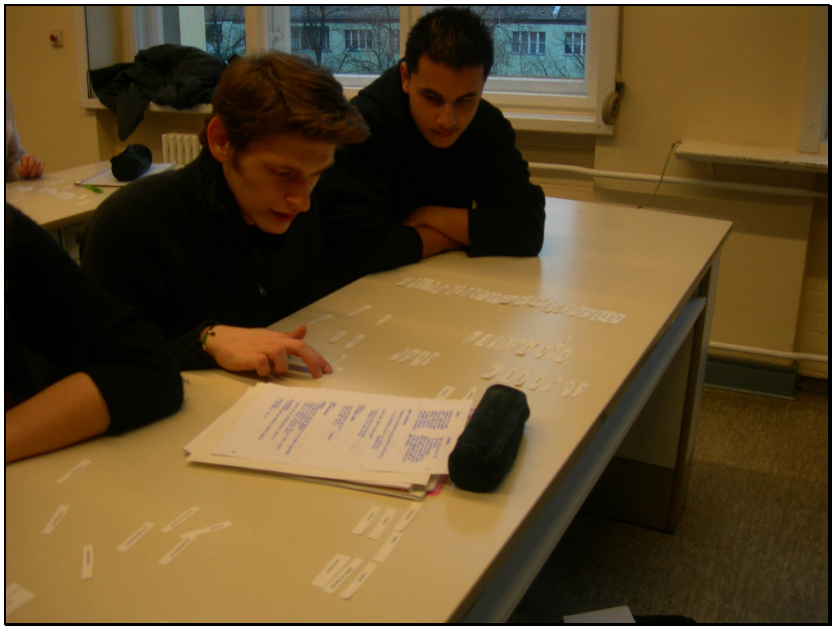
# Erprobung von ausgewählten Methoden des SOL zur Steigerung der Schüleraktivität im Rahmen einer Unterrichtsreihe zur Computersicherheit

Ein Unterrichtsvorhaben in einem Grundkurs Informatik der Luise-Henriette-Oberschule (Gymnasium)



Schriftliche Prüfungsarbeit zur Zweiten Staatsprüfung für das Amt des Studienrats

2. Schulpraktisches Seminar (S) Friedrichshain / Kreuzberg

vorgelegt von:
Kira Steffen
am 1. April 2008

# Inhalt

Das für das Deckblatt verwendete Foto wurde von mir während der Durchführung der Unterrichtsreihe erstellt und wird unter 6.4.2. näher erläutert.

**Lernen und Lehren in der Qualifikationsphase müssen dem besonderen Entwicklungsabschnitt Rechnung tragen, in dem die Jugendlichen zu jungen Erwachsenen werden. Dies geschieht vor allem dadurch, dass die Lernenden Verantwortung für den Lernprozess und den Lernerfolg übernehmen und sowohl den Unterricht als auch das eigene Lernen aktiv selbst gestalten.** [1]

---

# 1. Vorüberlegungen und Begriffsklärungen

Das einleitende Zitat aus dem Rahmenlehrplan Informatik verdeutlicht, dass „Mitverantwortung und Mitgestaltung von Unterricht“[2] in der Sekundarstufe II festgeschriebene Prinzipien sind. Vor diesem Hintergrund erscheinen mir ausgewählte Methoden des SOL geeignet, die Schüleraktivität zu steigern und damit genau diese Leitziele anzubahnen.

Entsprechend der Themenstellung erprobe ich im Rahmen einer Unterrichtsreihe zur Computersicherheit ausgewählte Methoden des SOL. Daraus ergibt sich die erste Frage, die in diesem Abschnitt geklärt werden muss: Was ist SOL?

Das Unterrichtsvorhaben zielt darauf, die Schüleraktivität zu steigern. Daher sollen auch hier zuerst folgende Punkte diskutiert werden: Was ist Schüleraktivität? Und: Wie steigere ich diese?

