

Krypto im Advent – Einladung zum Rätseln und Mitmachen

Dieser kostenlos zugängliche Online-Adventskalender führt in die Welt der Kryptologie ein. Schüler/innen der Klassen 3-9 sind dessen zentrale Zielgruppe, sie dürfen in 24 Tagen 24 verschiedene Krypto-Rätsel lösen. In kurzen Erklärvideos werden verschiedene Verschlüsselungsverfahren wie z.B. die Bilderverschlüsselung, Skytale und Cäsar-Verschlüsselung erläutert. Die Videos laden zum Mitmachen ein und unterstützen beim Lösen der Rätsel. Dieses Projekt wird von der Pädagogischen Hochschule Karlsruhe und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen durchgeführt.

1. Anlass und Idee für diesen Online-Adventskalender

Menschen haben schon immer den Wunsch, geheim miteinander zu kommunizieren. Geheim bedeutet in diesem Zusammenhang, dass zwei Menschen sich ein gemeinsames Wissen teilen, ohne dass ein Dritter in der Lage ist, dieses zu erhalten, die Wissenschaft dazu nennt man Kryptologie. Das kann man bewerkstelligen, in dem man das Wissen geschickt versteckt oder unkenntlich macht. Beispiele finden sich dazu schon in der Antike, so versteckt Herodot eine Nachricht unter den Haaren eines Sklaven (vgl. Herodot Buch VIII, Abschnitt 56ff.) oder Julius Cäsar verändert die Buchstaben einer Nachricht (vgl. Sueton, Kapitel 56). Im Laufe der Geschichte wurden von Regierungen und Geheimdiensten immer raffiniertere Verfahren zur Verschlüsselung von Wissen entwickelt. Bis vor kurzem handelte es sich hierbei um eine Spezialtechnologie, die heutzutage dank unserer smarten Umwelt von jedem Nutzer verwendet wird. Insbesondere unsere Kinder leben in dieser Umwelt, so spricht man in der aktuellen JIM-Studie von einer Vollausstattung der Jugendlichen mit einem Smartphone, beispielsweise besitzen 99% aller Jugendlichen ab 14 Jahren ein Smartphone (vgl. Medienpädagogischer Forschungsverbund Südwest, 2017). Wie kann man Jugendliche an das Wissen über Ver- und Entschlüsselung von Informationen heranführen? Dabei denkt man zuerst an die Schule, die das im Rahmen eines Projekts, einer Arbeitsgemeinschaft, des Informatikunterrichts oder integrativ im Unterricht (ein Vorschlag vgl. Borys 2011, S. 307ff.) leistet. Eine Möglichkeit, die Jugendlichen über die smarte Welt anzusprechen, ist die Entwicklung eines Online-Kurses. Nun stellt sich die Frage: Wie bewegt man Jugendliche, dass sie sich diesem Online-Kurs widmen? Eine sehr effiziente Idee ist die Verbindung des Online-Kurses mit einem Online-Gewinnspiel, erfolgreiche Beispiele hierfür sind „Mathematik im Advent“ oder „Physik im Advent“. So entstand die Idee, „Krypto im Advent“ zu entwickeln.

2. Inhalte Krypto im Advent

Wie jeder Adventskalender befindet sich auch hier hinter jedem Türchen eine Überraschung, hier ist es jeden Tag ein neues Krypto-Rätsel. Dieses besteht aus den beiden Elementen Erklärvideo und Krypto-Aufgabe. Die Erklärvideos bestehen wiederum aus zwei Teilen, im ersten Teil wird die Geschichte der Protagonisten erzählt und im zweiten Teil werden die Ver- und Entschlüsselungsverfahren erläutert, die für das Lösen der Aufgaben benötigt werden. Die Geschichte handelt von einem Spionageteam mit dem Agenten Krypto, einem Meister der Spionage und Kryptologie, seiner Assistentin Kryptina und dem brummigen Chef. Behindert wird deren Arbeit von den drei witzigen Spionen, die sich zum Ziel gesetzt haben, die Weihnachtsfeier der Agenten zu sabotieren.

Die 24 Krypto-Aufgaben sind in zwei Schwierigkeitsgraden differenziert: die „Einsteiger“ Aufgaben sind für Schülerinnen und Schüler der Klassen 3-6, die „Fortgeschrittenen“ für die Klassen 6-9. Die Klassenstufe 6 darf selbstständig wählen, in welchen Schwierigkeitsgrad sie sich einteilen. Im Durchgang 2017 wurden die folgenden Ver- und Entschlüsselungsverfahren behandelt: Bilderverschlüsselung, Cäsar-Verschlüsselung, Fantasiezeichen-Verschlüsselung, Freimaurercode, Codeknacken, Anagramme, geometrische Verschlüsselungen, B-Sprache, homophone Verschlüsselung, Skytale, Fleissner-Verschlüsselung, Tabellen-Verschlüsselung, Trithemius-Verschlüsselung und Vigenère-Verschlüsselung.



Abb. 1: Bildverschlüsselung

Um sich ein Bild von den Inhalten machen zu können, werden im Folgenden Aufgaben zur Bilderverschlüsselung und geometrischen Verschlüsselung vorgestellt. Bilderverschlüsselungen gehören in den Bereich der Steganographie. Das Kennzeichen dieser Art der geheimen Nachrichtenübertragung besteht darin, dass die Nachricht in einem Trägermedium versteckt wird. Bei einer Bilderverschlüsselung wird die Nachricht in dem Träger Bild versteckt. In der Abbildung 1 wurde eine Nachricht versteckt, man muss die versteckten Buchstaben finden und diese zu einem Wort zusammensetzen.

