Lernende an die Kryptologie heranführen: digital und haptisch zugleich – Praxisbericht über den Online-Adventskalender „Krypto im Advent“

Thomas Borys[1] und Dirk Fox[2]

Abstract: Die Kryptologie ist eine sehr alte Wissenschaft und war bis vor wenigen Jahrzehnten nur für Regierungen und Geheimdienste von Interesse. Heute findet sich die Kryptologie fast überall in unserem Leben. Trotz ihrer immensen Bedeutung für unsere moderne Kommunikations- und Informationstechnologie, derer sich fast jeder bedient, ist das Verständnis über die Funktionsweise, ihre Möglichkeiten und Grenzen nach wie vor wenig verbreitet. In diesem Praxisbericht wird gezeigt, wie man auf spielerische Weise Lernenden insbesondere der Primar- und Sekundarstufe I die fundamentalen Methoden der Kryptologie nahebringen kann. Dazu wurde der Online-Adventskalender „Krypto im Advent“ (https://krypto-im-advent.de) entwickelt. Der besondere Ansatz dieser Webseite besteht darin, digital und haptisch zugleich vorzugehen, d. h. es werden digitale Vermittlungsformate dazu verwendet, Lernende haptisch an eine kognitive Wissenschaft - hier die Kryptologie - heranzuführen. In diesem Beitrag werden die Ziele, die Kernelemente und ein Überblick zu den Teilnehmenden, sowie deren Lösungserfolge vorgestellt.

Keywords: Kryptologie, Online-Lernen, Adventskalender, Digital Escape Rooms, Digital Storytelling Learning

1 Einleitung

Die Geheimhaltung von Informationen spielt in der Geschichte der Menschheit schon immer eine Rolle. So reichen erste überlieferte Beispiele weit in die Vergangenheit zurück z. B. finden sich auf ägyptischen Steintafeln Hieroglyphen, die leicht verändert wurden und so den Lesenden verwirrten [PF07]. Aus der Antike berichtet Herodot von einer Nachricht, die unter den Haaren eines Sklaven versteckt wurde [He91], und Julius Cäsar verschlüsselte seine private Korrespondenz [Su93]. Aber auch das Entziffern einer Verschlüsselung spielte in der Zivilisationsentwicklung eine wichtige Rolle, beispielsweise trug die Entschlüsselung der Enigma durch die Alliierten wesentlich zur Verkürzung des zweiten Weltkriegs bei. An den historischen Beispielen ist die schon immer große Bedeutung der Geheimhaltung und Sicherung von Informationen ablesbar.

[1] Pädagogische Hochschule Karlsruhe, Institut für Mathematik, Bismarckstr. 10, Karlsruhe, 76133, thomas.borys@ph-karlsruhe.de
[2] Secorvo Security Consulting GmbH, Ettlinger Straße 12-14, 76137 Karlsruhe

doi: 10.18420/delfi2022-021

In der modernen Gesellschaft spielt die Sicherheit von Daten eine immer größere Rolle. Diese wachsende Bedeutung der Informationssicherheit findet ihren Niederschlag in den Bildungsplänen der Länder. Für das Land Baden-Württemberg findet sich beispielsweise in der Leitperspektive Medienbildung das grundlegende Feld „Datenschutz“ [BB6a]. Allerdings steht dieses Feld in Konkurrenz mit 11 weiteren grundlegenden Feldern. Detaillierter wird das Thema der Informationssicherheit in den inhaltsbezogenen Kompetenzen für das Wahlfach Informatik ab Klasse 8 aufgeführt [BB6b]. Leider werden mit dem Wahlfach nur wenige Lernende erreicht, die so direkt in den Kontakt mit der Kryptologie kommen. Innerschulisch lässt sich das Wissen über Ver- und Entschlüsselung von Informationen auch beispielsweise durch Projekte, das Angebot von Arbeitsgemeinschaften oder eine stärkere Integration in andere Unterrichtsfächer vermitteln. So gibt es einen Vorschlag für die integrative Ergänzung des Mathematik-Curriculums mit Themen aus der Kryptologie [vgl. Bo11]; außerdem wurde an der PH Karlsruhe eine „Lern-Box“ mit Lernmaterialien zur Kryptologie entwickelt. Neben diesen schulischen Wegen können auch außerschulische Wege beschritten werden, wie z. B. das Modul „Schatzsuche“ am Schülerlabor der RWTH Aachen. Aus den Erfahrungen in Karlsruhe entstand 2015 die Idee, einen jährlichen Online-Adventskalender „Krypto im Advent“ (https://krypto-im-advent.de) ins Leben zu rufen, wie es ihn bereits für andere naturwissenschaftliche Fächer wie Mathematik und Physik mit „Mathe im Advent“ und „Physik im Advent“ gibt.

