Kryptographie Blatt 8

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 11.12.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Irreduzible Polynome über endlichen Körpern

(a) Bestimmen Sie alle irreduziblen Polynome vom Grad 2, 3 und 4 über $\mathbb{F}_2$ und $\mathbb{F}_3$.

(b) Bestimmen Sie alle irreduziblen Polynome vom Grad d über $\mathbb{F}_2$, welche davon haben höchstens drei Koeffizienten $\neq 0$?

Aufgabe 2: Polynomberechnungen über endlichen Körpern, speziell dem AES-Körper

(a) Berechnen Sie den größten gemeinsamen Teiler der beiden Polynome $X^4 + X^2 + 1$ und $X^2 + X + 1$ im Polynomring $\mathbb{F}_2[X]$ und $\mathbb{F}_4[X]$.

(b) Berechnen Sie das multiplikative Inverse des Elements `0C` im AES-Körper $\mathbb{F}_{2^8}$ (vgl. Aufgabe 3 von Blatt 7).

(c) Warum ist im Ring $R = \mathbb{F}_{2^8}[X]/(X^4 + 1)$ das Element $X + 1 \in R$ nicht invertierbar?

(d) Warum ist das Element $c = \texttt{03}X^3 + X^2 + X + \texttt{02}$ im Ring $R = \mathbb{F}_{2^8}[X]/(X^4 + 1)$ invertierbar?

Aufgabe 3: Elliptische Kurve über endlichen Körpern

Sei p eine Primzahl. Gegeben sei die über dem endlichen Körper $\mathbb{F}_p$ durch folgende Gleichung definierte Teilmenge des $\mathbb{F}_p^2$:

$$E : y^2 = x^3 + x + 9.$$

Berechnen Sie für die $p \in \{2, 3, 5, 7, 19\}$ alle Punkte $(x, y) \in \mathbb{F}_p^2$, die in der Teilmenge liegen.