## 1.1. Was ist SOL?

Das Akronym SOL steht für „**S**elbst**O**rganisiertes **L**ernen“. Für dieses Konzept gibt es zahlreiche Bedeutungen. Ich konzentriere mich hier auf das SOL-Konzept, wie es Martin Herold und Birgit Landherr, die Autoren des derzeitigen Standardwerks zu SOL, in ihrem Buch vorstellen.[3] Beide Autoren forschen und unterrichten in Baden-Württemberg, wo seit den 1990er Jahren Erfahrungen mit diesem Unterrichtskonzept gemacht werden. Sie erklären SOL als einen „systemischen Ansatz für Unterricht“, bei dem es sich nicht um eine weitere Methode oder Methodensammlung sondern ein „ganzheitliches, zielorientiertes Lehr-/Lernsystem“[4] handelt. In der vom baden-württembergischen Kultusministerium herausgegebenen SOL-Broschüre wird betont, dass SOL zwar auf Ergebnissen pädagogischer Forschung basiert, jedoch nicht als wissenschaftliches Kon-

---

[1] RLP Informatik, S.6
[2] ebenda
[3] Herold, Martin; Landherr, Birgit. *SOL. Selbstorganisiertes Lernen*. Baltmannsweiler: Schneider-Verlag Hohengehren, 2003.
[4] Herold und Landherr, S. 5

zept verstanden sein will, sondern als Ansatz, die Schulrealität zu verändern.[5] Dabei werden als Ziele genannt:[6]

- Stärkung der individuellen Selbstständigkeit durch den systematischen Aufbau von Methoden- und Lernkompetenzen;
- Schaffung einer sozialen Lernstruktur durch die Abstimmung von Einzel - und Gruppenarbeit;
- Vertiefung des Wissens und Könnens durch Vernetzung fachlicher und überfachlicher Kompetenzen im Sinne zielorientierter Lernarrangements;
- Erhöhung der (Selbst-)Verantwortung für das eigene Lernen;
- Vermittlung und Beurteilung von Projektkompetenz im Rahmen von Themen- und Lernfeldern.

Herold: „Das Ziel von SOL ist unter anderem, durch organisatorische Innovationen eine systematische Veränderung der Aktivitätsverteilung zugunsten zunehmender Schüleraktivität zu erreichen.“[7]

Ideen kommen nicht aus dem Nichts, sondern haben konkrete Vordenker. So steht auch der Ansatz SOL in der Tradition der reformpädagogischen Konzepte aus den ersten Jahrzehnten des 20. Jahrhunderts. Herold und Landherr nennen dementsprechend als Vordenker ihrer Ideen Hugo Gaudig, Georg Kerschtensteiner, Maria Montessori und Peter Petersen.[8] Gleichzeitig sind Einflüsse der Bildungsdiskussionen der 1970er Jahre erkennbar, in denen die geforderte Demokratisierung aller Lebensbereiche, auf den Bereich Schule übertragen, nach anderen Lernformen verlangte.
Vereinfacht dargestellt geht es bei SOL um Veränderungen, die entlang folgender, in der Regel antonymer, Stichwortpaare jeweils von links nach rechts gefordert werden:

- autoritäre Strukturen / demokratische Strukturen
- fremdbestimmtes Lernen / selbstbestimmtes Lernen
- lehrerzentrierter Unterricht / schülerzentrierter Unterricht.

[5] SOL-Broschüre, S.4
[6] SOL-Broschüre, S.5
[7] Herold und Landherr, S. 29
[8] Herold und Landherr, S. 93 ff.

## 1.2. Was ist Schüleraktivität?

### 1.2.1. Einordung des Begriffs

**aktiv:** tätig, wirksam[9]
**passiv:** duldend, sich zurückhaltend; untätig, teilnahmslos[10]

Eine einfache Google-Suche mit dem Stichwort „Schüleraktivität“ ergab am 3. Januar 2008 rund 4760 Ergebnisse. Die ersten Einträge führten – erwartungsgemäß – zu den pädagogischen, erziehungswissenschaftlichen und schulpraktischen Instituten deutscher Hochschulen, in diesem Fall: Bremen, Münster und Bielefeld. Der fünfte Eintrag aber (siehe Abbildung) führte zu einem Antiquariat, das ein Buch des Titels *Unterricht und Schüleraktivität* anbietet.[11] Das Buch im Regal des Antiquariats ist 1987 erschienen und damit immerhin 21 Jahre alt. Schüleraktivität – alles andere als neu also.

