Kryptographie II – Übungsblatt 3

Aufgabe 1: Random Squares (9 Punkte)

A. Faktorisier die Zahl $N = 1504229$ mit Hilfe der Methode der Random Squares.

Verwende dabei folgende Werte anstelle von zufällig gewählten $x^{(j)}$:

$$x(1) = 1227 \quad , \quad x(2) = 6165 \quad , \quad x(3) = 2138 \quad , \quad x(4) = 3503 \quad , \quad x(5) = 83013 \quad .$$

(3 Punkte)

B. (i) Faktorisier die Zahl $N = 173441$ mit folgender „gelehrter“ Variante der Methode der Random Squares: Verwende Zahlen $x^{(i)}$ der Form $\lceil \sqrt{kN} \rceil + j$ mit kleinen $k, j \in \mathbb{N}$.

(4 Punkte)

(ii) Warum soll diese Idee (relativ) effizient sein? (2 Punkte)

Die Benutzung eines (Taschen-)Rechners ist in dieser Aufgabe und auch in der folgenden empfohlen.

Aufgabe 2: Faktorisieren mit Kettenbrüchen (16 Punkte)

Hier sollen Kettenbrüche bei der Faktorisierung helfen.

A. Berechne die ersten 15 Folgen der Kettenbruch-Entwicklung

$$\langle q_0; q_1, \dots, q_{14} \rangle$$

von $\sqrt{N}$ wobei $N = 53953$. (2 Punkte)

B. Berechne die ersten 15 Näherungsbrüche $\frac{n_k}{d_k} = \langle q_0; q_1, \dots, q_k \rangle$. (2 Punkte)

C. Beweise, dass $\left| \frac{n_k}{d_k} - \sqrt{N} \right| < \frac{1}{d_k^2}$. (3 Punkte)

D. Beweise, dass $n_k^2 - N d_k^2 = O(\sqrt{N})$. (3 Punkte)

E. Betrachte $n_k^2 \pmod{N}$. Was fällt auf? (2 Punkte)

F. Faktorisier $N = 53953$ mit Hilfe der Kettenbruchentwicklung von $\sqrt{N}$. (4 Punkte)

Abgabe: Freitag, 2.05.2008 bis 12:00 Uhr. Entweder im Kasten im Gebäude NA Ebene 02, oder per Mail an mansour.alsawadi@rub.de.