Die Kleine Senft knackt den Code

Das uralte Rätsel um die Verteilung der Primzahlen ist gelöst.

Und anders als Mathematiker bis heute glauben, folgt diese Verteilung faszinierend einfachen Gesetzen.

Dadurch entsteht eine völlig neue Situation für die Zahlentheorie und zugleich eine kritische Krise für einen veritablen Bereich der Internet-Architektur.

Weil man die Bildegesetze der Primzahlfolge nicht kannte, hat sich im Lauf der Jahre ein Sicherheitsstandard etabliert, der ausschließlich auf ein mathematisches Problem vertraut, das mit den Primzahlen zusammenhängt.

Davon betroffen sind nicht nur die E-Mail-Verschlüsselungen, zu denen man den Usern rät, sondern gleichermaßen Transaktionen und Authentifizierungen im Netz.

Auch die Firma Microsoft, um ein Beispiel zu nennen, muss sich bei ihren Kunden authentifizieren, bevor sie Updates schickt, und bedient sich dabei dieser Primzahlverschlüsselung. (Die Prozesse laufen unbemerkt im Hintergrund.)

Was wäre wohl, wenn jemand den Schlüssel geknackt hätte und drollige »Updates« an mehrere Milliarden Betriebssysteme schicken könnte?

»Ich bin's, Microsoft. Alle Daten löschen!«

Ich kann zunächst nur jedem Anwender raten, in dergestalt verschlüsselten E-Mails nichts mitzuteilen, was er in

unverschlüsselten nicht auch mitteilen würde. Schon sehr bald wird man alles lesen können, und eins ist sicher: Gerade die verschlüsselten werden in speziellen Datenfarmen, die Flüsse zur Kühlung ihrer Server verbrauchen, vorgehalten. Edward Snowden hat die Möglichkeiten solcher Kraken angesprochen.

Es ist i.Ü. ungeheuer wundersam, dass ihr noch nichts von diesen Sicherheitslücken vernommen habt. Ich habe bereits im März 2017 die Presse, Fachleute und Institute auf die Situation hingewiesen. Selbst der verschlafene Chaos Computerclub bekam Post von mir. Lest hier und hier die Pressemitteilungen, die – neben einem druckfrischen Exemplar meiner Publikation – all diesen Schreiben beilagen.

Besonders interessant ist der Fall eines Instituts für Kryptographie, das Abermillionen an Fördergeldern von der EU erhält, um genau diesem Problem vorzubeugen bzw. Lösungen zu finden für den Tag, an dem der RSA-Standard, (so heißt die Primzahlverschlüsselung), nicht mehr sicher ist . . .

Dieser Zeitpunkt liegt in der Vergangenheit, Leute, das

Kind ist bereits in den Brunnen gefallen, und der Erkenntnisfortschritt lässt sich nicht mehr aufhalten.

Die spektakuläre Entdeckung der entscheidenden Zusammenhänge gelingt in der genannten Publikation einer norddeutschen Schülerin, der kleinen Senft, wie sie genannt wird, und wenn es euch gefällt, könnt ihr anschließend lesen, wie es dazu kam.

Der erste Sreich

Es war im Herbst 2014, als ich anfing, mich mit Primzahlen zu beschäftigen. Tagsüber saß ich an einem umfangreichen Projekt, das enorm zehrte, abends war ich meistens ziemlich fertig.

Um nicht immer in die Röhre stieren zu müssen, nahm ich kleine Zettelchen und notierte Zahlenreihen. Ich wollte sehen, wo das Primzahlrätsel begraben liegt. Außerdem war es entspannend, weil unverbindlich nach den langen Tagen am Bildschirm.

Von den Primzahlen verstand ich damals nicht mehr als das, was man auch in Wikis nachlesen kann, insgesamt kaum mehr als nichts.

Immerhin fand ich in den Suchmaschinen Auskunft über das Sieb des *Eratosthenes*, der vor Jahrtausenden eine funktionierende, aber wenig praktikable Methode zur Bestimmung der Primzahlreihe gefunden hatte.

Außerdem hatte ich Wind bekommen von einer Erkenntnis, die Leibniz zugeschrieben wird und besagt, dass die Primzahlen in der Umgebung der Zahl sechs bzw. der Sechserreihe auftauchen. Nehmt einen Zettel und probiert es aus!

Ihr werdet sehen, dass es unendlich viele Ausnahmen gibt, obwohl zumindest eines richtig zu sein scheint: Abgesehen von der Zwei und der Drei, die aus dem Raster fallen, genügen alle anderen Primzahlen, die man testet, der Form n mal sechs plus eins oder n mal sechs minus eins.

Im Netz finden sich Tabellen bekannter Primzahlen, an denen man das prüfen kann.

Leider sind nicht alle Zahlen, die dieser Form genügen, prim. (Beispiel vier mal sechs plus eins. Oder sechs mal sechs minus eins.) Die Ausnahmen sind Legion und gehen vermutlich gegen unendlich. Was also tun?

Abend für abend nahm ich meine Zettelchen vor, damals im Herbst 2014, um stets neue Kombinationen auszuprobieren. Ich wollte unbedingt herausfinden, wo es zutrifft und wo nicht, das war die entscheidende Frage.

Irgendwann sah ich ein merkwürdiges Muster in meinen Tabellen. Ich sah Abstände, die sich wiederholten, und war erst einmal zufrieden. Die Sache drohte, in Arbeit auszuarten, was ich damals unbedingt vermeiden wollte.

Zunächst war es eine Spielerei, aus Neugierde inszeniert, jetzt sah es so aus, als müsse man systematisch forschen. Immerhin war klar: Da liegt etwas im Busch, möglicherweise die Lösung des Rätsels.

Ihr könnt jetzt selber spielen und die Lösung suchen, oder gleich lesen, wie es weiterging.

Der zweite Streich

Monatelang lagen meine Zettel in einer Hülle unter vielen, ohne beachtet zu werden. Im Sommer 2015 las ich in einem Online-Artikel, ich glaube auf Telepolis, dass ein »gigantisches Desaster« drohe, wenn der geniale RSA-Standard der Datenverschlüsselung, der auf Primzahlen beruhe, obsolet geworden sei.

Durch diesen Artikel, der auch den Namen eines Spezialisten der TH Darmstadt enthielt, erfuhr ich zum ersten Mal davon, dass Primzahlen eine Rolle bei der Verschlüsselung spielen. Ich bediente ein paar Suchmaschinen und fand genug Material, um meine Schmierzettel in einem neuen Licht zu sehen.

Besonders hilfreich fand ich einen Text, den ihr unter dem Titel das »Faktorisieren großer Zahlen« im Netz aufsuchen könnt. Auch über den RSA-Standard, Primzahltests u.a.m. findet man Wikis, immerhin, auch wenn die meisten nicht viel taugen.

Um es kurz zu machen: Die einfache Multiplikation zweier Primzahlen ergibt – je nach gewählter Größenordnung – ein Monstergebilde von Zahl, und für jemanden, der die enthaltenen Primfaktoren nicht kennt, ist es schier unmöglich, dieses Produkt wieder in die beiden Bestandteile zu zerlegen.

