Wolfgang K. Seiler
Tel. 2515

B6, B4.18

8. November 2019

9. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

a) Stellen Sie eine Tabelle der diskreten Logarithmen modulo 19 zur Basis zwei der Zahlen von 0 bis 18 zusammen!

b) Berechnen Sie mit Hilfe dieser Logarithmentafel die Zahlen

$$a = 13 \cdot 17 \bmod 19, \quad b = 13! \bmod 19 \quad \text{und} \quad c = 13^{100} \bmod 19\,!$$

Aufgabe 2: *(5 Punkte)*

Berechnen Sie über dem Körper $\mathbb{F}_2 = \{0, 1\}$ mit zwei Elementen der ggT der Polynome

$$f = X^8 + X^5 + X^2 + 1 \quad \text{und} \quad g = X^5 + X^3 + 1\,,$$

und stellen Sie ihn als Linearkombination dieser beiden Polynome dar!

Aufgabe 3: *(7 Punkte)*

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

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

c) Zeigen Sie, daß jedes dieser Polynome ein Teiler von $X^7 - 1$ ist!

d) Zeigen Sie: Sind $f, g \in \mathbb{F}_2[X]$ zwei irreduzible Polynome vom Grad drei, so sind die Körper $\mathbb{F}_2[X]/(f)$ und $\mathbb{F}_2[X]/(g)$ isomorph.

Aufgabe 4: *(3 Punkte)*

Zeigen Sie ohne Benutzung des Satzes, daß die multiplikative Gruppe eines endlichen Körpers stets zyklisch ist, daß in einem Körper k mit acht Elementen folgendes gilt: Ist $x \in k$ ungleich Null, so ist $k = \{0, x, x^2, x^3, x^4, x^5, x^6, x^7\}$!

Abgabe bis zum Freitag, dem 15. November 2019, um 11.55 Uhr