

Kryptographie II Übungsblatt 7

Abgabe bis Dienstag, 30.5.2006 NA 5/75.

Hausaufgabe 1 *Baby-Step-Giant-Step Algorithmus*

Berechnen Sie mit Hilfe des Baby-Step-Giant-Step Algorithmus den Diskreten Logarithmus von 67 zur Basis 5 in \mathbb{Z}_{103} .

Hausaufgabe 2 *Der Silver-Pohlig-Hellman Algorithmus*

1. Berechnen Sie mit Hilfe des Silver-Pohlig-Hellman Algorithmus den diskreten Logarithmus von 500 zur Basis 7 in \mathbb{F}_{601}^* .
2. Warum wird der Silver-Pohlig-Hellman Algorithmus praktisch unmöglich, wenn die Gruppenordnung durch eine Primzahl der Länge 60 Bit geteilt wird?
3. Wie kann man den Baby-Step-Giant-Step Algorithmus in Kombination mit dem Silver-Pohlig-Hellman Algorithmus nutzen, um Diskrete Logarithmen auch in der Situation von Aufgabenteil 2 zu berechnen?
4. Welche Anforderungen sollte man daher an die Gruppenordnung einer Gruppe G stellen, damit das Berechnen von Diskreten Logarithmen in G heutzutage praktisch unmöglich ist?