KRYPTOGRAPHIE UND EULERS ZAHLENTHEORIE

HANSPETER KRAFT

Die Idee des *öffentlichen Schlüssels* besteht darin, dass eine Person B einen Schlüssel öffentlich zur Verfügung stellt, mit dem jede andere Person eine Nachricht so verschlüsseln kann, dass nur die Person B diese Nachricht lesen kann. Die bekannteste Realisierung ist der sogenannte RSA-Schlüssel, welcher auf Rivest, Shamir und Adleman zurückgeht, [RSA78]. Die Grundlage dazu ist eine Formel von Euler sowie die Existenz bestimmter *Einweg-Funktionen*.

Die Eulersche Formel

Diese Formel besagt folgendes. Für beliebige teilerfremde ganze Zahlen a und n gilt

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Dabei ist $\varphi(n)$ gleich der Anzahl der zu n teilerfremden Zahlen b zwischen 1 und n. Weiter bedeutet die Kongruenz $a \equiv b \mod n$, dass die beiden Zahlen a und b bis auf Vielfache von n übereinstimmen, oder – was aufs Gleiche herauskommt, dass die Differenz $a-b$ durch n teilbar ist.

Beispiele.

(1) Sei $a = 5$ und $n = 6$. Dann sind $\{1, 5\}$ zu 6 teilerfremd, also $\varphi(6) = 2$, und es gilt $5^2 = 25 \equiv 1 \mod 6$.

(2) Sei $a = 2$ und $n = 15$. Dann sind $\{1, 2, 4, 7, 8, 11, 13, 14\}$ die zu n teilerfremden Zahlen, also ist $\varphi(n) = 8$. Und man rechnet leicht nach, dass $2^8 \equiv 1 \mod 15$ ist.

(3) Ist $n = p$ eine Primzahl, so sind alle Zahle $b < p$ zu p teilerfremd, also ist $\varphi(p) = p - 1$. Ist $n = pq$ ein Produkt von zwei verschiedenen Primzahlen, dann ist $\varphi(n) = (p-1)(q-1)$ (Übung!). Beides war natürlich Euler bekannt.

Einweg-Funktionen

In der modernen Kryptographie spielen sogenannte „Einweg-Funktionen" eine zentrale Rolle. Das sind Funktionen, die sich zwar leicht bestimmen lassen, deren Umkehrfunktion aber innert nützlicher Frist nicht berechenbar ist.

Eine solche Funktion ist das Produkt von zwei grossen Primzahlen $n = pq$. Es ist heute kein Problem 100-stellige Primzahlen herzustellen und solche Zahlen auch zu multiplizieren, denn moderne Primzahltests dauern nur Millisekunden, auch bei 100-stelligen Zahlen. Es gibt aber keine bekannten Methoden um innert vernünftiger Zeit aus dem Produkt $n = pq$ die beiden Primfaktoren p und q zu berechnen.

Eine andere solche Funktion ist das Potenzieren $x \mapsto x^s \mod n$, wobei wiederum s und n grosse Zahlen sind. Die Berechnung dauert Millisekunden; für die Umkehrfunktion, also die Bestimmung von x aus x^s bei bekanntem s würde es Milliarden von Jahren dauern. Dasselbe gilt für die Funktion $x \mapsto s^x \mod n$.

Die RSA-Verschlüsselung

Hierzu wählt die Person B zwei grosse Primzahlen p und q und berechnet das Produkt $n = pq$ sowie $\varphi(n) = (p-1)(q-1)$. Als zweites wählt B eine Zahl s, die teilerfremd zu $\varphi(n)$ ist. Der *öffentliche Schlüssel* ist dann das Paar (n, s). Die beiden Primfaktoren p und q sind jedoch geheim und nur der Person B bekannt.

Will nun eine beliebige Person eine geheime Nachricht in Form einer Zahl x an B senden, so geht sie folgendermassen vor. Sie berechnet $y = x^s \mod n$ unter Verwendung des öffentlichen Schlüssels (n, s). Und diese Zahl y schickt sie an die Person B.

Wie wir oben bemerkt haben, ist es nicht möglich, mit heute bekannten Methoden – auch mit den schnellsten Rechnern – innert nützlicher Frist aus der Potenz $y = x^s$ die Zahl x zu bestimmen. Kennt man jedoch die Primzahlzerlegung $n = pq$, welche allerdings nur B bekannt sein sollte, so kann man in der Tat x sehr einfach berechnen. Dazu löst B die Gleichung $sd \equiv 1 \mod \varphi(n)$, d.h. sie bestimmt ein d mit der Eigenschaft $sd - 1 = k\varphi(n)$ für ein geeignetes k. Mit der Eulerschen Formel folgt nun aus bekannten Regeln des Potenzrechnens

$$y^d = x^{sd} = x^{1+k\varphi(n)} = x\,(x^{\varphi(n)})^k \equiv x \mod n,$$

womit B die Nachricht x entschlüsselt hat.[1]

Etwas ausführlicher ist das Verfahren im Artikel [Kra00] beschrieben, welcher im Anhang abgedruckt ist (→ pdf).

[1] Für die Anwendung der Eulerschen Formel muss x teilerfremd zu n sein. Man sollte daher für x nur Zahlen zulassen, die weniger als halb soviele Stellen haben wie n.

Pretty Good Privacy – PGP

Eine Anwendung dieser Idee der öffentlichen Schlüssel ist das Verschlüsselungsprogramm PGP von Phil Zimmermann [Zim99]. Dieses ist öffentlich zugänglich und kann z.B. privat zur Verschlüsselung der eigenen Email verwendet werden. Das Verfahren ist auf Wikipedia gut beschrieben (→ PGP).

