

Konzepte und Anwendungen der asymmetrischen Verschlüsselung

Didaktische Hinweise

Zielgruppe

Die Materialien zur asymmetrischen Verschlüsselung richten sich an Schüler*innen in der Qualifikationsphase. Sie können sowohl in Kursen auf grundlegendem als auch auf erhöhtem Anforderungsniveau eingesetzt werden.

Voraussetzungen

Es werden die Kompetenzen aus dem Lernfeld *Informationen und Daten*, die im niedersächsischen Kerncurriculum für die gymnasiale Oberstufe¹ in der Einführungsphase vorgesehen sind, vorausgesetzt. So sollten die Schüler*innen mit dem Aufbau des Internets vertraut sein, um die Gefahren der Datenübertragung im Klartext einschätzen zu können. Außerdem wird davon ausgegangen, dass die Schüler*innen die Konzepte der symmetrischen Verschlüsselung anwenden können. Hier wird auch vorausgesetzt, dass die Konzepte der symmetrischen Verschlüsselung wie für die Qualifikationsphase vorgesehen bereits am Beispiel polyalphabetischer Verfahren, speziell dem Vigenère-Verfahren, vertieft wurden.

Lernziele

Anhand der vorliegenden Materialien können die folgenden Kompetenzen aus dem Modul Kryptologie im Lernfeld *Informationen und Daten* erworben werden.

Die Schülerinnen und Schüler ...

- beschreiben und unterscheiden die Prinzipien der symmetrischen und asymmetrischen Verschlüsselung
- beschreiben Anwendungsbereiche für symmetrische bzw. asymmetrische Verschlüsselungsverfahren
- erläutern das Prinzip von digitalen Signaturen und Zertifikaten

Zu beachten ist, dass sich die Materialien zwar am niedersächsischen Kerncurriculum für die gymnasiale Oberstufe orientieren, jedoch keinen Anspruch auf Vollständigkeit hinsichtlich der für die Abiturprüfung erwarteten Kompetenzen erheben. Die Autorin hat zum Teil individuelle Schwerpunkte gesetzt, die auch über die im KC geforderten Kompetenzen hinausgehen können. Verbindlich für das Abitur in Niedersachsen sind allein das niedersächsische Kerncurriculum für die gymnasiale Oberstufe sowie die ergänzenden Hinweise² in der jeweils aktuellen Fassung. Es obliegt daher den jeweiligen Fachlehrer*innen, den Unterricht so zu gestalten, dass die Schüler*innen umfassend auf das Abitur vorbereitet werden. Die vorliegenden Materialien stellen somit nur eine Anregung dar, die an die individuellen Bedürfnisse der Lerngruppe angepasst werden müssen.

¹ Niedersächsisches Kultusministerium (Hrsg.) (2017) *Kerncurriculum für das Gymnasium – gymnasiale Oberstufe, die Gesamtschule – gymnasiale Oberstufe, das Kolleg. Informatik*. Hannover: unidruck

² Niedersächsisches Kultusministerium (Hrsg.) (2018) *Ergänzende Hinweise zum Kerncurriculum Informatik für die gymnasiale Oberstufe am Gymnasium, an der Gesamtschule sowie für das Kolleg*.
<https://cuvo.nibis.de/cuvo.php?p=download&upload=174> [Datum des Zugriffs: 01.09.2020]

Ergänzende Materialien zur polyalphabetischen Substitution und zur Einschätzung der Sicherheit symmetrischer Verschlüsselungsverfahren sind in Arbeit.

Aufbau des Leitfadens

Im niedersächsischen Kerncurriculum ist in Bezug auf die asymmetrische Verschlüsselung nur eine Erarbeitung der Konzepte vorgesehen. Die Betrachtung konkreter mathematischer Verfahren wie dem RSA-Verfahren gehören hingegen nicht zu den im Kern erwarteten Kompetenzen. Daher sehen die Materialien die Erarbeitung der Prinzipien der asymmetrischen Verschlüsselung zum einen auf einer ikonischen Ebene vor. Zum anderen kommt die Software Gpg4win³ zum Einsatz, um die asymmetrische Verschlüsselung praktisch einzusetzen und die Konzepte auch auf Anwendungsebene zu veranschaulichen. Neben dem Leitfaden zur asymmetrischen Verschlüsselung enthält das Materialpaket daher entsprechende Anleitungen für Gpg4win. Diese sind in separaten Dateien enthalten, um den Lesefluss des Leitfadens nicht zu stören.

Der Leitfaden ist so aufgebaut, dass die Schüler*innen die Konzepte und Anwendungsmöglichkeiten der asymmetrischen Verschlüsselung Schritt für Schritt erarbeiten und entdecken können. Die ikonische Ebene und die praktische Anwendung in Gpg4win kommen dabei parallel zum Einsatz. Neben den Einsatzmöglichkeiten asymmetrischer Verschlüsselung steht dabei die Frage, wie Vertrauen in einem Netzwerk, in dem sich nicht alle Teilnehmer*innen persönlich kennen, aufgebaut werden kann, im Vordergrund.

Das Werkzeug Gpg4win

Das verwendete Programmpaket Gpg4win-3.1.15 unterstützt die beiden relevanten kryptographischen Standards OpenPGP und S/MIME (X.509). Es enthält Komponenten zur Schlüsselverwaltung, zur Ver- und Entschlüsselung sowie zur Signatur von Texten, E-Mails und Dateien. Ein entsprechendes Programmpaket steht mit GPG Suite⁴ auch für das Betriebssystem macOS zur Verfügung.

Das Softwarepaket Gpg4win enthält zwei verschiedene Programme zur Anwendung der asymmetrischen Verschlüsselung: *Kleopatra* und *GPA*.

Das Programm Kleopatra erlaubt in der hier verwendeten Version das Erzeugen eines Schlüssel-paares ohne Passwort. Da die Schüler*innen das Passwort zum Teil mit dem privaten Schlüssel verwechseln, kann dies für das Verständnis der Konzepte von Vorteil sein. In GPA ist hingegen das Ver- und Entschlüsseln sowie das Signieren von Texten in der Zwischenablage nach Ansicht der Autorin anschaulicher und übersichtlicher. Außerdem sind private und öffentliche Schlüssel in der Schlüsselverwaltung von GPA durch ein doppeltes zweifarbiges bzw. ein einfaches einfarbiges Schlüsselsymbol deutlich zu unterscheiden. Während Kleopatra bei der Installation des Programmpaketes vorausgewählt ist, muss GPA explizit angewählt werden. Die Anleitungen zum Erzeugen eines Schlüssels, zum Ver- und Entschlüsseln sowie zum Signieren, liegen für beide Varianten vor. Inzwischen sind die entsprechenden Verschlüsselungsverfahren auch in vielen E-Mail-Programmen integriert. Um das Vorgehen transparenter zu machen, wird hier jedoch weiterhin die eigenständige Software genutzt.

³ Gpg4win. GNU Privacy Guard for Windows. <https://www.gpg4win.de/> [Datum des Zugriffs: 27.01.2021]

⁴ GPG Suite. <https://gpgtools.org/> [Datum des Zugriffs: 19.04.2021]

Lizenz

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International Lizenz](#). Sie erlaubt Download und Weiterverteilung des vollständigen Werkes unter Nennung unserer Namen, jedoch keinerlei Bearbeitung oder kommerzielle Nutzung.