RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 11 / 10 July 2014

Pohlig-Hellmann algorithm

Exercise 1:
Let G be a group. Suppose that q is prime and that we have an access to an oracle $\mathcal{A}$ that solve discrete logarithm problem $\alpha^x = \beta$ in G whenever α has order q in $T_{\mathcal{A}}$ steps. Now let $\alpha \in G$ be an element of order q^e for some $e \geq 1$. Show how to solve the discrete logarithm problem $\alpha^x = \beta$ in $\mathcal{O}(eT_{\mathcal{A}})$.

Exercise 2:
Prove the following equalities:

1. $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle = \langle x^2 - 4, y^2 - 1\rangle$
2. $\langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle$

Exercise 3:
Let k be an infinite field, and let $f \in k[x_1, \ldots, x_n]$. Prove that $f = 0$ in $k[x_1, \ldots, x_n]$ if and only if $f : k^n \to k$ is the zero function. (*Hint.* To prove the non-obvious direction use the induction on n).