

Nikolaus Castell-Castell
MUDr. Tom Tietken

Prague Research Institute

Moeglichkeiten, auch ohne RSA-Entschluesselungs-Algorithmus Primzahlen zu identifizieren und RSA-Verschlusselungen (mittels einer speziellen Liste) indirekt zu dechiffrieren.

Ausgangssituation:

In einem bestimmten Teil der Logik (da wo viele identische Einzelteile nicht veraendert oder zerstoert, sondern nur umgestellt werden) sollte sich ein Ergebnis, das durch eine einfache Grundrechnungsart zustande kommt, auch mit einer einfachen Grundrechnungsart wieder zurueckverfolgen lassen.

Wenn es leicht ist, ein bestimmtes Ergebnis zu erhalten, wenn man zwei Zahlen (Faktoren) miteinander multipliziert, duerfte es nicht schwer sein, dieses Ergebnis mit einer gleich einfachen Grundrechnungsart wieder auf seine zwei Faktoren "zurueckzurechnen".

Seit 44 Jahren wird in der westlichen Welt, insbesondere bei Nachrichten, im Onlinehandel und im Zahlungsverkehr, einschliesslich dem der substanzlosen und manipulierten Kryptowaehrungen, der sog. RSA-Code zum Verschluesseln verwendet.

Dieser basiert auf dem Phaenomen, dass sich aus Primzahlen zwar per Multiplikation sog. "grosse Zahlen" herstellen lassen, dass es aber kein Verfahren gibt, diese grossen Zahlen umgekehrt wieder auf ihre Faktoren zurueckzurechnen (d.h. sie zu "faktorisieren").

Der Begriff "grosse Zahl" geht auf die Tatsache zurueck, dass fuer RSA-Verschlusselungen relativ grosse Primzahlen miteinander multipliziert werden, die entsprechend "grosse Zahlen" als Produkte herstellen. Von der Definition her wird hier allerdings jedes (auch noch so kleines) Multiplikations-Produkt "grosse Zahl" genannt, wenn sie aus zwei (auch noch so kleinen) Primzahlen hergestellt wurde.

Entsprechend der am Anfang genannten Vorgabe haben wir ein sehr einfaches Verfahren entwickelt, wie eine solche Rechnung vorgenommen werden kann.

Die bisherige Reaktion der mit dieser Behauptung konfrontierten Kryptologen (insbesondere Ron Rivest und seine zwei RSA-Miterfinder) waren Unglaeubigkeit, die damit begruetet wurde, dass unsere (noch nicht veroeffentlichte) wissenschaftlich gehaltene Darstellung nicht in Form eines Computerprogramms vorlag und sich darum in der Praxis nicht vorfuehren liess.

Solche praktischen Nachweise, inklusive jaehrliche Schaukaempfe von RSA und NSA, sind

sicherlich spannend und dienen der Ueberschaetzung des RSA-Codes, zumal, da sie seit 44 Jahren keine erwaehnungswerten Ergebnisse bringen. Und zusaetzlich sind sie fuer einen Teilnehmer vorteilhaft, weil er Wissen praesentieren kann, ohne seinen Quellcode preisgeben zu muessen.

Wenn wir allerdings, aus welchen Gruenden auch immer, (bis jetzt) vorgezogen haben, kein Computer-Programm zu schreiben und an keinen zero-knowledge-challenges teilzunehmen, dann muessen sich interessierte Nummertheoretiker eben die Muehe machen, unsere Arbeiten zu lesen und (was ohne Probleme jedem moeglich waere) zu verstehen. Das verursacht zwar die Muehe von Mitdenken und gegebenenfalls Umdenken, haette fuer einen Interessenten aber den Vorteil, zur Abwechslung mal einen neuen (einfacheren und u.E. sehr viel naeher liegenden) Ansatz kennengelernt zu haben.

Diese hier vorliegende Arbeit beschaeftigt sich ausdruuecklich nicht mit dem oben erwaehnten Verfahren, wie man eine Zahl, die aus der Multiplikation von zwei Zahlen (in der Praxis der Kryptographie sind dies Primzahlen) entstanden ist, wieder in diese beiden Primzahlen zerlegt ("faktoriert")!

Das hier vorliegende Manuskript soll lediglich veranschaulichen, was mit der Anwendung der Grundrechnungsarten, die jedem zugaeenglich sind, moeglich ist.

Zu diesem Zweck haben wir uns das Thema gestellt, wie man sogar ohne einen Algorithmus, der direkt "grosse Zahlen" (Produkte) zerlegt (faktoriert), zu aehnlich brauchbaren Ergebnissen kommen kann.

Ein Loesungsvorschlag koennte sein: Man kann die Primzahlen, aus denen grosse Produkte entstanden sind, auch indirekt erkennen, indem man Listen anlegt, in denen alle in Frage kommenden Zahlen, kontinuierlich anwachsend, geordnet abgelegt sind.

Die Grundidee des hier vorgeschlagenen Registers:

Der Grundgedanke fuer diesen Kompromiss hier (von uns "light"-Loesung genannt) besteht darin, Primzahlen indirekt zu ermitteln! Denn wenn Primzahlen, die dadurch definiert sind, dass sie durch nichts teilbar sind (ausser durch 0 und 1), bis jetzt nur mit grossem Aufwand erkannt werden koennen, dann liegt es nahe, benachbarte Zahlen, die ebenfalls die Endziffern 1, 3, 7 oder 9 aufweisen, und die sich im Gegensatz zu den Primzahlen durch andere Zahlen teilen lassen, zu erkennen.

