann von jedem Buchstaben des Klartexts im Alphabet um k Stellen weiter gezählt und den so erzielten Buchstaben als Geheimtextbuchstaben genommen.

Ist k = 2, so wird aus *A* der Buchstabe *C*, aus *B* wird *D*, usw. Aus dem jedem Lateinschüler unauslöschlich im Gedächtnis verankerten Satz

GALLIA EST OMNIS DIVISA IN PARTES TRES

würde also das scheinbare Kauderwelsch

ICNNKC GUV QOPKU FKXKUC KP RCTVGU VTGU.

Wenn man den Schlüssel k – in unserem Fall also die Zahl 2 – kennt, kann man durch Rückwärtszählen diesem Buchstabensalat wieder seinen scheinbar abhandengekommenen Sinn verleihen.

Aber es geht auch ohne: Selbst wenn man den Schlüssel nicht kennt, kann man durch systematisches Ausprobieren oder einfaches Auswerten der Buchstabenhäufigkeiten den Geheimtext entschlüsseln. Das ist so einfach, daß schon Caesar darauf hätte kommen müssen.

Heute gibt es viel bessere Algorithmen zur Verschlüsselung, die auch mit der besten Mathematik und den schnellsten Computern nicht zu knacken sind. Der berühmteste Algorithmus ist der DES (Data Encryption Standard), der seit vielen Jahren äußerst erfolgreich eingesetzt wird, vor allem im Bankenbereich.

Das zweite Ziel der Kryptographie heißt Authentikation. Hier ist das Ziel, die Authentizität von Daten – das heißt ihren Ursprung und ihre Unverändertheit – zu garantieren. Diese zweite Komponente hat in den letzten Jahren die erste sowohl in der Praxis als auch in der Theorie in den Hintergrund gedrängt.

Daß Authentizität von Daten in der Praxis oft wichtiger als Vertraulichkeit ist, macht das folgende Beispiel klar: Es ist relativ uninteressant, die Überweisung, die monatlich von der Zentralen Besoldungsstelle auf mein Konto überwiesen wird, zu verschlüsseln; denn mein Gehalt kann – jedenfalls größenordnungsmäßig – aus öffentlichen Listen erschlossen werden. Es ist jedoch äußerst wichtig zu garantieren, daß auf dem Übertragungsweg

keine (böswilligen) Veränderungen am Betrag oder an der Kontonummer vorgenommen werden, denn sonst würde mindestens einer der Beteiligten sich zu Recht beschweren.

Aber auch in der theoretischen Grundlegung hat die Authentizität in den letzten Jahren die wichtigste Rolle gespielt. Durch das Konzept einer „elektronischen Unterschrift" hat man dies begrifflich gefaßt.

Die Rolle der Mathematik in der Kryptologie

Was hat eigentlich die Mathematik mit Kryptologie zu tun? Könnte man die Ziele der Vertraulichkeit und Authentizität nicht auch ganz anders erreichen? Doch, es gibt viele andere Mechanismen für Vertraulichkeit und Authentizität. Das reicht von organisatorischen Maßnahmen wie dem Einsatz von sicherheitsüberprüftem Personal, Sicherheit der Gebäude, usw. bis zu ausgeklügelten technischen Maßnahmen. So ist zum Beispiel ein Wasserzeichen im Geldschein oder das Hologramm in einer ec-Karte ein Mittel, um die Authentizität, d.h. die Unfälschbarkeit eines Geldscheins bzw. einer Karte, zu gewährleisten.

Aber hier zeigt sich auch der Nachteil dieser Methoden besonders deutlich. In letzter Zeit mehren sich die Berichte über alarmierend zunehmende Fälschungen von Banknoten mit Hilfe von Farbkopierern. Das bedeutet: Eine neue Technologie kann „beste Sicherheit" von heute auf morgen zunichte machen.

Das ist bei Sicherheitsmechanismen, die auf mathematischen Verfahren beruhen, grundsätzlich nicht der Fall. Denn das Charakteristische an der Mathematik ist, daß dort Aussagen rein logisch b e w i e s e n werden. Das bedeutet, daß die Gültigkeit eines mathematischen Resultats nicht von „Expertenmeinungen" abhängt und schon gar nicht durch einen Technologiesprung außer Kraft gesetzt werden kann.