Öffentlicher Schlüsseltausch

Das Problem bei der geheimen Kommunikation ist nicht das Verfahren selber, sondern die Tatsache, dass Sender und Empfänger mit demselben Schlüssel arbeiten, und dieser also irgendwie ausgetauscht werden muss. Solange es um wenige Sender und Empfänger geht, etwa bei militärischen Anwendungen, ist das noch machbar, obwohl auch dort die *Schlüsselverwaltung* ein zentrales Problem ist und die Schwachstelle der Geheimhaltung darstellt.

In der modernen Kommunikation, etwa bei Bankgeschäften oder beim Einkauf übers Internet, wollen jedoch viele Partner geheime Informationen austauschen, auch Partner, die sich gegenseitig gar nicht kennen. Es ist offensichtlich, dass die klassischen Methoden sich hier nicht anwenden lassen.

Die Idee eines *öffentlichen Schlüsseltausches*, d.h. des Austausches eines geheimen Schlüssels über ein öffentliches Netzwerk, geht auf Diffie-Hellman und Merkle zurück, [DH76], [Mer78]. Die Realisierung von Diffie-Hellman beruht ebenfalls auf einfachen zahlentheoretischen Sätzen in Kombination mit Einweg-Funktionen. Eine Beschreibung des Verfahrens findet man ebenfalls in [Kra00]; der Artikel ist im Anhang abgedruckt (→ pdf).

Zur Geschichte der Eulerschen Formel[2]

Die oben beschriebene Eulersche Formel findet man in den beiden Arbeiten [Eul41] und [Eul63], welche im Band I 2 der Opera Omnia abgedruckt sind. Das „Theorema 11" aus [Eul63] lautet folgendermassen:

THEOREMA 11

55. *Si fuerit N ad x numerus primus et n numerus partium ad N primarum, tum potestas x^n unitate minuta semper per numerum N erit divisibilis.*[1])

[2]Die nachstehenden Angaben verdanke ich Martin Mattmüller.

In der späteren Arbeit [Eul84] führt Euler die Bezeichnung πn für die Anzahl der zu n teilerfremden Zahlen $\leq n$ ein, welche wir oben mit $\varphi(n)$ bezeichnet haben, und bestimmt die Werte für alle Zahlen $n \leq 100$.[3]

3. Hinc igitur ista quaestio nascitur: ut, proposito quocunque numero D, multitudo numerorum ipso minorum ad eumque simul primorum assignetur. Quod quo facilius praestari possit, denotet character πD multitudinem istam numerorum ipso D minorum, et qui cum eo nullum habeant divisorem communem. Ac primo quidem manifestum est, si fuerit D numerus primus, fore $\pi D = D - 1$. Ante autem quam numeros compositos examinemus, valores huius characteris πD pro omnibus numeris centenario non maioribus apponamus:

$\pi\ 1 = 0$	$\pi\ 21 = 12$	$\pi\ 41 = 40$	$\pi\ 61 = 60$	$\pi\ 81 = 54$
$\pi\ 2 = 1$	$\pi\ 22 = 10$	$\pi\ 42 = 12$	$\pi\ 62 = 30$	$\pi\ 82 = 40$
$\pi\ 3 = 2$	$\pi\ 23 = 22$	$\pi\ 43 = 42$	$\pi\ 63 = 36$	$\pi\ 83 = 82$
$\pi\ 4 = 2$	$\pi\ 24 = 8$	$\pi\ 44 = 20$	$\pi\ 64 = 32$	$\pi\ 84 = 24$
$\pi\ 5 = 4$	$\pi\ 25 = 20$	$\pi\ 45 = 24$	$\pi\ 65 = 48$	$\pi\ 85 = 64$
$\pi\ 6 = 2$	$\pi\ 26 = 12$	$\pi\ 46 = 22$	$\pi\ 66 = 20$	$\pi\ 86 = 42$
$\pi\ 7 = 6$	$\pi\ 27 = 18$	$\pi\ 47 = 46$	$\pi\ 67 = 66$	$\pi\ 87 = 56$
$\pi\ 8 = 4$	$\pi\ 28 = 12$	$\pi\ 48 = 16$	$\pi\ 68 = 32$	$\pi\ 88 = 40$
$\pi\ 9 = 6$	$\pi\ 29 = 28$	$\pi\ 49 = 42$	$\pi\ 69 = 44$	$\pi\ 89 = 88$
$\pi\ 10 = 4$	$\pi\ 30 = 8$	$\pi\ 50 = 20$	$\pi\ 70 = 24$	$\pi\ 90 = 24$
$\pi\ 11 = 10$	$\pi\ 31 = 30$	$\pi\ 51 = 32$	$\pi\ 71 = 70$	$\pi\ 91 = 72$
$\pi\ 12 = 4$	$\pi\ 32 = 16$	$\pi\ 52 = 24$	$\pi\ 72 = 24$	$\pi\ 92 = 44$
$\pi\ 13 = 12$	$\pi\ 33 = 20$	$\pi\ 53 = 52$	$\pi\ 73 = 72$	$\pi\ 93 = 60$
$\pi\ 14 = 6$	$\pi\ 34 = 16$	$\pi\ 54 = 18$	$\pi\ 74 = 36$	$\pi\ 94 = 46$
$\pi\ 15 = 8$	$\pi\ 35 = 24$	$\pi\ 55 = 40$	$\pi\ 75 = 40$	$\pi\ 95 = 72$
$\pi\ 16 = 8$	$\pi\ 36 = 12$	$\pi\ 56 = 24$	$\pi\ 76 = 36$	$\pi\ 96 = 32$
$\pi\ 17 = 16$	$\pi\ 37 = 36$	$\pi\ 57 = 36$	$\pi\ 77 = 60$	$\pi\ 97 = 96$
$\pi\ 18 = 6$	$\pi\ 38 = 18$	$\pi\ 58 = 28$	$\pi\ 78 = 24$	$\pi\ 98 = 42$
$\pi\ 19 = 18$	$\pi\ 39 = 24$	$\pi\ 59 = 58$	$\pi\ 79 = 78$	$\pi\ 99 = 60$
$\pi\ 20 = 8$	$\pi\ 40 = 16$	$\pi\ 60 = 16$	$\pi\ 80 = 32$	$\pi 100 = 40$

