Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
14. Juni 2000

Übungen zur Kryptologie

9. Übung

Abgabe am 5. Juli 2000

Aufgabe 32 (*schriftlich zu bearbeiten,* 8 Punkte)

Gesucht ist das Entschlüsselungs-Verfahren zu IDEA. Zeigen Sie, dass dazu der in Phase 1 modifizierte IDEA Algorithmus benutzt werden kann. Es müssen also ähnlich wie beim DES nur andere interne Schlüssel bestimmt werden. Geben Sie an, wie diese internen Schlüssel berechnet werden können.

Aufgabe 33 (*schriftlich zu bearbeiten,* 8 Punkte)

Zeigen Sie die Aussagen aus der Vorlesung zum (erweiterten) Euklidschen Algorithmus:

a) $a \geq f_{n+2}$.

b) Setzt man

$$\begin{aligned} p_i &= d_i p_{i-1} + p_{i-2},\ i \geq 1, \\ p_0 &= 1, \\ p_{-1} &= 0. \end{aligned}$$

Und

$$\begin{aligned} q_i &= d_i q_{i-1} + q_{i-2},\ i \geq 1, \\ q_0 &= 0, \\ q_{-1} &= 1. \end{aligned}$$

Dann gilt

$$b \cdot p_i - a \cdot q_i = (-1)^i \cdot r_i\,.$$

Aufgabe 34 (*schriftlich zu bearbeiten,* 12 Punkte)

Die Eingaben $a, b, m \in I\!N$ liegen als lange Bitstrings (Darstellung im Dualsystem) vor, die nicht mehr in eine Speicherzellen passen. Untersuchen sie die Zeitkomplexität für die Berechnung der folgenden Funktionen in Abhängigkeit der Länge der Binärdarstellung der Zahlen.

a) $a + b$,

b) $a \cdot b$,

c) $a \bmod m$,

d) a/m (Ganzzahldivision).

e) $\mathrm{ggT}(a, b)$,

f) $(a^b) \bmod m$.