Thomas BORYS, Karlsruhe

Codes und Verschlüsselungen integrativ im Mathematikunterricht: Vorschlag für ein Curriculum

Der berühmte französische Diplomat und Kryptograf Blaise de Vigenère (1523-1596) schreibt in seinem wichtigsten Werk „Traicté des Chiffres“ von 1586: „Toutes les choses de ce monde ne sont qu’un vray chiffre.“ Aus der Sicht des modernen Menschen ist dieser Satz heute bedeutender denn je, so finden sich im Alltag sehr viele Codierungen z. B. Strichcodes, EAN, ISBN, Brailleschrift. Neben diesen offensichtlichen Codierungen gibt es im Umfeld der modernen Medien eine Vielzahl von Codierungen, die eher versteckt sind z. B. ASCII-Code, Unicode. Des Weiteren gibt es in diesem Zusammenhang auch Codierungen, die das Ziel der Geheimhaltung von Informationen haben z. B. https, Onlinebanking. Im Allgemeinen bezeichnet man diese als Verschlüsselungen. Ziel dieses Artikels ist der Vorschlag eines Curriculums zur integrativen Behandlung der Themen Codierung und Kryptologie im Mathematikunterricht.

1. Didaktische Ausgangspunkte

Der erste Ausgangspunkt bildet das genetische Prinzip. Dieses bezeichnet Erich Wittmann in seinem populären Werk zur Mathematikdidaktik „Grundfragen des Mathematikunterrichts“ als „oberstes Unterrichtsprinzip“. Dank dieser Bedeutung für den Unterricht hat es eine sehr lange Tradition in der pädagogischen und didaktischen Diskussion. Dem genetischen Prinzip begegnet man in verschiedenen Facetten beispielsweise in Form des historisch-, organisch-, logisch- und psychologisch-genetischen Prinzips. Vor allem das historisch-genetische Prinzip wird bei der Erstellung des Curriculums berücksichtigt. Darunter versteht man beispielsweise nach Felix Klein: „Er [der Unterricht] sollte, an die natürliche Veranlagung der Jugend anknüpfend, sie langsam auf demselben Wege zu höheren Dingen und schließlich auch zu abstrakten Formulierungen führen, auf dem sich die ganze Menschheit aus ihrem naiven Urzustand zu höheren Erkenntnis gerungen hat!“ (Klein 1908).

Der zweite Ausgangspunkt bildet die Feststellung, dass man mit Inhalten aus der Codierung und Kryptologie in der Lage ist, die fundamentalen Ideen der Mathematik zu thematisieren (vgl. dazu Borys 2009, 2010), daher bietet sich gerade der Mathematikunterricht für die integrative Behandlung dieser Thematik an.

Der dritte Ausgangspunkt bildet die folgende Überlegung von Heinrich Winter: „Der Mathematikunterricht sollte anstreben, ... Erscheinungen der

Welt um uns, die uns alle angehen oder angehen sollten, aus Natur, Gesellschaft und Kultur in einer spezifischen Art wahrzunehmen und zu verstehen, ...“ (Winter 1995). Um diesem Anspruch gerecht zu werden, fordern die GDM und die MNU in einer Stellungnahme zur „Empfehlung der Kultusministerkonferenz zur Stärkung der mathematisch-naturwissenschaftlichen-technischen Bildung“ von 2010: „Ein zeitgemäßer Mathematikunterricht muss die von digitalen Medien geprägte Lebenswelt von Schülerinnen und Schüler berücksichtigen“. (Weigand 2010) Das bedeutet, dass die Thematik Codierung und Kryptologie entsprechend beachtet werden muss. Diesen Techniken, bedienen sich täglich die „modernen Menschen“, allerdings ohne sich dessen bewusst zu sein. Des Weiteren sind diese Themen sehr mathematikhaltig, Hans Werner Heymann meint dazu, „Diejenige Mathematik, auf der unser Lebensstandard beruht, ist in der Technik, die wir nutzen, sozusagen unsichtbar eingebaut. Sie macht sich selbst, aus der Sicht des Techniknutzers, überflüssig.“ (Heymann 1996) Timo Leuders meint dazu, dass an exemplarischen Beispielen eine Weltorientierung vermittelt werden soll, die die Zusammenhänge zwischen Mathematik und Technologie wieder offenbar werden lassen. (Leuders 2003) Genau dieses Ziel ist mit dem folgenden Curriculum beabsichtigt. Weitere Ausgangspunkte sind das Spiralprinzip nach Bruner, Vernetzungen von Mathematik mit anderen Gebieten, etc.