Ergebnisse **1** - **10** von ungefähr **4.760** für **Schüleraktivität**. (**0,17** Sekunden)

Unterricht und **Schüleraktivität**. Probleme und Möglichkeiten der Entwicklung von Selbststeuerungsfähigkeiten im Unterricht.; WENZEL, HARTMUT.
www.antiqbook.de/boox/haker/261303.shtml - 4k - Im Cache - Ähnliche Seiten

**Abbildung 1: Das Ergebnis einer Google-Suche mit dem Stichwort „Schüleraktivität“ führt zu einem Antiquariat. (Ausschnitt)**

Tatsächlich tritt die Forderung nach mehr Schüleraktivität bereits in der reformpädagogischen Bewegung zu Beginn des 20. Jahrhunderts auf und bezieht sich dort auf die Selbsttätigkeit und Selbstständigkeit der Schüler. Wie Herbert Gudjons beschreibt, sollte anstelle der verbreiteten „Wort-, Buch- und Lernschule“[12] des 19. Jahrhunderts eine neue Art des Unterrichts entstehen. Der Reformer Hugo Gaudig (1860-1923) formulierte diesen Ansatz folgendermaßen: „Es gilt, den Schüler aus dem Passivum in das Aktivum zu übersetzen.“[13] Ebenso forderte Georg Kerschensteiner (1854-1932) selbstständige Schülerarbeit und greift damit auf Grundgedanken des, von ihm auch übersetzten, amerikanischen Pädagogen John Dewey (1859-1952) zurück.[14] Dewey initiierte mit

[9] Duden. Das Herkunftswörterbuch. S.27
[10] Duden. Das Herkunftswörterbuch. S. 592
[11] Die weitere Recherche ergibt: „einige Seiten mit Bleistiftunterstreichungen und -anmerkungen, Einband leicht fleckig“.
[12] Gudjons, Pädagogisches Grundwissen, S. 94
[13] Gudjons, Handlungsorientiert lehren und lernen, S. 128
[14] Gudjons, Päd. Grundwissen, S.95

*learning by doing* den Projektunterricht, der sich heute – in verkürzter Form – als Projektwoche an vielen Schulen etabliert hat.
Doch auch die Reformpädagogen haben ihre Vordenker: Schon im 18. Jahrhundert lehnte Johann Pestalozzi eine Verengung auf kognitive Bildung ab und postulierte stattdessen eine ganzheitliche „Elementarbildung", die Kopf, Herz und Hand gleichermaßen einbezieht und damit die Bereiche Verstand/Erkenntnis, Emotion und Handeln gleichberechtigt anspricht.[15]
Für die Gegenwart lässt sich feststellen: Schüleraktivität steht im direkten Zusammenhang zu und ist wesentlicher Bestandteil von Konzepten des handlungsorientierten Unterrichts. Handlungsorientierung begründet sich im Konstruktivismus und bedeutet für den Unterricht: „Der Schüler erwirbt Wissen und Können durch aktives Gestalten im Fach als Einzelperson oder Gruppenmitglied."[16] Damit steht dieser Ansatz im klaren Gegensatz zu Lernformen, bei denen die bloße (passive) Rezeption von Informationen gefragt ist.

### 1.2.2. Schüleraktivität und Schule

Das Berliner Schulgesetz verpflichtet die Schülerinnen und Schüler in § 46, Absatz 2 „regelmäßig am Unterricht und den sonstigen verbindlichen Schulveranstaltungen **aktiv** teilzunehmen [...].[17] Als mündliche Note geht Schüleraktivität im sogenannten allgemeinen Teil in allen Unterrichtsfächern in die Gesamtnote auf dem Zeugnis ein.
Dennoch, laut Herold und Landherr gilt allgemein: „Der Unterrichtsalltag in deutschen Schulen wird auch 2001 noch sehr stark durch lehrerzentrierte Unterrichtsformen, die vorwiegend der Vermittlung von Wissen dienen, dominiert."[18] Auch für den Informatikunterricht kommen Schubert und Schwill zu dem ernüchternden Ergebnis: „Frontalunterricht, häufig verknüpft mit langen Lehrermonologen."[19]
Informatiklehrer halten dagegen, dass dies für ihr Fach anders aussieht, weil schon durch die praktische Arbeit am Computer der Anteil der schüleraktiven Unterrichtsphasen deutlich höher ist.[20] Tatsächlich sieht der Berliner Rahmenlehrplan Informatik Projektarbeit als wesentlichen Bestandteil des Unterrichts vor.[21] Darüber hinaus beinhaltet

