Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung

Niedersächsische Landesschulbehörde

Titel: Einstieg in die Kryptologie

Bei der Bearbeitung sind digitale Werkzeuge/Geräte erforderlich Ja **x** Nein ☐

Fach	**Klasse**	**Urheber**	**Erscheinungsdatum**
Informatik	11 Gymnasium Einführungsphase	Fachberatung Informatik Nds. Landesschulbehörde	04.2020

Kenntnisse und Fertigkeiten

Die Schüler*innen…

- beschreiben das Prinzip der Substitution zur Verschlüsselung von Daten.
- implementieren monoalphabetische Verfahren, u.a. Caesar-Verfahren.
- erläutern das Prinzip der Häufigkeitsanalyse.
- beurteilen die Sicherheit einfacher Verschlüsselungsverfahren.

Inhalt

Phase 1: Ein eigenes Verschlüsselungsverfahren entwickeln
Überlegen Sie sich ein Verfahren, mit dem Sie einfache Texte verschlüsseln können.

Erklären Sie Ihr Verfahren z.B. Ihren Eltern, Geschwistern, oder beispielsweise am Telefon oder in einer Videokonferenz Mitschüler*innen. Schicken Sie sich gegenseitig kurze verschlüsselte Texte zu und entschlüsseln Sie diese.

Bild von OpenClipart-Vectors auf Pixabay

Phase 2: Das Caesar-Verfahren
a) Das Caesar-Verfahren kennenlernen
Unter dem folgenden Link wird das Caesar-Verfahren erklärt:
https://www.inf-schule.de/kids/datennetze/verschluesselung/schritt2
(Version vom 06.04.2020)

Bauen Sie nach der Vorlage eine Caesar-Scheibe nach oder verwenden Sie die dortige digitale Scheibe. Bearbeiten Sie damit die Aufgaben 1 – 4.

b) Das Caesar-Verfahren variieren und analysieren
Mithilfe der folgenden Arbeitsblätter lernen Sie Varianten der Caesar-Verschlüsselung kennen und machen sich erste Gedanken, wie man dieses Verfahren „knacken“ kann.
Bearbeiten Sie dazu die folgenden Arbeitsblätter

- Stationsblatt Caesar
- Arbeitsblatt Caesar
- Lösungsblatt Caesar

Die Gesamtmaterialien finden Sie unter:
https://ddi.uni-wuppertal.de/website/index-ddi.html?navi=materialien&main=spioncamp
(Version vom 06.04.2020).

c) Zusatz: Implementierung des Caesar-Verfahrens
Diese Aufgabe können Sie nur bearbeiten, falls Sie bereits erste Erfahrungen im Programmieren im Unterricht sammeln konnten: Implementieren Sie das Caesar-Verfahren in einer aus dem Unterricht bekannten Programmiersprache. Gehen Sie zur Vereinfachung davon aus, dass die Eingabe nur aus Großbuchstaben besteht.

- Implementieren Sie zunächst die Verschiebung eines einzelnen Buchstabens. Eine mögliche Lösung in Snap! finden Sie unter HilfeCaesar1.pdf bzw. den Quelltext unter HilfeCaesar1.xml.

- Implementieren Sie damit die Verschlüsselung einer beliebigen Eingabe. Eine Lösung in Snap! finden Sie unter LoesungProgrammCaesar.pdf bzw. den Quelltext unter LoesungProgrammCaesar.xml.

Falls Sie keinen Ansatz finden, analysieren Sie jeweils die Hilfen/Lösungen HilfeCaesar1 und LoesungProgrammCaesar aus der .zip Datei für die Umsetzung in der grafischen Programmiersprache Snap!
https://snap.berkeley.edu/snap/snap.html
(Version vom 06.04.2020).
Vielleicht können Sie damit dann ja analog die Entschlüsselung implementieren?

Phase 3: Sicherheit einfacher Verschlüsselungsverfahren beurteilen
a) Beispiel Cäsar-Verschlüsselung
Unter
https://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_kryptoanalyseverschiebeverfahren
(Version vom 06.04.2020)
geht es um eine Kryptoanalyse des Caesar-Verfahrens (dort wird dieses als Verschiebeverfahren bezeichnet). Bearbeiten Sie Aufgabe 1. Statt des Tipps 2 können Sie den Text auch mit einer Textverarbeitungssoftware analysieren und die Häufigkeit der einzelnen Buchstaben über Strg+F bestimmen. Nutzen Sie dann zum „Knacken“ des Geheimtextes die Eigenschaft, dass der häufigste Buchstabe langer Texte in deutscher Sprache das E ist.

