Programmierpraktikum
Thema: Kryptographie
Sommersemester 2004

1. Übungsblatt

1. (*) Es wurde folgender Chiffretext abgefangen:

   `afb arbjjpqbk moldoxjjfbobo exybk afb afzhpqbk moldoxjjb`

   Es ist bekannt, dass das Caesar-Verfahren für die Verschlüsselung benutzt wurde. Es soll eine Tabelle mit den Buchstabenhäufigkeiten erstellt werden (ohne die Leerzeichen zu betrachten). Anhand der Tabelle soll eine Vermutung aufgestellt werden, welcher Schlüssel benutzt wurde und wie der dazugehörige Klartext lautet.

2. (Oliver/Philipp) Es soll folgende Funktion in Java programmiert werden:

   ```
   double[] frequency(String text)
   ```

   Als Parameter wird ein beliebig langer String übergeben. Als Rückgabewert wird ein Array mit 26 Feldern erwartet, das die Häufigkeiten der einzelnen Buchstaben als double Wert speichert (gerundet auf zwei Stellen nach dem Komma).
   Der Algorithmus soll nur die kleinen Buchstaben $a, b, \ldots, z$ zählen. Diese entsprechen den ASCII-Werten $97, 98, \ldots, 122$. Großbuchstaben sowie alle anderen Zeichen sollen ignoriert werden.

3. (Alex/Oleg/Yves)

   (a) Passend zu Aufgabe 2 soll eine Funktion geschrieben werden, die die Häufigkeiten graphisch darstellt:

   ```
   void drawFrequency(double[] frequencies)
   ```

   Ein kleines Popup soll die Häufigkeiten der Buchstaben a bis z in einem Diagramm anzeigen. Ein Beispiel für die Darstellung der Buchstabenhäufigkeiten findet man auf der Rückseite des Übungsblatts.

   (b) Zusätzlich soll eine Standardfunktion

   ```
   void drawStandardFrequency()
   ```

   programmiert werden, die die charakteristischen Häufigkeiten im Deutschen genau wie in Aufgabe (a) darstellt. Dazu benutzt man die Tabelle auf der Rückseite des Übungsblatts.

4. (Andreas/Claudia/Isabel) Integriert den CBC-Mode in den CryptoChatClient.

5. (David/Pavel/Tim) Überprüft den ChatClient auf alle bisherigen Features. Dies beinhaltet:
    - Anmelden beim Server
    - Verwalten der Buddyliste
    - Verwalten der Schlüsselliste, sowohl für private- (lokal) als auch public-key-Verfahren (auf dem Server)
    - Verschicken von Nachrichten mit allen vorhandenen Kryptosystemen
    - Integration von digitalen Signaturen in Nachrichten

Zeitfenster: bis Freitag, 21.5.2004

Buchstabe	**Häufigkeit**	**Buchstabe**	**Häufigkeit**
a	6.51%	n	9.78%
b	1.89%	o	2.51%
c	3.06%	p	0.79%
d	5.08%	q	0.02%
e	17.40%	r	7.00%
f	1.66%	s	7.27%
g	3.01%	t	6.15%
h	4.76%	u	4.35%
i	7.55%	v	0.67%
j	0.27%	w	1.89%
k	1.21%	x	0.03%
l	3.44%	y	0.04%
m	2.53%	z	1.13%

Tabelle 1: Charakteristische Buchstabenhäufigkeit im Deutschen

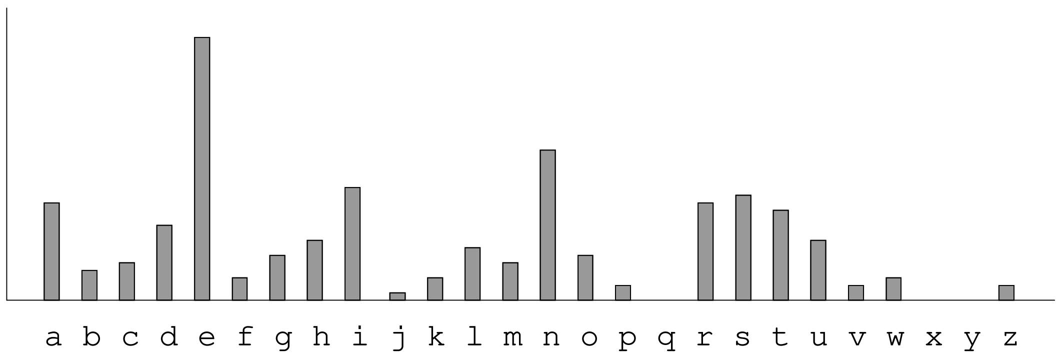

Abbildung 1: Häufigkeitsgebirge im Deutschen