[15] Internet: http://de.wikipedia.org/wiki/Johann_Heinrich_Pestalozzi
[16] Schubert/ Schwill. S. 33
[17] Berliner Schulgesetz, S. 44 (meine Hervorhebungen).
[18] Herold und Landherr, S. 106
[19] Schubert/ Schwill. S. 33
[20] Witten, Helmut et al. „SOL - Schule ohne Lehrer?" In: LOG IN Nr. 138/139, 2006, S.75
[21] RLP Informatik. S. 7

das Curriculum im 4. Kurshalbjahr sowohl im Grundkurs als auch im Leistungskurs Informatik explizit ein Softwareprojekt.[22]

### 1.2.3. Schüleraktivität steigern

Durch den Einsatz von SOL-Methoden in dieser Unterrichtsreihe sollen die Rahmenbedingungen des Unterrichts zugunsten einer höheren Schüleraktivität verändert werden. Eine systematische Messung der Steigerung von Schüleraktivität könnte beispielsweise eine weitere Lerngruppe, die bei gleichen Fachinhalten ohne SOL-Methoden unterrichtet wird, als Kontrollgruppe beinhalten. Idealerweise würde dann ein zusätzlicher Beobachter evtl. mithilfe von Videoaufzeichnungen den Unterricht begleiten und die Evaluation unterstützen. Herold gibt allerdings zu bedenken, dass eine komplette Umstellung auf SOL „von heute auf morgen“ nicht realisierbar ist.[23] Daher werde ich bei der Planung der Unterrichtsreihe einen Wechsel zwischen innovativen und gewohnten Unterrichtsformen realisieren und mich bei der Auswertung auf die folgenden Punkte konzentrieren:

1. Analyse des Einsatzes und der Durchführung von SOL-Methoden
2. Analyse der veränderten Lehrerrolle: „Der Lehrer fungiert als Berater – statt als Präsentator.“[24]

Die veränderte Lehrerrolle, die mit dem Einsatz von SOL-Methoden einhergeht, gibt mir als Lehrerin den Freiraum, während der Durchführung der Methoden die Lerngruppe hinsichtlich des Aspektes Schüleraktivität zu beobachten.

[22] RLP Informatik, S. 27 (Grundkurs) und S. 30 (Leistungskurs).
[23] Herold, S. 76.
[24] Hubwieser, S.11.

# 2. Sachanalyse: Computersicherheit

## 2.1. Vorbemerkung

Früher war alles einfacher: „Wenn jemand andere am Zugriff auf seine Dateien hindern wollte, schloss er einfach seine Bürotür ab.“[25] In Zeiten des Internet sind Computer keine Inseln mehr, sondern Teil eines Systems. Ein solches System ist das Rechnernetz einer Schule, aber auch das Internet ist ein Beispiel für ein – sehr komplexes – System. Wenn ich im Folgenden gelegentlich den Begriff Computer durch System ersetze, so geschieht dies vor dem Hintergrund, dass hier nicht isolierte Computer betrachtet werden, sondern solche, die Teil eines Netzwerks sind. Also: ganz normale Computer, wie sie zuhause auf den Schreibtischen der Schülerinnen und Schüler oder in den Rechnerräumen der Schule stehen. Für die Sachanalyse möchte ich folgende Fragen klären:

- Was soll gesichert werden?
- Welcherart sind die Angriffe?
- Wer sind die Angreifer?
- Wie sehen die Schutzmaßnahmen aus?
- Kryptologie

## 2.2. Was soll gesichert werden?

Bei Computersicherheit geht es in erster Linie um die Sicherheit der auf dem Computer gespeicherten Daten und Programme. Schneier nennt drei Aspekte der Computersicherheit: **Vertraulichkeit, Integrität und Verfügbarkeit**.[26]

Bei Vertraulichkeit geht es um den Schutz vertraulicher Daten. Daten sollen nur von zuvor autorisierten Benutzern gelesen werden können. Integrität bezieht sich in diesem Zusammenhang auf die Sicherheit beim Schreiben von Daten bzw. Programmen. Datenintegrität bedeutet, dass Daten nur von zuvor autorisierten Benutzern geändert oder gelöscht werden können. Programmintegrität bedeutet entsprechend, dass Programme nur von zuvor autorisierten Benutzern geändert oder gelöscht werden können. Verfügbarkeit betrifft die Zusicherung, dass (autorisierte) Benutzer Zugang zu ihren Systemen haben. Alle drei Aspekte – Vertraulichkeit, Integrität, Verfügbarkeit – beziehen sich auf Zugriffskontrolle.

