Wolfgang K. Seiler
Tel. 2515

A5, C201

18. November 2010

10. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*
Berechnen Sie über dem Körper $\mathbb{F}_2 = \{0, 1\}$ mit zwei Elementen den 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 2: *(4 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 Donnerstag, dem 25. November 2010, um 15.30 Uhr