Übungen zur Kryptologie 1 Wintersemester 07/08
Johannes Köbler/Sebastian Kuhnert

Übungsblatt 11

Aufgabe 48 (mündlich)

a) Berechnen Sie die Rundenschlüssel $K^0, \ldots, K^{10}$, die sich aus dem externen 128-Bit AES-Schlüssel

$$K = 2B7E151628AED2A6ABF7158809CF4F3C$$

ergeben.

b) Verschlüsseln Sie mit K den Klartext

$$x = 3243F6A8885A308D313198A2E0370734.$$

Aufgabe 49 (mündlich)

Der „normale“ Ablauf einer Entschlüsselung beim AES erfolgt nach folgendem Schema:

$\textsc{AddRoundKey}(K^{10})$
$\textsc{ShiftRows}^{-1}$
$\textsc{SubBytes}^{-1}$

```
for i:= 9 downto 1 do
```
   $\textsc{AddRoundKey}(K^i)$
   $\textsc{MixColumns}^{-1}$
   $\textsc{ShiftRows}^{-1}$
   $\textsc{SubBytes}^{-1}$
```
end
```
$\textsc{AddRoundKey}(K^0)$

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

Aufgabe 50 (mündlich)

Zeigen Sie, dass für jede Primzahlpotenz p^k die Kongruenz $x^2 \equiv_{p^k} 1$ genau zwei Lösungen $\pm a$ besitzt. *Hinweis:* p kann nicht $a + 1$ und $a - 1$ teilen.

Aufgabe 51 (mündlich)

Sei a ein Gruppenelement der Ordnung $\operatorname{ord}(a) = k$. Zeigen Sie

$$\operatorname{ord}(a^i) = \frac{k}{\operatorname{ggT}(k, i)}.$$

Aufgabe 52 (mündlich)

a) Zeigen Sie, dass $\mathbb{F}_{p^n}$ zusammen mit der Addition auf $\mathbb{F}_{p^n}$ und der Einschränkung der Multiplikation auf Skalarprodukte der Form $aq(x)$ mit $a \in \mathbb{F}_p$ und $q(x) \in \mathbb{F}_{p^n}$ einen Vektorraum über $\mathbb{F}_p$ bildet.

b) Zeigen Sie, dass die Multiplikation mit einem festen Körperelement $a_{n-1} \cdots a_0 \in \mathbb{F}_{p^n}$, also die Abbildung $b_{n-1} \cdots b_0 \mapsto a_{n-1} \cdots a_0 \cdot b_{n-1} \cdots b_0$ eine lineare Abbildung in dem Vektorraum $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ ist.

c) Folgern Sie, dass lineare Abbildungen über $\mathbb{F}_{p^n}$ auch linear über $\mathbb{F}_p$ sind.

Aufgabe 53 (schriftlich, 10 Punkte)

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

a) Zeigen Sie, dass für jedes $a \in G$ ein $k > 0$ existiert mit $a^k = 1$.

b) Sei nun $\operatorname{ord}(a) = k$. Zeigen Sie, dass die Menge

$$[a] = \{a^i \mid i \geq 0\}$$

eine Untergruppe von G mit genau k Elementen bildet. Folgern Sie $k|m$ und $a^m = 1$.

c) Zeigen Sie, dass genau dann $a^i = a^j$ ist, wenn $i \equiv_{\operatorname{ord}(a)} j$ gilt.

d) Zeigen Sie, dass die Gruppen $[a]$ und $(\mathbb{Z}_k, +)$ isomorph sind. Geben Sie einen Isomorphismus an.