Dieses »Faktorisierungsproblem« bildet die Vertrauensbasis des Internets. Für den Fall, dass es gelöst würde, so viel hatte ich begriffen, drohte ein gigantisches Desaster.

Was genau passieren würde, konnte ich mir allerdings

nicht vorstellen, dazu findet man nirgendwo brauchbare Hinweise. Vor allem konnte ich mir nicht vorstellen, dass die Lösung dermaßen simpel ist, wie meine Zettel nahelegten. Und dass vor mir niemand auf die Idee gekommen sein sollte.

Wie ihr gemerkt haben dürftet, bin ich ein Newbie in diesem Fach. Und wieder begann ich zu recherchieren.

Ich fand einen Menschen, besser gesagt sein Buch, der ein ganzes Weltgebäude auf den Primzahlen errichtet. Eine ernsthafte Auseinandersetzung mit seinen Thesen fand offenbar nie statt, obwohl er Lösungswege fand, die der Mathematik verborgen blieben. Der Name dieses Menschen, eines promovierten Chemikers, ist Peter Plichta, sein Auftritt im Netz leicht zu finden.

Ich fand die Lektüre faszinierend, darf mir ein Urteil über seine These vom vierdimensionalen Raum um einen Punkt (u.a.m.) wegen mangelnder Sachkenntnis aber nicht erlauben. Zumal ich schnell und oberflächlich lesen musste und vor allem eines wissen wollte: Hat er die Gitterstruktur, die aus meinen Schmierzetteln hervorging, gekannt oder nicht?

Ich habe nicht den leisesten Hinweis dafür gefunden, bin aber ziemlich sicher, dass *er* sie gesehen hätte, falls sein forschendes Interesse in diese Richtung gegangen wäre.

Tatsächlich hat er andere, sehr steile Pfade eingeschlagen, auf die man ihm als unvorbereiteter Laie nicht ohne Weiteres folgen kann, während mein Interesse in eine völlig andere Richtung ging.

Primzahlen immerhin als gemeinsamer Ausgangspunkt.

Die 24-Stunden-Uhr, die er verwendet, um das sog. Primzahlkreuz und die Ausbreitung des postulierten Zahlenraums zu veranschaulichen, war für meine Zwecke nicht geeignet, brachte mich aber auf die Idee der *6-Stunden-Uhr*.

Mit dieser Hilfskonstruktion, mehr ist es bei mir nicht, zeigen die Kinder im Buch leicht verständlich und auf amüsante Art, wie ich finde, dass zwei Drittel aller (natürlichen) Zahlen von vorneherein ausscheiden, wenn es um die Verteilung der Primzahlen geht. Und dass man das restliche Drittel systematisch fleddern muss, wenn die Primadonnen unter den Zahlen in all ihrer Herrlichkeit erscheinen sollen.

Um diesen Beweis zu führen, muss man *kombinatorisch* argumentieren, auch darauf hatte Plicht in einem Nebensatz hingewiesen.

Wenn ich den ganz Kleinen erkläre, wie das mit den Primadonnen läuft, (oder wahlweise Zahlentheoretiker zur Weißglut bringen will), verweise ich auf die Bienen mit ihren sechseckigen Waben und auf die daraus resultierende 6-Stunden-Uhr der Bienenvölker.

Ihr versteht doch, dass man nur dem Gesumsel dieser Völker zuhören muss, um das Geheimnis der Primadonnen zu finden? Zumindest bringt man Fachexperten mit solchen Reden zur Weißglut, ein Wunder ganz eigener Art.

Unabhängig von der Terminologie, Leute, das Ergebnis

ist jedes Mal dasselbe und unumstößlich wahr, obwohl ein streng mathematischer Beweis vielleicht anders aussieht. (Das wäre noch zu prüfen.)

Wollt ihr jetzt mehr von den fleißigen Bienchen und ihrer Stundenuhr erfahren?

Der dritte Streich

Meine Zettel waren in einem erbärmlichen Zustand. Ich hatte sie zunächst mit roter Tinte beschrieben, der Korrekturen wegen, die ich damals zu erledigen hatte, und die Schrift war z.T. verblichen. Ganz abgesehen von einer Sauklaue, die wirklich erstaunlich ist.

Ich musste das Pulver quasi neu erfinden, immerhin wusste ich, dass es eine Lösung gibt. So begann ich, am Computer Tabellen anzulegen und konnte die Gitterstruktur gut leserlich rekonstruieren. Diese Tabellen sind im Buch-Anhang zu sehen: Es hat sich alles bestätigt.

Die Lösung ist im Übrigen so simpel, falls noch nicht erwähnt, dass man es kaum glauben mag. Ist das »gigantische Desaster« demnach unvermeidlich?

Meine Freunde und Berater drängten mich, das Verfahren als Patent einzureichen, dazu hatte ich aber absolut keine Lust. Würdet ihr das aushalten? Gibt es etwas Langweiligeres unter der Sonne als Patentschriften? Weshalb dafür seine Zeit verplempern?

Mir schwebte eine Kindergeschichte vor, in der junge Helden die einfachen Zusammenhänge entdecken und publik machen.

Sorry, ihr Lieben, es ist diese unerklärliche Schwäche für skurrilen Humor, die mir solche Einfälle zuträgt. Außerdem dürft ihr den komischen Leuchteffekt nicht unterschätzen, der von weißglühenden Zahlentheoretikern ausgeht, die so schrecklich lange und völlig umsonst nach dem Primzahlcode gesucht haben.

Sie müssen ihre Wikis und Lehrbücher nach Maßgabe der Bienchen jetzt korrigieren, schrecklich. Tut mir natürlich leid, aber was soll's! Muss man deswegen dermaßen schmollen? Wo bleibt euer Sportsgeist, Leute?

Auch der Journalist, ihr erinnert euch, der auf Telepolis zum Thema Kryptographie publiziert und (abegesehen von einem druckfrischen Exemplar meines Buchs) unsere Pressemitteilungen erhielt, konnte mit der *Kindergeschichte* offenbar nichts anfangen. Was schade ist angesichts der Tatsache, dass er die Story seines Lebens hätte schreiben können. Zumal sein Wohnort und meiner kaum zehn Kilometer auseinander liegen.

Der erste Entwurf meiner Heldengeschichte entstand sehr schnell, es folgten Überarbeitungen, Ergänzungen, Feintuning und Lektorat, während die normale Tagesarbeit weiterging.

Ein Münsteraner Publisher, mit dem ich zusammenarbeiten wollte, verkaufte seinen Laden im September 2016 an einen Investor, der andere Ideen verfolgte, es gab neue Verzögerungen, und so kam *die Geschichte einer wundersamen Entdeckung* erst im März 2017 auf den Markt.

Sind nun seither Satelliten vom Himmel gefallen? Kam es zum gigantischen Desaster? Das wäre mir entgangen. Könnte aber noch kommen.

