

Übungsblatt 11

Abgabe der schriftlichen Lösungen am 25. 1. 2018 bis 13.10 Uhr

Aufgabe 51

mündlich, rechenintensiv

- Berechnen Sie die Rundenschlüssel K^0, \dots, K^{10} , die sich aus dem externen 128 Bit AES-Schlüssel $K = 2B7E151628AED2A6ABF7158809CF4F3C$ ergeben.
- Verschlüsseln Sie den Klartext $x = 3243F6A8885A308D313198A2E0370734$ mit K .

Aufgabe 52

mündlich

Der »normale« Ablauf einer Entschlüsselung beim AES erfolgt nach folgendem Schema:

```
1 AddRoundKey( $K^{10}$ )
2 ShiftRows-1
3 SubBytes-1
4 for  $i \leftarrow 9$  downto 1 do
5   AddRoundKey( $K^i$ )
6   MixColumns-1
7   ShiftRows-1
8   SubBytes-1
9 AddRoundKey( $K^0$ )
```

Zeigen Sie, dass alternativ auch dieselbe Reihenfolge der Operationen wie bei der Verschlüsselung benutzt werden kann.

Aufgabe 53

10 Punkte

Sei R der Polynom-Restklassenring $\mathbb{F}_{2^8}[y]/(y^4 + 1)$.

- Zeigen Sie, dass R kein Körper ist.
- Ist das Ringelement $a(y) = 03y^3 + 01y^2 + 01y + 02$ in R invertierbar?
- Zeigen Sie, dass die AES-Operation MIXCOLUMNS eine multiplikative Chiffre mit festem Schlüssel $a(y)$ im Ring R realisiert.

Aufgabe 54

mündlich

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $\text{ord}(a)$ und $\text{ord}(b)$.

- Zeigen Sie, dass ab die Ordnung $\text{ord}(ab) = \text{ord}(a)\text{ord}(b)$ hat, falls $\text{ord}(a)$ und $\text{ord}(b)$ teilerfremd sind.
- Lässt sich die Aussage in Teilaufgabe (a) zu $\text{ord}(ab) = \text{kgV}(\text{ord}(a), \text{ord}(b))$ verallgemeinern?

Aufgabe 55

mündlich

- Zeigen Sie, dass ein Polynom $p(x) \in \mathbb{F}[x]$ vom Grad $n \geq 1$ über einem Körper \mathbb{F} höchstens n Nullstellen besitzt.
- Zeigen Sie, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.
- Finden Sie Polynome $q_d(x) \in \mathbb{Z}_6[x]$ vom Grad $d = 1, 2$ mit möglichst vielen Nullstellen.

Aufgabe 56

mündlich

Sei G eine endliche Gruppe der Ordnung $\|G\| = m$ und sei 1 das neutrale Element von G .

- Zeigen Sie, dass für jedes $a \in G$ ein $k > 0$ existiert mit $a^k = 1$.
- Sei nun $\text{ord}(a) = k$. Zeigen Sie, dass die Menge $[a] = \{a^i \mid i \geq 0\}$ eine Untergruppe von G mit genau k Elementen bildet. Folgern Sie $k \mid m$ und $a^m = 1$.
- Zeigen Sie, dass genau dann $a^i = a^j$ ist, wenn $i \equiv_{\text{ord}(a)} j$ gilt.
- Zeigen Sie, dass $\text{ord}(a^i) = \text{ord}(a) / \text{ggT}(k, i)$ ist.
- Geben Sie einen Isomorphismus zwischen den beiden Gruppen $[a]$ und $(\mathbb{Z}_k, +)$ an.