TECHNISCHE UNIVERSITÄT
CHEMNITZ

Belegaufgabe Grundlagen Informatik I und Informatik I
für das WS 2019/20

Cäsar-Chiffre

Die Cäsar-Chiffre ist ein Verschlüsselungsverfahren, das auf dem Austausch von Buchstaben basiert.

Der Algorithmus

Bei der Verschlüsselung wird jedes Zeichen des Klartexts auf ein Geheimtextzeichen abgebildet. Diese Abbildung ergibt sich, indem man die Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch verschiebt. Zyklisch bedeutet, dass beim Verschieben über das letzte Zeichen hinaus wieder beim ersten Zeichen begonnen wird. Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt. Beispiel für eine Verschiebung um vier Zeichen: a wird zu e, b wird zu f, c wird zu g und so fort.

Die Daten

Für die Bearbeitung des Beleges bekommen Sie eine Programmvorlage, die das Einlesen eines Textes bereits vollständig beinhaltet. Außerden steht eine Textdatei mit einem verschlüselten Text zum Test Ihres Programms zum Download bereit. Beide Dateien müssen im selben Ordner abgelegt sein.

Die Berechnung

Schreiben Sie ein C++ Programm, das einen mittels Cäsar-Chiffre verschlüsselten Text aus einer Datei einliest und diesen in Klartext verwandelt, also entschlüsselt. Sie erkennen, dass Ihr Geheimtext richtig entschlüsselt wurde daran, dass das Wort *Linux* im Klartext enthalten ist. Der Klartext und der verwendete Code (Zahl der Verschiebung) sollen an den Nutzer ausgegeben werden.

Organisatorisches

Abzugeben ist bis zum **12. Januar 2020** ein C++-Programm, welches die oben gestellte Aufgabe löst. Gemeint ist dabei ausschließlich die Datei beleg.cpp (Beispielname), keine .zip-, .tar-, .exe- oder Projektdateien. Ihr Programm muss im Pool des FRIZ unter Linux kompilierbar sein, andernfalls gilt der Beleg als nicht bestanden. Sie können dies auf dem per ssh (unter Windows mit dem Programm putty) von außen nutzbaren Rechner

rotuma.informatik.tu-chemnitz.de testen. Gruppenarbeiten und das Verändern des vorgegebenen Quelltextes und Randbedingungen sind **nicht zulässig**.

Dieses Programm ist über die URL

`http://if-belege.informatik.tu-chemnitz.de/`

in den Belegbereich für die Lehrveranstaltung zu laden. Dabei müssen Sie sich mit URZ-Login und URZ-Passwort authentifizieren. Der Webserver if-belege.informatik.tu-chemnitz.de ist nur aus dem Campusnetz der TU Chemnitz erreichbar, das Laden des Programmes muss also von einem TU-Rechner oder einem mit VPN mit der TU verbundenen Rechner aus erfolgen! Verwenden Sie für den VPN-Zugang auf Ihren Rechnern installierte VPN-Clienten (z.B. CISCO anyconnect) oder den Zugang über WEB-VPN (siehe: `https://www.tu-chemnitz.de/urz/network/access/vpn.html`).

Bitte beachten Sie, dass ausschließlich Mailadressen zur Kommunikation verwendet werden dürfen, die Sie von der TU Chemnitz erhalten haben (DSGVO). Die erste Antwortmail signalisiert den ordnungsgemäßen Uploadvorgang. Die zweite Antwortmail belegt die Abgabe und enthält Informationen, ob die Belegaufgabe in ausreichender Form bearbeitet wurde. Bei Problemen mit dem Upload des Programmes bzw. bei der Bedienung schreiben Sie bitte eine E-Mail an dr.andreas.mueller@informatik.tu-chemnitz.de.

Das Programm soll als Kommentar enthalten:

- Name, Vorname, Matrikelnummer
- Falls nötig Hinweise zur Nutzung