Dr. Dirk Frettlöh 25.6.2025

Übungen zur Vorlesung Kryptographie

Blatt 12

Aufgabe 45: (AES: bytes subsen)

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

Aufgabe 46: (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 47: (MixColumns^{-1})

(a) Zeigen Sie, dass

$$(0By^3 + 0Dy^2 + 09y + 0E) \cdot (03y^3 + 01y^2 + 01y + 02) = 1 \text{ in } F[y]/(y^4 + 1)$$

(Obacht: hier steht $F[y]$, wobei $F = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$, vgl. Skript)

(b) Wie kann man das nutzen beim Entschlüsseln einer mit AES verschlüsselten Nachricht?

Aufgabe 49: (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 2.7.2025 bis 14 Uhr per Email an die Tutorin.

Lisa Harms lharms+krypto@techfak.de
Lisa Henetmayr lhenetmayr+krypto@techfak.de