Wolfgang K. Seiler
Tel. 2515

B6, B4.18

15. November 2019

10. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*
Berechnen Sie im AES-Körper $\mathbb{F}_{256}$ die Elemente $A5_{hex} + B6_{hex}$ und $1A_{hex} \cdot 2B_{hex}$!

Aufgabe 2: *(10 Punkte)*
Bestimmen Sie das Bild des Bytes $B6_{hex}$ unter der Bytesubstitution von AES!

Aufgabe 3: *(5 Punkte)*
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 bis zum Freitag, dem 22. November 2019, um 11.55 Uhr