2. Vorstellung des Curriculums

Für die integrative Behandlung der Codierung und Kryptologie im Mathematikunterricht ist gedacht, dass sich diese Themen wie ein roter Faden durch den Mathematikunterricht der Klassen 5-12 ziehen.

Das Kernziel ist in Form einer Leitidee formuliert: *Codierung und Kryptologie sind fundamentale, historisch bedeutsame und facettenreiche Kulturtechniken mit wichtigen Anwendungen in der modernen Kommunikations- und Wissensgesellschaft.*

Der Kursus beginnt in den Klassen 5/6 mit einfachen binären Codierungen, z. B. der Blindenschrift und dem ASCII-Code. Bei den genannten Beispielen handelt es sich um Codes, die im Alltag der Schüler vorkommen und einen starken Bezug zum Binärsystem aufweisen. Der Morsecode stellt in diesem Zusammenhang ein weiteres Beispiel dar, allerdings weist dieser keinen Alltagsbezug auf. Wenn man die Idee der Codierung sehr eindrucksvoll unterstützen möchte, bieten sich das Flaggenalphabet oder ein Fackelcode an. Schließlich wird das Thema Codierung durch die Codes im Supermarkt (EAN) und im Buchhandel (ISBN) sehr alltagsnah abgerundet.

Dabei ist aus der Seite der Codierungstheorie vor allem die Fehlererkennung durch die Prüfzifferberechnung hervorzuheben.

Klassenstufe	Thema	mathematische Inhalte
5/6	einfache Codierungen: – Blindenschrift, *Morsecode*, ASCII – *Flaggenalphabet* – EAN/ISBN kombiniert mit Strichcodes einfache Transpositionsverfahren: – Anagramme, Skytale – Fleissner-Schablone einfache Substitutionsverfahren (monoalphabetische Verschlüsselungen): – z. B. Freimaurerverschlüsselung – Cäsar-Verschlüsselung einfache Kryptoanalyse homophone Verschlüsselungen	Binärsystem geometrische Mustererkennung Grundrechenarten Permutation geometrische Abbildungen Division mit Rest Häufigkeitsanalyse
7/8	Polyalphabetische Verschlüsselung – Vigenère-Verfahren – Einmalschlüssel (One-Time-Pad) – Kasiski-Test	Modulorechnung
9/10	Huffman-Codierung Schlüsselaustauschverfahren nach Diffie-Hellman	Wurzelbäume Potenzieren, Modulorechung
11/12	RSA-Verfahren El Gamal-Verschlüsselung	Potenzieren, Modulorechnung

Übersicht des Curriculums zur integrativen Behandlung der Codierung und Kryptologie mit exemplarischen Bezügen zu mathematischen Inhalten.