Denn dieses war der dritte Streich, und der vierte folgt sogleich.

Der vierte Streich

Hand aufs Herz, Leute, haltet ihr für möglich, dass ausgewiesene Fachexperten weder mit Daten- und Prozess-Sicherheit, noch mit dem Erkenntnisfortschritt etwas am Hut haben? Kaum vorstellbar, korrekt?

Die Rede ist von Professoren angesehener Institute, die sich im Hauptzweck (forschend und lehrend) genau den Themen gewidmet haben, die von meiner Gitterstruktur in erster Linie betroffen sind.

Nichts auf der Welt, sollte man meinen, dürfte diese Glücklichen mehr begeistern als die Aussicht auf ein Verfahren, das Primzahlen und Primfaktoren auf Knopfdruck bestimmt, ganz zu schweigen von allem andern.

Oder seht ihr das genauso?

Das Problem besteht vielleicht nur darin, dass sie eine *Kindergeschichte* selbst dann nicht lesen, wenn sie die Lösung ihrer Probleme auf dem Silbertablett präsentiert.

Kinder? Das kann nicht seriös sein. Wäre viel zu einfach. Außerdem ganz ohne Formelsprache. Ich verstehe diese Vorbehalte. Und doch wirken sie ein wenig befremdlich in anbetracht der gigantischen Desaster, von denen die Herrschaften ansonsten erzählen.

Und warum haben sie die Zeit nicht genutzt, um bessere Schlüssel zu entwickeln? Muss man denn alles selber machen?

Die Unfähigkeit, mit einem erzählerischen Text klarzu-

kommen, könnte sich immerhin zum Desaster für den Forschungsstandort Deutschland erweisen. Hören wir in einigen Jahren von einer amerikanischen Garagenfirma, die aus der Gitterstruktur, die in meinem Buch zum ersten Mal beschrieben wird, eine neue Generation von Prozessoren entwickelte, während der deutsche Michel die Revolution wieder verschlief?

In diesem Moment sind technische Anwendungen allerdings reine Spekulation. Was man mit Sicherheit sagen kann, ist Folgendes.

- Mit der Gitterstruktur lassen sich Primzahlen der Reihe nach ad infinitum bestimmen
- Dabei entsteht keine einzige Lücke
- Es genügt ein Scanvorgang zweier Bereiche einer Datenbank
- Diese wird automatisch gefüllt
- Das Befüllen folgt einer einzigen Rechenvorschrift, die sich mit wenigen Zeilen Code programmieren lässt
- Innerhalb des Systems, in dem u.a. alle RSA-Zahlen enthalten sind, lassen sich die jeweiligen Primfaktoren auf unterschiedliche Art auslesen
- Beispielsweise durch die Subtraktion der Nachbarzahl
- Selbst ohne vollständige Datenbamk ist das Faktorisieren in jedem gewählten Zahlenbereich möglich
- Dieselbe Rechenvorschrift kann als Suchradar oder Plotterlcode eingesetzt werden, um die RSA-Nachbarn und damit ihre Primfaktoren zuverlässig aufzustöbern
- selbst ein direkt-rechnerisches Faktorisieren einzelner RSA-Produkte (ohne lange Siebeverfahren) liegt im Bereich des Möglichen, ich werde dazu gelegentlich Vorschläge machen

Es klingt unglaublich, ganz recht, und doch ist alles wahr. Wer die Gitterstruktur verstanden hat, wird nicht mehr zweifeln. Es gibt nur *ein* Problem: Das Zahlenformat.

In einem Taschenrechner bzw. einem kleinen Mathe-Programm könnt ihr Zahlen mit fünfzehn Ziffern möglicherweise noch darstellen und verarbeiten. Schon die Multiplikation zweier solcher Zahlen überfordert ein solches Programm bzw. die Darstellung. Das geht im Kopf dann schneller.

Auch Computer haben so gewisse Probleme mit sehr großen Zahlen, und das betrifft nicht nur die Fehleranfälligkeit, sondern auch die Laufzeiten u.a.m. Programme, die mit immerhin dreihundert Dezimalstellen halbwegs zurechtkommen, kosten richtig Geld, und es gibt nur zwei oder drei, die etwas taugen. (Für einzelne Rechenarten stehen gelegentlich freie Javaskripte u.ä. im Netz.)

Außerdem hört der Spaß und das Verschlüsseln bei dreihundert Ziffern ja nicht auf. Aber manchmal hilft ein Sprung in die Tiefe.

Lest jetzt, wie es dazu kam, und wie wir den Stein ins Rollen brachten.

Der fünfte Streich

Im Oktober 2017 leistete ich Nachbarschaftshilfe und sprang in diesem Zusammenhang von einem verdammt hohen Gerüst. Ich hätte die Leiter nehmen können, wäre aber langweilig gewesen, ihr wisst, wie Männer ticken.

Unten angekommen, hatte ich den Eindruck, dass der Boden unter meinem linken Fuß nachgab, und fragte den Nachbarn, warum er die Steinplatten nicht unterfüttert habe. In der Notaufnahme ergab sich freilich ein anderer Befund: Schien- und Wadenbein beide gebrochen, es wurde noch am gleichen Abend operiert.

Am zweitletzten Tag meines Aufenthalts in der Klinik, kurz nach Mitternacht, wurde ein junger Mann mit komplizierten Brüchen am rechten Oberarm in mein Zimmer geschoben. Er hatte ein fürchterlich umständliches Gestell unter der Schulter und konnte sich im Bett noch weniger bewegen als ich.

Wie sich am nächsten Tag zeigte, studierte er Informatik und war bestens vertraut mit dem Faktorisierungsproblem der Mathematik, dem RSA-Standard und der Primzahlthematik. Er kannte den Prof, dessen vorgenanten Aufsatz ihr im Netz aufsuchen solltet.

Außerdem hatte er Zugang zu einem Programm, das mit dreihundert Dezimalstellen klarkommt. Als ich erklärte, dass sechshundert plus besser wären, recherchierte er ein wenig und meinte dann, das könne er einrichten. Und er spürte eine urgesunde Lust, meine Gitterstruktur einem spektakulären Praxistest zu unterziehen.

Da wir handlungsunfähig waren und auf zehn Wochen hinaus beide nicht viel tun konnten, vereinbarten wir, uns danach zu treffen, um die Bombe scharf zu machen.

Lest, wenn es euch gefällt, wie es dann Schlag auf Schlag weiterging.

Der sechste Streich

Falls noch nicht erwähnt, hey, ich habe von Informatik keine und von Mathe nicht viel Ahnung. Es ist bald vierzig Jahre her, dass ich zuletzt mit Mathe zu tun hatte, während des Studiums nämlich, als ich »Mathematik für Sozialwissenschaftler I und II« belegen musste. Wenn ich heute, sagen wir, auch nur die Determinante einer Matritze berechnen oder das vollständige Integral einer bestimmten Ordnung angeben soll, bin ich erstmal aufgeschmissen.

