Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
08.07.2022

Datensicherheit und Kryptografie

12. Übung

Abgabe: Lösen Sie die Aufgabe **2**. Ihre Lösungen geben Sie bitte entweder

- bis zum 13.07.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 12.07.2022

ab.

1. Aufgabe:
Für eine gegebene Zahl m mit der Zerlegung $m - 1 = 2^t l$ mit $l \equiv 1 \pmod 2$ haben wir für den Miller-Rabin-Primzahltest die Zahl s durch

$$\exists a : a^{2^s l} \not\equiv 1 \pmod m \text{ und}$$
$$\forall a : a^{2^{s+1} l} \equiv 1 \pmod m$$

definiert.
Bestimmen Sie die Zahl s für die folgenden Carmichael-Zahlen aus den vorherigen Übungszetteln:

- $m = 561 = 3 \cdot 11 \cdot 17$,
- $m = 1729 = 7 \cdot 13 \cdot 19$,
- $m = 2465 = 5 \cdot 17 \cdot 29$ und
- $m = 8911 = 7 \cdot 19 \cdot 67$.

2. Aufgabe: $5 \cdot 2P$
Bestimmen Sie, ob die folgenden Zahlen Primzahlen sind.

- $m = 8481$,
- $m = 8911$,
- $m = 15841$,
- $m = 17377$ und
- $m = 41041$.

Hinweis: Pomerance et al. haben in „The pseudoprimes to $25 \cdot 10^9$“ gezeigt, dass es für Zahlen $m < 1373653$ ausreicht, den Miller-Rabin-Primzahltest mit $a = 2$ und $a = 3$ auszuführen.

3. Aufgabe:
Wir betrachten noch einmal die Elgamal-Signatur und die Elgamal-Verschlüsselung.
Alice hat den privaten Schlüssel $M_A = 383$, $S_A = 17$ und $g_A = 5$. Bob hat den privaten Schlüssel $M_B = 397$, $S_A = 13$ und $g_B = 13$.
Alice möchte die Nachricht $N = 123$ verschlüsselt und signiert übertragen. Wählen Sie geeignete Zufallszahlen und geben Sie alle benötigten Übertragungen und Rechnungen an.