Private Science Mitteilung Nr. 003

Leserbrief eines Kryptographen zu Alexander Gustav König: „Die Säulen Salomons“

Sehr geehrte Redaktion,

die Kryptographie ist nichts womit man leichtfertig herumspielen sollte. Wir haben zum Glück die RSA Verschlüsselung die uns allen große Sicherheit bietet. Wenn man das Buch ihres Autors König liest wird der Experte den Verdacht nicht los, dass der Autor keine Ahnung vom RSA Verfahren hat. Er erwähnt zwar den Eulerschen Satz wodurch jede natürliche Zahl m mit der Einerziffer (also z.B. x=71 → Einerziffer=1) hoch 4k+1 genommen in ihrer letzten Stelle dieselbe Einerziffer stehen hat wie vor dem potenzieren, aber dann macht sich dieser Pseudoheld K. immer Gedanken um große Primzahlen. Die sind doch angesichts der Säulen völlig egal! Es geht ja ums Primzahlprodukt! Also nochmal bitte zur Kenntnisnahme wie das wirklich funktioniert: Sei n ein Produkt zweier Primzahlen p und q, also n=p*q. Man wählt dann eine Zahl m die kleiner als n ist. Dann formuliert man den Eulersche Satz allgemein (das hat der Autor scheinbar nicht verstanden): $m^{k(p-1)*(q-1)+1}$. Der Rest von $m^{k(p-1)*(q-1)+1}$ dividiert durch n ist nun gleich m.

Jeder der eine verschlüsselte Nachricht empfangen möchte wählt nun zwei Primzahlen **p** und **q**, bildet ihr Produkt **n=p*q** und berechnet **(p-1)(q-1)**. Dann bestimmt er Zahlen **e** und **d** mit der Eigenschaft dass ihr Produkt **e*d** von der Form **k*(p-1)(q-1)** ist, wobei **k** irgendeine natürliche Zahl sein darf. Nun nennt er **e** zusammen mit **n** seinen öffentlichen Schlüssel und veröffentlicht diesen, andrerseits nennt er **d** seinen privaten Schlüssel und nennt diesen geheim. Jemand der diesem Menschen eine verschlüsselte Nachricht m senden möchte, verschlüsselt m mit Hilfe des öffentlichen Schlüssels. Das heißt: er stellt als Zahl dar, berechnet $\mathbf{m^e}$ und bestimmt dann den Rest, den $\mathbf{m^e}$ bei Division durch **n** liefert. Dieser Rest ist eine Zahl **c**, die der Geheimtext ist. Diese Zahl **c** schickt er an den Empfänger. Dieser wendet auf den Geheimtext seinen privaten Schlüssel an. Das heißt er berechnet $\mathbf{c^d}$ und bestimmt den Rest, der sich bei Division von $\mathbf{c^d}$ durch **n** ergibt. Der Satz von Euler garantiert, dass dabei die Originalnachricht **m** herauskommt.

Man muss als p und q solche Primzahlen wählen, dass man aus ihrem Produkt nicht auf p und q zurückschließen kann. 4 ist also weniger geeignet. Also sollte man für p und q große Primzahlen wählen. Im Jahr 2013 wählte man Primzahlen mit über 150 Dezimalstellen. Im Dezember 2009 lag der Weltrekord zur Faktorisierung einer RSA Zahl n=p*q bei einer Zahl mit 232 Dezimalstellen, die das Produkt von zwei Primzahlen mit je 116 Dezimalstellen ist.

Ich weiß zwar nicht was dieser König im Sinn hat, aber vom Produkt zweier Primzahlen, also dem Schnittpunkt dreier Schraubenlinien auf der Säule kann man relativ einfach auf die Primzahlen rückschließen und zwar egal wie groß, oder hab ich was falsch verstanden in dem Buch? Will dieser Irre nur um der Wahrheit willen alle verschlüsselten Geheimnisse offenlegen? Führt das nicht zur Unregierbarkeit des ganzen menschlichen Abschaums?

Ein besorgter Geheimdienstler,
Anonym

Antwort des Verlags:

wir verstehen sowieso nicht wie eine Botschaft aus 0,1,2,3,4,5,6,7,8 oder 9- also der möglichen Einerziffer irgendwas Sinnvolles aussagen kann. Es handelt sich hier wohl um metaphysische Anweisungen z.B: 5- verändere Dich! 1- fang an! 8- nicht schon wieder! 7- göttlich! Oder 0 Du Niete mit Potential! Allerdings ist RSA mit dem Quantencomputer eh überholt, meinen Sie nicht?

Gruß,
Ihr Charly Wiener