INFORMATIONEN ZUM SCHLEPPNETZ-CHIFFRIERVERFAHREN

Das dir bekannte *Vigenére-Chiffrierverfahren*, welches zu der Gruppe der *polyalphabetischen Chiffren* gehört, ist bereits ein sehr effektives Verfahren. Im Gegensatz zu den *monoalphabetischen Chiffren* ist das Knacken des Codes nicht über die Buchstabenhäufigkeit zu realisieren, da ein und der selbe Buchstabe stets unterschiedliche verschlüsselt wird. Dennoch birgt Vigenére Gefahren. Da sich das Schlüsselwort stets wiederholt ist der Code so gut wie geknackt, wenn die Länge des Schlüsselwortes bekannt ist. Ist die Schlüsselwortlänge z. B. 7, so weiß man, dass jeder siebte Buchstabe gleich verschlüsselt wurde. Fasst man nun die Folge der Buchstaben 1, 8, 15, 22, ... und die der Buchstaben 2, 9, 16, 23, ...usw. als einen Text auf, so kann man genau wie bei den monoalphabetischen Chiffren mit Hilfe der Buchstabenhäufigkeiten an den Schlüssel für jede Buchstabenfolge und somit auch zum Schlüsselwort gelangen.
Eine Verbesserung des Vigenére-Verfahrens muss also die ständige Wiederholung des Schlüsselwortes unterbinden. Dies tut das sogenannte ***Schleppnetz-Chifffierverfahren***. Der Trick ist der, dass man das Schlüsselwort nur einmal über den Klartext schreibt und anschließend mit dem Klartext als Schlüsselwort weiterarbeitet. Das Dechiffrieren ist deshalb möglich, da man mit Hilfe des Schlüsselwortes den Anfang des Klartextes und somit auch die Fortsetzung des Schlüsselwortes dechiffriert. Die Grundlage bleibt dabei das *Vigenère-Quadrat*:

Klartextalphabet	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
Geheimtextalphabete	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 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 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 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 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 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

Ein Beispiel: Das Schlüsselwort heißt wiederum HEFEZOPF, wird diesmal aber nicht wiederholt, sondern um den Klartext ergänzt. Die Chiffrierung erfolgt ansonsten wie beim Vigenére-Chiffrierverfahren.

Schlüsselwort	H	E	F	E	Z	O	P	F	B	A	C	K	E	B	A	C
Klartext	B	A	C	K	E	B	A	C	K	E	K	U	C	H	E	N
Geheimtext	I	E	H	O	D	P	P	H	L	E	M	E	G	I	E	P

Wird nun dechiffriert, so fängt man erst mal mit dem Schlüsselwort an und fügt dann nacheinander den Klartext an das Schlüsselwort hinten dran: Nach dem Dechiffrieren des 11. Buchstabens hat man folgende Situation (der kursiv gedruckte Klartext wurde bereits an das Schlüsselwort hinten angehängt):

Schlüsselwort	H	E	F	E	Z	O	P	F	B	A	C					
Geheimtext	I	E	H	O	D	P	P	H	L	E	M	E	G	I	E	P
Klartext	*B*	*A*	*C*	K	E	B	A	C	K	E	K					

AUFGABEN ZUM SCHLEPPNETZ-CHIFFRIERVERFAHREN

Aufgabe 1: Verschlüssle den Text „DAS SCHLEPPNETZ CHIFFRE IST GUT“ mit Hilfe des Schleppnetz-Chiffrierverfahrens. Verwende einmal das Schlüsselwort „TOR“ und einmal das Schlüsselwort „INFORMATIK“.
Hinweis: Bei der Verlängerung des Schlüsselwortes durch den Klartext ist darauf zu achten, dass sämtliche Sonderzeichen (Leerzeichen, Satzzeichen, Zahlen, etc,) im Klartext als Buchstabe ‚A’ in das Schlüsselwort eingehen. Der vollständige Schlüssel beim Schlüsselwort „TOR“ lautet dann wie folgt: „TORDASASCHLEPPNETZACHIFFREAISTA“

Wollen wir das Verfahren implementieren, so brauchen wir die Möglichkeit, in einer Textdatei beliebig hin- und herzuspringen. Schließlich müssen wir beim Chiffrieren a) den aktuellen Buchstaben lesen und b) diesen mit Hilfe eines anderen Buchstabens aus dem Klartext chiffrieren. Dafür bietet DELPHI den Befehl `Seek` an, der die Filemarke an eine bestimmte Stelle der Datei setzt. So setzt z. B. der Befehl `Seek(Dateivariable, 8)` die Filemarke auf den neunten (!) Buchstaben der Textdatei, da die Nummerierung mit 0 beginnt.
Schaue dir exemplarisch die Funktion zum Codieren eines einzelnen Zeichens mit Hilfe des Schleppnetzverfahrens an:

```
function Schleppnetz_Codieren_c(c: char; sw: string; Position: integer;
                                var Klar_Datei: TTextdatei): char;
var key: char;
begin
  if Position <= length(sw)
    then key:= sw[Position]
    else begin
           Seek(Klar_Datei, Position - Length(sw)-1);
           Read(Klar_Datei,key);
           key:= upcase(key);
           if (key<'A') or (key>'Z') then key:= 'A';
           Seek(Klar_Datei, Position);
         end;
  Schleppnetz_Codieren_c:= Caesar_Codieren_c(c,key);
end;
```

Im Interface-Teil muss nun noch die Typdeklaration des Typs TTextdatei erfolgen. Diese sieht wie folgt aus:

```
type TSchluesselwortTabelle = array[0..25] of Char; { hatten wir schon }
     TTextdatei= file of char; { ist das gleiche wie Textfile }
```

Die folgenden Funktionen/Prozeduren solltest du selbst hinbekommen:

```
function Schleppnetz_DeCodieren_c(c: char; sw: string; Position: integer;
                                  var Klar_Datei: TTextdatei): char;
procedure Schleppnetz_Codieren_file(eingabe, ausgabe: string; sw: string);
procedure Schleppnetz_Decodieren_file(eingabe, ausgabe: string; sw: string);
```

Aufgabe 2: Implementiere dieses Verfahren in deinem Chiffrierprogramm! Teste es anschließend mit den obigen Beispielen aus Aufgabe 1.
Hinweis: Die File-Routinen kannst du fast unverändert vom Vigenére-Verfahren übernehmen.