Mathematische Grundlagen der Kryptografie (01321) SS 08

Klausur am 16.08.2008:

Aufgabenstellungen

Aufgabe 1

Entschlüsseln Sie die folgenden Botschaften:

(a) E O X P H, wobei das Verschiebe-Kryptosystem mit dem Schlüssel 3 benutzt wurde.

(b) L W S A Y X M D T P U F F B I, wobei das Vigenère-Kryptosystem mit dem Schlüsselwort T U L P E benutzt wurde.

(c) D K E T Q N E V, wobei das Hill-Kryptosystem mit der Schlüsselmatrix $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$ benutzt wurde.

(d) V W S V T E, wobei das Permutationskryptosystem mit dem Schlüsselwort S C H W E R T L I L I E und dem Schlüsselbuchstaben O benutzt wurde.

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

[*2 + 2 + 4 + 2 = 10 Punkte*]

Aufgabe 2

Geben Sie jeweils ein Beispiel (mit kurzer Begründung) für:

(a) einen quadratischen Rest modulo 5147, der $\neq 1$ ist.

(b) einen quadratischen Nichtrest modulo 5147.

(c) ein Polynom $f \in \mathbb{F}_3[T]$, so dass $\mathbb{F}_3[T]/(f) \simeq \mathbb{F}_9$ gilt.

(d) ein Polynom $f \in \mathbb{F}_3[T]$, so dass $\mathbb{F}_3[T]/(f) \not\simeq \mathbb{F}_9$ gilt.

(e) eine endliche abelsche Gruppe, die nicht zyklisch ist.

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

Aufgabe 3

Sie sind Oscar und wissen, dass Alice und Bob das RSA-Kryptosystem mit dem öffentlichen Schlüssel $(n, e) = (97, 29)$ benutzen. Alice schickt den Wert 3 an Bob. Was ist der Klartext?

[*10 Punkte*]

Aufgabe 4

Sei $1 \neq n \in \mathbb{N}$. Die (multiplikative) Gruppe G enthalte genau ein Element g_0 der Ordnung n. Beweisen Sie:

(a) Es gilt $n = 2$.

(b) Die Menge $\{1, g_0\}$ ist eine Untergruppe von G.

(c) Die Menge $\{1, g_0\}$ ist ein Normalteiler von G.

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

Aufgabe 5

Es sei R ein kommutativer Ring, und das Ideal (T) sei ein Primideal in $R[T]$. Zeigen Sie, dass R ein Integritätsbereich ist.

[*4 Punkte*]

Aufgabe 6

Finden Sie 4 Quadratwurzeln von 4 in $\mathbb{Z}/209\mathbb{Z}$. (Hinweis: Es gilt $209 = 11 \cdot 19$.)

[*10 Punkte*]

Aufgabe 7

(a) Ist 6 eine Pseudoprimzahl zur Basis 5?

(b) Ist 15 eine Carmichael-Zahl?

(Begründung nicht vergessen!)

[*3 + 3 = 6 Punkte*]

Aufgabe 8

Sei $G = \{2 \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mid a, b, c \in \mathbb{Z}\} \cup \{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + 2 \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mid a, b, c \in \mathbb{Z}\}$. Zeigen Sie, dass G ein Gitter mit Basis $\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ist.

[*10 Punkte*]

Aufgabe 9

Beschreiben Sie kurz (4-5 Sätze reichen), warum elliptische Kurven über endlichen Körpern für die Kryptografie interessant sind und welche Vorteile sie gegenüber endlichen Körpern haben.

[*8 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