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

WS 2018/19
7. Nov. 2018

Übungen zur Vorlesung Kryptographie

Blatt 4

Aufgabe 13

Die Folge $z_i \in \mathbb{Z}_{25}$, $i \geqslant 0$, werde durch einen 'linearen Kongruenz-Generator'

$$f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}, \quad z \mapsto (az + b) \bmod 25,$$

mit einem Anfangselement $z_0 \in \mathbb{Z}_{25}$ durch die Rekursionsformel $z_{i+1} := f(z_i)$ erzeugt. Wir fassen die Folge $(z_1, z_2, \ldots, z_N) \in \mathbb{Z}_{25}^N$ als Pseudo-One-Time-Pad auf. Wir identifizieren $\mathbb{Z}_{25}$ mit dem Alphabet `A`, ..., `Z`, wobei `I/J` als ein Buchstabe gelte.

Der folgende Geheimtext der Länge $N = 41$ entstand aus einem englischen Klartext durch Addition modulo 25 des oben beschriebenen Pseudo-One-Time-Pads.

```
AXXLW OKIYN ZVZGT GQTQG LIYFG MHLEP IFBOD YVRER U
```

Der Klartext beginnt mit dem Trigramm `THE`. Man berechne a, b und bestimme den Klartext.

Aufgabe 14

a) Sei $F(X) = \sum_{\nu=0}^{n} a_\nu X^\nu \in \mathbb{F}_2[X]$, $a_n = 1$, ein irreduzibles Polynom vom Grad $n > 1$ über dem Körper $\mathbb{F}_2$. Man zeige:

(i) $a_0 = 1$.

(ii) Die Anzahl der $\nu \in \{0, 1, \ldots, n\}$ mit $a_\nu = 1$ ist ungerade.

(iii) Das "gespiegelte" Polynom

$$G(X) = \sum_{\nu=0}^{n} a_\nu X^{n-\nu}$$

ist ebenfalls irreduzibel.

b) Man erstelle eine Liste aller irreduziblen Polynome über $\mathbb{F}_2$ vom Grad $\leqslant 5$.

---

b.w.

Aufgabe 15

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 $u + v$, $u \cdot v$, v^2, u^2, u^3 und u^5.

b) Man beweise: Das Element $u =$ `'2'` ist eine *Primitivwurzel* von $\mathbb{F}_{16}^*$, d.h. ein erzeugendes Element der (15-elementigen) multiplikativen Gruppe $\mathbb{F}_{16}^*$.

c) Man stelle das Element v als Potenz von u dar.

Aufgabe 16

Sei K ein Körper und $F(X) \in K[X]$ das Polynom

$$F(X) := X^m - 1, \qquad m \geqslant 2.$$

Der Restklassenring $R := K[X]/(F(X))$ ist insbesondere ein m-dimensionaler Vektorraum über K mit der Basis

$$1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{m-1}, \quad \text{wobei} \quad \overline{X} := X \bmod F(X).$$

Weiter sei

$$\varphi(X) = a_0 + a_1 X + \ldots + a_r X^r \in K[X]$$

ein Polynom vom Grad $r \leqslant m - 1$.

a) Man zeige: Die Multiplikation mit $\varphi(X)$ induziert eine K-lineare Abbildung $\mu_\varphi : R \to R$. Man bestimme die Matrix

$$A_\varphi \in M(r \times r, K)$$

dieser Abbildung bzgl. der Basis $1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{m-1}$.

b) Man beweise: Die Matrix A_φ ist genau dann invertierbar, falls die Polynome $\varphi(X)$ und $F(X)$ teilerfremd sind. In diesem Fall gilt

$$A_\varphi^{-1} = A_\psi,$$

wobei $\psi(X) \in K[X]$ ein Polynom mit $\varphi(X)\psi(X) \equiv 1 \bmod F(X)$ ist.

Bemerkung. Matrizen der obigen Art kommen in der Beschreibung der AES-Verschlüsselung vor (einmal mit $K = \mathbb{F}_2$ und einmal mit $K = \mathbb{F}_{256}$).