Übungsblatt 10

Abgabe der schriftlichen Lösungen bis 07.07.2022, 24 Uhr

Aufgabe 50 ***10 Punkte***

(a) Zeigen Sie, dass die Operationen $\mathsf{AddRoundKey}(K^r)$, $\mathsf{SubBytes}$, $\mathsf{ShiftRows}$ und $\mathsf{MixColumns}$ invertierbar sind, und geben Sie explizite Beschreibungen für die inversen Operationen an.

(b) Geben Sie den Pseudocode für die Dechiffrierfunktion $\mathsf{AES}^{-1}(K,x)$ unter Verwendung der Rundenschlüssel $K^0,\ldots,K^{10}$ an.

(c) Zeigen Sie, dass die AES-Dechiffrierung auch dadurch möglich ist, dass man im Chiffrieralgorithmus $\mathsf{AES}(K,x)$ die Operationen $\mathsf{AddRoundKey}(K^r)$, $\mathsf{SubBytes}$, $\mathsf{ShiftRows}$ und $\mathsf{MixColumns}$ durch die entsprechenden inversen Operationen ersetzt (ohne deren Reihenfolge zu ändern), sofern der Key-Schedule Algorithmus entsprechend angepasst wird (dies ist für Hardware-Implementierungen vorteilhaft).

Aufgabe 51 ***mündlich***

(a) Berechnen Sie die Rundenschlüssel $K^0,\ldots,K^{10}$, die sich aus dem externen 128 Bit AES-Schlüssel $K = \texttt{2B7E151628AED2A6ABF7158809CF4F3C}$ ergeben.

(b) Berechnen Sie $AES(K,x)$ für $x = \texttt{3243F6A8885A308D313198A2E0370734}$.

Aufgabe 52 ***mündlich***

Eine $(k \times l)$-Matrix M heißt *zirkulant*, wenn jede Zeile von M relativ zur Zeile darüber um eine Position zirkulär nach rechts verschoben ist. Entsprechend heißt eine lineare Abbildung $f \in Lin((\mathbb{F}_q)^k,(\mathbb{F}_q)^l)$ *zirkulant*, falls sie durch eine zirkulante Matrix $Z \in \mathbb{F}_q^{(k\times l)}$ darstellbar ist (d.h. $f(c_{k-1},\ldots,c_0) = (c_{k-1},\ldots,c_0)Z$).
Zeigen Sie für einen beliebigen Faktorring R der Form $\mathbb{F}_q[y]/(y^k-1)$, q prim:

(a) R ist für kein $k \geq 2$ ein Körper.

(b) Für jede zirkulante Abbildung $f \in Lin((\mathbb{F}_q)^k,(\mathbb{F}_q)^k)$ existiert in R ein Polynom $z(y)$ mit $f(c_{k-1},\ldots,c_0) = (c'_{k-1},\ldots,c'_0)$, wobei $(c'_{k-1},\ldots,c'_0)$ der Koeffizientenvektor des Polynoms $c'(y) = z(y)c(y)$ für $c(y) = c_{k-1}y^{k-1}+\cdots+c_0$ ist.

(c) Die AES S-Box $\mathsf{MixColumns}$ realisiert im Ring $R = \mathbb{F}_{2^8}[y]/(y^4+1)$ eine multiplikative Chiffrierfunktion mit dem Schlüssel $z(y) = 03y^3+01y^2+01y+02$.

Aufgabe 53 ***mündlich***

(a) Alice verschlüsselt mit einer ℓ-Bit Blockchiffre eine Reihe von Klartextblöcken $x_1,x_2,\ldots,x_n$ zu Kryptotextblöcken $y_1,y_2,\ldots,y_n$ und sendet sie an Bob, der sie wieder entschlüsselt. Wie viele Klartextblöcke werden durch einen Übertragungsfehler bei Block y_i maximal verfälscht, wenn Alice den ECB-, CBC-, OFB-, CFB- bzw. CTR-Modus benutzt? (*Hinweis:* Beachten Sie, dass die Länge t der Blöcke x_i bei den letzten drei Modi auch kleiner als ℓ sein kann.)

(b) Wie wirkt sich der Verlust eines Blockes y_i bei der Übertragung auf den von Bob berechneten Klartext aus?

Aufgabe 54 Sei p prim. ***mündlich, optional***

(a) Zeigen Sie, dass zu jedem Polynom $q(x)$ vom Grad $d \geq 1$ in $\mathbb{Z}_p[x]$ ein endlicher Körper K existiert, der $\mathbb{Z}_p$ als Unterkörper enthält und in dem $q(x)$ in Linearfaktoren zerfällt (der kleinste solche Körper $K_p(q(x))$ ist bis auf Isomorphie eindeutig bestimmt und heißt der *Zerfällungskörper* für $q(x)$ über $\mathbb{Z}_p$).

(b) Zeigen Sie, dass der Zerfällungskörper $K = K_p(x^{p^n}-x)$ genau p^n Elemente enthält. Schließen Sie hieraus auf die Existenz eines irreduziblen Polynoms $m(x)$ vom Grad n über $\mathbb{Z}_p$, indem Sie zu einem beliebigen Erzeuger g der Einheitengruppe K^* von K ein Polynom $m(x) \neq 0$ kleinsten Grades mit $m(g) = 0$ bestimmen.

Hinweis: Benutzen Sie, dass die multiplikative Einheitengruppe K^* eines endlichen Körpers K *zyklisch* ist, d.h. es existiert ein Element $g \in K^*$ mit $K^* = \{g,g^2,\ldots,g^{q-1}\}$, wobei $q = |K|$ ist (g heißt *Erzeuger* von K^*).