**UV 9.4 Geheim ist geheim? Sichere Kommunikation mit Kryptographie**

|  |  |
| --- | --- |
| **Leitfragen:**   * *Wer hat Interesse am Versenden geheimer Botschaften?* * *Ist das Versenden geheimer Botschaften eine Erfindung des Computerzeitalters? Wurden auch in der Zeit vor der Erfindung des Computers Nachrichten verschlüsselt?* * *Wie arbeiten Verschlüsselungsverfahren?* * *Wie schützt man heutzutage seine Privatsphäre bei privater Kommunikation?* | **Ausschärfung der Inhaltsschwerpunkte:**   * *Anwendungskontexte für Verschlüsselungen* * *Strategien zur Verschlüsselung in der Vergangenheit (Cäsar, Skytale, …)* * *Analyse über die Buchstabenhäufigkeit* * *Versenden geheimer Botschaften (auch per Email)* |

**Vorhabenbezogene Konkretisierung:**

Am Anfang des Unterrichtsvorhabens wird das Thema an und für sich problematisiert. Schülerinnen und Schüler sehen oft - dem Gesichtspunkt „Ich habe gar keine Geheimnisse“ folgend - keinen Bedarf für Geheimhaltung. Insofern ist es sinnvoll, zunächst Beispiele für zwischenmenschliche Kommunikation zu sammeln, die nicht für eine breite Öffentlichkeit bestimmt ist. Diese gibt es zahlreich im Geschäftsleben, im Bankenwesen, in politischen Zusammenhängen, im militärischen Bereich und natürlich auch im Privatleben der Schülerinnen und Schüler selbst.

Weiterhin wird das Bewusstsein dafür geschärft, wie privat/öffentlich Nachrichten in sozialen Medien, in E-Mail oder auf anderen Internetplattformen sind. Fragestellungen können dabei z.B. sein:

* Kann jemand außer dem Empfänger meine E-Mails lesen? Wer kann das?
* Kann man Informationen aus dem Internet auch wirksam wieder entfernen?
* ...

Zunächst lernen die Schülerinnen und Schüler unterschiedliche steganographische Verfahren kennen. Solche Verfahren wurden bereits im Altertum (z.B. „unsichtbare Tinte“) entwickelt und finden auch noch heutzutage (z.B. „Codierung von Nachrichten in Bildern“) Verwendung.

Ein Nachteil steganographischer Verfahren besteht in der leichten Lesbarkeit der Botschaft, wenn die Botschaft entdeckt wird. Diese Erkenntnis führt zu einem Bedarf an kryptographischen Verfahren um Botschaften zu verschlüsseln. Ein einfaches Beispiel dafür bietet der Cäsar-Algorithmus. Ein darauf aufbauendes komplexeres Verfahren ist die Vigenère-Verschlüsselung. Damit das Unterrichtsvorhaben in der dafür vorgesehenen Zeit durchgeführt werden kann, bietet sich an, die Schülerinnen und Schüler in Gruppen kurze Einführungen in die Themen Steganographie, Skytale, Cäsar-Verfahren und Vigenère-Verfahren geben zu lassen mit anschließenden Übungen zur Cäsar- und Vigenère-Verschlüsselung. Dazu gibt es reichlich – auch für Schülerinnen und Schüler – verständliche Literatur. Das Cäsar-Verfahren soll im UV 10.1 im Rahmen der textorientierten Programmierung in Python umgesetzt werden.

Welche Chancen hat ein fremder Empfänger ohne Kenntnis des Schlüssels die Nachricht zu entschlüsseln? Bei Cäsar-verschlüsselten Nachrichten ist die Chance recht groß, wenn der fremde Empfänger eine Häufigkeitsauszählung der Zeichen vornimmt. Je länger der Text, desto größer ist seine Chance. Vigenère-verschlüsselte Botschaften lassen sich nur mit größerem Aufwand wieder entschlüsseln.

Die Diskussion komplexerer Verschlüsselungsverfahren bleibt dem Unterricht der Sekundarstufe II vorbehalten. Falls die Zeit dafür reicht und/oder großes Interesse besteht, lernen die Schülerinnen und Schüler ein modernes Verfahren der asymmetrischen E-Mail-Verschlüsselung kennen. Sie erfahren dazu, dass diese Verfahren mit einem öffentlichen und einem privaten Schlüssel arbeiten und dass nur der Besitzer des privaten Schlüssels die mit dem öffentlichen Schlüssel codierten Nachrichten auch lesen kann. Große E-Mail-Provider bieten solche Verfahren auf kostenfreien Portalen an. Das Joseph-Weizenbaum-Gymnasium ist technisch für die Verwendung ausgerüstet und der Versand verschlüsselter Mail wird im Unterricht abschließend beispielhaft durchgeführt.

**Zeitbedarf**: 6 Std.

**Sequenzierung des Unterrichtsvorhabens:**

|  |  |  |
| --- | --- | --- |
| **Unterrichtssequenzen** | **Zu entwickelnde (inhaltsfeldbezogene konkretisierte) Kompetenzen** | **Beispiele, Medien, Materialien** |
| Die geheime Botschaft   * Sammeln von Beispielen für geheime Botschaften * Diskussion der Notwendigkeit von Geheimhaltung im privaten Bereich und im Arbeitsleben | Die Schülerinnen und Schüler   * analysieren anhand ausgewählter Beispiele, wie personenbezogene Daten verarbeitet und genutzt werden können (DI), * bewerten auf Grundlage ihrer im Informatikunterricht erworbenen Kenntnisse Möglichkeiten der Datenverarbeitung hinsichtlich Chancen und Risiken in ausgewählten Kontexten (A), * beurteilen an ausgewählten Beispielen die gesellschaftlichen Auswirkungen des Einsatzes von Informatiksystemen und berücksichtigen das Recht auf informationelle Selbstbestimmung (A), * geben Beispiele für Auswirkungen von Informatiksystemen auf die Berufswelt (A). | Beispiele für den Einstieg:   * Schülerinnen und Schüler können evtl. über Verletzungen des eigenen Privatbereiches berichten * NSA - Skandal |
| Wie werden Nachrichten verschlüsselt?   * Überblick über historische Verfahren (z. B. Steganographie und Skytale) * Cäsar-Verschlüsselung * Vigenère-Verschlüsselung | Die Schülerinnen und Schüler   * codieren Daten für die Verarbeitung mit einem Informatiksystem (DI), * interpretieren Ergebnisse eines Datenverarbeitungsprozesses (DI), * verarbeiten Daten mithilfe von Informatiksystemen (MI), * verarbeiten gleichartige Daten mit Hilfe eines geeigneten Werkzeuges (DI), * erarbeiten sich die Funktionsweise einer Anwendung selbstständig (DI). | Literatur:   * Singh, Simon; CODES; Hanser; ISBN 3-446-20169-6 * Gallenbacher, Jens; Abenteuer Informatik; Elsevier; ISBN 978-3-8274-2965-0, <http://www.abenteuer-informatik.de> * Beutelspacher, Albrecht; Kryptologie; Vieweg; ISBN 978-3-8348-0253-8   Software:  - Cryptool  Materialien:  - SpionCamp der Uni Wuppertal |
| Wie werden Nachrichten entschlüsselt?   * Häufigkeitsauszählung * Sprachabhängigkeit der Häufigkeitsauszählung | Die Schülerinnen und Schüler   * erläutern die Unsicherheit eines einfachen Verschlüsselungsverfahrens (A). |  |
| Lernerfolgsüberprüfung durch eine Aufgabe in einer Klassenarbeit | | |