

Übungen zur Vorlesung Kryptographie**Blatt 12**

Führen Sie alle Berechnungen von Hand durch! (Sie können gerne mit dem Computer kontrollieren.)

Aufgabe 45: (Aufwärmübung Polynome über $\mathbb{F}_2$)

Wir betrachten 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) Berechnen Sie $(x^8 + x^7 + x^5 + x^4 + x^2 + 1) + (x^8 + x^6 + x^4 + x^3 + x^2 + x + 1)$ und $(x^4 + x^2 + 1) \cdot (x^3 + x + 1)$ in $\mathbb{F}_2[x]$.

(b) Sei $p = x^5 + x^4 + x^3 + x^2 + 1$. Berechnen Sie $p \bmod x^4 + 1$, $p \bmod x^4 + x$, und $p \bmod x^4 + x^2$ in $\mathbb{F}_2[x]$.

(c) Berechnen Sie den ggT von $x^3 + 1$ und $x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]$.

(d) Finden Sie Polynome p', q' , so dass $p' \cdot (x^3 + 1) + q' \cdot (x^4 + x^2 + x + 1) = x + 1$ in $\mathbb{F}_2[x]$.

(Tipp: Benutzen Sie bei (c) und (d) den euklidischen Algorithmus, angepasst an Polynome über $\mathbb{F}_2$, vgl. Beispiel 8.1 im Skript S. 45.)

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

Gegeben sind die Matrizen $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in (\mathbb{F}_2)^{2 \times 2}$ und $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in (\mathbb{F}_2)^{3 \times 3}$. 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 drei der vier Schritte des AES-Verfahrens. Gegeben sind die Eingabe

$$m = 00112233445566778899AABBCCDDEEFF$$

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

$$k = AABBCCDDAABBCCDDAABBCCDDAABBCCDD.$$

(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 SHIFTRows von M .

Aufgabe 48: (AES: sub-byten)

Berechnen Sie SUBBYTES für den ersten Eintrag links oben in der Matrix $M = \begin{pmatrix} 17 & 3A & 27 & 4E \\ D2 & 4B & 57 & 28 \\ 03 & 1A & 40 & CF \\ 74 & 16 & 24 & D4 \end{pmatrix}$.

Abgabe bis Mittwoch 7.7.2021 bis 14 Uhr per Email an den Tutor.

Jan-Philipp Brünger
Leonard Simon Ellinghaus
Kallias Stoupas

jbruenger@techfak.de
tellinghaus+krypto@techfak.de
kstoupas+krypto@techfak.de