

8. Übung zur Vorlesung Kryptographie

Achtung: Nächste Woche gibt es 2 Übungsgruppentermine: **Montag**, 14. Juni, 10:15 wie gewohnt im HS F; **Mittwoch**, 16. Juni, 8:15 wie gewohnt in Raum A7-0-025.

Aufgabe 28: RSA-Verschlüsselung **(4 Punkte)**

Verschlüsseln Sie den Klartext `anrufumelf` unter den gleichen Voraussetzungen ($n = 11413$ und $e = 3533$, Zahlenbasis 26, Input-Blocklänge 2, Output-Blocklänge 3) wie auf Seite 72 des Skripts.

Aufgabe 29: *Fermat_Test* und *Miller_Rabin* **(4+4 Punkte)**

- (a) Finden Sie einen Zeugen a nach Fermat (Korollar 1.5.7) gegen die Primalität von $n = 341$, d.h., einen Zeugen, der den Ausgang (1) von *witness* provoziert.
- (b) Finden Sie einen Zeugen x nach Bedingung (5.3) gegen die Primalität von $n = 341$, d.h., einen Zeugen, der den Ausgang (2) von *witness* provoziert.

Aufgabe 30: *Pollard_Rho* **(4 Punkte)**

Simulieren Sie *manuell* den *Pollard_Rho*-Algorithmus mit der Zahl $n = 1111$ als Eingabeparameter. Welcher Faktor wird gefunden? Geben Sie eine Tabelle aller erzeugten Werte i, k, x, y, d , bis der erste Faktor gefunden wird.

Aufgabe 31: Quadratisches Sieb **(4 Punkte)**

Faktorisieren Sie $n = 10910563$ mit Hilfe zweier Zahlen $x_1 = 5827689$ und $x_2 = 6439273$ und der Kenntnis der Tatsache, dass beide Zahlen x_1 und x_2 Quadratwurzeln von $c = 5907404$ modulo n sind.

Aufgabe 32: *Miller_Rabin* **(10 Punkte)**

Bonusaufgabe: Finden Sie die Zahl

$$N = \min\{ n \in \mathbb{N} \mid 12 \leq n \wedge \text{witness}(2, n) \neq \mathbf{true} \wedge \text{witness}(3, n) \neq \mathbf{true} \}.$$

Hinweis: Für diese Zahl liefert der Zeuge $a = 5$ eine Rückgabe $\text{witness}(5, n) = \mathbf{true}$.