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

WS 2015/16
18. Nov. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 5

Aufgabe 17

Gegeben seien die beiden irreduziblen Polynome 4. Grades

$$F(X) := X^4 + X + 1, \qquad G(X) := X^4 + X^3 + 1$$

über dem Körper $\mathbb{F}_2$, (vgl. Aufgaben 11 und 12). Sei ξ eine Nullstelle von $F(X)$ (in einem Erweiterungskörper) und η eine Nullstelle von $G(X)$.

Bekanntlich sind die Körper $K_1 := \mathbb{F}_2(\xi)$ und $K_2 := \mathbb{F}_2(\eta)$ isomorph (da sie gleich viele Elemente haben). Man konstruiere einen expliziten Isomorphismus $\phi : K_1 \to K_2$ mit Angabe der Matrix von ϕ bzgl. der Basen $1, \xi, \xi^2, \xi^3$ von K_1 und $1, \eta, \eta^2, \eta^3$ von K_2.

Aufgabe 18

Eine Verknüpfung $\boxtimes : \mathbb{Z}_{256} \times \mathbb{Z}_{256} \to \mathbb{Z}_{256}$ werde mithilfe der Bijektion

$$\phi : \mathbb{Z}_{256} \to \mathbb{F}_{257}^*, \quad x \mapsto \phi(x) := \begin{cases} 256 & \text{für } x = 0, \\ x & \text{für } x \neq 0, \end{cases}$$

wie folgt definiert: $x \boxtimes y := \phi^{-1}(\phi(x) \cdot \phi(y))$, wobei '$\cdot$' die Multiplikation im Körper $\mathbb{F}_{257}$ bedeutet. Man zeige:

a) $(\mathbb{Z}_{256}, \boxtimes)$ ist eine abelsche Gruppe, die zu $(\mathbb{Z}_{256}, +)$ isomorph ist.

b) $(\mathbb{Z}_{256}, +, \boxtimes)$ ist kein Ring.

Aufgabe 19

Man betrachte folgende Mini-Version eines 2-Runden Feistel-Netzwerks:
Die Blocklänge ist $16 = 2 \times 8$ Bits $= 2$ Bytes. Die i-te Runden-Transformation ist

$$(L, R) \mapsto (R, L \oplus f(R, K_i)) \quad \text{mit} \quad f(x, K_i) := (A_i \boxtimes x + B_i) \bmod 256,$$

wobei $\boxtimes$ wie in Aufgabe 18 definiert ist und $K_i = (A_i, B_i) \in \mathbb{Z}_{256}^2$, $i = 1, 2$, unabhängige Runden-Schlüssel sind. Nach der letzten (= zweiten) Runde wird die rechte und linke Hälfte nochmals vertauscht.

---

b.w.

Der folgende Geheimtext entstand aus einem deutschen Ascii-Klartext der Länge von 114 Bytes durch Block-Verschlüsselung (im ECB-Modus) mittels des oben beschriebenen Feistel-Netzwerks.

```
DD74 E31D 6D11 9715 8638 331A 2B58 E31D EB29 8BFF 68C0 062D 671A 6734 4FD5
A80C 8608 0906 640D 9952 5516 2B58 9268 C000 2B58 C000 6A88 D7A9 0906 BACC
3624 664E C000 5B2C C000 2B58 EB03 679D 9CD8 2905 D644 6541 062D C748 A81C
5312 C114 331A 797A FF0F C748 B002 FB32 0C06 895F 7157 3405
```

Der Klartext beginnt mit den vier Bytes "`Das `", hexadezimal `4461 7320`.

a) Man bestimme die Schlüssel $(A_1, B_1), (A_2, B_2)$ und den gesamten Klartext.

b) Wie lautet die Verschlüsselung desselben Klartextes mit denselben Schlüsseln im CBC-Modus mit Initialvektor $iv :=$ `ABCD`.

Aufgabe 20

Mit Hilfe des Polynoms $F(X) := X^8 + 1 \in \mathbb{F}_2[X]$ werde der Ring

$$R := \mathbb{F}_2[X]/(F(X))$$

definiert. R ist ein 8-dimensionaler Vektorraum über $\mathbb{F}_2$. Sei

$$G(X) := X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X].$$

Man betrachte die Abbildung

$$\psi : R \to R, \quad f \mapsto \psi(f) := G \cdot f \bmod F.$$

Man zeige:

a) Die Matrix von ψ bzgl. der Basis $(\overline{1}, \overline{X}, \ldots, \overline{X^7})$ von R über $\mathbb{F}_2$ ist

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Bemerkung. Diese Matrix kommt in der Beschreibung der Byte-Substitution von AES vor.

b) Es gilt $\gcd(F, G) = 1$. Man bestimme mit dem Erweiterten Euklidischen Algorithmus das Inverse von G mod F im Ring R.

c) Die Matrix $M \in \mathrm{M}(8 \times 8, \mathbb{F}_2)$ ist invertierbar. Man berechne M^{-1}.

Hinweis. Man benutze b).