Ich müsste das Skript unseres damaligen Profs, des hochverehrten und nicht genug zu rühmenden Walter Krautwald auskramen, der solche Sachen mit uns durchnahm, und bräuchte vermutlich Wochen, um mich wieder einzulesen in Methoden, die die höhere Mathematik ja noch kaum tangieren. Oder seht ihr das genauso?

Ich habe allen Grund zur Bescheidenheit. I'm a poet/ and I know it/ hope I don't blow it ... (Bob Dylan)

Informatik gab es damals noch nicht mal als Begriff, glaube ich, im Rechenzentrum der Uni wurden Lochstreifen eingelesen, und wenn wir unsere Fragebögen statistisch auswerten wollten, mussten wir entsprechende Streifen liefern. Auch der Begriff Stochastik kam erst später auf, wir belegten »Statistik für Sozialwissenschaftler I und II« bei einem Menschen, seines Zeichens Psychologe, der so hilflos war, dass er allen nur noch leid tat. Das aber nebenbei. Was ich meine, ist der unglaubliche Entwicklungsbogen in wenigen Jahrzehnten!

Ich hatte damals nicht mal Telefon auf meiner Bude, ein

Ferngespräch am Münzapparat – es gab ja keine Kärtchen – kostete einen Sack voll Geld. Meine Süße schickte manchmal mehrere Briefe am Tag. Genug davon!

Ich hatte nicht den Schimmer einer Ahnung von den Möglichkeiten der Informatik, als ich Simon, den jungen Mann, der mein Krankenlager teilte, zum ersten Mal traf.

Er amüsierte sich köstlich über meine Ahnungslosigkeit. Während ich von dem Zahlengitter erzählte und dann äußerst skeptisch fragte, ob es möglich sei, solche Reihen automatisch zu erzeugen, programmierte er nebenbei am Laptop ein paar Zeilen und hatte die Sachen bereits entwickelt, als ich aufhörte zu reden. Er produzierte fast ohne Zeitverzögerung Ergebnisse.

Und so hat sich alles dann bestätigt: Um eine Primzahlverschlüsselung nach RSA-Standard zu knacken, genügt eine einzige Nachbarzahl im Zahlengitter, und dieses Gitter kann mit wenigen Zeilen Code automatisch in eine Datenbank geschrieben werden.

Man braucht allein nur die Reihenfolge dieser Zahlen und eben jenen Zusammenhang, den die Kinder in dem genannten, sehr zu empfehlenden, rotzigen und witzigen Buch erklären.

Ihr braucht keine Angst mehr vor dem Quantencomputer zu haben, hey, die Sache ist jetzt schon gelaufen. Der RSA-Standard ist obsolet geworden. Selbst das Zahlenformat spielt kaum eine Rolle, es verzögert den absoluten Zusammenbruch dieses Verschlüsselungssystems nur unwesentlich. Ich kann nur eindringlich nochmal davor warnen. Teilt nichts mit, das ihr unverschlüsselt nicht

auch mitteilen würdet.

Stellt auch vor, bei einer Gaunerfirma wie der NSA sitzen täglich zehntausend Langweiler, die sich die Totalüberwachung zum Lebensinhalt gemacht haben, und popeln in ihren Nasen. Was sollten sie auch tun, die Sache ist im Grunde ja gelaufen, wie der nicht genug zu rühmende Edward Snowden darlegte. Die Archive werden automatisch gefüllt, so müssen wir annehmen, jede kleine Bewegung im Netz wird registriert, bei Bedarf oder Neugierde wird genauer hingeschaut.

Um sich nicht endlos zu langweiligen, was werden diese Pappnasen tun? Genau, sie nehmen die letzte Gurke von einem ausrangierten Rechner, der in der Rumpelkammer verstaubt, und lassen ihn ein halbes Dutzend Programmzeilen ausführen, um die Ergebnisse in eine präparierte Datenbank zu schreiben Zeile für Zeile. Mehr muss er ja nicht tun. Sie brauchen nur die Reihenfolge der Zahlen, die so generiert werden! Spreicherplatz kostet eh nichts, schon gar nicht bei diesen Gaunern, die eine winzige Partition des allerkleinsten, vor der Verschrottung stehenden Servers ihrer Abteilung dafür nutzen könnten.

Sie sorgen nur dafür, dass die Gurke nicht heißläuft, und warten dann ein paar Wochen.

Nehmt weiter an, sie hätten Lust zu schauen, worüber die Genies unsres jetzt so dödeligen Computerclubs sich verschlüsselt immerzu austauschen, was sie aktuell auf dem Schirm und mittelfristig geplant haben. Arbeiten sie mit 128-Bit-Verschlüsselung, wie sie dem Publikum arglos empfehlen? Mit 256? Egal, was immer sie nutzen, das nehmen die genannten Langweiler bei der Gaunerfirma

sich vor, um zu spielen. Man kann an jeder beliebigen Stelle in die Gitterstruktur einsteigen.

Nach ein paar Wochen, meinetwegen Monaten, die Zahlenmengen sind u.U. gigantisch, kriegen sie, wartend und popelnd, nicht nur die Schlüssel der CCC-Truppe, sondern einfach alles, was in diesem Zahlenbereich verschlüsselt ist. Ohne jede Ausdnahme. Denn dazu brauchen sie nur die Reihenfolge der entsprechenden Zahlen im Gitter. (Wahrscheinlich hat diese Firma Tausende Rechner rumstehen, die verstauben, und wenigstens das nebenbei noch leisten könnten. Es wäre dann an einem Nachmittag erledigt, falls sie genug Kühlwasser haben.)

Und während sie schauen, was die CCC-Truppe so treibt, schreiben ihre ausrangierten Gurkeen weiter, Zeile für Zeile den lieben langen Tag, in rasender Geschwindigkeit, weil sie nur addieren müssen. Und so füllt sich der Server mit Zahlenkolonnen jeder Größenordnung, die das Faktorisieren der Primzahlprodukte, aus denen RSA-Zahlen nun mal bestehen, in Sekunden erlauben. Schneller vermutlich, als der Quantenrechner mit dem umständlichen Shor-Algorithmus jemals könnte.

Ist das nicht schön? Natürlich nicht für die genannte Truppe, es sei denn, sie schicken eh nur Banalitäten hin und her, was umso schlimmer wäre.

Übrigens, selbst eine behäbige Chaos-Truppe könnte das im Prinzip leisten, (ein paar Zeilen Programm schreiben nämlich, popeln und warten), denn einen ausrangierten Gurkenrechner haben sie sicher auch noch, um dann Geheimdokumente Thüringer Behörden zur betreuten NSU für uns zu lesen. Natürlich nur ein Beispiel! Damit

ihr das noch viel, viel besser versteht, schlage ich vor, dass ihr euch ein kleines Beispiel zu Gemüte führt.

Der siebte Streich

Ich gebe euch hier das Produkt zweier kleiner Primzahlen und zeige dann, wie ihr den Code knacken könnt. Erinnern wir uns.

