Übungen zur Vorlesung Kryptographie

Abt. Reine Mathematik SS 06 – Blatt 8

Abgabetermin: Fr., 30.06.2006 um 12:30 Uhr vor Beginn der Übung

---

Für dieses Übungsblatt betrachten wir die Kongruenz $2^x \equiv -303 \pmod{1301}$.

1. Löse diese Kongruenz mit dem Giantstep-Babystep-Algorithmus
2. Löse diese Kongruenz mit dem Pollard-Rho-Algorithmus
3. Löse diese Kongruenz mit dem Pohlig-Hellmann-Algorithmus