Die Vigenère-Verschlüsselung

Übersicht

Substitution

monoalphabetisch polyalphabetisch

Cäsar Polybius Vigenère

Geheime Botschaften S.65-66 lesen lassen.

Die Vigenère-Verschlüsselung

Ein Substitutionsverfahren heißt **polyalphabetisch**, wenn beim Verschlüsseln des Klartextes das Geheimalphabet gewechselt wird (poly: viel).

Die **Vigenère-Verschlüsselung** ist ein polyalphabetisches Substitutionsverfahren, bei dem alle 26 Cäsar-Alphabete verwendet werden können. Welches der Alphabete wann genutzt wird, legt ein Schlüsselwort fest, im Beispiel ist es WORT:

Schlüssel	W	O	R	T	W	O
Klartext	A	N	A	N	A	S
Geheimtext						

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	Klartextalphabet
B	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	
C	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	
E	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	
F	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	
G	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	
H	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	
I	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	
L	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	
M	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	Geheimalphabet O
P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	
R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	Geheimalphabet R
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	
T	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	Geheimalphabet T
U	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	
V	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	
W	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	Geheimalphabet W
X	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	
Y	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	
Z	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	

1. Partnerarbeit: Jeder verschlüsselt einen der folgenden Texte. Im Anschluss entschlüsselt jeder den Text des Partners. Wenn ihr alles richtig gemacht habt, könnt ihr die Botschaft lesen.

   Schlüsselwort: **G E H E I M**
   Klartext: **T R I T H E M I U S U N D V I G E N E R E**

   Geheimtext: _____

   Schlüsselwort: **W O R T**

   Geheimtext: _____

   Klartext: _____

Die Vigenère-Verschlüsselung

Ein Substitutionsverfahren heißt **polyalphabetisch**, wenn beim Verschlüsseln des Klartextes das Geheimalphabet gewechselt wird (poly = viel).

Die **Vigenère-Verschlüsselung** ist ein polyalphabetisches Substitutionsverfahren, bei dem alle 26 Cäsar-Alphabete verwendet werden können. Welches der Alphabete wann genutzt wird, legt ein Schlüsselwort fest, im Beispiel ist es WORT:

Schlüssel	W	O	R	T	W	O
Klartext	A	N	A	N	A	S
Geheimtext						

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	Klartextalphabet
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A	
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B	
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C	
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D	
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E	
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F	
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G	
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H	
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I	
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J	
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K	
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L	
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M	
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N	Geheimalphabet O
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O	
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P	
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q	Geheimalphabet R
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R	
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S	Geheimalphabet T
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T	
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U	
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V	Geheimalphabet W
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W	
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X	
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y	

1. Partnerarbeit: Jeder verschlüsselt einen der folgenden Texte. Im Anschluss entschlüsselt jeder den Text des Partners. Wenn ihr alles richtig gemacht habt, könnt ihr die Botschaft lesen.

   Schlüsselwort: **W O R T**
   Klartext: **D A S I S T D E R K L A R T E X T**

   Geheimtext: _____

   Schlüsselwort: **G E H E I M**

   Geheimtext: _____

   Klartext: _____

Die Vigenère-Verschlüsselung

Gruppenarbeit (3 Personen pro Gruppe)

2. Die Entschlüsselung eines Textes bei bekanntem Schlüsselwort mit diesem Verfahren soll entworfen, als Struktogramm dargestellt und am Rechner implementiert werden.

   Entscheidet in der Gruppe, wie viele Hilfestellungen ihr braucht (am Lehrertisch holen).

   für schnelle Gruppen: Implementiert auch die Verschlüsselung.

```
K R E I S _____________________________________
O Z R M Y O Y I Q E C L T Z A PKMALOZRMKMYVQXDUMMYOYIQESJX
_____________________________________________________________
```

Als Lösungen liegen das Struktogramm und der Python-Quelltext bereit. Es gibt aber auch mehrstufige Hilfestellungen um selbst zum Ergebnis zu kommen. Entscheidet selbst.

Hilfestellung 1: Gehe die folgenden Schritte:

a. Hänge das Schlüsselwort so oft aneinander, dass die Anzahl der Schlüsselbuchstaben mindestens gleich der Anzahl der Zeichen im Geheimtext ist.
   Beobachte deine Vorgehensweise, notiere die einzelnen Schritte und formuliere die dazugehörigen Anweisungen. Beachte, wenn sich Schritte wiederholen, und wähle eine geeignete Schleifenart aus.
   Hole dir bei Schwierigkeiten die Hilfestellung 2a).
   Vergleiche mit Lösung 2a).
b. Entschlüssele das erste Geheimzeichen mit der folgenden Methode und überprüfe das Ergebnis mithilfe der Tabelle.
   - Notiere zum Schlüsselbuchstaben die Verschiebungszahl, welche die Cäsar-Verschlüsselungsmethode braucht.
   - Notiere den Funktionsaufruf
   - Verwende die Funktion `decaesar()` deines Python-Programms. (Der dort übergebene Geheimtext darf auch nur ein Zeichen enthalten.)
   - (Zu jedem Schlüsselbuchstaben gehört genau eine Zahl. - ASCII)

   Wiederhole den Schritt für alle Zeichen des Textes.

Hilfestellung 2a

KREISKREISKREISKREISKREISKREISKREISKREISKREIS
OZRMYOYIQECLTZAPKMALOZRMKMYVQXDUMMYOYIQESJX

Beschreibung der Vorgehensweise:

- Die Zeichenkette **schluesseltext** besteht zu Beginn nur aus der Zeichenkette **schlüsselwort**.
- Folgendes wird wiederholt:
  - An die Zeichenkette **schlüsseltext** wird die Zeichenkette **schlüsselwort** angehängt.