[3]**Übersetzung:** *Daraus ergibt sich also die folgende Frage: Wenn irgend eine Zahl D gegeben ist, soll die Anzahl der Zahlen angegeben werden, die kleiner als sie und zugleich teilerfremd zu ihr sind. Um das leichter zu erreichen, bezeichne der Ausdruck πD diese Anzahl der Zahlen, welche kleiner sind als D und keinen gemeinsamen Teiler damit haben. Zunächst ist dann offensichtlich, dass, wenn D eine Primzahl ist, $\pi D = D - 1$ sein wird. Bevor wir aber die zusammengesetzten Zahlen überprüfen, wollen wir die Werte dieses Ausdrucks πD für alle Zahlen anfügen, die nicht grösser sind als* 100.

Literatur

[DH76] W. Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 6, 644–654.

[Eul41] Leonhard Euler, *Theorematum quorundam ad numeros primos spectantium demonstratio*, Commentarii academiae scientiarum Petropolitanae **8** ((1736), 1741), 141–146, E 54. Opera Omnia Ser. I, Vol. 2., p. 33–58.

[Eul63] ———, *Theoremata arithmetica nova methodo demonstrata*, Novi commentarii academiae scientiarum Petropolitanae **8** ((1770/1), 1763), 64–73, E 271. Opera Omnia Ser. I, Vol. 2., p. 531–555.

[Eul84] ———, *Speculationes circa quasdam insignes proprietates numerorum*, Acta academiae scientiarum Petropolitanae **4 II** ((1780: II), 1784), 38–48, E 564. Opera Omnia Ser. I, Vol. 7. p. 105–115.

[Kra00] Hanspeter Kraft, *Öffentliche Geheimhaltung*, Uni Nova, Wissenschaftsmagazin der Univ. Basel **87** (2000), 28–35.

[Mer78] R.C. Merkle, *Secure Communicatons over an Insecure Channel*, Communications of the ACM **21** (1978), no. 4, 294–299.

[RSA78] R. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.

[Zim99] Philip R. Zimmermann, *Why I Wrote PGP*, Essays on PGP (1999).

Öffentliche Geheimhaltung

Hanspeter Kraft

Die *Informationstheorie* beschäftigt sich mit der örtlichen und zeitlichen Übertragung von Information. Ein zentrales Teilgebiet ist die *Kryptographie*, welche sich mit der Sicherheit der Datenübertragung befasst, insbesondere also mit der Problematik der passiven Beeinträchtigung der Übermittlung durch Abhören und der aktiven Beeinflussung durch Fälschen. Bei all diesen Theorien spielt die Mathematik eine wichtige Rolle.

Geheimhaltung und Authentizität

Zwei grundsätzliche Fragen stehen im Vordergrund, nämlich die Frage der Geheimhaltung und die Frage der Authentizität:

– *Geheimhaltung*: Wie stellt der Sender sicher, dass nur der vorgesehene Empfänger die Nachricht lesen kann?
– *Authentizität*: Wie stellt der Empfänger sicher, dass die Nachricht vom angegebenen Sender stammt?

Diese Problematik ist keineswegs neu; sie hat die Geheimdienste aller Länder seit jeher beschäftigt. Mit der globalen Vernetzung und den beinahe unbeschränkten Möglichkeiten des Informationsaustausches, etwa per E-Mail oder über das Internet, hat diese Problematik jedoch völlig neue und ungeahnte Dimensionen angenommen.

Moderne Kryptographie

Was ist neu in der heutigen Situation, im Unterschied zur klassischen (meist militärischen) geheimen Nachrichtenübertragung?

– Die möglichen Gesprächspartner sind nicht zum Vorneherein schon festgelegt. Im Prinzip möchte jeder mit jedem sicher kommunizieren können.
– Die verwendeten Übertragungsmedien (elektrische Leitungen, Glasfaser, elektromagnetische Wellen, via Satellit) sind öffentlich, und die Netzwerke sind unüberschaubar. Der Benutzer muss damit rechnen, dass sie leicht abgehört werden können.

Die globale Verfügbarkeit von Information kommt also einher mit der wachsenden Unsicherheit, ob die erhaltene Information auch stimmt und vom angegebenen Absender stammt und ob umgekehrt die gesendete Information unverfälscht am richtigen Orte ankommt.

Man denke dabei etwa an die Benutzung von Kreditkarten bei Bankautomaten oder in Geschäften, an die Bestellung und Bezahlung von Waren über das Internet (E-Commerce), an die elektronische Börse, an den Schutz vor Kopien, an das Signieren von Verträgen über Netzwerke, an elektronische Abstimmungen und so weiter.

Sicherheit

Eine erste mögliche Massnahme zur Absicherung gegen Missbrauch ist das systematische Sammeln (und Speichern) von Informationen über die Vertragspartner (Kreditwürdigkeit!). Was dies tatsächlich bedeutet ist jedoch den meisten nicht bewusst:

– Ihre Kreditkartenfirma weiss genau, wann und wo Sie in den Ferien waren, was Ihr Hotel gekostet hat, in welchen Restaurants Sie essen gehen, wo Sie Ihre Kleider kaufen und wofür Sie wie viel Geld ausgeben.
– Damit der Betreiber Ihres Mobiltelefons genau abrechnen kann, macht er eine sorgfältige Aufzeichnung Ihrer Telefongespräche und kann damit problemlos Ihre dienstlichen Reiseaktivitäten rekonstruieren.
– Mit Kundenkarten der Form «Cumulus» speichern Firmen Ihr Kaufverhalten und benützen dies, um ihr Angebot (und die Preise) zu optimieren.
– Der Betreiber Ihres Kabelfernsehens kann problemlos feststellen, welche Sender und Programme Sie regelmässig anschauen.

