Wolfgang K. Seiler
Tel. 2515

B6, B4.18

18. Oktober 2019

7. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

a) Wenden Sie Pollards $p-1$-Methode an auf den Zahl $N = 100\,037$ mit Basis $a = 2$ und Suchgrenze $B = 4$!

b) Erhöhen Sie nun auf $B = 6$!

Aufgabe 2: *(5 Punkte)*

a) Die Zahl $N = 955\,353\,719$ ist das Produkt zweier nicht garzu weit voneinander entfernter Primzahlen. Finden Sie diese!

b) Wie viele Versuche hätten Sie gebraucht, wenn Sie nach der klassischen Vorgehensweise Fermats für $x = 1, 2, 3, \ldots$ nacheinander getestet hätten, ob $N + x^2$ ein Quadrat ist?

Aufgabe 3: *(7 Punkte)*

Bereits 1931 entwickelten D.H. Lehmer und R.E. Powers folgende Methode zur Faktorisierung ganzer Zahlen: Ist a/b eine Konvergente der Kettenbruchentwicklung von $\sqrt{N}$; so ist $q = a^2 - Nb^2$ eine relativ kleine Zahl; falls $q = x^2$ eine Quadratzahl sein sollte, haben wir eine Relation der Form $a^2 \equiv x^2 \bmod N$, die uns vielleicht zu einer Faktorisierung von N führt.

a) Warum verwenden D.H. Lehmer und R.E. Powers Kettenbrüche und nicht irgendwelche rationalen Approximationen von $\sqrt{N}$?

b) Berechnen Sie die ersten fünf Konvergenten a_i/b_i der Kettenbruchentwicklung von $\sqrt{15}$!

c) Welche davon liefern direkt eine Relation der Form $a_i^2 \equiv x_i^2 \bmod 15$, und wann führt diese Relation zu einer Faktorisierung?

d) Was ändert sich, wenn Sie anstelle der Relation $a_i^2 - 15b_i^2 = q_i$ die Relation

$$a_i^2 \equiv (q_i \bmod 15) \bmod 15$$

verwenden?

Aufgabe 4: *(5 Punkte)*

a) Berechnen Sie für $N = 31\,123\,153$ das Polynom $f(x) = \left(x - \left[\sqrt{N}\right]\right)^2 - N$ explizit!

b) Bestimmen Sie für jede einstellige Primzahl p die Menge aller $x \in \mathbb{Z}$, für die $f(x)$ durch p teilbar ist!

Abgabe bis zum Freitag, dem 25. Oktober 2019, um 11.55 Uhr