Didaktische Hinweise

Die Kryptologie ist sicher einer der Bereiche der Mathematik und Informatik, der am nächsten am Alltag liegt und auch am motivierendsten für die Schülerinnen und Schüler sein kann. Gleichzeitig ist die Wissenschaft der Verschlüsselung aufgrund ihrer über 2000 Jahre alten Geschichte so vielfältig, dass eine Wahl des genauen Themas schon zur Herausforderung wird. Die Komplexität wächst von monoalphabetischen Verschlüsselungen in der Antike (Caesar-Chiffre) über polyalphabetischen Verschlüsselungen (Vigenère-Verschlüsselung) im 16. Jahrhundert bis hin zu asymmetrischen Verschlüsselungen (RSA) im 20. Jahrhundert. Kryptographie ist heute in höchstem Maße alltagsrelevant, von der Sicherheit von Kommunikationsformen (Chats, Telefonate, Dateiverschlüsselung, Logins, online-Banking) bis hin zu Restriktionen durch Ländercodes oder dem Kopierschutz von DVDs.
Die Frage ist nun, wie tief man in die Thematik einsteigen will und wieviel Zeit man investieren will.
Historisch lassen sich von Maria Stuart (Babington-Komplott) über den Wilden Westen (Beale-Chiffre) bis hin zum ersten und zweiten Weltkrieg (Enigma, Bletchley-Park) zahlreiche historisch interessante Geschichten in der Kryptologie finden.
Auch die Einschätzung, dass die Zahlentheorie als Teilbereich der Mathematik zwar nett ist, aber keine praktische Relevanz besitzt (Hardy), kann für Schülerinnen und Schüler motivierend sein, sich mit Mathematik zu befassen.
Die Kryptoanalyse spricht Schülerinnen und Schüler besonders an, weil hier die Möglichkeit besteht, Geheimnisse zu knacken. Mit Computerprogrammen lassen sich hier die Grenzen der klassischen mono- und polyalphabetischen Verfahren gut aufzeigen. Am Beispiel des Voynich-Manuskript oder der Skulptur Kryptos vor dem Hauptquartier der CIA kann man einen schnellen Blick auf noch ungeknackte Rätsel werfen

Das Geheimnisteilen von Shamir ist ein interessantes Beispiel, wie man ganzrationale Funktionen n-ten Grades nutzen kann, um Informationen zu verteilen. Ein Arbeitsblatt und Aufgaben hierzu finden sich weiter unten.

Weiterführende Literatur:
http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie
www.spiegel.de/wissenschaft/technik/code-raetsel-krypto-kuenstler-gibt-hinweis-auf-cia-geheimnis-a-730308.html
http://scienceblogs.de/klausis-krypto-kolumne/2013/10/13/top-25-der-ungeloesten-verschluesselungen-platz-1-bis-25-im-schnelldurchlauf/
https://de.wikipedia.org/wiki/Beale-Chiffre

Unterrichtsverlauf

Ein Unterrichtsverlauf soll hier nicht vorgegeben werden, weil dieser entsprechend der gewählten Schwierigkeit unterschiedlich aussehen kann.

Es erscheint jedoch sinnvoll, am Ende über Restklassenrechnen, Faktorisierung von großen Zahlen und den Kleinen Satz von Fermat auf das asymmetrische Verfahren von Rivest-Shamir-Adelman (RSA) zu kommen.

Methodische Hinweise

Teile der Unterrichtseinheit können sicher selbstorganisiert durchgeführt werden, für die Einführung in Restklassenrechnen, Faktorisierung und den Kleinen Satz von Fermat wird eine eher lehrerzentrierte Form empfohlen.

Fachliche Hinweise

keine

Unterrichtsmaterialien

Digitale Werkzeuge, Videos, …..

Filme und Filmsequenzen:

Enigma – Das Geheimnis, 2001

Verschlüsseln - Damit geheime Daten geheim bleiben, von Informatik Biber, www.youtube.com/watch?v=ONVkrL7heRw

Unterrichtseinheiten:

Unter www.cryptoportal.org/ sind zahlreiche Unterrichtseinheiten zum Thema Kryptographie gesammelt.

Bei Matheprisma sind drei Selbstlerneinheiten vorhanden.

www.matheprisma.uni-wuppertal.de/Module/Caesar/ Cäsar

www.matheprisma.uni-wuppertal.de/Module/RSA/ RSA

www.matheprisma.uni-wuppertal.de/Module/DES/ DES

Webseiten:

Unter www.cryptool.org/de/ ist einen der größten Sammlungen zum Thema, unter anderem sind hier zwei Lernprogramme. Die Webseite ist aus einem Projekt einer großen Bank entstanden, die ihre Mitarbeiter sensibilisieren wollte.

