Mathematisch interessierte Köpfe anregen (MiKa!)

Ein Konzept zur Begabtenförderung im Fach Mathematik für das Gymnasium

Maike Schindler – Eva-Maria Schauf – Jörn Hagen Hesse

Online-Ergänzung

MNU 68/6 (15.11.2015) Seiten 1–3, ISSN 0025-5866, © Verlag Klaus Seeberger, Neuss

2.2.2 Klasse 7/8 – »Geheimniskrämerei?!« Einblicke in die Kryptologie

Die Kryptologie bietet nicht nur durch die Aktualität der NSA-Affäre Unterrichtsinhalte, die für Schüler einen stark motivierenden Charakter haben. Das Entwickeln und Entschlüsseln von Geheimcodes fasziniert Lernende gleichermaßen, was beide Bereiche der Kryptologie – die Kryptographie und die Kryptoanalyse – für die Thematisierung im Rahmen einer IBF attraktiv macht.
Der Einstieg in den Themenkomplex erfolgte durch eine Problemstellung, in der ein kurzer Satz gegeben war, der monoalphabetisch mit dem Caesar-Code chiffriert wurde (Kasten 3). Kasten 4 stellt die Hintergrundinformationen für die Lehrkräfte dar.

Caesar-Code

- Entschlüssele folgenden Satz:
  EYD GWI OWD QJZ OEA CPA
- Welche Eigenschaften vereinfachen oder erschweren das Entschlüsseln? Warum? Notiere Kriterien, die eine Verschlüsselung sicher machen können.

Kasten 3. Aufgabenstellung zum Caesar-Code

Da die Kryptologie weder im Mathematik- noch im Informatikunterricht zu den Kernthemen gehört, setzten sich die Lernenden ohne spezifische Vorkenntnisse in einem kreativen Prozess mit der Dechiffrierung auseinander. Dabei entdeckten sie erste Kriterien, die eine Chiffrierung sicherer machen können. Da der Satz »Ich kam, sah und siegte« durch eine einfache Verschiebung des Alphabets codiert wurde, erarbeiteten die Schülerinnen und Schüler hierbei unter anderem folgende Kriterien:

- Die Verschiebung der festen Reihenfolge der Buchstaben im Alphabet erleichtert die Decodierung.
- Die Bündelung zu »Drei-Buchstaben-Wörtern« hebt die Wortgrenzen des Klartextes auf.
- Fehlende Satzzeichen erschweren die Dechiffrierung.

Anschließend konnten die Schüler kriteriengeleitet einen eigenen Geheimcode entwickeln. Dabei zeigte sich eine immense Fülle an Ideen. Naheliegend waren Zahlencodes, bei denen Zahlen die einzelnen Buchstaben codieren sollten, oder die Verwendung von Sonderzeichen. Der anschließende Austausch über die erschaffenen Geheimcodes machte das Prinzip von KERCKHOFF (vgl. HEMPEL 1995) einsichtig, dass der Algorithmus der Ver- und Entschlüsselung bekannt sein sollte und lediglich die Eingangsgrößen, der sogenannte Schlüssel, geheim gehalten werden muss. So wird bei der Überlieferung der geheimen Botschaft zwischen dem Sender und dem Adressaten nicht direkt der Algorithmus zum Lösen mitgeliefert, sondern nur der Schlüssel (hier: Verschiebung des Alphabets um x Stellen) im Vorhinein abgesprochen.

Im Anschluss daran erarbeiteten die Schüler ein ebenfalls monoalphabetisches, aber weiterführendes und damit schwieriger zu dechiffrierendes Verschlüsselungsverfahren, in dem der Schlüssel, in diesem Fall ein Schlüsselwort und ein Schlüsselbuchstabe, eine komplexere Rolle bei der Verschlüsselung spielt (Abb. 7).