[25] Schneier, S. 116

[26] In diesem Abschnitt beziehe ich mich auf das Kapitel 8 „Computersicherheit“ des genannten Buches von Bruce Schneier. (S. 112-126)

## 2.3. Angriffe

Welcherart sind die Angriffe? Claudia Eckert definiert Angriff als „nicht autorisierten Zugriff bzw. Zugriffsversuch auf das System.“[27] Sie unterscheidet Angriffe, welche die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Systemen beschädigen.[28] Tabelle 1 zeigt eine Übersicht dieses Schemas. Natürlich gibt es auch Angriffe, die den Verlust gleichzeitig mehrerer dieser Aspekte der Systemsicherheit zur Folge haben. So verursachte zum Beispiel der berühmt gewordene ILOVEYOU-Wurm den Verlust sowohl der Integrität, indem er Dateien auf den betroffenen Computern löschte, als auch der Verfügbarkeit, denn durch seine exponentielle Verbreitung überlastete und blockierte er Mailserver.[29]

| **Angriffe** | **PASSIVE** | **AKTIVE** | **DENIAL-OF-SERVICE** |
|---|---|---|---|
| **Folge: Verlust der ....** | Vertraulichkeit | Integrität | Verfügbarkeit |
| **Beispiel** | Passwörter ausspähen | Viren<br>Würmer<br>Trojaner | Überschwemmen von Rechnernetzen mit Nachrichten,<br>Blockieren eines Service-Ports |

**Tabelle 1: Angriffe auf Computer**

Allgemein gilt für Angriffe in der Onlinewelt: „Die Bedrohungen in der digitalen Welt sind ein Spiegelbild der Bedrohungen in der physischen Welt.“[30] Allerdings ändert sich durch das Internet die Art der Angriffe. Schneier nennt drei grundsätzliche Unterschiede:[31] Erstens macht die Automatisierung die millionenfache Wiederholung von Angriffsversuchen möglich. Angriffe, die ohne Computer zu lange dauern und dadurch unrentabel wären, können, automatisiert durchgeführt, rentabel sein. Zweitens ermöglicht die globale Vernetzung Angriffe aus der Ferne. (Was auch die Strafverfolgung komplizierter macht: die Angreifer sind nicht immer greifbar, denn weltweit unterscheiden sich die Gesetze gegen Computerkriminalität.) Drittens macht die weltweite Vernetzung es möglich, Angriffswerkzeuge schnell zu verbreiten. Sachkenntnis braucht hier nur noch der Entwickler, die Angriffe können dann auch von technisch weniger versierten Angreifern (den sogenannten Skript-Kiddies) mit Kopien gestartet werden.

[27] Eckert, S. 16
[28] Eckert, S. 16/17
[29] Wikipedia. Internet: <http://de.wikipedia.org/wiki/Loveletter>
[30] Schneier, S. 12
[31] Schneier, S. 15-19

Die genannten Unterschiede haben zur Folge, dass digitale Angriffe immer häufiger vorkommen und zunehmend weiter verbreitet sind.

## 2.4. Angreifer

Wer sind die Angreifer? Die Angreifer der Online-Welt sind im Prinzip die aus der Offline-Welt bekannten üblichen Verdächtigen: Kriminelle, denen es um Geld geht, Industriespione, die Wissen ausspähen wollen, nationale Geheimdienste, die „Feindnachrichten“ suchen.[32] Hinzu kommen die Hacker, die in der Regel (Stichwort: Hacker-Ethik) nicht finanzielle Vorteile verfolgen, sondern auf Schwachstellen der Systeme aufmerksam machen wollen.[33] Die Liste der Angreifer lässt sich noch erweitern, für diesen Rahmen sollen jedoch die genannten genügen.

