



4. Übungsblatt

Verwenden Sie zur Lösung der Aufgabe zusätzlich noch folgendes Dokument:
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

ÜBUNGEN

G1 (Konstruktion mit endlichen Körpern).

Konstruieren Sie einen endlichen Körper mit 9 Elementen. Geben Sie die entsprechende Multiplikationstabelle an. Die Wahl eines passenden Polynoms bleibt Ihnen überlassen.

Tipp: Polynome vom Grad ≤ 3 sind genau dann irreduzibel, wenn sie keine Nullstellen haben.

G2 (Invertieren in endlichen Körpern).

Sei p eine Primzahl, g ein irreduzibles normiertes Polynom in $\mathbb{F}_p[X]$. Dann ist $\mathbb{F} = \mathbb{F}_p[X]/g(X)\mathbb{F}_p[X]$ ein endlicher Körper. Die Elemente in \mathbb{F} sind von der Form $\alpha = h(x) + g(x)\mathbb{F}_p[X]$ wobei $h(x) \in \mathbb{F}_p[X]$ vom Grad $\leq \text{grad}(g)$ ist. Um α zu invertieren, berechnet man $h'(x) \in \mathbb{F}[X]$ mit $h(x)h'(x) \equiv 1 \pmod{g(x)}$. Dann ist $\alpha^{-1} = h'(x) + g(x)\mathbb{F}_p[X]$.

Invertieren Sie $X^2 + X + 1$ und $X^7 + X^6 + X^3 + X^2 + X + 1$ in $\mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)\mathbb{F}_2[X]$.
 Funktioniert diese Konstruktion auch für nicht normierte g ?

G3 (Substitutions Box in AES).

Ein kleiner Bestandteil von AES ist die sogenannte S-Box.

(a) Identifikation.

Generell sind viele Parameter bei AES fest. Zum Beispiel operiert man immer auf Bytes, also Bit-Strings der Länge 8. Ein Byte wird dafür mit den Elementen des aus Aufgabe 2 bekannten AES-Körpers $\mathbb{F} = \mathbb{Z}_2[X]/P(X)\mathbb{Z}_2[X]$ identifiziert. Um beim aufschreiben Platz zu sparen identifiziert man die Bytes auch oft mit den Hexadezimalzahlen der Länge 2.

Beispiel. Das Polynom $P(X) = X^6 + X^4 + X^3 + 1$ entspricht also sowohl dem Bit-String $P = 01011001_2$ oder dem Hex-String $P = 59_{16}$. Umgedreht ist mit $Q = AB_{16}$ der Bit-String $Q = 10101011_2$ und somit das Polynom $Q(X) = X^7 + X^5 + X^3 + X + 1$ gemeint.

Ergänze die fehlenden Darstellungen für: 00001011_2 , FF_{16} , X .

(b) Funktion.

Seien

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad \text{wobei} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \cong 10010011_2.$$

Dann entspricht die S-Box der Funktion

$$S: \mathbb{F} \longrightarrow \mathbb{F} : b \mapsto A \cdot b^{-1} + c.$$

Anmerkung. Man beachte das b hier invertiert wird. Damit ist eine Invertierung des Polynoms, was b repräsentiert im Körper \mathbb{F} gemeint. Ist $b = 0$, also nicht invertierbar, dann läßt man die Invertierung weg. $S(0) = c$. Der Rest der Operationen die in S passieren sind linear. Invertieren ist allerdings nicht linear! Das Anwenden der S-Box in AES garantiert, die Nicht-Linearität.

Berechne $S(X^2 + X + 1)$ und $S(X^7 + X^6 + X^3 + X^2 + X + 1)$. Gib das Ergebnis und die Eingabe auch in Binär- und Hex-Form an.

G4 (AES Modifikationen).

Wie wirken sich folgende Modifikationen auf (die Sicherheit von) AES aus?

- a) Angenommen Sie lassen in AES die Operation *MixColumns* weg. Wie unterscheiden sich die Chifretexte, die bei Verschlüsselung zweier Klartext (mit gleichem Schlüssel) entstehen, die sich nur in einem Bit unterscheiden?
- b) Angenommen Sie lassen *ShiftRows* bei AES weg (*MixColumns* wird ausgeführt). Wie wirkt sich der Unterschied von einem Bit im Klartext jetzt aus?
- c) Es wird nur eine einzige Runde AES (*AddRoundKey*, *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*) ausgeführt. Wie wirkt sich der Unterschied in einem Bit in den Klartexten bei dieser Version aus?