Übungsblatt 8

Aufgabe 41 ***mündlich***

(a) Zeigen Sie, dass der Kryptotext einer Feistel-Chiffre dadurch entschlüsselt werden kann, dass man ihn nochmals verschlüsselt, wobei die Rundenschlüssel in der umgekehrten Reihenfolge benutzt werden.

(b) Beweisen Sie, dass folgende vier Schlüssel (in Hexadezimaldarstellung) die einzigen schwachen Schlüssel für den DES-Algorithmus sind:

`0101010101010101, FEFEFEFEFEFEFEFE,`
`1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1`

(c) Begründen Sie, dass für schwache Schlüssel K gilt: $\mathrm{DES}(K, \mathrm{DES}(K, x)) = x$.

(d) Ein DES-Schlüssel K heißt semi-schwach, falls er genau zwei verschiedene Rundenschlüssel erzeugt (d. h. falls gilt $\left\|\{K^1, \ldots, K^{16}\}\right\| = 2$). Geben Sie zwei semi-schwache Schlüssel K und K' an, für die $\mathrm{DES}(K', \mathrm{DES}(K, x)) = x$ gilt.

Aufgabe 42 ***mündlich***

(a) Ermitteln Sie den 64-Bit-Schlüsselblock, der (bei ungerader Parität) zum 56-Bit-DES-Schlüssel `01 23 45 67 89 AB CD` (Hexadezimaldarstellung) gehört.

(b) Zeigen Sie: $\mathrm{DES}(\overline{K}, \overline{x}) = \overline{\mathrm{DES}(K, x)}$. ($\overline{x}$ ist die bitweise Negation von x.)

(c) Zeichnen Sie das Berechnungsdiagramm des DES-Schlüsselgenerators, der die Rundenschlüssel $K^1, \ldots, K^{16}$ in der umgekehrten Reihenfolge generiert.

Aufgabe 43 ***mündlich***

(a) Bestimmen Sie in $\mathbb{Z}_5[x]/3x^2 + 1$ den Repräsentanten für die Restklasse, in der das Polynom $2x^5 + x^4 + 4x + 3$ enthalten ist.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_2[x]$. Stellen Sie jeweils die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_2[x]/m(x)$ auf.

(c) Sei $m(x) = x^2 + 2$. Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf. Ist $\mathbb{Z}_3[x]/m(x)$ ein Körper?

(d) Berechnen Sie das multiplikative Inverse von $a(x) = x^4 + x^2 + 2x$ in $\mathbb{Z}_3[x]/m(x)$, wobei $m(x) = 2x^6 + x^3 + x^2 + 2$ ist. Ist $m(x)$ irreduzibel über $\mathbb{Z}_3$?

Aufgabe 44 ***mündlich***

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$.

(a) Zeigen Sie, dass ab die Ordnung $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$ hat, falls $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd sind.

(b) Lässt sich die Aussage in Teilaufgabe (a) zu $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$ verallgemeinern?

Aufgabe 45 ***mündlich***

(a) Zeigen Sie, dass ein Polynom $p(x) \in \mathbb{F}[x]$ vom Grad $n \geq 1$ über einem Körper $\mathbb{F}$ höchstens n Nullstellen besitzt.

(b) Finden Sie Polynome $q_d(x) \in \mathbb{Z}_6[x]$ vom Grad $d = 1, 2$ mit möglichst vielen Nullstellen.

Aufgabe 46 ***mündlich***

Zeigen Sie, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

Aufgabe 47 ***mündlich, optional***

(a) Zeigen Sie, dass der Polynomrestklassenring $\mathbb{Z}_p[x]/m(x)$ genau dann ein Körper ist, wenn $m(x)$ irreduzibel über $\mathbb{Z}_p$ ist.

(b) Zeigen Sie, dass zu jedem Polynom $f(x)$ in $\mathbb{Z}_p[x]$ ein endlicher Körper K existiert, der $\mathbb{Z}_p$ als Unterkörper enthält und in dem $f(x)$ in Linearfaktoren zerfällt (der kleinste solche Körper $K_p(f(x))$ ist bis auf Isomorphie eindeutig bestimmt und heißt der Zerfällungskörper für $f(x)$ über $\mathbb{Z}_p$).

(c) Zeigen Sie, dass der Zerfällungskörper $K = K_p(x^{p^n} - x)$ genau p^n Elemente enthält. Schließen Sie hieraus auf die Existenz eines irreduziblen Polynoms $m(x)$ vom Grad n über $\mathbb{Z}_p$, indem Sie zu einem beliebigen Erzeuger g der multiplikativen Gruppe K^* von K ein Polynom $m(x)$ kleinsten Grades mit $m(g) = 0$ bestimmen.

Aufgabe 48 ***10 Punkte***

(a) Alice verschlüsselt die Klartextblöcke $x_1, x_2, \ldots, x_n$ mit einer Blockchiffre zu Kryptotextblöcken $y_1, y_2, \ldots, y_n$ und sendet sie an Bob, der sie wieder entschlüsselt. Wie viele Klartextblöcke werden durch einen bei der Übertragung von Block y_i auftretenden Fehler maximal verfälscht, wenn der ECB-, CBC-, OFB-, CFB- beziehungsweise Counter-Mode benutzt wird? Unterscheiden Sie ggf. auch unterschiedliche Segmentlängen t.

(b) Wie wirkt sich der Verlust eines Blockes y_i bei der Übertragung auf den von Bob berechneten Klartext aus?