

# Datensicherheit und Kryptografie

## 7. Übung

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

- bis zum 26.05.2023 um 13:00 Uhr per Mail  
an `julian.pape-lange@informatik.tu-chemnitz.de`  
mit *Betreff:* DuK Hausaufgaben oder
- nach der Vorlesung am 23.05.2023

ab.

### 1. Aufgabe: 4P

Wir betrachten die folgende (brechbare) Elgamal-Signatur aus der Vorlesung.

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  $\text{ggT}(s, M - 1) = 1$  die Signatur fälschen kann.

### 2. Aufgabe: 6P

Wir betrachten jetzt die (richtige) Elgamal-Signatur aus der Vorlesung.

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

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

die Äquivalenz

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