Katharina KLEMBALSKI, Berlin

Seminarkurs Kryptografie – Zahlentheorie

Im Rahmen meines Forschungsprojektes habe ich ein Unterrichtskonzept zu den Themen Kryptografie und Zahlentheorie entwickelt. Dieses wird im Augenblick von mir erprobt.

Rahmenbedingungen

Das Unterrichtskonzept wird im Rahmen eines zweisemestrigen (zusätzlichen) Seminarkurses mit drei Wochenstunden in der Kursphase der gymnasialen Oberstufe an zwei Berliner Schulen umgesetzt. Die Schüler befinden sich gerade im zweiten Halbjahr der Kursphase und im zweiten Semester des Seminarkurses. Aus dem Seminarkurs heraus erstellt jeder Teilnehmer eine Facharbeit, deren Bewertung in die Abiturnote einfließt.

Anforderungen an einen Seminarkurs

Intention zur Einrichtung von Seminarkursen war es, Schüler besser auf die Anforderungen eines Studiums vorzubereiten. Eine zentrale Forderung an einen solchen Kurs ist daher die Vorbereitung auf das selbständige wissenschaftliche Arbeiten während des Studiums. In Berlin wird zusätzlich eine fachübergreifende Ausrichtung des Kurses gefordert (siehe [1] und [2]). Bei der Umsetzung dieser Forderungen haben die Lehrkräfte inhaltlich und methodisch große Gestaltungsspielräume.

Warum Kryptografie und Zahlentheorie?

Die Zahlentheorie ist ein Teilgebiet der Mathematik, das für mehr als zwei Jahrtausende der reinen, eher anwendungsfernen, Mathematik zuzuordnen war. Jedoch sind es gerade Erkenntnisse der Zahlentheorie – beispielsweise Sätze über Primzahlen oder der Satz von Euler – die in den letzten 40 Jahren die Entwicklung moderner kryptographischer Verfahren ermöglicht haben. Diese sind von enormer praktischer Bedeutung und werden unter anderem beim Onlinebanking (Übertragungsprotokolle wie SSH), bei der Telefon- und Internetinfrastruktur (Zertifikate) und bei der Emailverschlüsselung eingesetzt.
Bei diesen Anwendungen spielt häufig die klassische Aufgabe der Kryptografie – die Geheimhaltung – eine untergeordnete Rolle. Stattdessen ist der sichere Nachweis der Identität eines Kommunikationsteilnehmers (digitale Unterschrift) bzw. die Sicherheit, dass gesendete/empfangene Nachrichten unverändert ankommen, von entscheidender Bedeutung (siehe [3]).

Das Thema verbindet somit auf natürliche Weise klassische, reine Mathematik mit modernen Anwendungen.

Darüber hinaus leistet es einen Beitrag zur informationstechnischen Grundbildung, indem Möglichkeiten und Grenzen kryptographischer Verfahren thematisiert sowie Schüler in die Lage versetzt werden, selbst kritisch Sicherheitsversprechen nachzuprüfen.

Weiterhin ermöglicht die Behandlung geeigneter zahlentheoretischer Inhalte neue Sichtweisen auf für Schüler durch jahrelangen Umgang vertraute Themen. Beispielsweise können durch Gegenüberstellung geeigneter Mengen mit ihrer Verknüpfung spezielle Eigenschaften der natürlichen Zahlen wie Assoziativität der Multiplikation, Eindeutigkeit der Primfaktorzerlegung oder Nullteilerfreiheit herausgestellt werden.

Es ist von großer Bedeutung für die praktische Umsetzung des Kurses, dass das gewählte Thema voraussetzungsarm ist. Das bedeutet insbesondere, dass der Kurs nicht auf Leistungskurs- oder Profilkurswissen aus Mathematik (oder Informatik) aufbaut. Somit kann jeder interessierte Schüler ohne spezielle Vorkenntnisse den Kurs belegen.

