THOMAS BORYS; Karlsruhe

Welche Vernetzungsmöglichkeiten bietet die Kryptologie?

Die Kryptologie ist eine sehr alte Wissenschaft. War sie bis vor wenigen Jahrzehnten noch eine Wissenschaft für Regierungen, Militär, Geheimdienste und Spione, so ist sie aufgrund der vielen Anwendungen im Umfeld des Computers in unserem Leben nahezu allgegenwärtig. Man bedient sich ihrer täglich, Beispiele hierzu sind: das Einloggen auf dem E-Mail-Account, Arbeiten auf https-Seiten z. B. beim Onlinebanking und Telefonieren mit dem Handy.

Es stellt sich nun die Frage, welche Vernetzungsmöglichkeiten kryptologische Inhalte mit der Mathematik bieten, damit diese gewinnbringend im Mathematikunterricht eingesetzt werden können.

Ausgangspunkt der Überlegungen ist der Begriff der beziehungsvollen Mathematik im Sinne Freudenthals. Erörtert wird die Frage anhand exemplarischer Beispiele und der fundamentalen Ideen der Mathematik, die hier als Leitlinie zugrunde gelegt werden. Dabei wird folgender eigener Katalog fundamentaler Ideen verwendet: *Algorithmus, funktionaler Zusammenhang, mathematisches Modellieren, Zahl, Messen* und *Ordnen* (das beinhaltet das geometrische Strukturieren und das logische Ordnen). Ihm liegen die Sammlungen fundamentaler Ideen von Humenberger/Reichel, Schreiber, Tietze/Kilka/Wolpers und Heymann zugrunde.

1. Begriffsbestimmungen zur Kryptologie

Die Kryptologie ist die Wissenschaft, die einerseits zur Geheimhaltung von Information durch Verschlüsselung (Kryptografie) dient. Andererseits beinhaltet sie die Kunst des Entschlüsselns (Kryptoanalyse), die ihrerseits auch die Sicherheit von Verschlüsselungen analysiert. Diese Begriffsauffassung wird den folgenden Ausführungen zugrunde gelegt. (Allerdings gibt es auch andere Auffassungen, siehe z. B. Beutelspacher.)

Es gibt grundsätzlich zwei Methoden der Geheimhaltung. Die erste Möglichkeit besteht im *Verbergen der Existenz einer Information*, d. h. alleine durch das Verstecken der Information wird diese geschützt. Diese Methode gehört in den Bereich der Steganografie. Beispiele hierfür sind die Verwendung von Geheimtinte (z. B. Zitronensaft) und der berühmte doppelte Boden. Eine zweite Möglichkeit besteht im *Verschleiern der Information*, d. h. hier wird die Information durch eine geschickte Verschlüsselung geschützt. Diese Methode gehört in die Kryptografie.

2. Vernetzungsmöglichkeiten der Kryptologie mit der Mathematik

Für diesen Artikel werden die Vernetzungsmöglichkeiten exemplarisch anhand der fundamentalen Ideen des funktionalen Zusammenhangs und des mathematischen Modellierens gezeigt (weitere Beispiele vgl. Borys).

2.1 Funktionaler Zusammenhang

Der funktionale Zusammenhang ist bei der Kryptologie von zentraler Bedeutung. Grob gesprochen wird durch die Verschlüsselungsfunktion der Klartext, der die zu übermittelnde Information enthält, auf einen Geheimtext, der für Fremde nicht lesbar ist, abgebildet. Durch die Injektivität der Verschlüsselungsfunktion ist der Empfänger in der Lage, den Geheimtext zu entschlüsseln. Im Schaubild ist das durch den Doppelpfeil versinnbildlicht.