Im Internet gibt es eine riesige Anzahl an Seiten, die zum Thema passen. Eine Linksammlung ist z.B. unter http://wikis.zum.de/zum/Kryptographie zu finden.

Unter www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/cc-interaktiv/index.htm ist eine Sammlung von Beiträgen zur Thematik, die im Rahmen einer Vorlesung an der PH Karlsruhe erstellt wurde.

Programme:

Cryptool: Open-Source-Programm für Windows, das Möglichkeiten zur Kryptographie und Kryptoanalyse bietet. Das Programm beinhaltet einen E-Learning-Anteil. Download unter www.cryptool.org/de/ct1-download

Arbeitsblätter mit Beispielen
Shamir-Polynome

„Unter *Secret Sharing* versteht man ein Verfahren, eine geheime Information *S* auf *n* Teilnehmer aufzuteilen, so dass das Geheimnis *S* nur durch die Zusammenarbeit von hierfür qualifizierten Gruppen der Teilnehmer rekonstruiert werden kann. Wenn darüber hinaus gewährleistet ist, das eine nicht-qualifizierte Gruppe *keinerlei*, nicht einmal stochastische, Information über *S* erhält, so bezeichnet man das Verfahren als *perfekt*.
Eine weitergehende Forderung ist die *Robustheit* des Verfahrens. Hierbei wird verlangt, dass das Verfahren auch dann noch sicher bleibt, wenn sich einzelne Teilnehmer unehrlich verhalten, indem sie etwa Informationen zurückhalten oder verfälschen.
Die grundlegende Aufgabe von Secret Sharing besteht in der sicheren Aufbewahrung der durch kryptographische Verfahren angefallenen geheimzuhaltenden Schlüssel. Diese Verfahren sind mittlerweile derart ausgefeilt, dass es ohne den passenden Schlüssel nicht möglich ist, eine verschlüsselte Datei nutzbar zu machen, obwohl die verwendeten Algorithmen allgemein bekannt sind. Auch wenn dies natürlich gerade der Sinn einer Verschlüsselung ist, entsteht ein gewaltiges Problem im Verlustfalle des Schlüssels, was z.B. durch das Abhandenkommen eines Datenträgers leicht geschehen kann.
Daher ist man versucht, den Schlüssel auf mehrere Personen oder Orte zu verteilen, so dass einerseits eine gewisse Anzahl dieser Archive benötigt werden (Schutz gegen unbefugten Zugriff), aber andererseits auch nicht alle (Schutz gegen Datenverlust).
Eine andere in der Literatur häufig genannte Anwendung ist die Authentifikation wichtiger Dokumente für ein Unternehmen, z.B. von Schecks. Hierbei kommen Verfahren zur digitalen Signatur zum Einsatz, die ebenfalls auf Schlüsseln basieren. Ein Unternehmen kann etwa daran interessiert sein, dass nur Manager von ausreichendem Rang und Anzahl gewisse digitale Unterschriften leisten können.
Nicht zuletzt gibt es militärische Anwendungen. Eine Atommacht wird sicher sorgfältig darauf achten, dass die Aktivierungssequenzen ihrer Raketenbasen nur dann eingeleitet werden können, wenn kein Zweifel über die Autorität des Initiators und die Authentizität der diesbezüglichen Befehle herrscht.“

Quelle: Thilo Planz: www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T12/secret_sharing.htm

Zehn Geheimnisträger arbeiten an einem geheimen Projekt. Die Informationen sind nur zugänglich, wenn mindestens sechs beliebige Geheimnisträger bzw. ihre Schlüssel vorhanden sind.

Als Modell hierfür dienen ganzrationale Funktionen. Besitzt man n Punkte Pi(xi|yi), so kann man genau eine ganzrationale Funktion (n-1)-ten Grades durch diese Punkte legen, mit (n-1) Punkten geht dies nicht.

Konkret:

Ein Geheimnis wird mit einer ganzr. Funktion 3. Grades verschlüsselt. Die vier anwesenden Geheimnisträger besitzen die Schlüssel P(-1|64), Q(1|2762), R(2|11387) und S(-2|-2857).

