

E. Best

21.05.2004

Abgabe: 04.06.2004

Freitags in der Vorlesung

## 6. Übung zur Vorlesung Kryptographie

**Achtung 1:** Nächste Woche gibt es 2 Übungsgruppentermine: **Montag**, 24.5., wie gewohnt; **Mittwoch**, 26.5., 8:15 in Raum A7-0-025. Am Mittwoch, 2.6., gibt es **keinen** Übungsgruppentermin.

**Achtung 2:** Für das 6. Übungsblatt haben Sie 2 Wochen Bearbeitungszeit. **Schöne Pfingsten!**

**Aufgabe 20:** DES-Beispielanwendung (4 Punkte)

Sei folgender Klartext gegeben:

1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010 .

Zur Vereinfachung sei die Permutation  $IP$  die Identität, so dass der Anfangszustand  $L^0R^0$  ebenfalls diesem Klartext entspricht. Der erste Rundenschlüssel sei

$$K^1 = 000110 110000 001011 101111 111111 000111 000001 110010 .$$

Berechnen Sie den Zustand  $L^1R^1$  nach der ersten Runde.

**Aufgabe 21:** Polynomdivision (3+3 Punkte)

Geben Sie den größten gemeinsamen Teiler  $c = ggT(a, b)$  der beiden Polynome  $a$  und  $b$  an und liefern Sie eine Zerlegung  $c = u \cdot a + v \cdot b$  mit Polynomen  $u$  und  $v$ .

(a)  $a = x^5 - x^4 + x - 1$  und  $b = x^3 - 3x^2 + 3x - 1$ . Diese sollen als Polynome über dem Körper der rationalen Zahlen interpretiert werden.

(b)  $a = x^8 + x^4 + x^3 + x + 1$  und  $b = x^7 + x^5 + x^3 + x$ . Diese sollen als Polynome über  $F_2$  interpretiert werden.

**Aufgabe 22:** Der Polynomkörper  $GF(2^2)$  (3+2 Punkte)

(a) Zeigen Sie, dass das Reduktionspolynom  $x^2 + x + 1$  irreduzibel ist.

(b) Das Reduktionspolynom  $x^2 + x$  ist *nicht* irreduzibel; zeigen Sie, dass die entstehende Multiplikationstabelle Körperaxiome verletzt.

**Aufgabe 23:** Der Polynomkörper  $GF(2^4)$  (5 Punkte)

Wir betrachten  $p = 2$  und  $n = 4$ , d.h. den Körper  $GF(2^4)$  mit 16 Polynomen. Geben Sie ein möglichst einfaches Generatorpolynom  $a$  an (d.h., ein Polynom  $a \in GF(2^4)$  mit  $\langle a \rangle = GF(2^4) \setminus \{0\}$ ) und stellen Sie eine Tabelle auf (so wie im Skript die Tabelle nach Satz 4.2.7), die alle Polynome  $b \in GF(2^4)$  nach algebraischer Darstellung, Binärdarstellung, Hexadezimaldarstellung, Potenz von  $a$ , Logarithmus von  $b$  auflistet.

**Aufgabe 24:** **Zusatzaufgabe:** AES-Beispielanwendung (10 Punkte)

Berechnen Sie mit dem folgenden 128-Bit-AES-Schlüssel:

2B7E151628AED2A6ABF7158809CF4F3C

das Chifftrat des folgenden Klartextes:

3243F6A8885A308D313198A2E0370734

Sie können frei verfügbare AES-Implementierungen benutzen, sollten aber möglichst „vielsagende“ Ausgaben liefern.