Punkt, Komma, Strich
Das hr2-Kinderfunkkolleg Mathematik

2h 1h 2h

Kryptographie

Inhalt des Beitrags „Gibt es Geheimzahlen?“

- Nützlichkeit von geheimen Nachrichtenüberbringungen
- Verschiedene Geheimschriften und -sprachen
- Alltägliche Verwendung von mathematischen Codes

Zielgruppe

- Klassenstufe 3/4
- Keine Vorkenntnisse zum Thema Kryptographie nötig
- Vorerfahrungen der Schüler*innen: Einzel-, Partner- und Gruppenarbeit, Lerntheke
- Vier Grundrechenarten sollten beherrscht werden

Lernziele

- Verstehen der Bedeutung von Kryptographie, auch in Bezug zur Mathematik
- Kennenlernen verschiedener Geheimsprachen und -schriften
- Chiffrieren und Dechiffrieren verschiedener Geheimsprachen und -schriften
- Erstellen eigener Geheimsprachen und - schriften
- Umwelterschließung durch Alltagsbezug
- Stärkung der Medienkompetenz
- Auditive Erfassung mathematischer Themen
- Förderung der Zuhörkompetenz

Geförderte überfachliche Kompetenzen

- Kooperations- und Teamfähigkeit
- Rücksichtnahme und Solidarität
- Medienkompetenz
- Kommunikationskompetenz

Geförderte allgemeine mathematische Kompetenzen

- Kommunizieren
- Darstellen

Inhaltsfeld

- Muster und Strukturen
- Zahl und Operation

Sachanalyse des Themas „Kryptographie“

Das Wort Kryptographie stammt aus dem Griechischen und setzt sich aus den beiden Wörtern „kryptos“ (verborgen) und „graphein“ (schreiben) zusammen. Hier wird versucht, „möglichst sichere Methoden zur Verschlüsselung von Nachrichten zu finden“ (Rempe, Waldecker 2009: S. 103).

Bedeutung

Um eine geheime Nachricht zu ermitteln und zu speichern, gibt es nach Prof. Dr. Beutelspacher drei verschiedene Vorgehensweisen. Einerseits gibt es die so genannte organisatorische Maßnahme. Diese findet über eine Übermittlung durch einen vertrauenswürdigen Boten oder in einem vertraulichen Dokument statt. Diese Methode ist Kindern durch das Verschicken von geheimen Botschaften und Liebesbriefen sehr geläufig. Darüber hinaus gibt es die physikalische Maßnahme, bei der eine Nachricht in einem Tresor oder einem versiegelten Brief versteckt wird oder durch die Verwendung von Geheimtinte. Schließlich gibt es die kryptographische Maßnahme, mit der sich überwiegend in der Unterrichtseinheit beschäftigt wird. Sie beschreibt die Erstellung einer Nachricht, die für Unbeteiligte unsinnig erscheint. Für den Empfänger sollte die Nachricht jedoch durch Informationen, den sogenannten „Schlüssel“, zu entschlüsseln sein. Der Vorgang des Verschlüsselns wird als „Chiffrieren“ bezeichnet. Der Sender besitzt einen Klartext, den er mit Hilfe des Schlüssels zu einem Geheimtext verschlüsselt. Umgekehrt nutzt der Empfänger den Schlüssel um den Geheimtext zu entschlüsseln und den Klartext zu rekonstruieren. Dies wird auch als „Dechiffrieren“ bezeichnet.

Die Kryptographie umfasst in der heutigen Zeit zwei wesentliche Aufgaben: Die eigentliche Aufgabe, auf die sich auch die Durchführung im Mathematikunterricht bezieht, besteht darin, „Nachrichten und Daten vor unbefugtem Lesen und vor Verfälschung zu schützen“. (Diekert, Kufleiter & Rosenberger 2013: S. 52). Eine weitere Funktion, die erst mit Einführung des Mediums Internet zum Tragen kommt, ist das Verschlüsseln von digitalen Unterschriften oder elektronischen Verpflichtungen.

Beispiele

Julius Cäsar war einer der ersten Menschen, der die Techniken und Verschlüsselungsverfahren der Kryptographie genutzt haben soll. Das Verfahren des Cäsar-Codes ist eine „monoalphabetische Substitution“ (ebd. S. 55). Hier werden die Buchstaben des Alphabets vertauscht und dieses Schlüsselalphabet wird dann zur Chiffrierung des gesamten Textes verwendet. Die Caesar-Chiffre verschiebt alle Buchstaben des Alphabets drei Plätze nach rechts. Man nutzt das „Klartextalphabet“ aus 26 Buchstaben von A bis Z. Dieses schreibt man auf und notiert darunter den „Geheimtext“: das Alphabet um drei Stellen nach links verschoben.

