Diskrete Mathematik *SoSe 2013*
Barbara Baumeister

9. Übungsblatt

Abgabe: Donnerstag, 13.06.2013

Aufgabe 1 Simmulieren Sie den Schlüsselaustausch zwischen Alice und Bob beruhend auf dem Konjugations-Such-Problem. Öffentlich bekannt sei die Gruppe

$$G = SL_3(\mathbb{F}_2) \text{ und das Element } w = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in G.$$

Suchen Sie geeignete $a, b \neq 1$ und führen Sie den Schlüsselaustausch durch.

Aufgabe 2 Der Schüsselaustausch von Anshel, Anshel und Goldfeld:
Es sind $G = Sym(5)$ und die Elemente $a_i = (i, i+1)$, $1 \leq i \leq 4$ und $b_1 = (123), b_2 = (234), b_3 = (345), b_4 = (1234)$ aus G gegeben. Alice wählt $x = (12345)$ und Bob $y = (25)$. Bestimme den gemeinsamen Schüssel K.

Aufgabe 3

(a) Benutzen Sie die Gruppe G und die Untergruppe H in Aufgabe 3 von Blatt 7 um mit dem Kryptosystem basierend auf dem Reidemeister-Schreier Algorithmus den Text "Bach" zu verschlüsseln. Verwenden Sie hierfür die Schreier-Transversale $T = \{b^n \mid n \in \mathbb{Z}\}$.

(b) Ist H eine geeignete Untergruppe für dieses Kryptosystem?

Aufgabe 4

(a) Sei G eine Gruppe, die transitiv auf einer Menge Ω operiert. Weiter sei w ein Element in Ω und $G_w = \{g \in G \mid g(w) = w\}$ der Stabilisator von w in G. Wähle zu jedem $t \in \Omega$ genau ein Element g_t, welches w auf t abbildet. Zeigen Sie, dass $T := \{g_t \mid t \in \Omega\}$ eine Transversale von G_w in G ist.

(b) Geben Sie eine Transversale von $Sym(n)_1 \cong Sym(n-1)$ in $Sym(n)$ an.