Professor Dr. F. Schweiggert   Abteilung Angewandte Informationsverarbeitung   14. Dezember 2000
Johannes Mayer   Blatt 8

Allg. Informatik für WiWi (WS 2000)

Abgabetermin: 21. Dezember 2000

1 Geheimsache (15 Punkte)

Wir wollen uns ein wenig mit Kryptographie, d. h. der Verschlüsselung von Daten befassen. Eine sehr einfache Art der Verschlüsselung ist die sogenannte Cäsar-Chiffre. Hierbei werden die Buchstaben zyklisch verschoben. Die Anzahl der zyklischen Verschiebungen ist der Schlüssel, d. h. die geheime Information, mittels der die Nachricht auch wieder entschlüsselt werden kann. Haben wir als Schlüssel beispielsweise 3 gewählt, so wird aus dem Buchstaben `a` der Buchstabe `d` und so weiter und aus dem Buchstaben `z` wird der Buchstabe `c`. Man sieht also, dass als Schlüssel nur die Zahlen von 1 bis 25 sinnvoll sind, da im Falle des Schlüssels 0 der Text nicht verändert wird und alle anderen Schlüssel (d. h. Zahlen) zu einem dieser Schlüssel äquivalent sind (dies liegt daran, dass die Verschiebung zyklisch erfolgt und die Länge des Zyklus 26 ist).

(a) Schreiben Sie zunächst ein Modul `Encrypt`, das Zeichen für Zeichen von der Standardeingabe liest (solange noch ein Zeichen vorhanden ist). Falls das eingelesene Zeichen ein Buchstabe ist, soll es wie beschrieben verschlüsselt (d. h. zyklisch nach rechts verschoben) und danach ausgegeben werden. Alle anderen Zeichen sollen unverändert ausgegeben werden. Verwenden Sie für den Schlüssel eine Konstante, die Sie am Anfang der Moduldatei definieren. (10 Punkte)

(b) Schreiben Sie analog zu (a) ein Modul `Decrypt`, das die Standardeingabe entschlüsselt. Dazu müssen Sie nur eine zyklische Verschiebung in der entgegengesetzten Richtung durchführen. (2 Punkte)

(c) Sie bekommen die Datei *text.txt*, von der sie wissen, dass es sich um einen Text handelt, der mit dem hier vorgestellten Algorithmus verschlüsselt wurde. Finden Sie durch Probieren den verwendeten Schlüssel und den Originaltext heraus. (3 Punkte)
(Hinweis: Ändern Sie jeweils die Konstante in `Encrypt.om` ab und übersetzen Sie das Modul dann neu.)

P.S.: Auf dem FTP-Server befinden sich die beiden Dateien *Cat.od* und *Cat.om*, die in den Übungen vorgestellt wurden.

Viel Erfolg!