Geometrische Verschlüsselungen gehören zu den Transpositionsverschlüsselungen, diese verschleiern die Informationen. Dazu wird die Reihenfolge der Buchstaben in einer nachvollziehbaren Weise durcheinandergebracht. Die Nachvollziehbarkeit ist hier von entscheidender Bedeutung, nur sie gewährleistet, dass die Buchstaben wieder in die richtige Reihenfolge gebracht werden können. Dazu wurde die folgende Aufgabe gestellt: Krypto hat eine Nachricht von Kryptina bekommen. Kannst du sie entschlüsseln? Wo möchte sich Kryptina mit Krypto treffen?

Geheime Nachricht: T RM IZE FONU FOPIN MBINA IENE
CIG HD I

Wenn man die geheime Nachricht in das Gitter aus Abbildung 2 einträgt, ist die Nachricht leicht zu entziffern:

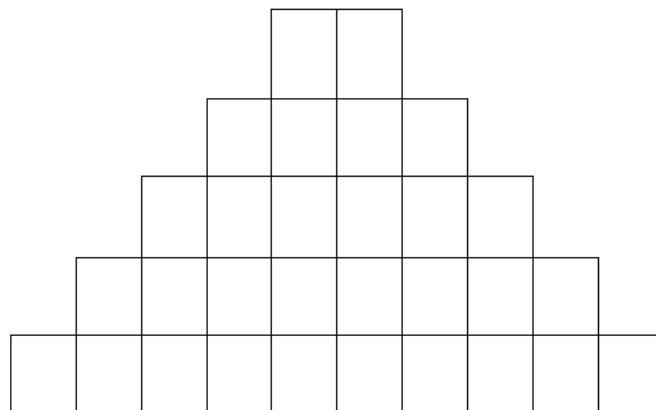


Abb. 2: Geometrische Verschlüsselung

3. Die Webseite und Rückmeldungen

Die Webseite und der Wettbewerb werden von der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) betreut. Auf der Startseite findet man die wesentlichen Informationen, so kommt man durch das Navigationsmenu zu den Seiten „Adventskalender“, „Gewinne“, „Über KiA“, „Spielregeln“, „Punkteübersicht“, „Registrieren“ und „Anmelden“. Des Weiteren kommt man zu unserem YouTube-Kanal, auf dem das Einführungsvideo abrufbar ist, auch

findet man Links, die Rätselbeispiele führen und man kann den Newsletter abonnieren. Für die weiteren Details verweise ich auf die Homepage (www.krypto-im-Advent.de).

Seit nun drei Jahren ist die Homepage aktiv. Am vergangenen Durchgang (Advent 2017) haben 2.262 aktiv die Türchen geöffnet. Von den 2.261 Teilnehmerinnen und Teilnehmer waren 1.464 Schülerinnen und Schüler (26% Einsteiger und 74% Fortgeschrittene). Dazu sollte man erwähnen, dass nur die Schülerinnen und Schüler von den Klassen 3-9 an dem Wettbewerb teilnehmen dürfen, alle anderen dürfen nur als Profis, also außer Konkurrenz miträtseln. Da nur sehr wenige Daten erhoben werden, kann keine Auskunft darüber geben werden, woher die Teilnehmerinnen und Teilnehmer kommen, nur bei den Preisträgerinnen und Preisträgern verfügen wir über die entsprechenden Daten. So kamen diese aus fast allen Bundesländern, der Schweiz, aus Österreich, Schweden und Südtirol. Schließlich seien noch exemplarisch einige Zitate der Teilnehmerinnen und Teilnehmer über diesen Kalender erwähnt:

- Theo: "Ich finde cool, dass man bei Krypto viel lernt und dass man etwas lernt, was man vorher nicht kannte. Mich hat die Caesarverschlüsselung beeindruckt: vor allem wie man mit den übersetzten Wörtern Sätze und anderes herausbekommt."
- Lars: "Ich habe schon viel gelernt, zum Beispiel, dass ich jetzt mit jemandem "reden" kann, ohne dass mich jeder versteht."
- Leonie: "Es macht Spaß und ich finde cool, dass es Rätsel gibt. Mein Lieblingsrätsel war das erste: die Bilderverschlüsselung."

Auf Grund der großen Teilnehmerzahl und den vielen positiven Rückmeldungen auch von Lehrerinnen und Lehrer, die mit ihren ganzen Klassen daran teilgenommen haben, ist das eingangs genannte Ziel, möglichst viele Jugendliche an die Wissenschaft der Kryptologie heranzuführen, erreicht worden.

Literatur

- Borys, T. (2011). *Codierung und Kryptologie - Facetten einer anwendungsorientierten Mathematik im Bildungsprozess*. Wiesbaden: Vieweg+Teubner
- Herodot (1991, 2). *Historien V-IX*. Übersetzt von Marg, W., Bibliothek der Antike, München: Deutscher Taschenbuch Verlag, Artemis Verlag
- Medienpädagogischer Forschungsverbund Südwest (2017). JIM 2017 – Jugend, Information, (Multi-) Media. URL: https://www.mpfs.de/fileadmin/files/Studien/JIM/2017/JIM_2017.pdf (Stand: 25.02.2018)
- Sueton, G. (1993). *Kaiserbiographien*. In der Reihe: Schriften und Quellen der alten Welt, Band 39, Berlin: Akademie Verlag