Nimmt man alle diese Informationen zusammen, so kann man ein sehr detailliertes «Profil» von Ihnen erstellen, das Ihre Lebensgewohnheiten beinhaltet und Ihr Verhalten in bestimmten Situationen voraussagt. Von hier ist der Schritt zur unbemerkten Beeinflussung und Kontrolle nur noch ein kleiner!

Öffentliche Schlüssel

Es herrscht allgemein die Ansicht, dass diese Problematik in der Natur der Sache liegt, dass man sich also gegen Missbrauch nur absichern kann, wenn man bereit ist, gewisse Informationen über sich selbst preiszugeben.

Das Erstaunliche ist nun, dass diese Ansicht falsch ist. Die mathematische Theorie der «Public Keys» (d.h. der öffentlichen Schlüssel) ermöglicht einen sicheren Datenaustausch zwischen beliebigen Partnern, ohne dass die beiden sich kennen und persönliche Daten und Referenzen preisgeben müssen. Mehr noch, die Methode erlaubt auch die sichere und vertrauliche Verwendung von «digitalem Geld», das heisst die Bezahlung mit einer Art Kreditkarte, wobei das Kreditinstitut die Summe risikolos garantieren kann, ohne den Empfänger des Geldes zu kennen!

Es ist mir klar, dass das sehr unglaubwürdig tönt; es scheint dem gesunden Menschenverstand völlig zu widersprechen! Umso grossartiger ist die bahnbrechende Arbeit der beiden Mathematiker W. Diffie und M.E. Hellman aus dem Jahre 1976, in der die Idee des öffentlichen Schlüssels eingeführt und verschiedene Realisierungen dargestellt werden.

In den folgenden Abschnitten möchte ich diese geniale Idee an ein paar einfachen Beispielen vorstellen und erläutern. Zunächst müssen wir uns kurz über die Grundprinzipien der geheimen Nachrichtenübertragung unterhalten.

Geheime Nachrichtenübertragung

Um Information vom Sender zum Empfänger zu transportieren, wird diese zunächst *digitalisiert*. Dies bedeutet, dass der Text oder das Bild (oder die akustischen Signale) mittels eines elektronischen Gerätes (z.B. eines Computers) und geeigneter Software in eine Bitfolge, d.h. in eine Folge 00101101010011000101010010 01 … von Nullen und Einsen verwandelt wird. Diese Folge wird portionenweise über das Netzwerk verschickt und vom Empfänger mit entsprechendem Gerät und Software in die ursprüngliche Information zurückverwandelt. Dazu ist es gar nicht nötig, im Detail zu wissen, mit welchen Geräten und welcher Software die Digitalisierung gemacht wurde: Für Experten ist es kein Problem, aus der Bitfolge die ursprüngliche Information wieder herzustellen.

Chiffrierung

Für die *geheime* Nachrichtenübertragung braucht man daher eine «Chiffrierung». Darunter versteht man ein Verfahren, welches die gegebene Bitfolge, den *Klartext*, in eine neue Bitfolge, das *Chiffrat*, verwandelt und dieses an den Empfänger verschickt. Diese Umwandlung erfolgt nach einem wohldefinierten (bekannten) Algorithmus unter Verwendung eines (geheimen) *Schlüssels*, welcher in der Praxis selbst eine Bitfolge von bestimmter Länge ist. Verfügt der Empfänger ebenfalls über diesen Schlüssel, so kann er den Klartext wieder herstellen und somit die Nachricht entziffern (siehe Tafel I).

Solche Verfahren werden durch integrierte Schaltungen (Chips) und spezielle Software geliefert. Ein bekannter Chiffrieralgorithmus ist der DES (= Data Encryption Standard); er ist in vielen Geräten fest eingebaut.

Es gibt heute absolut sichere Chiffrierverfahren, mit denen schnell und risikolos über öffentliche Leitungen geheime Nachrichten übertragen werden können. Hierzu müssen allerdings Sender und Empfänger über einen *gemeinsamen geheimen Schlüssel* verfügen.

Die zentralen Probleme bei der geheimen Nachrichtenübertragung liegen nicht beim Chiffrierverfahren, sondern beim *Schlüsselaustausch* und bei der *Schlüsselverwaltung*.

Tafel I

Eine einfache Blockchiffer

Die Nachricht N sei als Folge von Ziffern gegeben, etwa

$$N = 13859834138728774128347712 3667.$$

Als Schlüssel verwenden wir die ersten 10 Stellen der Zahl

$$\pi = 3{,}141592653\ldots$$

(jede andere 10-stellige Zahl erfüllt den gleichen Zweck).

