Wolfgang K. Seiler
Tel. 2515

A5, C201

24. Oktober 2007

7. Übungsblatt Kryptologie

Aufgabe 1: (*3 Punkte*)
Faktorisieren Sie die Zahl 990 675 589 nach der Methode von Fermat!

Aufgabe 2: (*5 Punkte*)

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

b) 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?

c) 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 3: (*4 Punkte*)
Faktorisieren Sie die Zahl $N = 56\,723$ nach der Kettenbruchmethode!

Aufgabe 4: (*8 Punkte*)
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 bis zum Dienstag, dem 30. Oktober 2007, um 12.00 Uhr