EDUCAÇÃO e TECNOLOGIA

Revista do Instituto Politécnico da Guarda

"EDUCAÇÃO E TECNOLOGIA"
Revista do Instituto Politécnico da Guarda

Director: **João Bento Raimundo**

Redacção: **Rua Comandante Salvador do Nascimento**
Telf. 21634/23982 **6300 GUARDA**

Propriedade: **Instituto Politécnico da Guarda**

Execução Gráfica: **Secção de Reprografia do IPG**

Depósito Legal Nº 17.891/87

Nº VII / Janeiro de 1991

PROGRESSO POR OBJECTIVO

O sétimo número de "*Educação e Tecnologia*" coincide com o início de mais um ano lectivo, o mesmo é dizer, com uma nova fase do Instituto Politécnico da Guarda. Nova, porque o Instituto Politécnico da Guarda cresceu em número de cursos, de alunos e professores, aumentando as exigências, qualitativas e quantitativas. Enfim, o Instituto Politécnico lançou já os seus primeiros diplomados.

Hoje são já umas dezenas; o amanhã, que é breve, os fará crescer.

Isto significa que a nossa Instituição é posta à prova em termos práticos.

Estamos a desenvolver uma formação que dê aos nossos jovens uma realização académica a par das exigências da sociedade moderna; que da justaposição de ambas surja uma adequação o mais perfeita possível à resposta interior do indivíduo no campo do estar, do fazer, do ter, do ser.

O espaço de diálogo, de abertura, de confronto de ideias, de registo de experiências que vem constituindo "*Educação e Tecnologia*", ficaria incompleto se nele não viessem a tomar lugar também aqueles que primeiro motivaram a sua existência.

Bem-vindos serão, também, os registos de quantos, como empregadores, vão testar, no terreno, o que laboriosamente proporcionámos que se ajustasse às solicitações de uma produção eficaz e digna.

Quisemos dar mais oportunidades ao nosso Distrito - por isso existimos como Instituição de Ensino Superior. Quisemos dar mais oportunidades à juventude - por isso aumentámos o número de vagas e de cursos, apostámos na qualidade e formação do corpo docente, continuamos a melhorar as instalações. Queremos dignificar o ensino e engrandecer o País - dialogar, modificar, adequar.

Parafraseando A. Comte:

"*Amor por princípio / Competência por base / Progresso por objectivo*".

João Bento Raimundo
Presidente da C.I. do I.P.G.

Moderne Chiffrierverfahren und Faktorenzerlegung bei grossen Zahlen

[Public Key Cryptosystems and factorization of large numbers]

a)

Wolfgang Biegert*

Abstract: 20 Years ago, the factoring of large numbers was not interesting for many mathematicians, because it is well known, that every number is definitly dividing in prime numbers. Everybody knows, that $91 = 7 \times 13$, but who knows the factorization of 62 773 913 ? (it is 7919×7927)! New methods for mathematical Cryptography based on the impossibility to factor very large numbers with a reasonable expense and in reasonable time. Naturally the mathematicians now are searching for new methods of factoring large numbers in order to break the secret information. Since July 1990, the record holders are Manasse and Lenstra, they have factored a 155-digit number.

Die neuere Entwicklung im Bereich der grossen Datenverarbeitungsanlagen zeigt einen extremen Preisverfall für Speicherplätze. Zusammen mit der Entwicklung der Mikroprozessoren wird dies dazu führen, dass grosse DV–Anlagen immer mehr zum Speichern von Informationen verwendet werden, also eine Art elektronischer Bibliothek bilden.

Wenn grosse Mengen von Informationen gespeichert werden, muss sichergestellt sein, dass nur Berechtigte Zugriff zu diesen Daten erlangen können. Daher müssen solche Daten auf irgendeine Weise verschlüsselt werden. Aus diesem Grund sind Chiffrierverfahren aus der modernen Informatik kaum mehr wegzudenken.

*Dr.rer.nat.
Professor am Fachbereich Mathematik der Fachhochschule für Technik, Stuttgart, Alemanha

Mit modernen grossen Rechnern ist es heute möglich, bei einer 200–stelligen Zahl in Minuten zu erkennen, ob sie prim oder zusammengesetzt ist. Wenn sie aber als zusammengesetzt erkannt ist, kann es viele Jahre Rechenzeit erfordern, bis man deren Teiler (die z.B. 101– und 99–stellig sein können) tatsächlich bestimmt hat.