Beim RSA-Verfahren der Verschlüsselung werden immer zwei den jeweiligen Anforderungen größenmässig genügende Primzahlen multipliziert, und das Ergebnis dieser Multiplikation bildet den öffentlich einsehbaren Teil des Schlüssels.

Welche Primfaktoren enthalten sind, ist nicht bekannt, und da es bisher nicht möglich war, diese Faktoren mit halbwegs zuträglichem Aufwand zu finden, (sofern sie groß genug gewählt waren), sehnen sich die Berufsüberwacher der Völker dieser Welt nach dem Quantenrechner, der es dann richten soll, während die Chaos-Clubs den Usern empfehlen, ihre E-Mails mit 128 Bits zu verschlüsseln.

Jetzt kommt meine Gitterstruktur ins Spiel, ich habe euch gewarnt.

Merke: Nicht alle Zahlen in diesem Gitter sind RSA-Zahlen, denn es gibt dort auch Produkte von mehr als zwei Primzahlen, aber alle RSA-Zahlen ohne Ausnahme sind im Gitter, und die Primfaktoren können dann sehr einfach ausgelesen werden.

Hier also meine Übungs-RSA, damit ihr seht, wie das geht. Sie ist für echte Verschlüsselungen viel zu klein, denn es sind heute reguläre Algorithmen auf dem Markt, (Methoden, die nicht auf das Gitter zurückgehen), die

solche und sogar beträchlich längere Schlüssel in Bruchteilen von Sekunden zerlegen, wie ich auf Simons Laptop zu sehen bekam.

Ich meinerseits habe eine große Hochachtung vor den Mathematikern und Programmierern, die diese Algorithmen entwickelt haben, das möchte ich ausdrücklich betonen.

Hier also die Zahl. (Weshalb ich eine so kleine gewählt habe, seht ihr später.)

75.770.353

Hübsch, nicht? Und nun zerlegt mal schön ohne Algorithmen, es sind genau zwei Primzahlen enthalten.

Das Programm, zu dem Simon Zugang hat und das den Stand des Könnens der Mathematik auf dem Gebiet repräsentiert, braucht dafür allenfalls Bruchteile von Millisekunden und scheitert doch bei Schlüsseln ab einer gewissen Größenordnung. Ich möchte euch hier aber zeigen, wie ihr dasselbe (und mehr) von Hand machen könnt, mit Stift und Zettel, denn das beherrschen diese von mir ansonsten wirklich sehr bewunderten Genies eben nicht.

Ist das ein Wort?

Also, aufgepasst, jetzt gebe ich euch die Nachbarzahl, wie sie im Gitter steht. Sie lautet:

75.750.731

Wie ihr seht, ist es der Nachbar, der *vor* der RSA-Zahl steht, weil kleiner. Ich hätte auch die nächstgrößere Zahl nehmen können, wir brauchen egal welchen dieser beiden allernächsten Nachbarn.

Und jetzt möchte ich euch bitten, die beiden Zahlen mit dem Stift zu subtrahieren. Nicht wahr, das kann auch ein Erstklässler, um den folgenden Abstand zu kriegen, falls ihr einverstanden seid:

19.622

Diese Zahl, ihr Lieben, müsst ihr nun noch durch zwei teilen, das machen auch Zweitklässler mit ihrem Stift, und schon haben wir die erste der beiden enthaltenen Primadonnen:

9.811

War das jetzt schwierig? Habe ich zu viel versprochen?

Und wer die erste hat, kriegt die zweite sogleich durch Division. Da ich die Zahlen klein gewählt habe, dürfte euer Taschenrechner mit der Darstellung und Verarbeitung kaum überfordert sein. Die erwähnten Profi-Programme berechnen solche Einzeldivisonen selbst mit sehr großen Zahlen wiederum in Bruchteilen von Sekunden.

Durch die Wahl kleiner Zahlen gab ich euch die Möglichkeit, zu schummeln, denn tatsächlich wollte ich euch ermuntern, auch die zweite Primadonna aus der Nachbarzahl zu bestimmen, um das Prinzip noch besser zu verstehen. Zuerst haben wir mit einem horizontalen Nachbarn gearbeitet, jetzt arbeiten wir mit einem vertikalen, falls

ihr einverstanden seid. Diese andere Nachbarzahl, wie sie aus der Gitterstruktur hervorgeht, lautet:

75.801.245

Diesmal ist es die nächstgrößere, und ich möchte euch bitten, mit dem Stift zunächst zu subtrahieren und das Ergebnis dann durch vier zu teilen oder von einem Zweitklässler teilen zu lassen. Als Ergebnis bekommt ihr auf jeden Fall die andere Primadonna, wie mit dem Taschenrechner schummelnd wahrscheinlich vorweggenommen. Der Abstand beträgt

30.892

Korrekt? Die Primadonna wäre demnach

7.723

Die Probe darauf hätte man zu meiner Zeit als Zweitklässler noch mit dem Stift gemacht, ihr langweiligen Schummler, denn niemand hatte einen Taschenrechner.

Nun, ist das nicht ein schönen Lied?

Dasselbe gilt für alle Zahlenformate: Erst subtrahieren, dann entweder durch zwei oder vier teilen, mehr ist es nicht. Wann zwei und wann vier erklären die Kinder im Buch.

Und wie versprochen brauchen wir nur die Reihenfolge der Gitterzahlen, um jeden RSA-Schlüssel im Handumdrehen zu faktorisieren.

Seht ihr, dass das Spiel gelaufen ist? Aus die Maus ganz ohne Quantencomputer und Shor-Algorithmus.

Ich schlage vor, dass wir im Anschluss noch eine große RSA-Zahl zusammen zerlegen, ein Biest von einer Zahl, bei der ihr nicht schummeln könnt, ein Monster, Leute, das wir nur mit Stift und Zettel zähmen werden.

Der achte Streich

Hier ist das Biest, hey, eine Zahl mit sehr vielen Ziffern, wie ihr sehen könnt:

27.997.833.911.221.327.870.829.467.638.722.601.
621.070.446.786.955.428.537.560.009.929.
326.128.400.107.609.345.671.052.955.
360.856.061.822.351.910.951.365.788.637.105.
954.482.006.576.775.098.580.557.613.
579.098.734.950.144.178.863.178.946.
295.187.237.869.221.823.983

Hübsch. nicht? Und jetzt zerlegt mal schön, es sind genau zwei Primzahlen enthalten, soviel darf ich verraten, jede bestehend aus einhundert Ziffern.

Aufgrund der ungeheuren Menge von Möglichkeiten bietet ein solcher Schlüssel im Prinzip einen recht guten Schutz, je größer das Zahlenbiest, desto besser, denn die Möglichkeiten wachsen fast exponentiell.

Andererseits ist das Biest wie alle anderen RSA-Biester Bestandteil meiner Gitterstruktur! Was haltet ihr also davon, zwei Nachbarzahlen zu nehmen und dann mit dem Stift in einer Viertelstunde simsalabim die Primfaktoren auszurechnen?

