Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2011/12
21. Dez. 2011

Einführung in die Kryptographie

Übungsblatt 5

Aufgabe 17

Die Elemente des Körpers $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(\varphi(X))$, wobei φ das irreduzible Polynom $\varphi(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$ bezeichnet, seien mit 4-Bit-Zahlen identifiziert, wobei $\xi = \sum_{i=0}^{3} a_i 2^i$ dem Körperelement $\sum a_i X^i \bmod \varphi(X)$ entspreche. Wir benutzen hexadezimale Notation für die 4-Bit-Zahlen.

a) Sei $u :=$ `'2'`, $v :=$ `'A'`. Man berechne $u + v$, $u \cdot v$, u^3 und u^5.

b) Man beweise: Das Element $u =$ `'2'` ist eine Primitivwurzel von $\mathbb{F}_{2^4}^*$, d.h. ein erzeugendes Element der multiplikativen Gruppe $\mathbb{F}_{2^4}^*$.

Aufgabe 18

Sei K ein Körper und R der Ring $R := K[T]/(T^4 - 1)$, der ein 4-dimensinaler Vektorraum über K ist. Multiplikation mit dem Polynom

$$a(T) := a_3T^3 + a_2T^2 + a_1T + a_0 \in K[T]$$

induziert eine K-lineare Abbildung

$$a : R \to R, \quad g(T) \bmod (T^4 - 1) \;\mapsto\; a(T)g(T) \bmod (T^4 - 1).$$

a) Man berechne die Matrix $C = C(a_0, a_3, a_2, a_1) \in M(4\times 4, K)$ der Abbildung a bezüglich der Basis $(\overline{1}, \overline{T}, \overline{T^2}, \overline{T^3})$ von R über K.

Bemerkung. Eine Matrix der Form $C(a_0, a_3, a_2, a_1)$ heißt *zirkulante* Matrix. Eine solche Matrix kommt in der Operation `MixColumns` von AES vor.

b) Man zeige, dass die Matrix C genau dann invertierbar ist, wenn die Polynome $a(T)$ and $T^4 - 1$ teilerfremd sind. In diesem Fall ist die Inverse von C ebenfalls eine zirkulante Matrix.

c) Sei jetzt $K = \mathbb{F}_{16}$ der in Aufgabe 17 definierte Körper und

$$a(T) = \text{`3'} \cdot T^3 + T^2 + T + \text{`2'} \in \mathbb{F}_{16}[T]$$

Man berechne die Matrix $C(a_0, a_3, a_2, a_1)^{-1}$ für diesen Fall.

---

b.w.

Aufgabe 19

Sei $N = pq$ ein RSA-Modul und e ein zugehöriger Verschlüsselungs-Exponent.
a) Man beweise, dass die Verschlüsselungs-Abbildung

$$E : \mathbb{Z}/N \to \mathbb{Z}/N, \quad x \mapsto E(x) := x^e \bmod N,$$

mindestens 9 Fixpunkte besitzt, d.h. Elemente $x \in \mathbb{Z}/N$ mit $E(x) = x$.
Genauer gilt: Die Anzahl der Fixpunkte beträgt

$$r = (1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1)).$$

b) Man bestimme alle Fixpunkte für $(N, e) = (866959, 17)$.

Aufgabe 20

Ein Mini-RSA-System mit öffentlichem Schlüssel $(N, e) = (61823, 17)$ werde als ASCII-Bigramm-Verschlüsselung

$$\mathbb{Z}_{256}^2 \to \mathbb{Z}_{256}^2, \quad (a, b) \mapsto (\overline{a}, \overline{b}),$$

benutzt, die wie folgt definiert sei:

$$x := a \cdot 256 + b, \quad y := x^e \bmod N, \quad y = \overline{a} \cdot 256 + \overline{b}.$$

Der folgende Geheimtext aus 36 Bytes entstand auf diese Weise.

```
3DEB B539 DBF7 2D10 6D9B E872 DF6C 0706 00F4
4382 2839 0389 1825 116E 9AA2 596F D7BA 80D7
```

Man finde den Klartext.