Der Algorithmus besteht darin, die obige Folge N in 10er-Blöcke einzuteilen und zu jedem Block den Schlüssel zu addieren, wobei die Addition ziffernweise erfolgt und die Überträge ignoriert werden, also 6 + 7 = 3 gesetzt wird:

Klartext:	$N =$	1385983413 '8728774128 '3477123667
Schlüssel:	$S =$	3141592653 '3141592653 '3141592653
Chiffrat:	$N + S =$	4426475066 '1869266771 '6518615210

Falls der Empfänger den Schlüssel S kennt, so kann er aus dem Chiffrat den Klartext N wieder herstellen, nämlich durch blockweise Subtraktion von

$$S = 3141592653,$$

wobei wiederum ziffernweise subtrahiert wird und gegebenenfalls 10 addiert wird, also 3 – 5 = –2 = 8 gesetzt wird:

Chiffrat:	$C =$	4426475066 '1869266771 '6518615210
Schlüssel:	$S =$	3141592653 '3141592653 '3141592653
Klartext:	$C - S =$	1385983413 '8728774128 '3477123667

Öffentlicher Schlüsselaustausch

Eine unglaubliche Geschichte

Stellen Sie sich nun folgende Situation vor. In einem grossen Raum sitzen viele Leute, alle mit einem Laptop und geeigneter Software ausgerüstet und alle auf dem gleichen Wissensstand. Nun möchte ein beliebiges Paar im Raum, etwa Alice und Bob, einen geheimen Schlüssel austauschen. Die beiden kennen sich nicht und haben bisher nie miteinander geredet.

Nun beginnen die beiden einen öffentlichen Dialog, der von allen Anwesenden mitgehört wird. Am Schluss haben Alice und Bob einen gemeinsamen geheimen Schlüssel, etwa eine 200-stellige Zahl, und keiner der Anwesenden hat die geringste Chance, diesen Schlüssel herauszufinden!

Wenn man dies zum ersten Mal hört, dann glaubt man das nicht. Im Gegenteil, es ist doch offensichtlich, dass dies nicht gehen kann, denn die Unterhaltung ist ja öffentlich, und deshalb sind alle Leute auch nach der Diskussion auf dem gleichen Kenntnisstand. Dass dies trotzdem möglich ist, beruht auf der schon oben angedeuteten genialen Idee der beiden Mathematiker Diffie und Hellman, die ich nun erläutern möchte. Dazu sind ein paar einfache «mathematische» Vorbereitungen nötig.

Mathematische Grundlagen

Die Grundlage für diese Methode ist das *Rechnen modulo N*, wobei *N* eine positive, meist sehr grosse Zahl ist (siehe Tafel II). Beim obigen Beispiel eines Chiffrierverfahrens haben wir z.B. die Ziffern modulo 10 addiert, d.h. wir haben mit nur einer Stelle gerechnet und alle Vielfachen von 10 ignoriert.

Das Rechnen modulo *N* eignet sich besonders für den Umgang mit grossen Zahlen. Andernfalls läuft man Gefahr, besonders beim Multiplizieren und Potenzieren, dass die Zahlen zu gross werden und nicht mehr gespeichert werden können. Im Folgenden ist das *Potenzieren modulo N* von entscheidender Bedeutung, also das Berechnen von Potenzen der Form $a^n = a\,a\,a\,a \ldots a \mod N$. Dabei wird die Zahl *a* sukzessive mit sich selber multipliziert, und zwar *n*-mal.

Tatsache 1:
Ein heutiger Laptop kann sehr schnell modulo *N* potenzieren, das heisst Zahlen der Form $a^n = a\,a\,a\,a \ldots a \pmod N$ ausrechnen. Für 1000-stellige Zahlen *a*, *n* und *N* dauert dies nur wenige Millisekunden.

Dies ist keineswegs offensichtlich. Würde man nämlich die Zahlen sukzessive miteinander multiplizieren, so müsste man *n* Multiplikationen von grossen Zahlen durchführen, und dies würde bei 1000-stelligen Zahlen selbst auf den schnellsten heutigen Rechnern etwa 10^{100} Jahre dauern! Dass dies so viel rascher geht, beruht auf einer sehr intelligenten Methode des Potenzierens, bei der die Anzahl der notwendigen Multiplikationen nur etwa der Stellenanzahl des Exponenten entspricht (siehe Tafel III).

Man beachte: 10^{100} ist eine Eins mit 100 Nullen!

Tafel II

Das Rechnen modulo *N*

Das Rechnen mit ganzen Zahlen modulo *N* besteht darin, dass man nach dem Ausführen der Rechenoperation vom Ergebnis so oft mal *N* subtrahiert (oder addiert, falls das Ergebnis negativ ist), bis man eine Zahl zwischen 0 und *N* erreicht.
$5 + 8 = 3 \pmod{10}$; $7 \cdot 8 = 1 \pmod{11}$
$3^3 = 1 \pmod{13}$, $(-11) \cdot 9 = 1 \pmod{100}$
Ist $N = 10^n$, das heisst eine 1 mit *n* Nullen, so bedeutet das Rechnen modulo *N*, dass man vom Ergebnis nur die letzten n Stellen betrachtet und alle anderen ignoriert.
$2^{10} = 24 \pmod{1000}$
In den Anwendungen ist *N* eine sehr grosse Zahl (mehrere hundert bis tausend Stellen). Dies hat den Vorteil, dass man zwar mit sehr grossen Zahlen arbeitet, die Grösse aber dennoch bei allen Rechenoperationen beschränkt bleibt, nämlich $\leq N$.

Tafel III

Schnelles Potenzieren

Das Potenzieren a^n kann auch für grosse Exponenten *n* sehr schnell durchgeführt werden. Ist zum Beispiel $n = 128$, so scheint man für die Berechnung von a^{128} total 127 Multiplikationen zu benötigen. In Tat und Wahrheit kommt man mit 7 Multiplikationen aus! Es gilt nämlich
$(((((((a^2)^2)^2)^2)^2)^2)^2 = a^{2^7} = a^{128}$
das heisst, man quadriert 7-mal hintereinander.