Für f(x) gilt: $f(x) = ax^3 + bx^2 + cx + d$

Weiterhin gilt:

Das Problem ist also ein Gleichungssystem mit 4 Gleichungen und 4 Unbekannten. Wenn nur 3 Geheimnisträger anwesend wären, wäre das Gleichungssystem nicht zu lösen. Die Lösung laute a=716, b=972, c=697, d=377

Für f(x) gilt: $f(x) = ax^3 + bx^2 + cx + d$

Weiterhin gilt:

$$\begin{cases} f(-1) = 64 \\ f(1) = 2762 \\ f(2) = 11387 \\ f(-2) = -2857 \end{cases}$$

Der Zugangsschlüssel zum (mathematischen) Schloss ist also die Funktion

$f(x) = 716x^3 + 972x^2 + 697x + 377$ oder 71 69 72 69 73 77 oder _____

Aufgaben:

1) Bestätige, dass das Geheimwort SCHWER lautet, d. h. finde das Polynom zu Q1(-1|42), Q2(1|3466), Q3(0|982) und Q4(-2|-4370) und übersetze die Koeffizienten!

2) Finde das Polynom zu Q1(2|6449), Q2(-1|-382), Q3(-2|-3771) und Q4(0|663). Die Lösung ist die Fortsetzung aus 1)

3) (Partnerarbeit) Verschlüssele ein Wort/einen Text von mindestens 7 Zeichen zu einem Polynom 4. Grades, berechne 5 Schlüssel und lass deinen linken Nachbarn entschlüsseln. Hast du keinen linken Nachbarn, gib deine Aufgabe dem, der ganz rechts in deiner Reihe sitzt.

4) (Bonusaufgabe, für eine sehr gute zusätzliche Note) Schreibe ein Programm mit dem TI-92+, das Texte in Polynome und Punkte umwandelt bzw. umgekehrt.

ASCII-Zeichensatz

ASCII-Zeichensatz

65	66	67	68	69	70	71	72	73	74	75	76	77
a	b	c	d	e	f	g	h	i	j	k	l	m
78	79	80	81	82	83	84	85	86	87	88	89	90
n	o	p	q	r	s	t	u	v	w	x	y	z
32	33	34	40	41	44	46	48	49	.....	56	57	63
	!	"	(	)	,	.	0	1	.....	8	9	?

Weiterführende Literatur:

www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T12/secret_sharing.htm
www.zenger.informatik.tu-muenchen.de/lehre/vorlesungen/konkr_math/02_03/prog/BlattPA2.pdf
Horak, Müller: Mathematik 11, BSV München, 3. Auflage

Aufgaben

Mögliche Klassenarbeitsaufgaben:

1. Erläutere die Funktionsweise des Geheimnisteilens mit Shamir-Polynomen.
2. Gegeben sind folgende Punkte: P(-3|6248), Q(-2|-2070), R(-1|-6822), S(2|738). Wie lautet die Botschaft/das Geheimwort?

ASCII-Zeichensatz

65	66	67	68	69	70	71	72	73	74	75	76	77
a	b	c	d	e	f	g	h	i	j	k	l	m
78	79	80	81	82	83	84	85	86	87	88	89	90
n	o	p	q	r	s	t	u	v	w	x	y	z
32	33	34	40	41	44	46	48	49	.....	56	57	63
	!	"	(	)	,	.	0	1	.....	8	9	?

Weiterführende Literatur

Bücher:

- Borys, Thomas: Codierung und Kryptologie, Vieweg+Teubner Research, 2011
- Simon Singh: Geheime Botschaften, dtv, 2001
- Barnett, I.A.: Some ideas about number theory. National Council of teachers of mathematics, Washington DC, 1972
- Beutelspacher, A.: Kryptologie. Vieweg, Braunschweig/Wiesbaden, 1987
- Beutelspacher; Schwenk; Wolfenstetter: Moderne Verfahren der Kryptographie. Vieweg, Braunschweig, 1998
- Beutelspacher, A.: In Mathe war ich immer schlecht. Vieweg, Braunschweig, 1996
- Conway, John H.: Über Zahlen und Spiele. Vieweg, Braunschweig, 1983
- Conway, John H.; Guy, Richard K.: Zahlenzauber. Birkhäuser Verlag, Basel, Berlin, Boston, 1997
- Endres; Schimmel: Das Mysterium der Zahl. Diederichs Verlag, München, 1992
- Enzensberger, Hans Magnus: Der Zahlenteufel. Carl Hanser Verlag, München, Wien, 1997
- Freund, H.: Elemente der Zahlentheorie. B.G. Teubner, Stuttgart, 1979
- Gallin, Peter (Hrsg.): 101 Mathematikaufgaben. Aulis Verlag Deubner, Köln, 1997
- Kalouinine, L.A.: Primzahlzerlegungen. VEB Deutscher Verlag der Wissenschaften, Berlin, 1971
- Kempermann, T.: Zahlentheoretische Kostproben. Verlag Harri Deutsch, Thun und Frankfurt am Main, 1995
- Konforowitsch, A.G.: Logischen Katastrophen auf der Spur. Fachbuchverlag Leipzig, 1990