Wahrscheinlich existieren Expertenvereinigungen, die schon sehr umfangreiche Verzeichnisse von Primzahlen angelegt haben. Um aber sicher sein zu koennen, bis zu dieser von ihnen bis jetzt hoechsten, gefundenen Primzahl keine kleineren Primzahlen "uebersehen" oder uebersprungen zu haben, bedarf es dieser hier von uns gefundenen Methode, nur mit Zahlen (d.h. auch nicht-Primzahlen!) zu rechnen, die 1,3, 7, 9 als Endziffern aufweisen, und diese Zahlen aller Art lueckenlos hochzuzaehlen!

Dabei sind die teilbaren Zahlen erkennbar, wenn man sie alle von unten nach oben hochzaehlt und dabei festhaelt, welche Zahlen miteinander multipliziert werden, um schliesslich (meist nach vielen weiteren Multiplikationen) die vorliegende Zahl zu ergeben.

Es ergeben sich dabei drei Arten von Zahlen:

a) Zahlen, die aus Multiplikationen von nicht-Primzahlen entstanden sind, insbesondere, wenn diese zuvor mehrfach miteinander multipliziert wurden, sind Zahlen, die nichts mit der RSA-Verschlüsselung zu tun haben.

b) Zahlen, die per Multiplikation aus nur 2 Primzahlen entstanden sind, sind sog. "grosse Zahlen", bei denen bei Ent-Schlüsselungen ihre Primzahlen gesucht (und im Register gefunden) werden.

c) Und alle Zahlen, die in dieser regelmaessigen Zahlenreihe von natuerlichen Zahlen von 1 bis 20001 usw. mit 1, 3, 7 oder 9 als Endziffer, keine Faktoren haben, also keine Zahlen, die zuvor miteinander multipliziert wurden, um diese vorliegende Zahl herzustellen, sind Primzahlen!

Alle diese drei Arten von Zahlen sind in dem vorgeschlagenen Register zu erkennen.

Weiteres zu den lueckenlosen Register-Zahlen mit den Endziffern 1, 3, 7 und 9:

Unser erster Algorithmus vom Februar 2020 zerlegt sog. grosse Zahlen direkt in ihre beiden Prim-Faktoren (d.h. in einen der beiden, der andere Faktor ergibt sich dann aus der Division der grossen Zahl durch den ermittelten ersten Faktor) und unterstellt dabei, dass es sich bei diesen Faktoren um Primzahlen handelt. Wenn die Zerlegung (Faktorisierung) nicht funktioniert, kann lediglich vermutet werden, dass die vorliegende Zahl keine sog. "grosse Zahl", sondern selbst eine Primzahl war.

Die hier vorgestellte Ergaenzung mit einem Register aber loest die Fragen zuverlaessiger und eindeutiger,

a) ob es sich bei den Faktoren tatsaechlich in beiden Faellen um Primzahlen handelt und

b) ob es sich bei der zu faktorisierenden vorliegenden Zahl tatsaechlich um eine "grosse Zahl" handelt, die per Multiplikation aus zwei Primzahlen entstanden ist..

Diese Eindeutigkeit wird besonders mittels dieses sich selbst aufbauenden Registers moeglich, da in diesem Register durch das regelmaessige Hochzaehlen saemtliche fuer das hier vorliegende Verfahren relevanten Zahlen garantiert enthalten sind! Dieses grundsatzlich unbegrenzte Register ist fuer die Entschlüsselung einer sog. grossen Zahl, z.B. in der Groesse von 2.000 Stellen, geeignet, kann mit einem extrem einfachen Algorithmus selbststaendig aufgebaut werden. Denn fuer den Aufbau und die Nutzung eines solchen Registers sind keine Grossrechenanlagen noetig, die nach der sog. "brute force" Methode alle Zahlen durchprobieren und Glueck benoetigen, um irgendwann (moeglich vor dem statischistischen Mittel) auf ein

passendes Ergebnis zu stossen.

Dieses selbst zu entwickelnde Zahlenregister ist in jedem Fall lueckenlos, da in ihm alle Zahlen bereits im Voraus vorhanden sind. Denn diese Zahlen werden nicht nur kardinal hochgezählt (wobei lediglich die Zahlen mit 0, 5, 2, 4, 6 und 8 als letzte Ziffer ausgeschlossen sind), sondern beschraenken sich in jeder 10-er-Reihe nur auf Zahlen mit den Endiffern 1, 3, 7 und 9. Damit ist das sog. Hochzaehlen innerhalb von aufsteigenden Zehner-Zeilen in nur vier Rubriken (1, 3, 7, 9) fuer das Programm sehr einfach und stets zweifelsfrei. Es kann keine Zahl vergessen werden. Denn das Register beinhaltet saemtliche existierenden natuerlichen Zahlen mit den Endziffern 1, 3, 7 oder 9. Und saemtliche Primzahlen und sog. "grossen Zahlen" haben stets nur die Endziffern 1, 3, 7 oder 9.

Falls eine natuerliche Person oder die eingesetzte Maschine zaehlen kann, ist der hier benoetigte numerische Aufbau ohne Rechenleistung moeglich. Denn die Zahlen sehen immer wieder nur wie folgt aus:

(1)	3	7	9	(1. Reihe mit den 4 o.g. Endziffern)
11	13	17	19	(2. Reihe mit den 4 o.g. Endziffern)
21	23	27	29	(3. Reihe mit den 4 o.g. Endziffern)

usw.

2001	2003	2007	2009	(201. Reihe mit den 4 o.g. Endziffern)
2011	2013	2017	2019	(202. Reihe mit den 4 o.g. Endziffern)
2021	2023	2027	2029	(203. Reihe mit den 4 o.g. Endziffern)

usw.