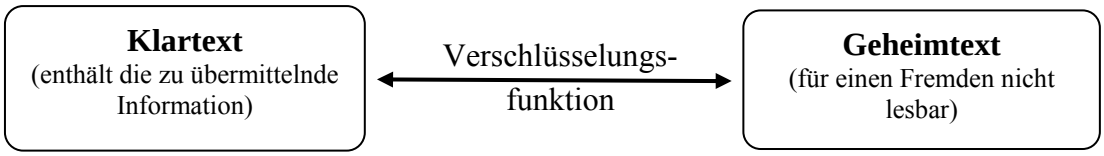

Abbildung 1

Sehr deutlich tritt die fundamentale Idee des funktionalen Zusammenhangs bei den beiden Basistransformationen: *Transposition* und *Substitution* zum Verschleiern der Information zutage.

Mit *Transposition* ist gemeint, dass zur Verschlüsselung die Positionen der Schriftzeichen des Klartextes verändert werden, sodass dieser nicht mehr zu lesen ist, so wird z. B. aus dem Klartext `Edgar Allan Poe` der Geheimtext `der analoge Alp`. Wenn wie im Beispiel eine sinnvolle Buchstabenfolge entsteht, bezeichnet man diese als Anagramm. Das Kennzeichen dieser Verschlüsselungsmethode ist also, dass alle Schriftzeichen erhalten bleiben und nur deren Position im Text geändert wird. Mathematisch steckt dahinter die Permutation. Wenn man die Leerzeichen auch als Buchstaben auffasst, wäre P die dazu gehörige Permutation.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 1 & 10 & 5 & 3 & 4 & 7 & 8 & 14 & 13 & 6 & 12 & 15 & 9 & 11 \end{pmatrix}$$

Weitere Beispiele für Transpositionsverfahren sind die Skytala von Sparta und die Verschlüsselungsschablonen nach Fleißner.

Mit Substitution ist gemeint, dass zur Verschlüsselung die Schriftzeichen des Klartextes durch andere Schriftzeichen ersetzt werden. Ein Beispiel hierfür ist die bekannte Cäsar-Verschlüsselung, die auf Gaius Julius Caesar (100 – 44 v. Chr.) zurückgeht. Jeder Buchstabe des Klartextes wird durch den Dritten ihm im Alphabet folgenden Buchstaben ersetzt. Die Buchstaben x, y, und z werden mit den Buchstaben a, b, c verschlüsselt. Für den

Klartext `Edgar Allan Poe` erhält man `Hgjdu Diidq Srh`. An dieser Stelle sind zwei bijektive Funktionen zu erkennen:

- Zuordnung der Klartextbuchstaben zu den Geheimtextbuchstaben, wobei der Definitions- und der Wertebereich gleich sind,
- Zuordnung des Klartextes zu genau einem Geheimtext.

Weitere Beispiele in diesem Zusammenhang sind der Freimaurercode und die Verschlüsselung von Karl dem Großen (vgl. Bauer). Allerdings sind bei den genannten Beispielen Definitions- und Wertebereich der Verschlüsselungsfunktion unterschiedlich.

Dass es sich, wie in Abbildung 1 dargestellt, bei der Zuordnung von Klar- zum Geheimtext nicht immer um eine Verschlüsselungsfunktion handelt, wird an den homphonen Verschlüsselungen deutlich. Bei diesen ist die Zuordnung des Klar- zum Geheimtext nicht mehr eindeutig. Beim Verschlüsseln ein und desselben Klartextes können unterschiedliche Geheimtexte entstehen. Somit liegt dann keine Verschlüsselungsfunktion mehr vor, sondern eine Verschlüsselungsrelation.

2.2 Mathematisches Modellieren

Frage: Können zwei Personen einen geheimen Schlüssel austauschen, ohne dass sie sich je im Leben persönlich begegnet sind?

Die Antwort lautet ja. Allerdings beantworteten diese Frage Martin Hellman und Whitfield Diffie erst 1976 in ihrem Artikel *New Direction in Cryptography*. Ziel dieses Verfahrens ist die sichere Vereinbarung eines gemeinsamen geheimen Schlüssels (K) in Form einer Zahl über eine unsichere, d. h. einer öffentlichen Verbindung. (Diffie und Hellman beschrieben ihre Verfahren sehr allgemein.) Im Folgenden wird das Verfahren spezialisiert auf einen Restklassenkörper Z_q mit q als Primzahl dargestellt.