Kursaufbau

Die zwei Kurshalbjahre sind jeweils grob in drei größere Themenblöcke unterteilt – Kryptografie (I), Zahlentheorie (II), Kryptografie und Vertiefung (III). Die ersten beiden Blöcke dienen insbesondere der Vermittlung fachlicher Grundlagen und dem Bewusstmachen der verwendeten heuristischen Strategien. Sie nehmen zusammen knapp die Hälfte der Lernzeit ein. Die angewandten sowohl schüler- als auch lehrerzentrierten Unterrichtsmethoden sollen möglichst eigenverantwortliche Schülertätigkeit fördern. Im dritten Block ist zur Unterstützung individueller Interessen der Schüler sowie zur Stärkung der Methodenkompetenz, gerade in Vorbereitung auf das Schreiben der Facharbeit, eine längere Arbeitsphase integriert, in der Schüler längere Zeit eigenverantwortlich an verschiedenen Themen arbeiten. Diese werden am Ende dieser Phase den anderen Schülern präsentiert.

Das von den Schülern gewählte und bearbeitete Thema im dritten Block des zweiten Kurshalbjahres ist auch Thema der resultierenden Facharbeit. Dort hat die Präsentation zusätzlich eine unterstützende Funktion in Vorbereitung auf das Schreiben dieser Facharbeit. Die Abgabe der Arbeit erfolgt zwar erst am Ende des dritten Semesters, jedoch erscheint die (ausschnittsweise) Präsentation des Themas bzw. eines Zwischenstandes der Arbeit durch den Schüler zu diesem Zeitpunkt außerordentlich sinnvoll. Das betrifft einerseits die Unterstützung des Zeitmanagements dieser (in der Regel ersten längeren, schriftlichen und vorwissenschaftlichen) Arbeit, andererseits das Feedback zur Angemessenheit des Inhalts und der Darstellung durch die anderen Schüler und die Lehrkraft.

Im Folgenden stelle ich kurz wesentliche Inhalte und Leitgedanken für das erste Kurshalbjahr des Seminarkurses vor.

I. (Klassische) Kryptografie

Anhand ausgewählter überwiegend historischer Verschlüsselungsverfahren werden zentrale Begriffe und einfache Verfahren der Kryptoanalyse eingeführt. Probleme der Schlüsselübergabe oder der notwendigen Schlüsselzahl (und deren Verwaltung) bei modernen Anwendungen zeigen Grenzen dieser symmetrischen Verfahren.

II. Zahlentheorie

In diesem Abschnitt werden die mathematischen Grundlagen für moderne Verschlüsselungsverfahren auf Basis der Kongruenzrechnung unterrichtet. Inhalte sind: Sätze zur Teilbarkeit (mit Beweis), Rechnen mit Kongruenzen, Ermitteln des ggT mit Hilfe des Euklidischen Algorithmus (mit Beweis), Primzahlen, Verteilung von Primzahlen, kleiner Satz von Fermat (mit Beweis), Vielfachsummensatz (mit Beweis).

III. (Moderne) Kryptografie

Die Idee asymmetrischer Verschlüsselungsverfahren wird zunächst anhand der nach Rivest, Shamir und Adleman benannten RSA-Chiffre einführt. Für den Nachweis der Korrektheit des Verfahrens, d. h. den Beweis, dass das Ver- und Entschlüsseln eine Nachricht unverändert lässt, nutze ich einen Spezialfall des Satzes von Euler mit dem Produkt zweier Primzahlen als Modul. Auf diese Weise sind alle notwendigen Beweise elementar – also auf Grundlage des bereits vorhandenen Wissens – möglich.

Wesentliche Vertiefungen im Zusammenhang mit der Anwendung des RSA-Verfahrens erarbeiten die Schüler in Partnerarbeit: Angriffe auf RSA, Chinesischer Restsatz und Anwendung auf RSA, Schweizer Postcard, u.a.

