Kryptography Sheet 8

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 11.12.2023, before the lecture starts

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

Exercise 1: Irreducible polynomials over finite fields

(a) Determine all irreducible polynomials of degree 2, 3 and 4 over $\mathbb{F}_2$ und $\mathbb{F}_3$.

(b) Determine all irreducible polynomials of degree d over $\mathbb{F}_2$, which ones have at most three coefficients that are $\neq 0$?

Exercise 2: Calculations with polynomials over finite fields, especially the AES-field

(a) Calculate the greatest common divisor of the two polynomials X^4+X^2+1 and X^2+X+1 in the polynomial ring $\mathbb{F}_2[X]$ and $\mathbb{F}_4[X]$.

(b) Calculate the multiplicative inverse of the element `0C` in the AES-field $\mathbb{F}_{2^8}$ (cp. Exercise 3 of Sheet 7).

(c) Why is the element $X+1 \in R$ in the ring $R = \mathbb{F}_{2^8}[X]/(X^4+1)$ not invertible?

(d) Why is the element $c = \texttt{03}X^3 + X^2 + X + \texttt{02}$ in the ring $R = \mathbb{F}_{2^8}[X]/(X^4+1)$ invertible?

Exercise 3: Elliptic curve over finite fields

Let p be prime. Consider the subset of $\mathbb{F}_p^2$ which is given by the following equation over the finite field $\mathbb{F}_p$,

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

Calculate for $p \in \{2, 3, 5, 7, 19\}$ all points $(x, y) \in \mathbb{F}_p^2$ that lie in this subset.