Für die Kryptologie bedeutet das insbesondere: Kryptologische Verfahren zur Vertraulichkeit oder Authentizität sind grundsätzlich beweisbar sicher. Man muß allerdings der Ehrlichkeit halber hinzufügen, daß bis jetzt nur wenige Verfahren gefunden wurden, die sowohl beweisbar sicher als auch praktikabel sind.

Ein weiterer Vorteil ist der, daß man kryptologische Verfahren im Prinzip „beliebig sicher" machen kann. Wenn sich eines Tages das Hologramm einer ec-Karte als fälschbar herausstellen sollte, hätte es keinen Sinn, von nun an Karten mit zwei Hologrammen zu produzieren. In der Kryptologie kann man aber durch Vergrößerung des Schlüssels prinzipiell die Sicherheit beliebig hoch treiben.

Projekte an der Universität Gießen

Im Mathematischen Institut der Universität Gießen beschäftigt sich eine Arbeitsgruppe an der Professur für Geometrie und Diskrete Mathematik (Professor Albrecht Beutelspacher) mit modernen Methoden der Kryptologie. Besonders günstig ist der Umstand, daß hier mathematisches Know-how und praktische Erfahrung zusammenkommen. Prof. Beutelspacher war drei Jahre lang im Forschungslabor der Firma Siemens in München verantwortlich für Kryptologie tätig. Eine enge Zusammenarbeit besteht nicht nur mit Siemens, sondern auch mit dem Forschungsinstitut der Deutschen Bundespost TELEKOM in Darmstadt. Zwei Projekte verdienen es, besonders herausgestellt zu wurden; sie wurden auch am Hessischen Hochschulstand auf der diesjährigen CeBIT in Hannover gezeigt.

Das erste Projekt behandelt den sicheren Zugang zu Geheimnissen. Aus dem täglichen Leben kennt man die Methode, geheime Dinge in einem Tresor sicher zu verwahren. In gewissen Situationen wird die Sicherheit dadurch erhöht, daß man ein Vieraugenprinzip einführt: Um den Tresor zu öffnen, sind zwei Personen notwendig, etwa der Besitzer des Geheimnisses und ein Bankangestellter. Dies kann zum Beispiel so realisiert werden, daß beide ihre individuellen Geheimcodes eingeben müssen.

Dieses Prinzip kann man mit mathematischen Methoden in einer sehr komfortablen Weise verallgemeinern. Man kann Systeme konstruieren, die sich von dem üblichen Vieraugenprizip in drei Punkten unterscheiden:

- Man kann beliebig viele Personen zulassen. Es muß also nicht so sein, daß immer Herr Müller und Frau Meier zusammenkommen müssen, sondern es reicht zum Beispiel, wenn zwei beliebige der Personen Herr Müller, Frau Maier, Herr Schulze, Frau Becker ihre Zustimmung geben. Damit wird das System natürlich viel flexibler, denn ein krankheits- oder urlaubsbedingter Ausfall von Herrn Schulze bringt nicht das gesamte System zum Erliegen.

- Man kann den Schwellenwert beliebig erhöhen. Wenn die Sicherheit des Systems verlangt, daß die Anwendung nur dann anläuft, wenn mindestens drei Personen ihre Zustimmung geben, so kann man ohne weiteres Systeme entwerfen, die dies realisieren. Allgemein gibt es solche Syteme für einen beliebigen Schwellenwert t. Das bedeutet, daß in einem solchen System das Geheimnis nur freigegeben wird, wenn mindestens t Personen zustimmen.

Besonders bemerkenswert ist, daß in diesen mathematischen Systemen jeder Teilnehmer nach wie vor nur einen „mathematischen Schlüssel" hat. Wenn man ein entsprechendes System mit mechanischen Schlüsseln realisieren wollte, wüchse die Anzahl der Schlüssel, die ein einzelner Benutzer besitzen muß, schnell ins völlig Unpraktikable. Das folgende Beispiel macht dies drastisch klar: Um mechanisch ein System mit Schwellenwert t = 5 und elf Peronen zu realisieren, müßte jeder einzelne 252 Schlüssel besitzen; der „Tresor" müßte sage und schreibe 462 Schlösser besitzen. Gegenüber dieser Monstrosität zeichnet sich die mathematische Lösung, bei der jeder Benutzer nur einen „Schlüssel" braucht und auch der Tresor nur ein „Schloß" besitzen muß, durch bewundernswerte Einfachheit und Eleganz aus. Diese mathematischen Systeme sind aber nicht nur elegant, sondern auch sicher:

- Die Sicherheit eines Schwellenwertschemas kann auf jedes beliebige Niveau gesteigert werden. Natürlich gibt es im strengen Sinn keine 100prozentige Sicherheit. Ein Angreifer könnte Glück haben und bei einem gewöhnlichen Tresor die Zahlenkombination raten. Vielleicht hat er auch bessere Kenntnisse und kann die Zahlenkombination durch andere Methoden leichter herausbekommen. Bei den mathematischen Systemen ist es so: Wenn ein Anwender verlangt, daß die Sicherheit höchstens 1 zu einer Million sein soll, so können wir ihm ein System liefern, das g a r a n t i e r t diese Sicherheit bietet; wenn er vorsichtiger ist, und eine Betrugssicherheit von 1 zu 100 Milliarden will, so kann er auch das haben. Man muß sich dabei klarmachen, daß schon 1 zu einer Million eine extrem hohe Sicherheit ist: Die Wahrscheinlichkeit (in Deutschland!) einen Unfall im Haushalt mit tödlichem Ausgang zu erleiden, ist nur 1 zu 10.000.

Dabei ist alles ganz einfach zu programmieren. Auf der CeBIT wurde der Zugang zu einem Tresor gezeigt. Dazu sind Kärtchen mit teilnehmerspezifischen Geheimzahlen vorbereitet; wenn zwei dieser Geheimcodes eingegeben werden, öffnet sich die Tür des Tresors – sonst nicht. Das Sicherheitsniveau ist 1 zu 2^{64}, das heißt etwa 1 zu 16 Millionen.*

Das zweite Projekt betrifft elektronische Schecks. Hier wird eine überzeugende Lösung des folgenden praktischen Problems angeboten: Wenn immer mehr Zahlungsvorgänge nicht mehr in Papierform, sondern in elektronischer Form abgewickelt werden, stellt sich das Problem der Sicherheit ganz neu. Im normalen Zahlungsverkehr haben sich seit Jahrhunderten gewisse Formen eingespielt und bewährt, die einen sicheren Zahlungsverkehr gewährleisten. Diese Methoden können nicht ohne weiteres für die Elektronik übernommen werden.

* Unser Tresor ist aus Fischer-Technik-Steinen gefertigt, die freundlicherweise Dr. Artur Fischer, Ehrendoktor der Universität Gießen, zur Verfügung gestellt hat.

Ein besonders drängendes Problem ist das der Echtheit eines elektronischen Schecks. Kann man einem Datensatz – also letztlich einer Zahl – ansehen, ob er garantiert von dem angegebenen Sender kommt und ob der Sender den Scheck wirklich mit dem Betrag losgeschickt hat, mit dem er bei der Bank angekommen ist? Zur Lösung dieser Probleme reicht es nicht, daß der Absender und der Betrag aus dem Datensatz erkennbar ist; vielmehr müssen beide auch garantiert unverändert beim Empfänger ankommen. Ein Betrüger darf keine Chance haben, bei einem gültigen elektronischen Scheck den Absender oder den Betrag zu ändern. Die Lösung dieser Probleme ist offenbar eine notwendige Vorbedingung für die Einführung eines elektronischen Zahlungssystems.

Der grundsätzliche Lösungsansatz sieht dabei so aus, daß der Sender nicht nur die nackten Daten, Name und Betrag, schickt, sondern diese zusätzlich elektronisch „unterschreibt". Darunter versteht man nicht die digitalisierte handschriftliche Unterschrift, sondern einen raffinierten mathematischen Mechanismus, der im folgenden beschrieben wird.

Um den Mechanismus anzuwenden, braucht sowohl der Aussteller des Schecks als auch die Bank, bei der der elektronische Scheck eingelöst werden soll, einen kryptographischen Algorithmus f und einen geheimen Schlüssel. Der Aussteller des Schecks berechnet aus den Scheckdaten mittels des geheimen Schlüssels einen Prüfwert, die „Unterschrift":

Prüfwert
= f(Scheckdaten, geheimer Schlüssel).

