Kryptographie *WS 2012/13*
Barbara Baumeister

8. Übungsblatt

Abgabe: Donnerstag, 6.12.2012

Aufgabe 1 Sei $G = \mathbb{Z}_{1999}^*$.

(a) Überprüfen Sie, ob 1996 in $\langle 5 \rangle$ liegt.

(b) Berechnen Sie unter Verwendung eines Computer-Algebra-Systems den diskreten Logarithmus $\log_5 1996$ in G mit Hilfe des Baby-Step-Giant-Step-Algorithmus.

Aufgabe 2 Berechnen Sie mit dem Index-Calculus-Algorithmus unter Verwendung der Faktorbasis $\{2, 3, 5, 7, 11\}$ die Lösung von $5^x \equiv 13 \bmod 2053$.

Aufgabe 3 Sei A eine rechteckige Matrix über $\mathbb{Z}$ und sei p eine Primzahl. Für jeden ganzzahligen Vektor b sei das Gleichungssystem $Ax \equiv b \bmod p$ mit einem ganzzahligen Vektor x lösbar. Geben Sie an, wie man explizit eine ganzzahlige Lösung von $Ax \equiv b \bmod p^l$ für $l \in \mathbb{N}$ findet.
Hinweis: Ist $Ax \equiv b \bmod p^l$, so mache den Ansatz $A(x + py) \equiv b \bmod p^{l+1}$.

Aufgabe 4 Alice besitze den öffentlichen Schlüssel $(p, \alpha, \beta) = (107, 2, 80)$. Als Verifikation für eine ElGamal-Signatur gibt sie

$$v(x, u_1, u_2) = \text{ wahr genau dann, wenn } 80^{u_1} u_1^{u_2} \equiv 2^x \bmod 107$$

bekannt. Alice signiert die Nachricht x mit $(9, 93)$. Welche der folgenden Nachrichten $x = 10, x = 83, x = 17$ sind nicht von Alice?