Universität des Saarlandes
FR 6.2 Informatik

Prof. Dr. Kurt Mehlhorn, Dr. Konstantinos Panagiotou **WiSe 2011/2012**

Übungen zu Computational Thinking

http://www.mpi-inf.mpg.de/departments/d1/teaching/ws11/ct/

Blatt 6 Abgabeschluss: 12.12.11 16:00

Regeln: Bis zum Semesterende müssen mindestens 42% der maximal erreichbaren Punkte aller Übungszettel erworben werden.
Programmcode ist elektronisch per E-Mail abzugeben. Zusätzlich müssen die Ausgaben einer exemplarischen Programmausführung mitgeliefert werden.

Bleistiftaufgaben

Aufgabe 1 (*10 Punkte*) [Caesarchiffrierung]: Der Schlüssel ist eine Zahl $k \in \{1, \ldots, 25\}$. Bei der Chiffrierung ersetzen wir jeden Buchstaben durch seinen k-ten Nachfolger. Für $k = 3$, etwa

$$A \to D, B \to E, \ldots, X \to A, Y \to B, Z \to C.$$

a) Verschlüsseln Sie „`HIERKOMMTKURT`" mit dem Schlüssel $k = 3$.

b) Wie würden Sie versuchen, einen nach dem Caesarverfahren kodierten Text zu entschlüsseln?

c) Wie würden Sie vorgehen, wenn Sie zudem wüssten, dass ein deutscher Text verschlüsselt wurde? Hinweis: in deutschen Texten ist E der weitaus häufigste Buchstabe.

d) Entschlüsseln Sie „`FJOFTFMHFIU`". Der Klartext ist ein deutscher Text.

Aufgabe 2 (*10 Punkte*) [Baby-Version des ElGamal-Verfahrens] Spielen Sie das ElGamal-Verfahren aus der Vorlesung mit konkreten Zahlen durch: Der Empfänger wählt den privaten Faktor $p = 11$ und den öffentlichen Faktor $f = 9$. Der Sender möchte $m = 5$ senden und benutzt als geheime Zahl $s = 7$.

Aufgabe 3 (*10 Punkte*) [Binärdarstellung] Die Darstellung einer Zahl als Summe von Zweierpotenzen nennt man Binärdarstellung der Zahl. Etwa $5 = 4 + 1 = 2^2 + 2^0$ oder $21 = 16 + 4 + 1 = 2^4 + 2^2 + 2^0$.

a) Stellen Sie 63 als Summe von Zweierpotenzen dar.

b) Statt $2^4 + 2^2 + 2^0$ schreibt man auch die Binärzahl "10101". Was ist der Zusammenhang? Wie schreibt sich 63 als Binärzahl?

c) Überlegen Sie sich ein effizientes Verfahren, mit dem man jede Zahl in Binärschreibweise umwandeln kann.

Python

Aufgabe 4 (*10 Punkte*) [Berechnung von Potenzen] Wir möchten a^n berechnen, wobei a und n natürliche Zahlen sind.
Hier ist das naive Verfahren. Wir berechnen nacheinander $a^1, a^2, \ldots, a^n$, indem wir jedes Element aus dem vorhergehenden durch Multiplikation mit a berechnen.

a) Wie viele Multiplikationen brauchen Sie?

b) Schreiben Sie eine Funktion, die dieses Verfahren umsetzt.

Jetzt kommt das geschickte Verfahren: Exponentiation durch wiederholtes Quadrieren.

> Wir berechnen zunächst $p = [a^1, a^2, a^4, a^8, a^{16}, \ldots, a^K]$, indem wir jedes Element durch Quadrieren des vorhergehenden Elements erzeugen. Dabei ist $K = 2^k$ die größte Zweierpotenz kleiner gleich n.
> Dann schreiben wir die Zahl n in ihrer Binärdarstellung und multiplizieren die Potenzen von a, die Einsen in der Binärdarstellung von n entsprechen. Etwa
>
> $$a^{21} = a^{16+4+1} = a^{16}a^4a^1.$$

c) Stellen Sie a^{59} entsprechend dar.

d) Wie viele Multiplikationen brauchen Sie zur Erzeugung der Folge p?

e) Argumentieren Sie, dass man a^n mit höchstens $K - 1$ Multiplikationen aus p berechnen kann. Wie viele Multiplikationen haben Sie insgesamt gebraucht?

f) Implementieren Sie dieses Verfahren.

g) Vergleichen Sie für verschiedene n die Effizienz dieser beider Verfahren mit der in Python eingebauten Funktion `pow`.

Aufgabe 5 (*20 Punkte*) [Vigenèrechiffrierung] Diese Chiffrierung ist eine Verallgemeinerung des Caesarverfahrens. Der Schlüssel ist jetzt ein Paar von Zahlen zwischen 1 und 25, etwa $(3, 5)$. Man teilt den Klartext in Paare von Buchstaben ein und ersetzt den ersten Buchstaben im Paar durch seinen 3-ten Nachfolger und den zweiten Buchstaben im Paar durch seinen 5-ten Nachfolger. Im Beispiel wird also *DI* ersetzt durch *GN*, da *G* der dritte Nachfolger von *D* ist und *N* der fünfte Buchstabe nach *I*. Es gibt nur 25^2 Schlüssel.

a) Schreiben Sie Funktionen, die gegeben einen Schlüssel und einen Text (in dem nur Buchstaben des Alphabets vorkommen), den Text ver- bzw. entschlüsseln.

b) Wie würden Sie versuchen diesen Code zu brechen, wenn Sie wüssten, dass der Klartext ein deutscher Text ist? *Hinweis*: Der Wikipedia Artikel über Bigramme ist wahrscheinlich hilfreich.

   Schreiben Sie eine Funktion, die einen verschlüsselten deutschen Text ohne einen Schlüssel zu kennen wieder entschlüsselt.

Hilfreiche Funktionen für diese Aufgabe sind `ord` und `chr`.