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

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

Chiffriert wird, indem der Klartextbuchstabe durch den des Geheimtextes ersetzt wird. Umgekehrt wird dechiffriert, indem der Buchstabe des Geheimtextes in den Klartextbuchstaben übersetzt wird. Die Verschiebung um drei Stellen innerhalb des Cäsar-Codes ist ein Beispiel der Verschiebungschiffren. Insgesamt gibt es gemäß des klassischen Alphabets 26 mögliche Chiffrierungen.

Die Informationsverschlüsselung mithilfe des im Unterricht eingesetzten Verfahrens „Zahnstocher-Methode“ fällt unter das Gebiet der „Steganografie“. (vgl. Beutelspacher, Neumann & Schwarzpaul 2005: S. 9). Hier geht es nicht darum, eine Nachricht unleserlich zu machen, sondern von der Existenz der Nachricht überhaupt abzulenken. Es wird versucht, die Kommunikation geheim zu halten, z.B. indem man, wie bei der „Zahnstocher-Methode“, ein leeres Blatt Papier vortäuscht, das erst noch mit einem Bleistift bearbeitet werden muss, um die Nachricht leserlich zu machen. Kryptographie und Steganografie sind beide „Teilbereich[e] der Informationssicherheit“ (vgl. ebd.).

Die B-Sprache ist eine Geheimsprache, eine sogenannte Spielsprache. Spielsprachen bedienen sich verschiedener Mechanismen: Einfügung, Umordnung, Auswechslung und Streichung. Bei der B-Sprache wird mit einer Einfügung gearbeitet. Nach jedem Vokal wird der Konsonant „b“ mit dem davorstehenden Vokal eingefügt.

Punkt, Komma, Strich
Das hr2-Kinderfunkkolleg Mathematik

Unterrichtsablauf der ersten Sequenz 1 h

Die Schüler*innen …

- sollen die B-Sprache ver- und entschlüsseln.
- sollen die Verbindung zwischen Geheimschriften und Mathematik realisieren.

Zeit/Phase	Geplanter Unterrichtsverlauf	Methoden und Medien
10 Minuten / Begrüßung	Die Lehrkraft begrüßt die SuS in der B-Sprache: *„Gubuteben Moborgeben libiebebe Kibindeber“* Anschließend findet ein gemeinsames Gespräch über die B-Sprache statt. Hierbei sollen außerdem Beispiele mit den Kindern bearbeitet und an der Tafel gesammelt werden.	L-S-Gespräch, Sitzkreis Sonstiges: Tafel
20 Minuten / Erarbeitung	Die Lehrkraft bespricht mit den SuS das Arbeitsblatt, welches anschließend in Einzelarbeit gelöst wird. Bei dem Arbeitsblatt geht es um das ver- und entschlüsseln der B-Sprache.	SuS-Aktivität, Einzelarbeit **AB 1: Begriffskarten**
15 Minuten / Ergebnis-sicherung und Reflexion	**Radiobeitrag „Gibt es Geheimzahlen?“ (3:43 – 4:38 Min)** abspielen, die SuS hören zu. *Inhalt des Radiobeitrags* • *Zwei Geheimagenten müssen einen Code knacken* • *Erläuterung des Begriffs Kryptographie* Besprechung des Radiobeitrages und Erläuterung des Themas Geheimschriften in Bezug zur Mathematik durch Lehrkraft. Zudem wird die Bedeutung des Begriffs Kryptographie erarbeitet. Anschließend findet eine Diskussion statt, in der es um die Frage geht, ob die B-Sprache eine Geheimsprache ist.	L-S-Gespräch, Sitzkreis Sonstiges: Audio Radiobeitrag, CD-Spieler o.ä.

Methodisch-didaktischer Kommentar

Das Begrüßen in der B-Sprache dient als Einstimmung und weckt die Neugierde der SuS.

Die SuS werden in dieser Unterrichtseinheit zu Geheimagenten. Dazu wird zunächst ein Steckbrief ausgefüllt, bei dem sowohl das Ver- als auch das Entschlüsseln geübt wird.

