Wolfgang K. Seiler
Tel. 2515

B6, B4.08

19. November 2022

11. Übungsblatt Kryptologie

Aufgabe 1:

a) Zeigen Sie: Ein Polynom vom Grad zwei oder drei über einem Körper k ist genau dann irreduzibel, wenn es keine Nullstelle in k hat.

b) Bestimmen Sie alle irreduziblen Polynome vom Grad zwei und drei mit Koeffizienten in $\mathbb{F}_2$!

c) Zeigen Sie, daß in einem Körper k mit acht Elementen jedes von Null verschiedene Element die multiplikative Gruppe erzeugt!

d) Gilt dies auch in einem Körper mit sechzehn Elementen?

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!

Besprechung am Mittwoch, dem 23. November 2022, um 15.30 Uhr