PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *26.05.2025*
***Abgabe**: bis FR 23.05. 12:00 an uhl@cs.sbg.ac.at*

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.

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

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

VIEL ERFOLG !!