In einer weiteren Problemstellung entschlüsselten die Lernenden einen Text, der monoalphabetisch mithilfe eines Schlüsselwortes und eines Schlüsselbuchstaben verschlüsselt wurde und eine Länge von etwa 70 Wörtern hatte. Dabei lernten sie die Möglichkeit einer Dechiffrierung ohne Schlüsselwort und Schlüsselbuchstaben kennen und setzten sich zunächst ausgie-

Monoalphabetische Verschlüsselung

Caesar 3 – Verschlüsselung:

Bei der Caesar 3 – Verschlüsselung wird das Klartextalphabet um drei Buchstaben verschoben, sodass jeder Buchstabe einem anderen zugeordnet ist:

Klartextalphabet:	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
Geheimtextalphabet:	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

So kann z. B. die Aussage »Mathematik ist cool« in » PDW KHP DWL NLV WFR RO« übersetzt werden.

Verschlüsselung mit Schlüsselwort und Schlüsselbuchstabe:

Häufig wird die Methode des Schlüsselwortes verwendet, d. h. Sender und Empfänger vereinbaren ein **Schlüsselwort** und einen **Schlüsselbuchstaben**.

Zur Vereinfachung wird folgendes angenommen:

Schlüsselwort: MATHEMATIK Schlüsselbuchstabe: H

Zur Chiffrierung werden nun die im Schlüsselwort mehrfach auftretenden Buchstaben bei Wiederholung gestrichen, wir erhalten also MATHEIK.

Dann wird der Rest des Schlüsselwortes unter das Klartextalphabet geschrieben, beginnend beim Schlüsselbuchstaben. Es folgt das Auffüllen der restlichen Alphabetbuchstaben.

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

So kann z. B. die Aussage »Mathematik ist cool« in » ISJ MXI SJA HAG JVB BE« übersetzt werden.

Kasten 4. Hintergrundinformationen zur Verschlüsselung (vgl. HEMPEL 1995)

MNU 68/6 (15.11.2015), ISSN 0025-5866, © Verlag Klaus Seeberger, Neuss

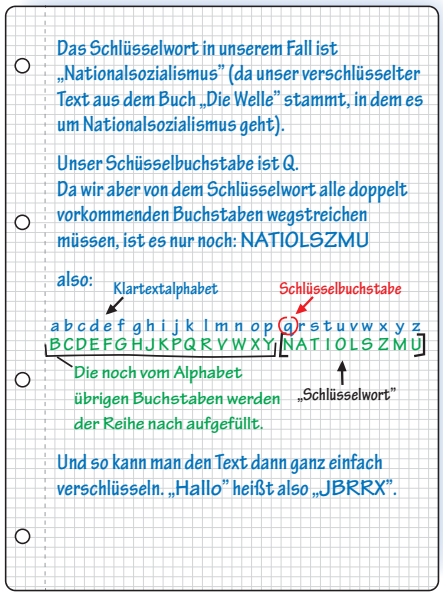

Abb. 7. Schülerlösung zur Chiffrierung mit Schlüsselwort und Schlüsselbuchstabe

big mit einer Häufigkeitstabelle (HEMPEL 1995, 6) auseinander, in der die Vorkommenshäufigkeit aller Buchstaben und Bigramme (z. B. ch, er, ei) in der deutschen Sprache dargestellt war. Dabei erkundeten sie die Zusammenhänge zur Entschlüsselung (»Welcher Buchstabe kommt in der Geheimschrift am häufigsten vor?«, »Welcher Buchstabe könnte dies im Klartextalphabet sein?«).

Folgende Gemeinsamkeiten wurden dabei in Augenschein genommen (Abb. 8).

- Die 2–3 häufigsten Buchstaben sind leicht zu erkennen.
- Kurze Wörter wie »ein«, »und«, »der«, »die«, »das« helfen beim Zuordnen weiterer Buchstaben.
- Die fehlenden Buchstaben können durch die Vervollständigung halbfertiger Wörter hergeleitet werden.

