



Wie wir uns sicher in der digitalen Welt bewegen können - Kryptografie -



Verfasser: Kurt Kunze (KK), Thomas Oelsner (TO) , Matthias Rothe (MR)

Lizenz: CC-BY-SA-NC

Kurz-Info:

Informatischer Inhalt:

Informatik und Gesellschaft, Kryptografie

Jahgangsstufe:

10 (Oberschule)

Vorwissen:

persönliche Erfahrungen

KURZINFORMATION FÜR DIE LEHRKRAFT

Titel: *Wie wir uns sicher in der digitalen Welt bewegen können – Kryptografie –*

Schulstufe: *Sekundarstufe 1 (Oberschule)*

optimale Jahrgangsstufe: *Klasse 10*

Themenbereich:

- Informatik und Gesellschaft
- Kryptografie

Einordnung in Rahmenvorgaben

Lehrplan Informatik: *LB1 und LB2 Klassenstufe*

nach Lehrplanentwurf Oberschule (Stand März 2021)

Bildungsstandards der GI: *passende Inhalts- und Prozessbereiche*

Einbindung in den Unterricht:

Vorkenntnisse: *persönliche Vorerfahrungen in der digitalen Welt*

Dauer: *8 Stunden LB1 (Informatik und Gesellschaft) 6 Stunden LB2 (Kryptografie)*

Inhaltsbeschreibung:

Im Verlauf dieses Moduls setzen sich die Lernenden mit den immer stärker zunehmenden Auswirkungen der Digitalisierung auf Alltag und Berufsleben auseinander. Auf einen digital begleiteten, von Diskussionen geprägten Teil, folgt eine Einführung in ausgewählte Methoden der Kryptografie.

Um vor allem die Chancen der Digitalisierung zu untermauern, können im Verlauf des gesamten Moduls zahlreiche digitale Möglichkeiten eingesetzt werden, welche den (Informatik-) Unterricht sinnvoll erweitern können. Der überwiegende Teil, der verwendeten Tools, kann von den Lernenden auch außerhalb der Schule problemlos verwendet werden. Bspw. während der bevorstehenden Berufs- und Weiterbildung können diese digitalen Helfer weiterführend von den Lernenden eingesetzt werden.

Anschließend beleuchtet dieses Modul die Kryptografie. Dank H5P-Inhalten können Lernende konkrete Methoden der symmetrischen Verschlüsselung kennen lernen. Das Prinzip der asymmetrischen Verschlüsselung wird abschließend vermittelt. Die Lernenden erhalten auf diese Weise ein Grundverständnis zu Verschlüsselungsverfahren. Dies kann einen Beitrag zur sicheren und selbstbewussten Nutzung der Möglichkeiten der digitalen Welt leisten.

INHALTSVERZEICHNIS

Kurzinformation für die Lehrkraft	2
Motivation & Lernziele	6
Fachliche Analyse	9
Einordnung in Rahmenvorgaben	17
Lehrplan Informatik	17
Bildungsstandards der GI (KK)	20
Überblick über das Modul	21
Einbettung in den Schulunterricht	25
Voraussetzungen (MR)	25
Nachhaltigkeit (MR)	25
Stoffverteilungsplan und Stundenplanung	26
Vorstellung der Verwendeten und erzeugten Tools	36
Didaktische/Methodische Schwerpunktsetzung	51
Arbeitsmaterialien	57
Didaktische Analyse - Materialien	59
Reflexion	69

Zusammenfassung

Im vorliegenden Modulhandbuch werden zentral die Kernstunden des Lernbereiches 2 der Klassenstufe 10 „ausgewählte Methoden der Kryptografie“ beschrieben. Diese schließen sich an das Thema Datenschutz aus dem Lernbereich 1 „Informatik und Gesellschaft“ an. Die als Doppelstunde konzipierte Unterrichtseinheit ermöglicht Lernenden die selbstständige Erarbeitung und Anwendung ausgewählter symmetrischer kryptografischer Verfahren. Dazu wurden Arbeitsblatt-begleitete digitale H5P-Lernelemente entwickelt, welche hier im Rahmen der Expertengruppen-Methode eingesetzt werden. In einer abschließenden Diskussion sollen die erarbeiteten kryptographischen Verfahren hinsichtlich der Ziele der Kryptografie diskutiert werden. In einer Folgestunde sollen asymmetrische Verschlüsselungsverfahren thematisiert werden. Folgend werden zusammenfassend die Stationen der Kernstunden zu den Methoden der Kryptografie beschrieben.

KK

Die Cäsar-Verschlüsselung stellt das simpelste, hier vorgestellte, Verschlüsselungsverfahren dar. Zu Beginn des Lernelements bekommen die Lernenden einen Eindruck, von der lang zurückreichenden Geschichte der Kryptografie. In kleinen Lerneinheiten werden dann zunächst die Grundbegriffe der Kryptografie, dann das Verfahren der Cäsar-Verschlüsselung erklärt. Durch kleine Abfragen nach jedem theoretischen Input können die Lernenden stets ihren Lernfortschritt überprüfen. abschließend muss das Verfahren in abwechslungsreichen Übungsaufgaben, welche trotz Einfachheit des Verfahrens einen anspruchsvollen Charakter erhalten, angewendet werden.

Die Einfachheit des Verfahrens selbst stellt in diesem Lernelement die didaktische Reduktion dar. An diesem einfachen Verfahren können grundsätzliche Konstruktionsmethoden moderner Verschlüsselungsverfahren anschaulich vermittelt werden. Durch abwechslungsreiche Übungsaufgaben kann das Wissen zum Verfahren von den Lernenden überprüft werden.

TO

Die Gartenzauntransposition wird als Vertreter der Transpositionsverfahren erlernt. Den Schwierigkeitsgrad zum Erlernen des Algorithmus zur Ver- bzw. Entschlüsselung schätze ich als niedrig ein. Es wurde dafür ein digitales H5P-Lernmodul als „All-in-One-Datei“ im HTML-Format erstellt, das mit einem Doppelklick in jedem herkömmlichen Webbrowser geöffnet werden kann. Das Lernmodul ist darauf ausgelegt, einen niedrigschwelligen Einstieg in das Modul zu ermöglichen und auch leistungsstärkeren Schülerinnen und

Schülern Aufgaben auf höherem Niveau zu stellen. Dies geschieht, indem erst alle Schritte der Ver- und Entschlüsselung mit dem kleinsten Schlüssel 2 eingeübt werden, um dann diese Schritte mit Schlüssel 3 zu wiederholen. Das Lernmodul ist in viele kleine Abschnitte unterteilt, die im Lernprozess jeweils einen Schritt weitergehen und dann eine Aufgabe dazu abfragen, die den Lernenden die Rückmeldung gibt, ob sie den nächsten Schritt verstanden haben. Das Lernmodul ist in ein Agentenszenario eingebettet. Agenten müssen sich über verschlüsselte Botschaften ihren geheimen Aufenthaltsort mitteilen, ohne dass Dritte mitlesen können. Darum sind alle Wörter, die zu ver- oder entschlüsseln sind, Ortsbezeichnungen, d.h. Ländernamen, Städtenamen bzw. Stadtteile.

MR

Der Einstellungstest stellt den Einstieg in die hier ausführlich vorgestellte Lerneinheit zu den Kryptografiemethoden dar. Er dient einerseits zur Einstimmung der Lernenden in das hier zu Grunde liegende Agenten-Thema, andererseits sollen die Ergebnisse dieses Tests zur homogenen Verteilung der Lernenden auf die Arbeitsgruppen gewährleisten. Hier soll auf Grundlage der jeweils erreichten Punktezahl die in der Lerngruppe vorherrschende Heterogenität gerecht und gleichmäßig auf die Arbeitsgruppen verteilt werden.

Die Erarbeitung der Grundbegriffe stellt die essenzielle Bedingung dar, sich mit den hier vorgestellten Methoden der Kryptografie überhaupt beschäftigen zu können. Aus diesem Grund wurde dieses Element zwar eigenständig geplant und umgesetzt, wurde aber letztendlich vor jedes Lernelement vorgeschaltet, da nur damit gewährleistet werden kann, dass wirklich jeder Lernende die benötigten Voraussetzungen zur weiteren Arbeit erfüllt. Konkret muss jede Gruppe die Erarbeitung der Grundbegriffe abgeschlossen und auf dem jeweiligen Arbeitsblatt eines jeden Lernmoduls gefestigt haben, bevor die Bearbeitung der eigentlichen Kryptografiemethode beginnen kann.

Der an manchen Stellen anklingende Versuch Inhalte des Lernbereiches 1 in diesem Modul näher zu beleuchten konnte leider nicht in die Realität umgesetzt werden. Die entsprechenden Hinweise wurden auf Grund der folgerichtigen Bedeutung für den Lernbereich 2 jedoch im Modulhandbuch belassen. Der Stoffverteilungsplan zum Modul liefert zahlreiche Ideen zur Unterrichtsgestaltung und bietet zahlreiche digitale Tools an, die eingesetzt werden können.

MOTIVATION & LERNZIELE

Informatiksysteme nehmen eine zunehmende, nicht mehr weg zu denkenden Rolle in unserer Gesellschaft ein. Dies hatte in den letzten zwanzig Jahren tiefgreifende Auswirkungen auf den Alltag und das Berufsleben von Menschen zur Folge.

Die Bearbeitung dieser Thematik in der Schule ist umso wichtiger, da traditionelle Wissensvermittlung über „die Älteren“ an dieser Stelle nicht funktionieren kann, da keine Generation zuvor unter solch stetem und schnellem technologischem Fortschritt aufgewachsen ist.

Auch kursieren zahlreiche Fehlinformationen in den neuen Medien. Die Lernenden sollten daher mit zentralen Fragestellungen der zunehmenden Digitalisierung konfrontiert werden, um zu lernen, Informationen und Meinungen kritisch zu hinterfragen. Es sollten daher viele Facetten der „Digitalisierung“ angesprochen werden. Es muss viel Platz für Diskussionen eingeräumt werden. Die eigenen Erfahrungen der SuS sollten zentral in den Unterricht eingebunden werden. Die im Stoffverteilungsplan angedachten Einzelstunden sind aufgrund des hohen Anteils persönlicher Vorerfahrungen der Lernenden hier kaum vorhersagbar, deren Detailplanung soll daher hier vernachlässigt werden. Das Übergeordnete Lernziel des Lernbereich 1 der Klasse 10 lässt sich jedoch hier konkret formulieren.

- Lernende schätzen Chancen und Risiken der digitalen Welt kritisch ein und leiten daraus Handlungsmaximen für das eigene selbstbestimmte Verhalten im digital vernetzten Kontext ab.

Die anschließende Auseinandersetzung mit der Kryptografie im LB2 soll dann das Verständnis und das Handwerkszeug für einen sicheren Umgang mit Informatiksystemen liefern. Dabei werden verschiedene symmetrische Verschlüsselungsverfahren detailliert vorgestellt, deren Schwachstellen thematisiert, um abschließend die Funktionsweise asymmetrischer Verschlüsselungsverfahren vorzustellen. Daraus lassen sich folgende Groblernziele für den Lernbereich ableiten.

- Lernende erlangen ein Grundverständnis für Verschlüsselungsverfahren, um die Möglichkeiten der digitalen Welt sicher ausschöpfen zu können.

Cäsar-Verschlüsselung (KK)

Die Cäsar-Verschlüsselung ist eine 2000 Jahre alte Verschlüsselungsmethode. Sie ist zwar mit kryptoanalytischen Methoden (z.B. einer Häufigkeitsanalyse der Buchstaben) sehr leicht zu entschlüsseln und findet daher in der Informatik praktisch keine Anwendung mehr. Jedoch kann sie als Vorstufe moderner Verschlüsselungsmethoden (wie bspw. der Vigenere-Methode) betrachtet werden. Sie gibt einen historischen Einblick in die Entwicklung moderner Verschlüsselungsmethoden. Durch Bezugnahme auf Julius Cäsar und die Zeit des Römischen Reiches erhält die Unterrichtseinheit eine fächerverbindende Komponente.

Vor allem die Einfachheit des Verfahrens gibt auch leistungsschwachen Lernenden die Möglichkeit, sich selbstständig in eine Methode der Kryptografie einzuarbeiten. Durch die Einbindung des Moduls „Grundbegriffe der Kryptografie“ (von Matthias) werden die Lernenden mit den prinzipiellen Schritten beim Ver- und Entschlüsseln vertraut gemacht. Sie erhalten ein Grundverständnis um Begriffe wie „Schlüssel“ oder „Geheim- und Klartext“, welche auch in anspruchsvolleren Verfahren eine zentrale Rolle spielen. Auch die Erarbeitung des Cäsar-Verfahrens geschieht selbstständig durch Bearbeiten des Moduls. Das Festhalten der so gewonnen Kenntnisse auf einem Arbeitsblatt und das abschließende Erklären des Verfahrens fordert das Verstehen der erlernten Inhalte.

Durch Aufgabentypen mit steigendem Schwierigkeitsgrad können sowohl leistungsstarke wie -schwache Lernende das erworbene Wissen spielerisch und fordernd anwenden.

Alle hier eingesetzten Aufgabentypen sind prinzipiell für Leistungskontrollen denkbar.

Die kryptografischen Schwächen der Cäsar-Verschlüsselung richten zudem den Blick der Lernenden auf die Anforderungen, die moderne Verschlüsselungsverfahren erfüllen müssen. In einem diese Unterrichtseinheit abschließendem Vergleich verschiedener Verschlüsselungsverfahren trägt somit auch das Verständnis um die Cäsar-Methode dazu bei, die Leistungsfähigkeit verschiedener Methoden besser einzuschätzen zu können. Lernende können damit auch die abschließende Diskussion über Kriterien guter Verschlüsselungsverfahren bereichern.

Zusammenfassend können also folgende Kompetenzen bei der Behandlung der Cäsar-Methode erworben werden (Teillernziele innerhalb der Stunde):

- Lernende kennen den allgemeinen Ablauf von Verschlüsselungsverfahren sowie der Cäsar-Verschlüsselung, indem sie beide Abläufe mit eigenen Worten schriftlich und mündlich erklären.
- Lernende wenden die Cäsar-Verschlüsselung an, indem sie konkreten Beispiele mit steigendem Schwierigkeitsgrad bearbeiten und eigene Übungsaufgaben erstellen.

- Lernende bewerten das erarbeitete Verfahren, indem es mit anderen Verfahren vergleichen und dessen Anwendbarkeit hinsichtlich der Ziele der Kryptografie mit Mitlernenden diskutieren.

Gartenzauntransposition (TO)

Die Kryptographie kennt zwei grundlegende Verschlüsselungsklassen, nämlich die Substitution und die Transposition. Moderne Verfahren der Verschlüsselung beruhen auf der mehrfachen Wiederholung von Substitution und Transposition. Cäsar- und Vigenère-Verschlüsselung stellen Substitutionsverfahren dar. Die Gartenzauntransposition wird in diesem Modul als Stellvertreter der Transpositionsverfahren eingeführt. Dass man durch Vertauschen der Buchstaben unlesbare Texte erzeugen kann, ist trivial. Der Mehrwert des Themas liegt eher darin, dass die SuS begreifen, dass die Vertauschung von Zeichen nach bestimmten Regeln erfolgen muss, damit der Empfänger einer verschlüsselten Botschaft diese auch mit akzeptablem Aufwand wieder in die richtige Reihenfolge bringen kann.

- Die SuS können nach dem Absolvieren des Moduls selbständig Texte mit der Gartenzauntransposition mit Schlüssel 2 (und 3) mit kariertem Papier und Stift analog ver- und entschlüsseln.

Vigenere-Verschlüsselung (MR)

Die Vigenere-Verschlüsselung schließt fachlich wie didaktisch an die Caesar Verschlüsselung an und zeigt eindrücklich wie sich derartige Verfahren weiterentwickeln können. Den Lernenden wird durch den Vergleich von Caesar- und Vigenere-Verfahren klar, dass durch konsequentes Weiterdenken der ursprünglichen Idee ein Verfahren an wachsende Herausforderungen und technische Möglichkeiten angepasst werden kann. Die starke Ähnlichkeit beider Verschlüsselungsverfahren wird durch Parallelen im Bearbeitungsprozess wie im Festigungsprozess deutlich. Den SuS wird durch die Bearbeitung beider Verfahren in den Lernmodulen die Weiterentwicklung der Caesar Verschlüsselung durch die Vigenere Methode klar.

Durch die Einbindung des Lernmoduls „Grundbegriffe der Kryptografie“ können sich die Schülerinnen und Schüler dieses Einstiegsthema kleinschrittig erarbeiten und im dazugehörigen Arbeitsblatt sichern. Hierbei werden die Lernenden mit den prinzipiellen Schritten beim Ver- und Entschlüsseln vertraut gemacht. Sie erhalten ein Grundverständnis um Begriffe wie „Schlüssel“ oder „Geheim- und Klartext“, welche auch in anspruchsvolleren Verfahren eine zentrale Rolle spielen.

Alle verwendeten Aufgabentypen sind prinzipiell zur Leistungsermittlung geeignet.

Durch Einarbeitung verschiedener Schwierigkeitsstufen ist es möglich auch leistungsstarke Schüler zu fordern.

Zusammenfassend können durch die Bearbeitung des Moduls Vigenere-Verschlüsselung folgende Kompetenzen erarbeitet werden:

- Lernende wenden die Vigenere-Verschlüsselung an, indem sie konkreten Beispiele mit steigendem Schwierigkeitsgrad in Gruppenarbeit bearbeiten.
- Lernende bewerten das erarbeitete Verfahren, indem es mit anderen Verfahren vergleichen und dessen Anwendbarkeit hinsichtlich der Ziele der Kryptografie mit Mitlernenden diskutieren.

FACHLICHE ANALYSE

Kryptografie (TO)

Die Methoden der **Kryptographie** machen eine Nachricht für Unbefugte unlesbar und unverständlich. Der Leser erkennt aber, dass es sich um eine Geheimschrift handelt, deswegen spricht man in diesem Fall auch von **offenen Geheimschriften**. Ein wichtiges Prinzip der Kryptographie ist der 1883 von Auguste Kerckhoffs formulierte Grundsatz dass ein kryptographisches Verfahren nur auf der **Geheimhaltung des Schlüssels** beruhen darf, niemals auf der Geheimhaltung des Verfahrens selbst^{T1}. Das heißt, dass ein potenzieller Angreifer zwar wissen darf, dass es den Geheimtext gibt, dass es ein Geheimtext ist und darüber hinaus noch, mit welchem Algorithmus der Klartext verschlüsselt wurde, aber er darf den Geheimtext nicht ohne den dazugehörigen Schlüssel entziffern können.

Bei der **Steganographie** handelt es sich im Gegensatz dazu um **verdeckte Geheimschriften** und das Ziel der Steganographie ist es, die bloße Existenz einer Nachricht zu verbergen. Dieses dem Kerckhoffs' Prinzip gegenübergestellte Prinzip wird „**Security through obscurity**“ (Deutsch: Sicherheit durch Unklarheit) genannt.^{T2}

Die Übersicht zeigt eine Hierarchie der Begrifflichkeiten. Neben dem Begriff Kryptographie wird noch der Begriff der **Kryptanalyse** benutzt, der sich ausschließlich auf die Wissenschaft, verschlüsselte Texte zu entziffern, bezieht. Die weiteren Unterteilungen **klassisch** und **modern** sind, wie folgt, zu verstehen. Mit klassischen Verfahren sind Verfahren gemeint, die sich damit beschäftigen, Buchstaben oder Buchstabenfolgen zu ver- bzw. entschlüsseln. Die zwei grundlegenden Techniken nennt man **Substitution**, also das Austauschen von Buchstaben mit anderen Buchstaben oder Zeichen und **Transposition**, also das Verändern der Anordnung von Zeichen in einem Text. Heutzutage

werden die Methoden der Verschlüsselung hauptsächlich im IT-Bereich angewendet und Computer arbeiten nicht direkt mit Buchstaben, sondern sie basieren auf Binärzahlen. Der Begriff Moderne Verfahren bezeichnet also in diesem Sinne Verfahren, die sich mit der Ver- und Entschlüsselung von Binärzahlen beschäftigen. Als **symmetrische Verfahren** werden die bezeichnet, bei denen der Schlüssel zum Verschlüsseln derselbe wie zum Entschlüsseln ist, während das bei **asymmetrischen Verfahren** nicht der Fall ist. Bei letzterem werden jeweils Schlüsselpaare erzeugt, die aus einem öffentlichen und einem privaten Schlüssel bestehen. Der öffentliche Schlüssel dient dazu, Daten zu verschlüsseln, die dann nur mit dem dazugehörigen privaten Schlüssel wieder entschlüsselt werden können. Damit entfällt der bei den symmetrischen Verfahren notwendige Schlüsseltausch.

