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 14 / 26. Januar 2011

AUFGABE 1:
Berechnen Sie $S(f, g)$ für lexikographische Ordnung mit $x > y > z$.

1) $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$,

2) $f = x^4y - z^2$, $g = 3xz^2 - y$,

3) $f = x^7y^2z + 2xyz$, $g = 2x^7y^2z + 4$,

4) $f = xy + z^3$, $z^2 - 3z$.

AUFGABE 2:
Benutzen Sie das Buchberger Kriterium, um zu entscheiden, ob folgende Mengen eine Gröbnerbasis bzgl. lexikographischer Ordnung mit $x > y > z$ bilden.

1) $\{x^3 - z, x^2 - y\}$,

2) $\{x^2 - y, y - z\}$,

3) $\{xy^2 - xz + y, xy - z^2, x - yz^4\}$.

AUFGABE 3:
Bestimmen Sie zum Ideal $I = \langle x^2y - 1, xy^2 - x\rangle$ eine minimale Gröbnerbasis bzgl. lexikographischer Ordnung mit $x > y$ an. Bestimmen Sie daraus die reduzierte Gröbnerbasis und geben Sie $V(I)$ an.