5. Übungsblatt
Diskrete Strukturen (Winter 2019/20)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Dr. Stefan Lucks, Jannis Bossert
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`

Abgabe: Bis zum 07. Januar 2020 vor Beginn der Übung oder per E-Mail an `jannis.bossert(at)uni-weimar.de`. Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung.

Aufgabe 1 – Isomorphismus (4 Punkte)
Überprüfen Sie, ob die folgenden Gruppoide Isomorph sind.

a) $(\mathbb{Z}_7^*, \cdot)$ und $(\mathbb{Z}_6, +)$

b) $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_6, -)$

Hinweis: Beachten Sie dass für einen Generator $g \in \mathbb{Z}_p^*$ bekanntlich gilt: $g^{a+b} \bmod p = (g^a \cdot g^b) \bmod p$.

Aufgabe 2 – Diffie-Hellman-Schlüsselaustausch (3 Punkte)
Alice und Bob haben sich mit Hilfe des Diffie-Hellman-Schlüsselaustausches auf einen geheimen Schlüssel K geeinigt. Eve hat im Laufe des Austausches folgende Parameter von der unsicheren Leitung abgehört: $p = 67$, $g = 13$, $A = 64$, $B = 2$. Ermitteln Sie den geheimen Schlüssel K nur mit Hilfe dieser Informationen.

Aufgabe 3 – Secret Sharing (4 Punkte)
Um ein Geheimnis $S = p(0)$ eines Polynoms p nicht einer einzelnen Person anzuvertrauen, wurden 3 Paare $(x_i, p(x_i))$ an 3 Personen weitergereicht. Finden Sie an Hand der Wertepaare

$$(a_1, b_1) = (3, 207)$$
$$(a_2, b_2) = (6, 274)$$
$$(a_3, b_3) = (7, 53),$$

mit $a_i, b_i \in \mathbb{Z}_{503}$ das Geheimnis $S = p(0)$ mit Hilfe der Interpolationsformel von Lagrange heraus.

Aufgabe 4 – Irreduzible Polynome (6 Punkte)
Betrachten Sie den Körper $\mathbb{Z}_2[X]_{p(\mathtt{x})}$.

a) Zeigen oder widerlegen Sie: $p(\mathtt{x}) = \mathtt{x}^4 + \mathtt{x} + \mathtt{1}$ ist irreduzibel über $\mathbb{Z}_2$.

b) Zeigen oder widerlegen Sie: $p(\mathtt{x}) = \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x}^2 + \mathtt{1}$ ist irreduzibel über $\mathbb{Z}_2$.

c) Stellen Sie für alle Elemente aus $\mathbb{Z}_2[X]_{p(\mathtt{x})}$ mit $p(\mathtt{x}) = \mathtt{x}^3 + \mathtt{x}^2 + \mathtt{1}$ die Additions- und Multiplikationstabelle auf.

Aufgabe 5 – Galoiskörper Multiplikation (4 Punkte)

Berechnen sie folgende Aufgaben im $\mathbb{GF}(2^8)$ zum irreduziblen Polynom $p(x) = x^8 + x^4 + x^3 + x + 1$.

a) $(x^7 + x^6 + x + 1) \cdot (x^2 + 1)$

b) $(x^5 + x^4 + x^2) \cdot (x^2 + 1)$

Aufgabe 6 – CRC – Python (6 Punkte)

Implementieren Sie das CRC Verfahren von Folie 203 ff. der Vorlesung in Python3. Ihr Programm soll dabei zwei Parameter entgegen nehmen:

- Das Generatorpolynom P(x) von Grad n
- Eine Empfangene Nachricht der Länge $s + n$ Bit, wobei s variabel ist

Beide Eingaben sollen als Binärstring via Kommandozeilenparameter eingelesen werden. Ihr Programm soll ausgeben, ob ein Fehler bei der Übertragung aufgetreten ist und wenn nein, die entsprechende Nachricht.

Beispielaufruf:

```
python3 crc_xxxxxx.py 10001 011100110100
Die Nachricht 01110011 wurde fehlerfrei übertragen!

python3 crc_xxxxxx.py 10001 011100101100
Bei der Übertragung ist ein Fehler aufgetreten!

python3 crc_xxxxxx.py 10001 001100110000
Die Nachricht 00110011 wurde fehlerfrei übertragen!
```

Bitte senden Sie ihre Datei als `crc_<matrikel>.py` an `jannis.bossert(at)uni-weimar.de`.

Fröhliche Weihnachten und einen guten Start ins Neue Jahr!