Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
02.06.2022

Datensicherheit und Kryptografie

8. Übung

Abgabe: Lösen Sie die Aufgabe **1**. Ihre Lösungen geben Sie bitte

- bis zum 02.06.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe: (3+3+2+2)P
Wir betrachten noch einmal die (richtige) Elgamal-Signatur mit $M = 37$ und $g = 2$.

(a) Finden Sie ein Beispiel, in der die Formel

$$g^{S_{Al}r+ks} \equiv g^N \pmod{M}$$

erfüllt ist und $k = M - 1$ gilt.

Hinweis: Wählen Sie die Variable N als letztes.

(b) Finden Sie ein Beispiel, in der die Formel

$$g^{S_{Al}r+ks} \equiv g^N \pmod{M}$$

erfüllt ist und $1 < \text{ggT}(k, M-1) < M - 1$ gilt.

(c) Wie kann mit Hilfe der Primfaktorzerlegung von $M - 1 = 2 \cdot 2 \cdot 3 \cdot 3$ effizient entschieden werden, ob für ein gegebenes r die Ungleichung $\text{ggT}(k, M-1) > 1$ gilt?

Hinweis: g wurde so gewählt, dass

$$g^i \equiv 1 \pmod{M} \quad \Leftrightarrow \quad i \equiv 0 \pmod{M-1}$$

gilt.

(d) Welches Problem tritt auf, wenn $\text{ggT}(k, M-1)$ groß ist?

2. Aufgabe:
Kann Alice $g^{S_{Al}g^k+ks} \bmod M$ effizient berechnen?
Sind $g^{S_{Al}g^k+ks} \bmod M$ und $g^{S_{Al}(g^k \bmod M)+ks} \bmod M$ gleich?
Wenn nein, warum nicht und welches Problem ergibt sich für die Signatur?

3. Aufgabe:
Vergleichen Sie die Funktionswerte der Funktionen
$\log_2(\log_2(x))$, $\log_2(x)$, $log_2(x)^2$, $log_2(x)^3$, $log_2(x)^4$, $log_2(x)^5$, $log_2(x)^6$, x und $x \log(x)$
für die Funktionswerte
$x = 10$, $x = 10^3$, $x = 10^6$, $x = 10^9$ und $x = 10^{12}$.

4. Aufgabe:
Die Ordnung eines Elements a modulo p ist definiert durch

$$\mathrm{ord}_p(a) = \min\left(i | i > 0, a^i \equiv 1 \pmod{p}\right).$$

Zeigen Sie, dass es für jede Primzahl p ein a mit $\mathrm{ord}_p(a) = p - 1$ gibt.
Hinweise:
In Übung 6 haben wir gesehen, dass für Elemente a, b mit $\mathrm{ggT}(\mathrm{ord}_p(a), \mathrm{ord}_p(b)) = 1$ die Gleichung $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a)\,\mathrm{ord}_p(b)$ gilt.
Sie dürfen verwenden, dass wenn $P \neq 0$ ein Polynom mit Grad n ist, dann hat P höchstens n Nullstellen.
Zeigen Sie, dass für alle n, m, das Polynom $x^{nm} - 1$ durch $x^n - 1$ teilbar ist.