Diese Diskrepanz nützten die Mathematiker Rivest, Shamir und Adleman vor ungefähr 13 Jahren aus, um daraus ein Chiffrier–Verfahren zu entwickeln (RSA–Verfahren), das ganz ohne geheimen Transport von Schlüsselmaterial auskommt. Es beruht gerade darauf, dass die Zerlegung einer grossen Zahl (wenigstens 50–stellig) nur unter unverhältnismässig grossem Zeitaufwand möglich ist, während die Multiplikation der Faktoren in kürzester Zeit erfolgen kann.

Wenn man in eine Geheimschrift, die nach dem RSA–Verfahren verschlüsselt wurde, unberechtigt eindringen möchte, ist dies praktisch nur möglich, wenn man –neue– Verfahren entwickelt, die die Zerlegung einer grossen Zahl viel rascher erlauben als unsere bisher bekannten Verfahren. Daher ist die Frage nach der Faktorisierung einer grossen Zahl auch wichtig geworden für den Datenschutz und damit für die gesamte Informatik.

Vor etwa fünf Jahren ist im US–amerikanischen Sandia–Institut in Albuquerque /New Mexico ein Verfahren entwickelt worden, das wenigstens 40–stellige Zahlen in knapp einer Stunde in Faktoren zu zerlegen gestattet. Nach meinem Wissen ist die Arbeit von Davis, Frau Holdridge und Simmons immer noch nicht veröffentlicht. Ich verdanke dem persönlichen Kontakt mit Herrn Simmons das Manuskript und die Erlaubnis, darüber berichten zu dürfen.

Wie schon das Schroeppelsche Verfahren beruht auch das Sandia–Verfahren im Grundsatz auf einem Quadratischen Sieb, das Pomerance aus Athens /Georgia vorgeschlagen hat. Davis, Holdridge und Simmons haben auf diese Weise eine beliebige 40–stellige Zahl unter Einsatz eines der ganz grossen CRAY II–Rechner in knapp einer Stunde in ihre Faktoren zerlegt. (1985).

Ist nun durch dieses Sandia–Verfahren das RSA–Chiffrierverfahren unbrauchbar geworden ?
Die Antwort heisst auch heute noch ganz klar: Nein !

Es scheint, und darauf weisen die Sandia–Leute hin, so zu sein, dass es eine Art "natürliche Grenze" für dieses Zerlegungsverfahren gibt, die bei den derzeit vorhandenen Rechnern bei etwa 45 Stellen liegt. Obwohl das Sandia–Verfahren selbst auch hier grundsätz-

lich schnell geht, brauchen die vorbereitenden Berechnungen, also die Bestimmung der möglichen Primzahlen und die Bereitstellung einer genügend grossen Faktorbasis so viel Zeit vorab, dass das Sandia-Verfahren bei Zahlen mit mehr als 50 Stellen nicht schneller ist als das reine Probieren, dass dann also auch dieses Verfahren Jahre für die Zerlegung benötigt.

Damit war das RSA–Verfahren (noch einmal) gerettet, wenn man die beiden Primzahlen dafür wenigstens 60–stellig wählt.

Frau Holdridge und Davis prognostizierten im Jahr 1985, dass es vielleicht möglich sein könnte, um das Jahr 2000 auch 150–stellige Zahlen innerhalb von Tagen zu zerlegen, sei es mit der Sandia– oder einer anderen Methode. Das RSA-Verfahren wird aber auch dann noch brauchbar sein — man muss dann eben 100–stellige Primzahlen verwenden.

Und wie gut ist es, dass schon vor mehr als 2000 Jahren Euklid nachgewiesen hat, dass die Primzahlen nie "aufhören", dass es also sicher auch 200– oder 300–stellige Primzahlen gibt. Er hat wohl als Mathematiker nie daran gedacht, dass man seine Feststellung jemals würde "brauchen" können. Gerade dies ist typisch für die Mathematik, dass sie Ergebnisse "auf Vorrat" bereitstellt, ohne die Frage zu stellen, ob man solche Ergebnisse auch praktisch anwenden kann.

