# Mathematische Grundlagen der Kryptografie (1321) SS05

**Klausur am 20.08.2005:**

**Aufgabenstellungen**

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

### Aufgabe I.1

Verschlüsseln Sie das Wort HALLO mit

(a) der Caesar-Verschiebung und dem Schlüssel 5.

(b) dem Permutationskryptosystem mit Schlüsselwort = (Ihr Vorname) und Schlüsselbuchstaben = (erster Buchstabe Ihres Nachnamens).

(c) dem affinen Kryptosystem und dem Schlüssel $(a, b) = (3, 5)$.

[*2 + 2 + 2 = 6 Punkte*]

### Aufgabe I.2

Zählen Sie alle primitiven Elemente von $\mathbb{F}_{11}$ auf.

[*4 Punkte*]

### Aufgabe I.3

Welchen Grad hat das Minimalpolynom von $\sqrt{1+\sqrt{3}}$ über $\mathbb{Q}$?

[*4 Punkte*]

### Aufgabe I.4

Welche Gruppenstruktur kann eine elliptische Kurve mit 72 Elementen haben?

[*4 Punkte*]

**Aufgabe I.5**

Formulieren Sie den Satz von Lagrange.

[*4 Punkte*]

**II. Die Lösungen der folgenden Aufgaben sollen begründet werden.**

### Aufgabe II.1

Der Text DPYDBLUZJOLUPOULUCPLSLYMVSNPUKLYRSHBZBY ist mit der Caesar-Verschiebung verschlüsselt. Wie lautet der Klartext?

[*10 Punkte*]

### Aufgabe II.2

Beschreiben Sie das Diffie-Hellman-Schlüsselaustauschsystem über elliptischen Kurven:

(a) Gegeben sei eine elliptische Kurve $E(a, b, \mathbb{K})$. Was ist der öffentliche Schlüssel, und welche Bedingungen sollten der öffentliche Schlüssel und die elliptische Kurve erfüllen?

(b) Was machen Alice und Bob, um den gemeinsamen Schlüssel zu erzeugen?

(c) Was ist der gemeinsame (geheime) Schlüssel?

(d) Auf welchen Annahmen beruht die Sicherheit dieses Systems?

[$3 + 2 + 2 + 3 = 10$ *Punkte*]

### Aufgabe II.3

Sei $L = \{x \in \mathbb{Z}^3 \mid x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ und $x_1 \equiv x_2 (\mathrm{mod} 3)$ und $x_1 \equiv x_3 (\mathrm{mod} 4)\}$.

(a) Zeigen Sie, dass $L$ ein Gitter ist und bestimmen Sie eine Basis des Gitters.

(b) Bestimmen Sie $\det L$.

[$8 + 2 = 10$ *Punkte*]

### Aufgabe II.4

Sei $q$ eine Primpotenz. Zeigen Sie: Jedes quadratische Polynom aus $\mathbb{F}_q[T]$ zerfällt über $\mathbb{F}_{q^2}$ in Linearfaktoren.

[*10 Punkte*]

### Aufgabe II.5

(a) Sei $p$ eine Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$. Sei $a^{-1} \in \mathbb{Z}$ mit $aa^{-1} \equiv 1 \bmod p$. Zeigen Sie: $(\frac{a^{-1}}{p}) = (\frac{a}{p})$.

(b) Sei $p$ eine Primzahl und $a, b \in \mathbb{Z}$. Zeigen Sie: Es gilt $(\frac{a}{p}) = (\frac{b}{p})$ genau dann, wenn es ein $z \in \mathbb{Z}$ mit $z \neq 0$ und $a \equiv bz^2 (\mathrm{mod} p)$ gibt.

[*4 + 6 Punkte*]

### Aufgabe II.6

Wenn man mit dem RSA-Verfahren eine Nachricht $n$ zweimal verschlüsselt und zwar mit den öffentlichen Schlüsseln $(m, e)$ und $(m, f)$, und wenn $\mathrm{ggT}(e, f) = 1$ gilt, dann kann man den Klartext $n$ aus den beiden Schlüsseltexten $c_e = n^e \bmod m$ und $c_f = n^f \bmod m$ berechnen. Wie?

[*8 Punkte*]