Durch das Hören des Radiobeitrages sollen die Definition von Kryptographie und der damit verbundene Bezug zur Mathematik den SuS bewusst gemacht werden. Im anschließenden Gespräch kann dies vertieft werden sowie eine Diskussion darüber stattfinden, ob die B-Sprache tatsächlich eine Geheimschrift.

Punkt, Komma, Strich
Das hr2-Kinderfunkkolleg Mathematik

Unterrichtsablauf der zweiten Sequenz 2h

Die Schüler*innen …

- sollen die Caesar-Scheibe ver- und entschlüsseln.

Zeit/Phase	Geplanter Unterrichtsverlauf	Methoden und Medien
20 Min / Einstieg	**Radiobeitrag „Gibt es Geheimzahlen?“ (2:01 – 3:04 Min)** abspielen, die SuS hören zu. *Inhalt des Radiobeitrags* • *Historischer Rückblick* Gemeinsame Besprechung des Radiobeitrages. **Radiobeitrag „Gibt es Geheimzahlen?“ (4:38 – 6:35 Min)** abspielen, die SuS hören zu. *Inhalt des Radiobeitrags* • *Erklärung des Caesar Codes* Gemeinsame Besprechung des Radiobeitrages. Danach werden an der Caesar-Scheibe gemeinsam Beispiele ent- und verschlüsselt.	L-S-Gespräch, Plenum Sonstiges: Audio Radiobeitrag, CD-Spieler o.ä., Caesar-Scheibe (selbst basteln für Tafel)
10 Min / Hinführung	Die SuS basteln in Einzelarbeit nach Anleitung eine Casar-Scheibe. Die Lehrkraft bastelt die Scheibe zeitgleich mit.	SuS-Aktivität, Einzelarbeit **AB 1: Bastelanleitung Caesar—Scheibe** Sonstiges: Spreizklammern

Methodisch-didaktischer Kommentar

Der Radiobeitrag gibt eine Erklärung für das Entstehen und Verwenden von Geheimschriften. Zudem wird die Art der Verschlüsselung durch den Caesar-Code und dessen frühere Verwendung erklärt.

Die Lerntheke ermöglicht das selbstständige Bearbeiten und Auswählen der Arbeitsblätter. Manche der Angebote können in Partnerarbeit bearbeitet werden.

In dem Reflexionsgespräch kann Inhaltliches und Organisatorisches angesprochen werden. Außerdem sollen die SuS reflektieren wie schwierig oder nützlich die Caesar-Scheibe ist bzw. in welchen Gebieten sie eingesetzt werden könnte.

45 Minuten / Arbeitsphase	Lerntheke • Caesar-Code entschlüsseln • Memory • Um wie viele Stellen ist das Alphabet verschoben • Meine verschlüsselten Wörter (Wörter für den Partner verschlüsseln)	SuS-Aktivität, Einzel- und Partnerarbeit **Alle ABs Sequenz 2, Lerntheke** Sonstiges: Schülerprodukte der Stationen
15 Minuten / Reflexion	Reflexion über die Arbeit mit der Cäsar-Scheibe und der Lerntheke.	L-S-Gespräch, Plenum **Alle ABs Sequenz 2, Lerntheke**

Zur Lerntheke

Caesar-Code entschlüsseln:

Benötigtes Material: AB 1: Caesar-Scheibe, AB 2 und AB 3: Lerntheke

Mit dem Caesar-Code verschlüsselte Wörter, sollen hier durch die Schülerinnen und Schüler entschlüsselt werden. Als Hilfe wird bereits vorgegeben, um wie viele Stellen das Alphabet verschoben ist.

Memory

Benötigtes Material: AB 1: Caesar-Scheibe, AB 7 und AB 8: Lerntheke

Wörter und ihre verschlüsselten Wörter müssen zu Paaren zusammengefunden werden. Das Memory kann sowohl in Einzel- als auch in Partnerarbeit bearbeitet werden.

Um wie viele Stellen ist das Alphabet verschoben

Benötigtes Material: AB 1: Caesar-Scheibe, AB 4 und AB 5: Lerntheke

Bei diesem Arbeitsblatt soll die Verschiebungszahl des Alphabets herausgefunden werden. Vorgegeben sind dabei die verschlüsselten Wörter und einzelne Buchstaben der jeweiligen entschlüsselten Wörter.

Meine verschlüsselten Wörter

Benötigtes Material: AB 1: Caesar-Scheibe, AB 6: Lerntheke

Hierbei sollen eigene Wörter verschlüsselt und von einem Partner entschlüsselt werden. Als Hilfestellung wird die jeweilige Verschiebungszahl angegeben.

