G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Wiederholung Endliche Körper

Aufgabe 1 *Komponentenfunktionen*
Sei

$$f : \mathrm{GF}(2^2) \to \mathrm{GF}(2^2)$$

mit

$$f(x) = \begin{cases} x^{-1} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

gegeben.

1. Berechnen Sie zwei Komponentenfunktionen f_1 und f_2 mittels derer f als Abbildung von $\mathrm{GF}(2)^2$ nach $\mathrm{GF}(2)^2$ beschrieben werden kann. Nutzen Sie hierfür das irreduzible Polynom
$$p(\alpha) = \alpha^2 + \alpha + 1$$
2. Bestimmen Sie die Menge
$$Bild(f) := \{f(x) \mid x \in \mathrm{GF}(2^3)\}$$

Aufgabe 2 *Isomorphe Körper*
Seien $f(X) = X^3 + X + 1$ und $g(X) = X^3 + X^2 + 1$. Zeigen Sie das die beiden Körper

$$F = \mathbb{F}_2[X]/(f) \text{ und } L = \mathbb{F}_2[X]/(g)$$

isomorph sind.

Aufgabe 3 *Teilkörper*
Welche Teilkörper K sind in $\mathbb{F}_{2^{12}}$ enthalten?

Aufgabe 4 *Irreduzible Polynome*
Bestimmen Sie alle irreduziblen Polynome vom Grad kleiner gleich 3 über

1. GF(2) und
2. GF(3).

Aufgabe 5 *Rechnen in endlichen Körpern I*
Berechnen Sie für den Körper $\mathrm{GF}(2^3)$ eine Additions- und Multiplikations-Tabellen. Nutzen Sie für die Darstellung des Körpers eines der irreduziblen Polynome aus Aufgabe 1.

Aufgabe 6 *Erweiterter Euklidischer Algorithmus*
Berechnen Sie für die Polynome $a, b \in \mathrm{GF}(2)[x]$ mit

$$a = x^4 + x^3 + 1 \text{ und } b = x^3 + x^2 + 1,$$

Polynome $x, y \in \mathrm{GF}(2)[x]$ so dass

$$ax + by = \gcd(a, b)$$