Wäre es nicht genial?

Ich gebe euch zunächst eine horizontale Nachbarzahl aus dem Gitter, kleiner als das RSA-Biest selber, wie ihr vielleicht sehen könnt. (Oder auch nicht.) Hier ist sie jedenfalls:

27.997.833.911.221.327.870.829.467.638.722.601.
621.070.446.786.955.428.537.560.009.929.
326.128.400.107.609.345.671.052.955.
360.856.045.970.612.001.994.699.721.942.934.
271.521.887.201.299.146.865.829.173.
657.630.074.267.232.643.117.542.642.
024.424.419.259.741.453.049

Ihr wisst, was zu tun ist: Das Ergebnis der Subtraktion dividieren, hier durch zwei, schon habt ihr die Primaballerina in all ihrer Herrlichkeit. (Als ich Drittklässler war, haben wir solche Übungen morgens vor dem Zähneputzen erledigt. Allerdings hatten wir nicht ständig so ein Ding am Kopf, sag schon. Mikrowelle, genau. Irgendwann ist die Hirnmasse schätzungsweise gar.)

Hier noch die vertikale Nachbarzahl, die ich für euch ausgewählt habe:

27.997.833.911.221.327.870.829.467.638.722.601.
621.070.446.786.955.428.537.560.009.929.
326.128.400.107.609.345.671.052.955.
360.856.068.887.275.779.756.906.031.182.315.
910.878.935.314.117.493.380.952.863.
626.397.341.887.696.421.370.537.792.
695.304.333.782.278.000.681

Sie ist größer als das RSA-Biest, ein Zugeständnis an eure Begeisterungsfähigkeit, wie ich sie einschätze, denn seht doch nur: Auch da müsst ihr den Abstand nur durch zwei teilen, um die Ballerina am Wickel zu kriegen.

Die Kinder erklären im Buch, wie es möglich ist, dieses Schonprogramm für euch aufzulegen. Aber Hand aufs

Herz, Leute: Selbst wenn ich euch jeweils durch vier hätte teilen lassen, so wäre das doch ein lächerlicher Aufwand für eine dermaßen gewaltige Aufgabe. Oder seht ihr das genauso? (Die Kinder im Buch machen etwas Ähnliches mit einer Kilometerzahl.)

Ihr habt quasi im Handumdrehen die Primfaktoren einer Monsterzahl bestimmt, während die Chaos-Clubs dieser Welt von früh bis spät erzählen, dass auch viel kleinere Schlüssel sicher genug seien für eure vertraulichen Mitteilungen.

Tatsächlich habt ihr ein Wunder vollbracht, denn die besten Spezialisten dieser Welt, äußerst fähige, von mir uneingeschränkt bewunderte und auf exakt diese Thematik spezialisierte Genies, waren bis dato nicht in der Lage, das zu leisten. Sie müssen rumprobieren und halten Dutzende oder Hunderte parallel rechnende Computer jahrelang damit beschäftigt, wobei smarte Algorithmen zum Einsatz kommen, die das Ausprobieren gewissermaßen systematisieren. (In diesem Fall das »Allgemeine Zahlkörpersieb«.)

Nehmt es tief in euch auf, bevor ihr lest, wie ausgewiesene Zahlentheoretiker und vergleichbare Kapazitäten mit der kleinen Aufgabe umgehen, die *ihr* soeben freihändig erledigt habt.

Was muss ich da hören, die Probe wollt ihr machen?

Ihr wollt wissen, ob ihr euch vertan habt bei der Behandlung des Zahlenmonsters? Nun, freut mich riesig, dass ihr's tatsächlich in Angriff genommen habt. Das ist heute nicht mehr selbstverständlich.

Ihr findet das Ergebnis im Netz unter dem Suchbegriff RSA-200. Schon gut, schon gut, dankt mir später. *

Der neunte Streich

Mit Simons kleinem Programm, das ist ja klar, dauert das, was ihr freihändig erledigt habt, allenfalls Sekunden. Und selbstverständlich haben auch die vorgenannten Kapazitäten solche Programme oder können sich welche schreiben.

Was sie nicht haben, ist das Gitter.

Statt sich mit ihren Zahlkörpern rumzuschlagen, sollten sie mit der Gitterstruktur arbeiten, wie die Kinder im Buch sie erklären. Ist das Konsens?

Diese Struktur ist ein einzigartiges Wundergebilde mit verschränkten Reihungen, Entwicklungen, Gesetznäßigkeiten, Dynamiken, Zusammenhängen und Möglichkeiten. Und alles tanzt quasi im Walzertakt, wartet mal, das klingt gefährlich. Ich möchte wirklich niemanden ärgern.

Schaut euch zum Vergleich die digitale Datenverarbeitung an. Zuerst gibt es zwei Möglichkeiten, ja oder nein, korrekt? Bei der nächsten Speichergröße sind es bereits vier, und diese Progression entspricht exakt einem Walzerschritt: Rumm-Bummbumm.

Dann wird von vier auf acht, von acht auf sechzehn, von sechzehn auf zweiunddreißg usw. verdoppelt: immer dieselbe Progression, derselbe stochastische Takt: Rumm-Bummbumm. Klar soweit?

Während wir aber im digitalen Fall nur diese eine, ewig gleiche Progression haben, ist in meiner Gitterstruktur eine unendliche Fülle verschieden verschränkter Dynami-

ken vorhanden, die sich im gleichen (Walzer)-Takt und doch gewissermaßen multidimensional ausbreiten.

Darauf kann und will ich aber nicht näher eingehen, ich gehe statt dessen zurück zu jenem Siebeverfahren, mit dem die Experten bei ihren Näherungen an Monsterzahlen häufig arbeiten.

Das Faktorisieren des vorgenannten Monsters, wie von euch vor dem Zähneputzen erledigt, gelang im Jahr 2005, haltet euch fest, einem stattlichen Team von Zahlentheoretikern und anderen Experten mit Hilfe des »Zahlkörpersiebs« in bald zweijähriger Rechenzeit, und zwar durch einen Verbund von bis zu achtzig Rechnern.

Manche Wikis geben für das zentrale Siebe-Verfahren ein Laufzeit-Äquivalent von 55 CPU-Jahren eines bestimmten Rechnertyps an. Was *ihr* also im Halbschlaf nach einer Viertelstunde erledigt habt, würde mit der wissenschaftlichen Methode nach 55-jährigem Dauerbetrieb eines Computers ebenfalls gelingen. Er dürfte die ganze Zeit allerdings nichts tun als Zahlkörper auf wiederkehrende Sequenzen sieben. (Ich kann nicht erklären, was genau sie tun, weil ich es nicht weiß, tut mir leid.)

Jetzt stellt euch das vor! Diese Leistung sorgte damals für großes Aufsehen unter den Fachexperten dieser Welt, und die Leute der Uni Bonn, die dafür verantwortlich waren, bekamen weltweit Anerkennung. Verdientermaßen, denn sie hatten die Gitterstruktur ja nicht und kamen trotzdem irgendwann ans Ziel.

