Übungsaufgaben HP Übung 10 Strings

Aufgabe 10.1

Die ***Caesar-Verschlüsselung*** (auch als Cäsar-Chiffre, Cäsar-Algorithmus, Caesar-Verschiebung, Verschiebechiffre oder als Einfacher Caesar bezeichnet) ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert.

Als eines der einfachsten und unsichersten Verfahren dient es heute hauptsächlich dazu, Grundprinzipien der Kryptologie anschaulich darzustellen.

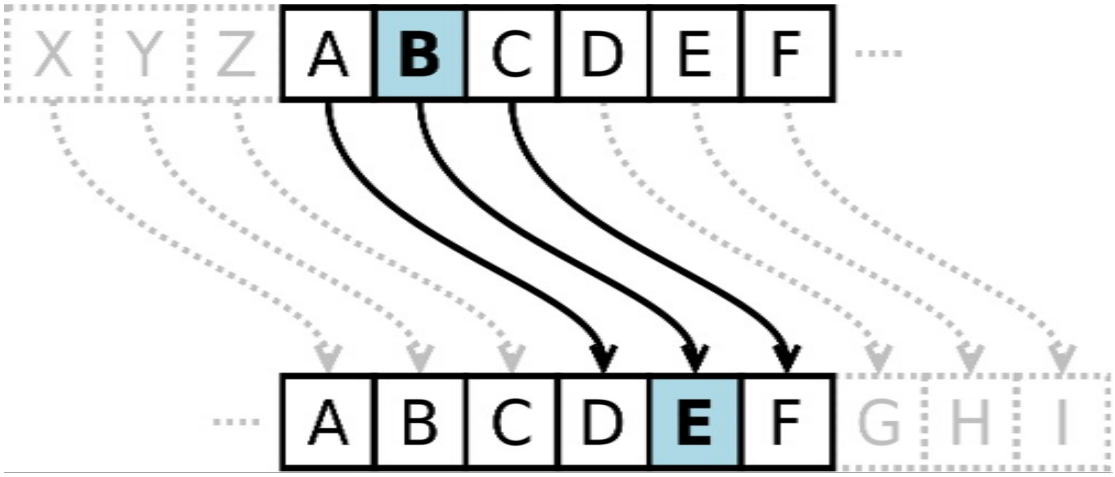
Bei der Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Geheimtextbuchstaben abgebildet. Diese Abbildung ergibt sich, indem man die Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch nach rechts verschiebt (rotiert); zyklisch bedeutet, dass man beim Verschieben über Z hinaus wieder bei A anfangend weiterzählt.

Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt.

Beispiel für eine Verschiebung um drei Zeichen:

Klar: 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

Geheim: 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



Schreiben Sie ein Programm ***caesar***. Dieses Programm soll vom Benutzer einen Schlüssel (integer) und einen zu verschlüsselnden Text (string) abfragen und anschließend den verschlüsselten Text ausgeben.

Aufgabe 10.2

Ändern Sie das Programm ***kegel3*** aus der Übung 7.1 so ab, dass die Kegelparameter als Eingabeparameter im Terminal eingegeben werden können.