2 Zielsetzung und Inhalte des Online-Adventskalenders

2.1 Ziele und didaktische Überlegungen

Mit dem Online-Adventskalender sollen Lernende möglichst aller Altersstufen an die fundamentalen Methoden der Kryptologie herangeführt werden. Dabei handelt es sich um einen Adventskalender, bei dem sich hinter den Türchen keine süßen Überraschungen, sondern Krypto-Rätsel befinden, die von den Lernenden gelöst werden sollen. Der Kalender kann mit unterschiedlichen Zielsetzungen bei der primären Zielgruppe der Schülerinnen und Schüler der Primar- und Sekundarstufe I eingesetzt werden. So können interessierte Schülerinnen und Schüler motiviert werden, sich spielerisch den Herausforderungen des Ver- und Entschlüsselns zu stellen. Der Kalender kann auch im Rahmen der thematischen Vorbereitung und Ergänzung des schulischen Unterrichts eingesetzt werden, z. B. wenn das grundlegende Feld „Datenschutz“ im Rahmen der Leitperspektive Medienbildung [Mi16a] behandelt wird.

Die Einführung in die Kryptologie erfolgt digital und haptisch. Auf den ersten Blick scheinen sich die beiden Methoden gegenseitig auszuschließen. So bedeutet digital „Signale, Daten in Ziffern darstellend“ und haptisch „den Tastsinn betreffend“ [We05]. Hier ist gemeint, dass die Kryptologie haptisch erfahrbar mittels digitaler Vermittlungsformate wird.

Dem Haptischen kommt dabei eine große Bedeutung zu, denn schon Johann Amos

Comenius (1592-1670) fordert ein „Lernen durch Tun“ [Sc09]. Insbesondere wenn sich das Lernangebot auch an Lernende der Primarstufe richtet, die sich nach der Stufentheorie von Piaget in ihrer kognitiven Entwicklung meist auf dem „konkret-operativen Stadium“ befinden [Wi81], also ausgehend von konkreten Objekten lernen. So findet sich die Forderung nach einem handlungsorientierten Unterricht in vielen Handreichungen für die Gestaltung des Unterrichts. Gerade für das abstrakte Thema „Kryptografie“ ist die haptische Vermittlung besonders wichtig und kann, wie unsere Erfahrung mit einer „Krypto-Box“ in der Primarstufe gezeigt hat, Schülerinnen und Schüler für das Thema begeistern.

Die Aufgabentypen für den Adventskalender wurden daher so gewählt, dass ihre Lösung die Nutzung von kleinen Hilfsmitteln aus Papier oder Pappe erfordert, deren Herstellung in Schriftform und Videos erläutert wird. Die konkrete Umsetzung erfolgt beispielsweise solcherart, dass die Lernenden mittels eines Erklärvideos in die Lage versetzt werden, eine Verschlüsselungsscheibe herzustellen, die sie anschließend für die Lösung von Ver- und Entschlüsselungsaufgaben verwenden können.

2.2 Inhalte

In der Kryptologie werden grundsätzlich zwei Methoden der Geheimhaltung verwendet [Ka96]. Die erste Methode besteht im Verbergen der Existenz einer Information (Steganografie), d. h. alleine durch das Verstecken der Information wird diese geschützt. In den Aufgaben des Adventskalenders wird das z. B. mit Bilderverschlüsselungen umgesetzt. Eine zweite Methode besteht im Verschlüsseln der Information. Dabei unterscheidet man symmetrische und asymmetrische Verschlüsselungen. Da die primäre Zielgruppe der Aufgaben nicht über die für asymmetrische Verschlüsselungen notwendigen mathematischen Kenntnisse verfügt, werden nur symmetrische Verschlüsselungsverfahren behandelt. Bei symmetrischen Verschlüsselungsverfahren werden grundsätzlich zwei verschiedenen Basistransformationen verwendet – einerseits die Änderung der Zeichenreihenfolge (Transposition), anderseits die Ersetzung von Zeichen (Substitution). In den Aufgaben des Kalenders werden insbesondere die folgenden (historischen) symmetrischen Verschlüsselungsverfahren behandelt:

- Monoalphabetische Substitutionsverschlüsselungen: Freimaurer-Code, Cäsar-Verschlüsselung
- Polyalphabetische Substitutionsverschlüsselungen: Vigenère-Verschlüsselung, Trithemius-Verschlüsselung
- Transpositions-Verschlüsselungen: Skytale, Fleissner-Schablone.

Neben den Verschlüsselungsverfahren wird auch eine einfache Möglichkeit der Kryptoanalyse, d. h. zur Entschlüsselung einer Nachricht ohne Kenntnis des Schlüssels, vorgestellt.

