Übungen zur Vorlesung Angewandte Diskrete Mathematik

Institut für Reine Mathematik WS 08/09 – Blatt 07

Abgabetermin: Freitag, 05.12.2008 um 14:15 Uhr vor Beginn der Übung

---

1. Beim RSA-Verfahren wählt Teilnehmer **A** die Primzahlen $p = 13$, $q = 23$, und den Exponenten $e = 13$.

   (a) Geben Sie den privaten Schlüssel von **A** an. (4 P)

   (b) **B** möchte an **A** die Zahl 99 senden. Was erhält **A** ? (4 P)

   (c) **A** erhält von **C** die verschlüsselte Nachricht 159 . Wie lautet die Nachricht von **C** ursprünglich? (4 P)

   (d) **Z** hat durch Spionage den privaten Schlüssel aus Aufgabenteil (a) herausgefunden. Zeigen Sie, dass **Z** mit der Basis $a = 5$ erfolgreich die Zahl $N = pq$ faktorisieren kann. (4 P)

   (e) Zeigen Sie, dass die Wahl der Basis $a = 3$ in (d) nicht zum Ziel führt. (4 P)

   In Aufgabenteilen (b) – (e) benötigen Sie den schnellen Potenzieralgorithmus. Dabei dürfen Sie für die Zwischenschritte **ausnahmsweise** einen Taschenrechner benutzen.