Hans U. Simon
Michael Kallweit
Malte Darnstädt

Bochum, den 14.11.2009

Abgabe: 22.12.2009 (bis 8:15 Uhr)

Übungen zur Vorlesung

Diskrete Mathematik

WS 09/10

Übungsblatt 09

Aufgabe 9.1 Beim USB-Protokoll wird u.a. der CRC-5 Prüfcode mit Generatorpolynom $g(x) = x^5 + x^2 + 1$ verwendet.

a) Berechne (von Hand) die CRC-5 Prüfbits der binären Nachricht

$$110100101011$$

b) Ist folgender Block (Nachrichtbits und CRC-5 Prüfbits) korrekt empfangen worden

$$110011100111 \quad ?$$

Aufgabe 9.2 Folgende Nachricht wurde mit dem öffentlichen Schlüssel $n = 7387$ und $k = 4811$ gemäß RSA verschlüsselt.

$$0046\,4812\,5431\,1048\,6273$$

Dabei wurde folgende Codierung von Buchstaben verwendet und jeweils 2 aufeinander folgende Buchstaben (also vier Klartextziffern) verschlüsselt.

	A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	!
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Bestimme den Klartext! (Kleiner Tipp: $83|n$)

Aufgabe 9.3 Um das Maximum und das Minimum einer $n = 2^k$-elementigen Menge zu bestimmen, kann man nach dem Divide-and-Conquer Verfahren rekursiv Minima und Maxima einer Aufteilung der Menge in zwei gleich große Teilmengen bestimmen und das Ergebnis daraus zusammen setzen.

a) Gib den entsprechenden Algorithmus an.

b) Bestimme die Anzahl der Vergleiche, die der Algorithmus ausführt, um Maximum und Minimum einer $n = 2^k$-elementigen Menge zu bestimmen und zeige, daß dies besser als $2n - 2$ wie bei einer naiven Berechnung ist.

Aufgabe 9.4 Gib einen Algorithmus an, der das folgende Problem löst: Wir möchten eine DVD optimal mit einer Auswahl aus n Dateien füllen, d.h. es soll möglichst wenig Speicherplatz ungenutzt sein. Genauer:

Eingabe: Datenträgerkapazität K, Dateigrößen $g_1, \ldots, g_n$

Ausgabe: Eine Auswahl $I \subseteq [n]$ der Dateien, die den Restspeicherplatz $K - \sum_{i \in I} g_i$ minimiert

Hinweis: Verwende/Modifiziere den Knapsack-Algorithmus aus der Vorlesung am Mittwoch