Wolfgang K. Seiler
Tel. 2515
A5, C201

1. Dezember 2004

6. Übungsblatt Kryptologie

Aufgabe 1: (*7 Punkte*)

a) Zeigen Sie, daß $R = \{x + iy \mid x, y \in \mathbb{Z}\}$ mit

$$\nu\colon \begin{cases} R \to \mathbb{N}_0 \\ x + iy \mapsto x^2 + y^2 \end{cases}$$

ein Euklidischer Ring ist!

b) Zeigen Sie: Ein Element $z \in R$ hat genau dann ein multiplikatives Inverses in R, wenn $\nu(z) = 1$ ist.

c) Bestimmen Sie alle Elemente mit dieser Eigenschaft!

d) Berechnen Sie den ggT von $1+7i$ und $1-7i$ in R und stellen Sie ihn als Linearkombination der Ausgangszahlen dar!

Aufgabe 2: (*6 Punkte*)

a) Zeigen Sie: Ein Element $x \in \mathbb{F}_{256}$ hat genau dann die Eigenschaft, daß sich jedes Element aus $\mathbb{F}_{256} \setminus \{0\}$ als x-Potenz schreiben läßt, wenn die drei Elemente x^{15}, x^{51} und x^{85} von eins verschieden sind.

b) Zeigen Sie, daß X modulo $X^8 + X^4 + X^3 + X + 1$ ein solches Element ist!

Aufgabe 3: (*7 Punkte*)

Die S-Box von Rijndael wird realisiert durch die Funktion

$$\begin{cases} \mathbb{F}_{256} \to \mathbb{F}_{256} \\ \quad x \mapsto \begin{cases} x^{-1} & \text{für } x \neq 0 \\ 0 & \text{für } x = 0 \end{cases} \end{cases}.$$

Betrachten Sie die Menge aller Paare $(x, y) \in \mathbb{F}_{256} \times \mathbb{F}_{256}$ mit einer festen Differenz $x \oplus y = \Delta_1 \neq 0$, und bestimmen Sie, wie viele solche Paare nach Durchgang durch die S-Box eine vorgegebene Differenz Δ_2 haben!

Abgabe bis zum Dienstag, dem 6. Dezember 2004, um 12.00 Uhr