

Übungen zur Vorlesung Kryptographie

Blatt 11

Aufgabe 41: (Polynome über $\mathbb{F}_2$ — Level 4 bis 5)

Wir betrachten wieder Polynome in $\mathbb{F}_2[x]$, also Polynome von der Form $a_n x^n + \dots + a_1 x + a_0$ mit $a_i \in \mathbb{F}_2$ für $0 \leq i \leq n$.

- (a) Finden Sie Polynome p', q' , so dass $p' \cdot (x^4 + 1) + q' \cdot (x^4 + x^3 + x + 1) = x^2 + 1$ in $\mathbb{F}_2[x]$.
 (b) Finden Sie das Inverse p^{-1} zu $q = (x^3 + x^2 + x + 1)$ in $\mathbb{F}_2[x] \setminus (x^4 + x + 1)$.

(Tipp: Benutzen Sie bei (c) und (d) den euklidischen Algorithmus, angepasst an Polynome über $\mathbb{F}_2$, vgl. Beispiel 8.1 im Skript S. 44.)

Aufgabe 46: (Aufwärmübung Lineare Algebra über $\mathbb{F}_2$)

Gegeben sind die Matrizen $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in (\mathbb{F}_2)^{2 \times 2}$ und $B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{3 \times 3}$. Wir rechnen alles in $\mathbb{F}_2$ (also modulo 2).

- (a) Berechnen Sie die inverse Matrix zu A .
 (b) Finden Sie eine Matrix $X \in (\mathbb{F}_2)^{2 \times 2}$, so dass $A \cdot X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
 (c) Berechnen Sie die inverse Matrix zu B .

(Wie man über $\mathbb{R}$ eine inverse Matrix berechnet steht z.B. hier:

<https://www.math.uni-bielefeld.de/~frettlöe/teach/alte-vorles/ueb/auff-skript-1-20.pdf>

auf Seite 47. Das geht in $\mathbb{F}_2$ genauso, nur das Rechnen wird einfacher.)

Aufgabe 47: (AES: addieren und schieben)

In den folgenden Aufgaben berechnen Sie jeden der vier Schritte des AES-Verfahrens. Gegeben sind die Eingabe

$$m = 00112233445566778899AABBCCDDEEFF$$

(in Hexadezimalschreibweise) und der Schlüssel (auch in Hexadezimalschreibweise)

$$k = ABABABABBCBCBCBCCDCDCDCDDDEDEDEDE.$$

- (a) Schreiben Sie m und k nach der bei AES benutzten Methode als Matrizen M bzw K .
 (b) Berechnen Sie ADDROUNDKEY für die vier Einträge in der ersten Spalte von M .
 (c) Berechnen Sie SHIFTRROWS von M .

Aufgabe 48: (AES: sub-byten)

Berechnen Sie SUBBYTES für den ersten Eintrag links oben in der Matrix $M = \begin{pmatrix} 15 & 31 & 27 & 4E \\ D2 & 42 & 57 & 38 \\ 03 & 1A & 20 & CF \\ 74 & 15 & 24 & D4 \end{pmatrix}$.

Abgabe bis Mittwoch 1.7.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
 Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de