Alle Zahlen (auch die zu eruierenden Primzahlen und zu faktorisierenden "grossen Zahlen") sind also praktisch bereits in diesem Register lueckenlos vorhanden. Sie muessen nur noch definiert werden:

Es muss erkannt werden, welche dieser Zahlen Primzahlen sind, welche dieser Zahlen Produkte sind (und wenn sie das sind und aus Primzahlen entstanden sind, dann sind das die sog. "grossen Zahlen"), und welche Zahlen nicht oder nicht mehr zu diesen beiden vorgenannten Gruppen gehoeren und darum hier "sonstige Zahlen" genannt werden.

Die Bestimmung der Zahlen:

Es gibt in diesem Register also, mit der Zahl "3" beginnend (denn die "1" entfaellt hier bei den Einerstellen, denn sonst muesste $1*3$ gerechnet werden und dann waere das Ergebnis "3" keine Primzahl mehr, sondern eine sog. "grosse Zahl", die durch Multiplikation von $1*3$ entstanden ist) bis hin z.B. zu 2.000 oder mehr folgende Arten von Zahlen:

a) Primzahlen (die sich innerhalb der Tabelle daran erkennen lassen, dass bei den Zahlen der Tabelle auf der linken, also rechnerisch vorher liegenden, Seite, keine Faktoren vorhanden sind, die auf die jeweilige Primzahl hinweisen),

b) sog. "grosse Zahlen", auf die zwei miteinander multiplizierte Prim-Faktoren hinweisen und

c) sonstige Zahlen, die weder Primzahlen, noch sog. grosse Zahlen (also Produkte aus Primfaktoren) sind, aber ebenfalls die Endungen 1, 3, 7 oder 9 haben.

Sie koennen vorher Primzahlen und/oder grosse Zahlen gewesen sein, jetzt aber, nach weiteren Teilmultiplikationen, sind sie nur noch "sonstige Zahlen" und werden dies im Register auch immer bleiben. Sie fuellen das Register auf, sind aber selbst fuer die RSA-Verschluesselung nicht mehr zu gebrauchen.

Ausserdem gibt es Doppelbelegungen bei vielen "sonstigen Zahlen", d.h. solche Zahlen sind das Produkt von 2 oder mehr Faktorenpaaren. Die Anzahl der Faktorenpaare ist aber weniger wichtig, als die Tatsache, dass ueberhaupt Faktoren auf diese Zahl verweisen. Denn dann kann es sich bei dieser Zahl nicht um eine Primzahl handeln.

Auch als "grosse Zahl" ist eine solche doppel belegte Zahl uninteressant, weil sie bei Doppelbelegung von Faktoren keine der grossen Zahlen ist, die fuer eine Entschluesselung benoetigt wird.

Was das Finden der hier vorliegenden, u.E. neuen, Idee, mit allen Arten von Zahlen zu rechnen, solange sie die Endziffern 1, 3, 7 und 9 aufweisen, bis jetzt erschwert haben koennte:

Was den Zugang zu diesem offensichtlich neuen und naheliegenden Verfahren erschwert, ist das Nicht-Zusammenpassen von Festlegungen, was eine Primzahl ist und die teilweise Abweichung von Primzahlen und Primendziffern voneinander.

Bei 1, 3, 7 und 9 handelt es sich um sog. Primendziffern. Allerdings koennen auch alle anderen Arten von Zahlen (Primzahlen, sog. "grosse Zahlen" und sonstige ungerade Zahlen, sogar solche sonstigen Zahlen, die mit den Zahlen des Registers schon viele mal multipliziert wurden) diese Endziffern haben.

Auch ist die "9" eine Primendziffer, obwohl sie als Produkt aus den beiden Primzahlen $3 \cdot 3$ eine sog. "grosse Zahl" ist.

Aber auch vorgenannte Definition ist fraglich, wenn bedacht wird, dass die Primzahl "3" auch als "grosse Zahl" angesehen werden koennte, die aus $1 \cdot 3$ entstanden ist.

Fuer eine "grosse Zahl" sind allerdings zwei Primfaktoren noetig, und die "1" gehoert ausdruuecklich nicht zu den Primzahlen. Sie ist allerdings eine wichtige Prim-Endziffer.

Als Primzahl wurde stattdessen die "2" erkluert, die nach unserer eigenen (also offiziell falschen) Definition nichts weniger als eine Primzahl ist, sondern eine gerade Zahl. Auch als Primendziffer taugt sie nichts, da alle Zahlen, denen die "2" als Endziffer angehaengt wird, gerade Zahlen werden.

Nach eigener Definition, dass in dem hier vorgeschlagenen Register keine zwei Faktoren auf eine Primzahl hindeuten duerfen, ist die "5" tatsaechlich eine Primzahl (denn "5" dividiert durch die links vor ihr liegende "3" ist mit geradem Ergebnis nicht moeglich). Aber aus unserem Register

wurde sie verbannt, da sie als Endziffer jede Zahl (auch eine Trillion und 5) sofort durch 5 teilbar macht.

Was die in unserem Register stringente Verwendung nur von Zahlen mit den Endungen 1, 3, 7 und 9 bestaetigt, ist die Ordnung, dass Zahlen mit diesen Endungen (gleichgueltig, um was fuer Zahlen es sich dabei handelt) immer diese Endungen 1, 3, 7 oder 9 beibehalten.

Ein hilfreiches Phaenomen der vorgenannten Idee, dass alle Zahlen (gleichgueltig, zu welcher der drei genannten Arten sie gehoeren oder wie gross sie numerisch sind) ihre Endziffern 1, 3, 7 und 9 stets behalten:

Folgende 4 Rechenbeispiele zeigen, wie die Endziffern 1, 3, 7 und 9 (ganz gleichgueltig, welchen Zahlen sie als Endziffern angehaengt sind) durch Multiplikationen immer wieder nur 1, 3, 7 oder 9 als Endziffern hervorbringen. Der Einfachheit halber werden hier nur die einstelligen Endziffern multipliziert, aber auch bei mehrstelligen Zahlen faende das Gleiche statt: Zum Beispiel ergeben $3*7=21$, also ein Resultat mit der Endziffer "1". Dieses Prinzip bleibt auch bei allen numerisch groesseren Zahlen bestehen. Auch z.B. $27689473 * 56287$ ergeben mit = 1.558.557.366.751 ein Ergebnis mit "1" als Endziffer.