Ist der Exponent keine Zweierpotenz, so benutzt man die duadische Zerlegung. Es ist zum Beispiel $100 = 2^6 + 2^5 + 2$. Damit findet man durch «optimales Ausklammern»
$100 = 2^6 + 2^5 + 2 = ((2 + 1)2^4 + 1)2$
und erhält
$a^{100} = ((a^2 \cdot a)^{2^4} \cdot a)^2$,
was total 8 Multiplikationen benötigt!

Die Umkehrung des Potenzierens, also die Bestimmung des Exponenten n aus dem Ergebnis $b = a^n \pmod N$, heisst *diskreter Logarithmus*: $n = \log_a b \pmod N$.

Tatsache 2:
Es sind keine schnellen Algorithmen für die Berechnung des diskreten Logarithmus $\log_a b \pmod N$ bekannt. Für 200-stellige Zahlen a, b und N würden die schnellsten heutigen Rechner etwa 10^{100} Jahre brauchen.

Man beachte, dass dies eine gänzlich andere Aussage ist als die Tatsache 1! Die Mathematiker vermuten zwar, dass es keine schnellen Algorithmen für den diskreten Logarithmus gibt, aber bisher ist kein Beweis dafür gelungen.

Was hier vorliegt, ist eine so genannte *Einwegfunktion*, also eine Funktion – hier das Potenzieren $p(n) = a^n \pmod N$ mit dem Exponenten n –, die man auch für sehr grosse Werte von n schnell berechnen kann, deren Umkehrfunktion – hier der diskrete Logarithmus $l(b) = \log_a b \bmod N$ – jedoch nicht innert nützlicher Zeit berechenbar ist.

Das Verfahren

Damit haben wir alle Begriffe zusammen, um den oben angedeuteten *öffentlichen Schlüsselaustausch* zu beschreiben. Wir kehren zurück zu Alice und Bob und erleben folgenden Ablauf:

– Als erstes werden *öffentlich* zwei etwa 200-stellige Zahlen a und N bekannt gegeben, wobei a kleiner als N ist.
– Nun wird Alice gebeten, sich *im Geheimen* eine Zahl n der gleichen Grössenordnung zu notieren, und die gleiche Aufforderung geht an Bob, der sich eine Zahl m notiert. (Die Zahl n kennt also nur Alice und m kennt nur Bob, während die Zahlen a und N öffentlich bekannt sind.)
– Nun wird Alice aufgefordert, mit ihrem Laptop die Potenz $p = a^n \pmod N$ zu berechnen. Entsprechend berechnet Bob die Potenz $q = a^m \pmod N$. (Wie wir oben in «Tatsache 1» bemerkt haben, ist diese Berechnung leicht und schnell möglich.)
– Diese beiden Ergebnisse p und q werden nun zwischen Alice und Bob öffentlich ausgetauscht. Jedermann kennt also diese beiden Zahlen. (Wir haben oben in «Tatsache 2» bemerkt, dass es den Anwesenden (ausser Alice bzw. Bob) dennoch unmöglich ist, innert nützlicher Frist aus diesen Angaben die geheimen Zahlen n von Alice beziehungsweise m von Bob zu berechnen.)
– Nun nimmt Alice die Zahl q von Bob und berechnet, unter Benutzung ihrer geheimen Zahl n, die Potenz $s = q^n \pmod N$. Das entsprechende tut Bob: Er nimmt die Zahl p von Alice und berechnet $t = p^m \pmod N$. (Da die Zahlen n und m geheim sind, kann niemand anders diese Berechnung durchführen.)
– Behauptung: *Es gilt $s = t$, und dies ist der gemeinsame geheime Schlüssel*, den nur Alice und Bob kennen! Der Beweis beruht auf elementarem Potenzrechnen: $s = q^n = (a^m)^n = a^{(mn)} = a^{(nm)} = (a^n)^m = p^m = t \pmod N$

Eine typische Anwendung

Wenn man auf dem Internet Zahlungen und Bankgeschäfte erledigt, so verwendet man üblicherweise Passwörter. Nun muss man aber bedenken, dass der Verkehr auf dem Internet öffentlich ist und von einem Hacker leicht abgehört werden kann. Insbesondere kann dieser den Login-Namen und das Passwort herausfinden und den ganzen Datenverkehr mitverfolgen.

Um dies zu vermeiden, wird anders vorgegangen. Sobald man die entsprechende Stelle auf der Homepage der Bank anklickt, führen der Bankcomputer und der eigene PC einen öffentlichen Schlüsselaustausch durch, etwa nach dem oben beschriebenen Schema, und produzieren so einen gemeinsamen geheimen Schlüssel. Dieser wird dann benutzt, um mit einem bekannten Chiffrierverfahren, etwa dem DES, die weiteren Informationen verschlüsselt über das Internet zu schicken. (Voraussetzung ist natürlich, dass auf den verwendeten Computern die notwendige Software installiert ist, was bei den bekannten Browsern heute der Fall ist.)

Das gleiche Verfahren wird benutzt, wenn man über das Internet einkauft und dabei seine Kreditkartennummer sowie weitere persönliche Informationen mitteilt. Auch hier wird zunächst ein Schlüssel ausgetauscht und dann mit einem bekannten Chiffrierverfahren der weitere Datenverkehr verschlüsselt über das Netz gesendet.

Public Keys (öffentliche Schlüssel)

Die bisher betrachteten Chiffrierverfahren haben eines gemeinsam, nämlich dass man für das Verschlüsseln und das Entschlüsseln denselben Schlüssel benutzt. Wollen also 1000 Personen auf einem Netzwerk sicher miteinander kommunizieren, so muss für jedes Paar von Benutzern ein geheimer Schlüssel zur Verfügung gestellt werden, was total etwa eine halbe Million Schlüssel ergibt. Auf dem Netzwerk einer grossen Organisation oder gar auf dem Internet ist dies völlig undenkbar, nicht nur wegen der grossen Anzahl der Schlüssel, sondern vor allem wegen der Frage, wie man diese Schlüssel verwaltet und verteilt.