Im ersten Durchgang durch die Kryptologie sollten die beiden Basisverschlüsselungen Transposition und Substitution thematisiert werden. Die Reihenfolge, ob Transposition oder Substitution zuerst behandelt wird, spielt keine Rolle. Beginnt man beispielsweise mit den Transpositions-verschlüsselungen, bieten sich Anagramme und die Skytale als Einstieg in dieses Thema an. Auch die Gartenzaunmethode und geometrische Verschlüsselungen sind dafür geeignet. Allerdings ist die Skytale wegen ihres tatsächlich in der Geschichte nachgewiesenen Einsatzes zu bevorzugen. Erst in einem zweiten Schritt sollte die Fleissner-Verschlüsselung behandelt werden. Diese ist gerade wegen ihrer Bezüge zur Mathematik genauer gesagt zur Geometrie sehr interessant. Zur Einführung in die Substitutionsverfahren sind Verschlüsselungen mit Fantasiezeichen sehr geeignet, da sie in besonderem Maße den Rätselinstinkt der Schüler wecken und andererseits ihre Kreativität beim Erfinden eigener Zeichen fördern. Erst in einem zweiten Schritt sollte die Cäsar-Verschlüsselung behandelt werden, da es sich hierbei um eine systematische Substitution handelt. Durch eine einfache Häufigkeitsanalyse und homophoner Verschlüsselung wird der

erste Durchgang durch die Kryptologie abgerundet. Zur Fortsetzung der Kryptologie in den Klassen 7-8 empfiehlt sich das Vigenère-Verfahren, es knüpft passgenau an die Idee des Cäsar-Verfahrens aus den Klassen 5/6 an. Die Verschlüsselung mit Einmalschlüsseln ist in diesem Zusammenhang das Paradebeispiel für einen unknackbaren Code und sollte deshalb nicht vergessen werden. Die Idee der Kryptoanalyse wird durch den Kasiki-Test passend fortgesetzt. Durch die bisherigen Themen in den unteren Klassen ist die Behandlung symmetrischer Verschlüsselungen abgeschlossen. Weitere Verfahren, wie z. B. DES oder AES, bringen nicht wesentliche neue Ideen, sie bedienen sich auch nur der Substitution und der Transposition als Verschlüsselungsmethode. Die ASCII-Codierung und der Morsecode werden sehr gut durch den Huffman-Code in den Klassen 9/10 weitergeführt und rücken vor allem den Aspekt der Datenkompression in den Fokus der Schüler. Außerdem bedient man sich dabei moderner mathematischer Hilfsmittel wie Graphen. Zur Fortführung der Kryptologie ist das Diffie-Hellman-Schlüsselaustausch-verfahren geeignet, da es den alten kryptologischen Traum, die öffentliche Vereinbarung eines geheimen Schlüssels verwirklicht und ihm eine besondere mathematische Modellierung zugrunde liegt. Schließlich wird durch die RSA- und El Gamal-Verschlüsselungen in der Oberstufe (Klasse 11-12), die in den alltäglichen Computeranwendungen vorkommen, der integrative Kursus durch die Kryptologie abgerundet.

Literatur

Borys, T. (2009): Codierungen im Spiegel der fundamentalen Ideen der Mathematik. In: Beiträgen zum Mathematikunterricht

Borys, T. (2010): Welche Vernetzungsmöglichkeiten bietet die Kryptologie? In: Beiträgen zum Mathematikunterricht

Heymann, H.W. (1996): Allgemeinbildung und Mathematik. Aus der Reihe: Studien zur Schulpädagogik und Didaktik Band 13, Weinheim und Basel: Beltz Verlag

Klein, F. (1908): Elementarmathematik vom höheren Standpunkt aus. Teil 1: Arithmetik, Algebra, Analysis. Leipzig: B. G. Teubner

Leuders, T. (Hrsg.) (2003). Mathematik Didaktik – Praxishandbuch für die Sekundarstufe I und II. Berlin: Cornelsen Scriptor

Weigand, H.-G., & Langlet, J. (2010). Stellungnahme der Gesellschaft für Didaktik der Mathematik ..., Mitteilungen der GDM, 89, S. 32-33

Winter, H. (1995). Mathematikunterricht und Allgemeinbildung. Bezugsquelle: Universität Bayreuth
URL: http://blk.mat.uni-bayreuth.de/material/db/46/muundallgemeinbildung.pdf
(Stand: 24.02.2011)

Wittmann, E. (1981). Grundfragen des Mathematikunterrichts (6. Auflage). Braunschweig: Friedrich Vieweg & Sohn Verlagsgesellschaft mbH