1-er Reihe, bei der der Zaehler "1" die Endziffern 1, 3, 7 und 9 multipliziert:

$$1*1=1; \quad 1*3=3; \quad 1*7=7; \quad 1*9=9;$$

3-er Reihe, bei der der Zaehler "3" die Endziffern 1, 3, 7 und 9 multipliziert:

$$3*1=3; \quad 3*3=9; \quad 3*7=(2)1; \quad 3*9=(2)7;$$

7-er Reihe, bei der der Zaehler "7" die Endziffern 1, 3, 7 und 9 multipliziert:

$$7*1=7; \quad 7*3=(2)1; \quad 7*7=(4)9; \quad 7*9=(6)3;$$

9-er Reihe, bei der der Zaehler "9" die Endziffern 1, 3, 7 und 9 multipliziert:

$$9*1=9; \quad 9*3=(2)7; \quad 9*7=(6)3; \quad 9*9=(8)1;$$

Bei diesem o.g. Rechenbeispiel befinden sich die Zaehler 1, 3, 7, 9 von oben nach unten senkrecht, und die gezaehlten Endziffern 1, 3, 7, 9 befinden sich von links nach rechts zaehlend in waagerechten Positionen.

Die Endziffern der vorgenannten Ergebnisse werden hier im Folgenden noch einmal wiederholt, um ihre Ordnung und immer gleichen Endziffern zu zeigen:

1	3	7	9
3	9	1	7
7	1	9	3
9	7	3	1

Der Anfang des Registers von 3 bis 293 (die Anfaenge der 3-er, 7-er, 9-er, 11-er, 13-er und 17-er Reihe):

a)

Das folgende Register (Quelle: Hiesiges Institut) beginnt links oben mit der "1".

Die ersten Multiplikationen sind $3*3$, $7*7$, $9*9$, $11*11$ usw., also Multiplikationen, in denen die beiden Multiplikatoren identisch sind. Mit einer solchen Multiplikation mit sich selbst erfolgt eine Zahlenreihe, bei der der Zaehler fuer die Dauer der Reihe konstant bleibt.

Bei der 3-er-Reihe ist die "3" der konstante Zaehler. Diese Reihe sieht dann so aus: $3*3$, $3*7$; $3*9$, $3*11$ usw.

Bei der 7-er-Reihe ist die "7" der konstante Zaehler: $7*7$, $7*9$; $7*11$; $7*13$ usw.

Wenn einer Zahl im Register also die Multiplikation mitgeteilt wird, aus der sie entstanden ist, koennen die Multiplikatoren z.B. $3*7$ auch als $7*3$ (oder die $3*9$ als $9*3$ usw.) geschrieben werden.

Aber aus Platzgruenden, und vor allem, um die Ordnung des sukzessive von unten nach oben Zaehlens nicht in Unordnung zu bringen, wird in diesem Register immer der kleinere Faktor zuerst genannt.

Ausserdem interessieren hier nicht die Reihenfolgen der Faktoren, sondern die Frage,

(1) ob es ueberhaupt Faktoren gibt (wenn dies naemlich nicht der Fall ist, handelt es sich bei der vorliegenden Zahl um eine Primzahl), und wenn dies der Fall ist, interessiert,

(2) ob beide Faktoren prim sind.

Auch auf der rechten Seite einer jeden Zahl im Register koennten weitere "Prognosen" geschrieben stehen. Also anstatt nur $3*3=9$ rechts von der "3" hinzuschreiben, koennte rechts von der "3" auch noch $3*7=21$, $3*9=27$, $3*11=33$; $3*13=39$ usw. stehen. Oder anstatt nur $7*7=49$ rechts von der "7" stehen zu haben, koennte dort auch noch $7*9=63$, $7*11=77$; $7*13=91$; $7*17=119$ usw. geschrieben stehen.

Letzteres ist aber aus Platzgruenden nicht moeglich, zumal jede, ab der Multiplikation mit sich selbst beginnende, Zahlenreihe unlimitiert lang ist.

Was die Bedeutung des folgenden Registers ausmacht, sind die drei Tatsachen:

1) Die zugrunde liegenden Zahlen des Registers sind leicht zu beschaffen, da dabei lediglich nur a) in Zehnerschritten kardinal hochgezaehlt werden muss und

b) pro Dekade immer nur die Zahlen mit den Endziffern in der Reihenfolge 1, 3, 7 und 9 aufgezeigt werden muessen.

Mit dieser Methode ist sichergestellt, dass saemtliche Zahlen, die auf 1, 3, 7 oder 9 enden, im Register erfasst sind.

2) Da Primzahlen stets mit 1, 3, 7 oder 9 enden, ist sichergestellt, dass auch saemtliche Primzahlen im Register enthalten sind.

3) Da auch die Produkte von Primzahlen stets mit 1, 3, 7 oder 9 enden, ist sichergestellt, dass auch diese Produkte (die "grosse Zahlen" genannt werden und die Zahlen darstellen, die bei RSA-Entschlüsselungen vorliegen) lueckenlos im Register enthalten sind.

Alle weiteren Zahlen mit den Endziffern 1, 3, 7 und 9, die keine Primzahlen oder sog. "grosse Zahlen" sind (oder nicht mehr sind, denn die wiederholten Multiplikationen veraendern sie) und hier "sonstige Zahlen" genannt werden, koennen bei der RSA-Verschluesselung nicht verwendet werden und blaehen das Register auf.

