Monoalphabetische Verschlüsselung

Eine Schwachstelle bei der Konstruktion der Cäsar-Verschlüsselung ist die geringe Anzahl möglicher Schlüssel, da nur 26 Drehungen der Scheibe möglich sind.

Verbesserung: Wenn man die Buchstaben auf der inneren Scheibe willkürlich (nicht nach dem Alphabet) anordnet, bekommt man viel mehr Möglichkeiten. Jedem Buchstaben wird dann willkürlich ein anderer Buchstabe zugeordnet. Dies bezeichnet man als **monoalphabetische Verschlüsselung**. Der Empfänger muss diese Reihenfolge der Buchstaben natürlich kennen.

Aufgaben:

1. *Schreibe auf die innere Scheibe unter die aufgedruckten Buchstaben eine weitere Reihe Buchstaben. Verwende dabei jeden Buchstaben genau einmal. Dein Briefpartner muss genau die Buchstaben in der gleichen Reihenfolge auf seine Scheibe schreiben.*
2. *Schreibe an deinen Partner eine kurze verschlüsselte Nachricht.*
3. *Entschlüssele die Nachricht deines Partners.*
4. *Beschreibe, was bei diesem Verfahren der Schlüssel ist.*
5. *(*) Wie viele verschiedene Schlüssel sind möglich?*

Brechen der Verschlüsselung

Es ist nicht mehr möglich, alle Schlüssel durchzuprobieren (Brute Force-Verfahren).

6. *Begründe, warum die Häufigkeitsanalyse immer noch eine Angriffsmöglichkeit bietet.*
7. *Der folgende Kryptotext soll von dir entschlüsselt werden. Da es sehr viel Arbeit ist, die Buchstaben auszuzählen, macht dies das Programm BreakMono.jar für dich.*

VCS YPAPKFTUKESZCBNUS BIEBZCZIZCPA CBZ SCAS DSQESBBSQIAG VSB NKSBKQ-KFGPQCZUYIB, VK SB YSUQ YPSGFCNUS BNUFISBBSF GCEZ. FSCVSQ HKAA YKA YCZ VSQ UKSIMCGHSCZBKAKFWBS CYYSQ APNU VSA HFKQZSJZ SQYCZZSFA. YKA UKZ KESQ KINU UCSQMISQ XSCZSQSAZXCNHFIAGSA, VCS VI HSAASAFSQABZ, XSAA VI XSCZSQ CAMPQYKZCH CA VSQ BNUIFS YKNUBZ. SB GCEZ R.E. VCS DCGSASQS-DSQBNUFISBBSFIAG, VKB KIZPHSW-DSQMKUQSA PVSQ VKB PAS-ZCYS TKV. VKB FSZRZS DSQMKUQSA CBZ RXKQ IATQKHZCBNU, KESQ ECSZSZ TSQMSHZS BCNUSQUSCZ. SB XIQVS R.E. MISQ VCS KEBCNUSQIAG VSQ HPYYIACHKZCPA RXCBNUSA KYSQCHKACBNUSA TQKSBCVSAZSA IAV QIBBCBNUSA TQKSBCVSAZSA DSQXSAVSZ.

Starte das Programm, füge den Text per Copy-Paste aus der Datei kryptotext.txt in das obere Textfeld ein. Lasse dir die Buchstabenhäufigkeit bestimmen. Zusätzlich kannst du noch die Häufigkeit von Bigrammen (zwei aufeinanderfolgende Buchstaben) und Doppelbuchstaben (zweimal der gleiche Buchstabe) zählen lassen.

Versuche zu ermitteln, welcher Buchstabe das E sein könnte und trage das E unter diesem Buchstaben ein.

Versuche mit Hilfe der Häufigkeiten weitere Buchstaben herauszufinden.

Sobald du einige Buchstaben ermittelt hast, versuche im entschlüsselten Text Wörter zu erkennen, die dir Hinweise auf weitere Buchstaben liefern.