Eine Arbeit von Silverman aus Bedford /Massachusetts aus dem Jahr 1986 schlägt vor, die vorbereitenden Aufgaben auf viele parallel rechnenden Personal–Computer oder auf viele parallel rechnende Mikrochips zu verteilen. Silverman erreichte damit die Zerlegung einer (speziellen) 75–stelligen Zahl und im Jahr 1988 einer 90–stelligen Zahl in zwei 41– bzw. 49–stellige Primfaktoren.

Dann aber lag es eigentlich nahe, statt der relativ langsamen Mikrochips die grossen schnellen Rechner mit den "Vorarbeiten" zu betrauen, die weltweit überall in Rechenzentren "herumstehen". Man muss dazu "nur" einen Internationalen Rechnerverbund schaffen und die Teilaufgaben auf diese Grossrechner verteilen.

Manasse und Lenstra gelang es, die Betreiber der verschiedenen Grossrechner in aller Welt zu veranlassen, dass sie ihre freie Kapazität hierfür zur Verfügung stellen. Auf diese Weise konnte im Jahr 1988 eine hundertstellige Zahl in ihre beiden 41– und 60– stelligen Primfaktoren zerlegt werden:

8675922231342839081221807709585070804897 7 und
1084881048536374706129613998429729484098346115257905772167 53.

Die 100–stellige Zahl wurde von Wagstaff vorgeschlagen. Sie entsteht dadurch, dass man die Zahl

$$11^{104} + 1$$

durch den "offensichtlichen" Teiler 214 358 882 dividiert. Dieser Teiler ist seinerseits wiederum zerlegbar in die Primteiler

2, 7 und 6 304 673.

Die Fermat–Zahlen der Form

$$F_k = 2^{2^k} + 1$$

reizten schon immer die Zahlentheoretiker.
Fermat (1660) vermutete, dass alle diese Zahlen prim seien, was für k = 0 bis k = 4 auch richtig ist.
Doch konnte Euler im Jahr 1770 zeigen, dass F_5 den Teiler 641 besitzt, also nicht prim ist.
Für k = 6 gelang die Zerlegung in einen 6– und einen 14–stelligen Primteiler im Jahr 1880,
für k = 7 erst 1970, obwohl Klein schon 1895 gezeigt hat, dass F_7 nicht prim sein kann,
für k = 8 wurde die Fermat–Zahl im Jahr 1980 zerlegt.
Die einzelnen Faktoren sind
für k = 5
641 und 6700417,
für k = 6
274177 und 67280421310721,
für k = 7
59649589127497217 und 5704689200685129054721,
für k = 8
1238926361552897 und
93461639715357977769163558199606896584051237541638188558028032 1

Die Zerlegung berechneten

für k = 5 Euler (1770)
für k = 6 Landry und Le Lasseur (1880)
für k = 7 Morrison und Brillhart (1970)
für k = 8 Brent und Pollard (1980).
Man beachte die zeitlichen Unterschiede.

Die Fermat–Zahl für k = 9 war besonders hartnäckig. Man weiss zwar schon seit 1903, dass F_9 den Teiler

2424833

besitzt, 1967 hat Brillhart weiter nachgewiesen, dass der Rest noch einmal zerlegbar sein muss.
Am 15.Juli 1990 ist es gelungen, auch diese Zahl zu zerlegen. Manasse und Lenstra benutzten dazu eine Erweiterung des Quadratischen Siebs nach Pomerance, die Pollard erst Ende 1989 entwickelt hat, und die er als "Zahlkörper–Sieb" (number field sieve) bezeichnet. Und wieder benützten Manasse und Lenstra die von ihnen schon früher organisierte Internationale Zusammenarbeit.

Die jetzt zerlegte Zahl besitzt 155 Stellen – es ist eine erstaunliche Entwicklung von der 100–stelligen Zahl im Jahr 1988 zur 155–stelligen Zahl 1990 in nur knapp zwei Jahren. Der verwendete Rechnerverbund schaffte diese Arbeit, für die ein einzelner Grossrechner wohl etwa 500 Jahre benötigen würde. Auch das Zusammenfügen der Einzelergebnisse wurde über einen Parallelrechner geleistet, der diese Aufgabe in etwa 3 Stunden löste.

Das Nachprüfen durch Ausmultiplizieren war nach einer knappen Minute erledigt.

