Wolfgang K. Seiler
Tel. 2515

A5, C201

14. November 2007

10. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)

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

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

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: (*5 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: (*5 Punkte*)

a) Berechnen Sie das Ergebnis der Byte-Substitution, angewandt auf das Byte FF!

b) Hat auch AES wie DES die Eigenschaft, daß für alle Schlüssel s und alle Blöcke x gilt

$$\mathrm{AES}(\overline{s}, \overline{x}) = \overline{\mathrm{AES}(s, x)}\,,$$

wobei $\overline{x}$ das 1-Komplement von x bezeichnet?

Aufgabe 4: (*6 Punkte*)

Die beiden Bytes x, y werden durch die Byte-Substitution von AES in $\widetilde{x}, \widetilde{y}$ übergeführt. Wie viele Möglichkeiten gibt es bei bekannter Differenz $\Delta = x \oplus y$ für den Wert der Differenz $\widetilde{x} \oplus \widetilde{y}$? Was folgt daraus für die Sicherheit von Rijndael gegen differentielle Kryptanalyse?

Abgabe bis zum Dienstag, dem 20. Dezember 2007, um 12.00 Uhr