Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Dr. Peter Ullrich

WS 2004/05
Übungsblatt 1
21. Oktober 2004

Elliptische Kurven-Kryptosysteme

Besprechung in der 1. Übungsstunde

Aufgabe 1

LiDIA ist eine C++-Bibliothek speziell für den Bereich der algorithmischen Zahlentheorie. Studieren Sie das LiDIA Manual (siehe Homepage der Vorlesung unter "Sonstiges") und schreiben Sie – unter Verwendung der LiDIA-Bib – ein C++-Programm, das eine natürliche Zahl n von der Standard-Eingabe einliest und die Faktorisierung von n auf die Standard-Ausgabe wieder ausgibt.

Aufgabe 2

Ein Kryptosytem sei gegeben durch $\mathcal{P} = \{0, 1\}$, $\mathcal{K} = \{A, B\}$, $\mathcal{C} = \{a, b\}$ und

$$E(0, A) = a, \quad E(1, A) = b, \quad E(0, B) = b, \quad E(1, B) = a.$$

Weiterhin seien folgende Wahrscheinlichkeitsverteilungen gegeben: $\Pr(0) = 1/4$, $\Pr(1) = 3/4$, $\Pr(A) = 1/4$, $\Pr(B) = 3/4$.
Zeigen Sie, dass dies kein perfekt sicheres Kryptosystem ist.