Sie sind aber fuer die Vollstaendigkeit saemtlicher Zahlen mit den Endziffern 1, 3, 7 und 9 noetig. Ohne sie waere keine Bestimmung moeglich, an welcher Stelle sich eine Primzahl oder sog. "grosse Zahl" numerisch befindet.

1 **PRIM 3** ($3*3=9$) **PRIM 7** ($7*7=49$) ($3*3=9$) **9** ($9*9=81$)
PRIM 11 ($11*11=121$) **PRIM 13** ($13*13=169$) **PRIM 17** ($17*17=289$) **PRIM 19**
 ($19*19=361$)
 ($3*7=21$) **21** ($21*21=441$) **PRIM 23** ($23*23=529$) ($3*9=27$) **27** ($27*27=729$) **PRIM 29**
 ($29*29=841$)
PRIM 31 ($31*31=961$) ($3*11=33$) **33** ($33*33=1089$) **PRIM 37** ($37*37=1369$) ($3*13=39$)
39 ($39*39=1521$)
PRIM 41 ($41*41=1681$) **PRIM 43** ($43*43=1849$) **PRIM 47** ($47*47=2209$) ($7*7=49$) **49**
 ($49*49=2401$)
 ($3*17=51$) **51** ($51*51=2601$) **PRIM 53** ($53*53=2809$) ($3*19=57$) **57** ($57*57=3249$) **PRIM**
59 ($59*59=3481$)
PRIM 61 ($61*61=3721$) ($3*21=63$ und $7*9=63$) **63** ($63*63=3969$) **PRIM 67** ($67*67=4489$)
 ($3*23=69$) **69** ($69*69=4761$)
PRIM 71 ($71*71=5041$) **PRIM 73** ($73*73=5329$) ($7*11=77$) **77** ($77*77=5929$) **PRIM 79**
 ($79*79=6241$)
 ($3*27=81$ und $9*9=81$) **81** ($81*81=6561$) **PRIM 83** ($83*83=6889$) ($3*29=87$) **87**
 ($87*87=7569$) **PRIM 89** ($89*89=7921$)
 ($7*13=91$) **91** ($91*91=8281$) ($3*31=93$) **93** ($93*93=8649$) **PRIM 97** ($97*97=9409$)
 ($3*33=99$ und $9*11=99$) **99** ($99*99=9801$)
PRIM 101 ($101*101=10.201$) **PRIM 103** ($103*103=10609$) **PRIM 107** ($107*107=11449$)
PRIM 109 ($109*109=11881$)
 ($3*37=111$) **111** ($111*111=12321$) **PRIM 113** ($113*113=12769$) ($3*39=117$ und
 $9*13=117$) **117** ($117*117=13689$) ($7*17=119$) **119** ($119*119=14161$)
 ($11*11=121$) **121** ($121*121=14641$) ($3*41=123$) **123** ($123*123=15129$) **PRIM 127**
 ($127*127=16129$) ($3*43=129$) **129** ($129*129=16641$)
PRIM 131 ($131*131=17161$) ($7*19=133$) **133** ($133*133=17689$) **PRIM 137**
 ($137*137=18769$) **PRIM 139** ($139*139=19321$)
 ($3*47=141$) **141** ($141*141=19881$) ($11*13=143$) **143** ($143*143=20449$) ($3*49=147$ und
 $7*21=147$) **147** ($147*147=21609$) **PRIM 149** ($149*149=22201$)
PRIM 151 ($151*151=22801$) ($3*51=153$ und $9*17=153$) **153** ($153*153=23409$)
PRIM 157 ($157*157=24649$) ($3*53=159$) **159** ($159*159=25281$)

