Mathematische Grundlagen der Kryptografie (1321) SS04

Klausur am 21.08.2004:

Aufgabenstellungen

Alle Lösungen sollen begründet werden! Wir wünschen Ihnen

Viel Erfolg!

Aufgabe 1

Der folgende Geheimtext ist mit dem Permutations-Kryptosystem mit dem Schlüssselwort Klausur und dem Schlüsselbuchstaben J verschlüsselt worden.

FRZFRZFRZ

Wie lautet der Klartext?

[*12 Punkte*]

Aufgabe 2

Sei $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2+T+1)$ und sei $\alpha = [T] = T \bmod (T^2+T+1)$. Berechnen Sie alle Punkte von $E(1, \alpha, \mathbb{F}_4)$.

[*12 Punkte*]

Aufgabe 3

Sei $n \in \mathbb{N}$ ungerade und zusammengesetzt, und sei n eine Eulersche Pseudoprimzahl zur Basis b mit $(\frac{b}{n}) = -1$. Zeigen Sie: n ist eine starke Pseudoprimzahl zur Basis b.

[*6 Punkte*]

Aufgabe 4

Beschreiben Sie 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 + 2 Punkte*]

Aufgabe 5

Sei p eine ungerade Primzahl, und sei $a \in \mathbb{F}_p^\times$ ein quadratischer Rest. Zeigen Sie, dass a nicht primitives Element von $\mathbb{F}_p^\times$ sein kann.

[*8 Punkte*]

Aufgabe 6

Sei IK ein Körper und $\sigma : \mathsf{IK} \longrightarrow \mathsf{IK}$ ein Automorphismus. Zeigen Sie: $M = \{x \in \mathsf{IK} \mid \sigma(x) = x\}$ ist ein Unterkörper von IK.

[*10 Punkte*]

Aufgabe 7

Untersuchen Sie, wie viele Punkte der Ordnung 2 es auf einer elliptischen Kurve $E(a, b, \mathbb{F}_4)$ mit $a, b \in \mathbb{F}_4$ und $b \neq 0$ geben kann, und schließen Sie daraus, dass $E(a, b, \mathbb{F}_4)$ immer zyklisch ist.

[*10 Punkte*]

Aufgabe 8

Sei $R \neq \{0\}$ ein Integritätsbereich mit nur endlich vielen Idealen. Zeigen Sie: R ist ein Körper.

[*10 Punkte*]