Wiederum legt dies die Schlussfolgerung nahe, dass das in der Natur der Sache liegt, dass es also keine sichere und geheime weltweite Kommunikation etwa via E-Mail geben kann. Und auch diese Schlussfolgerung ist falsch! Es waren ebenfalls die beiden Mathematiker Diffie und Hellman, die eine überraschende und wiederum geniale Lösung vorschlugen, nämlich die Idee des *öffentlichen Schlüssels*.

Die Grundidee

Die Grundidee ist sehr einfach: *Man finde ein Chiffrierverfahren mit ZWEI Schlüsseln, einem öffentlichen Chiffrierschlüssel zum Verschlüsseln und einem geheimen Dechiffrierschlüssel zum Entschlüsseln, wobei es auch bei Kenntnis des Chiffrierschlüssels (aber ohne Kenntnis des Dechiffrierschlüssels!) nicht möglich ist, einen verschlüsselten Text innert nützlicher Frist zu entziffern.*

Mit anderen Worten, mit dem Chiffrierschlüssel kann man chiffrieren, aber nicht dechiffrieren; das Chiffrierverfahren ist also eine *Einwegfunktion*, wie wir sie oben beim öffentlichen Schlüsseltausch kennen gelernt haben. Allerdings braucht man noch eine geheime Hintertür, welche es dank zusätzlichen Kenntnissen erlaubt, die Umkehrfunktion doch zu berechnen. Solche Funktionen haben den Namen «one-way trap door function» erhalten.

Wenn es so ein Verfahren gäbe, so wäre damit das Problem der geheimen Übermittlung von Nachrichten gelöst. Jeder potentielle Benutzer würde ein solches Paar von Schlüsseln kreieren, den Chiffrierschlüssel öffentlich bekannt geben, zum Beispiel im Telefonbuch, und den Dechiffrierschlüssel geheim halten. Will nun Alice an Bob eine Nachricht schicken, so verwendet sie den im Telefonbuch unter Bob angegebenen Schlüssel, um diese zu verschlüsseln. Dann ist sichergestellt, dass nur Bob diese Nachricht lesen kann.

Das tönt zwar sehr überzeugend, doch kann man sich nicht vorstellen, dass es so ein Verfahren gibt.

Das RSA-Kryptosystem

Im Jahre 1978 haben R.L. Rivest, A. Shamir und L.M. Adleman, drei Mathematiker am MIT, ein solches Verfahren angegeben. Es läuft heute unter dem Namen *RSA-Kryptosystem* und dient vor allem der Übermittlung von Schlüsseln für die klassischen Chiffrierverfahren, aber auch der Authentifizierung von Nachrichten und als digitale Unterschrift. Auf dieser Methode beruht die Sicherheit der heutigen Netzwerkkommunikation, insbesondere auf dem Internet. Ein solches Programm, das vor allem bei der E-Mail eingesetzt wird, ist öffentlich und läuft unter dem Namen «pgp» (= pretty good privacy).

Zur Beschreibung der RSA-Methode benutzen wir wiederum das Rechnen modulo N und benötigen zudem etwas elementare Zahlentheorie. (Die mathematischen Details werde ich im Folgenden unterschlagen.)

– Alice wählt zwei grosse Primzahlen p und q (etwa 150 Stellen) und berechnet die beiden Produkte $N = p \cdot q$ und $R = (p\text{-}1)(q\text{-}1)$. Weiter wählt Alice eine beliebige Zahl $d < N$ von der gleichen Grössenordnung, welche zudem zu R teilerfremd ist.
– Nun gibt Alice das Paar der Zahlen d und N öffentlich bekannt. Dieses Paar (d, N) bildet den *öffentlichen Schlüssel.*
– Das Chiffrierverfahren besteht nun in Folgendem: Will Bob die Zahl x ($< N$) an Alice übermitteln, so berechnet er die Potenz $y = x^d \pmod N$ und sendet dann die Zahl y an Alice. (Entsprechend wie beim diskreten Logarithmus ist es nicht möglich, aus der Kenntnis von y, d und N die Zahl x innert nützlicher Frist zu berechnen.)
– Alice kennt auch die Zahl R und bestimmt damit eine Zahl f mit der Eigenschaft, dass $d \cdot f = 1 \pmod R$ gilt. (Diese Berechnung ist mit wenig Aufwand möglich.)
– Behauptung: Es gilt $y^f = x \pmod N$. Also kann Alice aus der empfangenen Zahl y das ursprüngliche x bestimmen!

(Der Beweis dieser Behauptung beruht auf einem Satz von Euler, welcher den bekannten «Kleinen Satz von Fermat» verallgemeinert, siehe Tafel IV)

Bei der obigen Beschreibung wurde noch nicht klar gesagt, wieso nur Alice x aus y berechnen kann. Der Grund ist der folgende: Das einzige bekannte Verfahren besteht darin, dass man die Zahl $R = (p\text{-}1)(q\text{-}1)$ bestimmt und dann die Gleichung $d \cdot f = 1 \pmod R$ löst. Hierfür ist notwendig, dass man die beiden Primzahlen p und q kennt. Nun hat Alice aber nur das Produkt $N = p\,q$ bekannt gegeben. Es geht also darum, die Primzerlegung dieser etwa 300-stelligen Zahl zu bestimmen. Und hier liegt der entscheidende Punkt: Auch mit den schnellsten heutigen Rechnern und den besten bekannten Verfahren würde dies über 10^{10} Jahre dauern!

Authentifizierung und digitale Unterschrift

Die RSA-Methode lässt sich auch für die Authentifizierung von öffentlichen Informationen verwenden (digitale Unterschrift). Dabei geht es um folgendes Problem.