  Bedingung für die Wiederholung: Die Zeichenkette **schlüsseltext** soll zum Schluss nicht mehr kürzer als die Zeichenkette **geheimtext** sein.

Wiederholung:
Es gibt zwei Arten von Schleifen:

- Zählschleife `for i in range(0,10):`
- bedingte Schleife
  - vorprüfende Schleife
    ```
    while i<10:
      i=i+1
    ```
  - nachprüfende Schleife nicht in Python

Lösung 2a:
Dazugehörige Anweisungen in Python:

- Die Zeichenkette **schluesseltext** besteht zu Beginn nur aus der Zeichenkette **schlüsselwort**. → **schluesseltext** = **schluesselwort**
- Folgendes wird wiederholt:
  - An die Zeichenkette **schlüsseltext** wird die Zeichenkette **schlüsselwort** angehängt. → **schluesseltext** = **schluesseltext** + **schluesselwort**

  Bedingung für die Wiederholung: Die Zeichenkette **schlüsseltext** soll zum Schluss nicht mehr kürzer als die Zeichenkette **geheimtext** sein.
- Schleifenart: Schleife mit Bedingung - `while len(geheimtext)<len(geheimtext):`

Hilfestellung 2b

10 17 4 8 18 …
K R E I S …
O Z R M Y …

… KREISKREISKREISKREISKREISKREISKREISKREISKREIS
… OYIQECLTZAPKMALOZRMKMYVQXDUMMYOYIQESJX

- Verschiebungszahl für K: 10
-

Hilfestellungen 2c - grob

Entschlüssle den Text und beobachte deine Vorgehensweise.

Lege die Signatur der Funktion fest.

Beschreibe deine Vorgehensweise beim Entschlüsseln. Welche strukturierten Anweisungen brauchst du? Stelle deine Vorgehensweise mithilfe eines Struktogramms dar.

Implementiere die Funktion und teste sie.

Hilfestellungen 2c - detaillierter

Hilfestellung zur Festlegung der Signatur der Funktion: Überlegt, welche Informationen ihr bekommen habt.

Hilfestellung zum Entwurf der Schleifen:

- Als ersten Schritt ist es sinnvoll, die Zeile mit den Schlüsselwörtern zu vervollständigen. Formuliere eine Bedingung, an der das Programm erkennt, wann Schlüsselwort oft genug kopiert worden ist.
- Formuliere Anweisungen, mit denen aus dem Schlüsselwort eine Schlüsselkette erzeugt werden kann.

```
KREISKREISKREISKREISKREISKREISKREISKREISKREIS
__________________________________________
OZRMYOYIQECLTZAPKMALOZRMKMYVQXDUMMYOYIQESJX
______________________________________________
```

- Nimm das erste Geheimzeichen.
- Notiere zum Schlüsselbuchstaben die Verschiebungszahl, welche die Cäsar-Verschlüsselungsmethode braucht (Zu jedem Schlüsselbuchstaben gehört genau eine Zahl. - ASCII) und den Funktionsaufruf zur Ermittlung der Verschiebungszahl.
- Verwende die Funktion deCaesar() deines Python-Programms. (Der dort übergebene Geheimtext darf auch nur ein Zeichen enthalten.) Notiere den dazugehörigen Funktionsaufruf.
- Wiederhole den Schritt für alle Zeichen des Textes.
- Implementiere die Funktion und teste sie.

Hinweise zu c – sehr detailliert:

- Zwei Schleifen müssen im Struktogramm enthalten sein.
- Die Bedingungen orientieren sich an der Länge des Geheimtextes.

```
Algorithmus devigenere(geheimtext, schluessel)
geheimtext in Großbuchstaben umwandeln
schluessel in Großbuchstaben umwandeln
klartext leer anlegen
schluesselkette leer anlegen
schluesselkette kürzer als geheimtext
    schluessel an schluesselkette anhängen
i=0, i<Länge von geheimtext
    szeichen = schluesselkette an Stelle i
    verschiebung = (ASCII von szeichen) - 65
    kzeichen = decaesar(geheimtext[i], verschiebung)
    kzeichen an ktext anhängen
klartext in Kleinbuchstaben umwandeln
Rückgabe: klartext
```

```
Algorithmus devigenere(geheimtext, schluessel)
geheimtext in Großbuchstaben umwandeln
schluessel in Großbuchstaben umwandeln
klartext leer anlegen
schluesselkette leer anlegen
schluesselkette kürzer als geheimtext
    ...
i=0, i<Länge von geheimtext
    ...
klartext in Kleinbuchstaben umwandeln
Rückgabe: klartext
```

```
Algorithmus devigenere(geheimtext, schluessel)
geheimtext in Großbuchstaben umwandeln
schluessel in Großbuchstaben umwandeln
klartext leer anlegen
schluesselkette leer anlegen
schluesselkette kürzer als geheimtext
    schluessel an schluesselkette anhängen
i=0, i<Länge von geheimtext
    szeichen = schluesselkette an Stelle i
    verschiebung = (ASCII von szeichen) - 65
    kzeichen = decaesar(geheimtext[i], verschiebung)
    kzeichen an ktext anhängen
klartext in Kleinbuchstaben umwandeln
Rückgabe: klartext
```

```
Algorithmus devigenere(geheimtext, schluessel)
geheimtext in Großbuchstaben umwandeln
schluessel in Großbuchstaben umwandeln
klartext leer anlegen
schluesselkette leer anlegen
schluesselkette kürzer als geheimtext
    ...
i=0, i<Länge von geheimtext
    ...
klartext in Kleinbuchstaben umwandeln
Rückgabe: klartext
```