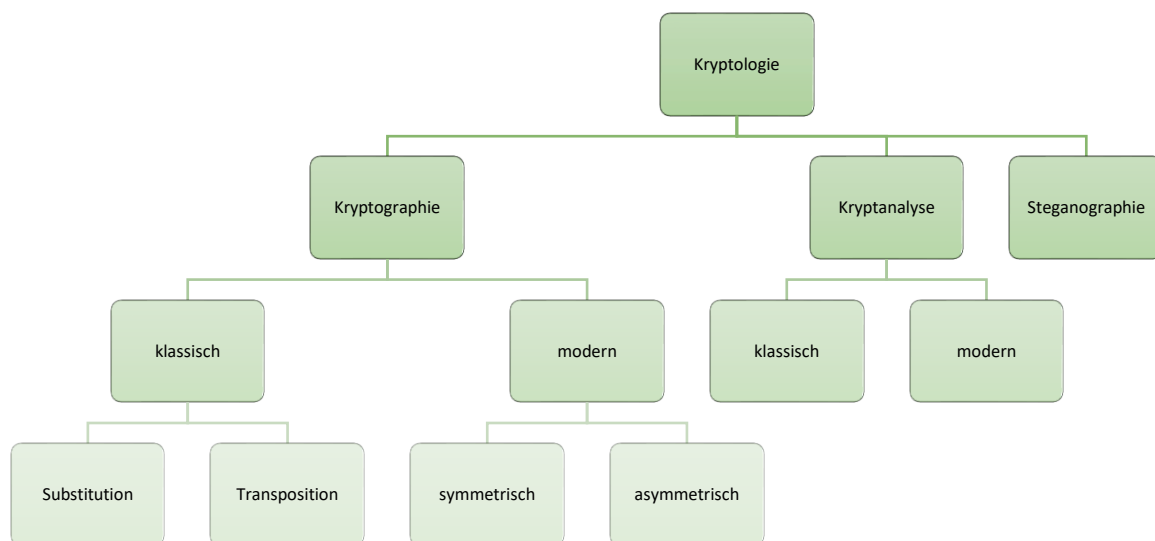


Abbildung 1 - (modifiziert aus den Quellen: T3, T4, T5)

Cäsar-Verschlüsselung (KK)

Bei der Cäsar-Verschlüsselung handelt es sich um ein monografisches monoalphabetisches Substitutionsverfahren ^{K1}. Sie wird den symmetrischen Verschlüsselungsverfahren zugeordnet. Bei Substitutionsverfahren werden, Zeichen oder Zeichengruppen eines zu verschlüsselnden Klartextes durch andere Zeichen ersetzt (substituiert) ^{K2}. Die Position oder Reihenfolge der Zeichen bleibt dabei unverändert. Als monographisch wird es bezeichnet, da genau ein Zeichen des Klartextes jeweils durch genau ein anderes Zeichen in der Geheimbotschaft ersetzt wird ^{K3}. Die Bezeichnung monoalphabetisch beschreibt die Tatsache, dass genau ein Geheimalphabet beim Substituieren verwendet wird. Ein bestimmtes Zeichen wird also immer durch genau ein anderes bestimmtes Zeichen ersetzt ^{K4}. Die Substitution der Zeichen beruht diesem

Verfahren auf einer cyclischen Verschiebung der Zeichen entlang des geordneten Alphabets, wobei cyclisch bedeutet, dass beim Verschieben über das Z hinaus beim A anfangend weiter verschoben wird. Der Schlüssel gibt an, um wie viele Buchstaben der Klartext verschoben werden muss. Die Cäsar-Verschlüsselung wird daher in der Literatur auch als Cäsar-Verschiebung oder Verschiebechiffre bezeichnet.

Die Cäsar-Verschlüsselung geht auf den römischen Feldherrn und Politiker Julius Cäsar (110 - 44 v. Chr.) zurück. Vor allem in seiner Funktion als Feldherr und Politiker war er darauf angewiesen sensible Informationen in Briefen vor unbefugten Lesern zu schützen. Cäsar begnügte sich jedoch nur einer speziellen Form der heute als Cäsar-Verschlüsselung bekannten Methode. Er verwendete stets den Schlüssel drei (A→D) ^{K5}.

Erst das Aufkommen sogenannter Cäsar-Scheiben (siehe Abbildung 2) im 15. Jahrhundert verweist darauf, dass das Verfahren auf alle 25 möglichen Schlüssel ausgeweitet wurde, um auch im Mittelalter Botschaften vor ungewollten Einblicken zu schützen. Im Laufe der Geschichte von der frühen Antike bis ins ausgehende Mittelalter waren weitere vergleichbare Geheimschriften, wie bspw. das Atbash-Alphabet (Substitutionsverfahren hebräischer Gelehrter seit 600. v. Chr.), das Alphabetum Kaldeorum (Geheimschrift österreichischer Herzöge, 15. Jh.) oder das Freimaurer-Alphabet (Geheimtextalphabet aus Zeichen des sog. Freimaurer-Quadrats, 18. Jh.) geläufig, welche große Parallelen zur Cäsar-Chiffre aufweisen ^{K6}.

Die Cäsar-Verschlüsselung, welche nun mehr 2000 Jahre alt ist, gilt heute als sehr einfach und unsicher. Neben der mittlerweile fast durchgehenden Alphabetisierung der Bevölkerung (in westlichen Ländern), machen es vor allem Informatik-Systeme möglich, Cäsar-verschlüsselte Texte in wenigen Augenblicken zu entschlüsseln. Das Verfahren wird heute daher in der Regel nur dafür eingesetzt, Grundprinzipien der Kryptografie anschaulich darzustellen ^{K7}. Auch beinhaltet dieses Verfahren keine sichere Möglichkeit zum Schlüsselaustausch. Dieser muss, soll er denn geheim bleiben, bei persönlichen Treffen oder auf anderer Weise verschlüsselt ausgetauscht werden. Das Verfahren ist also auch aus dieser Perspektive nicht für eine sinnvolle Verschlüsselung im informatischen Kontext nutzbar.

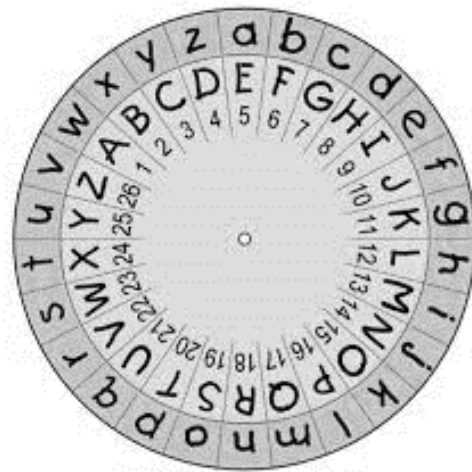


Abbildung 2 - Cäsar-Scheibe mit dem Klartext außen und dem Geheimtext innen. Zusätzlich sind im inneren Kreis die numerischen Schlüssel angegeben. (Screenshot der digitalen Cäsar-Scheibe, siehe Materialsammlung)

Nichtsdestotrotz kann es als einfaches digitales oder Pen-and-Paper-Verfahren für bestimmte Zwecke zwar als schwaches, aber durchaus alltagstaugliches Verfahren betrachtet werden. Denn immerhin sind Botschaften vor schnellem ungewünschten Lesezugriff geschützt. Der potenzielle „Fremdleser“ muss zumindest den Willen aufbringen die Nachricht zu entschlüsseln.

So findet das Verfahren gelegentlich auch im weiteren Sinne informatischen Kontext als ROT-Verfahren (von ‚rotate‘, engl. für drehen / verschieben) noch Verwendung. Üblicherweise wird dabei nach dem ROT13-Verfahren gearbeitet. Dabei wird mit dem festen Schlüssel 13 gearbeitet, sodass sowohl beim Ver- als auch Entschlüsseln um 13 Zeichen verschoben werden muss. Einsatzgebiete dieses ROT13-Verfahrens beschränken sich jedoch auf z.B. auf Rätselseiten oder beim Geocaching, um Hinweistexte zu Rätseln, sog. Spoiler, unkenntlich zumachen. Verschiedene Varianten des ROT-Verfahrens sind beschrieben. In manchen Foren ist diese Funktion integriert ^{K8}. Das ROT13-Verfahren könnte im Lernbereich 3 (Komplexe Programmieraufgabe) als Projektidee aufgegriffen werden.

In der Geschichte der Kryptografie kann die Cäsar-Chiffre als Vorgänger weitere Verfahren gesehen werden. Hier sei nur kurz die Verschlüsselung nach VIGENERE erwähnt, bei der das Cäsar-Verfahren um einen polyalphabetischen Schlüssel erweitert wurde. Dieses Verfahren wiederum kann als Vorläufer moderner Verschlüsselungstechnologien gesehen werden, mit deren Hilfe heute bspw. sichere Kommunikation in WLAN-Netzen gewährleistet werden kann (Der WLAN-Key ist ein polyalphabetischer Schlüssel) ^{K9}.

Zusammenfassend kann das Cäsar-Verfahren als eine einfache und unsichere Verschlüsselungsmethode beschrieben werden. Der Einsatz im Unterricht ist jedoch „didaktisch sinnvoll, da es Substitutionsverfahren als grundsätzliches Konstruktionsprinzip moderner Verschlüsselungs-Methoden verständlich darstellt“ ^{K7}.

Zur weiteren Einarbeitung ins Thema empfiehlt es sich die angebenen Quellen zu lesen. Besonders das freizugängliche Werk „Das CrypTool-Buch: Kryptographie lernen und anwenden mit CrypTool und SageMath“ ^{K7} gibt einen weitreichenden Einblick in vergleichbare Methoden der Kryptografie. Vor allem die historische Entwicklung der Kryptografie lässt sich in dem Buch „Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.“ gut verständlich nachlesen. Auch Internetseite www.Kryptowissen.de oder www.Kryptografie.de liefern zahlreiche leicht zugängliche Fakten rund um die Kryptologie, die Kryptografie sowie die Kryptoanalyse. Beide Seiten bieten Online-Tools, zum Ver- und Entschlüsseln von Botschaften u.a. mit der Cäsar-Methode.

Gartenzauntransposition (TO)

Die Gartenzauntransposition, auch Gartenzaun-Chiffre, Jägerzaun-Chiffre oder im englischen Sprachgebrauch rail fence cipher oder zig zag cipher bekannt, beschreibt ein einfaches Transpositionsverfahren. Dabei werden die fortlaufenden Zeichen eines Textes fortlaufend im Zickzack auf **S** Zeilen verteilt und dann zeilenweise ausgelesen. **S** ist dabei gleichzeitig der Schlüssel.

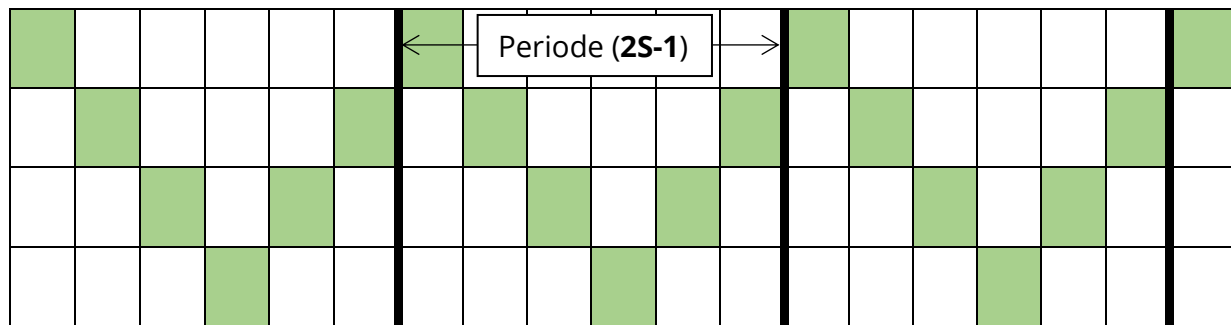
Ein Beispiel für **S = 4** mit dem Klartext „GARTENZAUN“:

G						Z			
	A				N		A		
		R		E				U	
			T						N

Zeilenweise gelesen ergibt sich der Geheimtext „GZ ANA REU TN“. Die Leerzeichen werden in der Regel weggelassen und dienen hier nur der Übersichtlichkeit.

Das Entschlüsseln kurzer Geheimtexte mit vorgegebenem Schlüssel **S** auf Papier ist trivial. Man zählt die Länge **L** des Geheimtextes und erstellt einen Gartenzaun mit **S** Zeilen und **L** Buchstabenfeldern. Dort trägt man zeilenweise den Geheimtext ein und liest im Zickzack den Klartext aus. Bei nicht vorhandenem Schlüssel **S** muss die Anzahl der Zeilen variiert werden, bis ein sinnvoller Klartext erscheint.

Längere Geheimtexte, deren Entschlüsselung per Hand zu zeitaufwendig wäre, können mit Hilfe eines Computers und der Brute-Force-Methode entschlüsselt werden, obwohl dazugesagt werden muss, dass der Sinn des Klartextes von einem Menschen erfasst werden muss. Dabei ist der wesentliche Punkt die **Verteilung der Buchstaben pro Zeile** zu berechnen. Ist der Schlüssel unbekannt, kann die Verteilung der Buchstaben in Abhängigkeit der Länge **L** und des Schlüssels **S** auf die Zeilen des Gartenzauns berechnet werden. Dazu sind einige einfache mathematische Überlegungen notwendig. Da es sich beim Gartenzaun um eine Zickzacklinie handelt, kann man ähnlich einer Cosinus-Funktion von Periodizität sprechen. Die Periodenlänge **P** variiert mit der Größe des Schlüssels und entspricht **P = 2S-1**.



Jede Periode besteht aus genau zwei „Spitzen“, also ein Buchstabe in der obersten Zeile und ein Buchstabe in der untersten Zeile. In der Cosinusfunktion entspricht das den Sattelpunkten. In den Zeilen dazwischen gibt es zwei Buchstaben pro Periode. Weniger trivial ist die Berechnung der Buchstabenverteilung einer unvollständigen Periode. Ein Rest entsteht, wenn die Länge **L** des Geheimtextes nicht durch die Periodenlänge **P** teilbar ist. Man berechnet die Anzahl der Perioden **N** per ganzzahliger Division mit $N = \frac{L}{P}$. Für den Rest **R**, der aus der Division hervorgeht, muss eine Fallunterscheidung getroffen werden:

1. Der Rest **R** ist kleiner oder gleich des Schlüssels **S**: Es wird von oben nach unten an **R** Zeilen ein Buchstabe „addiert“.
2. Der Rest **R** ist größer als der Schlüssel und kleiner als **P-1**: Von unten nach oben werden zu **S-R** Zeilen noch Buchstaben hinzuaddiert.

Gehen wir zurück zum Beispiel GARTENZAUN / GZANAREUTN. Der Text GZANAREUTN hat die Länge **L = 10**. Der Schlüssel ist bekannt mit **S = 4**, damit errechnet sich eine Periodenlänge $2 \times (4 - 1) = 6$. Dividiert man ganzzahlig mit **P = 6** ergibt sich **N = 1 R 4**. Damit ist der Rest genauso groß wie der Schlüssel und zu jeder der 4 Zeilen wird noch ein Buchstabe zur Verteilung hinzugefügt.^{T6}

Zeile	N = 1	R = 4	Summe	Buchstabenverteilung
Zeile 1	1	1	2	GZ
Zeile 2	2	1	3	ANA
Zeile 3	2	1	3	REU
Zeile 4	1	1	2	TN

jeweilig zueinanderstehenden Buchstaben des Schlüssels sowie des Klartextes herausucht und notiert. Um die Länge des Schlüssels in der Übertragung nicht kenntlich zu machen, wird der Geheimtext am Block oder in Gruppen fester Länge übertragen. Die Entschlüsselung beim Empfänger kann durch die Umkehrung der beschriebenen Verschlüsselung erfolgen.

MR1 Quelle: <https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre>

Quellen zur weiteren Einarbeitung:

- ^{MR2} <https://www.cryptool.org/de/cto/vigenere>

Einstellungstest / Grundbegriffe (MR)

In Wissenschaft, Forschung und Wirtschaft ist es gängige Praxis die Eignung entsprechender Kandidaten über Tests zu ermitteln. Besonders der Bereich des logischen Denkens ist mit einer Vielzahl an Aufgaben abgedeckt und stellt oftmals einen Großteil der Tests dar. Hierbei unterscheiden diese in unterschiedliche Kategorien: zahlengebundene, grafikgebundene und sprachgebundene Logikaufgaben, zudem wird oft das räumliche Vorstellungsvermögen abgeprüft. Ein gewisses Maß an Logik hilft Zusammenhänge zu erkennen, Informationen zu verknüpfen und Schlussfolgerungen zu ziehen. Zudem spielt Logik eine wesentliche Rolle bei der Lösung von Problemen auf eine effiziente oder kreative Art. Im Gegensatz zu fachlichen Tests geht es hierbei vielmehr darum, dass der Kandidat beweist, wie er in herausfordernden Situationen reagiert und passende Schlussfolgerungen zieht. Dies wird erreicht indem vornehmlich das abstrakte Denkvermögen abgefragt wird. All diese Eigenschaften und Fähigkeiten sind speziell in der Anfangs- und Einarbeitungsphase neuer Mitarbeiter essenziell, um Arbeitsfähigkeit eines neuen Mitarbeiters schnell zu erreichen.

MR3 Quelle <https://testhelden.com/der-logiktest/>

Die Grundbegriffe der Kryptografie müssen von den Lernenden verinnerlicht werden, da diese die Grundlage bilden, auf der das weitere Arbeiten in den ausgewählten Kryptografiemethoden erst ermöglicht wird. Besonders die, zur Lebenswelt der Schüler, semantischen Unterschiede der Begriffe bieten ein großes Risiko hinsichtlich Fehlvorstellungen und Fehldeutung. Diese gilt es kleinschrittig abzubauen und im fachlichen Zusammenhang korrekt zu festigen.

EINORDNUNG IN RAHMENVORGABEN

LEHRPLAN INFORMATIK

Einordnung des Moduls (TO)

Unser Hauptaugenmerk in diesem Modul lag auf dem Lernbereich 2 in Klasse 10 „Kryptografie“. Kryptografie steht eng im Bezug zu den Themen Datenschutz und verschlüsselter Übertragung von Informationen. In Kl. 7 LB 2 „Repräsentation von Daten“ kommen die SuS im Informatikunterricht das erste Mal in Kontakt mit dem Thema „schützenswerte Daten“ und auch mit Manipulation von Daten. In Klasse 9 wird das Thema Datenschutz an zwei Stellen aufgegriffen, nämlich am Ende des Lernbereich 1 „Informationen und Daten“, wenn es um die Chancen und Risiken bei der automatisierten Verarbeitung großer Datenmengen geht und in Kl. 9 LB 2 „Netzwerke in der Informatik“ werden sich die SuS zu „Gefahren in einer vernetzten Welt“ positionieren. Die Ziele der Kryptografie leiten sich aus ebendiesen Gefahren ab, sodass die Lehrkräfte in diesem Lernbereich schon einmal demonstrieren können, wie diese Ziele durch Angriffe kompromittiert werden können.

Der Lernbereich 1 Klasse 10 „Informatik und Gesellschaft“ stellt eine Wiederkehr und Verknüpfung sehr vieler Themen aus den vorangegangenen Klassenstufen dar, die die nun entsprechend ihrem Alter und in ihrer persönlichen Reife fortgeschrittenen SuS noch einmal auf einem höheren Niveau vernetzen und diskutieren können. Die SuS haben in diesem Lernbereich die Aufgabe, sich zu Auswirkungen der automatisierten Generierung von Daten zu positionieren. In jeder der Klassen 7-9 wird das Thema Generierung von Daten aus einem anderen Blickwinkel beleuchtet. In Klasse 7 LB 2 „Repräsentation von Daten“ wird die Generierung von Daten mit Hilfe von Sensoren und Automaten thematisiert. In Klasse 8 LB 1 „Algorithmen und Programme“ lernen die SuS, wie Computerprogramme die Sammlung und Auswertung von Daten unterstützen und in Klasse 9 LB 1 „Informationen und Daten“ wurde durch den Unterricht im Thema Datenbanken der Grundstein zu Organisation solch gesammelter Daten gelegt.

Im zweiten Teil Kl. 10 LB 1 ist das Lernziel, die Auswirkungen der Digitalisierung im Privatbereich und in der Wirtschaft zu beurteilen. Um zu verstehen, wie menschliche Tätigkeiten und technische Prozesse überhaupt digitalisiert werden können, haben die SuS bereits in Kl. 7 LB 1 „Informatik im Alltag“ einige Beispiele für Informatiksysteme kennengelernt und wissen, dass diese nach dem EVA-Prinzip funktionieren. In Klasse 8 LB 1 wenden die SuS dann „Algorithmen zur Lösung einfacher lebenspraktischer Problemstellungen“ an und in Klasse 9 LB 2 „Netzwerke in der Informatik“ wird dieses

Wissen darum erweitert, wie Informatiksysteme miteinander vernetzt werden, was ein Kernpunkt der Digitalisierung ist.

Einordnung der Kernstunden zu Methoden der symmetrischen Verschlüsselung (KK)

Die hier konkret behandelten Inhalte sind im Lernbereich 2 der Klassenstufe 10 einzuordnen (nach Lehrplanentwurf Informatik für die Oberschule, Stand März 2021). Konkret wird der im Lehrplan verpflichtend geforderte Inhalt „Ausgewählte Methoden der Kryptografie“ bearbeitet. Das in dieser Einheit vermittelte Wissen zur Funktionsweise von Verschlüsselungsverfahren liefert Hintergrundwissen zu Fragestellungen einer „unmittelbaren“ Vorstunde des Lernbereichs 1 (Inhalt: „Beurteilung der Digitalisierung – im Privatbereich: Datensicherheit im privaten Bereich“). Durch das Wissen der grundlegenden Konzepte der symmetrischen Verschlüsselung erhalten die Lernenden Zugang zur Notwendigkeit asymmetrischer Verfahren, welche in einer Folgestunde thematisiert werden. Nach Behandlung der asymmetrischen Verschlüsselung haben die Lernenden somit Grundlagenwissen erlangt, mit dessen Hilfe sie gegenwärtig Informationen vertraulich in der digitalen Welt versenden und empfangen können. Es wird also ein Betrag geleistet Datensicherheit im privaten Bereich herzustellen.

Bezugnehmend auf die Ziele des Informatikunterrichts der Klasse 10 leistet diese Stunde einen Beitrag zu den folgenden Forderungen.

- DARSTELLEN UND INTERPRETIEREN → „Sie nutzen Informatiksysteme [...] zum Wissenserwerb und interpretieren die Ergebnisse hinsichtlich ihrer Plausibilität und Bedeutung“

Die Lernenden erarbeiten sich Wissen anhand moderner Informatiksystem-gestützter Medien (H5P-Inhalte). In der angeschlossenen Diskussionsphase kann dieses Wissen im Kontext weiterer Verschlüsselungsverfahren interpretiert werden. Die Plausibilität und Bedeutung moderner Verschlüsselungsverfahren wird hervorgehoben.

