# Übungsblatt 9

***Abgabe der schriftlichen Lösungen bis 30.06.2022, 24 Uhr***

**Aufgabe 44** ***mündlich***

(a) Ermitteln Sie den 64-Bit DES-Schlüssel $K$, der bei ungerader Parität der 8-Bit Subkeys $K_{(1)}, \ldots, K_{(8)}$ zum 56-Bit Schlüssel $K^- = \texttt{0123456789ABCD}$ (in Hexadezimaldarstellung) gehört.

(b) Zeigen Sie, dass für alle $K, x \in \{0,1\}^{64}$ die Gleichung $\mathsf{DES}(\overline{K}, \overline{x}) = \overline{\mathsf{DES}(K, x)}$ gilt (hierbei bezeichnet $\overline{v}$ das bitweise Komplement des Bitvektors $v$).

**Aufgabe 45** ***mündlich***

(a) Zeigen Sie, dass der Kryptotext $y$ einer Feistel-Chiffre nach demselben Verfahren wieder entschlüsselt werden kann, wenn dabei die Rundenschlüssel in der umgekehrten Reihenfolge zur Anwendung kommen. Warum gilt dies auch für die DES-Chiffre?

(b) Fertigen Sie eine graphische Skizze des Key-Schedule Algorithmus' für die DES-Dechiffrierung an, der die zugehörigen Rundenschlüssel bei Eingabe $K$ in umgekehrter Reihenfolge generiert.

**Aufgabe 46** ***mündlich***

(a) Zeigen Sie, dass die vier DES-Schlüssel (in Hexadezimaldarstellung)

`0101010101010101, FEFEFEFEFEFEFEFE,`
`1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1`

schwach sind, indem Sie die zugehörigen Rundenschlüssel ermitteln, und beweisen Sie, dass der DES-Algorithmus keine weiteren schwachen Schlüssel hat.

(b) Zeigen Sie, dass alle schwachen DES-Schlüssel $K$ eine involutorische Chiffrierfunktion $\mathsf{DES}_K$ realisieren (d.h. es gilt $\mathsf{DES}_K = \mathsf{DES}_K^{-1}$).

(c) Ein DES-Schlüssel $K$ heißt semi-schwach, falls er genau zwei verschiedene Rundenschlüssel erzeugt (d. h. es gilt $|\{K^1, \ldots, K^{16}\}| = 2$). Bestimmen Sie die Anzahl aller semi-schwachen DES-Schlüssel und zeigen Sie, dass sie sich zu Paaren $\{K, K'\}$ mit $\mathsf{DES}_K = \mathsf{DES}_{K'}^{-1}$ kombinieren lassen.

**Aufgabe 47** ***mündlich***

Zeigen Sie, dass der Faktorring $\mathbb{Z}_m[x]/m(x)$ genau dann ein Körper ist, wenn $m = p$ prim und $m(x)$ irreduzibel über $\mathbb{Z}_p$ ist.

**Aufgabe 48** ***mündlich***

(a) Bestimmen Sie das Restpolynom $q(x) = 2x^5 + x^4 + 4x + 3 \bmod 3x^2 + 1$ über $\mathbb{Z}_5$.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 im Polynomring $\mathbb{Z}_2[x]$. Stellen Sie jeweils die Additions- und Multiplikationstafeln für den Faktorring $\mathbb{Z}_2[x]/m(x)$ auf.

(c) Sei $m(x) = x^2 + 2$. Stellen Sie die Additions- und Multiplikationstafeln für den Faktorring $\mathbb{Z}_3[x]/m(x)$ auf. Ist $\mathbb{Z}_3[x]/m(x)$ ein Körper?

(d) Berechnen Sie das multiplikative Inverse von $a(x) = x^4 + x^2 + 2x$ im Faktorring $\mathbb{Z}_3[x]/m(x)$, wobei $m(x) = 2x^6 + x^3 + x^2 + 2$ ist. Ist $m(x)$ irreduzibel über $\mathbb{Z}_3$?

**Aufgabe 49** ***10 Punkte***

(a) Bestimmen Sie das Restpolynom $q(x) = p(x) \bmod m(x)$ über $\mathbb{Z}_7$ für die Polynome $m(x) = 3x^2 + 1$ und $p(x) = 2x^5 + x^4 + 4x + 3$.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad $\mathsf{deg}(m) = 2$ in $\mathbb{Z}_3[x]$.

(c) Stellen Sie die Additions- und Multiplikationstafeln für den Faktorring $\mathbb{Z}_3[x]/m(x)$ auf, wobei $m(x)$ das lexikographisch kleinste irreduzible Polynom vom Grad 2 in $\mathbb{Z}_3[x]$ ist.