Wolfgang K. Seiler
Tel. 2515

B6, B4.18

30. Oktober 2019

8. Übungsblatt Kryptologie

Aufgabe 1: *(6 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 $[1, 40]$!

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)*
Ein Anwender wählt 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: *(6 Punkte)*

a) Zeigen Sie, daß die Zwei in $(\mathbb{Z}/295)^\times$ die Ordnung 116 hat!

b) Lösen Sie die Gleichung $2^x \equiv 9 \bmod 295$ durch Kombination der Methode von Pohlig-Hellman und dem *baby step – giant step* Algorithmus!
Hinweis: Bei so kleinen Zahlen empfiehlt es sich, die Anzahl der *baby steps* nicht viel größer als die Wurzel des Moduls zu wählen.

Abgabe bis zum Freitag, dem 8. November 2019, um 11.55 Uhr