Dr. Dirk Frettlöh 1.7.2020

# Übungen zur Vorlesung Kryptographie

## Blatt 13

**Aufgabe 49:** Berechnen Sie MixColumns für die erste Spalte der Matrix

$$\begin{pmatrix} 02 & AC & 55 & CE \\ 72 & D3 & 28 & DF \\ 13 & C2 & 01 & 28 \\ E4 & 79 & 9B & 1E \end{pmatrix}$$

**Aufgabe 50: (SubBytes$^{-1}$)**
Seien $p_1 = x^4 + x^3 + x^2 + x + 1$ und $p_0 = x^6 + x^5 + x + 1$ wie in SubBytes.

**(a)** Zeigen Sie, dass $\mathrm{ggT}(p_1, x^8 + 1) = 1$ in $\mathbb{F}_2[x]$.

**(b)** Berechnen Sie das Inverse von $p_1$ in $R = \mathbb{F}_2[x]/(x^8 + 1)$.

**(c)** Zeigen Sie, dass für alle $p \in R$ gilt: $p_1 \cdot p + p_0 = p_1 \cdot (p + x^2 + 1)$ in $\mathbb{F}_2[x]/(x^8 + 1)$.

**(d)** Es seien

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{und} \quad Q = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Zeigen Sie, dass $Q$ die inverse Matrix zu $P$ über $\mathbb{F}_2$ ist. Was ist der Zusammenhang mit Ihrem Ergebnis aus (b)?

**(e)** Zeigen Sie, dass für alle $p \in F = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ mit $p \neq 0$ gilt:
$p^{-1} \equiv p^{254} \bmod x^8 + x^4 + x^3 + x + 1$. *(Tipp: $F$ ist ein Körper.)*

*Es folgen zwei Aufgaben zu Anwendungen, im Vorgriff auf Kapitel 9. Die sind leichter und vielleicht interessanter als weitere Aufgaben zu AES.*

**Aufgabe 51: (Secret Sharing)**
Für manche Zwecke möchte man, dass $n$ Personen $A_1, A_2, \ldots, A_n$ nur gemeinsam ein Dokument lesen/ein Tresorfach öffnen/... können. Kryptographisch kann man das so erreichen: Sei

$$p : \mathbb{R} \to \mathbb{R},\ p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

Die geheime Zahlenkombination für den Tresor sei $a_0$. Die Person $A_i$ kennt den Wert $p(i)$ von $p$ an der Stelle $i$.

**(a)** Wie ermitteln alle $n$ Personen den Wert $a_0$?

**(b)** Wieso können weniger als $n$ Personen nicht den Wert $a_0$ ermitteln?

**(c)** Angenommen es sei $n = 4$. $A_1$ kennt $p(1) = 76$, $A_2$ kennt $p(2) = 49$, $A_3$ kennt $p(3) = 0$ und $A_4$ kennt $p(4) = -113$. Was ist der Wert von $a_0$?

**Aufgabe 52: (Gehaltsvergleich)**
In vielen Unternehmen weiß fast niemand in den gehobenen Positionen, was die Kollegen verdienen, und niemand möchte sein Gehalt verraten. Alice, Bob und Carol möchten wissen, ob sie "genug" verdienen in dem Sinne, ob sie jeweils mehr oder weniger als das Durchschnittsgehalt der drei verdienen. Dazu nutzen sie folgendes Verfahren:

1. Alice wählt eine geheime Zufallszahl $r$, addiert ihr Gehalt $a$ und gibt $a + r$ an Bob weiter.
2. Bob addiert sein Gehalt $b$ und gibt $a + b + r$ an Carol weiter.
3. Carol addiert ihr Gehalt $c$ und gibt $a + b + c + r$ an Alice weiter.
4. Alice subtrahiert $r$ und gibt $\frac{1}{3}(a + b + c)$ bekannt.

**(a)** Begründen Sie, warum das Verfahren sicher ist, d.h.: Warum kann Alice nicht $b$ oder $c$ ermitteln, warum Bob nicht $a$ oder $c$, und warum Carol nicht $a$ oder $b$?

**(b)** Analog zum oben geschilderten anonymen Berechnen des Durchschnittsgehalts von drei Leuten, finden Sie eine Methode zum anonymen Berechnen des Durchschnittsgehalts von $n$ Leuten ($n \geq 3$).

**(c)** Wie viele Leute müssen sich oben bzw bei Ihrer Methode mindestens verabreden, um alle Gehälter ermitteln zu können? (Sie teilen untereinander alle Informationen, die sie haben; sie verraten damit natürlich auch Ihre eigenen Gehälter, zumindest untereinander.) Angenommen, alle Beteiligten sitzen an einem runden Tisch, wie genau muss diese Minimalzahl von verabredeten Leuten sitzen, um alle Gehälter zu erfahren?

---

Abgabe bis Mittwoch 8.7.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de