Einführung in die Kryptologie — Wintersemester 2013/14
Prof. Dr. J. Köbler — 17. Dezember 2013

Übungsblatt 10

Aufgabe 49 ***mündlich***

(a) Berechnen Sie die Rundenschlüssel $K^0, \dots, K^{10}$, die sich aus dem externen 128 Bit AES-Schlüssel $K = $ *2B7E151628AED2A6ABF7158809CF4F3C* ergeben.

(b) Verschlüsseln Sie den Klartext $x =$ `3243F6A8885A308D313198A2E0370734` mit K.

Aufgabe 50 ***mündlich***

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

```
AddRoundKey(K^10)
ShiftRows^-1
SubBytes^-1
for i ← 9 downto 1 do
    AddRoundKey(K^i)
    MixColumns^-1
    ShiftRows^-1
    SubBytes^-1
AddRoundKey(K^0)
```

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

Aufgabe 51 ***10 Punkte***

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

(a) Zeigen Sie, dass R kein Körper ist.

(b) Ist das Ringelement $a(y) = 03y^3 + 01y^2 + 01y + 02$ in R invertierbar?

(c) Zeigen Sie, dass die AES-Operation MixColumns eine multiplikative Chiffre mit festem Schlüssel $a(y)$ im Ring R realisiert.

Aufgabe 52 ***mündlich***

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

(a) Zeigen Sie, dass ab die Ordnung $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$ hat, falls $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd sind.

(b) Lässt sich die Aussage in Teilaufgabe (a) zu $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$ verallgemeinern?

Aufgabe 53 ***mündlich***

(a) 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.

(b) Zeigen Sie, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

(c) Finden Sie Polynome $q_d(x) \in \mathbb{Z}_6[x]$ vom Grad $d = 1, 2$ mit möglichst vielen Nullstellen.

Aufgabe 54 Sei p eine ungerade Primzahl und $\mathrm{ggT}(a, p) = 1$. ***mündlich***

(a) Sei $i \geq 2$ und $b^2 \equiv_{p^{i-1}} a$. Zeigen Sie, dass es genau ein $x \in \mathbb{Z}_{p^i}$ gibt mit $x^2 \equiv_{p^i} a$ und $x \equiv_{p^{i-1}} b$. Wie kann x effizient berechnet werden?

(b) Berechnen Sie mit Ihrem Verfahren ausgehend von $6^2 \equiv_{19} 17$ die Wurzeln von 17 modulo 19^2 und modulo 19^3.

(c) Zeigen Sie für jedes $i \geq 1$, dass die Kongruenz $x^2 \equiv_{p^i} a$ entweder 0 oder 2 Lösungen hat.

Aufgabe 55 ***mündlich***

Zeigen Sie, dass für jede Primzahlpotenz p^k ($p > 2$, $k \geq 1$) die Kongruenz $x^2 \equiv_{p^k} 1$ genau zwei Lösungen $\pm a$ besitzt.

Hinweis: p kann nicht sowohl $a+1$ als auch $a-1$ teilen.

Aufgabe 56 Sei $a \in G$ ein Gruppenelement der Ordnung k. ***mündlich***

Zeigen Sie, dass $\mathrm{ord}(a^i) = k/\mathrm{ggT}(k, i)$ ist.

Aufgabe 57 ***mündlich***

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 $\mathrm{ord}(a) = k$. 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 $i \equiv_{\mathrm{ord}(a)} j$ gilt.

(d) Geben Sie einen Isomorphismus zwischen den beiden Gruppen $[a]$ und $(\mathbb{Z}_k, +)$ an.