MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Dr. W. Spann, G. Kleen

SS 2023

Programmieren I für Studierende der Mathematik

Aufgabe 8

Die Vigenère-Verschlüsselung ist ein einfaches Chiffrierverfahren, bei dem periodisch an Hand eines Schlüsselworts zeichenweise eine zyklische Verschiebung des Klartexts vorgenommen wird. Im Klartext, Geheimtext und Schlüssel werden nur Großbuchstaben verwendet. Den Buchstaben im Schlüssel entsprechen folgende zyklische Verschiebungen: A$\widehat{=}$0, B$\widehat{=}$1,..., Z$\widehat{=}$25.

Beispiel: Schlüsselwort `ABC`

`TEXTZEILEN`	Klartext
`ABCABCABCA`	Schlüssel - periodisch wiederholt
`TFZTAGIMGN`	Geheimtext

(a) Erstellen Sie ein Programm, das einen Schlüssel und einen Eingabetext im Hauptprogramm einliest. Verschlüsseln sie in einer Funktion `encrypt` den eingegeben Text mit dem beschriebenen Verfahren und geben Sie das verschlüsselten Text im Hauptprogramm aus. Übergeben Sie den Schlüssel und den verschlüsselten Text zudem, zur Kontrolle, an eine Funktion `decrypt`. Dort soll der Text wieder entschlüsselt werden und das Ergebnis ebenfalls im Hauptprogramm ausgegeben werden.

(b) Um Texte, die mit diesem Verfahren verschlüsselt wurden, ohne Kenntnis des Schlüssels zu entschlüsseln (*Kryptoanalyse*) ist es wiederum zielführend zunächst die Länge des verwendeten Schlüssels zu bestimmen. Hierfür ist es zielführend im Geheimtext nach gleichen Substrings einer beliebigen aber festen Länge zu suchen und deren Positionen zu bestimmen.

Beispiel: Schlüsselwort `ABCD`

`DIESERTEXTBLEIBTNICHTLANGEGEHEIMWEILDIEVIGENERE`	Klartext
`VERSCHLUESSELUNGKEINSICHERESVERFAHRENIST`	Klartext fortgesetzt
`DJGVESVHXUDOEJDWNJEKTMCQGFIHHFKPWFKODJGYIHGQESG`	Geheimtext
`YESUFHMWHSTGOUOINEJPVIDJHRFUYESHDHSGQITV`	Geheimtext fortgesetzt

Erstellen Sie ein anderes Programm, das einen Geheimtext einliest und für alle Substrings der Länge drei alle Positionen der jeweiligen Vorkommen bestimmt. Betrachten Sie im Folgenden den Substring, der am häufigsten vorkommt. Geben Sie für diesen jeweils für jedes Vorkommen den Abstand zu allen darauf folgenden Vorkommen aus.

Führen Sie ihr Programm mit der bereitgestellten Datei `ciphertext.txt` aus. Können Sie einen Aussage über die Länge des verwendeten Schlüssels treffen?

Bearbeitungszeitraum: bis Freitag, 30.6.2023, 12^{00}