Punkt, Komma, Strich
Das hr2-Kinderfunkkolleg Mathematik

Unterrichtsablauf der dritten Sequenz 2h

Die Schüler*innen...

- sollen zwischen einer Geheimschrift und einer Geheimsprache unterscheiden können.
- sollen eigene Geheimschriften/Geheimsprachen entwickeln.

Zeit/Phase	Geplanter Unterrichtsverlauf	Methoden und Medien
10 Min / Einstieg	Thematisierung der Unterschiede zwischen Geheimsprache und Geheimschrift. Klären der Definitionen mit Bezug auf die bisher gelernten Verschlüsselungsmethoden.	L-S-Gespräch, Plenum
30 Min / Arbeitsphase	Die Lehrkraft teilt die Gruppen zunächst in Stammgruppen ein. Die SuS sollen in Gruppenarbeit eigene Geheimsprachen entwickeln und diese schriftlich oder auditiv festhalten. Wichtig ist, dass jedes der Gruppenmitglieder anschließend ein Produkt hat, welches in der Expertengruppe vorgestellt werden kann.	SuS-Aktivität, Gruppenarbeit **AB 1: Eigene Geheimschrift/-sprache entwickeln** Sonstiges: Papier, Audio-Aufnahmegeräte
30 Min / Arbeitsphase	Die SuS stellen ihre Ergebnisse aus der Arbeit in der Stammgruppe nun in den Expertengruppen vor. Diese wurden zuvor von der Lehrkraft eingeteilt. Die anderen Gruppenmitglieder müssen dann versuchen, die Geheimsprache oder -schrift zu entschlüsseln.	SuS-Aktivität, Gruppenarbeit Sonstiges: Papier, Audio-Aufnahmegeräte
20 Min / Reflexion	Gemeinsames Gespräch zwischen Lehrkraft und SuS: - *Welche Verschlüsselung war besonders schwer zu knacken?* Anschließend werden die Ergebnisse der SuS verglichen: *Geheimschrift oder Geheimsprache?*	L-S-Gespräch, Sitzkreis Sonstiges: Papier, Audio-Aufnahmegeräte

Methodisch-didaktischer Kommentar

Die bisher kennengelernten Verschlüsselungsmethoden (B-Sprache, Caesar-Code) werden erneut thematisiert und eingeordnet, so dass die SuS in der Lage sind, anschließend eine eigene Geheimsprache/Geheimschrift zu entwickeln

Falls die SuS keine Idee haben, was sie entschlüsseln sollen, kann die Lehrkraft als Unterstützung Sätze vorgeben (Schwierigkeit an Lerngruppe anpassen).

Durch das Gruppenpuzzle kennen die SuS die Geheimschriften/Geheimsprachen der anderen Gruppen. Daher können die einzelnen Verschlüsselungen gemeinsam in einem Kreisgespräch diskutiert

Literaturverzeichnis

Beutelspacher, A.; Neumann, H. & Schwarzpaul, T. (2005): Kryptografie in Theorie und Praxis. Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk. Wiesbaden: Vieweg + Teubner.

Diekert, V.; Kufleitner, M. & Rosenberger, G. (2013): Diskrete algebraische Methoden, Arithmetik, Kryptographie, Automaten und Gruppen. Berlin: De Gruyter.

Hessisches Kultusministerium (2011): Bildungsstandards und Inhaltsfelder – Das neue Kerncurriculum für Hessen. Primarstufe, MATHEMATIK. Wiesbaden.

Rempe, L. & Waldecker, R. (2009): Primzahltests für Einsteiger. Zahlentheorie - Algorithmik – Kryptographie. Wiesbaden: Springer Spektrum.

Beutelspacher, A.; Neumann, H. & Schwarzpaul, T. (2005): Kryptografie in Theorie und Praxis. Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk. Wiesbaden: Vieweg + Teubner.

Diekert, V.; Kufleitner, M. & Rosenberger, G. (2013): Diskrete algebraische Methoden, Arithmetik, Kryptographie, Automaten und Gruppen. Berlin: De Gruyter.

Hessisches Kultusministerium (2011): Bildungsstandards und Inhaltsfelder – Das neue Kerncurriculum für Hessen. Primarstufe, MATHEMATIK. Wiesbaden.

Rempe, L. & Waldecker, R. (2009): Primzahltests für Einsteiger. Zahlentheorie - Algorithmik – Kryptographie. Wiesbaden: Springer Spektrum.