Angewandte Kryptographie 2 Prof. Dr.-Ing. Kerstin Lemke-Rust
SoSe 2023 Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 2

C.1 Untersuchung der Erfolgswahrscheinlichkeit des klassischen Teils des Shor-Algorithmus, verwenden Sie trotz kleiner Zahlen eine Langzahlbibliothek.

(a) Erzeugen Sie einen eigenen "kleinen" RSA-Schlüssel durch Auswahl von tabellierten Primzahlen. ("Klein" ist hier relativ zu verstehen, finden Sie Ihren Kompromiss für die Größe des RSA-Schlüssels und eine akzeptable Rechenzeit in der nächsten Aufgabe. Die Primzahlen sollten jeweils größer als 100 sein.)

(b) Berechnen Sie für alle möglichen Basen a Ihres RSA-Schlüssels die Periode r von $a^i \bmod n$ durch Ausprobieren für i und testen Sie für die gefundene Periode r, ob Sie n erfolgreich faktorisieren können.

(c) Geben Sie eine Statistik zur Erfolgswahrscheinlichkeit des klassischen Teils des Shor-Algorithmus für Ihren gewählten RSA-Schlüssel aus.