3 Umsetzung

Für den Online-Adventskalender wurde eine eigene digitale Lernplattform unter Verwendung von Moodle erstellt. Die Lernenden können darüber die notwendigen Informationen herunterladen und ihre Lösungen hochladen. Sie erhalten eine automatisierte Rückmeldung über die Korrektheit ihrer Lösungen und können ihren aktuellen Punktestand abfragen. Nach dem Ende der Abgabefrist werden ausführliche Lösungen zur Verfügung gestellt. Für die Aufgaben an Wochenenden wurde auf Wunsch vieler Teilnehmenden ein bis Montag verlängerter Abgabezeitraum konfiguriert.

Als zusätzlicher Teilnahme-Anreiz werden einige hundert Preise (Spiele, Eintrittskarten etc.) im Wert von mehreren Tausend Euro ausgelobt. Für die Hälfte der Preise ist der erreichte Punktestand am Ende entscheidend; die andere Hälfte wird unter allen Teilnehmerinnen und Teilnehmern verlost, um das weitere Mitmachen unabhängig von der erreichten Punktezahl zu motivieren.

Die Krypto-Rätsel, die von den Lernenden im Verlaufe des Advents zu lösen sind, werden nicht als einfache „Liste“ von Aufgaben dargeboten, sondern sind in eine zusammenhängende Rahmengeschichte eingebunden, ganz im Sinne des „Digital Storytelling Learning“ [Ro08]. Die Rahmengeschichte wird in verschiedenen Formaten dargeboten, um unterschiedliche Lernmethoden zu unterstützen. So wird sie jeweils mit einem Video zu Beginn eröffnet und am 24. mit einem Video beschlossen; dazwischen wird sie textuell und in Form von Podcasts erzählt.

In kurzen Erklärvideos werden die für das Lösen der Krypto-Rätsel notwendigen Ver- und Entschlüsselungsverfahren bereitgestellt, bei deren Entwicklung didaktische Kriterien für gute Erklärvideos [DW20] berücksichtigt wurden.

Der Nachbau der haptischen Elemente wird durch die Bereitstellung entsprechender Bastelbögen und detaillierter Anleitungen zur Verfügung gestellt. So gibt es beispielsweise einen Bastelbogen für eine Cäsar-Scheibe, eine Fleissnersche Verschlüssselungsschablone, Tableaus für die Trithemius- und Vigenère-Verschlüsselung oder Tabellen für die Four-Square- und Polybios-Verschlüsselung.

Der Heterogenität der Gruppe der Lernenden wird durch eine Differenzierung in zwei Niveaustufen begegnet. So ist die Stufe der Einsteiger für Schülerinnen und Schüler der Klassen 3-6 und die Stufe der Fortgeschrittenen für Schülerinnen und Schüler der Klassen 7-9 gedacht. Die Begleitgeschichten und die Aufgaben für die Fortgeschrittenen lehnen sich dabei stark an die Konzepte der „Digital Escape Rooms“ [MVM21] an.

Nach dem Ende der Adventszeit werden die Aufgaben, Erklärvideos und Hilfsmittel auf einer eigenen Unterseite zusammengefasst, damit sie im Jahresverlauf auch im Unterricht eingesetzt werden können. So können die Aufgabe direkt auch für den offline Einsatz heruntergeladen werden. Die Videos sind auch direkt über den Youtube-Kanal „Krypto im Advent“ erreichbar.

4 Auswertung

Der Online-Adventskalender wird seit dem Jahr 2015 jährlich angeboten. Die Anzahl der Teilnehmenden hat sich seitdem auf rund 4.300 Anmeldungen verfünffacht. Diese verteilten sich etwa in gleichen Teilen auf die Gruppe der Einsteiger und der Fortgeschrittenen. Die Verteilung der aktiven Teilnehmenden hinweg über die Klassen 3-9 war relativ gleichverteilt, wobei die Teilnehmenden der Klassen 5 und 6 die größten Gruppen stellten. Von den angemeldeten Teilnehmenden für den Durchgang 2021 haben ca. 70% das erste Türchen geöffnet und eine Lösung der Aufgabe abgegeben; das letzte Türchen wurde von 40% der Teilnehmenden der Gruppe der Einsteiger und 30% der Gruppe der Fortgeschrittenen geöffnet und eine Lösung abgegeben. An den Daten wird deutlich, dass die Gruppe der Einsteiger über eine höhere Persistenz verfügt. Von den abgegebenen Lösungen waren in der Gruppe der Einsteiger im Schnitt 85% der Lösungen richtig, 7% falsch und 8% konnten nicht bewertet werden. Das zeigt, dass das Niveau der Aufgaben und der Erläuterungen gut an die Teilnehmenden angepasst und (nach den abschließenden Bewertungen der Teilnehmenden) die Aufgabenstellungen dennoch herausfordernd waren.