- KOMMUNIZIEREN UND KOOPERIEREN → „Die Schüler arbeiten kooperativ und kollaborativ mit anderen Schülern zusammen. Sie diskutieren aktuelle Tendenzen der Entwicklung von Informatiksystemen sowie deren Einfluss auf die Gesellschaft. Die Schüler nehmen ihr Recht auf informationelle Selbstbestimmung wahr.“

Einordnung zu den Kryptografiemethoden (MR)

Kryptografiemethoden allgemein stehen im hier zugrundeliegenden Lehrplanentwurf nahezu mit jedem Schuljahr in Kontakt. Beginnend in Klassenstufe 7 LB1: Informatik im Alltag. Hier kann direkt auf die Lebenswelt der Lernenden eingegangen werden und diverse Messenger, soziale Netzwerke und eine Vielzahl an mobilen Applikationen bezüglich der Sicherheit und der Transport von Daten besprochen werden. Die Techniken dazu werden gleichwohl vorerst zurückgehalten. Nichtsdestotrotz kann man Lernenden dieser Klassenstufe durchaus zutrauen erste Überlegungen diesbezüglich anzustellen.

Auch in Klassenstufe 8 LB1: Algorithmen und Programme kann ein Bezug hergestellt werden. Im Lernbereich werden den Lernenden grundlegende informatischen Strukturen und Vorgänge nähergebracht. Hier kann angeknüpft werden, um zu verdeutlichen, dass es mittlerweile keiner Menschen mehr bedarf, um Transport und Sicherheit der Daten zu gewährleisten.

In Klassenstufe 9 bieten sich gleich mehrere Lernbereiche zur Verknüpfung an. Lernbereich 1: Informationen und Daten sowie Lernbereich 2: Netzwerke in der Informatik bieten im Pflichtteil natürlich eine direkte Korrelation. Hier ist es ein Leichtes Verbindungen über den Aufbau von Daten und die Wirkungsweise von Netzwerken hin zur Kryptografie zu ziehen.

In Klassenstufe 10 werden dann im LB1: Informatik und Gesellschaft durch einen diskussions-lastigen Bereich die Notwendigkeit für Kryptografiemethoden erörtert und der Übergang zum hier vorgestellten Modul gezogen.

Einordnung zur Caesar-Verschlüsselung (KK)

Bei der Hinführung zur Methode „Caesar-Verschlüsselung“ über deren geschichtlichen Kontext werden Inhalte des Lehrplan Geschichte der Klasse 6 (Lernbereich 1 „Rom auf dem Weg zur Weltmacht“ → „Einblicke Gewinnen in wichtige Stationen der Entstehung des römischen Imperiums“) aufgegriffen. Da Lernende der Klassenstufe 10 die Option auf eine mündliche Prüfung im Fach Geschichte haben, kann im Lernelement eine Wissensauffrischung im Sinne der Prüfungsvorbereitung angestoßen werden. Für Lernende, welche keine Geschichtsprüfung ablegen werden, kann der historische Einblick eine Auffrischung des Allgemeinwissens darstellen.

Da nur sehr banale mathematische Fähigkeiten notwendig sind, um die Caesar-Verschlüsselung zu verstehen und anzuwenden, finden sich keine wirklichen

Anknüpfungspunkte zum Fach Mathematik. Lediglich interessierten Lernenden kann hier ein Hinweis zum Modulo-Operator und den Restklassen gegeben werden.

Als Lehrplan-unabhängiger Anknüpfungspunkt, also ein Anknüpfungspunkt eher intrinsischer Natur, können hier unter Lernenden vor allem kleinerer Klassenstufen (Klassenstufe 3 bis 6) verbreitete Geheimschriften sein, welche sie einsetzen, um Informationen für Lehrpersonal oder Mitschülern und Mitschülerinnen unzugänglich zu machen. Diese Geheimschriften zeigen häufig deutliche Parallelen zur Cäsar-Verschlüsselung (Ist es denn nicht schön zu sehen, dass einst Staatsmänner Methoden nutzten, welche heute bereits ein Teenager beherrscht?).

Über das Angebot weiterführender Informationen können Anreize für interessierte Lernende geschaffen werden, sich tiefergehend mit den Inhalten der Kryptografie auseinanderzusetzen.

BILDUNGSSTANDARDS DER GI (KK)

In den hier vorgestellten Lernsequenzen werden verschiedene Prozess- und Inhaltsbereiche der Bildungsstandards der Gesellschaft für Informatik aufgegriffen. Analog der Lehrplanforderung nach „Kommunikation und Kooperation“ wird mit gleicher Begründung der ebenso benannte Prozessbereich „Kommunizieren und Kooperieren“ bedient.

In der Diskussion der in den Expertengruppen erarbeiteten Wissensblöcken kann auch der Prozessbereich „Begründen und Bewerten“ bedient werden, da die Lernenden erarbeitetes Wissen bewerten müssen, um schließlich die Notwendigkeit asymmetrische Verschlüsselungsverfahren begründen zu können.

Auch Kompetenzen verschiedener Inhaltsbereiche werden gefördert. Offensichtlich wird ein Beitrag zum Inhaltsbereich „Informatik, Mensch und Gesellschaft“ geleistet. Es werden Verfahren thematisiert, welche für einen sicheren Umgang in der digitalen Welt unumgänglich sind.

Da nur ein sicherer Umgang mit digitalen Inhalten einen zielgereichten Umgang mit Informatiksystemen ermöglicht, kann auch der Inhaltsbereich „Informatiksysteme“ unterstützend bedient werden.

ÜBERBLICK ÜBER DAS MODUL

Überblick zum Modul (KK)

Im hier vorgestellten Modul wird der grobe Ablauf der Lernbereiche 1 „Informatik und Gesellschaft“ und 2 „Kryptografie“ der Klassenstufe 10 skizziert (nach Lehrplanentwurf März 2021). Zur Bearbeitung des Moduls werden insgesamt 16 Unterrichtsstunden benötigt, wobei 2 Stunden für Leistungsüberprüfungen reserviert wurden. Beide Lernbereiche sind inhaltlich stark miteinander verknüpft. Im Lernbereich 1 werden vor allem Auswirkungen der immer stärker voranschreitenden Digitalisierung thematisiert. Der Lernbereich 2 wiederum behandelt verschiedene Verfahren der Kryptografie, durch welche eine sichere Datenübertragung in der digitalen Welt ermöglicht wird. Die Lernbereiche wurden daher ineinander verzahnt. Das bedeutet nachdem in Stunde 3 Datensicherheit thematisiert wird, folgt ein kurzer Ausblick in den Lernbereich 2, welcher einen Einblick in die Kryptografie gewährt. Anschließend wird der Lernbereich 1 fortgeführt. Den Lernenden werden damit Konzepte vorgestellt, welche eine sichere Datenübertragung vorgestell, bevor die Auswirkungen der Digitalisierung auf Beruf- und Privatleben thematisiert werden. Damit kann eine sinnvolle Diskussionsbasis geschaffen werden. Eventuell vorhandene Ängste vor der digitalen Welt können abgebaut werden. Der grobe Ablauf des Moduls ist in Tabelle 1 dargestellt.

Tabelle 1 - grober Ablaufplan des Moduls

Lernbereich	Inhaltsbeschreibung	Stundenumfang
1	Datensammlung und Datensicherheit	3
2	Einführung in die Kryptografie	1
1	Auswirkung der Digitalisierung auf Wirtschaft, Beruf und das Privatleben	6
	Leistungsermittlung	1
2	Ziele und Verfahren der Kryptografie	5
	Leistungsermittlung	1
	Anwendung kryptografischer Verfahren auf konkrete Anwendungsbeispiele	1

Die Gestaltung des Lernbereiches 1 beschränkt sich in diesem Modulhandbuch jedoch auf eine Ideensammlung, welche mit zahlreichen Methoden- und Toolvorschlägen untermauert wurde. So erhalten Lehrende die Ideenanstöße, welche dann auf die konkrete Lerngruppe zugeschnitten werden können.

Detaillierter ist hier der Lernbereich 2 beschrieben. In sechs Unterrichtsstunden werden Ziele, Methoden und konkrete Anwendungen der Kryptografie vorgestellt. Hauptaugenmerk liegt dabei auf den Kernstunden 12 und 13, in denen im Rahmen eines Gruppenpuzzles und anschließender Diskussion mit der gesamten Lerngruppe konkrete symmetrische Verfahren der Kryptografie von den Lernenden erarbeitet und beispielhaft angewendet werden. Diese sehr Lernenden-zentrierten Kernstunden werden im Folgenden ausführlich beschrieben. Darauf aufbauend soll in der Folgestunde das Prinzip der asymmetrischen Verschlüsselung erarbeitet werden. Eine Leistungsüberprüfung und die Anwendung des Wissens um die Kryptografie an realen Anwendungsbeispielen, wie Dokumenten- oder E-Mail-Verschlüsselung schließen den Lernbereich 2 ab.

Es folgt eine kurze Beschreibung der einzelnen Lernelemente der Kernstunden.

Überblick zum Lernelement zur Cäsar-Verschlüsselung (KK)

Im hier vorliegenden H5P-Lernelement zur Cäsar-Verschlüsselung erhalten Lernende die Möglichkeit sich selbstständig die zum Verständnis notwendigen Fakten zu erarbeiten und diese anzuwenden. Durch ein begleitendes Arbeitsblatt können die Ergebnisse gesichert werden, um sie nach Abschluss des Lernelementes auch an Mitschülern und Mitschülerinnen weiterzugeben. Das Arbeitsblatt selbst liefert Hinweise an welchen Stellen der Präsentation wichtige Inhalte behandelt werden.

Die interaktive Präsentation liefert den Lernenden auf den ersten Folien einen kurzen geschichtlichen Rückblick zur Zeit der Entstehung des Verschlüsselungsverfahrens. Dazu lesen die Schüler und Schülerinnen einen kurzen Fachtext und beantworten anschließend kurze Fragen zu diesem. Im Zuge dieser Wissensabfrage, werden die Lernenden mit den Grundlegenden Aufgabentypen der späteren Übungssequenz vertraut gemacht.

Nach dem der geschichtliche Kontext behandelt wurde, werden die Lernenden in einer kurzen Einheit mit Grundbegriffen der Kryptografie vertraut gemacht, um Missverständnisse beim Erarbeiten der Verschlüsselungsmethode nach Cäsar vorzubeugen.

Diese zentrale Erarbeitungsphase schließt sich unmittelbar an. Mittels kurzer Texte und erklärenden Abbildung kann sich der Lernende mit der Methode vertraut machen. Durch einfache konkrete Beispiele wird die Vorgehensweise verdeutlicht. Eine Wissensabfrage

stellt sicher, dass die Inhalte korrekt erarbeitet wurden. Diese Erarbeitungsphase abschließend werden verschiedenen digitale und analoge Hilfsmittel vorgestellt.

Es folgt eine Übungs- und Anwendungsphase. Hier sollten die Lernenden, die meiste Zeit investieren. In dieser Phase sollen Aufgaben verschiedenen Formats und Schwierigkeitsgrades gelöst werden. Bei einfachen Aufgaben können sie schnell unter Beweis stellen, dass sie das Verfahren verstanden haben. Schwierigere Aufgaben fordern die Lernenden zum Knobeln und vor allem zum sinnvollen Einsatz der gegebenen Hilfsmittel auf.

Das Lernelement wird durch Hinweise auf weiterführende Informationen zur Methode sowie den Verweis auf ähnliche historische Verschlüsselungsmethoden abgeschlossen. Nach einer automatisch generierten Auswertungsseite bezüglich der Bearbeiteten Übungsaufgaben ist das Lernelement abgeschlossen.

Überblick zum Einstellungstest (MR)

Die Eingangsfrage des Tests sowie die Gestaltung stimmen die Lernenden auf das im Konzept verankerte Agenten-Thema ein. Die Kategorisierung der Fragen stützt sich, wie in der fachlichen Analyse bereits erwähnt, auf die 4 Eingruppierungen in sprachgebundene, zahlengebundene, grafikgebundene Logikfragen sowie Aufgaben zur Abfrage des räumlichen Vorstellungsvermögens. Es werden Fragen unterschiedlicher Schwierigkeit pro Kategorie gestellt. Der zeitliche Rahmen für die Lösung des Einstellungstests ergibt eine weitere Anforderungsstufe. Dieser muss allerdings in Zukunft erst noch evaluiert werden, da bis zum Zeitpunkt der Abgabe dieser Arbeit kein Testlauf im realen Schulumfeld möglich war. Alle Aufgaben sind zu großen Teilen einheitlich als Single-Choice-Aufgabe gestellt, um die Lernenden nicht zusätzlich mit zu vielen unterschiedlichen Aufgabentypen zu verwirren. Alle Aufgaben sind entweder direkt oder in abgewandelter Form bereits veröffentlichten Logiktests entnommen, da diese bereits größtenteils sehr gut auf die angestrebten Ziele des Tests abgestimmt waren. Dieser Test bildet die erste Schülerhandlung ab in dem, des ganzen Moduls zu Grunde liegenden, Agenten-Frame.

Es ist angedacht eine automatisierte Zuordnung der Lernenden zu ihren Arbeitsgruppen auf Grundlage der erreichten Punkte in diesem Test umzusetzen. Dies war zum Zeitpunkt der Abgabe dieser Arbeit allerdings noch nicht möglich und wird nach erster Annäherung an das Thema auch zukünftig nicht ohne Weiteres umsetzbar sein. Der zur Umsetzung des Tests benutzte H5P Editor Lumi besitzt derzeit noch nicht die Möglichkeit Testergebnisse der Gestalt auszuwerten, als dass die angestrebte Auswertung bzw. Zuordnung aufgrund der Ergebnisse automatisiert möglich wäre.

Überblick zum Lernelement „Grundbegriffe“ (MR)

Das hier vorliegende H5P Element zu den Grundbegriffen der Kryptografie ist, wie bereits erwähnt, zwar als eigenständiges Modul entworfen und erstellt worden, ist aber aus nachvollziehbaren Gründen den jeweiligen Modulen zu den verschiedenen Verfahren vorgeschaltet, um für alle Lernenden eine einheitliche Grundlage zur Erarbeitung zu schaffen. Diese Arbeitsweise unterstreicht den modularen und flexiblen Charakter dieses Gesamtmoduls und erlaubt an nahezu allen Stellen ein schnelles, unkompliziertes Anpassen der einzelnen Lernelemente an sich verändernde Bedingungen. Im Grundbegriffe-Element werden zunächst Fehlvorstellungen und Risiken zu Fehlinterpretationen ausgeräumt, indem die fachlich korrekte Bedeutung aller Begriffe kleinschrittig und anschaulich erarbeitet und erklärt werden. Schaubilder mit den Begriffen und passenden Piktogrammen zu den gesamten Vorgängen der Ent- und Verschlüsselung runden die Erarbeitung ab. Anschließend werden alle Begriffe in einer Zuordnungsaufgabe nochmals aufgegriffen und somit gefestigt.

Zusätzlich und als Ergänzung bzw. Differenzierung gedacht, wurde ein weiteres Mini-Lernelement zu den Grundbegriffen erstellt. Hier müssen die Lernenden aus einem „Buchstabensalat“ gegebene Begriffe herausuchen und markieren. Zusätzlich zum Grundmodul werden hier die Begriffe durch die Synonyme Chiffre, chiffrieren und dechiffrieren sowie um das Wort symmetrisch erweitert.

Überblick zum Lernelement zur Vigenere-Verschlüsselung (MR)

Dieses Modul ist zum Zeitpunkt der Abgabe noch nicht vollständig in H5P umgesetzt. Hier wurden zur allgemeinen Arbeitserleichterung Parallelen zur Semesterarbeit im Kurs „Projektmanagement SoSe 2021“ gezogen. Dort wurde das Modul bereits auf Grundlage des ONYX-Editors umgesetzt. Es beinhaltet Aufgaben der Kategorien Drag&Drop (Zuordnung) und Textbox (Mehrfachauswahl vorgegebener Lösungsworte) in drei verschiedenen Schwierigkeitsstufen. Um eine homogene Arbeitsumgebung für die Lernenden zu schaffen, muss dies Modul passend zu den anderen, hier vorgestellten Modulen in H5P umgesetzt werden.

EINBETTUNG IN DEN SCHULUNTERRICHT

VORAUSSETZUNGEN (MR)

Die gewählte Methode des Gruppenpuzzles ist den Lernenden in Klassenstufe 10 bekannt. Es ist davon auszugehen, dass auch außerhalb des Informatikunterrichtes diese Methode mehrfach zum Einsatz gekommen ist. Sie ist aus unserer Sicht an dieser Stelle besonders geeignet, da durch den geplanten Ablauf und die vorgeschalteten Fragen, diskutierten Sachverhalte und Problemstellungen eine gesteigerte Motivation erreicht wurde und die Lernenden über diese Methode ein erhöhtes Maß an Aktivität und effektiver Lernzeit erreichen können.

Fachliche Vorkenntnisse bieten hier die direkte Vorstufe zu den Zielen der Kryptografie. Anderweitige Vorkenntnisse sind aufgrund der Einfachheit der hier vorgestellten Verfahren aus Sicht der Autoren nicht erforderlich. Abgesehen von grundlegenden mathematischen Rechenfertigkeiten ist kein fachfremdes Wissen zur Bearbeitung des hier beschriebenen Moduls notwendig. Gleichwohl sollte die Notwendigkeit diverser Ver- und Entschlüsselungsverfahren im vorangegangenen, diskussions-lastigen und hier in Teilen vorgestellten LB10/1: Informatik und Gesellschaft in den Vordergrund gestellt werden und damit die Motivation der Lernenden sich mit diesen Verfahren auseinander zu setzen gesteigert werden.

NACHHALTIGKEIT (MR)

Abgesehen von wenigen, kompakten Arbeitsblättern ist die Erarbeitung der gewählten Kryptografieverfahren rein digital. Einzig die Sicherung und kleine Teile der Übung erfolgen noch klassisch und schonen somit Ressourcen.

Nachhaltigkeit im Sinne der Arbeitszeit der Lehrperson ist aufgrund des offenen und modularen Konzeptes ebenfalls gegeben. Die Gruppenaufteilung und die Menge an Verfahren kann nahezu stufenlos an die gegebene Lerngruppenstärke angepasst werden. Vor- und Nachbereitung fallen somit sehr effizient aus.

Auch im Hinblick auf eine eventuell erneute häusliche Lernzeit ist dieses Modul besonders geeignet. Hier kann durch eine oder mehrere einleitende Videokonferenzen der Ablauf des Moduls im Vergleich zur schulischen Bearbeitung nahezu beibehalten werden. Durch die Bereitstellung der H5P-Elemente als html-Export können den Lernenden diese barrierefrei zur Verfügung gestellt werden. So ist eine Bearbeitung mit nahezu jedem Endgerät auf Seiten der Lernenden ohne weiteres möglich.

STOFFVERTEILUNGSPLAN UND STUNDENPLANUNG

Stoffverteilungsplan

Schulform	Oberschule
Klassenstufe	10
Lernbereich Nr.	1 + 2
Lernbereich Name	„Informatik und Gesellschaft“ + „Kryptografie“
Autoren	Thomas Oelsner, Kurt Kunze, Matthias Rothe
Bemerkung	Große Teile des LB1 (digitaler Fußabdruck + Wirtschaft) bedingen die Notwendigkeit der Behandlung des LB2 (Kryptografie). Daher ist es sinnvoll die Lernbereiche miteinander zu verknüpfen. Die Stunde 4, welche zum LB2 zählt, wurde daher in den LB 1 vorgezogen.

