Wolfgang K. Seiler
Tel. 2515

B6, B4.08

11. November 2022

10. Übungsblatt Kryptologie

Aufgabe 1:

a) Angenommen, ein DSA-Anwender wählt für die Unterschriften unter zwei verschiedene Nachrichten m und m' die gleiche Zufallszahl k. Zeigen Sie, daß jeder, der die beiden Nachrichten und die beiden Unterschriften kennt, den geheimen Schlüssel dieses Anwenders bestimmen kann!

b) 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 2:

a) Stellen Sie eine Tabelle der diskreten Logarithmen modulo 19 zur Basis zwei der Zahlen von 0 bis 18 zusammen!

b) Berechnen Sie mit Hilfe dieser Logarithmentafel die Zahlen

$$a = 13 \cdot 17 \bmod 19, \quad b = 13! \bmod 19 \quad \text{und} \quad c = 13^{100} \bmod 19\,!$$

Aufgabe 3:

a) Zeigen Sie, daß $p = 113$ eine Primzahl ist!

b) Modulo $p = 113$ gelten die Kongruenzen $3^8 \equiv 7 \bmod p$ und $2^{14} \equiv 3^{56} \equiv 112 \bmod p$ (die Sie *nicht* nachrechnen müssen). Bestimmen Sie die Ordnungen der Elemente zwei, drei und sechs in $(\mathbb{Z}/113)^\times$.

c) Bestimmen Sie den diskreten Logarithmus modulo p von zwölf zur Basis drei!

Aufgabe 4:

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 eine des *baby step – giant step* Algorithmus mit dem chinesischen Restesatz!
Hinweis: Bei so kleinen Werten von p empfiehlt es sich, die Anzahl der *baby steps* nicht viel größer als die Wurzel des Moduls zu wählen.

Besprechung am Mittwoch, dem 16. November 2022, um 15.30 Uhr