Wolfgang K. Seiler
Tel. 2515

A5, C201

31. Oktober 2007

8. Übungsblatt Kryptologie

Aufgabe 1: (*4 Punkte*)
Finden Sie alle Primzahlen $p \equiv 1 \bmod 41$ zwischen 10 000 und 11 000.
Hinweis: Jede zusammengesetzte Zahl $n \equiv 1 \bmod 41$ zwischen 10 000 und 11 000 hat einen Primteiler kleiner zwanzig.

Aufgabe 2: (*4 Punkte*)
Ihr geheimer ElGamal-Schlüssel ist 32; das System arbeitet mit der Basis $a = 2$ und modulo der Primzahl $p = 100\,003$.

a) Welchen öffentlichen Schlüssel müssen Sie bekanntgeben?

b) Entschlüsseln Sie die an Sie gerichtete Nachricht $(23\,094,\ 72\,676)$!

Aufgabe 3: (*4 Punkte*)
P.D.G. Wichtig verwendet für seine elektronischen DSA-Unterschriften die Parameter $q = 1\,009$, $p = 1\,124\,027$ und $g = 2\,952$. Sein öffentlicher Schlüssel ist $u = 9\,275$. Er unterschreibt die Nachricht 456 mit $(1006, 199)$, die Nachricht 789 mit $(1006, 202)$. Berechnen Sie seinen geheimen Schlüssel!

Aufgabe 4: (*4 Punkte*)
Zeigen Sie, daß drei eine primitive Wurzel modulo der Fermat-Primzahl $F_4 = 2^{16} + 1$ ist, daß sich also jede Zahl zwischen eins und 2^{16} modulo F_4 als Potenz von drei schreiben läßt!

Aufgabe 5: (*4 Punkte*)
$G = Gl_2(\mathbb{R})$ sei die Gruppe aller invertierbarer 2×2-Matrizen mit reellen Einträgen, und $M = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$. Bestimmen Sie intelligenter als durch systematisches Ausprobieren den diskreten Logarithmus der Matrix

$$A = \begin{pmatrix} 3\,363 & 2\,378 \\ 4\,756 & 3363 \end{pmatrix}$$

zur Basis M !

Abgabe bis zum Dienstag, dem 6. November 2007, um 12.00 Uhr