Alice möchte eine Nachricht verbreiten und zwar so, dass jedermann sicherstellen kann, dass die Nachricht wirklich von Alice stammt. Hierzu geht Alice folgendermassen vor:

– Auf den Text der Nachricht wendet Alice eine so genannte Hash-Funktion an, welche ebenfalls öffentlich bekannt ist und leicht berechnet werden kann. Das Ergebnis ist eine Zahl y.
– Nun berechnet Alice die Zahl $x = y^f \pmod N$ unter Verwendung ihres *geheimen* Schlüssels f. Diese Zahl x wird dann an den veröffentlichten Text angehängt.
– Die Kontrolle für Bob besteht nun darin, dass er die (bekannte) Hash-Funktion auf den Text anwendet und das Ergebnis y mit der Potenz $x^d \pmod N$ unter Verwendung des öffentlichen Schlüssels (d, N) von Alice vergleicht. Sind die beiden Resultate gleich, so kann die Nachricht nur von Alice stammen, denn nur Alice kennt den Dechiffrierschlüssel f und kann daher aus dem Wert y der Hash-Funktion die Zahl $x = y^f \pmod N$ berechnen.
– Gleichzeitig ist damit auch nachgewiesen, dass der Text nicht verändert wurde, da sonst die Hash-Funktion einen anderen Wert angenommen hätte.

Dies ist nur eine der unzähligen Möglichkeiten, wie die RSA-Methode und die Idee der öffentlichen Schlüssel in intelligenter Weise eingesetzt werden kann. Alle am Anfang erwähnten Probleme (elektronische Abstimmungen, Signieren von Verträgen usw.) haben damit Lösungen gefunden.

Schlussbemerkung
Die Sicherheit des öffentlichen Schlüsselaustausches und des RSA besteht darin, dass für bestimmte zahlentheoretische Aufgaben (diskreter Logarithmus bzw. Primzahlzerlegung) keine schnellen Algorithmen bekannt sind. Es ist allerdings nicht *bewiesen*, dass es keine solchen gibt. Eine gewisse Unsicherheit ist also vorhanden. Dazu kommt noch das Problem, dass die Forschung auf diesem Gebiet auch an Orten passiert, welche striktester Geheimhaltung unterliegen. (Man vergleiche hierzu auch den folgenden Abschnitt.)

Addendum

Zur Geschichte
(von Geheimdiensten und Spionen)
Die Idee der öffentlichen Kryptographie entstand lange vor der Erfindung des Internets. Niemand hätte damals daran gedacht, welche zentrale Rolle sie schon 20 Jahre später spielen wird! Whitfield Diffie war ein junger Hacker und Martin Hellman Professor an der Stanford University. Ihre geniale Entdeckung hat eine völlig neue Ära der modernen Kryptographie eingeleitet. Sie lag keineswegs in der Luft; die beiden waren ihrer Zeit weit voraus.

Aber waren sie auch wirklich die ersten?

Nein, die öffentliche Kryptographie wurde schon früher, nämlich 1970, von Mitarbeitern des Britischen Geheimdienstes, J. Ellis, C. Cocks und M. Williamson, entdeckt und beschrieben. Auch die RSA-Methode war ihnen bereits 1973 bekannt. Aber erst 1997 wurden die Archive geöffnet und die «Helden» durften reden. Doch inzwischen war J. Ellis schon gestorben.

Diffie und Ellis trafen sich allerdings bereits 1982 und wurden später gute Freunde. Anscheinend hat sich Ellis nie dazu geäussert, dass ihm für seine wirklich revolutionäre Entdeckung die verdiente Würdigung zeitlebens vorenthalten wurde.

(Einen kurzen Bericht über diese Ereignisse findet man auf dem Internet unter
www.wired.com/wired/archive/7.04/crypto_pr.html.)

Quantum Computing
Seit ein paar Jahren denken Physiker und Mathematiker intensiv über den Quantencomputer nach. Ein solcher würde völlig neue Algorithmen zulassen, insbesondere auch zahlentheoretische, die die Zerlegung von grossen Zahlen in Primfaktoren in polynomialer Zeit ermöglichen würden. Damit wäre die Sicherheit des RSA klar in Frage gestellt. Die Experten sind sich allerdings nicht einig, ob es je einen funktionierenden Quantencomputer von der notwendigen Kapazität geben wird. Die Theorie ist auf jeden Fall faszinierend, die bisher erreichten experimentellen Resultate sind (noch) nicht sehr viel versprechend. Die NSA (National Security Agency in den USA) scheint allerdings etwas nervös zu sein!

Ich danke meinem Kollegen Prof. Ueli Maurer von der ETH Zürich für wertvolle Hinweise.

Prof. Dr.phil. Hanspeter Kraft ist Ordinarius für Mathematik am Mathematischen Institut der Universität Basel.

Tafel IV

Der Satz von Euler
Wir starten mit zwei verschiedenen, ungeraden Primzahlen p und q und setzen $N = p \cdot q$.
Weiter sei s eine beliebige Zahl mit
$s = 1 \pmod R$,
wobei $R = (p-1)(q-1)$ ist.
Dann gilt für jede Zahl x:
$x^s = x \pmod N$.
Damit kann man das Dechiffrieren des RSA erklären. Die beiden Zahlen d und f wurden so gewählt, dass $d \cdot f = 1 \pmod R$ gilt.
Hieraus folgt durch einfaches Potenzrechnen:
$y^f = (x^d)^f = x^{d \cdot f} = x \pmod N$.

Departement Mathematik und Informatik
Universität Basel, Spiegelgasse 1, CH-4051 Basel
Email address: Hanspeter.Kraft@unibas.ch