$(7 \cdot 23 = 161)$ **161** ($161 \cdot 161 = 25921$) **PRIM 163** ($163 \cdot 163 = 26569$) **PRIM 167**
 $(167 \cdot 167 = 27889)$ $(13 \cdot 13 = 169)$ **169** ($169 \cdot 169 = 28561$)
 $(3 \cdot 57 = 171 \text{ und } 9 \cdot 19 = 171)$ **171** ($171 \cdot 171 = 29241$) **PRIM 173** ($173 \cdot 173 = 29929$)
 $(3 \cdot 59 = 177)$ **177** ($177 \cdot 177 = 31329$) **PRIM 179** ($179 \cdot 179 = 32041$)
PRIM 181 ($181 \cdot 181 = 32761$) $(3 \cdot 61 = 183)$ **183** ($183 \cdot 183 = 33489$) $(11 \cdot 17 = 187)$ **187**
 $(187 \cdot 187 = 34969)$ $(3 \cdot 63 = 189 \text{ und } 7 \cdot 27 = 189 \text{ und } 9 \cdot 21 = 189)$ **189** ($189 \cdot 189 = 35721$)
PRIM 191 ($191 \cdot 191 = 36481$) **PRIM 193** ($193 \cdot 193 = 37249$) **PRIM 197** ($197 \cdot 197 = 38809$)
PRIM 199 ($199 \cdot 199 = 39601$)
 $(3 \cdot 67 = 201)$ **201** ($201 \cdot 201 = 40401$) $(7 \cdot 29 = 203)$ **203** ($203 \cdot 203 = 41209$) $(3 \cdot 69 = 207$
und $9 \cdot 23 = 207)$ **207** ($207 \cdot 207 = 42849$) $(11 \cdot 19 = 209)$ **209** ($209 \cdot 209 = 43681$)
PRIM 211 ($211 \cdot 211 = 44521$) $(3 \cdot 71 = 213)$ **213** ($213 \cdot 213 = 45369$) $(7 \cdot 31 = 217)$ **217**
 $(217 \cdot 217 = 47089)$ $(3 \cdot 73 = 219)$ **219** ($219 \cdot 219 = 47961$)
 $(13 \cdot 17 = 221)$ **221** ($221 \cdot 221 = 48841$) **PRIM 223** ($223 \cdot 223 = 49729$) **PRIM 227**
 $(227 \cdot 227 = 51529)$ **PRIM 229** ($229 \cdot 229 = 52441$)
 $(3 \cdot 77 = 231 \text{ und } 7 \cdot 33 = 231 \text{ und } 11 \cdot 21 = 231)$ **231** ($231 \cdot 231 = 53361$) **PRIM 233**
 $(233 \cdot 233 = 54289)$ $(3 \cdot 79 = 237)$ **237** ($237 \cdot 237 = 56169$) **PRIM 239** ($239 \cdot 239 = 57121$)
PRIM 241 ($241 \cdot 241 = 58081$) $(3 \cdot 81 = 243 \text{ und } 9 \cdot 27 = 243)$ **243** ($243 \cdot 243 = 59049$)
 $(13 \cdot 19 = 247)$ **247** ($247 \cdot 247 = 61009$) $(3 \cdot 83 = 249)$ **249** ($249 \cdot 249 = 62001$)
PRIM 251 ($251 \cdot 251 = 63001$) $(11 \cdot 23 = 253)$ **253** ($253 \cdot 253 = 64009$) **PRIM 257**
 $(257 \cdot 257 = 66049)$ $(7 \cdot 37 = 259)$ **259** ($259 \cdot 259 = 67081$)
 $(3 \cdot 87 = 261 \text{ und } 9 \cdot 29 = 261)$ **261** ($261 \cdot 261 = 68121$) **PRIM 263** ($263 \cdot 263 = 69169$)
 $(3 \cdot 89 = 267)$ **267** ($267 \cdot 267 = 71289$) **PRIM 269** ($269 \cdot 269 = 72361$)
PRIM 271 ($271 \cdot 271 = 73441$) $(3 \cdot 91 = 273 \text{ und } 7 \cdot 39 = 273 \text{ und } 13 \cdot 21 = 273)$ **273**
 $(273 \cdot 273 = 74529)$ **PRIM 277** ($277 \cdot 277 = 76729$) $(3 \cdot 93 = 279 \text{ und } 9 \cdot 31 = 279)$ **279**
 $(279 \cdot 279 = 77841)$
PRIM 281 ($281 \cdot 281 = 78961$) **PRIM 283** ($283 \cdot 283 = 80089$) $(7 \cdot 41 = 287)$ **287**
 $(287 \cdot 287 = 82369)$ $(17 \cdot 17 = 289)$ **289** ($289 \cdot 289 = 83521$)
 $(3 \cdot 97 = 291)$ **291** ($291 \cdot 291 = 84681$) **PRIM 293** ($293 \cdot 293 = 85849$)

.....und unbegrenzt so weiter
(Quelle: Autoren)

b)
Um die Reihenfolge der Multiplikationen und ihrer Ergebnisse und das Erkennen von Primzahlen noch plausibler darzustellen, eignet sich folgende Zusatztable (Quelle: Autoren):

Man verbindet graphisch (in einer Art Matrix) saemtliche natuerliche Zahlen mit den Endziffern 1, 3, 7 und 9 in der oben beschriebenen Reihenfolge in einer waagerechten Reihe mit genau denselben Zahlen in derselben Reihenfolge in der senkrechten Spalte links und laesst bei den Multiplikationen eine dieser beiden Zahlenreihen (in diesem Fall die Zahlen in der senkrechten Spalte links) als Zaehler fungieren.
Man erhaelt dabei Objekte (Produkte), die ebenfalls auf 1, 3, 7 oder 9 enden.

1	3	7	9	11	13	17	19	21	23	counted factors
3	9	21	27	33	39	51	57	63	69	3-s row
7		49	63	77	91	119	133	147	161	7-es row
9			81	99	117	153	171	189	207	9-s row
11				121	143	187	209	231	253	11-s row
13					169	221	247	273	299	13-s row
17						289	323	357	391	17-s row
19							361	399	437	19-s row
21								441	483	21-s row
23									529	23-s row
counting factors										etc.

Erklaerungen zur vorigen Tabelle:

Auf der Diagonalen von "1, 9, 49, 81, 121, 169, 289, 361 usw." (in Richtung nach rechts unten) wuerden auf der rechten Seite an den analogen Positionen genau dieselben Multiplikations-Ergebnisse wie auf der linken Seite dieser Diagonalen. Darum werden sie in dieser Graphik weggelassen.

Die Anfangszahlen auf dieser Diagonalen entstehen durch Multiplikationen mit sich selbst.

Um die gleichen Produkte auf der rechten und linken Seite der Diagonalen zu vermeiden, beginnt eine Zahlenreihe immer erst mit der Zahl, die diese Zahlenreihe einleitet, durch Multiplikation dieser Zahl mit sich selbst.

Indem jede neue Zahlenreihe mit der Multiplikation der Anfangszahl mit sich selbst beginnt, wird vermieden, dass z.B. eine Multiplikation in der Reihenfolge $7*3$ erfolgen muss. Die "7" wird erst ab "7" multipliziert, und zwar mit sich selbst ($7*7=49$). Die "21" zuvor entstand bereits bei der Multiplikation in der 3-er Reihe durch $3*7$ (und nicht $7*3$).

Diese Tabelle zeigt besonders anschaulich die moeglichen Reihenfolgen:

Man koennte zuerst die 3-er-Zahlenreihe, die mit der Selbstmultiplikation $3*3$ beginnt, "zu Ende" fuehren ($3*7=21$, $3*9=27$, $3*11=33$, $3*13=39$ usw.), was aber wegen ihrer Endlosigkeit nicht moeglich ist.

