Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung

Niedersächsische Landesschulbehörde

Titel: Kryptologie

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

Fach	**Klasse**	**Urheber**	**Erscheinungsdatum**
Informatik	12 Gymnasium Qualifikationsphase	Fachberatung Informatik Nds. Landesschulbehörde	04.2020

Kenntnisse und Fertigkeiten

Die Schüler*innen…

- beschreiben das Prinzip der polyalphabetischen Substitution, u.a. am Beispiel des Vigenère-Verfahrens
- beurteilen die Sicherheit eines gegebenen symmetrischen Verschlüsselungsverfahrens
- beschreiben und unterscheiden die Prinzipien der symmetrischen und asymmetrischen Verschlüsselung
- erläutern das Prinzip von digitalen Signaturen

Inhalt

Phase 1: Wiederholung des Caesar-Verfahrens

Mithilfe der folgenden Arbeitsblätter wiederholen Sie Varianten der Caesar-Verschlüsselung und machen sich erste Gedanken, wie man dieses Verfahren „knacken“ kann. Bearbeiten Sie dazu die folgenden Arbeitsblätter unter:
https://ddi.uni-wuppertal.de/website/index-ddi.html?navi=materialien&main=spioncamp
(Version vom 06.04.2020).

- Stationsblatt Caesar
- Arbeitsblatt Caesar
- Lösungsblatt Caesar

Implementieren Sie anschließend das Caesar-Verfahren in einer aus dem Unterricht bekannten Programmiersprache. Gehen Sie zur Vereinfachung davon aus, dass die Eingabe nur aus Großbuchstaben besteht.

Hinweis: Falls Sie keinen Ansatz finden, analysieren Sie das fertige Snap!-Programm LoesungProgrammCaesar. Entwickeln Sie analog einen Algorithmus zur Entschlüsselung. Snap! ist eine grafische Programmiersprache:
https://snap.berkeley.edu/snap/snap.html
(Version vom 06.04.2020)

Phase 2: Vigenère-Verfahren

a) Häufigkeitsanalyse bei monoalphabetischer Verschlüsselung wiederholen:
Monoalphabetische Verschlüsselungsverfahren können mithilfe einer Häufigkeitsanalyse häufig „geknackt“ werden. Falls nötig können Sie die dafür nötigen Grundlagen mithilfe des folgenden Materials wiederholen

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

b) Polyalphabetisches Vigenère-Verfahren erarbeiten:
Im Folgenden erarbeiten Sie sich daher ein polyalphabetisches Verschlüsselungsverfahren.

Erarbeiten Sie zunächst die grundlegende Verfahrensweise beim Verschlüsseln durch das Vigenère-Verfahrens mithilfe des folgenden Materials:

- Stationsblatt Vigenère
- Arbeitsblatt Vigenère
- Material Vigenère
- Lösungen Vigenère

Vergleichen Sie das Vigenère-Verfahren mit dem Caesar-Verfahren.
Zusatzaufgabe: Begründen Sie, dass wenn man die Länge des Schlüssels beim Vigenère-Verfahren kennt, man den Schlüssel evtl. mithilfe mehrerer Häufigkeitsanalysen rekonstruieren könnte.

Implementieren Sie anschließend das Vigenère-Verfahren in einer aus dem Unterricht bekannten Programmiersprache. Sie können dafür Ihr Programm zur Caesar-Verschlüsselung weiterentwickeln.

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

Phase 3: unterschiedliche Verschlüsselungsverfahren anwenden, beurteilen und implementieren

Ziel dieser Phase ist die Analyse eines neuen Verschlüsselungsverfahrens, ein Vergleich mit bekannten Verfahren wie Vigenère oder Caesar, eine Implementierung eines neuen Verfahrens, sowie eine Einschätzung, ob es sich jeweils um ein Transpositions- oder Substitutionsverfahren handelt. (Ziel ist nicht, diese neuen Verfahren auswendig zu lernen.)

Entscheiden Sie sich für eines oder mehrere der folgenden Verschlüsselungsverfahren:

- Freimaurer
- Strom-Chiffre
- Playfair
- Pflügen

Bearbeiten Sie die zugehörigen Arbeitsblätter und -materialien des Spioncamps:
https://ddi.uni-wuppertal.de/website/index-ddi.html?navi=materialien&main=spioncamp
(Version vom 06.04.2020).

Ergänzende Informationen zu Ihrem Verfahren finden Sie möglicherweise auch unter
https://www.inf-schule.de/kommunikation/kryptologie
(Version vom 06.04.2020)

Falls möglich, implementieren Sie Ihr Verfahren in einer aus dem Unterricht bekannten Programmiersprache. Testen Sie Ihre Implementierung mithilfe Ihrer Lösungen zu den Arbeitsblättern.

Phase 4: Ausblick
Weitere Verschlüsselungsverfahren finden Sie beispielsweise unter
https://www.cryptool.org/de/cryptool-online
(Version vom 06.04.2020).

Unter
https://www.inf-schule.de/kommunikation/kryptologie/modernechiffriersysteme
(Version vom 06.04.2020) werden moderne Chiffriersysteme betrachtet.

In der Kryptologie beschäftigt man sich nicht nur mit Verschlüsselung. Genauso wichtig sind Authentizität und Integrität von Nachrichten:
https://www.inf-schule.de/kommunikation/kryptologie/sicherheitsprobleme/konzept_sicherheitsziele
Version vom 06.04.2020).

Eine interaktive Anwendung zur Simulation der Vertraulichkeit durch asymmetrische Kryptografie findet man unter
http://it-lehren.de/asym/Vertraulichkeit-durch-asymmetrische-Kryptographie-herstellen.html
(Version vom 06.04.2020).

Zur digitalen Signatur findet man Lernmaterialien unter
https://www.inf-schule.de/kommunikation/kryptologie/digitalesignatur
(Version vom 06.04.2020).

Eine interaktive Anwendung zur Simulation der Integrität einer Nachricht und Authentizität ihres Absenders mit einer digitalen Signatur findet man unter
http://it-lehren.de/asym/Integritaet-und-Authentizitaet-mit-digitaler-Unterschrift-sicherstellen.html
(Version vom 06.04.2020).

Zusammenfassend ist möglicherweise auch der Brickfilm unter
https://www.inf-schule.de/kommunikation/kryptologie
(Version vom 06.04.2020) interessant.

Anlagen

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
- Stationsblatt Vigenère: https://ddi.uni-wuppertal.de/website/repoLinks/v240_substitution-p-vigenere-station.pdf
- Arbeitsblatt Vigenère: https://ddi.uni-wuppertal.de/website/repoLinks/v254_substitution-p-vigenere-ab1.pdf
- Material Vigenère: https://ddi.uni-wuppertal.de/website/repoLinks/v282_substitution-p-vigenere-mat0.pdf
- Lösungen Vigenère: https://ddi.uni-wuppertal.de/website/repoLinks/v253_substitution-p-vigenere-loesung.pdf

Selbst erstellte Materialien in der angefügten Zip-Datei

- LoesungProgrammCaesar.pdf
- LoesungProgrammCaesar.xml