Universität Ulm - Abteilung Angewandte Informationsverarbeitung
Dr. Johannes Mayer und Hans Braxmeier, Wintersemester 2003

4. Übungsblatt zur Vorlesung Allgemeine Informatik III

Abgabetermin: Dienstag, 18.11.2003

Geheimcode Caesar-Shiffre *(3 Punkte)*

Jeder von Euch hat sicher schon von geheimen Codes gehört, mit denen sich Texte verschlüsseln lassen. Ein Beispiel ist die Caesar-Shiffre, die einfach einen Buchstaben um n Buchstaben nach rechts shifted.

```
n = 3 : Hallo => Kdoor
n = 12: Hallo => Tmxxa
```

Implementieren Sie ein Programm, mit dem die Caesar Shiffrierung durchgeführt werden kann. Dabei soll die Anzahl n ($0 \leq n \leq 25$) der Buchstaben, um die geshifted wird, als Kommandozeilenparameter übergeben werden könnnen. Die Operation soll nur bei Groß- und Kleinbuchstaben durchgeführt werden, andere Zeichen bleiben unverändert. Z und z sind Sonderfälle. Ein Shift um 1 erzeugt dabei ein A bzw. a, ein Shift um 2 ein B bzw. b usw.

Geheimcode Bit-Shift-Shiffre *(3 Punkte)*

Ein weitere Verschlüsselungsmethode ist die Bit-Shift-Shiffre. Hier werden die Bits eines jeden Bytes zyklisch um n Positionen nach rechts geshifted.

```
n = 3:
H = 72 (ASCII) = 01001000 => 00001001 = 9 (ASCII) = Horizontal Tab
a = 97 (ASCII) = 01100001 => 00101100 = 44 (ASCII) = Komma
```

Implementieren Sie auch hierzu ein Programm, welches die Anzahl n ($0 \leq n \leq 7$)der Bits, um die geshifted werden soll, als Kommondozeilenparameter erhält und eine entsprechende Bit-Shiftung ausführt.

One-Time-Tape-Shiffre *(3 Punkte)*

Lesen Sie wieder von der Kommandozeile einen Schlüssel n ($0 \leq n \leq 255$) ein. Jedes Zeichen von der Eingabe soll so verschlüsselt werden, dass die Bits im ASCII-Code des jeweils gelesenen Zeichens komplementiert werden, welche bei n gesetzt sind.

```
Schlüssel: 01101111
Zeichen A: 01000001 (ASCII-Code von A)
Ausgabe:   00101110
```

Decodieren *(1 Punkte)*

Überlegen Sie sich für jede Teilaufgabe, mit welchem Schlüssel der codierte Text decodiert werden kann.

Viel Erfolg!