

## 11. Übung zur Vorlesung Kryptographie

**Achtung 1:** Nächste Woche gibt es 2 Übungsgruppentermine: **Montag**, 5. Juli, 10:15 wie gewohnt im HS F; **Mittwoch**, 7. Juli, 8:15 wie gewohnt in Raum A7-0-025.

**Achtung 2:** Dies ist das **LETZTE** Übungsblatt für dieses Modul.

**Achtung 3:** Abgabetermin für die Bonusaufgabe ist **der 16.7.2004** (in der Vorlesung).

**Aufgabe 38:** Diffie-Hellmann **(4 Punkte)**

*Alice* und *Bob* vereinbaren mit Hilfe des Diffie-Hellmann-Protokolls einen symmetrischen Schlüssel  $K$ . *Oscar* fängt das Folgende ab:  $p = 43$ ,  $g = 3$ ,  $A = 30$ ,  $B = 24$ . Wie lautet  $K$ ?

*Hinweis:* Legen Sie sich eine Tabelle mit  $3^k \pmod{43}$  für  $k = 0, \dots, 41$  an. Zur Vereinfachung können Sie verwenden, dass  $3^{21+k} \equiv -3^k \pmod{43}$  für jedes  $k \in \mathbb{Z}$  gilt.

**Aufgabe 39:** ElGamal **(4 Punkte)**

*Alice* erhält den ElGamal-Chiffretext  $(y_1, y_2) = (24, 7)$ . Wie lauten ihr privater Schlüssel und der Klartext, wenn ihr öffentlicher Schlüssel  $(p, g, b) = (43, 3, 30)$  ist?

*Hinweis:* Man kann die vorige Aufgabe benutzen.

**Aufgabe 40:** Shanks **(6 Punkte)**

353 ist eine Primzahl und 3 ist eine Primitivwurzel modulo 353. Wenden Sie den Babystep-Giantstep-Algorithmus von Shanks „per Hand“ an, um ein  $x$  derart zu finden, dass

$$3^x \equiv 143 \pmod{353}$$

gilt.

**Aufgabe 41:** Pollard-Rho-DL **(6 Punkte)**

$p = 458009$  ist eine Primzahl und  $g = 2$  hat die Ordnung 57251 in  $\mathbb{Z}_{458009}^*$  (ist also *kein* Generator). Verwenden Sie den Pollard-Rho-DL-Algorithmus, um den diskreten Logarithmus von  $a = 56851$  zur Basis  $g = 2$  zu bestimmen. Benutzen Sie den gleichen Startwert  $(1, 0, 0)$  und die gleiche Gruppeneinteilung  $(G_1, G_2, G_3)$  wie in der Vorlesung (und im Skript). Finden Sie den kleinsten Index  $i$  mit  $b_i = b_{2i}$  und berechnen Sie dann den gesuchten Logarithmus.

*Hinweis:*  $i$  liegt ziemlich nah bei 500; es wird also kaum ohne Programm gehen.

**Aufgabe 42:** **Bonusaufgabe:** Existenz von Primitivwurzeln **(10 Punkte)**

Zeigen Sie, dass:

- es für  $n = 2$ ,  $n = 4$ ,  $n = p^e$  und  $n = 2p^e$  ( $p$  ungerade Primzahl,  $e \in \mathbb{N} \setminus \{0\}$ ) Primitivwurzeln modulo  $n$  in  $\mathbb{Z}_n^*$  gibt;
- es für alle anderen  $n$  *keine* Primitivwurzeln modulo  $n$  gibt.

Die Aufgabe eignet sich gut auch für Teil-Lösungsversuche (die dann natürlich auch Teil-Bonuspunkte geben), wie beispielsweise: zeige, dass es für Zahlen  $n = 4p$  ( $p$  Primzahl) keine Primitivwurzel gibt; oder: zeige, dass für Zahlen  $n = p^2$  Primitivwurzeln existieren.