Die Datenerhebung bei der Anmeldung beschränkt sich auf die Abfrage der E-Mail-Adresse, daher sind Aussagen beispielsweise über die genaue Herkunft der Teilnehmenden oder den Schultyp, den sie besuchen, nicht möglich. Nur bei den Preisträgerinnen und Preisträgern ist der Wohnort bekannt. Im Durchgang 2021 kamen die Preisträger aus allen Bundesländern, die meisten aus Baden-Württemberg. Außerdem gab es Preisträgerinnen und Preisträger aus Schweden, Österreich, der Schweiz, Italien und England. Aus den Rückmeldungen, die von etwa 230 Teilnehmenden geschickt wurden, war ablesbar, dass die Aufgaben zum Freimaurer-Code am besten gefallen hatten, gefolgt von der B-Sprache und dem Weihnachtspecial.

5 Schlussbetrachtung

Inzwischen hat sich der Online-Adventskalender etablieren können. Damit dieser Adventskalender eingerichtet werden konnte, war eine intensive und arbeitsteilige Zusammenarbeit der beiden herausgebenden Institutionen, der Pädagogischen Hochschule Karlsruhe (PHKA) und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) notwendig. So werden von den Studierenden der PHKA die Erklärvideos, die Rahmengeschichte und die Krypto-Rätsel für die Gruppe der Einsteiger erstellt. Die KA-IT-Si ist für die Webseite, den Wettbewerb inklusive der Einwerbung der Preissponsoren und der Benachrichtigung der Gewinner sowie für die Entwicklung der Rahmengeschichte und der Aufgaben der Fortgeschrittenen zuständig.

Als weiterer Entwicklungsschritt ist geplant, auch die Anmeldung von Schulklassen zu ermöglichen. Das ist bisher nur möglich, wenn sich die Lehrenden in Vertretung der Klasse anmelden.

Daher soll noch zum Schluss auch eine Lehrende aus der Grundschule zu Wort kommen: „Liebes Krypto-Team, ich habe schon mehrfach mit meiner Grundschulklasse (3. oder 4. Schuljahr) teilgenommen. Die Kinder waren dieses Jahr mal wieder sehr angetan und haben sogar eigene Nachrichten verschlüsselt verschickt, die von den anderen entschlüsselt werden mussten… Ich fand es sehr gut, dass manche Verschlüsselungen kombiniert wurden oder auch kompliziertere Verfahren wie die Four-Square-Chiffre oder die Bifid-Chiffre verwendet wurden. Die Kinder empfanden diese Aufgabe zwar als schwer, hatten aber eine hohe Motivation und ein Erfolgserlebnis, wenn sie diese verstanden hatten."

Literaturverzeichnis

[BB6a] Bildungspläne Baden-Württemberg, Stand: https://www.bildungsplaene-bw.de/,Lde/LS/BP2016BW/ALLG/LP/MB, 14.06.22.

[BB6b] Bildungspläne Baden-Württemberg, Stand http://www.bildungsplaene-bw.de/,Lde/LS/BP2016BW/ALLG/SEK1/INFWF/IK/8/04, Stand: 14.06.22.

[Bo11] Borys, T.: Codierung und Kryptologie – Facetten einer anwendungsorientierten Mathematik im Bildungsprozess. Vieweg+Teubner, Wiesbaden, 2011.

[DW20] Dorgerloh, S.; Wolf, D.: Lehren und Lernen mit Tutorial und Erklärvideos. Beltz, Weinheim, 2020.

[He91] Herodot: Historien V-IX. Deutscher Taschenbuch Verlag, Artemis Verlag, München, Zürich, 1991.

[Ka96] Kahn, D.: The Codebreakers. Scribner, New York, 1996.

[MVM21] Makri, A., Vlachopoulos, D., Martina, R.: Digital Escape Rooms as Innovative Pedagogical Tools in Education: A Systematic Literature Review. Sustainability 13/08, 4587, 2021.

[PF07] Pincock, S.; Frary, M.: Geheime Codes. Lübbe, Bergisch Gladbach, 2007.

[Ro08] Robin, B.: The Effective Uses of Digital Storytelling as a Teaching and Learning Tool. In (Flood, J. et al ed.): Research on Teaching Literacy through the Communicative and Visual Arts. Routledge, New York, S. 429-440, 2008.

[Sc09] Schipper, W.: Handbuch für den Mathematikunterricht an Grundschulen. Schroedl, Hannover, 2009.

[Su93] Sueton, G.: Kaiserbiographien. Akademie Verlag, Berlin, 1993.

[We05] Wermke, M. (Hrsg.): Fremdwörterbuch. 8. Auflage, Dudenverlag, Mannheim, 2005.

[Wi81] Wittmann, E.: Grundfragen des Mathematikunterrichts. 6. Auflage, Vieweg, Wiesbaden, 1981.