Mathematische Grundlagen der Kryptografie (01321) SS 08

Klausur am 27.09.2008:

Aufgabenstellungen

Aufgabe 1

(a) Verschlüsseln Sie das Wort R H E I N mit dem Verschiebe-Kryptosystem und dem Schlüssel 5.

(b) Der Geheimtext V D P W ist mit dem Permutations-Kryptosystem mit dem Schlüsselwort N E B E N F L U S S und dem Schlüsselbuchstaben R verschlüsselt. Wie lautet der Klartext?

(c) Verschlüsseln Sie das Wort D O N A U mit dem Vigenère-Kryptosystem und dem Schlüsselwort K A N A L.

(d) Der Geheimtext L P M F ist mit dem Selbstschlüssel-Kryptosystem und dem Schlüssel 7 verschlüsselt. Wie lautet der Klartext?

(e) Verschlüsseln Sie das Wort O D E R mit dem Hill-Kryptosystem und der Schlüsselmatrix $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

(Hinweis: Die numerischen Äquivalente zu den Buchstaben finden Sie am Schluss der Klausur.)

[*2 + 2 + 2 + 2 + 2 = 10 Punkte*]

Aufgabe 2

Geben Sie jeweils ein Beispiel (ohne Begründung) für

(a) einen Ring mit Charakteristik 5, der kein Körper ist.

(b) ein Element in $\mathbb{C}$, dessen Minimalpolynom über $\mathbb{Q}$ den Grad 3 hat.

(c) eine unendliche Gruppe, die abelsch ist.

(d) eine unendliche Gruppe, die nicht abelsch ist.

(e) eine Pseudoprimzahl zur Basis 2.

[*2 + 2 + 2 + 2 + 2 = 10 Punkte*]

Aufgabe 3

(a) Zeigen Sie, dass $|(\mathbb{Z}/7\mathbb{Z})^\times| = |(\mathbb{Z}/9\mathbb{Z})^\times|$ und $|(\mathbb{Z}/5\mathbb{Z})^\times| = |(\mathbb{Z}/8\mathbb{Z})^\times|$ gilt.

(b) Zeigen Sie, dass die Gruppen $(\mathbb{Z}/7\mathbb{Z})^\times$ und $(\mathbb{Z}/9\mathbb{Z})^\times$ isomorph sind, und geben Sie einen Gruppenisomorphismus konkret an.

(c) Zeigen Sie, dass die Gruppe $(\mathbb{Z}/5\mathbb{Z})^\times$ nicht isomorph zu $(\mathbb{Z}/8\mathbb{Z})^\times$ ist.

[*4 + 3 + 3 = 10 Punkte*]

Aufgabe 4

Sei R ein Ring und $a \in R$. Dann heißt a **Idempotent**, wenn $a^2 = a$ gilt.

(a) Zeigen Sie, dass in einem Integritätsbereich 0 und 1 die einzigen Idempotente sind.

(b) Geben Sie ein Beispiel für einen kommutativen Ring R und ein Idempotent $a \in R$, das nicht 0 oder 1 ist.

[*5 + 2 = 7 Punkte*]

Aufgabe 5

Es sei (m, e) ein Schlüssel für das RSA-Kryptosystem. Weiter sei $s > 1$ mit $e^s \equiv 1 \pmod{\varphi(m)}$. Sei $x \in \mathbb{Z}/m\mathbb{Z}$ ein Klartext, und sei $y \in \mathbb{Z}/m\mathbb{Z}$ der zugehörige Geheimtext. Zeigen Sie, dass $y^{e^{s-1}} = x$ in $\mathbb{Z}/m\mathbb{Z}$ gilt.

[*6 Punkte*]

Aufgabe 6

Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$ mit $(\frac{a}{p}) = (\frac{b}{p}) = 1$. Zeigen Sie, dass die Kongruenz $ax^2 \equiv b \pmod{p}$ eine Lösung besitzt.

[*8 Punkte*]

Aufgabe 7

Alice und Bob möchten mit dem Diffie-Hellman-System einen gemeinsamen Schlüssel vereinbaren. Sie wählen sich als endlichen Körper $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$ und als erzeugendes Element $g = [T+1] = T+1 \pmod{T^3+T+1}$. Alice wählt $e_A = 3$ und Bob wählt $e_B = 4$.

(a) Welches Körperelement schickt Alice an Bob?

(b) Welches Körperelement schickt Bob an Alice?

(c) Was ist der geheime Schlüssel?

Alle Körperelemente sollen dabei aus der Menge $\{0, 1, [T], [T+1], [T^2], [T^2+1], [T^2+T], [T^2+T+1]\}$ stammen.

[*3 + 3 + 3 = 9 Punkte*]

Aufgabe 8

Sei $q = p^n$ eine Primzahlpotenz, und sei $f \in \mathbb{F}_q[T]$ mit $\text{Grad}(f) = m \geq 1$. Zeigen Sie, dass f genau dann m verschiedene Nullstellen in $\mathbb{F}_q$ besitzt, wenn f ein Teiler des Polynoms $T^q - T \in \mathbb{F}_q[T]$ ist.

[*8 Punkte*]

Aufgabe 9

Beschreiben Sie kurz - jeweils in 1-2 Sätzen - das Knapsack-Kryptosystem.

(a) Welches algorithmisch schwierige Probelm liegt dem Knapsack-Kryptosystem zugrunde?

(b) Was ist der geheime Schlüssel?

(c) Wie sieht der öffentliche Schlüssel aus und wie wird er konstruiert?

(d) Wie wird verschlüsselt?

(e) Wie heißt der Algorithmus, mit dem das Kryptosystem gebrochen werden konnte? Was sind die Eingabe und die Ausgabe von diesem Algorithmus?

[*2 + 2 + 2 + 2 + 4 = 12 Punkte*]

Hinweis: Die Buchstaben A,..,Z entsprechen folgenden Elementen aus $\mathbb{Z}/26\mathbb{Z}$:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25