Wolfgang K. Seiler
Tel. 2515

A5, C201

16. November 2016

9. Übungsblatt Kryptologie

Aufgabe 1: *(5 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 mit Ausnahme von $10\,579 = 71 \cdot 149$ hat einen Primteiler kleiner zwanzig.

Aufgabe 2: *(5 Punkte)*
g sei eine primitive Wurzel modulo p und $a \in \mathbb{N}$. Zeigen Sie: $g^a \bmod p$ ist genau dann eine primitive Wurzel modulo p, wenn a teilerfremd zu $p - 1$ ist!

Aufgabe 3: *(5 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 4: *(5 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!

Abgabe bis zum Dienstag, dem 22. November 2016, um 15.25 Uhr