Verschlüsselungen mit der Caesar-Scheibe

Verschlüsselungen sind ein grundlegender Bestandteil der Umwelt von Schülerinnen und Schülern. Die Caesar-Chiffre bietet sich als Verschiebe-Chiffre gut zum Einstieg in diese Thematik an.

Die Caesar-Chiffre geht auf Gaius Julius Caesar zurück, der zur Verschlüsselung seiner Nachrichten die Buchstaben immer um drei Buchstaben verschob. Statt eines A schrieb er also ein D. In diesem Modul sollen die Schülerinnen und Schüler neben dieser historischen Verschlüsselungsmethode auch die allgemeinere Verschiebe-Chiffre und die Caesar-Scheibe als Hilfsmittel kennenlernen.

Mit der Verschiebe-Chiffre kann ein Text leicht ver- oder entschlüsselt werden, wenn man Klartext- und Chiffretextalphabet untereinander schreibt.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

(Beispiel für die Caeser-Chiffre, oben Klartextalphabet)

Dies führt jedoch zu der Problematik, dass man für jede einzelne Verschiebung eine solche Liste erstellen müsste. Die Caesar-Scheibe bietet hier eine gute und handliche Alternative.

Zum Bau benötigen die Schülerinnen und Schüler nur die beigefügte [Bastelanleitung](Caesar_Scheibe_Bauanleitung.docx), sowie eine Musterbeutelklammer.

Die beiden Kreise müssen ausgeschnitten werden und der Kleinere mittig auf den Größeren gelegt werden, so dass sich die Felder an der Außenseite nicht überdecken. Durch eine Musterklammer werden die beiden Kreise aufeinander fixiert. Um die Musterklammer einsetzten zu können, sind auf den Scheiben Einschnitte vorgesehen.

Anschließend müssen in die leeren Felder der beiden Scheiben noch jeweils die Buchstaben von A bis Z in alphabetischer Reihenfolge eingetragen werden. Die Buchstaben sind absichtlich in der Vorlage noch nicht eingetragen, da mache Schüler später die Verschlüsselung auch durch phantasievoll gestaltete Symbole realisieren möchten.

Es ist sinnvoll den Bastelbogen auf dickerem Papier zu drucken bzw. die Vorlagen auf Tonkarton aufzukleben, damit die Scheibe stabiler ist.

Durch Drehen der kleinen Scheibe kann nun der Buchstabe A (Klartext) auf jeden beliebigen Buchstaben (Chiffre) eingestellt werden. Zum Verschlüsseln suchen die Schüler den Buchstaben des Klartextes auf der großen Scheibe und ersetzen ihn durch den zugehörigen Buchstaben der kleinen Scheibe.

Zum Entschlüsseln ist der Vorgang genau entgegengesetzt. Die Schüler suchen den Buchstaben der Chiffre auf der kleinen Scheibe und ersetzen ihn durch den zugehörigen Buchstaben der großen Scheibe.

Bei gegebenem Schlüssel ist die Entschlüsselung einer Verschiebe-Chiffre recht einfach. Fehlt der Schlüssel jedoch, so führt dies zu größeren Problemen. Da es allerdings nur 25 Verschiebungen gibt, ist es möglich, sämtliche Schlüssel auszuprobieren und so eine Nachricht zu entschlüsseln. Einfacher ist jedoch eine Eingrenzung des Schlüssels durch eine Häufigkeitsanalyse als einfachste Kryptoanalyse. In einem ausreichend langen Text kommen, abhängig von der verwendeten Sprache, verschiedene Buchstaben gemäß einer bestimmten Verteilung vor. So ist im Deutschen der häufigste Buchstabe das E (17,4%) gefolgt von N (9,78%) und I (7,55%). Bei einem längeren verschlüsselten Text kann man also durch Zählen der Buchstaben Kandidaten für den Buchstaben E herausfinden und so die Verdrehung der Caesar-Scheibe schneller herausfinden.

Reihenfolge für das Vorgehen in der AG-Sitzung

Die Schüler basteln zunächst die Caesar-Scheibe. Das Basteln der Scheibe wird vorangestellt, da zur Einführung in das Thema das Vorlesen eines Textes empfohlen wird und die Schüler die Handlungen der Geschichte haptisch nachvollziehen können.

Die [beigefügte Textpassage](Caesar_Scheibe_Text_Beutelspacher.docx) aus dem Buch Beutelspacher, Albrecht: *Christian und die Zahlenkünstler. Ein Mathe-Krimi;* Deutscher Taschenbuchverlag Verlag, München 2008 bietet einen gelungen Einstieg in die Thematik.

Folgend auf den Text erhalten die Schüler das [Arbeitsblatt](Caesar_Scheibe_Schueler.docx).

Die angebotenen Aufgaben sind nach wachsendem Schwierigkeitsgrad geordnet.

Aufgabe 1: original Caesar-Code

(Lösung: kryptographieistsehrspannend)

Aufgabe 2: vorgegebene Verschiebung

(Lösung: auchmiteineranderenverschiebungfunktioniertdiecaesarchiffre)

Aufgabe 3: Entschlüsselung ohne bekannten Schlüssel

(Lösung: A->I; diecaesarchiffreistsehrunsicherundleichtzuknacken)

Aufgabe 4 wird von Schülern besonders gerne bearbeitet, da sie sich gegenseitig Aufgaben stellen können.

Werden weitere Nachrichten zur Entschlüsselung benötigt, können diese leicht mit einem Applet unter der Adresse <http://cryptoclub.math.uic.edu/shiftcipher/shiftcipher.htm> durch den Lehrer selbst erstellt werden.

Das Applet kann auch den Schülern angeboten werden, um größere Texte zu ver- oder zu entschlüsseln. Die Anweisungen des Applets sind in englischer Sprache verfasst. Die Vokabeln encrypt und decrypt werden den Schülern in der Regel nicht bekannt sein und sollten daher vom Lehrer angegeben werden.

Ein besonderes Merkmal des Programms besteht darin, dass es den Schülerinnen und Schülern nicht vollständig die Arbeit abnimmt. Zu Beginn einer Ent- bzw. Verschlüsselung müssen jeweils die ersten drei Buchstaben selbstständig bearbeitet werden. Wird dabei ein Fehler gemacht, gibt das Programm einen Warnhinweis.