RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 15 / 03. Februar 2011

AUFGABE 1:
Zeigen Sie, dass das Eliminationsideal I_ℓ ein Ideal über $\mathbb{F}[x_{\ell+1}, \ldots, x_n]$ ist.

AUFGABE 2:
Bestimmen Sie alle Lösungen des folgenden Gleichungssystem über $\mathbb{R}$.

$$\begin{aligned} x_1^2 + 2x_2^2 &= 2 \\ x_1^2 + x_1 y_2 + y_2^2 &= 2 \end{aligned}$$

Gehen Sie dabei wie folgt vor: Bestimmen Sie die reduzierte Gröbnerbasis (bzgl. lex). Bestimmen Sie I_1 und $V(I_1)$ und erweitern Sie diese Lösung auf I.

AUFGABE 3:
Zeigen Sie, dass folgendes System keine Lösung besitzt.

$$\begin{aligned} xy + y + 1 &= 0 \\ x^2 + 2x + 1 &= 0. \end{aligned}$$