Abkürzungsverzeichnis

EA	Einzelarbeit
GA	Gruppenarbeit
HA	Hausaufgabe
LB	Lernbereich
LK	Leistungskontrolle
LV	Lehrervortrag
PA	Partnerarbeit
SJ	Schuljahr
Std.	Stunde
SuS	Schüler und Schülerinnen
SV	Schülervortrag
UG	Unterrichtsgespräch
Verschl.	Verschlüsselung
WDH	Wiederholung

Std.	Stundenthema	Lernziel (SuS...)	Inhalt	Fachbegriffe	Materialien / Ideen
1	Kennen der gesellschaftlichen Bedeutung der Informatik	... können Inhalte der letzten Schuljahre benennen, diese einordnen und hinsichtlich ihrer Alltagsrelevanz analysieren.	- Rückblick der SJ 5 bis 9 (4 Gruppen: 5-6, 7, 8, 9) - GA (Mindmap mittels kollaborativem Dokument) - gemeinsame Auswertung (Alltagsrelevanz HEUTE) - HA: „reflektiere die Relevanz des bisher erworbenen Wissens in Zukunft (privat und Beruf)“		- Vokabelliste der Schuljahre 5-9 - (digitale) Hefter der Vorjahre - kollaboratives Mindmap-Tool (z.B. Miro oder Padlet)
2	Datensammlung und Datenspeicherung	... können die Notwendigkeit redundanter Datensicherung ableiten. ... kennen Strategien zur redundanten Datenspeicherung.	- Szenario, Rechnerabsturz in der Prüfungsvorbereitung nach Corona-geprägter digitaler Lernzeit - 3-2-1-Regel (3 Kopien, 2 Datenträgertypen, 1ne Kopie außer Haus) (Recherche) - Weitere einfache Regel zur red. Speicherung (SV/LV) - Clouddienste	Backupstrategien, redundante Speicherung (Home-)Cloud Spezialwissen: RAID-verbund	- Rollenspiel - Filmsequenz (Trancendence - Jonny Depp)

3	Datensicherheit (Gläserner Mensch, Datenschutz, Passwortsicherheit)	... können anhand versch. Beispiele die Notwendigkeit der Datensicherheit erläutern.	- Datensicherheit - wozu? - Szenario Rechner Diebstahl oder Daten Hack (UG) - Welche Daten gebe ich auch so Preis? (Kleingruppen-/PA) - Wie erstelle ich sichere Passwörter (Textarbeit/EA) - Welche anderen Möglichkeiten habe ich meine Daten zu schützen? (Kleingruppen-PA) - An wen kann ich mich wenden, wenn ich Opfer bin? (LV)	Einverständnis-erklärung zur Datenspeicherung Datenschutz-gesetze	- Soziale Medien - Passwortmanager - Onlinetool zur Passwortsicherheit https://checkdeinpasswort.de/ - Phishing-Quiz: https://phishingquiz.withgoogle.com/
4	Einführung in die Kryptografie	... kennen die Begriffe Codieren, Verschlüsseln und Kryptografie	- Wie kann ich die Risiken mindern? - Erfahrungen der Lernenden zu Verschlüsselung erfassen - Beispiel für Notwendigkeit der Kryptografie sammeln - Verstecken von Informationen (Steganographie)	Codieren/ Verschlüsseln Kryptographie	- Erinnerung an Geheimschriften (5./6. Klasse) - Historische Entwicklung - Steganographie-Tools: online: https://www.geocachingtoolbox.com/index.php?lang=de&page=steganography - open-source: https://www.stegano.org/

5	Digitaler Fingerabdruck	...können die Datennutzung der soz. Medien einschätzen.	- Eingangsbeispiel Freimaurer-Alphabet - Wer hat (so wie so) auch ohne Hack/Diebstahl Zugriff auf meine Daten? - Was kann ich dagegen tun? - Was gebe ich preis? (Erklär-Filmchen mit anschließender Erarbeitung der Fachbegriffe -> Handbuch digitaler Fingerabdruck)	Cookies, Standortdaten, GPS, Standort via Einwahlpunkt,	https://www.onlinesicherheit.gv.at/Themen/Gefahren-im-Netz/Privatsphaere/Digitaler-Fingerabdruck.html
6	Zu Auswirkungen der automatisierten Generierung von Daten positionieren	...können Schlüsse über den Nutzen der Datenerhebung der Unternehmen ziehen.	- Sind es wirklich Menschen, die diese Daten sammeln und auswerten? - Mit welchem Interesse werden diese Daten gesammelt und ausgewertet? (LV/UG → Einfache Auswerte-Algorithmen schreiben)	Automatisierung WDH Algorithmen	- Seiten-Nutzungsstatistiken auswerten → Rückschlüsse auf verschiedene Homepagedesigns - Einfache Datensätze
7	Auswirkungen der Digitalisierung im privaten Bereich	...erkennen Vor- und Nachteile der Digitalisierung und können das eigene Verhalten dahingehend analysieren.	- Alltagserfahrungen der SuS sammeln (vorbereitende Hausaufgabe) - positive und negative Beispiel Stationsarbeit zu Einzelszenarien	Social Media SMART-Home Internet- und Medienabhängigkeit blended learning	- social-media - Film „The Circle“ - entertainment-Plattformen - Smart-Home - Messenger-Portale (→ Klassenchat) - Cybermobbing/ Homeschooling/ blended learning

8	Auswirkungen der Digitalisierung in der Wirtschaft	...erkennen Vor- und Nachteile der Digitalisierung und können Risiken einschätzen.	- Wie würde unser Leben aussehen, ohne Informatiksysteme? (UG/Planspiel, „heute ohne Informatiksysteme“) - Berufsbilder für die informatische Grundkenntnisse nötig sind (Recherche in EA →Gruppen-Mindmap)	globale Arbeitsteilung	- Beispiel Bestellung bei großem Warenhändler mit Expressversand - blended learning auch in der Berufswelt (Fort-/Ausbildung)
9	Auswirkung der Digitalisierung beurteilen	... diskutieren die Auswirkungen der Digitalisierung im eigenen Alltag, in dem sie Vor- und Nachteile zu konkreten Alltagserfahrungen benennen.	- Resümee, ob ich trotz der in den Vorstunden diskutierten Bedenken auf Informatiksysteme und die damit verbundenen Risiken verzichten möchte? Chancen vs. Risiken	Internet der Dinge Anschluss an Std. 3 und 7 (Cyberkriminalität)	- Elektronische Krankenakte - Elektronische Behördengänge - „Wikipedia“ u.a. digitale Nachschlagewerke und andere digitale Lernhelfer - Zeitmanagement
10	LK Positionierung in der digitalen Welt		- Stellungnahme zu gegebenem Beispiel. - Nennen und begründen eigener Handlungsoptionen		

11	Vertiefung Kryptografie	...kennen den die Ziele der Kryptografie, indem sie diese anhand eines konkreten Beispiels erläutern	Ziele der Kryptographie - Verschiedene Beispiele aus Realwelt und digitaler Welt	Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit	Anschluss an Stunde 4 Bsp.: Brief vs. Mailverkehr oder Paket vs. Datenübertragung (analog Übung AWS Datenübertragung mit Fokus auf Zielen der Kryptografie)
12/ 13	Ausgewählte Methoden de Kryptografie	...können symmetrische Verschlüsselung anwenden, indem sie mittels ausgewählter Verfahren Nachrichten ver-/ entschlüsseln. ...beurteilen symmetrische Verfahren, indem sie Vor- und Nachteile benennen.	- symmetrische Verfahren Gruppenpuzzle, EA/PA) → Cäsar → Gartenzaun → Vigenere → Fackeltelegraph	symmetrische Verschlüsselung Schlüssel Verschlüsseln Entschlüsseln Klartext Geheimtext Transposition Substitution	- CAESAR-Tabelle/-Scheibe (analog, digital) online: https://www.kryptowissen.de/caesar-chiffre-praxis.php - Geheimbotschaften mittels Cesar-Scheibe austauschen -- Tools und Informationen: https://www.cryptool.org/de/cto/
14	Asymmetrische Verschlüsselung	...können asymmetrische Verschl. anhand des Bob-Alice-	Prinzip asym. Verschl. mit BOB und ALICE	asym. Verschlüsselung privater und öffentlicher Schlüssel	- Erklär-Film RSA : https://studyflix.de/informatik/rsa-verschlüsselung-1608

		Models erklären.			
15	LK Kryptografie		- Ablauf Verschlüsselung - Fachbegriffe - Bob-Alice-Modell (asym. Verschl.)		
16	Anwendungsbeispiele	...erhalten Einblick in reale Anwendungen der Kryptografie	- HTTPS (<u>vor</u> Login verschl.) - Emails - Office-Dokumente - Messenger	HTTPS PGP Ende-zu-Ende Verschl.	

Geplanter Stundenverlauf

Kurs:	Klasse 10 Informatik	Lernziel:	Die SuS lernen verschiedene symmetrische Verschlüsselungsverfahren kennen und können diese auf vorgegebene Übungsaufgaben anwenden.
Schulstunde in der Reihe:	Verfahren der Kryptografie	Teillernziele:	Die SuS • Die SuS wenden Verschlüsselungsmethoden wie CAESAR, Gartenzauntransposition, Fackeltelegraph, ... auf kurze Wörter an ... • Die SuS beurteilen die Sicherheit symmetrischer Verfahren
Thema der Stunde:	Methoden der symmetrischen Kryptographie		

Zeit	Phase	Inhalt	Sozial-form	Medien	Materialien	Vorwissen	Intendierter Lernprozess
10'	Motivation	Ihr seid Agenten und müsst geheime Botschaften austauschen. Bevor ihr das Handwerkszeug dazu lernt, müsst ihr euch einem Einstellungstest unterziehen.	EA	PC	Einstellungstest	-	Die SuS machen kleine Logikrätsel. Diese dienen der geistigen Aufwärmung und der Lehrkraft als Auswahl für die Gruppenzusammenstellung
5'		Gruppenbildung Lehrkraft stellt sicher, dass in jeder Gruppe ein*e Lernende*r sitzt, der im Einstellungstest gut- oder sehr gut abgeschnitten hat.	UG		Skatblatt 16 Karten, 4 x (Bube, Dame, König, Ass)	-	-

20'	Erarbeitung	Gruppenpuzzle Alle B, D, K, A setzen sich in ihre Stammgruppen zu einem Verschlüsselungsverfahren und lösen eine Testaufgabe	GA		Spezifisches Material zu den Verfahren „Agentenframe beibehalten“		Erarbeitung von Fachbegriffen (Klartext, Geheimtext, Schlüssel, verschlüsseln, entschlüsseln) Selbständige Erarbeitung der Verfahren, dann Austausch Buben = CAESAR Damen = Fackeltelegraph Könige = Gartenzauntransposition Asse = Vigenere
20'		Experten setzen sich nach Farbe (Karo, Herz, Pik, Kreuz) zusammen und erklären ihr Verfahren der Reihe nach an Beispielaufgaben.	GA				Lernende können erworbenes Wissen mit eigenen Worten erklären.
20'	Sicherung	Freiarbeit in Gruppen mit vermischten Aufgaben. SuS lösen von der Gruppe erstellte Aufgaben.	GA		Aufgaben der SuS		Damit das im Gruppenpuzzle erlernte geübt werden kann, dürfen die SuS noch einmal verschiedene Aufgaben mit unt. Schwierigkeitsgrad bearbeiten.
10'	Erarbeitung	Diskussion/Beiträge zu Sicherheit symmetrischer Verfahren (Provokation: Würdest du dein Messenger-Verkehr CAESAR verschlüsseln?)	UG				Lernende reflektieren Ergebnisse des Gruppenpuzzles inhaltlich hinsichtlich der Alltagstauglichkeit symmetrischer Verfahren

5'	Sicherung	Vor- und Nachteile symmetrischer Verfahren	PA		https://www.datenschutzzentrum.de/artikel/1099-Symmetrische-und-asymmetrische-Verschluesselung.html		Lernende erarbeiten in Textarbeit Vor- und Nachteile
----	-----------	--	----	--	---	--	--

Abkürzungsverzeichnis

EA	Erarbeitung
GA	Gruppenarbeit
PA	Partnerarbeit
SuS	Schüler und Schülerinnen

VORSTELLUNG DER VERWENDETEN UND ERZEUGTEN TOOLS

Der H5P-Editor von Lumi (TO)

H5P ist ein Plugin, mit dem man interaktive Inhalte erstellen kann, z.B. interaktive Videos, Präsentationen, Spiele, Quizze usw. Um diese zu erstellen, eignet sich das deutschsprachige Desktop-Programm LUMI, welches auf <https://lumi.education/#download> heruntergeladen werden kann. Es erfordert keine Programmierkenntnisse, die Oberfläche ist übersichtlich und der Einstieg leicht gemacht. Nach ein paar Klicks kann man aus ca. 50 Möglichkeiten auswählen, ein Lernmodul zu entwerfen (Abbildung 4: Screenshot Inhaltsauswahl). Die Caesar-Lerneinheit und die Erarbeitung der Grundbegriffe der Kryptografie wurden auf Grundlage der „interaktiven Präsentation“ entworfen, das Lernmodul Gartenzauntransposition auf Grundlage des „interaktiven Buches“ und der Einstellungstest wurde als Quiz im Rahmen der Vorlagen entworfen. Auf den Folien bzw. Seiten können dann Texte, Bilder, Videos etc. mit verschiedenen Aufgabentypen, z.B. Lückentexte, Drag-and-Drop-Aufgaben, Multiple Choice und viele mehr, kombiniert werden, sodass ein Wechsel zwischen Lerninput, Schüleroutput und dazugehörigem Feedback gestaltet werden kann. Inhalte können anschließend modular hinzugefügt und an die richtige Stelle geschoben werden. Eine Hilfe und Tutorials kann man vom Programm aus anklicken und wird von da aus auf die englischsprachigen Unterseiten der Homepage <https://h5p.org/> im Webbrowser verlinkt. Sehr komfortabel ist, dass zwischen einer Vorschauansicht und der Bearbeitungsansicht (Abbildung 5) mit einem Mausklick umgeschaltet werden kann. Die Inhalte lassen sich dann als HTML-Datei exportieren und können lokal gespeichert und im Webbrowser geöffnet werden. Zu bemängeln ist, dass es bei einigen Kollegen des Öffterers zum Absturz kam. Als Alternative gibt es die Plattform OPAL, die die Erstellung ganz ähnlicher Inhalte unterstützt. Ein klarer Nachteil von OPAL ist, dass man dafür registriert sein muss und für LUMI nicht und dass die gemeinsame Bearbeitung von Lerninhalten der Vergabe von speziellen Rechten bedarf.

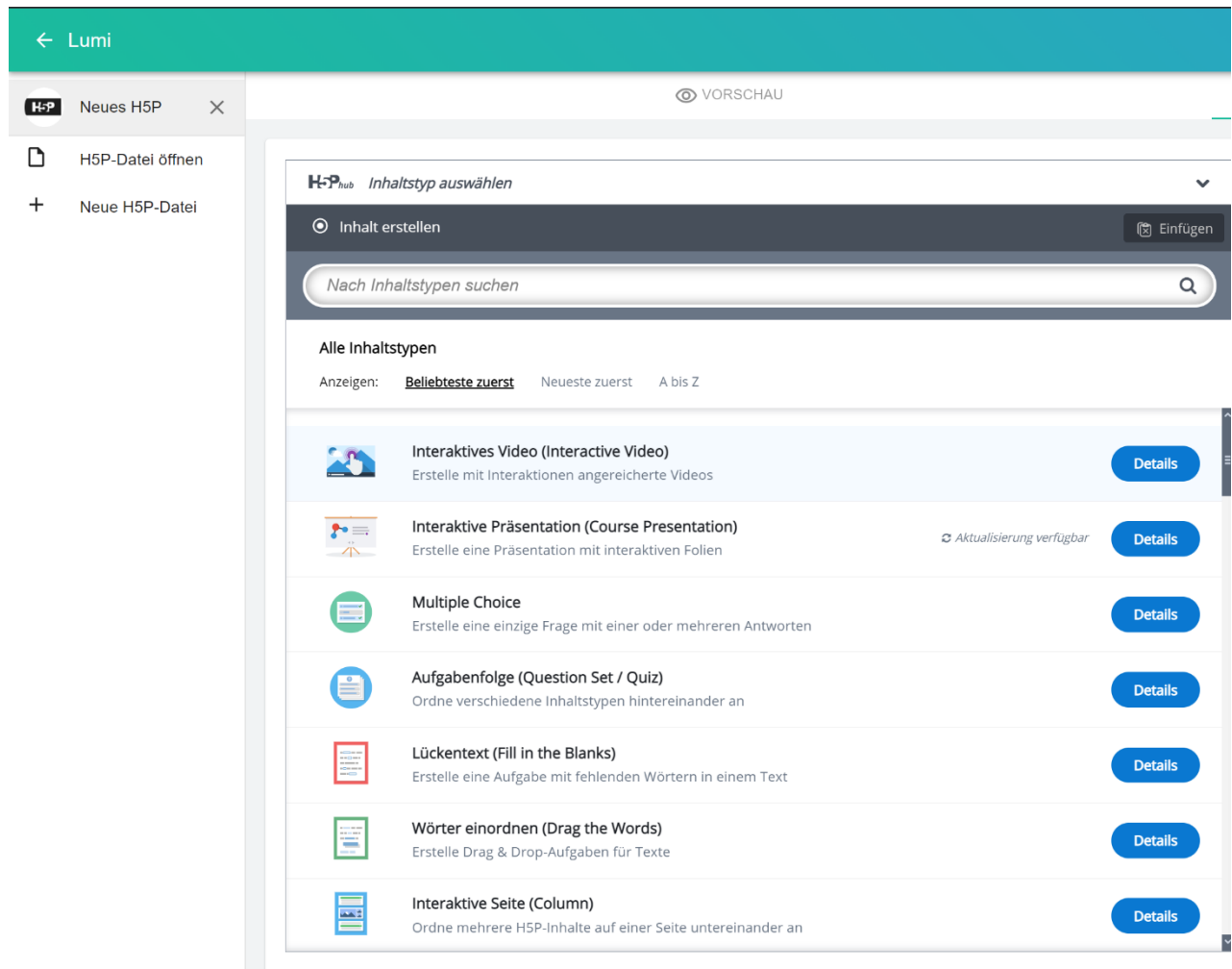


Abbildung 4: Screenshot Inhaltsauswahl

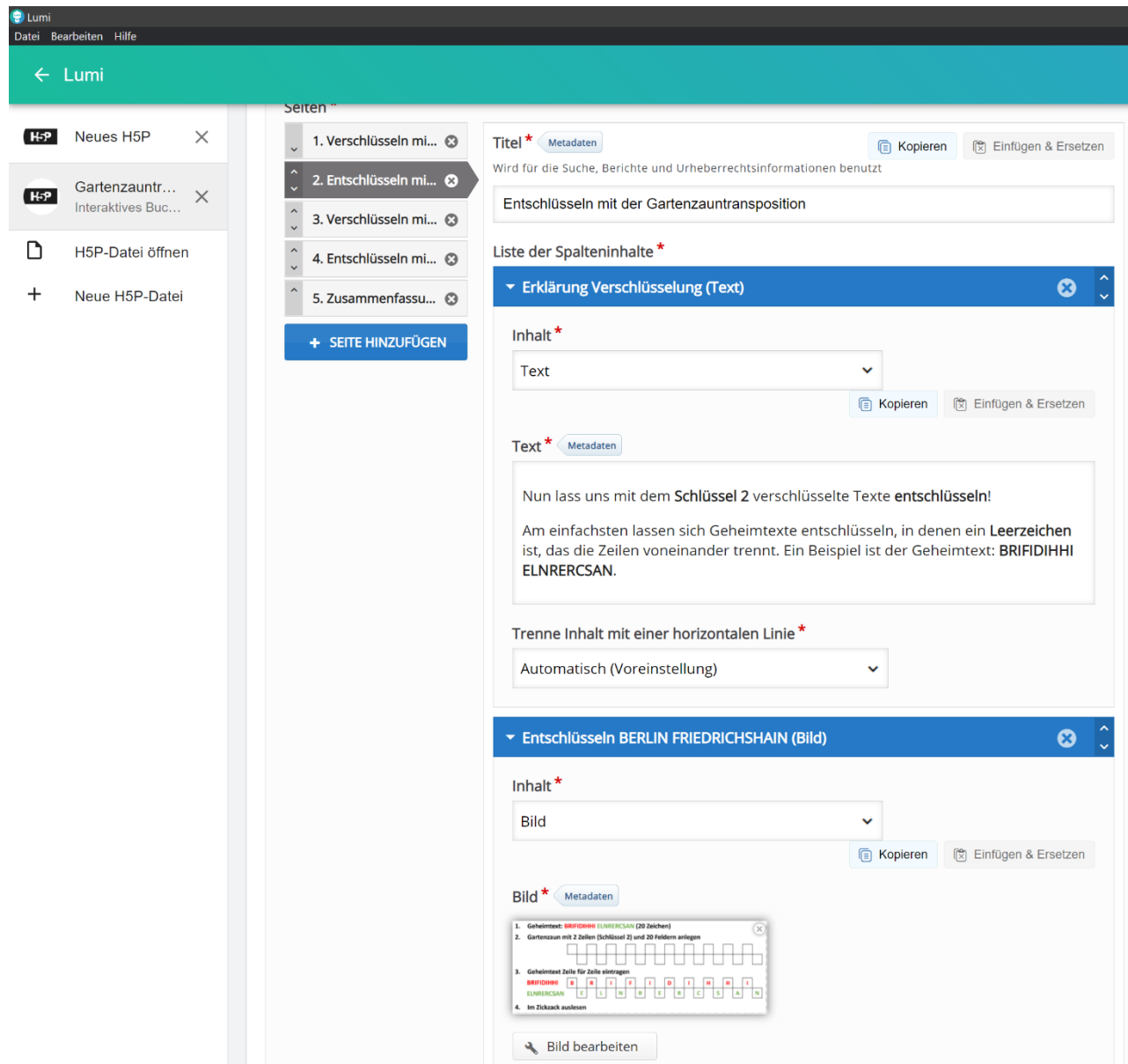


Abbildung 5: Bearbeitungsansicht eines "interaktiven Buches" in LUMI

Interaktive H5P-Präsentation zur Cäsar-Verschlüsselung (KK)

Wie im einleitenden Text beschrieben, kam auch hier die für das digitale Lernelement zur Cäsar-Verschlüsselung der H5P-Editor Lumi zum Einsatz. Für das Lernelement, welches nun vorgestellt wird, wurde das Format „interaktive Präsentation“ gewählt.

Das erstellte Lernelement umfasst 25 Folien, welche den Lernenden das Verfahren der Cäsar-Verschlüsselung erklärt und Übungsaufgaben zum erlernten Verfahren anbietet. Die Navigation durch die Präsentation sollte durch die eingefügten **weiter**-Schaltflächen erfolgen.

Die **Folien 1 bis 4** führen Lernende in den historischen Kontext um Julius Cäsar ein. Dabei wird der Lernende auf den Folien 1 und 2 mit einem Bild des römischen Feldherrn und Politikers empfangen. Durch kurze Texte wird er darauf aufmerksam gemacht, dass das Verschlüsselungsverfahren tatsächlich nach der berühmten historischen Person benannt wurde. Ab der Folie 3 gelangt der Lernende nun durch Anklicken eines Infobuttons (i) zu einem kurzen Text zur Vita Julius Cäsars. Auf Folie 4 (s. Abbildung 6) werden dann die in der interaktiven Präsentation verwendeten Aufgabentypen vorgestellt. Die Aufgabentypen Single-Choice (👉, *die richtige Antwort anklicken*), Drag-and-Drop (👉, *das Lösungswort an die richtige Stelle des Lückentextes ziehen*) sowie ein Lückentext (👉, *per Eingabe das Lösungswort in eine Lücke eintragen*) befassen sich dabei zunächst mit Inhalten des auf Folie 3 gelesenen Textes. Das Infosymbol zum erneuten Nachlesen ist weiterhin anklickbar.

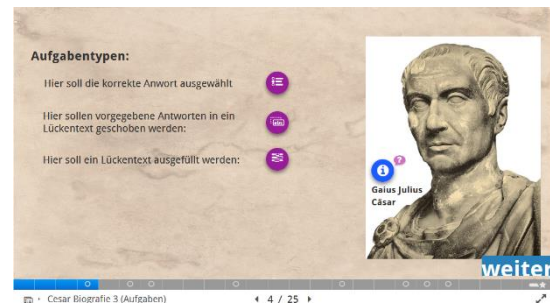


Abbildung 6 - Folie 4 - Cäsar-Verschlüsselung

Auf den **Folien 5 bis 11** wurde das Lernelement „Grundbegriffe der Kryptografie“ (Modul von Matthias) eingefügt. Dieses beinhaltet zwei Drag-and-Drop-Aufgaben (Folie 6 und 11), eine Ein-Lücken-Text-Aufgabe (Folie 7) sowie zwei erklärenden Textfolien (Folien 8 und 10).

