Mathematische Grundlagen der Kryptografie (1321)SoSe 07

Nachklausur am 29.09.2007:

Aufgabenstellungen

Aufgabe 1

Entschlüsseln Sie folgende Nachrichten:

(a) V K A Z G, wobei der Text mit dem Verschiebe-Kryptosystem und dem Schlüssel 21 verschlüsselt ist.

(b) V J E U S F J X, wobei der Text mit dem Vigenère-Kryptosystem und dem Schlüssel OBST verschlüsselt ist.

(c) B B N N R V, wobei der Text mit dem Hill-Kryptosystem und der Schlüsselmatrix $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ verschlüsselt ist.

(d) K V Y O L, wobei der Text mit dem affinen Kryptosystem und dem Schlüssel $(9, 1)$ verschlüsselt ist.

(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 für

(a) ein Gitter $L(a_1, a_2)$ in $\mathbb{R}^2$ und eine Basis b_1, b_2 von $\mathbb{R}^2$ mit $b_1 \neq \pm a_1$, $b_1 \neq \pm a_2$, $b_2 \neq \pm a_1$, $b_2 \neq \pm a_2$ und $L(a_1, a_2) = L(b_1, b_2)$.

(b) ein $f \in \mathbb{F}_3[T]$, so dass $\mathbb{F}_3[T]/(f) = \mathbb{F}_{27}$ gilt.

[4 + 4 = 8 Punkte]

Aufgabe 3

Wie kann die Struktur einer elliptischen Kurve, die 100 Elemente besitzt, als abelsche Gruppe aussehen?

[*4 Punkte*]

Aufgabe 4

Formulieren Sie das quadratische Reziprozitätsgesetz (für das Legendre-Symbol).

[*4 Punkte*]

Aufgabe 5

Sei $G = (\mathbb{Z}/27\mathbb{Z})^\times$.

(a) Wie viele Elemente besitzt G?

(b) Wie viele erzeugende Elemente von G gibt es?

(c) Ein erzeugendes Element von G ist 2. Welches sind die anderen?

(d) Bestimmen Sie die Untergruppe der Ordnung 3 von G.

(e) Wie sieht die Zerlegung von G nach dem Struktursatz endlicher zyklischer Gruppen aus?

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

Aufgabe 6

(a) Bestimmen Sie die letzten drei Ziffern von 3^{2405}.

(b) Zeigen Sie, dass es ein $b \in \mathbb{Z}$ gibt, so dass $b^2 - 7$ durch $64959 = 3 \cdot 59 \cdot 367$ teilbar ist (Die Zahlen 7, 59 und 367 sind Primzahlen).

[$4 + 8 = 12$ *Punkte*]

Aufgabe 7

Sei $a \in \mathbb{Z}$ mit $a \neq 0$. Zeigen Sie, dass es nur endlich viele Ideale in $\mathbb{Z}$ gibt, die a enthalten.

[*8 Punkte*]

Aufgabe 8

Sei R ein endlicher Ring und $a \in R$, so dass $ra \neq 0$ für alle $r \in R$ mit $r \neq 0$ gilt. Zeigen Sie, dass a invertierbar ist.

(Hinweis: Betrachten Sie die Abbildung $f : R \longrightarrow R$ mit $f(r) = ra$ für alle $r \in R$.)

[*10 Punkte*]

Aufgabe 9

Stellen Sie sich vor, Sie sind Bob und Ihre Freundin Alice möchte Ihnen eine Nachricht schicken. Dazu benutzen Sie das ElGamal-Kryptosystem, wobei $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T + 1)$ und $g = [T]$ als Ihr öffentlicher Schlüssel dienen. Nachrichten sind Bit-Folgen (a_2, a_1, a_0) der Länge drei, wobei (a_2, a_1, a_0) mit $a_i \in \{0, 1\}$ für $0 \leq i \leq 2$ mit $[a_2T^2 + a_1T + a_0]$ identifiziert wird. Ihr geheimer Schlüssel ist $a = 3$, und Alice schickt Ihnen $([T^2+T], [T+1])$. Wie lautet Alices Nachricht als Bit-Folge?

[*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