Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 9

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen					**Gruppe**	**Tutor**
1	2a	b	c	3	**Summe**	**bearbeitet**
1	1	1	1	1	4 Pkte=100%	

Aufgabe 1

In der Vorlesung wurde das Pohlig-Hellman-Verfahren nur für multiplikative Gruppen von Primkörpern $\mathbb{Z}_p^*$ mit $p = p_1 \cdot \ldots \cdot p_n + 1$ eingeführt, mit verschiedenen Primzahlen $p_1, \ldots, p_n$.

Wie sollte man das Verfahren anpassen, wenn z.B. $p = p_1^2 p_2 p_3 + 1$?

Aufgabe 2

Lösen Sie das diskrete Logarithmusproblem

a) $2^x = 19356956$ in $\mathbb{Z}_p^*$, p= 22493753 mit Hilfe des Baby-Step/Giant-Step Verfahrens,
b) $2^x = 64877795$ in $\mathbb{Z}_q^*$, q=75857209 mit Hilfe des Pollard-Rho-Verfahrens,
c) $2^x = 4129861$ in $\mathbb{Z}_r^*$, r= 76558673 mit Hilfe des Pohlig-Hellman-Verfahrens.

Aufgabe 3

Lösen Sie mit Hilfe des Pohlig-Hellman Verfahrens das diskrete Logarithmusproblem
$2^x = 22904651255958484536488100 7318$ in $\mathbb{Z}_p^*$, p=587685663648225002008697227 5827.