Auf den **Folien 12 und 13** werden die Lernenden mit einer konstruierten Geheimbotschaft Cäsars an seinen Adoptivsohn Oktavian konfrontiert. Diese Botschaft kann durch Betätigen des **Umdrehen**-Buttons in einen Klartext übersetzt werden.

Die **Folien 14 bis 16** sollen den Lernenden den Ablauf der Cäsar-Verschlüsselung näherbringen. Folie 14 dient dabei der Erklärung des Verschlüsselungsverfahrens. Anhand einer kurzen 3-Punkte-Anleitung sowie zwei unterstützenden Abbildungen werden die, zuvor erlernten, Begriffe „Schlüssel“ sowie „Ver- und Entschlüsseln“ in den konkreten Kontext der Cäsar-Verschlüsselung gebracht. Zur weiteren Unterstützung des Verständnisses folgt Folie 15 (s. Abbildung 7), auf der je zwei einfache Beispiele zu den Schlüsseln 1 und 2 präsentiert werden. Durch Wählen des **Umdrehen**-Buttons kann erneut zwischen Geheimtext und Klartext umgeschaltet werden. Durch Auswahl des **>**-Symbols kann zwischen Schlüssel 1 und 2 gewählt werden. Durch Anklicken des **i**-Symbols wird eine Erklärung des Begriffes Substitutionsverfahren eingeblendet. Schließlich bietet die Folie 16 einen Drag-and-Drop-Lückentext, der den Lernenden zur Überprüfung des Wissenserwerbs dient.

Die **Folien 17 bis 21** zählen nun zum Übungsteil dieses Lernelements. Wobei auf Folie 18 zunächst noch zwei digitale Hilfsmittel erklärt werden. Zwei neue Buttons, welche für den gesamten Übungsteil anwählbar bleiben werden hier eingeführt. Das **🖼️**-Symbol führt die Lernenden zu einer Schlüsseltabelle. Das **🔗**-Symbol öffnet einen Link, nach dessen Anklicken eine digitale Cäsar-Scheibe in einem neuen Tab oder Fenster erscheint. Die Folie 19 (s. Abbildung 8) enthält Aufgaben zum Verschlüsseln von Klartexten bei einem gegebenen Schlüssel in Form einer Single-Choice-Aufgabe sowie einer Drag-and-Drop-Aufgabe. Folie 20 (s. Abbildung 9) fordert dann das Entschlüsseln von Geheimbotschaften bei gegebenen Schlüsseln. Dies geschieht durch eine Drag-and-Drop-Aufgabe und eine Lückentext-Aufgabe. Auf der Folie 21 (s. Abbildung 10) Herausfinden des Schlüssels gefordert. In Aufgabe a) ist der Klartext gegeben

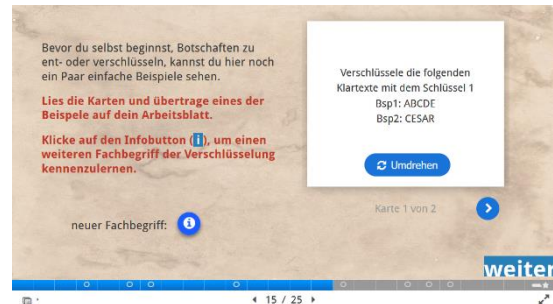


Abbildung 7 - Folie 15 - Cäsar-Verschlüsselung

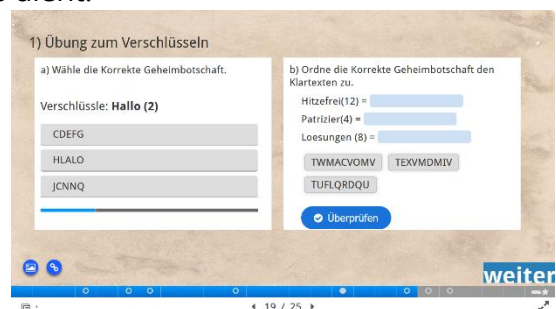


Abbildung 8 - Folie 19 - Cäsar-Verschlüsselung

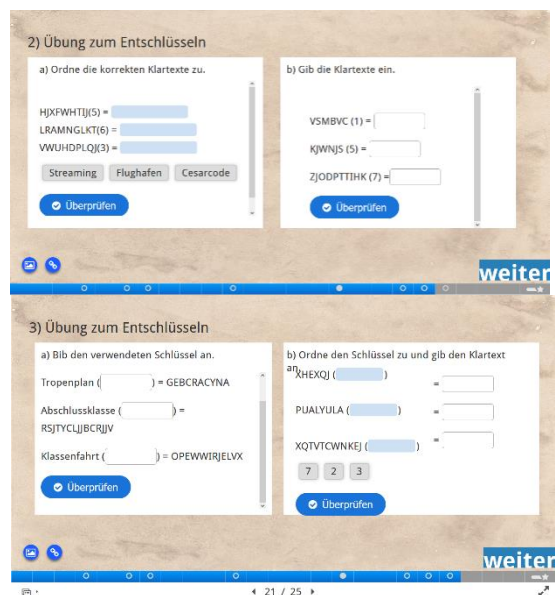


Abbildung 10 - Folie 21 - Cäsar-Verschlüsselung

und es soll der gesuchte Schlüssel in die Textfelder eingegeben werden. Aufgabe b) die Auswahl des verwendeten Schlüssels (per Drag-and-Drop) sowie die Eingabe der Klartexte in weiße Kästen.

Die **Folien 22 und 23** fordern die Lernenden durch zwei konkrete Arbeitsaufträge zur Vorbereitung der sich anschließenden Stammgruppenphase auf.

Die **Folie 24** bietet Verweise zu weiterführenden Informationen an. Auf **Folie 25** wird dann abschließend das Ergebnis aller Übungsaufgaben für die Lernenden ausgewertet. Diese Folie wird automatisch durch Lumi generiert.

Der Umgang mit der digitalen Cäsar-Scheibe, welche auf Folie 18 eingeführt wird, muss nicht weiter erläutert werden. Das Tool selbst ist mit entsprechenden Hinweisen ausgestattet (s. Abbildung 11). Allerdings lässt sich dieses Hilfsmittel im Gegensatz zum restlichen Lernelement nur bei vorhandener Internet-Verbindung benutzen, da diese nichts lokal gespeichert werden kann.

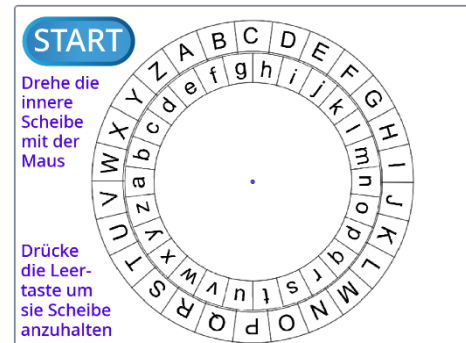


Abbildung 11 - digitale Cäsar-Scheibe aus dem Scratch-Edu-Pool (screenshot; <https://scratch.mit.edu/projects/382413373/embed/>)

Interaktives Buch: Gartenzauntransposition (TO)

Das interaktive Buch ist in fünf Abschnitte untergliedert:

1. Einleitung und Verschlüsseln mit Schlüssel 2
2. Entschlüsseln mit Schlüssel 2
3. Verschlüsseln mit Schlüssel 3
4. Entschlüsseln mit Schlüssel 3
5. Zusammenfassung

Öffnet man das interaktive Buch, erscheint die Titelseite mit dem Logo der „KRYPTO AGENCY“, dem Namen des Moduls als Überschrift und einem Appell an den Lernenden mit dem Auftrag, dieses Verfahren der Kryptografie zu erlernen.

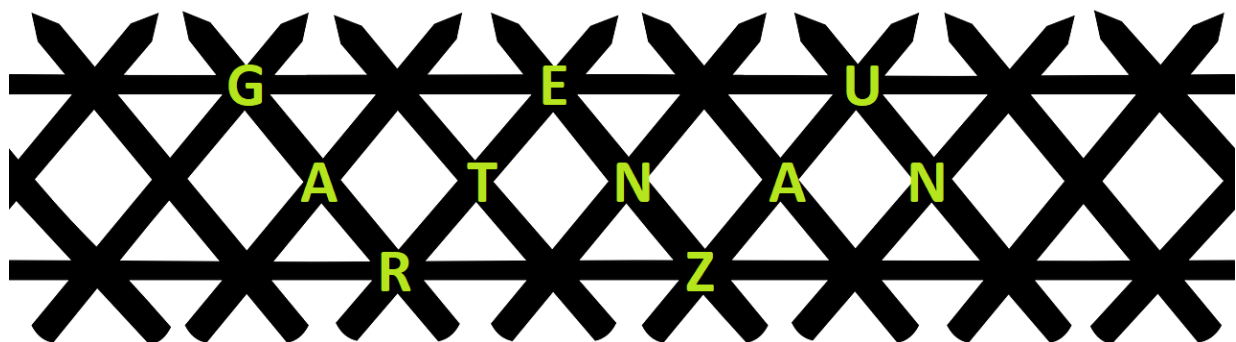


Abbildung 12: Bild Gartenzauntransposition

Zu 1.: Ein einleitendes Bild (Abbildung 12) veranschaulicht, weshalb dieses Verfahren Gartenzauntransposition heißt. Im darunter stehenden Text werden Gründe für ein nach Regeln funktionierendes Verfahren geliefert. Mit einem Bild (Abbildung 13) wird noch einmal visualisiert, wie der Klartext „VEREINIGTE STAATEN VON AMERIKA“ mit dem Schlüssel 2 verschlüsselt wird.

V	E	R	E	I	N	I	G	T	E	S	T	A	A	T	E	N	V	O	N	A	M	E	R	I	K	A
V		R		I		I		T		S		A		T		N		O		A		E		I		A
	E		E		N		G		E		T		A		E		V		N		M		R		K	

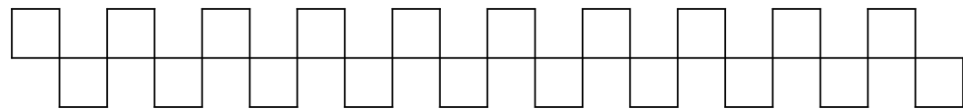
Abbildung 13: Verschlüsseln 2

Daran knüpft sich eine Drag-and-Drop-Aufgabe, die die SuS dazu auffordert, dasselbe mit dem Klartext „DEUTSCHLAND“ zu tun und anschließend zu überprüfen, ob es richtig ist. Der entstehende Geheimtext muss anschließend in ein Lückentextfeld eingetragen werden, um zu signalisieren, ob die Vorgehensweise klar ist. Im Anschluss daran soll die Verschlüsselung mit dem Schlüssel 2 anhand der Beispiele „ARGENTINIEN“ und „TADSCHIKISTAN“ auf kariertem Papier geübt und die Geheimtexte in Lückentextfelder eingetragen werden.

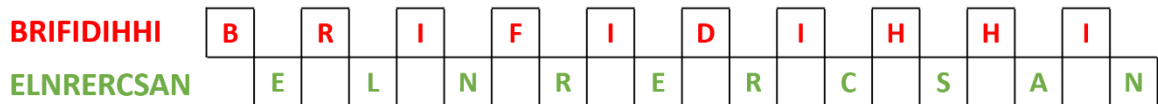
Zu 2.: Es folgt eine Anleitung zum Entschlüsseln von mit Schlüssel 2 verschlüsselten Geheimtexten, welches direkt am Beispiel von „BRIFIDIHHI ELNRERCSAN“ in 4 Schritten erklärt wird (Abbildung 14). Das entstehende Lösungswort „BERLIN FRIEDRICHSHAIN“ müssen die SuS aber selbst eintragen, um sicher zu gehen, dass das Auslesen verstanden wird. Es folgt eine Übung zur Entschlüsselung mit drei kurzen Geheimtexten auf kariertem Papier und Eingabe in Lückentextfelder. SuS, die bis zu dieser Stelle kommen, haben gezeigt, dass sie zumindest das grundlegende Prinzip der Gartenzauntransposition verstanden haben.

1. **Geheimtext: BRIFIDIHHI ELNRERCSAN (20 Zeichen)**

2. **Gartenzaun mit 2 Zeilen (Schlüssel 2) und 20 Feldern anlegen**



3. **Geheimtext Zeile für Zeile eintragen**



4. **Im Zickzack auslesen**

Abbildung 14: Entschlüsseln 2

Zu 3.: Für alle SuS, die interessiert sind und schneller arbeiten, gibt es die Möglichkeit, das Gartenzaunverfahren mit Schlüssel 3 zu erlernen. Die Lerneinheit ist analog zum 1. Teil aufgebaut. Es gibt Text und Bild zum Beispiel „VEREINIGTE STAATEN VON AMERIKA“ (Abbildung 15), danach muss „DEUTSCHLAND“ per Drag and Drop auf drei Zeilen verteilt und der Geheimtext in ein Lückentextfeld eingetragen und zum Schluss die Klartexte „ARGENTINIEN“ und „TADSCHIKISTAN“ verschlüsselt werden.

V	E	R	E	I	N	I	G	T	E	S	T	A	A	T	E	N	V	O	N	A	M	E	R	I	K	A
V				I				T				A				N				A						
	E		E		N		G		E		T		A		E		V		N		M		R		K	
		R				I				S				T				O				E				A

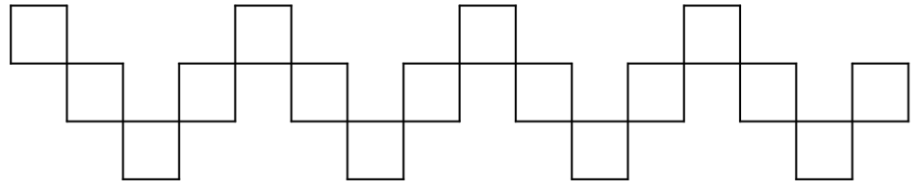
Abbildung 15: Verschlüsseln 3

Zu 4.: Beim Üben der Entschlüsselung ist es wenig motivierend und auch nicht sinnvoll, dieselben Geheimtexte zu verwenden, darum wird im Tutorial der Geheimtext „DDLS RSE KOZCE ENTH“ verwendet (Abbildung 16). Die SuS müssen „DRESDEN KLOTZSCHE“ in das Lückentextfeld eintragen, um ihren Punkt zu bekommen, um anschließend die Entschlüsselung mit Schlüssel 3 an „PAGE AUNUUNA PEI“ (PAPUA NEUGUINEA) und „VSUKN OKRPBICIA LELH“ (VOLKSREPUBLIK CHINA) auf kariertem Papier zu üben. Bei den Lösungswörtern habe ich darauf geachtet, wenig alltäglich gebräuchliche

Ortsbezeichnungen zu verwenden, damit den SuS wenig Spielraum bleibt, das Transpositionsrätsel durch einfaches Probieren zu lösen.

1. Geheimtext: DDLS RSEKOZCE ENTH (16 Zeichen)

2. Gartenzaun mit 3 Zeilen (Schlüssel 3) und 16 Feldern anlegen

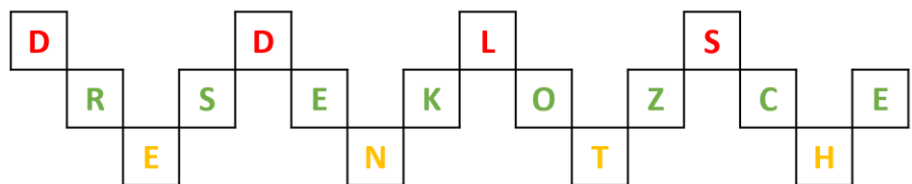


3. Geheimtext Zeile für Zeile eintragen

DDLS

RSEKOZCE

ENTH



4. Im Zickzack auslesen

Abbildung 16: Entschlüsseln 3

Zu 5.: Die Zusammenfassungsseite fasst das Verfahren noch einmal mit dem Punkten „Schlüssel“, „Verschlüsseln“ und „Entschlüsseln“ zusammen. Am Ende werden die SuS aufgefordert eine Beispielaufgabe zu erstellen, mit Hilfe derer sie das Verfahren in ihre Expertengruppen tragen.

Einstellungstest (MR)



- Um einer Art „Corporate Design“ für das gesamte Modul zu erreichen, wurde zunächst ein Logo, passend zum gewählten Agenten-Thema“, entworfen.

Hierfür wurden Piktogramme aus MS-Powerpoint kombiniert und eine Ansprechende Schriftart für den Namen gewählt.

Abbildung 17: Logo der "KRYPTO AGENCY"

Wie im einleitenden Text beschrieben, kam auch hier der H5P-Editor Lumi zum Einsatz. Für das Lernelement, welches nun vorgestellt wird, wurde das Format „interaktive Präsentation“ gewählt.

The screenshot shows a test interface for the KRYPTO AGENCY. At the top, there are two stylized figures in suits and hats. Below them, the text reads: "Sie absolvieren hier den Einstellungstest der Krypto-Agency. Nur die aufmerksamsten und konzentriertesten Teilnehmer haben hier eine Chance." Below this, it says: "Antworten sie mit 'WAHR' wenn sie bereit für den Test sind." There are two buttons: "Wahr" and "Falsch". The "Falsch" button is highlighted with a red border and a red 'X' icon. Below the buttons, there is a blue text box that says: "Dies bedauern wir sehr, da sie allerdings einige Mitarbeiter bereits gesehen haben, müssen wir sie leider.....". At the bottom, there is a progress bar showing "0/1" and a "Wiederholen" button. A blue arrow button is also visible on the right side of the interface.

Um einen gewissen Unterhaltungswert zur Motivationserhöhung zu schaffen, wurden einige witzige Antwortreaktionen im Test versteckt.

Abbildung 18: "Falsch-Reaktion" der Eingangsfrage

Heute ist Dienstag. Welcher Tag ist einen Tag nach morgen?

(Quelle: <https://www.stepstone.de/Karriere-Bewerbungstipps/lc>)

☐ Dienstag

☐ Samstag

☐ Sonntag

☐ Mittwoch

☐ Freitag

☐ Donnerstag

☐ Montag

• • • • •

Die zweite Aufgabe im Bereich der textgebundenen Logikfragen zielt auf die Fähigkeit ab, den tiefgreifenden Sinn eines, evtl. unbekannten Ausdrucks, zu erfassen. Auch hier werden Textverständnis und abstraktes Denken abgefordert. Konkret soll der Sinn bzw. die Aussage eines gegebenen Sprichwortes abgefragt, die Antworten sind wiederum als Sprichworte angegeben.

Abschließend für den Bereich der textgebundenen Aufgaben steht die Bewältigung einer Zuordnungsaufgabe an. Hier sollen die Lernenden Synonyme für bekannte Worte richtig zuordnen.

Auf den folgenden drei Folien werden die textgebundenen Logikaufgaben bearbeitet.

Hierbei gilt es zunächst die Frage logisch zu erfassen und die entsprechende Antwort per Single-Choice auszuwählen. Dieser Aufgabentyp zielt speziell auf Textverständnis und textlich, logische Verknüpfung ab.

Abbildung 19: textgebundene Aufgaben, Frage 1

Welche Aussage hat dieselbe Bedeutung wie folgendes Sprichwort?

"Rom wurde nicht an einem Tag erbaut"

(Quelle: <https://www.stepstone.de/Karriere-Bewerbungstipps/logiktes>)

☐ Alle Wege führen nach Rom.

☐ Die spinnen die Römer.

☐ Gut Ding will Weile haben.

☐ Rom sehen und sterben.

• • • • •

Abbildung 20: textgebundene Aufgaben, Frage 2

Ziehe die Wörter in die richtigen Felder!

ist ein anderes Wort für rechnen

ist ein anderes Wort für rätseln

ist ein anderes Wort für arbeiten

ist ein anderes Wort für spielen

ist ein anderes Wort für zögern

• • • • •

Abbildung 21: textgebundene Logikaufgaben Frage

Als Auftakt der zahlengebundenen Logikaufgaben wurde wieder auf eine in verschiedenen Logiktests verwendete Aufgaben zurückgegriffen. Den Symbolen sollen Zahlenwerte so zugeordnet werden, damit die abgebildete „Gleichung“ mathematisch Sinn ergibt. Im konkreten Fall erfüllt einzig die Nummer fünf diesen Anspruch.

$$\triangle \times \triangle = \bigcirc \triangle^+$$

Für welche Zahl steht das Dreieck?

(Quelle: <https://www.stepstone.de/Karriere-Bewe>)

☐ 2

☐ 5

☐ 7

☐ 3

✓ Überprüfen



Abbildung 22: zahlengebundene Logikaufgabe, Frage 1

In der Folgefrage soll lediglich im Kopf eine Überschlagsrechnung angestellt werden. Diese Aufgabe zielt auf die Fähigkeit ab, Problemstellungen in kleine, gut bewältigbare, Einzelprobleme zu zerlegen und im Anschluss wieder zu einer Gesamtlösung zu kombinieren.

Welche Lösung ist richtig?

36.993.702 : 6 = ?

☐ 4.123

☐ 4.123.916

☐ 6.165.617

☐ 11.986.245

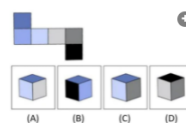
☐ 8.329.712

✓ Überprüfen



Abbildung 23: zahlengebundene Logikaufgaben, Frage 2

Anschließend folgt eine Aufgabe, bei der eine gegebene Zahlenreihe logisch fortgesetzt werden soll. Es handelt sich hierbei um 7 Ziffern aus der Fibonacci-Folge. Es wird davon ausgegangen, dass ein Großteil der Lernenden diese Zahlenfolge nicht bekannt ist und sie somit selbst auf die Weiterführung dieser auf Grundlage des Erkennens eines logischen Musters kommen müssen.



Welcher der Würfel A, B, C und D wurden hier auseinander gefaltet?

