Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
27.05.2022

Datensicherheit und Kryptografie

7. Übung

Abgabe: Lösen Sie die Aufgaben **1** und **2**. Ihre Lösungen geben Sie bitte entweder

- bis zum 01.06.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 31.05.2022

ab.

1. Aufgabe: 4P
Wir betrachten die Elgamal-Signatur aus der Vorlesung vom 17.05.2022.
In der Vorlesung haben wir gesehen, dass die Signatur (g^k, s, N) mit $g^{S_A+ks} = g^N$ für $s = 1$ ohne den geheimen Schlüssel S_A gefälscht werden kann.
Zeigen Sie, dass man auch bei beliebigem s mit $\mathrm{ggT}(s, M-1) = 1$ die Signatur fälschen kann.

2. Aufgabe: 6P
Wir betrachten jetzt die (richtige) Elgamal-Signatur aus der Vorlesung vom 24.05.2022.
Alice möchte die Nachricht $N = 7$ signiert übertragen. Sie verwendet den Modul $M = 37$ und die Basis $g = 2$. Ihr geheimer Exponent ist $S_A = 11$ und ihr Zufallszahl ist $k = 5$.
Geben Sie an, welche Werte Alice berechnen muss, welche Werte Sie bei der Signierung überträgt und welche Werte Bob schon vorher kennen muss.

3. Aufgabe:
Die (richtige) Elgamal-Signatur kann gebrochen werden, wenn die Zufallszahl k wiederverwertet wird.
Zeigen Sie, dass wir Informationen über k effizient berechnen können, wenn verschiedene Nachrichten mit dem gleichen k signiert werden.
Wann können wir k aus den zwei Nachrichten exakt berechnen?
Hinweis: Aus

$$ab \equiv c \pmod{m}$$

folgt mit

$$b' = \frac{b}{\mathrm{ggT}(b,m)},\ c' = \frac{c}{\mathrm{ggT}(b,m)} \text{ und } m' = \frac{m}{\mathrm{ggT}(b,m)}$$

die Äquivalenz

$$a \equiv (b')^{-1}c' \pmod{m'}.$$