Prof. Dr. Jens Zumbrägel
WiSe 2023/24

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Top Secret · Geheimnisvolle Faktoren

Lehrerfortbildung 2023

Übung 1

Alice und Bob benutzen das RSA-Verfahren zur verschlüsselten Nachrichtenübertragung.

a) Der öffentliche Schlüssel von Alice lautet $(n, e) = (55, 13)$. Verschlüsseln Sie den Klartext $m = 8$.

b) Der öffentliche Schlüssel von Bob lautet $(55, 23)$. Bestimmen Sie seinen privaten Schlüssel (p, q, d).

Übung 2

Sei n eine RSA-Zahl.

a) Sei $n = 1457$ und angenommen $\varphi(n) = 1380$ ist bekannt. Finden Sie die Faktoren p und q von n.

b) (Low encryption exponent Attacke.)
Angenommen n_1, n_2, n_3 sind paarweise teilerfremde RSA-Moduli und wir erhalten drei Verschlüsselungen der Nachricht $m \in \mathbb{Z}$ modulo n_i mit $e = 3$. Angenommen, dass $m^3 < n_1 n_2 n_3$ gilt, zeigen Sie dass dann die Nachricht mittels der drittten Wurzel in $\mathbb{Z}$ gefunden werden kann.

Übung 3

Zeigen Sie: Wenn $2^m + 1$ eine Primzahl ist (wobei $m \in \mathbb{N}$), so ist m eine Zweierpotenz.

Hinweis: Sind $a, k \in \mathbb{N}$ und k ungerade, zeigen Sie dass $a+1$ Teiler von a^k+1 ist. Zerlegen Sie dann $n = k \cdot \ell$ mit ungeradem $k \in \mathbb{N}$ und betrachten Sie $a = 2^\ell$.

Übung 4

Seien p, q verschiedene ungerade Primzahlen und sei $n := p \cdot q$. Seien e und d ganze Zahlen derart, dass $\mathrm{ggT}(e, \varphi(n)) = 1$ sowie $e \cdot d = 1 \bmod \varphi(n)$ gilt, wobei φ die Euler-Funktion ist. Zeigen Sie: Für alle Zahlen $m \in \mathbb{Z}$ gilt dann

$$m^{e \cdot d} \equiv m \mod n\,.$$

Übung 5

Sei n eine zusammengesetzte Zahl.

a) Faktorisieren die Zahl $n = 9\,366\,341$ mit Pollards $p-1$-Methode.

b) Wenn $n = p \cdot q$ mit $p \approx q$, warum ist dann die Faktorisierung von n einfach? Faktorisieren Sie die Zahl $n = 99\,997\,501$.

Übung 6

Betrachten Sie das quadratische Sieb zur Faktorisierung von n.

a) Warum benötigt man für die Faktorbasis nur jene Primzahlen p für welche $n \bmod p$ quadratischer Rest ist?

b) Mittels der Faktorbasis $S := \{-1, 2, 3, 5, 11\}$, wenden Sie den Algorithmus auf $n = 29\,041$ an.