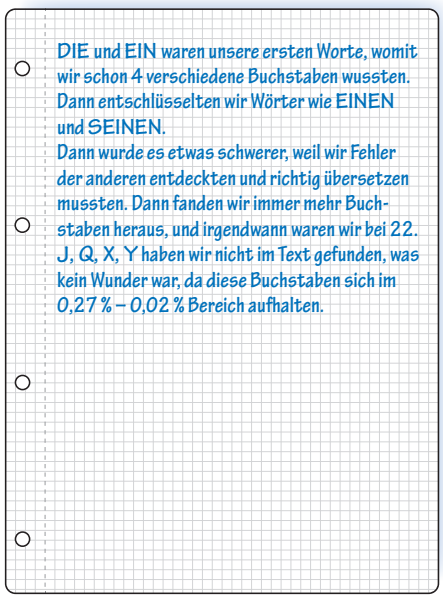

Abb. 8. Forschungsheftеintrag zur Entschlüsselung mit einer Häufigkeitstabelle

Im Rahmen der Besprechung der Auffälligkeiten und Gemeinsamkeiten wurde von allen Schülern die – im Vergleich zum Caesar-Code – zwar erheblich aufwändigere, aber trotzdem noch relativ einfach zu entschlüsselnde Methodik hervorgehoben. Es wurden Überlegungen angestellt, wie man solch eine Verschlüsselung sicherer gestalten kann. So wurde über die Einführung von Sonderzeichen (0–9, !, ?, %, usw.) diskutiert und die Verwendung von mehreren Schlüsselwörtern vorgeschlagen, so dass ein Buchstabe im Klartextalphabet nicht mehr eindeutig einem Buchstaben im Geheimtextalphabet zugeordnet wird. Damit war die Idee der polyalphabetischen Chiffrierung (HEMPEL 1995) als sicherere Codierung naheliegend. Bei dieser können einem Buchstaben des Klartextalphabetes mehrere Buchstaben im Geheimtextalphabet zugeordnet werden, womit die Entschlüsselung durch Häufigkeitstabellen nicht mehr möglich ist. Eine Behandlung dieser Thematik ist im Unterricht zwar möglich, jedoch ist die eigenständige Bearbeitung durch die Schülerinnen und Schüler aufgrund des größeren Entwicklungsaufwands einer solchen Chiffrierung stark eingeschränkt. Eine sinnvolle Alternative kann ein Exkurs in die Modulo-Rechnung bieten, um anschließend das RSA-Verfahren zu besprechen (STEGER 2002, 96ff.). Dies wurde jedoch bislang noch nicht im Unterrichtseinsatz erprobt.

Bei den Schülern konnte während dieser Unterrichtssequenz zur Kryptologie eine konstant hohe Motivation beobachtet werden. Die meisten Lernenden hatten bereits Erfahrungen mit einfachsten Verschlüsselungen gemacht – sei es im Zusammenhang mit dem »Zettelchenschreiben« mit Geheimschrift im Unterricht oder mit dem »Geheimschreiber«, bei dem man das Gelesene mithilfe einer Flüssigkeit wieder sichtbar machen kann. Insbesondere die Entschlüsselung von durch Mitschülerinnen und Mitschüler verschlüsselten Texten wurde mit großem Eifer durchgeführt. Bei diesem Vorgehen zeigte sich jedoch, dass sich die von Schülerinnen und Schülern verschlüsselten Texte in Quantität und Qualität stark unterscheiden können, was den Austausch erschweren kann. Angereichert mit geschichtlichen (Cäsar, Enigma) und gegenwartsbezogenen Fakten (E-Mailkonten, NSA) kann dieser Themenbereich die Verknüpfung der alltäglichen Realität mit der Fachwissenschaft Mathematik an vielen Beispielen verdeutlichen.

Literatur

HEMPEL, T. (1995). Einführung in die Kryptologie. *http://www.tinohempel.de/info/info/kryptografie/download/krypto.pdf* (23.06.2014).

STEGER, A. (2002). *Diskrete Strukturen. Band 1. Kombinatorik – Graphentheorie – Algebra.* Berlin: Springer.

Dr. MAIKE SCHINDLER, maike.schindler@rub.de, ist am Institut für Naturwissenschaft und Technik an der Örebro Universität in Schweden tätig, Örebro universitet, T2212, Fakultetsgatan 1, SE-702 81 Örebro.

EVA-MARIA SCHAUF unterrichtet die Fächer Mathematik und Biologie am Albert-Martmöller-Gymnasium, Oberdorf 9, 58452 Witten.

JÖRN HAGEN HESSE unterrichtet die Fächer Mathematik und Erdkunde am Albert-Martmöller-Gymnasium, Oberdorf 9, 58452 Witten.