Zu Beginn der Kommunikation vereinbaren die Kommunikationspartner, nennen wir sie A(lice) und B(ob), eine gemeinsame Primzahl q und eine weitere Zahl g (sog. Generator), dies sollte eine Primitivwurzel von q sein. Diese beiden Startinformationen können ruhig über einen unsicheren Kanal, d. h. für einen Unbefugten Dritten lesbar, übermittelt werden. Beide Partner wählen sich aus der Menge $\{1, \ldots, q\text{-}2\}$ eine beliebige Zahl. Sagen wir Alice wählt a und Bob wählt b. Diese beiden Zahlen werden nicht ausgetauscht, sondern sind streng geheim.

Alice berechnet: $x_A = g^a \bmod q$ und gibt diese Zahl an Bob weiter.

Bob berechnet: $x_B = g^b \bmod q$ und gibt diese Zahl an Alice weiter.

Auch der Austausch dieser Information kann wieder über einen unsicheren Kanal erfolgen. Aus dieser Information können beide Kommunikationspartner wie folgt ihren gemeinsamen Schlüssel *K* berechnen:

A berechnet	B berechnet
$K = x_B^a \bmod q$	$K = x_A^b \bmod q$

Obwohl beide den Schlüssel K ganz unterschiedlich berechnen, erhalten sie beide denselben Schlüssel. Bei diesem Schlüssel handelt es sich um einen geheimen Schüssel, den nur die beiden Kommunikationspartner kennen. Da x_A und x_B durch die diskrete Exponentialfunktion, die eine Einwegfunktion darstellt, berechnet werden, ist ein Angreifer, der die Zahlen q, g, x_A und x_B abgefangen hat, nicht in der Lage a bzw. b zu berechnen. Genau diese Stelle ist Kern der mathematischen Modellierung, denn durch die Mathematik ist sichergestellt, dass die Kommunikation geheim ist. Die Sicherheit des Verfahrens hängt hauptsächlich an der Wahl der beiden Zahlen q und g. In der Praxis reichen üblicherweise Primzahlen q der Größenordnung 2048 Bit aus.

Insgesamt wird an den Ausführungen deutlich, dass die Kryptologie viele Vernetzungsmöglichkeiten mit der Mathematik bietet, daher sind kryptologische Themen eine besonders lohnenswerte Bereicherung für den Mathematikunterricht.

Literatur

Bauer, F. (1997): *Entzifferte Geheimnisse*. Berlin, Heidelberg: Springer-Verlag

Beutelspacher, A.; Neumann, H.; Schwarzpaul, T. (2005): *Kryptographie in Theorie und Praxis*. Wiesbaden: Friedrich Vieweg & Sohn/GWV Fachverlag

Borys, T. (2008): *Geheimnisvolle Mathematik - Codierungen im Spiegel der fundamentalen Ideen der Mathematik*. In: *Karlsruher Pädagogische Beiträge*, 69/2008, S. 65-83

Diffie, W.; Hellman, M. E. (1976): *New Directions in Cryptography*. In: *IEEE Transactions on Information Theory*. IEEE 22. Jahrgang, Heft 6, S. 644-654.

Freudenthal, H. (1977): *Mathematik als pädagogische Aufgabe.* Band 1, 2. Auflage, Stuttgart: Klett Verlag

Heymann, H. W. (1996). *Allgemeinbildung und Mathematik*. Weinheim: Beltz Verlag

Humenberger, J., Reichel H.-Ch.: *Fundamentale Ideen der angewandten Mathematik*. Aus der Reihe Lehrbücher und Monographien zur Didaktik der Mathematik Band 31, Mannheim: Bibliographisches Institut & F.A. Brockhaus

Schreiber, A. (1979). *Universelle Ideen im mathematischen Denken – ein Forschungsgegenstand der Didaktik.* In: mathematica didactica 2, 165-171

Tietze, U.-P., Klika, M., Wolpers, H. (Hrsg.) (2000). *Mathematikunterricht in der Sekundarstufe II.* Band 1, 2. Auflage, Wiesbaden: Vieweg,