(Quelle: <https://www.stepstone.de/Karriere-Bewerbungsti>)

☐ D

☐ A

☐ B

☐ C

✓ Überprüfen

Abbildung 24: Aufgaben zur räumlichen Vorstellungskraft, Frage1

Mit den letzten drei Fragen werden nun die zwei fehlenden Kategorien abgeprüft. Das räumliche Vorstellungsvermögen wird mittels Aufgaben abgeprüft, in denen die Lernenden zuerst aus einem gegebenen Würfelnetz den korrekten fertigen Würfel ableiten sollen. Anschließend soll ein abgebildeter Würfel im Geiste mehrfach nach Vorgaben gedreht werden und angegeben werden, welche Augenzahl nach oben zeigt.

Abschließend wird die Kategorie der symbolgebundenen Logikfrage abgearbeitet, indem wieder eine Reihe logisch fortgesetzt werden soll. Diesmal besteht die Reihe allerdings aus mehrfach kombinierten geometrischen Formen. Hier wird im Speziellen die Abstraktionsfähigkeit der Lernenden abgeprüft.

Die abschließende Auswertung unterscheidet in 3 Bereiche der erreichbaren Punkte. Es

▼ Gesamtrückmeldung

Lege Rückmeldungen für einzelne Punktebereiche fest

Klicke auf den "Bereich hinzufügen"-Button, um so viele Bereiche hinzuzufügen, wie du brauchst. Beispiel: 0-20% Schlechte Punktzahl, 21-91% Durchschnittliche Punktzahl, 91-100% Großartige Punktzahl!

Punktebereich*	Rückmeldung für jeweiligen Punktebereich
0 % - 33 %	Schauen wir mal, worin du besser bist.
34 % - 66 %	Na das klappt doch schon ganz gut.
67 % - 100 %	Logisch - du bist ein Denker.

wurde versucht, jeden Bereich mit einer kurzen, motivierenden Floskel zu versehen.

Abbildung 25: Auswertung

Lernelement zu den Grundbegriffen der Kryptografie (MR)

Im vorliegenden H5P-Lernelement zu den Grundbegriffen der Kryptografie werden den Lernenden nach einem sehr kurzen, einführenden Text auf Seite 1 auf den folgenden zwei Seiten die, hier im fachlichen Kontext, korrekte Bedeutung des Grundbegriffes „Schlüssel“ nähergebracht. Dies geschieht zunächst über eine sehr einfache grafische Zuordnungsaufgabe aus Folie 2, welche nach erfolgreicher Bearbeitung eine ebenso einfache textliche Lösung der Frage ausgibt. Diese Zuordnung greift zuerst die lebensweltnahe Bedeutung des Begriffs „Schlüssel“ auf, um sie danach auf Folie 3 zu abstrahieren und der informatischen Bedeutung zuzuführen. Hier ist eine Texteingabe zu bewältigen, welche jedoch nach Lesen des zu Grunde liegenden Textes für keinen Lernenden eine Schwierigkeit darstellen soll. Diese Aufgabe dient lediglich des Transfers der Bedeutung des Begriffes.

Was benötigst du, um den Schatz vor anderen zu schützen?



Überprüfen

Abbildung 26: Schatztruhe

Das Anwenden eines Schlüssels auf einen klar lesbaren Text nennt man **VERSCHLÜSSELN**.
Dieses Verschlüsseln verändert einen **KLARTEXT** nach vorgegebenen Regeln so, dass dieser eben nicht mehr lesbar ist.
Es handelt sich nach dem Verschlüsseln um einen **GEHEIMTEXT**.

Es folgen zwei Folien in denen zunächst textlich die Begriffe Klartext und Geheimtext, sowie die Vorgänge ver- und

 + Klartext = Geheimtext

Abbildung 27: Erklärung Geheimtext

entschlüsseln anschaulich erklärt werden. Dies ist aus Sicht des Erstellers ausreichend, da an dieser Stelle bereits das Problem einer Fehlvorstellung oder Fehldeutung der Begriffe durch die vorherige Bearbeitung nahezu ausgeschlossen ist.

Im Anschluss wird der Gesamtprozess der Übermittlung eines geheim zu haltenden Textes mittels Vorgangsdiagramm, zuerst auf Sender-Seite, danach auf der Empfänger-Seite, dargestellt. Hier werden an den, im Vorgang korrekten Stellen, die im Vorfeld erarbeiteten und erklärten Begriffe erneut aufgegriffen und mit passenden



Hier siehst du einmal den kompletten Vorgang in dem eine Nachricht verschlüsselt vom Sender zum Empfänger übermittelt wird.

Zuerst die Seite des Empfängers:

Abbildung 28: Ablaufdiagramm Sender

Piktogrammen ergänzt. Einzig der Vorgang des Transportes wird hier neu benutzt. Da dieser Begriff aber keiner Erklärung bedarf, da er sich hier semantisch nicht vom bekannten Begriff unterscheidet, wird auch nicht näher darauf eingegangen.

Auf der letzten Folie wird die Festigung der hier bearbeiteten Begriffe durchgeführt. Dies geschieht über eine mehrfache Zuordnungsaufgabe der Begriffe zu, in der interaktiven Folie, bereits benutzen, kurzen Umschreibungen.

Die analoge Sicherung geschieht auf den Arbeitsblättern der jeweiligen Kryptografiemethoden. Hier ist einheitlich eine Tabelle analog zur letzten Seite des Grundlagenmoduls eingearbeitet.

Ordne die Begriffe den Definitionen zu und übernimm dir diese Übersicht in dein Arbeitsblatt.

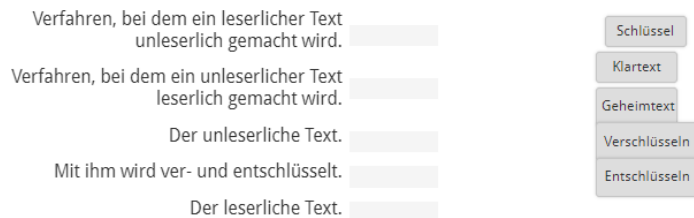


Abbildung 29: Zuordnung alle Begriffe

Ergänzend wurde ein weiteres Minilernelement zu den Grundbegriffen erstellt, bei dem besonders lernstarke Schüler differenziert, die hier behandelten, aber auch weiterführende Begriffe in Form eines Buchstabensalates finden und markieren müssen. Zusätzlich zu den bereits im Grundmodul behandelten Begriffen, werden diese hier um die Synonyme Chiffre, chiffrieren und dechiffrieren sowie den neuen Begriff symmetrisch erweitert. Um eine Überforderung seitens der Lernenden bei dieser recht anspruchsvollen Aufgabe vorzubeugen, sind die Orientierung der gesuchten Begriffe wie folgt begrenzt:

- horizontal, links nach rechts
- vertikal, oben nach unten
- diagonal, links-oben nach rechts-unten

Finde alle 10 Begriffe

S	C	H	L	Ü	S	S	E	L	J	M	C	I
D	E	C	H	I	F	F	R	I	E	R	E	N
S	C	T	E	U	N	A	V	B	C	G	V	E
Y	S	G	U	W	C	Z	B	Q	H	I	U	H
U	O	S	Y	M	M	E	T	R	I	S	C	H
N	U	V	D	I	L	X	Ü	U	F	D	M	L
P	K	Ä	F	J	X	R	S	V	F	F	V	V
L	B	J	H	U	Ä	E	V	Y	R	K	X	J
K	L	A	R	T	E	X	T	O	E	K	G	T
U	K	R	Y	P	T	O	G	R	A	F	I	E
E	N	T	S	C	H	L	Ü	S	S	E	L	N
Y	N	R	C	Ä	S	A	R	Q	P	O	B	F
V	E	R	S	C	H	L	Ü	S	S	E	L	N

Finde diese Begriffe

Kryptografie	Cäsar	Chiffre	Schlüssel	Klartext
chiffrieren	dechiffrieren	entschlüsseln	verschlüsseln	
symmetrisch				

⌚ Zeit: 0:00 0 von 10 gefunden

✓ Check

Abbildung 30: Buchstabensalat

Bei einer korrekten Markierung eines der gesuchten Begriffe, wird dieser in der Übersicht grün markiert und die Anzahl der bereits gefundenen Begriffe um eins erhöht. Wurden alle Begriffe korrekt markiert, wird die Bearbeitung abgeschlossen und die erreichten Punkte und die benötigte Zeit ausgegeben.

Bei erneutem Starten werden die Buchstaben neu angeordnet, so dass auch eine mehrfache Bearbeitung durch mehrere Lernende EINER Arbeitsgruppe möglich und sinnvoll ist.

DIDAKTISCHE/METHODISCHE SCHWERPUNKTSETZUNG

Unser Schwerpunkt in diesem Modul liegt auf dem Thema Kryptographie und Sicherheit im Internet. Wir wollen, dass die Schüler verstehen, wie Daten im Internet sicher übertragen werden können. Dazu müssen sie Methoden der Kryptographie kennen. Wir sind der Meinung, dass wir den größten Lerneffekt bei den Lernenden erreichen, wenn sie selbstständig an den Verschlüsselungsmethoden arbeiten. Darum haben wir als Unterrichtsmethode Gruppenpuzzle und Freiarbeit für unsere Schlüsselstunde gewählt.

Methodische Analyse zum Stundenverlauf der Kernstunden

Methodenwahl Gruppenpuzzle (KK)

Als zentrale Methode der vorgestellten Kernstunden wurde das Gruppenpuzzle gewählt. Die Grundlage dieser Entscheidung lässt sich sowohl inhaltlich als auch didaktisch begründen. Auf inhaltlicher Seite ermöglicht ein Gruppenpuzzle die Bearbeitung mehrerer Verfahren trotz begrenzter Zeit. Da die Erarbeitung der einzelnen Verfahren sehr zeitaufwändig ist und abhängig vom Schwierigkeitsgrad einige Lernende abgehängt werden könnten scheint es unmöglich die Verfahren einzeln der gesamten Lerngruppe zu vermitteln.

Aus didaktischer Sicht werden Differenzierungsmöglichkeiten (vgl. Differenzierung nach Hubwieser) eröffnet. Durch die Auswahl von Verschlüsselungsmethoden unterschiedlichsten Schwierigkeitsgrades können auch bei einer sehr heterogenen Lerngruppenszusammensetzung möglichst vielen Lernenden die Möglichkeit gegeben werden, selbstständig eine Verschlüsselungsverfahren zu erarbeiten. Durch die Steuerung der Gruppenbildung durch einen Einstellungstest (siehe unten) kann ein Lernerfolg für alle Teilnehmer erreicht werden, wie auch im Prinzip Motivierung (nach Hubwieser) formuliert.

Beim einführenden Lehrervortrag zum Gruppenpuzzle sollte betont werden, dass es das Ziel der Expertenrunden-Phase ist, das Verfahren anderen erklären zu können und eigene Übungsaufgaben für Mitschüler und Mitschülerinnen zu entwerfen. Dies fördert eine klare Strukturierung der Arbeitsphase.

In der Stammgruppenphase des Gruppenpuzzles werden die Lernenden aufgefordert, ihre Ergebnisse auszutauschen.

Das gewählte Medium einer „interaktiven-H5P-Präsentation“ eignet sich hervorragend für die gewählte Methode. Als All-in-One-HTML-Datei sind diese praktisch auf jedem PC verwendbar. Durch Kombination mit dem Arbeitsblatt wird die Ergebnissicherung gesteuert. Es verhindert, dass Folien ohne Beachtung der wesentlichen Inhalte, durchgeklickt werden. Es kann abgeheftet werden und zum Lernen verwendet werden.

Freiarbeit (TO)

Die Freiarbeit wurde im Anschluss an das Gruppenpuzzle gewählt, damit die SuS die Möglichkeit haben, die Verschlüsselungsmethoden, die sie im Gruppenpuzzle nicht selbst erarbeitet haben, zu üben (Übung). Freiarbeit bietet hier den Vorteil, dass die SuS ihrem Interesse entsprechend Aufgaben auswählen und diese in ihrem eigenen Lerntempo (individuelles Lerntempo) bearbeiten können. Die SuS hatten im Gruppenpuzzle den Auftrag, eigene Verschlüsselungsaufgaben zu entwerfen, die sie untereinander austauschen und lösen können. Die SuS können sich mit ihren Aufgaben also ähnlich einem sportlichen Wettbewerb gegenseitig herausfordern (Motivierung).

Sinn und Ablauf des Diskussionsteils (MR)

Die dem hier beschriebenen Erarbeitungsteil nachgestellte, offene Diskussionsrunde soll, zusätzlich zu einer weiteren Festigungsebene, die Zusammenfassung der jeweiligen Vor- und Nachteile der gezeigten Kryptografieverfahren und den Vergleich untereinander darstellen. Es soll gezeigt werden, dass im speziellen so einfache Verfahren wie die Caesar-Chiffre durchaus eine sinnvolle und wirkungsvolle Methode darstellten, Informationen geheim zu halten. Den Blick immer auf die jeweilige Epoche oder Zeitraum gerichtet, soll den Lernenden klar werden, dass sich mit zunehmenden Anforderungen auch die Kryptografieverfahren entwickelt und verbessert haben.

Ist dies geschehen, soll der Fokus der Diskussion auf unsere heutige, hochgradig digitalisierte Welt gerichtet werden und die zuvor verglichenen Verfahren unter modernen Gesichtspunkten bewertet werden. Hierbei sollte jedem Lernenden klar werden, dass diese Kryptografieverfahren heutzutage, in der hier gezeigten, einfachen Form, kaum sinnvolle Einsatzmöglichkeiten mehr bieten. Zur Verdeutlichung kann an dieser Stelle eine Demonstration einiger Online-Tools zu den verschiedenen Verfahren herangezogen werden. So kann gezeigt werden, dass z.B. eine Caesar-Chiffre eines beliebig langen Textes mit wenigen Maus-Klicks im entsprechenden Tool leicht entschlüsselt werden kann.

(<https://www.cryptool.org/de/cto/caesar>)

Darauf Bezug nehmend und auf die stetig wachsende Menge an zu sendenden Daten muss den Lernenden klar gemacht werden, dass weiterentwickelte, sicherere Methoden zum Einsatz kommen müssen.

Dieser letzte Schritt der Diskussion bildet die Überleitung zur Erarbeitung der asymmetrischen Kryptografieverfahren welche in der Folgestunde erfolgt.

Es ist ergänzend zu bemerken, dass vor allem in einer Kombination aus der Methode Gruppenpuzzle und einem Diskussionsteil die Lernenden zum Kommunizieren und Kooperieren gezwungen sind. Zum einen fordert die Stammgruppenphase des Gruppenpuzzles ein Austausch des erlangten Wissens. Zum anderen muss auch in der Diskussion ein Austausch über Vor- und Nachteile der kennengelernten Verfahren stattfinden. Durch die Methode Gruppenpuzzle und vor allem auch das Erarbeiten eigener Übungsaufgaben für Mitschüler und Mitschülerinnen, wird deren aktiv Lernweg mitgestaltet. Es besteht also eine gegenseitig bereichernde Kooperation beim Erlernen neuer Inhalte.

Didaktische Analyse zu den Lernelementen

Einstellungstest (MR)

Aus der fachlichen Beschreibung der Logiktests ist zu entnehmen, dass diese Tests gut dazu geeignet sind, das logische und abstrakte Denkvermögen von Lernenden einschätzen zu können. Speziell das Verständnis und die Anwendung verschiedener Kryptografieverfahren erfordert eben jene Fähigkeiten der Lernenden.

Allen hier vorgestellten Lernmodulen ist ein „Einstellungstest“ vorangeschaltet. Dieser soll die SuS einerseits auf das im Konzept verankerte Agenten-Themas einstimmen, des Weiteren die Fähigkeiten im Bereich des logischen Denkens eines jeden Lernenden erfassen. Auf Grundlage der Ergebnisse dieses Tests werden die Lernenden entsprechend auf die Gruppen verteilt. Damit kann sichergestellt werden, dass Lernende mit einer besonders großen Begabung gleichverteilt auf alle Gruppen eingesetzt werden können. Es soll verhindert werden, dass die gegebene Heterogenität in der Lerngruppe unverhältnismäßig auf die Arbeitsgruppen abgebildet wird. Darüber hinaus ist durch dieses Instrument die Gruppenbildung größtenteils vorgegeben und mit der damit einhergehenden Zeitersparnis auch die Erhöhung der echten Lernzeit gegeben (Hilbert Meyer – 2). Die heterogene Struktur einer jeden Arbeitsgruppe wiederum ermöglicht, bei entsprechenden Vorgaben, ebenfalls das individuelle Fördern (Hilbert Meyer – 7) indem unterschiedliche Anforderungsniveaus innerhalb der Gruppe so verteilt werden, dass jeder Lernende entsprechend seinen Fähigkeiten einen Beitrag zur Lösung der Gesamtaufgabe leisten kann. Somit ist theoretisch eine maximale Aktivierung aller Lernenden möglich und damit der Anteil an aktiver Lernzeit möglichst groß.

Grundbegriffe der Kryptografie (MR)

Wie bereits an mehreren Stellen dieser Arbeit erwähnt, bilden die Grundbegriffe der Kryptografie an dieser Stelle die Grundlage für die Lernenden, sich mit dem Themenfeld der hier vorgestellten Kryptografie-Verfahren überhaupt erst beschäftigen zu können. Demzufolge wird die Erarbeitung dieser jedem Themengebiet vorangestellt, um so gleiche Voraussetzungen für alle Lernenden zu schaffen. Auf didaktische Reduktion kann hier, aufgrund der Einfachheit der Begriffe und der simplen Zusammenhänge, gänzlich verzichtet werden. Es werden hier durch die anfängliche Kleinschrittigkeit und die Bezugnahme auch lebensweltnahe Begrifflichkeiten das Prinzip der Veranschaulichung (DP-B3) angewendet. Des Weiteren werden durch die ständige Aufnahme der Grundbegriffe in den Erarbeitungsphasen aller Abschnitte diese ständig wiederholt und somit das Prinzip der Stabilisierung (DP-B4) realisiert.

Cäsar-Verschlüsselung (KK)

Da die Cäsar-Verschlüsselung sehr einfachen Prinzipien folgt, ist eine inhaltliche didaktische Reduktion zum Verfahren kaum nötig. Auf die Einführung des Modulo-Operators, welcher bei Schlüsseln größer 25 eingesetzt werden kann, sollte unbedingt verzichtet werden. Bei Rückfragen von Lernenden bezüglich Schlüssel größer 25, kann auf die Subtraktion des größtmöglichen Schlüssels verwiesen werden. Weiterhin sollte auf die Unterscheidung in Groß- und Kleinbuchstaben verzichtet werden. Die Verschlüsselung von Ziffern sollten ebenfalls aus der Betrachtung ausgeklammert werden. Bei Nachfragen von Lernenden kann hier der Hinweis Abhilfe schaffen, dass jede Zahl auch als Wort ausschreibbar ist und somit ebenfalls verschlüsselt werden kann.

Mit diesen Einschränkungen kann das Verfahren in wenigen Worten erklärt werden. Vorkenntnisse, die zwingend wiederholt werden müssten, sind nicht zwingend notwendig. Mathematische Kenntnisse, außer die Fähigkeit zur Addition und Subtraktion, sind nicht notwendig. Das Wissen um den historischen Kontext kann hilfreich für eine Diskussion zur Anwendbarkeit dieses Verfahrens sein ist aber stark reduziert auch in dieser Lerneinheit vermittelbar.

Durch das Auslagern von der Vermittlung der Fach- bzw. Grundbegriffe „Schlüssel“ sowie „Ver- und Entschlüsseln“, sowie durch gut gewählte Abbildungen kann das der Cäsar-Verschlüsselung zu Grunde liegende Prinzip gemäß dem didaktischen „Prinzip der Veranschaulichung“ (nach Baumann und Hubwieser) nachvollziehbar verdeutlicht werden. Durch schrittweises Zerlegen des Erkenntnisgewinns auf einzelne Folien mit anschließenden Wissensabfragen kann schließlich auch dem didaktischen „Prinzip des sachstrukturellen Aufbaus“ (nach Baumann) bzw. dem „Prinzip der Strukturierung“ (nach

Hubwieser) Folge geleistet werden. Einzelne Inhalte können durch eine klare Gliederung voneinander getrennt, als logisch aufeinander aufbauendes Wissen vermittelt werden. Durch wiederholtes Aufgreifen eingangs vermittelter kryptografischer Fach- bzw. Grundbegriffe, kann auch in dieser kurzen Unterrichtseinheit das Prinzip der Stabilisierung (nach Baumann) bedient werden. Die Lernenden sollten selbstständig in der Lage sein, die Funktionsweise der Cäsar-verschlüsselung zu erarbeiten.

Auch bietet diese Thematik zahlreiche Möglichkeiten Übungsaufgaben zu gestalten, was nach Hubwieser („Prinzip Übung“) bedeutet, dass durch sinnvolle Übungsaufgaben Wissen gefestigt werden kann. Somit kann an dieser Stelle erneut das didaktische „Prinzip der Stabilisierung (nach Baumann) zitiert werden, da gelernte Inhalte in verschiedenen Aufgabentypen angewendet werden können. Der Erkenntnisgewinn kann sich somit gut verankern. Durch Variabilität der Übungsaufgaben vom Ver- und Entschlüsseln von Texten über das Herausfinden von Schlüsseln bis hin zum Knacken von Geheimbotschaften (ohne Hilfestellung), kann (nach Hubwieser) Langeweile vermieden werden, um gleichzeitig verschiedene Perspektiven dieser Verschlüsselungsmethode zu bedienen. Aus dieser Vielfalt möglicher Aufgabenstellungen birgt die Bearbeitung Cäsar-Verschlüsselung auch ein großes Differenzierungspotential. Aufgaben können so gestellt werden, dass sie binnen Sekunden lösbar sind. Aufgaben können jedoch auch schwierig gestaltet werden und die Lernenden zum Knobeln auffordern. Die Lernenden können zudem problemlos selbst Übungsaufgaben für Mitschüler oder Mitschülerinnen erstellen, um somit nach dem Integrationsprinzip (nach Baumann) selbst kreativ an der Gestaltung des Lernprozesses der gesamten Lerngruppe mitwirken. Auch beim Lösen der möglichen Aufgabenstellung sollten den Lernenden gemäß dem operativen Prinzip (nach Baumann) verschiedene digitale und/oder analoge Hilfsmittel zur Verfügung gestellt werden, um die gestellten Aufgaben zu lösen. Von einer digitalen Cäsar-Scheibe bis hin zur simplen Pen-and-Paper-Taktik sind viele Lösungswege denkbar. Diese können von den Lernenden probiert werden, um schließlich zu einer individuell passenden Lösungsstrategie zu gelangen.

