Wolfgang K. Seiler
Tel. 2515

B6, B4.08

15. Mai 2025

11. Übungsblatt Kryptologie

Aufgabe 1:

a) Schreiben Sie die Dezimalzahlen $10, 100, 1000$ und $10\,000$ im Hexadezimalsystem!

b) Wie sehen die Hexadezimalzahlen 10_{hex}, 100_{hex}, 1000_{hex} und $10\,000_{\text{hex}}$ im Dezimalsystem aus?

c) Welchen Polynomen aus $\mathbb{F}_2[X]$ und welchen Dezimalzahlen entsprechen die Hexadezimalzahlen AA_{hex} und FF_{hex} ?

Aufgabe 2:

Berechnen Sie im AES-Körper $\mathbb{F}_{256}$ die Elemente $A5_{\text{hex}} + B6_{\text{hex}}$ und $1A_{\text{hex}} \cdot 2B_{\text{hex}}$!

Aufgabe 3:

Bestimmen Sie das Bild des Bytes $B6_{\text{hex}}$ unter der Bytesubstitution von AES!

Aufgabe 4:

Zeigen Sie, daß AES sicher ist gegen differentielle Kryptanalyse, indem Sie für jede Differenz $d \in \mathbb{F}_{256}$ bestimmen, für wie viele Paare $(x, y) \in \mathbb{F}_{256}^2$ mit Differenz $x \oplus y = d$ die Ergebnisse der Bytesubstitutionen von x und y eine vorgegebene Differenz haben!

Abgabe und Besprechung am Mittwoch, dem 21. Mai 2025, um 15.30 Uhr