Wolfgang K. Seiler
Tel. 2515

B6, B4.08

30. April 2025

9. Übungsblatt Kryptologie

Aufgabe 1:

a) Finden Sie die kleinste dreistellige Primzahl $p \equiv 1 \bmod 11$!

b) Welche Primzahlen p zwischen 100 und 200 sind von der Form $2p'+1$ mit einer Primzahl p'?

Aufgabe 2:

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 3:

Vom vorigen Übungsblatt kennen wir die diskreten Logarithmen modulo 23 zur Basis fünf:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

Berechnen Sie mit Hilfe dieser Logarithmentafel die Zahlen

$$a = 13 \cdot 17 \bmod 23, \quad b = 13! \bmod 23 \quad \text{und} \quad c = 13^{100} \bmod 23\,!$$

Aufgabe 4:

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 5:

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

b) Lösen Sie die Gleichung $2^x \equiv 9 \bmod 295$ mit dem *baby step – giant step* Algorithmus und 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.

Abgabe und Besprechung am Mittwoch, dem 7. Mai 2025, um 15.30 Uhr