Der vollständige elektronische Scheck besteht dann aus den Scheckdaten zusamen mit dem Prüfwert. Ein Angreifer kann einen solchen Scheck nicht fälschen, da er den geheimen Schlüssel nicht kennt, und also zu anderen Scheckdaten keinen passenden Prüfwert berechnen kann. Demgegenüber kann die Bank die Scheckdaten verifizieren, da sie ebenfalls im Besitz des geheimen Schlüssels ist.

Die Mathematik stellt Strukturen zur Verfügung, mit denen man solche optimalen Authentikationssysteme konstruieren kann.

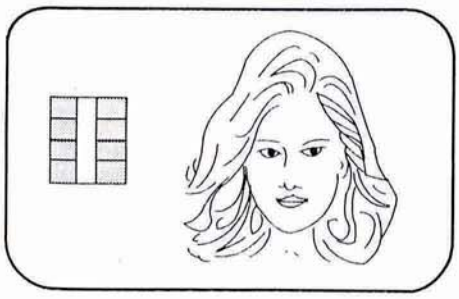

Abb. 1: Auch über Chipkarten wird an der Professur für Geometrie und Diskrete Mathematik in Gießen geforscht; in Zusammenarbeit mit der Deutschen Bundespost TELEKOM wurde auf der CeBIT auch ein Chipkartenzugang gezeigt.

Zwei Geheimcodes müssen in den Computer eingegeben werden, dann öffnet sich die Tür des Tresors. *Foto: Lauterbach*

Ausblick

Welche Art von Mathematik wird in der Kryptologie eingesetzt? Überraschenderweise spielen bei diesen Anwendungen Teile der „reinen" Mathematik die entscheidende Rolle. Es handelt sich dabei um die sog. diskrete Mathematik, die prädestiniert dafür ist, Anwendungen für Computer zu erforschen. Speziell in den Anwendungen zur Datensicherheit sind zahlentheoretische und geometrische Methoden der diskreten Mathematik von besonderer Wichtigkeit. Dies ist ein Grund, weshalb Mathematiker die Entwicklung der Kryptologie der letzten 20 Jahre geprägt haben.

Ein anderer Impuls kommt von der Technik, insbesondere der Halbleitertechnik. Durch die immer höhere Integrationsdichte können heute Chips produziert werden, die in eine Plastikkarte im üblichen Scheckkartenformat eingebettet werden können. Diese echten Minicomputer nennt man Chipkarten. „Einfache" Chipkarten sind heute als vorbezahlte Telefonkarten millionenfach verbreitet. Für die hier beschriebenen Anwendungen braucht man „intelligentere" Chipkarten, die es aber auch schon gibt (siehe Abb. 1).

Literatur:

BEUTELSPACHER, A.: Kryptologie. 2. Aufl. 1991, Verlag Vieweg

BEUTELSPACHER, A., KERSTEN, A., PFAU, A.: Chipkarten als Sicherheitswerkzeug. Springer-Verlag 1991.

Zum Autor:

Prof. Dr. Albrecht Beutelspacher: *Geboren 1950 in Tübingen; 1969 bis 1973 Studium der Mathematik, Physik und Philosophie in Tübingen, 1973 bis 1985 wissenschaftlicher Mitarbeiter, Hochschulassistent und Professor auf Zeit an der Universität Mainz, 1986 bis 1988 Mitarbeiter im Zentralbereich Forschung der Siemens AG in München; seit 1988 Professor für Geometrie und Diskrete Mathematik im Fachbereich Mathematik der Justus-Liebig-Universität Gießen. In seiner Arbeitsgruppe werden schwerpunktmäßig drei Gebiete bearbeitet: endliche Geometrie, Kryptographie und symbolische Inzidenzgeometrie (Geometrie auf dem Rechner). Ein wichtiger Aspekt ist die Frage, wie die theoretische Mathematik für praktische Anwendungen nutzbar gemacht werden kann. Dies wird u. a. in zwei größeren Projekten mit der Siemens AG und der Deutschen Bundespost TELEKOM bearbeitet.*