Erste Ergebnisse

Von den 11 bzw. 14 Schülern, die sich für den Kurs entschieden haben, haben 9 bzw. 12 das erste Kurssemester beendet. In zwei Fällen musste die Kurswahl aus schulorganisatorischen Gründen korrigiert werden, bei den anderen zwei Schülern haben Noteneinbrüche beim Übertritt in die Kursphase zu der Entscheidung geführt von dem – zusätzlichen – Seminarkurs zurückzutreten. Die vergebenen Noten am Ende des ersten Kurssemesters wichen bis auf 2 Fälle um höchstens eine Note von der entsprechende Kursnote im Fach Mathematik ab, sind mit dieser also vergleichbar (Notenskala von eins bis sechs).

Meine Beobachtungen bezüglich der Anzahl derjenigen Schüler, die im Anschluss an den Kurs tatsächlich eine Facharbeit schreiben, entsprechen denen anderer Lehrkräfte. So besuchen statt 9 bzw. 12 Schülern nur noch 9

bzw. 6 Schüler das zweite Kurshalbjahr, von denen wiederum nur 7 bzw. 4 eine Facharbeit angefangen haben. Das ist in erster Linie darauf zurückzuführen, dass Schüler in Berlin bis zum Ende des dritten Kurshalbjahres zu Gunsten einer Präsentationsprüfung von ihrer Wahl des Seminarkurses und der Facharbeit zurücktreten können. Beides sind Möglichkeiten, den Wahlpflichtbestandteil des fünften Prüfungsfaches zu erfüllen. Entscheidet sich der Schüler jedoch für eine Präsentationsprüfung, kann er nur eines der beiden Halbjahre des Seminarkurses in die Abiturwertung einbringen.
Daher ist der Anteil der Schüler, die nur im ersten Kurshalbjahr teilgenommen haben, nachvollziehbar, denn der Besuch eines weiteren Kurshalbjahres sowie das Schreiben einer Facharbeit ist im Gegensatz zur Präsentationsprüfung mit deutlich mehr Arbeitsaufwand verbunden.
Dass die Zahl der Schüler, die den Kurs besuchen, diejenige übersteigt, die eine Facharbeit schreiben, kann mit diesem Hintergrund als starkes Indiz für das hohe Interesse am Thema Kryptografie und Zahlentheorie gewertet werden. Dies wird durch entsprechende Äußerungen der Schüler im Unterricht und Fragebögen unterstützt.

Das hohe Schülerinteresse, die Intensität der Auseinandersetzung mit den behandelten Themen- und Problemstellungen sowie die beobachtete Qualität der Schülerleistungen (beispielsweise der Schülervorträge, aber auch der Klausuren) lassen das erstellte Kurskonzept sowie die ausgewählten Inhalte für den Schulunterricht geeignet erscheinen.

Ausblick

Seit Einführung der Seminarkurse wurden in Berlin außer den von mir erprobten nur fünf weitere im Fach Mathematik durchgeführt. Einer der Hauptgründe dafür ist der erhebliche Planungsaufwand für die durchführende Lehrkraft. Ich hoffe diesen durch die von mir erstellten Unterrichtsmaterialien verringern zu können.
Andere Bedenken seitens der Lehrer sind organisatorischer Art und beziehen sich auf eine ausreichende Anzahl der Schüler pro Schule, die sich für einen Seminarkurs entscheiden oder die „Ausbeute“ von Facharbeiten im Verhältnis zur Schülerzahl zu Beginn. Hier ist zu untersuchen inwieweit durch andere schulübergreifende Organisationsformen die attraktive Idee des Seminarkurses in der Praxis „gerettet“ werden kann.

Literatur

[1] Verordnung über die gymnasiale Oberstufe in der Fassung vom 18. April 2007. Hrsg. von der Senatsverwaltung für Bildung, Jugend und Sport

[2] Die fünfte Prüfungskomponente im Abitur – Handreichung. Hrsg. von der Senatsverwaltung für Bildung, Jugend und Sport. 2006

[3] J. Buchmann: Einführung in die Kryptographie. Springer, 2004