Die Lösung des neuen Problems, nämlich das Nachprüfen, ob die gefundenen Faktoren tatsächlich schon prim sind, lieferte Odlyzko wenig später. [1]

Die nun gefundenen Primfaktoren der Zahl

$$\frac{2^{512}+1}{2424833}$$

=

55293737465394924514694517099552200615379969757061180616246815528004460637386355995657739308921082102107781683053991969153149444980114382913931182 09

[1]Ich verdanke den Hinweis auf diese gelungene Zerlegung Herrn Fricker, Marburg

sind

7455602825647884208337395736200454918783366342657

und

741640062627530801524787141901937474059940781097519023905821316144
415759504705008092818711693940737

Es ist bemerkenswert, mit welchem immensen Aufwand die Mathematiker und Informatiker an das Problem der Faktorisierung von grossen Zahlen herangehen, seit es die public key–Chiffrierverfahren gibt. Dabei sah es bis vor zwanzig Jahren so aus, als ob dieses Problem mathematisch vollkommen uninteressant sei.

Ein Internationaler Verbund von Grossrechnern zur Lösung eines mathematischen Problems ist eigentlich ein grossartige Sache.

Nur kann dieser Verbund in diesem Falle zu einem Paradoxon führen:

Um ein Verschlüsselungssystem nach dem RSA–Verfahren einzurichten, benötigt man sehr viel Speicherplatz. Man muss zum Beispiel eine 200–stellige Zahle mit einem 80–stelligem Exponenten potenzieren und das Ergebnis mit einem 200–stelligen Modul reduzieren. Da ein solch aufwendiges Chiffriersystem nur bei vielen Teilnehmern rentabel ist, benötigt man zur Speicherung der geheimen Nachrichten sehr grosse Rechner. Die geheimen Nachrichten sind für einen nichtberechtigten Empfänger nur entschlüsselbar, wenn es ihm gelingt, eine sehr grosse Zahl zu zerlegen. Und dazu benötigt man wiederum viele Grossrechner. Wenn nun der Rechner, der die geheimen Informationen enthält, in den Internationalen Verbund einbezogen wird, kann es sein, dass gerade dieser Rechner mithilft, genau die Nachrichten, die in ihm gespeichert sind, unberechtigt zu knacken.

Sicher ist dies jetzt kein mathematisches Problem mehr, sondern ein organisatorisches. Doch muss man jetzt unbedingt darauf achten, dass solche "Selbsthilfen" zum Zerstören des Chiffrierverfahrens sicher ausgeschlossen bleiben. Und dies könnte ein Ende des Internationalen Verbunds in naher Zukunft bedeuten.

(Abschluss des Manuskripts 15.XII.1990)

Literatur

[1] Adleman, Pomerance, Rumely
On distinguishing prime numbers from composite numbers.
Ann.d.Math. (2), 177, (1983)

[2] Cohen, Lenstra
Primality testing and Jakobi sums.
Math.Comp., 42, (1984)

[3] Davis, Holdridge
Most wanted Faktorizations using the Quadratic sieve.
Sandia Report, Albuquerque, (1984)

[4] Davis, Holdridge, Simmons
Status Report on Factoring.
(Unveröffentlichtes Manuskript), (1985)

[5] Fricker
Persönliche Mitteilung (November 1990)

[6] Keller
Primfaktorisierung durch weltweite Rechnervernetzung.
Spektrum der Wissenschaft, 2, (1989)

[7] Lenstra, Lenstra, Manasse, Polland
The number field sieve.
Proc.of the 22nd annual acm Symp. on the Theory of Computing (STOC), (1990)

[8] Pomeranca
Analysis and compar. of some integer factoring algorithm.
Number Theory and Comp. MC tracts

[9] Rivest, Shamir, Adleman
A Method for obtaining digital signatures and Public-key Cryptosystems.
Comm. ACM 21, (1978)

[10] Silverman, Caron
Parallel Inplementation of the Quadratic Sieve.
(Unveröffentlichtes Manuskript) (1987)

a) - *Este artigo surge na sequência da visita do autor, Professor Dr. Wolfang Biegert, docente da Escola Superior Técnica de Estugarda, ao Instituto Politécnico da Guarda.*

Com a referida deslocação e com a publicação deste trabalho pretende-se fomentar a colaboração entre estas duas instituições europeias de ensino superior, nomeadamente no campo da Matemática aplicada.