Didaktische Analyse zur Gartenzauntransposition (TO)

Die zwei grundlegenden Techniken der klassischen Verschlüsselung sind Substitution und Transposition. Als einfache Transpositionsverfahren wurden als Alternativen die Gartenzauntransposition, die Spaltentransposition und die Skytale nominiert. Die Skytale lässt sich in digitalen Lernmodulen nur schwer darstellen und übersteigt möglicherweise die Vorstellungskraft der Oberschüler. Die Gartenzaunmethode erschien hier bezüglich der Vorstellbarkeit als am wenigstens abstrakt und sie ist gut grafisch darstellbar (Prinzip der Veranschaulichung). Sie kann darüber hinaus ohne Probleme mit kariertem Papier und einem Stift durchgeführt werden. Um die Ver- und Entschlüsselung zu erlernen, werden zunächst keine mathematischen Vorkenntnisse benötigt und damit bietet sie einen optimalen Einstieg gerade für leistungsschwächere Schülerinnen und Schüler. Der Zusammenhang zwischen dem Wert des Schlüssels und des Ergebnisses der Verschlüsselung ist gut nachvollziehbar. Die Methode kann also schnell erlernt werden und hat damit das Potenzial, die Schülerinnen und Schüler durch Erfolgserlebnisse zu motivieren. Der Schwierigkeitsgrad kann im Sinne der Differenzierung weiter gesteigert werden, z.B. kann aus dem Ver- und Entschlüsseln mit kleineren Schlüsseln die Vorgehensweise mit höheren Schlüsseln abgeleitet werden bzw. als Herausforderung kann man leistungstärkeren, motivierten Schülerinnen und Schülern Entschlüsselungsaufgaben ohne Schlüssel stellen. Da dies ohne Probleme möglich ist, Texte ohne bekannten Schlüssel zu entschlüsseln, offenbart es zugleich auch eine Diskussionsgrundlage zur Sicherheit von kryptografischen Verfahren.^{T7, T8, T9}

ARBEITSMATERIALIEN

Inhalt	Bezeichnung
Kurt Kunze	
• Standalone html-Export des Moduls „interaktive Präsentation zur Cäsar-Verschlüsselung“ • Arbeitsblatt zur interaktiven Präsentation • Schlüsseltabelle Caesar • Caesar-Scheibe Bastelvorlage • Lösungsblatt zur interaktiven Präsentation	• caesar-Verschlüsselung.html • Arbeitsblatt_Caesar-Verschlüsselung.pdf • Schlüsseltabelle zum Ausdrucken.png • Caesar-Scheibe Bastelvorlage.pdf • Lösungsblatt-Caesar.pdf
Thomas Oelsner	
• Standalone html-Export des Moduls „Interaktives Buch zur Gartenzauntransposition“ • Excel-Tool zum Ver- und Entschlüsseln bis Schlüssel 6 zum Erstellen und Überprüfen von Aufgaben • Schülerarbeitsblatt zum Interaktiven Buch Gartenzauntransposition • Lösungen zum Interaktiven Buch bzw. Schülerarbeitsblatt	• Gartenzauntransposition mit Grundbegriffen.html • Gartenzaun Tool.xlsx • Arbeitsblatt_Gartenzauntransposition.docx • Gartenzaun_Lösungen.docx

Matthias Rothe

- | | |
|---|--|
| <ul style="list-style-type: none">• Arbeitsblatt-Vorlage zu den Verfahren• Lösungsblatt zu „Grundlagen der Kryptografie“• Lösungsblatt zu „Einstellungstest“• Standalone html-Export des Moduls „Buchstabensalat“• Standalone html-Export des Moduls „Grundbegriffe der Kryptografie“
• Standalone html-Export des Moduls „Einstellungstest“• Manuelles Excel-Tool zur Vigenere-Verschlüsselung | <ul style="list-style-type: none">• Arbeitsblatt_Krypto_Master(MR).pdf• Lösungen_Grundlagen(MR).pdf
• Lösungen_Einstellungstest(MR).pdf• Buchstabensalat(MR).html
• Grundbegriffe_Krypto(MR).html

• Einstellungstest_Krypto(MR).html
• Vigenere_Tool_manuell.xlsx |
|---|--|

DIDAKTISCHE ANALYSE - MATERIALIEN

Interaktive H5P-Präsentation zur Cäsar-Verschlüsselung (KK)

Das Lernelement „interaktive Präsentation zur Cäsar-Verschlüsselung“ aus insgesamt 25 Folien und einem begleitenden Arbeitsblatt ist in die folgenden sieben Abschnitte gegliedert.

- 1.) Historische Einordnung der Cäsar-Verschlüsselung (Folie 1 bis 4)
- 2.) Lernelement zu den Grundbegriffen der Kryptografie (Folie 5 bis 11; Modul von Matthias)
- 3.) Motivation zur Cäsar-Verschlüsselung anhand eines fiktiv historischen Beispiels (Folie 12 und 13)
- 4.) Erarbeitungsphase zur Cäsar-Verschlüsselung (Folie 14 bis 16)
- 5.) Übungsphase zur Cäsar-Verschlüsselung (Folie 17 bis 21)
- 6.) Sicherungsphase zur Cäsar-Verschlüsselung (Folie 22 bis 23)
- 7.) Abschluss des Lernelements (Folie 24 und 25)

Durch diese Gliederung erhält das Lernelement, gemäß den didaktischen Prinzipien „Prinzip des sachstrukturellen Aufbaus“ (nach Baumann) sowie dem „Prinzip der Strukturierung“ (nach Hubwieser) einen nachvollziehbaren roten Faden. Die einzelnen Abschnitte behandeln jeweils inhaltlich oder didaktisch/methodisch klar voneinander getrennte Einheiten. Neue Inhalte werden einzeln und kleinschrittig eingeführt. Die logisch aufeinander aufbauenden Abschnitte geleiten die Lernenden sicher durch das Lernelement. So werden in Abschnitt 1 Hintergrundwissen und in Abschnitt 2 Grundlagen zum Lernelement geliefert. Die Abschnitte 3 bis 6 folgen dann dem klassischen Aufbau einer Unterrichtseinheit, mit einer Motivations-, Erarbeitungs-, Übungs-/Festigungs- und Sicherungsphase. Abschnitt 7 rundet das Lernelement ab und gibt den Lernenden Hinweise zu weiterführenden Informationen sowie eine Rückmeldung zu den Übungsaufgaben.

Zur klaren Strukturierung des Lernelements trägt auch die Tatsache bei, dass sich Arbeitsaufträge an die Lernenden durch rote Textfarbe optisch deutlich von inhaltlichen Texten abtrennen. Neu eingeführte Schaltflächen sind durch farbliche Markierungen oder eine räumliche Zuordnung stets eindeutig erklärt. Den Lernenden sollte zu jedem Zeitpunkt dieser Lerneinheit klar sein, was sie zu tun haben. Auch Lernenden deren Muttersprache nicht deutsch ist, erleichtern die optischen Hervorhebungen den Umgang mit diesem Lernelement.

Der immer wiederkehrende Aufbau aus Erarbeitung und Übung dient der Festigung der in kleinen Hapten gelernten Inhalte, wie dies in den didaktischen Prinzipien „Stabilisierung“ (nach Baumann) oder „Übung“ nach Hubwieser gefordert wird. So enthalten zum einen die Abschnitte 1 und 2 eigene kurze Übungs- bzw. Festigungssequenzen. Zum anderen bietet Abschnitt 5 die zentrale Übungsphase des Lernelements.

Im Folgenden werden die didaktischen Entscheidungen der einzelnen Abschnitte dargelegt, abschließend wird kurz auf das Arbeitsblatt eingegangen.

1.) Historische Einordnung des Verfahrens (Folie 1 bis 4)

Folie 1 entspricht einem Deckblatt. Die Lernenden werden hier von 2 Bildern empfangen. Zum einen werden sie mit einem Bild des berühmten Römers Julius Cäsar konfrontiert. Ein kurzes Spannungsmoment soll aufgebaut werden, weil zunächst Unklarheit herrschen sollte, was eine über 2000 Jahre lang verstorbene Person mit modernen Verschlüsselungsverfahren zu tun haben könnte. Neugier soll geweckt werden, um die Lernenden, wie von Hubwieser gefordert, zu motivieren. Zum anderen taucht hier das Logo der Krypto-Agency aus dem Eingangstest auf. Dies soll die, zu Stundenbeginn beabsichtigte, Motivation aufzugreifen. Die Lernende werden nebenbei an die klare Zielvorstellung erinnert am Ende des Lernelements ein Verschlüsselungsverfahren zu beherrschen. Die Folien 2 und 3 lösen dann das eben erwähnte Spannungsmoment um Julius Cäsar auf und klären die Lernenden über den Ursprung der Cäsar-Verschlüsselung auf. In Sinner der klaren Strukturierung (Nach Baumann und Hubwieser) sind die Lernenden auf Folie 4 dazu angehalten, sich mit den Aufgabentypen des Lernelements vertraut zu machen. Unklarheiten beim Bearbeiten der inhaltlich relevanten Übungsaufgaben soll damit zuvorgekommen werden. Da zum Lösen Inhalte eines kurzen Textes wiedergegeben werden müssen, ist Konzentration von den Lernenden gefordert. Das im Folgende Notwendige Kurzzeitgedächtnis der Lernenden sollen aktiviert werden.

2.) Lernelement zu den Grundbegriffen der Kryptografie (Folie 5 bis 11; Modul von Matthias)

Die didaktische Analyse dieses Abschnittes wurde (HIER) bereits vorgenommen. Es sei an dieser Stelle nur zu erwähnen, dass die ersten Inhalte auf dem Arbeitsblatt festgehalten werden müssen. Dessen didaktische Analyse wird am Ende dieser Ausführung zu lesen ist.

3.) Motivation zur Cäsar-Verschlüsselung anhand eines fiktiv historischen Beispiels (Folie 12 und 13)

Auf den Folien dieses Abschnittes taucht eine fiktive verschlüsselte Botschaft in historischem Gewand von Julius Cäsar an seinen Stiefsohn und späteren Nachfolger Oktavian auf. Die Lernenden kommen nun zum ersten Mal mit einem Geheimtext in Kontakt. Im Sinne des sachstrukturellen Aufbaus (nach Baumann und Hubwieser) werden sie, nach der kurzen Einheit zu den Grundbegriffen gedanklich wieder auf das spezielle Verfahren gelenkt, welches sie erlernen sollen. Durch einen Button kann zwischen Geheim- und Klartext umgeschaltet werden. Die intrinsische Motivation der Lernenden die Geheimschrift „entziffern“ zu können soll angesprochen werden. Diese Motivation soll durch Begleittexte, wie „Vielleicht hast du sogar schon eine Idee, wie die Verschlüsselung funktioniert?“ oder „Am Ende dieser Einheit wirst du solche Botschaften entschlüsseln können!“ gesteigert werden.

4.) Erarbeitungsphase (Folie 14 bis 16)

Die Erarbeitungsphase ist durch einen hohen Grad der Veranschaulichung geprägt, wie in gleichnamigen didaktischen Prinzipien von Baumann und Hubwieser gefordert. Das Verfahren wird auf Folie 14 mit drei kurzen Anstrichen erklärt und zwei Abbildungen. Die Erklärung ist einfach und bildhaft formuliert, um deren Eingängigkeit zu erhöhen. Die zwei Abbildungen, welche so gewählt wurden, dass der gleiche Sachverhalt auf unterschiedliche Weise dargestellt ist, helfen eventuelle Unklarheiten, aus der Erklärung, auszuräumen. Die Abbildungen sind auf Grund ihrer Einfachheit zudem sehr einprägend. Um weitere Lernkanäle anzusprechen und die Veranschaulichung weiter zu erhöhen, könnte hier zusätzlich ein Erklärvideo in Form eines Links angeboten werden. Auch zwei Beispiele, welche auf der folgenden Folie betrachtet werden können, sollen ihren Beitrag zum Verstehen durch Veranschaulichung leisten. Auf dieser Folie werden die Lernenden an die Existenz des Arbeitsblattes erinnert, da eins der veranschaulichenden Beispiele darauf übertragen werden soll. Ein Beitrag zur Festigung wird geleistet. Dieser Beitrag wird durch eine Drag-and-Drop Lückentext-Aufgabe auf Folie 16 untermauert. Auf einen Freitext-Lückentext wurde hier verzichtet, damit diese Wissensabfrage nur wenig Zeit in Anspruch nimmt. Auch dem Problem, dass automatisch ausgewertete Eingaben, weder Rechtschreibfehler noch semantisch ähnliche Antworten gelten wird damit Vorsorge getragen. Es wird Frustmomenten vorgebeugt. Die Motivation wird durch niedrigschwellige Erfolgserlebnisse aufrechterhalten. Im Sinne der Stabilisierung (nach Baumann) sowie der Forderung nach Übung (nach Hubwieser) werden, wie schon im Abschnitt 2, auch kleinschrittige Lernerfolge wiederholt und geübt. Die abschließende Aufforderung an die

Lernenden, das Verfahren auf dem Arbeitsblatt zu beschreiben ist ebenfalls in diesem Sinne zu verstehen. Dies stellt zudem sicher, dass die erarbeiteten Inhalte auch in der Stammgruppenphase korrekt abrufbar sind. Nicht zuletzt können die Lernenden eine eindeutige Rückmeldung erhalten, ob sie das Verfahren verstanden haben (Denn nur wer etwas verstanden hat, kann es auch erklären).

5.) Übungsphase (Folie 17 bis 21)

Nach der Wissensvermittlung folgt nun die zentrale Übungsphase des Lernelements. Um den Lernenden individuelle Lösungswege der folgenden Aufgaben zu eröffnen, werden auf Folie 18 die „Cäsar-Scheibe“ sowie eine „Klar-/Geheimtext-Tabelle“ als Hilfsmittel vorgestellt. Beide Hilfsmitteln werden sowohl digital als auch analog angeboten. Gemäß dem operativen Prinzip (nach Baumann) oder dem Prinzip Variabilität und Flexibilität (nach Hubwieser), können die Lernenden frei aus den angebotenen Hilfsmitteln wählen, auf welche Weise sie die Aufgaben lösen möchten. Nun können die Übungsaufgaben der Folien 19 bis 21 gelöst werden. Eine Begründung dieser Übungsphase ist erneut in den didaktischen Prinzipien Stabilisierung (nach Baumann) und Übung (nach Hubwieser) zu finden.

Die Übungsaufgaben sind abwechslungsreich gestaltet. Sie gliedern sich in drei Übergeordnete Aufforderungen „1) Verschlüsseln“, „2) Entschlüsseln“ und „3) Schlüssel herausfinden“. Jede dieser Aufforderungen wird durch je zwei Aufgabentypen repräsentiert. Durch die verschiedenen Aufforderungen sowie deren abwechselnde Aufgabentypen wird Variabilität erzeugt (vgl. didaktisches Prinzip Variabilität und Flexibilität nach Hubwieser). Die Aufgabentypen als jeweils als a und b bezeichnet, weisen zu dem von a zu b steigende Schwierigkeitsgrade auf. Hier wird dem Prinzip der Differenzierung (nach Hubwieser) Rechnung getragen. Zum Lösen der a-Aufgaben genügt das Anwenden des Verfahrens auf nur einen Buchstaben der Verschlüsselten Nachricht, was bei Bestehen ausreichend bestätigt, dass die Lernenden das Verfahren grundsätzlich verstanden haben. Zum Lösen der b-Aufgaben muss jedoch etwas genauer nachgedacht werden, da nicht jeder Buchstabe „zum Entschlüsseln geeignet“ ist (Aufgabe 1b), ganze Worte entschlüsselt werden müssen (Aufgabe 2b) oder vor dem Entschlüsseln die korrekten Schlüssel zugeordnet werden müssen (Aufgabe 3b). Vor allem die b-Aufgaben regen sinnvollen Einsatz der angebotenen Hilfsmittel an.

6.) Sicherungsphase (Folie 22 bis 23)

Mit der Aufforderung auf dem Arbeitsblatt „eigene Übungsaufgaben für Mitschüler oder Mitschülerinnen zu entwerfen“ wird auf Folie 22 die Sicherungsphase eingeleitet. Gemäß

des Integrationsprinzips (nach Baumann) können die Lernenden durch das Erstellen eigener Übungsaufgaben den Lernprozess in diesem Fall speziell von Mitschülern und Mitschülerinnen mitgestalten. Den Lernenden werden bezüglich der Aufgabenformate keine Restriktionen gesetzt. Die Lernenden haben im Sinne der Kreativitätsförderung (nach Hubwieser) freie Hand. Zudem wird wie zuvor bereits mehrfach erläutert den Prinzipien Übung (nach Hubwieser) und Stabilisierung (nach Baumann) Folge getragen. Da gelerntes durchdacht werden muss, um sinnvolle Aufgaben entwickeln zu können.

Zuletzt soll die Folie 23 dazu anregen, das bisher nur theoretisch erprobte Wissen, auf alltägliche Relevanz zu prüfen, um schließlich den Bogen zu den in der Vorstunde diskutierten Zielen der Kryptografie zu schlagen. Zugleich werden die Lernenden auf die bevorstehende Diskussion vorbereitet. Die Folie 23 kann als Beitrag der von Baumann geforderten Lebensnähe und Aktualität gesehen werden, da abstraktes Wissen um ein (zwar einfache) Verschlüsselungsverfahren auf die (sehr komplexen) Umstände der Realität übertragen werden muss.

7.) Abschluss (Folie 24 und 25)

Durch das Anbieten weiterführender Informationen auf Folie 24 können Lernende motiviert werden, sich über den Unterricht hinaus weiteres Wissen anzueignen.

Folie 25 gibt den Lernenden abschließend eine quantitative Rückmeldung zu den bearbeiteten Übungsaufgaben. Wie von Hubwieser unter dem Prinzip Bewertung & Erfolgssicherung formuliert, bekommen die Lernenden das Ergebnis ihrer Arbeit klar abrechenbar präsentiert. Auch wenn die absolut erreichte Punktzahl keinen wirklichen Rückschluss auf das Verständnis zur Methode zulässt, da hier bspw. auch die Aufgaben aus Abschnitt 1 einfließen, so werden gewissenhafte Lernende für gute Ergebnisse belohnt. Lernende die das Lernelement zunächst oberflächlich bearbeitet haben, können angeregt werden einzelne Aufgaben zu wiederholen.

Das Arbeitsblatt

Die Entscheidung ein begleitendes Arbeitsblatt zu entwerfen, leitet sich aus zwei während der Grobplanung der Stunde getroffenen Entscheidungen ab; der Medienwahl und der Methodenwahl. Digitale Medien wie dieser H5P-Inhalt bieten Lehrenden zwar neue vielfältige Möglichkeiten Unterrichtssequenzen zu gestalten und erlauben Lernenden oft selbstständigeres Lernen als mit traditionellen Medien. Jedoch bieten digitale Inhalte selten die Möglichkeit erarbeitete Inhalte und erledigte Übungsaufgaben dauerhaft und nachschlagbar festzuhalten. Durch das vorliegende Arbeitsblatt kann dieser Nachteil ausgeglichen werden. Die wichtigsten Fakten sowie einige Übungsaufgaben sollen darauf

festgehalten werden. Dies ist auch im Hinblick auf die für diese Stunde getroffene Methodenwahl von direkter Bedeutung.

Nach Abschluss dieses Lernelements müssen die erlernten Inhalte im Rahmen einer der Stammgruppenphase des Gruppenpuzzles an Mitschüler und Mitschülerinnen weitergegeben werden. Dieses Arbeitsblatt dient damit sowohl als roter Faden und Erinnerungshilfe bei der Wissensweitergabe durch den Lernenden an seine Mitschüler und Mitschülerinnen.

Sowohl das Arbeitsblatt als auch der H5P-Inhalt sind aufeinander abgestimmt. So bietet das Arbeitsblatt Hinweise, auf welchen Folien die gefragten Inhalte zu entdecken sind. Vor allem aber werden Lernende beim Bearbeiten des digitalen Lernelements direkt aufgefordert entsprechende Inhalte auf dem Arbeitsblatt festzuhalten.

Einstellungstest (MR)

Das Element des Einstellungstests kann hier weniger als Lernelement bezeichnet werden, ist nichtsdestotrotz für den geplanten Ablauf unerlässlich. Wie an mehreren Stellen bereits erwähnt, kann auf Grundlage der erreichten Punkte in diesem Test eine Gruppeneinteilung in der Art vorgenommen werden, als dass sich eine gerechte Verteilung hinsichtlich der logischen Leistungsfähigkeiten der Lernenden realisieren lässt. Dies erlaubt einerseits eine erhebliche Zeitersparnis, andererseits wird gewährleistet, dass alle Gruppen ähnlich arbeitsfähig sind und so die Ergebnisse der einzelnen Gruppen auch die erwartete Qualität aufweisen. Die ansprechende Gestaltung und die, an einigen Stellen versteckten und unterhaltsamen „Reaktionen“ schaffen hier ein hohes Maß an Motivation für diesen Abschnitt des Lernbereiches. Diese Motivation wird durch den Aufbau aller hier im Modul vorgestellten Lernelemente und durch die generelle Struktur der Planung dieser Lernbereiche im weiteren Verlauf aufrechterhalten. Die klare Struktur aller hier vorgestellten Lernelemente erzeugt Ziel- und Inhaltsklarheit, welche wiederum Unsicherheiten der Lernenden verringert und somit gute Lernerfolge ermöglicht.

