**FTK3, WS 2023/24**
**3. Übungsblatt für den 13.11.2023**

1. Bestimme mithilfe von Satz 2.12 die Ordnung von 6 in $\mathbb{Z}_{131}^*$.

2. Bestimme mithilfe von Satz 2.12 die Ordnung von 3116701003 in $\mathbb{Z}_{3696837919}^*$.

3. Berechne den diskreten Logarithmus von 37 zur Basis 6 in $\mathbb{Z}_{131}^*$ mit einem einfachen Brute-Force-Angriff.

4. Implementiere den einfachen Brute-Force-Angriff in der Programmiersprache deiner Wahl. Versuche damit den diskreten Logarithmus von 1059878588 zur Basis 3116701003 in $\mathbb{Z}_{3696837919}^*$ zu berechnen und miss die benötigte Zeit. Falls das zu lange dauert, mache nur 1000000 (zufällige) Versuche und miss die benötigte Zeit. Rechne nun hoch auf die zu erwartende Gesamtzeit des Angriffs.

5. Berechne den diskreten Logarithmus von 37 zur Basis 6 in $\mathbb{Z}_{131}^*$ mit dem Baby-Step-Giant-Step-Algorithmus.

6. Implementiere den Baby-Step-Giant-Step-Algorithmus für $\mathbb{Z}_p^*$ ($p \in \mathbb{P}$) in der Programmiersprache deiner Wahl. Berechne damit den diskreten Logarithmus von 1059878588 zur Basis 3116701003 in $\mathbb{Z}_{3696837919}^*$. Miss die benötigte Zeit.

   → *Optional:* Berechne damit auch den diskreten Logarithmus von 50802253956985 zur Basis 175733327981079 in $\mathbb{Z}_{250559608662463}^*$. Miss die benötigte Zeit.

7. Berechne den diskreten Logarithmus von 37 zur Basis 6 in $\mathbb{Z}_{131}^*$ mit dem Pohlig-Hellman-Algorithmus.

8. Implementiere den Pohlig-Hellman-Algorithmus unter Verwendung des Baby-Step-Giant-Step-Algorithmus für $\mathbb{Z}_p^*$ ($p \in \mathbb{P}$) in der Programmiersprache deiner Wahl. Berechne damit den diskreten Logarithmus von 1059878588 zur Basis 3116701003 in $\mathbb{Z}_{3696837919}^*$. Miss die benötigte Zeit.

   → *Optional:* Berechne damit auch den diskreten Logarithmus von 50802253956985 zur Basis 175733327981079 in $\mathbb{Z}_{250559608662463}^*$.

   → *Optional:* Berechne damit auch den diskreten Logarithmus von $A$ zur Basis $g$ in $\mathbb{Z}_p^*$ mit den Parametern aus beiliegendem Textfile.