

Codeknacker

Um Informationen vor unbefugtem Zugriff zu schützen, werden sie zur Übertragung oft verschlüsselt. Beim Vigenère-Verfahren (das schon im 16. Jahrhundert benutzt wurde) wird ein Passwort verwendet, das aus mehreren Zeichen besteht. Klartext und Passwort enthalten dabei nur Großbuchstaben (aber keine Umlaute) und Leerzeichen. Das Leerzeichen wird als 27. Zeichen des Alphabets nach dem **Z** eingeordnet. Jedes Zeichen des Klartextes wird mit dem entsprechenden Zeichen des Passwortes verschlüsselt, indem es im Alphabet um so viele Stellen verschoben wird, wie es der Nummer des Zeichens im Passwort entspricht. Ein **A** im Passwort bedeutet dabei eine Verschiebung um 0 Zeichen, ein **B** um ein Zeichen usw. Ergibt sich ein Zeichen, das nach dem Leerzeichen käme, geht es wieder bei **A** los. Hat der Klartext mehr Zeichen als das Passwort, beginnt man wieder mit dem ersten Zeichen des Passwortes. Das Passwort soll nicht länger sein als fünf Zeichen.

Der Klartext „**EIN GANZ GEHEIMER TEXT**“ wird mit dem Passwort „**BERT**“ folgendermaßen verschlüsselt:

Klartext: **EIN GANZ GEHEIMER TEXT**

Passwort: **BERTBERTBERTBERTBE**

Geheimtext: **FMDSHEDRAKV FMCXSDJXYX**

Aufgaben:

- a) Begründen Sie die Verschlüsselung des ersten, dritten und zwölften Zeichens (Leerzeichen im Geheimtext) in dem angegebenen Beispiel. 3 Punkte
- b) Entwickeln Sie eine Computerlösung, mit der ein Klartext und ein Passwort eingegeben werden können und die den Geheimtext erzeugt und ausgibt. 3 Punkte

Zum „Knacken“ eines Geheimtextes (wenn also ein Unbefugter, der das Passwort nicht kennt, trotzdem den Klartext herauskriegen will) gibt es verschiedene Verfahren, darunter den sogenannten Brute-Force-Angriff. Dazu werden alle möglichen Passwörter gebildet und auf den Geheimtext angewendet. Wir wollen zur Vereinfachung davon ausgehen, dass die Länge des Passwortes bekannt ist.

- c) Entwickeln Sie eine Computerlösung, die alle möglichen Passwörter einer gegebenen Länge (maximal 5) erzeugt. 3 Punkte
- d) Wenn man alle Passwörter auf einen Geheimtext anwendet, entstehen natürlich sehr viele potenzielle Klartexte, von denen nur einer dem Original entspricht. Beschreiben Sie zwei verschiedene Möglichkeiten, mit der automatisiert Kandidaten für den originalen Klartext ermittelt werden können. 2 Punkte
- e) Setzen Sie ein Verfahren aus Aufgabe d) in eine Computerlösung um und versuchen Sie damit, die Geheimtexte aus der Vorgabedatei 24L31.txt zu entschlüsseln. 4 Punkte