Aufgabe 3.6: Vigenère-Chiffre

Beschreibung

Man kann einen Text zum Beispiel dadurch verschlüsseln, dass man jeden Buchstaben um eine feste Anzahl von Stellen im Alphabet verschiebt. Dabei fängt man nach dem Ende 'Z' wieder am Anfang 'A' an. In der deutschen Sprache ergeben sich zwei Schwierigkeiten:

1. Umlaute: ä, ö, ü, sowie das ß
2. Groß- und Kleinschreibung

Daher wird ein Text vor dem Verschlüsseln transformiert indem Umlaute und 'ß' ersetzt werden und alle Groß- in Kleinbuchstaben gewandelt werden.

Das Problem mit dieser Art von Verschlüsselung ist, dass die Buchstabenhäufigkeiten einer Sprache nicht verändert werden. Daher geht die Vigenère-Chiffre einer Schritt weiter und betrachtet *alle* möglichen Verschiebungen gleichzeitig. Es gibt genauso viele Verschiebungen wie Buchstaben des Alphabets. Diese möglichen Verschiebungen werden in einer Matrix angeordnet. Die Auswahl der jeweiligen Verschiebung erfolgt durch ein Schlüsselwort. Für jeden Buchstaben des Textes wird der entsprechende Buchstabe des Schlüsselwortes verwendet, um die Verschiebung zu bestimmen. Dabei entspricht dieser Buchstabe dem Buchstaben 'a' und damit der entsprechenden Zeile der Matrix. Nachdem genauso viele Buchstaben des Textes verschlüsselt wurden wie das Schlüsselwort enthält, fängt man für den nächsten Buchstaben des Textes wieder mit dem ersten Buchstaben des Schlüsselwortes an. Ist t_i der i-te Buchstabe des Textes und s_j der j-te Buchstabe des Schlüsselwortes, welcher zur Verschlüsselung verwendet wird, so ist $j = ((i-1) \mod n) + 1$, wobei n die Länge des Schlüsselwortes ist.

Aufgabenstellung

Schreiben Sie ein Programm, welches Texte mit der Vigenère-Chiffre ver- und entschlüsselt. Speichern Sie den verschlüsselten Text in Gruppen à 5 Buchstaben, wobei die Gruppen durch Leerzeichen getrennt werden.

Testprogramme

1. (a) Verschlüsseln Sie den Text in "Gedicht.txt" mit dem Schlüsselwort "scheune".
   (b) Entschlüsseln Sie den verschlüsselten Text mit dem Schlüsselwort "scheune".
2. (a) Verschlüsseln Sie den Text in "Gedicht.txt" mit einem Schlüsselwort mit wenigen, mit einem Schlüsselwort mit vielen verschiedenen Buchstaben, und dem in den Hinweisen beschriebenen Pangramm.
   (b) Entschlüsseln Sie den verschlüsselten Text mit dem gewählten Schlüsselwort.

Eingabe
Art: Chiffrierung oder Dechiffrierung; Schlüsselwort; Dateinamen für Klartext und Geheimtext

Ausgabe
Chiffrier- und Dechiffriertabelle; Chiffrierter bzw. Dechiffrierter Text; Ausgabe in Datei und auf dem Bildschirm

Abbruch
Das Programm bricht nach der Ausführung ab.

Hinweise

Bemerkungen

- Das Verfahren funktioniert nur mit Buchstaben-basierten Sprachen.
- Groß-/Klein-Schreibung, Sonderzeichen, diakritische Zeichen, Satzzeichen und Zahlen bereiten große Schwierigkeiten.
- Die Stärke der Verschlüsselung hängt sehr stark vom Schlüsselwort ab. Je mehr *verschiedene* Buchstaben das Schlüsselwort hat, desto besser der Schlüssel.
  - Gut: Pangramme, das sind Sätze, die jeden Buchstaben mindestens einmal, aber nicht zu häufig enthalten. Zum Beispiel: "the big brown fox jumps over the lazy dog" (Leerzeichen werden zur Kodierung ignoriert)
  - Schlecht: Mississippi. Anzahl Buchstaben: 11; Anzahl *verschiedener* Buchstaben: 4.
- Andere als die oben angegebenen Sonderzeichen werden nicht verschlüsselt – insbesondere Leerzeichen und Zahlen. Dies erlaubt es, Rückschlüsse von dem chiffrierten Text auf den Originaltext zu ziehen.

Chiffrierung Von Hand wird chiffriert, indem alle Alphabete jeweils um einen Buchstaben verschoben untereinander geschrieben werden.

```
abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyza
cdefghijklmnopqrstuvwxyzab
defghijklmnopqrstuvwxyzabc
...
zabcdefghijklmnopqrstuvwxy
```

Verschlüsselung von "polyalphabetisch" mit "scheune":

```
Schlüssel:            scheunescheunesc
Klartext:             polyalphabetisch
Verschlüsselter Text: hqscuatzciinvwuj
```

Soll per Computer verschlüsselt werden, so ist es am günstigsten, die zugehörige Tabelle zu erzeugen und dann den Text zu verschlüsseln.

Dechiffrierung Ist das Schlüsselwort bekannt, kann obige Tabelle genutzt werden, um den Geheimtext zu dechiffrieren.