Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

8. Übungsblatt

Abgabe: Donnerstag, 17.12.2015

Aufgabe 1 Wie kann man aus zwei ElGamal-Chiffretexten einen dritten ElGamal-Chiffretext machen, ohne den geheimen Schlüssel zu kennen? Wie kann diese Attacke verhindert werden?

Aufgabe 2 Der öffentliche Schlüssel von Alice ist $(p, \alpha, \beta) = (47, 5, 11)$. Bob schickt Alice den ElGamal-Chiffretext $(43, 4)$. Bestimmen Sie den zugehörigen Klartext.

Aufgabe 3 Sei $G = \mathbb{Z}^*_{1999}$.

(a) Überprüfen Sie, ob 1996 in $\langle 12 \rangle$ liegt.

(b) Berechnen Sie unter Verwendung eines Computer-Algebra-Systems den diskreten Logarithmus $\log_{12} 1996$ in G mit Hilfe des Baby-Step-Giant-Step-Algorithmus.

Aufgabe 4 Berechnen Sie mit dem Index-Calculus-Algorithmus unter Verwendung der Faktorbasis $\{2, 3, 5, 7, 11\}$ die Lösung von $7^x \equiv 13 \bmod 2039$.