Und nach $7*7=49$ koennte mit der 7-er-Zahlenreihe ($7*9=63$; $7*11=77$; $7*13=91$; $7*17=119$ usw. fortgefahren werden.

Und danach waere die 9-er-Zahlenreihe und weitere Zahlenreihen (wie 11-er, 13-er, 17-er usw. an der Reihe.

Aber ein solches Verfahren ist wegen der unbegrenzten Laenge einer jeden Zahlenreihe nicht praktikabel.

Auch wenn vielstellige Zahlen in Registern und Tabellen graphisch nicht darstellbar sind, werden alle Zahlen mit den Endziffern 1, 3, 7, 9 nach der hier vorliegenden Theorie immer nur in genau dieser hier beschriebenen Weise geordnet! Dies also auch in der Vorstellung (ohne Register und Tabellen).

Die Zahlen werden kardinal hochgezaehlt, wobei je schrittweise groesser werdender 10-er Reihe immer nur die 4 Zahlen mit den Endziffern 1, 3, 7, 9 erfasst werden.

Dabei ergeben sich 5 Thesen:

1) Am Anfang dieses Zaehlens beginnen alle diese, in der hier geschilderten Weise ermittelten, Zahlen mit den Endziffern 1, 3, 7, 9 mit den Primzahlen 3 und 7.

Nach der Ausnahme "9" setzen sich diese Primzahlen fort (11, 13, 17, 19).

Dann folgt als naechste Ausnahme "21" (aus den Primfaktoren "3" und "7"), um danach mit der Primzahl "23" fortzufahren.

2) Da auch saemtliche Primzaehlen mit saemtlichen Primzahlen multipliziert werden, wird diese Zahlenreihe aus Primzahlen von Produkten unterbrochen, die sich aus diesen Multiplikationen der Primzahlen miteinander ergeben und in der Kryptographie "grosse Zahlen" genannt werden (large integers).

3) Da gemaess Postulat dieser Arbeit alle Zahlen mit allen Zahlen miteinander multipliziert werden, kommt es an spaeteren Stellen immer haeufiger dazu, dass Zahlen miteinander multipliziert werden, die

a) keine Primzahlen mehr sind und entsprechend auch keine "grossen Zahlen" (Produkte aus Primzahlen) mehr sind, sondern

b) nach ein paar weiteren Schritten nach eigener Benennung "sonstige Zahlen" werden.

Das sind Produkte aus einer Primzahl und einer "grossen Zahl" oder Produkte aus 2 "grossen Zahlen" oder Produkte aus dem Rest, d.h. zwei "sonstigen Zahlen".

4) Nach der Logik ist es vorstellbar, dass diese "sonstigen Zahlen", relativ zu den anderen Zahlen, immer haeufiger auftreten, zumal sie staendig weiter miteinander multipliziert werden.

5) Da Letztere ebenfalls stets die Endziffern 1, 3, 7, 9 aufweisen, waere die Behauptung naheliegend, dass es diese anwachsende Anzahl "sonstiger Zahlen" ist, die die Primzahlen und damit auch die sog. "grossen Zahlen", zunehmend verdraengt.

An der Stelle 81 wurden erstmalig 2 sog. "grosse Zahlen" miteinander multipliziert ($9*9$).

Danach folgen dann weitere solcher Produkte (aus $21*21$, $27*27$ usw.).

Und wenn danach deren Produkte (aus grossen Zahlen), z.B. $21(\text{grosse Zahl}) * 21(\text{grosse Zahl}) = 441(\text{sonstige Zahl})$ und daraufhin $441(\text{sonstige Zahl}) * 441(\text{sonstige Zahl})$

Zahl)=194.481(sonstige Zahl) zu Faktoren fuer weitere Multiplikationen werden (und immer sofort), handelt es sich auch wieder nur um "sonstige Zahlen".

Allerdings aus "sonstigen Zahlen", die aus bereits unuebersichtlich vielen Multiplikationen entstanden sind.

Genauere Benennungen werden bei den sog. "sonstigen Zahlen" von uns nicht vorgenommen, da diese sonstigen Zahlen fuer die Kryptographie keine Bedeutung haben.

Die Reihenfolge der Bearbeitungsschritte und das sukzessive Erkennen der Primzahlen:

Durch diese Zusatztafel wird deutlich, dass die Zahlenreihen (3-er, 7-er, 9-er, 11er, 13-er, 17-er, 19-er-Reihe usw.) nicht nacheinander abgearbeitet werden sollten, sondern, dass zuerst immer die direkte Umgebung der jeweils vorliegenden Zahl vervollstaendigt werden sollte, um fruehstmoeglich die Primzahlen und dadurch die sog. "grossen Zahlen" identifizieren zu koennen.

Es ist die Diagonale in der Tabelle, die die kardinale Reihenfolge der Schritte vorgibt und indirekt klarstellt, welche Zahlen Primzahlen sind:

a) In der waagerechten Zeile ganz oben, die die gezaehlten Faktoren zeigt, und in der senkrechten Spalte ganz links kommen die Zahlen 3 und 7 vor. Da diese Zahlen aber in den Reihen innen im Feld nicht vorkommen, sind 3 und 7 als Primzahlen zu erkennen.

b) Zwischen 9 und 23 fehlen im Feld die Zahlen 11, 13, 17, 19, 23, wodurch diese als Primzahlen erkannt werden.

c) Genau in dieser Weise kann unbegrenzt fortgefuehrt werden:

Auf der Diagonalen fehlen zwischen 49 und 81 die Zahlen: 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79. Davon finden sich im Feld die Zahlen 51, 57, 63, 69 (hier in der Tabelle nicht sichtbar, da die $69=23*3$ erst an 23. Stelle der links senkrecht stehenden Zaehler auftritt) und 77 wieder, sodass die Zahlen 53, 59, 61, 67, 71, 73, 79 als Primzahlen uebrig bleiben usw.