Der Wettbewerbscharakter eines solchen Tests stellt eine weitere Aktivierungsebene innerhalb einer Lerngruppe dar, da oftmals der Vergleich innerhalb der Gruppe von den Lernenden hinsichtlich nahezu aller Kategorien der Fähigkeiten gesucht wird. Hier ist ein Ansporn bezüglich des natürlichen Verlangens zu den Besten zu gehören in den Grenzen des lernförderlichen Klimas durchaus erwünscht.

Grundbegriffe der Kryptografie (MR)

Durch die Kleinschrittigkeit der hier vorgestellten Elemente, sowie der anfänglich sehr niedrigen Anforderungen können die Aktivierungsschwellen nahezu aller Lernenden überwunden werden. So erreicht man eine annähernd gleichverteilte Aktivität aller Mitglieder der Lerngruppe und erhöht auch den Gruppenzusammenhalt, da sich einerseits kein Lernender ausgeschlossen oder zurückgelassen fühlt, andererseits kein Mitglied der Gruppe befürchten muss, ausgenutzt zu werden bzw. einen ungerecht hohen Anteil der Arbeit leisten zu müssen.

Auch hier stellt die klare Strukturierung des Lernelementes die Ziel- und Inhaltsklarheit sicher. Dieses Lernelement wechselt immer wieder zwischen Phasen des aktiven Handelns durch Aufgabenstellung der Art „Drag&Drop“ oder „Textbox“ und Phasen des verstehenden Lesens. Hierbei soll trotz der Kürze des Elements eine abwechslungsreiche Wissensvermittlung erreicht werden. Des Weiteren soll auf Grund des Grundlagen-Charakters dieses Elements eine zu Starke Forderung der Lernenden vermieden werden, da die Erarbeitung des eigentlichen Themas, der ausgewählten Kryptografieverfahren, im

Vordergrund stehen sollte. Ein nicht zu unterschätzender Faktor der Vorschaltung eines, von jeder Gruppe im gleichen Ausmaß zu erfüllenden, einheitlichen Grundlagenelements ist der Gedanke der Gerechtigkeit der verteilten Aufgaben. Ein jeder Lernende steht zu Beginn der Erarbeitungsphase vor einer identischen Problemstellung. Dies senkt wiederum die Aktivitätsschwelle. Nachdem einmal alle Lernenden aktiv bei der Sache sind, spielen eventuelle Unterschiede in der Komplexität bzw. Schwierigkeit der gestellten Aufgaben eine deutlich geringere Rolle als zu Beginn. Die Aufmerksamkeit eines jeden Mitgliedes der Arbeitsgruppe ist danach auf das jeweilige Thema gerichtet und die Konzentration auf das Gruppenthema steht im Mittelpunkt.

Wie an einigen Stellen bereits erwähnt wird anfänglich die lebensweltnahe Bedeutung der hier zu vermittelnden Begriffe erst aufgenommen, dann abstrahiert um das „Prinzip der Veranschaulichung“ zu realisieren. Dies geschieht besonders kleinschrittig, um den Workflow der Arbeitsgruppe zunächst in Gang zu bringen und fortwährend zu beschleunigen. Durch ständige Wiederaufnahme der Begriffe innerhalb des Elements soll schon während der Erarbeitungsphase eine Stabilisierung der Begriffe stattfinden, welche in der Festigung zu Ende des Grundlagenelementes und im Eintragen der Begriffe auf dem Arbeitsblatt des jeweiligen Verfahrens endet.

Interaktives Buch Gartenzauntransposition (TO):

Das interaktive Buch ist in fünf Abschnitte untergliedert:

1. Einleitung und Verschlüsseln mit Schlüssel 2
2. Entschlüsseln mit Schlüssel 2
3. Verschlüsseln mit Schlüssel 3
4. Entschlüsseln mit Schlüssel 3
5. Zusammenfassung

Wir haben uns im Team dazu entschieden, den Unterricht in einem Agentenframe zu inszenieren. Dazu gibt es in diesem Modul die Titelseite, die erstens motivierend (DP-H1 Motivierung) wirken soll und den SuS eine klare Zielvorstellung (DP-B11 Zielvorstellung) gibt. Es erschien mir sinnvoll, die Klar- und Geheimtexte mit dem Agentenframe zu verknüpfen und deswegen habe ich hier ausschließlich Ortsangaben verwendet, z.B. Argentinien oder Berlin Friedrichshain.

Während meiner Arbeit habe ich die persönliche Erfahrung gemacht, dass viele SuS der Oberschule ungern längere Texte lesen, bzw. das Leseverständnis für Fachtexte oft nicht ausreichend ausgeprägt ist, daher ist das ganze Modul so strukturiert, dass es nur kleinere Textbausteine gibt, die notfalls auch nur oberflächlich oder gar nicht gelesen werden können, ohne den Lernerfolg maßgeblich zu behindern. In den Texten wurden konsequent die Fachbegriffe Klartext, Geheimtext, Schlüssel, verschlüsseln und entschlüsseln direkt verwendet, ohne die Definitionen im Vorfeld in Form von zusätzlichen Aufgaben abzufragen, da diese im Kontext klar werden. Der Begriff der Transposition wird zu Beginn kurz erläutert, sowie die Notwendigkeit, bei der Transposition ein von Sender- und Empfängerseite vereinbartes System zu haben. Des Weiteren wurden Farben und fett gedruckte Wörter dazu verwendet, um die wesentlichen Informationen des Textes hervorzuheben.

Bei der Aufgabenerstellung habe ich das Ziel verfolgt, dass die SuS möglichst viel selbst machen und dass die gegebenen Hilfestellungen von Aufgabe zu Aufgabe abnehmen. Die Lernenden sind dazu angehalten, zu jedem Schritt eine Lösung anzugeben (DP-B1 Aktives Lernen). Ein Beispiel:

Zuerst wird den Lernenden kurz im Text mit Bild beschrieben, wie die Gartenzauntransposition mit Schlüssel 2 funktioniert. Danach, wird dazu aufgefordert, die Transposition per Drag and Drop nachzubilden und das Ergebnis zu überprüfen. Die Aufgaben können so lange und so oft wiederholt werden, bis die richtige Lösung gefunden wurde (DP-B12 Individuelles Lerntempo). Im nächsten Schritt gibt es direkt eine Rückmeldung für ihr Verständnis, indem der entstehende Geheimtext in ein Lückentextfeld eingetragen und überprüft wird. (DP-H6 Bewertung und Erfolgssicherung). Anschließend

müssen zwei Begriffe auf kariertem Papier verschlüsselt und wieder in ein Lückentextfeld eingetragen werden. So wird in kleinen Schritten sukzessive Hilfestellung entzogen und nach jedem Schritt gibt es direktes Feedback, ob der Schritt gelungen ist, was auch den SuS selbst ein Gefühl von Sicherheit vermittelt und damit zum Weiterarbeiten motiviert.

Die Mindestanforderung an die Lernenden ist, Klar- und Geheimtexte mit Schlüssel 2 zu ver- bzw. entschlüsseln. Um schnelleren SuS (DP-H8 Differenzierung) die Chance zu geben, tiefer einzusteigen, wird derselbe Lernweg mit derselben Struktur (DP-H3 Strukturierung), den es für Schlüssel 2 gab, für Schlüssel 3 angeboten.

Um die Arbeit für die SuS zu erleichtern, werden die Schlüssel stets vorgegeben und die Geheimtexte zum Entschlüsseln enthalten Leerzeichen, damit die SuS den „Zeilenumbruch“ erkennen.

Zum Schluss gibt es noch eine Zusammenfassung, die noch einmal wiederholend die oben genannten Fachbegriffe auflistet und eine Schrittfolge zum Ver- und Entschlüsseln angibt. Ich weise an der Stelle explizit darauf hin, dass man nicht nur Ländernamen als Texte verwenden kann und dass die Gartenzauntransposition auch mit größeren Schlüsseln als zwei und drei funktioniert, was schlussendlich noch einmal die Kreativität der Lernenden anregen und motivieren soll, sich in der Freiarbeit auch den schwierigeren Gartenzaunaufgaben zuzuwenden, z.B. der Arbeit mit größeren Schlüsseln, längeren Texten oder dem Entschlüsseln ohne Schlüssel.

Das Lernmodul lässt sich somit sowohl in diesem Gruppenpuzzle als kurze Lerneinheit verwenden, kann aber auch beliebig auf größere Schlüssel und längere Texte erweitert werden, bzw. auf das Entschlüsseln von längeren Botschaften ohne vorgegebenen Schlüssel.^{T7, T8, T9}

REFLEXION

Lernelement „Cäsar-Verschlüsselung“ (KK)

In einem Testdurchlauf wurde der H5P-Inhalt zur Cäsar-Verschlüsselung vom Mitstudierenden getestet und mit Hilfe eines vorbereiteten Miro-Boards beurteilt. Dabei wurde in einer vorangestellten Ampelabfrage Inhalt durchweg grün, also positiv bewertet. In einem zweiten Beurteilungsfeld konnten die Testenden kurze Kommentare und Verbesserungsvorschläge notieren. Es folgt eine Auflistung dieser Kritikpunkte kurzen Erläuterungen wie von mir auf diese Kritikpunkte reagiert wurde.

- 1.) Rechtschreibfehler auf verschiedenen Folien wurden aufgezählt. Diese wurden umgehend von mir entfernt, sodass der dargebotene Inhalt gänzlich der deutschen Rechtschreibung entspricht.
- 2.) Die Schriftgrößen einzelner Inhalte wurde als zu klein empfunden. Die interaktive Präsentation wurde zu Beginn mit einer niedrigen Auflösung angelegt. Diese Auflösung kann im Nachhinein nicht verändert werden. Der daraus resultierend geringe Platz auf den Folien, macht es an einigen Stellen unumgänglich auf kleine Schriftgrößen auszuweichen. Die Schriftgrößen wurden also nicht angepasst. Jedoch können die Inhalte durch Anklicken des entsprechenden Buttons in der Präsentation und durch die in heutigen Browsern standartmäßig integrierte Zoomfunktion, zu einer angenehmen Lesbarkeit vergrößert werden. Dieser Hinweis sollte ggf. den Lernenden von der Lehrkraft vor oder beim Bearbeiten der Aufgaben gegeben werden.
- 3.) Fehlende weiter Schaltflächen wurden angemerkt. Diese wurden umgehend ergänzt. Jede Folie weist nun zusätzlich der möglicherweise nicht für jeden intuitiv erscheinenden Navigationsleiste weiter-Buttons, welche ein definitiv intuitives schrittweises Voranschreiten durch die Präsentation ermöglichen.
- 4.) Der Inhalt wurde als „durchgängig motivierend und differenziert mit rotem Faden“ beschrieben. Dieses Lob beschreibt wie in der didaktischen Analyse beschrieben Teilmotivationen beim Erstellen des Inhaltes.

Mündlich wurde nach dem Testlauf der logische Aufbau der Präsentation gelobt. Die Lernenden sollten demzufolge selbstständig in der Lage sein, die Funktionsweise der Cäsar-Verschlüsselung zu verstehen. Auch die Vielfältigkeit der Aufgabentypen und -schwierigkeiten wurde gelobt. Lernende sollten also durch abwechslungsreiche Übungsaufgaben in der Lage sein, dass erworbene Wissen selbstständig zu überprüfen und anzuwenden. Dabei sollten dank einfacher Aufgaben leistungsschwächere Lernender die Möglichkeit erhalten zu zeigen, dass sie das Prinzip der Verschlüsselung verstanden

haben. Schwierige Aufgaben sollten aber auch leistungsstärkeren Lernende eine fordernde Möglichkeit geben ihr Wissen zu überprüfen.

Zusammenfassend lässt sich hier also feststellen, dass der erstellte H5P-Inhalt, nach Korrektur der Formfehler, inhaltlich korrekt, logisch aufgebaut und ansprechend gestaltet daherkommt. Er bietet Differenzierungsmöglichkeiten. Er scheint also für den Einsatz im Unterricht geeignet und für Lernende ansprechend gestaltet zu sein.

Lernelement „GARTENZAUNTRANSPOSITION“ (TO)

- **Positive Rückmeldungen**

1. „Verfahren optisch ansprechend und verständlich übermittelt.“
2. „Interaktivität, motivierend, super in LUMI umgesetzt.“
3. „Wirklich schicke LUMI-App mit sehr flüssigen Animationen.“
4. „Direktes Feedback, ob richtig oder falsch.“

- **Verbesserungsvorschläge**

1. „Evtl. kurz Erläutern, dass die roten Pfeile den Verschlüsselungsweg darstellen.“
2. „Tadschikistan und Argentinien separat“
3. „Kleine Anfangsmotivation fehlt. vielleicht noch ein motivierendes Bild/GIF an den Anfang setzen, das in Richtung Agenten/geheim geht.“
4. „Fachlich hat eine Chiffre immer einen Schlüssel -> Schlüssel ist hier die Anzahl der Zaunreihen. Sollte so genannt werden. Weiterhin sollte eine Chiffre nichts an ihrer Sicherheit einbüßen, wenn das Verfahren dem Angreifer bekannt ist. Die "Sicherheit" muss im Schlüssel liegen. Das ist hier und bei CAESAR immer ein bisschen ein Problem, I know, aber bei großer Anzahl von Zaunreihen ist es dennoch schwer die Chiffre zu knacken, auch wenn man weiß wie sie funktioniert. Security by obscurity ist ein Problem in der realen Welt und sollte nicht als valide Option im Unterricht erwähnt werden.“
5. „Bezug zum Begriff "Gartenzaun" fehlt --> Vielleicht Bild einfügen.“

Aus den positiven Rückmeldungen „optisch ansprechend“, „verständlich“, „motivierend“, „super [...] umgesetzt“ kann ich entnehmen, dass das Lernmodul grundsätzlich geeignet ist, um das Verfahren der Gartenzauntransposition zu übermitteln. Darum habe ich am grundsätzlichen Aufbau keine Veränderungen vorgenommen.

Da ich den Text so kurz wie möglich halten möchte, verzichte ich auf die Verbesserung von Punkt 1, zumal die Drag-and-Drop-Aufgabe „DEUTSCHLAND“ Missverständnisse ausräumt.

Punkt 2: Tadschikistan und Argentinien zu trennen würde bedeuten, zweimal denselben Aufgabentext einstellen zu müssen, was eine unnötige Redundanz darstellt.

Punkt 3 und 5: Bilder wurden ergänzt, die diesem Zweck entsprechen. Mein Teamkollege Matthias Rothe hat ein Agentenbild der „KRYPTO AGENCY“ entworfen, das ich direkt auf meiner Titelseite positioniert habe. Das Bild eines Gartenzauns wurde so modifiziert, dass zu Beginn schon ungefähr klar wird, worum es in der Gartenzauntransposition geht, indem das Wort „Gartenzaun“ auf den drei Zeilen des Gartenzauns im Zickzack eingetragen wurde.

Punkt 4: Der Bezug zwischen Gartenzauntransposition und Schlüssel als Anzahl Zeilen wurde hergestellt und durch Wiederholung immer wieder kenntlich gemacht.

Lernelement „Einstellungstest“ (MR)

Aufgrund der immer noch aktuellen pandemischen Lage war eine Durchführung dieses Moduls im realen Unterricht nicht möglich. Grundlage dieser Reflektion sind die Testläufe innerhalb der Seminar Gruppe und das dahingehend eingeforderte Feedback der Studenten und Dozenten.

Positives Feedback:

- Hohe Motivation der Schüler aufgrund des gewählten Formates und Gestaltung
- Gute Umsetzung

Verbesserungsvorschläge:

- Weniger schwere, eher „spaßigere“ Aufgaben
- Aufgabenstellung/Handlungsanweisung „Würfel drehen“ schwer verständlich

Aufgrund des größtenteils positiven Feedbacks kann man erwarten, dass dieses Modul in großen Teilen im realen Unterricht funktionieren wird. Da es sich in der Feedbackrunde allerdings um erwachsene, studierte Menschen handelt, ist die Komplexität beziehungsweise die Formulierung der Fragen in Hinblick auf die Einsetzbarkeit in der Oberschule noch fraglich und im realen Einsatz zu evaluieren.

Die Aufgabenstellung und ihre Bearbeitung zielen sehr genau auf bestimmte Fähigkeiten der Lernenden ab, diese zusätzlich in einen unterhaltenden oder spaßigen Rahmen zu bringen, birgt aus meiner Sicht das Risiko den eigentlichen Zweck der Fragen zu gefährden.

Lernelement „Grundbegriffe der Kryptografie“ (MR)

Aufgrund der immer noch aktuellen pandemischen Lage war eine Durchführung dieses Moduls im realen Unterricht nicht möglich. Grundlage dieser Reflektion sind die Testläufe innerhalb der Seminar Gruppe und das dahingehend eingeforderte Feedback der Studenten und Dozenten.

Positives Feedback:

- Grundbegriffe erläutert und geprüft
- Festigung der Begriffe findet statt

Verbesserungsvorschläge:

- Folie mit der Übersicht über das Vorgehen bei der Verschlüsselung könnte Schülerinnen und Schüler etwas erschlagen, ganz schön viel in einem Schaubild
- Es können nur die richtigen Antworten auf die Felder gezogen werden, demnach ist bei den Zuordnungsaufgaben die Auswertung obsolet

Nachdem die Verbesserungsvorschläge umgesetzt wurden entsteht auch hier aufgrund des immer noch größtenteils positiven Feedbacks der Eindruck, als dass dieses Modul im realen Unterricht funktionieren könnte.

Die Abbildung über das Vorgehen bei Verschlüsselung wurde aufgrund der Verbesserungsvorschläge in 2 Teile geteilt. Auf der ersten Folie ist nun einzig der Vorgang der Verschlüsselung beim Absender zu sehen. Auf der zweiten Folie entsprechend der Vorgang der Entschlüsselung beim Empfänger. Somit sollte eine Überlastung der lernenden aufgrund eines zu komplexen Schemas verhindert werden. Die Umsetzung des zweiten Verbesserungsvorschlages ergab sich einzig in einer Änderung der Optionen in der Zuordnungsaufgabe. Es ist nun möglich Begriffe auch falsch zuzuordnen ohne, dass dies dem Schüler ersichtlich ist.



QUELLENVERZEICHNIS

KURT

- K1 - <https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsslung>
 - K2 - [https://de.wikipedia.org/wiki/Substitution_\(Kryptographie\)](https://de.wikipedia.org/wiki/Substitution_(Kryptographie))
 - K3 - <https://de.wikipedia.org/wiki/Monographisch>
 - K4 - https://de.wikipedia.org/wiki/Monoalphabetische_Substitution
 - K5 - <https://kryptografie.de/kryptografie/chiffre/caesar.htm>
 - K6 - <https://kryptografie.de/kryptografie/zeitstrahl.htm>
 - K7 - Prof. Bernhard Esslinger und das Entwickler-Team von CrypTool; „Das CrypTool-Buch: Kryptographie lernen und anwenden mit CrypTool und SageMath“
 - K8 - <https://kryptografie.de/kryptografie/chiffre/rot-13.htm>
 - K9 - Vorlesung Mathematik SoSe21 Wolf Spalteholz
-
- Online Cäsar-Scheibe -
<https://scratch.mit.edu/projects/382413373/embed/>
 - Bastelvorlage Cäsar-Scheibe -
https://lehrerfortbildung-bw.de/u_matnatech/informatik/gym/bp2016/fb1/3_rechner_netze/2_kopier/5_caesar/

MR

- ^{MR1} Quelle: <https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre>
- ^{MR2} <https://www.cryptool.org/de/cto/vigenere>
- ^{MR3} Quelle <https://testhelden.com/der-logiktest/>

TO

- T¹ https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%9999_Prinzip
- T² Friedrich L Bauer, *Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie*. 3. Überarbeitete und erweiterte Auflage. Springer, Berlin u.a. 2000, **S. 9**
- T³ Friedrich L Bauer, *Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie*. 3. Überarbeitete und erweiterte Auflage. Springer, Berlin u.a. 2000, **S. 26**
- T⁴ <https://www.cryptool.org/de/education/awareness>
- T⁵ Video: Nils Kopal, <https://youtu.be/jbumW7Ym03o>
- T⁶ https://en.wikipedia.org/wiki/Rail_fence_cipher
- T⁷ Rüdiger Baumann, *Didaktik der Informatik*, 2., vollst. neu bearb. Aufl., Ernst Klett Verlag, Stuttgart, 1996, **S. 174-176**
- T⁸ Peter Hubwieser, *Didaktik der Informatik*, Grundlagen, Konzepte, Beispiele. Zweite, überarbeitete Auflage, Springer, Berlin u.a., 2004. **S. 15 – 23**
- T⁹ Nadine Bergner, Vorlesung *Didaktische Prinzipien für den Informatikunterricht*, Professur für Didaktik der Informatik TU Dresden, Wintersemester 2020/2021



ABBILDUNGSVERZEICHNIS

Alle hier nicht mit Quellen benannten Abbildungen wurden ohne Nutzung lizenzpflichtiger Materialien erzeugt.

Titelbild

- <https://pixabay.com/de/photos/internet-sicherheit-online-rechner-2296269/>, lizenzfrei

KURT H5P-Inhalt Cäsar-Verschlüsselung

- **Bild Cäsar-Scheibe** - [GI17] Gesellschaft für Informatik e. V. (Hrsg.): Bildungsstandards Informatik für den Primarbereich – zur Diskussion, Version 542, <http://metager.to/gibspdf>, Stand: 25.02.2017.
- **Bild Cäsar-Büste** - photographer: Anderson / Alfred von Domaszewski - Alfred von Domaszewski Geschichte der Römischen Kaiser Verlag von Quelle & Meyer in Leipzig 1914.
- **Bild Verschiebe-Prinzip** - <https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsslung#/media/Datei:Caesar3.svg>
- **Logo Kryptowissen** - Screenshot von Kryptowissen.de
- **Bild „Schloss“** (Folie 5) - <https://pixabay.com/de/vectors/vorh%C3%A4ngeschloss-sicherheitsperre-146537/>
- **Hintergrundtextur „Pergament“** - <https://pixabay.com/de/photos/papier-alt-textur-pergament-1074136/>