Pfaff, Florian (2011): RSA - Ein Beispiel für die Verantwortung der Wissenschaft. Ein Denkanstoß.

Eine bekannte Regel im Finanzwesen lautet: Je höher der Gewinn sein soll, desto höher ist auch das Risiko der Geldanlage. Was passiert, wenn man den Bogen überspannt, erleben wir in Zeiten des Zusammenbruchs des Finanzwesens. Diese Regel gilt aber auch in anderen Bereichen, die maßgeblich unser Leben beeinflussen. Wir leben ja nicht nur von Kapital und seiner Anlage, sondern z.B. auch vom sicheren Fluss von Informationen. Dass auch hier Risiken verharmlost werden und ein "doch hoffentlich nie" eintretender, letztlich aber unabwendbarer Zusammenbruch in Kauf genommen wird, wenn wir so weitermachen, davon handelt dieser Denkanstoß. Die Rede ist vom "RSA"-Verfahren.

Was alles nicht mehr sicher ist, wenn dieses Verfahren nicht mehr “funktioniert”, kann hier nicht dargelegt werden. Weshalb die Aussage, RSA sei “praktisch sicher”, nicht haltbar ist, das soll nun dargestellt werden.

Man muss nicht Experte sein, um das Problem zu verstehen. Der Kern ist, dass die Sicherheit des Verfahrens und damit der Anwendungen – aller Anwendungen - (unter anderem) darauf beruht, dass es angeblich nicht möglich sei, in einer großen Zahl, die aus zwei (Prim-) Faktoren besteht, diese beiden Faktoren zu entdecken; vorausgesetzt, die Zahl ist lang genug. Ein paar Hundert Dezimalstellen sollten es schon sein.

Um die beiden Primfaktoren einer (großen) Zahl jedoch (schnell) zu finden, genügt es, eine der beiden Zahlen zu finden, die die vorgegebene lange Zahl ohne Rest teilen. Es geht also nur um eine einfache Division. Zumindest grafisch ist es im Gegensatz zu anders lautenden Vermutungen einfach, die sehr geringe Komplexität eines Produktes bzw. umgekehrt einer Division (das ist grafisch das Gleiche und darum geht es ja nur) zu zeigen.

Trägt man das Ergebnis auf der X-Achse und den Rest auf der Y-Achse ein, zeigt die daraus entstehende Gesamtgrafik vollständig die Komplexität der Division durch alle ganzen Zahlen von 1 bis zu der gegebenen Zahl selbst (Bild 1).

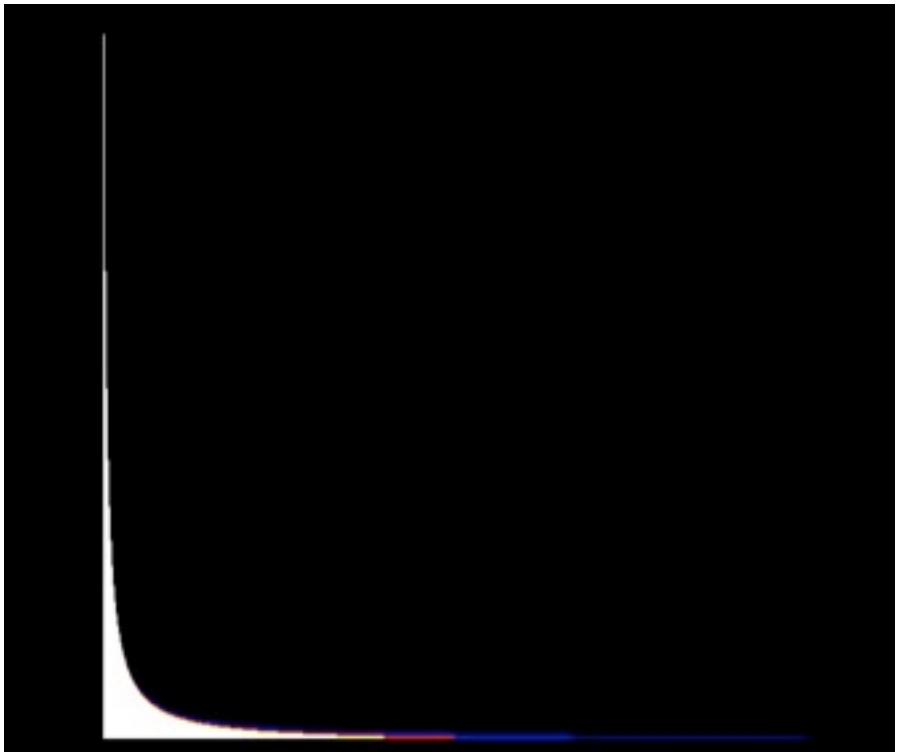

Bild 1

Wie der Grafik unschwer zu entnehmen ist, handelt es sich dabei lediglich um eine Hyperbel. Die einzige zusätzliche echte “Schwierigkeit” liegt darin, dass es sich nicht um eine stetige, sondern eine Treppenfunktion handelt. Es gibt also Stufen, wie man sieht.