Könnt ihr sehen, wie der Hase läuft?

Die haben zwanzi Monate rotiert, (über die Vorbereitungszeit ist nichts bekannt), um einen einzigen Schlüssel durch Rumprobieren zu knacken, während sie dank der Kinder im Buch mit einem Bruchteil des Aufwands alle vergangenen, gegenwärtigen und zukünftigen RSA-Schlüssel dieser Größenordnung hätten erledigen können. Alle auf einen Streich. Sie müssten nie wieder Rumprobieren, sondern könnten jeden gewünschten Faktor in Sekunden auslesen. Sie hätten einen Dauerlutscher und darüber hinaus.

Denn tatsächlich hätten sie ohne jede Aunahme auch alle Primzahlen dieses Zahlenbereichs durch einfache Scan-Verfahren aus derselben Struktur heraus bestimmt. (Ich habe in diesem Zusammenhang vorgeschlagen, den Algorithmus, aus dem die Reihenfolge der Gitterzahlen hervorgeht, BOTH-Radar zu nennen: Man bekommt beides zugleich. Wer weiß im Übrigen, was noch!)

Und nun erinnert euch. Habt ihr oder habt ihr nicht die Nachbarzahlen subtrahiert, um Primadonnen zu kriegen? Na also! Diese schönsten aller Zahlen strukturieren, zusammen mit ihren unechten Zwillingen, siehe Buch, das Gitter durch und durch, weshalb wir umgekehrt nur addieren müssen, um es aufzubauen.

Gleichförmige Additionen, das dürft ihr glauben, werden von Computern aber in Windeseile erledigt, selbst wenn sie im Hauptzweck und vordergründig durchs Internet surfen. Und nun erst unsere Überwacher und andere Halunken! Sie müssen nur popeln und warten, bis sie das Gitter der benötigten Größenordnung im Kasten haben, dann liegen alle Geheimnisse offen.

Werden Grundbucheinträge bei euch zuhause digital erfasst? Das ist verlockend. Ob verschlüsselt oder nicht, sie lassen sich jetzt ändern. »Hoppla, weg das Häuschen.« Natürlich nur ein Beispiel.

Habt ihr einen Betrieb? Bravo, dann müsst ihr die Steuererklärung und Voranmeldungen online übermitteln. Was soll ich sagen? Verschlüsselt oder nicht, das ist alles Makulatur. Nicht in fünfzehn Jahren, wenn es evtl. einen brauchbaren Quantenrechner gibt, nicht in zehn, wenn vielleicht noch smartere Algorithmen aufkommen, sondern jetzt. Da ist keine Hilfe, wie der Chinese sagt, ein echter Notstand hier und jetzt.

Während ansonsten hunderte Milliarden regelrecht zum Fenster hinausgeworfen werden, die Rede ist von Merkel-Deutschland, gibt es keinen müden Teuro, um den Notstand zu beheben. Und doch sitzen sie in der Klemme, die Regierungsverantwortlichen.

Einerseits fürchten ja nicht nur Diktatoren die sichere, unkontrollierbare Kommunikation der Bürger, wie mir scheint. Andererseits könnten die Bürger bald auch Regierungsgeheimpapiere lesen. Da wird Heulen und Zähneklappern sein!

Wenn es euch also gefällt, ihr Helden, lest jetzt in Zusammenfassung, warum wir unseren Staatsdienern Feuer unter dem Amtsarsch machen sollten.

Muss mein Buch konfisziert werden? Oder werden die nötigen Gelder endlich bewilligt? Motto: Nicht kleckern, sondern klotzen. Fähige Leute wären ja vorhanden.

Das Letzte

Im Grunde brauchen wir eine kryptographische Revolution, aber hey, ich bin extrem skeptisch, dass sie vom deutschen Michel ausgehen wird. Trotz bester Voraussetzungen. Dieses Land ist dermaßen kaputt, und in anderen EU-Enklaven, fürchte ich, sieht es kaum besser aus. Europa bewirbt sich um den Titel eines kontinentalen Irrenhauses, an den Früchten der vorherrschenden Politik, will mir scheinen, ist das ehrgeizige Anliegen bereits zu erkennen. Freiheit der Wissenschaften bedeutet jetzt, dass alles, was an die Aufklärung erinnert, im freien Fall ist: Vernunft, Rationalität, Widerspruch, Kritik . . .

Zwar gibt es hier und da Widerstandsnester – oder sollte man sagen, es gab sie? Glaubt irgendjemand da draußen, (um ein Beispiel zu nennen), dass wir gelegentlich vom spektakulären Hack einer aufgeweckten Chaos-Truppe hören werden, der auf den beschriebenen Notstand hinweist? Beispielsweise dadurch, dass er die selbst genutzte und überall empfohlene E-Mail-Verschlüsselung mit Hilfe eines kleinen Segments meiner Gitterstruktur knackt?

Und während sie diese Anfänger-Aufgabe lösen, würde der Gurkenhobel in der Ecke das Gitter der nächsten Größenordnung aufbauen, um das Feuer unter den Allerwertesten der schwerhörigen Entscheidungsträger immer heißer zu machen.

Ich höre euch lachen. Das sind Illusionen. Früher hatten die Leute Mumm in den Knochen und Humor, heute würde ein solches Tun Karrieren gefährden. Der Schnee ist nach offizieller Auslegung jetzt bekanntlich schwarz, und jede andere Deutung nicht wirklich zu empfehlen.

Sie sollten mein Buch wirklich konfiszieren. Es wäre die logische Konsequenz der allseits beliebten Zerstörungstendenzen. Tatsächlich ist es jugendgefährdend. Die kritische Einstellung und eine zersetzende Neigung, sich des eigenen Verstandes zu bedienen, ist nicht mehr zeitgemäß. Das will man der Jugend nicht mehr zumuten. Ist das exakte Gegenteil der betreuten Verblödung, pardon: der gewollten Absenkung des Bildungsniveaus. Man will die *Betroffenen* schließlich nicht überfordern.

Längst hat sich außerdem gezeigt, dass es genügt, eine Verschlüsselung nur oft genug als sicher zu *bezeichnen*, um dasselbe zu erreichen, ja, mehr sogar als durch Forschung: Man spart sich den lästigen Aufwand.

Eher glaube ich an den niederländischen Sinterclaas, (Bruder des stiefelfüllenden Nikolausi), der ein Pferd hat und in Spanien Urlaub zu achen pflegt laut Überlieferung, als dass ich der Bundesregierung vernüftige Entscheidungen zutraue. Egal, auf welchem Gebiet. Oder seht ihr das genauso?

Habe ich Regierung gesagt? Entschuldigung! Ist ein Begriff aus ferner Zeit, ein Relikt.

Heute muss man Hosenanzug sagen und fragen: »Ist er so schlicht, wie er spricht, oder schlichter?« Andererseits hochmodern, vielen gefällt das. Einige würden es selbst gern tragen, was gar nicht so einfach ist.

