Dr. Dirk Frettlöh 21.6.2023

Übungen zur Vorlesung Kryptographie

Blatt 12

Aufgabe 45: (AES: addieren und schieben)
In den folgenden Aufgaben berechnen Sie alle vier Schritte des AES-Verfahrens. Gegeben sind die Eingabe

$$m = 00112233445566778899AABBCCDDEEFF$$

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

$$k = ABABABABBCBCBCBCCDCDCDCDDEDEDEDE.$$

(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 46: (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 47: (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 48: (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?

Abgabe bis Dienstag 28.6.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de