Vergleichen Sie Ihr Ergebnis mit der Lösung Loesung_KryptoanalyseCaesar.pdf.

b) Häufigkeitsanalyse bei monoalphabetischer Verschlüsselung:
Sie haben sicherlich bemerkt, dass das Caesar-Verfahren relativ leicht zu knacken ist. Es gibt weitere monoalphabetische Substitutionsverfahren, vgl. hierzu:
https://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_ersetzungsverfahren
(Version vom 06.04.2020).
Vergleichen Sie Ihr selbst entwickeltes Verfahren mit dem hier beschriebenen Ersetzungsverfahren.

Mit hoher Wahrscheinlichkeit war Ihr Verfahren auch ein Ersetzungsverfahren (man sagt auch „Substitutionsverfahren"), wobei Sie zum Verschlüsseln statt Buchstaben möglicherweise Zeichen oder Symbole zugelassen haben. All diese monoalphabetischen Substitutionsverfahren lassen sich relativ leicht mit einer Häufigkeitsanalyse „knacken".

Darum geht es in den folgenden Materialien:
https://ddi.uni-wuppertal.de/website/index-ddi.html?navi=materialien&main=spioncamp
(Version vom 06.04.2020).

- Stationsblatt Kryptoanalyse
- Material Kryptoanalyse
- Arbeitsblatt Kryptoanalyse
- Lösung Kryptoanalyse

Hinweise für begleitende Erwachsene

Zur Phase 1
Neben inhaltlichen Kompetenzen (z.B. die Implementierung bekannter Verschlüsselungsverfahren) sind in der Informatik prozessbezogene Kompetenzen wie beispielsweise das kreative Schaffen und Problemlösen mindestens genauso wichtig. Daher sollten Sich Schüler*innen zunächst eigene Verschlüsselungsverfahren ausdenken und an diesen das Ver- und Entschlüsseln mehrfach erproben, bevor sie historische und später auch moderne Verschlüsselungsverfahren kennenlernen.

Lassen Sie Ihrem Kind Zeit bei der Entwicklung des eigenen Verfahrens. Insbesondere das Ver- und Entschlüsseln darf ruhig mehrfach durchgeführt werden.

Zur Phase 2
Die Teile a) und b) können in eigenem Tempo bearbeitet werden, im Anschluss sollte mit den vorhandenen Lösungen verglichen werden.

Teil c) kann von Ihrem Kind nur bearbeitet werden, wenn es vorher im Unterricht bereits ausreichend Programmiererfahrungen sammeln konnte. Setzen Sie es nicht unter Druck, falls dies nicht der Fall sein sollte.

Verweise

Liste aller Links zum Spioncamp, entwickelt an der Bergischen Universität Wuppertal:

- Stationsblatt Caesar:
https://ddi.uni-wuppertal.de/website/repoLinks/v284_substitution-m-caesar-station.pdf
- Arbeitsblatt Caesar:
https://ddi.uni-wuppertal.de/website/repoLinks/v251_substitution-m-caesar-ab1.pdf
- Lösungsblatt Caesar:
https://ddi.uni-wuppertal.de/website/repoLinks/v296_substitution-m-caesar-loesung.pdf
- Stationsblatt Kryptoanalyse:
https://ddi.uni-wuppertal.de/website/repoLinks/v293_buchstabenhaeufigkeit-station.pdf
- Material Kryptoanalyse:
https://ddi.uni-wuppertal.de/website/repoLinks/v273_buchstabenhaeufigkeit-mat0.pdf
- Arbeitsblatt Kryptoanalyse:
https://ddi.uni-wuppertal.de/website/repoLinks/v236_buchstabenhaeufigkeit-ab1.pdf
- Lösung Kryptoanalyse:
https://ddi.uni-wuppertal.de/website/repoLinks/v229_buchstabenhaeufigkeit-loesung.pdf

Selbst erstellte Materialien in der angefügten Zip-Datei:

- HilfeCaesar1.pdf
- HilfeCaesar1.xml
- LoesungProgrammCaesar.pdf
- LoesungProgrammCaesar.xml
- Loesung_KryptoanalyseCaesar.pdf