Übungen zur Vorlesung Kryptographie

Blatt 12

Aufgabe 45: (AES: columns mixen)

Berechnen Sie MixColumns für die erste Spalte von $M = \begin{pmatrix} 62 & A3 & 76 & E2 \\ D3 & 7A & 81 & A4 \\ DF & B6 & 23 & 6E \\ 1E & 49 & 24 & D8 \end{pmatrix}$.

Aufgabe 46: (SubBytes^{-1})

Seien $p_0 = x^6 + x^5 + x + 1$ und $p_1 = x^4 + x^3 + x^2 + x + 1$ wie in SubBytes.

(a) Überprüfen Sie, dass $\mathrm{ggT}(p_1, x^8 + 1) = 1$ in $\mathbb{F}_2[x]$.
(b) Berechnen Sie p_1^{-1} in $\mathbb{F}_2[x]/(x^8 + 1)$.
(c) Zeigen Sie, dass $p_1 \cdot a + p_0 = p_1 \cdot (a + (00000101))$ für alle 8-bit Worte a.
(d) Die Ausgabe von Subbytes ist $q = x^7 + x^6 + x^4 + x^3$. Berechnen Sie ohne Verwendung von p_0 das ursprüngliche Polynom p.

Aufgabe 47: (MixColumns^{-1})

Es gilt $(0By^3 + 0Dy^2 + 09y + 0E) \cdot (03y^3 + 01y^2 + 01y + 02) = 1$ in $F[y]/(y^4 + 1)$, wobei wieder $F = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$.

(a) Wie kann man das Nutzen zum Entschlüsseln der MixedColumns-Operation?

(b) Die MixedColumns-Operation liefert die Spalte

$$\begin{pmatrix} 35 \\ 00 \\ 01 \\ 4F \end{pmatrix}$$

Berechnen Sie die ursrpüngliche Spalte, bevor sie mit MixedColumns verschlüsselt wurde.

Aufgabe 48: (AES-Fixpunkte)

Für jede der vier Operationen AddRoundKey, ShiftRows, SubBytes und MixColumns: Bestimmen Sie, wieviele Eingaben m es jeweils gibt, so dass die Ausgabe auch m ist. Begründen Sie Ihre Antworten. Geben Sie jeweils auch an, wieviel Prozent das sind im Vergleich mit allen möglichen Eingaben (auf drei Nachkommastellen gerundet).

(Bei AddRoundKey dürfen Sie annehmen, dass der Rundenschlüssel nicht ausschließlich Nullen enthält. Bei SubBytes dürfen Sie sich erinnern, dass das per table-lookup gemacht werden kann, und die Antwort im Internet recherchieren.)

Abgabe bis Mittwoch 8.7.2026 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