Aufgabenblatt 09

PS Einführung in die Kryptographie

Andreas Schlager

21. Mai 2025

Inhaltsverzeichnis

Aufgabe 31. Recherchieren sie ein weiteres Kriterium zur Bestimmung einer Primitivwurzel (zu dem auf Slide 150 der VO) und implementieren sie Experimente, in denen sie, für wachsende Modulgrösse, den Zeitbedarf beider Kriterien bestimmen. Hinweis: z.B. in Mathematica sind diverse hilfreiche zahlentheoretische Funktionen - wie z.B. Faktorisierung - implementiert.

Aufgabe 32. Beweisen sie die Korrektheit der RSA Ver- und Entschlüsselungsformel für $(m_i, n) = 1$ und $(m_i, n) = 1$.

Aufgabe 33. Warum ist RSA in der bisherigen Beschreibung (sog. Textbook RSA) nicht IND-CPA? Wie wird mit RSA typischerweise diese Sicherheitsstufe erreicht?