Kryptosysteme, Keymanagment (KSK3) für CMS
6. Übungsblatt für den 21. November 2006

21. Gegeben sei die Primzahl $p = 1223$ und die Primitivwurzel $g = 5$ modulo p. Bestimme die diskreten Logarithmen (in der Gruppe $\mathbb{Z}_p^*$) zur Basis g aller Primzahlen der Faktorbasis $\mathcal{F}(7) = \{2, 3, 5, 7\}$. Stelle dazu wie in der Vorlesung ein lineares Gleichungssystem auf und löse dieses unter Verwendung des Chinesischen Restsatzes.

22. (*Fortsetzung von Bsp. 21*) Gesucht ist der diskrete Logarithmus (in $\mathbb{Z}_p^*$) zur Basis g von $a = 605$. Weise zuerst nach, dass $\text{Mod}(a \cdot g^{71}, p)$ eine 7-glatte Zahl ist. Verwende diese Tatsache, um den diskreten Logarithmus von a mit Hilfe der diskreten Logarithmen der Faktorbasiselemente $2, 3, 5, 7$ zu berechnen.

23. Beschreibe den *Baby-Step Giant-Step* Algorithmus und führe ihn anhand eines Beispiels durch.