- Kracke, Helmut: Mathe-musischen Knobelisken. Dümmler, Bonn, 1992
- Kranzer, Walter: So interessant ist Mathematik. Aulis Verlag Deubner & Co KG, Köln, 1989
- Niven; Zuckerman: Einführung in die Zahlentheorie I. BI - Wissenschaftsverlag, 1991
- Padberg, Friedhelm: Didaktik der elementaren Zahlentheorie. Herder, Freiburg, 1981
- Pieper, H.: Zahlen aus Primzahlen. VEB Deutscher Verlag der Wissenschaften, Berlin, 1974
- Schräder, Wilhelm: Einführung in die Zahlentheorie. Pädagogischer Verlag Schwann, Düsseldorf , 1973
- Schwarz, Friedrich: Einführung in die Elementare Zahlentheorie. B.G. Teubner, Stuttgart, 1998
- Singh, Simon: Fermat's Last Theorem. 4th, 1998
- Wells, David: Das Lexikon der Zahlen. Fischer Taschenbuch Verlag, Frankfurt am Main, 1991
- Worobjow, N.N.: Die Fibonacci Zahlen. VEB Deutscher Verlag der Wissenschaften, Berlin, 1971

Zeitschriften:

- Burau, Werner: Elementare Zahlentheorie. Ernst Klett Verlag, Stuttgart, 1970
- Batzer, Peter: Die Enigma. LOGIN-Verlag, Berlin, 1996
- Becker, Klaus-Ch.; Beutelspacher, A.: Datenverschlüsselung. LOGIN-Verlag, Berlin, 1996
- Beutelspacher, A.: Kryptographie - eine Einführung in die Wissenschaft von der Geheimhaltung der Daten: Codieren und Chiffrieren. MU Der Mathematikunterricht, Friedrich Verlag, Mai 1987
- Glatfeld, Martin: Konzeptionelle Bemerkung zur unterrichtlichen Behandlung von Euklids Beweis der Unendlichkeit der Primzahlmenge. Mathematik Lehren: Primzahlen I: Friedrich Verlag, Heft 57, April 1993b
- Glatfeld, Martin: Über die Verteilung der Primzahlen. Mathematik Lehren: Primzahlen II, Friedrich Verlag, Heft 61, April 1993
- Gorini, Catherine A. : Using Clock Arithmetic to Send Secret Messages. The Mathematic Teacher, Vol 89, No 2, Feb. 1996
- Herget, W.: Artikelnummern und Zebrastreifen, ... ISTRON 3,
- Michl, Martin: So funktioniert Verschlüsselung. CHIP 9/98, Vogel Verlag Würzburg, 1998

- Müller, Horst: Aufgaben über und um Primzahlen. Mathematik Lehren: Primzahlen I: Friedrich Verlag, Heft 57, April 1993
- Ribenboim, Paulo: Primzahlrekorde. Didaktik der Mathematik, Heft 1, 1993
- Scheu, G.: Endeckungen in der Menge der Primzahlen mit DERIVE. Praxis der Mathematik, 3/34, 1992
- Schmundt, Hilmar: Die Macht der Zahlen. konr@d, Gruner + Jahr AG & Co, 1999
- Schubert, Sigrid: Basismechanismen der Informationssicherheit. LOGIN-Verlag, Berlin, 1996
- Schulz, Ralph-Hardo : Primfaktorzerlegung. LOGIN-Verlag, Berlin, 1996
- Schulz, Ralph-Hardo : Primzahlen in öffentlichen Chiffrierverfahren. Mathematik Lehren: Primzahlen II, Friedrich Verlag, Heft 61, April 1993
- Siegler, H.; König, G.: Kleines Primzahllexikon. Mathematik Lehren: Primzahlen II, Friedrich Verlag, Heft 57, April 1993
- Sommer, Heike: Zahlentheorie in der Schule?. Praxis der Mathematik, August 1998
- Wallasch, Joachim M.: Elementare Beweise einiger zahlentheoretischer Sätze von Pierre Fermat. Praxis der Mathematik, 1/34, 1992
- Wallasch, Joachim M.: Die Pellsche Gleichung. Praxis der Mathematik, 3/35, 1993
- Witten; Letzner; Schulz: RSA & Co in der Schule. LOGIN-Verlag, Berlin, 1998
- Zita, K.: Kleiner Beitrag zum Palindrom-Problem. Praxis der Mathematik, 3/36, 1994