Mathematische Grundlagen der Kryptografie (1321) SS06

Klausur am 19.08.2006:

Aufgabenstellungen

I. Die Lösungen der folgenden Aufgaben brauchen Sie nicht zu begründen.

Aufgabe I.1

Verschlüsseln Sie das Wort KLAUSUR

(a) mit dem Verschiebe-Kryptosystem und dem Schlüssel 15.

(b) mit dem Permutationskryptosystem mit dem Schlüsselwort KRYPTOGRAFIE und dem Schlüsselbuchstaben S.

(c) mit dem Vigenère-Kryptosystem und dem Schlüsselwort EUKLID.

(d) mit dem Selbstschlüsselkryptosystem und dem Schlüssel 10.

$[2 + 2 + 2 + 2 = 8 \ Punkte]$

Aufgabe I.2

Berechnen Sie die folgenden Jacobi-Symbole:

(a) $(\frac{117}{37})$

(b) $(\frac{58}{113})$.

$[2 + 2 = 4 \ Punkte]$

Aufgabe I.3

Geben Sie jeweils ein Beispiel für Ringe R und S und einen surjektiven Ringhomomorphismus $\phi : R \longrightarrow S$ mit

(a) S ist ein Integritätsbereich und R nicht.

(b) R ist ein Integritätsbereich und S nicht.

[*3 + 3 = 6 Punkte*]

Aufgabe I.4

Geben Sie ein Beispiel für ein Gitter im $\mathbb{R}^3$ mit Determinante 15, das den Vektor $\begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$ enthält.

[*4 Punkte*]

II. Die Lösungen der folgenden Aufgaben sollen begründet werden.

Aufgabe II.1

Die folgende Botschaft ist mit dem Hill-Kryptosystem und der Schlüsselmatrix $\begin{pmatrix} -8 & -9 \\ -9 & -8 \end{pmatrix}$ verschlüsselt.

UHUSQHKX

Wie lautet der Klartext?

[*6 Punkte*]

Aufgabe II.2

(a) Zeigen Sie, dass $(\mathbb{Z}, +)$ ein Normalteiler von $(\mathbb{Q}, +)$ ist.

(b) Zeigen Sie, dass jedes Element von $\mathbb{Q}/\mathbb{Z}$ endliche Ordnung hat.

(c) Zeigen Sie, dass $\mathbb{Q}/\mathbb{Z}$ unendlich viele Elemente besitzt.

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

Aufgabe II.3

(a) Zeigen Sie, dass $11^{84} - 5^{84}$ durch 7 teilbar ist.

(b) Zeigen Sie (mit dem Satz von Euler und dem Chinesischen Restsatz), dass $n^{12} \equiv 1 (\mathrm{mod} 72)$ für alle $n \in \mathbb{N}$ mit $\mathrm{ggT}(n, 72) = 1$ gilt.

[*5 + 5 = 10 Punkte*]

Aufgabe II.4

Zeigen Sie, dass Vielfache von 21 keine Carmichael-Zahl sein können.

[*8 Punkte*]

Aufgabe II.5

Alice und Bob möchten mit dem Diffie-Hellman-Verfahren einen Schlüssel austauschen. Sie vereinbaren als endlichen Körper $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3+T+1)$ und als primitives Element $[T] = T \bmod (T^3+T+1)$. Alice wählt $e_A = 6$ und Bob wählt $e_B = 3$. Was ist der Schlüssel?

[*10 Punkte*]

Aufgabe II.6

Beschreiben Sie (jeweils kurz in 1-2 Sätzen) das RSA-Kryptosystem.

(a) Woraus besteht der öffentliche Schlüssel?

(b) Welches ist der geheime Schlüssel?

(c) Wie wird chiffriert?

(d) Wie wird dechiffriert?

(e) Warum ist das RSA-Verfahren sicher?

(f) Warum ist das RSA-Verfahren effizient?

[*2 + 2 + 2 + 2 + 2 + 4 = 14 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