Wolfgang K. Seiler
Tel. 2515

B6, B4.08

2. April 2025

7. Übungsblatt Kryptologie

Aufgabe 1:

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 2:

Um 1931 entwickelten D.H. Lehmer und R.E. Powers folgende Methode zur Faktorisierung ganzer Zahlen: Ist p/q eine Konvergente der Kettenbruchentwicklung von $\sqrt{N}$; so ist $a = p^2 - Nq^2$ eine relativ kleine Zahl. Falls $a = x^2$ eine Quadratzahl sein sollte, haben wir eine Relation der Form $a^2 \equiv p^2 \bmod N$, die 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 p_i/q_i der Kettenbruchentwicklung von $\sqrt{15}$!

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

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

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

verwenden?

Aufgabe 3:

a) Zeigen Sie, daß das quadratische Polynom $f(x) = \left(x - \left[\sqrt{N}\right]\right)^2 - N$ die Diskriminante N hat!

b) Berechnen Sie dieses Polynom für $N = 31\,123\,153$ explizit!

c) Bestimmen Sie alle einstelligen Primzahlen p mit der Eigenschaft, daß es ganze Zahlen x gibt, für die $f(x)$ durch p teilbar ist, und geben Sie die Menge dieser Zahlen x jeweils an!

Aufgabe 4:

Faktorisieren Sie die Zahl $N = 851$ mit dem quadratischen Sieb mit Hilfe der Faktorbasis $\mathcal{B} = \{2, 5, 11, 17, 23\}$ und dem Siebintervall $[1, 40]$!

Abgabe und Besprechung am Mittwoch, dem 9. April 2025, um 15.30 Uhr