Nee, bin abgeschweift. Ich verstehe gar nicht, wie das passieren konnte. Liegt dann wohl an mir. Es wäre nur relevant, wenn es noch so was wie Verantwortung im Regierungsamt gäbe. Ist aber nicht mehr en vogue und hätte

verhehrende Auswirkungen. Eines würde mich persönlich interessieren. Habt ihr oder hat irgendjemand, den ihr kennt, jemals einen Hosenanzug zur Rechenschaft gezogen? War er teflonbeschichtet? Antwortet bitte bald!

Was könnt ihr also tun?

Ihr könntet wie die genannten politischen Schläferzellen morgens aufstehen und überlegen: »Was mache ich heute am Besten mal kaputt?«

Oder eben das Buch lesen, die Gitterstruktur studieren und eventuell eine Revolution einleiten.

Neben allem, was ich schon gesagt habe, hey: Es ist witzig, unterhaltsam und unkorrekt, sogar in der Mathematik. Habt ihr gewusst, dass acht mal acht dreizehn ergibt? Doch, es hängt von den kosmischen Gegebenheiten ab.

Im Buch wird natürlich alles erklärt. Außerdem macht es Vorschläge zur Bereicherung eures Speisezettels. Erdkrebs an Sauerampfer, um ein Beispiel zu nennen. Fast schon haute cuisine. (Wenn ich etwas mehr Zeit gehabt hätte, wer weiß, was da noch ausgekocht worden wäre.)

Und wenn ihr damit durch seid, lest sogleich auch meinen Freund Timo Haberbosch, der, Achtung, lieber Tänzerinnen aus Fleisch und Blut behandelt, als Zahlen-Primadonnen. Und zwar sehr »sinnlich«, wie Nadine O. in der Pressemitteilung schrieb. Motto:

»Man muss verrückt sein, einen solchen Liebesbrief zu schreiben.« Absolut korrekt!

Das Ergebnis ist immer dasselbe, Kinder: Man hat einen Dauerlutscher. Sechshundert Seiten bei Timo, zweihundert bei mir.

Ach ja, und gebt den Leuten diesen Link:

www.ummfrapp.de/prim/intro.pdf

Grüezi wohl, euer Thomas B.

PS: Auch hinter dem nachfolgenden Foto eines wachsenden, im Frühjahr jäh aufblühenden Beziehungsgeflechts verbirgt sich ein cooler Link. Einmal klicken genügt.

* 7.925.869.954.478.333.033.347.085.841.480.059.687.737.975.857.364.219.960.734.330.341.455.767.872.818.152.135.381.409.304.740.185.467 * 3.532.461.934.402.770.121.272.604.978. 198.464.368. 671.197.400.197.625.023.649.303.468.776.121.253.679.423.200.058.547.956.528.088.349

RSA-200/ minus zwei mal p1 (die große)

27.997.833.911.221.327.870.829.467.638.722.601.
27.997.833.911.221.327.870.829.467.638.722.601.

621.070.446.786.955.428.537.560.009.929.
621.070.446.786.955.428.537.560.009.929.

326.128.400.107.609.345.671.052.955.
326.128.400.107.609.345.671.052.955.

360.856.061.822.351.910.951.365.788.637.105.
...000.015.851.739.908.956.666.066.694.171.

360.856.045.970.612.001.994.699.721.942.934.

954.482.006.576.775.098.580.557.613.
682.960.119.375.475.951.714.728.439.

271.521.887.201.299.146.865.829.173.

579.098.734.950.144.178.863.178.946.
921.468.660.682.911.535.745.636.304.

657.630.074.267.232.643.117.542.642.

295.187.237.869.221.823.983
270.762.818.609.480.370.934

024.424.419.259.741.453.049

RSA-200/ plus zwei mal p2 (die kleine)

27.997.833.911.221.327.870.829.467.638.722.601.
27.997.833.911.221.327.870.829.467.638.722.601.

621.070.446.786.955.428.537.560.009.929.
621.070.446.786.955.428.537.560.009.929.

326.128.400.107.609.345.671.052.955.
326.128.400.107.609.345.671.052.955.

360.856.061.822.351.910.951.365.788.637.105.
...000.007.064.923.868.805.540.242.545.209.

360.856.068.887.275.779.756.906.031.182.315.

954.482.006.576.775.098.580.557.613.
956.396.928.737.342.394.800.395.250.

910.878.935.314.117.493.380.952.863.

579.098.734.950.144.178.863.178.946.
047.298.606.937.552.242.507.358.846

626.397.341.887.696.421.370.537.792.

295.187.237.869.221.823.983
400.117.095.913.056.176.698

695.304.333.782.278.000.681

RSA-200/ minus Nachbar klein horizontal/ durch zwei

27.997.833.911.221.327.870.829.467.638.722.601.
27.997.833.911.221.327.870.829.467.638.722.601.

621.070.446.786.955.428.537.560.009.929.
621.070.446.786.955.428.537.560.009.929.

326.128.400.107.609.345.671.052.955.
326.128.400.107.609.345.671.052.955.

360.856.061.822.351.910.951.365.788.637.105.
360.856.045.970.612.001.994.699.721.942.934.
000.000.015.851.739.908.956.666.066.694.171.
000.000.007.925.869.954.478.333.033.347.085.

954.482.006.576.775.098.580.557.613.
271.521.887.201.299.146.865.829.173.
682.960.119.375.475.951.714.728.439.
841.480.059.687.737.975.857.364.219.

579.098.734.950.144.178.863.178.946.
657.630.074.267.232.643.117.542.642.
921.468.660.682.911.535.745.636.304.
960.734.330.341.455.767.872.818.152.

295.187.237.869.221.823.983
024.424.419.259.741.453.049
270.762.818.609.480.370.934
135.381.409.304.740.185.467

Nachbar vertikal groß/ minus RSA-200/ durch zwei
27.997.833.911.221.327.870.829.467.638.722.601.
27.997.833.911.221.327.870.829.467.638.722.601.

621.070.446.786.955.428.537.560.009.929.
621.070.446.786.955.428.537.560.009.929.

326.128.400.107.609.345.671.052.955.
326.128.400.107.609.345.671.052.955.

360.856.068.887.275.779.756.906.031.182.315.
360.856.061.822.351.910.951.365.788.637.105.
000.000.007.064.923.868.805.540.242.545.209.
000.000.003.532.461.934.402.770.121.272.604.

910.878.935.314.117.493.380.952.863.
954.482.006.576.775.098.580.557.613.
956.396.928.737.342.394.800.395.250.
978.198.464.368.671.197.400.197.625.

626.397.341.887.696.421.370.537.792.
579.098.734.950.144.178.863.178.946.
047.298.606.937.552.242.507.358.846.
023.649.303.468.776.121.253.679.423.

695.304.333.782.278.000.681
295.187.237.869.221.823.983
400.117.095.913.056.176.698
200.058.547.956.528.088.349