Divisionen als Moeglichkeit, ohne Register und Tabellen dieselben Resultate zu erzielen:

Wenn keine optisch sichtbaren oder sonstwie abrufbaren Register oder Tabellen der hier beschriebenen Art vorliegen, kann man auch von der einen vorliegenden Zahl direkt ausgehen und fragen: "Ist dies eine grosse Zahl, die fuer eine Entschluesselung in zwei Primzahlen zu zerlegen ist?".

Oder man geht im Falle einer Verschluesselung von zwei vorliegenden Zahlen aus und fragt vor ihrer Multiplikation miteinander: "Sind diese beide Zahlen beides Primzahlen?"

Beide Fragen koennen durch Divisionen beantwortet werden, die in der gleichen Art wie der hier beschriebenen (d.h. nur mit Zahlen mit den Endziffern 1, 3, 7, 9 zu rechnen) vorgenommen werden.

Zahlenbeispiel fuer Division:

Es liegt also eine vielstellige Zahl vor, die die Endziffern 1, 3, 7 oder 9 hat, der aber nicht anzusehen ist, ob sie eine Primzahl, eine sog. "grosse Zahl" oder eine "sonstige Zahl" ist und aus wievielen Teilmultiplikationen diese "sonstige Zahl" besteht.

Indem diese durch alle hier aufgezeigten Zahlen (3, 7, 9, 11, 13, 17, 19, 21, 23 usw.) in genau dieser hier vorliegenden Reihenfolge dividiert wird, kommt man "irgendwann" (nach der Wahrscheinlichkeit nach 50% aller Moeglichkeiten, in der Praxis aber sehr viel frueher, da ja nur zwei von mehreren Moeglichkeiten gesucht werden: Ist die vorliegende Zahl eine Primzahl oder ist eine vorliegende Zahl eine sog. "grosse Zahl" aus zwei Primzahlen?) zu der gewuenschten Loesung.

Die Anzahl der Divisionen wird dadurch verkuerzt, dass ja nur herausgefunden werden soll, 1) ob es sich um eine Primzahl handelt. Schon bei der ersten Teilbarkeit, ist klar, dass keine Primzahl vorliegt und sich diese Zahl nicht zur Herstellung einer Verschluesselung eignet. 2) Soll aber eine Entschluesselung vorgenommen werden, kann davon ausgegangen werden, dass die zwei Faktoren der vorliegenden "grossen Zahl" Primzahlen sind (ein Versuch, bei Zweifel auch diese beiden Primzahlen noch einmal einzeln in der Weise, wie in Punkt 1) beschrieben, zu ueberpruefen, ist zusaetzlich moeglich).

Hier ein kleines Zahlenbeispiel, das genauso auch fuer unbegrenzt vielstellige Zahlen gilt:
-) Liegt z.B. die Zahl "7843" vor, koennen Divisionen durch 3, 7, 9, 11, 13, 17 usw. helfen, herauszufinden, dass 7843 keine Primzahl ist, da sie sich durch den Divisor "11" teilen laesst und dabei den Quotienten "713" ergibt.
-) Die verbleibende Frage ist nun, ob diese "713" eine sog. "grosse Zahl (d.h. ein Produkt aus zwei Primzahlen) ist, da einer ihrer Divisoren, die vorgenannte "11", eine Primzahl ist. Dafuer wird auch dieser jetzige Dividend "713" nacheinander durch die Zahlen 3, 7, 9, 11, 13, 17, 19, 21, 23 usw. dividiert und ergibt bei dem erfolgreichen Divisor "23" das Ergebnis "31". Damit ist belegt, dass auch die Zahl "713" keine Primzahl war. Allerdings ist "713" eine sog. grosse Zahl aus dem Primfaktoren "23" und "31".
-) Dass "23" und "31" Primzahlen sind, kann wiederum mit der gleichen Methode wie oben festgestellt werden: Tatsaechlich aber lassen sich weder "23" noch "31" durch 3, 7, 9, 11 (mehr Versuche sind nicht noetig, denn der Divisor sollte nicht groesser sein, als die Haelfte des kleineren Faktors, hier ist das die Haelfte von "23") teilen, sind also Primzahlen.
-) Als Gesamtergebnis stellt sich mithilfe dieser vorgenannten Divisionen heraus, dass die Zahl "7843" eine "sonstige Zahl" ist, die aus mehreren Multiplikations-Schritten entstanden ist, also fuer eine Ver- oder Ent-Schluesselung ungeeignet.

Schluss:

Das vollstaendige Vorhandensein aller Zahlen mit den Endungen 1, 3, 7 und 9 und ihre hochgezaehlte kardinale Anordnung und das Verfahren, alle diese Zahlen mit allen diesen Zahlen einzeln zu multiplizieren, ergeben die theoretischen Moeglichkeiten, a) saemtliche Primzahlen zu identifizieren und b) saemtliche "grosse Zahlen" zu zerlegen.

Quellenverzeichnis:

Es koennen hier keine Zitate und Quellen angegeben werden, da uns keine Quellen fuer diesen hier vorgelegten Ansatz oder Teile von ihnen bekannt sind.

Dieser Ansatz wurde hier im Institut mit einfachsten Mitteln und naheliegenden Ueberlegungen selbst entwickelt.

Nikolaus Graf zu Castell-Castell

Dipl. Vw. (Universitaet Hamburg)

Tom Hermann Tietken

MUDr. (Charles-University Prague)

Prague Research Institute

Zug (CH) und Prague (CR)

mob. 00420 778 037 633

fix line 00420 226 223 026