Auch das ist allerdings kein k.o.-Kriterium, wenn man weiß, dass der gesuchte Teiler die einzige Zahl ist, die rechts von der Wurzel unten auf der X-Achse liegt. Zieht man von der langen Zahl 1 ab, muss der gesuchte Teiler dagegen exakt auf der Hyperbel liegen. Anders ausgedrückt: Vergrößert man die gegebene Zahl, “fällt” ein Punkt, der auf der Hyperbel liegt, genau auf die X-Achse “herunter” - genau das ist gesucht. Wenn man die gegebene lange Zahl umgekehrt um 1 verringert, muss ein Teiler ohne Rest genau auf der Hyperbel liegen. Dabei handelt es sich dann mit Sicherheit um den einzigen Punkt auf der Hyperbel, die sich sehr wohl (einfach) berechnen lässt.
Hier von einer großen Komplexität zu sprechen, wäre wohl fehl am Platz. Bei der in Bild 2 erkennbaren extrem einfachen Systematik wage ich die Behauptung, dass ein schneller Lösungsalgorithmus auch für so genannt “doppelt sichere” Primzahlen nur noch eine Frage von wenigen Jahren ist.

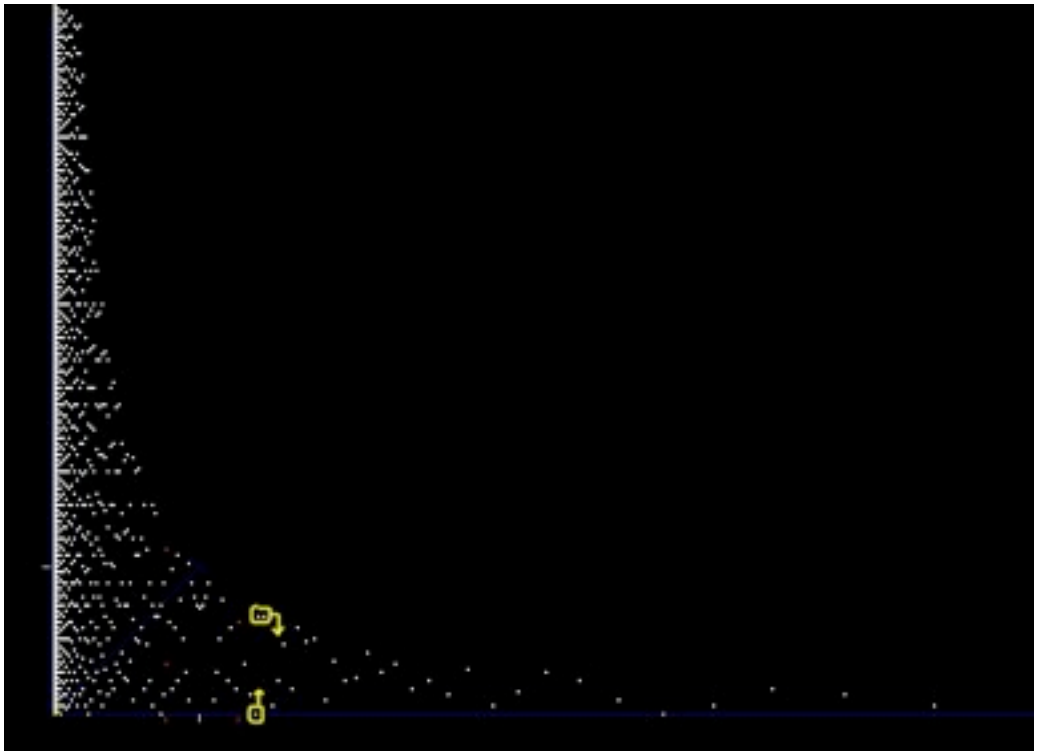

Bild 2

Bei einer solchen Regelmäßigkeit wird es jemanden geben, der einen Umkehr-Algorithmus findet, also eine Regel oder Formel, die sehr schnell zu jeder großen Zahl, die er um 1 erniedrigt, eine Zahl auf der Hyperbel ergibt. Das ist aber genau die Zahl, die die lange Zahl ohne Rest teilt – und zwar die einzige (rechts der Wurzel).

Wenn bald das RSA-Verfahren "stirbt", kann man nicht sagen, das mathematische Erdbeben habe niemand ahnen können.

Warum es sogar noch schneller gehen könnte, vielleicht schon in einem Jahr einen Lösungsalgorithmus gibt, liegt daran, dass man, um ein (ganzzahliges) Produkt zu bilden, gar keiner Multiplikation bedarf. Sie lässt sich in zwei Additionen und eine Division umwandeln. Mit Ausnahme der Fälle "Null" und a=b (Produkt identischer Zahlen bzw. Wurzel) gilt nämlich zudem die Formel:
(a + b) / (1/a +1/b) = a * b.

Nun sollten wir vielleicht doch einmal nachsehen, was alles nicht mehr sicher ist, wenn es das RSA-Verfahren nicht mehr gibt. Selbst Hobby-Mathematiker haben da gute Chancen aufzuzeigen, was die selbstbewusste Fachwelt für "unmöglich" erklärt.