## 2.5. Schutzmaßnahmen

Im Zusammenhang von Sicherheit und Schutzmaßnahmen wird in der Fachliteratur gerne auf das Bild der Kette, die bekanntlich nur so stark ist wie ihr schwächstes Glied, zurück gegriffen.[34] Glieder dieser Kette sind beispielsweise der Benutzer des Computers, die Software des Computers, ein internes Netz, Protokolle, die von den Computern ausgeführt werden und die Verwendung von Kryptografie. Die Rolle der Kryptografie in dieser Sicherheitskette beschreibt Schneier folgendermaßen: „Sie ist die Technologie, mit der wir Sicherheit in den Cyberspace einbauen [...].“[35]

## 2.6. Kryptologie

von griechisch „krýptein“: verbergen, verstecken[36]

### 2.6.1. Terminologie

Die Begriffe Kryptologie und Kryptografie werden in der Literatur oft synonym verwendet, genau genommen ist Kryptologie jedoch der Oberbegriff für Kryptografie und Kryptoanalyse. Kryptografie (griechisch „graphein“: schreiben) beschäftigt sich mit dem Verschlüsseln von Nachrichten. Kryptoanalyse (griechisch „analýein“: auflösen) befasst sich mit dem Entschlüsseln von verschlüsselten Nachrichten ohne die Kenntnis des Schlüssels.

[32] Schneier, S. 39
[33] Eckert, S. 19
[34] z.B. Eckert, S. 32
[35] Schneier, S. 79
[36] Duden. Herkunftswörterbuch. S. 456

| Kryptologie | | |
|---|---|---|
| **Kryptografie →** | | **← Kryptoanalyse** |
| unverschlüsselte Nachricht | *Verschlüsseln →*<br>———————<br>*← Entschlüsseln* | verschlüsselte Nachricht |
| Klartext (message) | Schlüssel (key) | Geheimtext, Chiffretext (code) |

**Tabelle 2: Terminologie zu Begriffen der Kryptologie**

### 2.6.2. Chronologie

Historisch betrachtet ist der Wunsch nach sicherem Nachrichtenverkehr so alt wie der Nachrichtenverkehr selbst. Durch Techniken des Verbergens, durch Kryptografie, sollte sicher gestellt werden, dass nur der eigentliche Empfänger die Botschaft lesen kann. Eine mögliche Einteilung der kryptografischen Verfahren von der Antike bis in die Gegenwart kann anhand folgender drei Phasen vollzogen werden:

1. „Klassische“ Verfahren: Caesar, Alberti, Vigenère
2. Mechanische Verfahren bis in die 1950er Jahre
3. Computergestützte Verfahren bis in die Gegenwart

#### 2.6.2.1. „Klassische“ Verfahren

Zu den bekanntesten „klassischen“ Verfahren der Kryptografie zählt das nach dem römischen Kaiser Julius Caesar benannte und von ihm verwendete Transpositionssverfahren. Dabei werden die einzelnen Buchstaben der Nachricht um einen festgelegten Wert, den Schlüssel, innerhalb des Alphabets verschoben. Caesar selbst soll ausschließlich den Schlüssel 3 verwendet haben. Aus dem Klartext „CAESAR“ wird nach diesem Algorithmus der Geheimtext „FDHVDU“. Da bei diesem Verfahren dem Klartextalphabet genau ein Geheimtextalphabet zugeordnet wird, zählt das Caesarverfahren zu den monoalphabetischen Verschlüsselungsverfahren.[37]

[37] Beispiel für ein weiteres monoalphabetisches Verfahren ist die von Edgar Allan Poe in seiner Erzählung „The Gold-Bug“ ersonnene Chiffre, die jedem Klartextbuchstaben ein Zeichen eines Geheimalphabets zuordnet.

Anders als das Caesarverfahren verwenden polyalphabetische Verfahren wie Alberti und Vigenère mehrere Geheimtextalphabete für die Verschlüsselung.
Das im 15. Jahrhundert von Leon Battista Alberti entwickelte Alberti-Verfahren verschlüsselt eine Nachricht mit zwei oder mehr Geheimtextalphabeten so, dass den Klartextbuchstaben alternierend der entsprechende Buchstabe der Geheimtextalphabete 1 und 2 zugeordnet wird (siehe Tabelle). Beispielsweise würde der Klartext „CAESAR“ zu „BGKVFS“ verschlüsselt.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Geheimtextalphabet1 | F | Z | B | V | K | I | X | A | Y | M | E | P | L | S | D | H | J | O | R | G | N | Q | C | U | T | W |
| Geheimtextalphabet2 | G | O | X | B | F | W | T | H | Q | I | L | A | P | Z | J | D | E | S | V | Y | C | R | K | U | H | N |

**Tabelle 3: Alberti-Verfahren**[38]

Im 16. Jahrhundert entwickelte der französische Diplomat Blaise de Vigenère die Idee Albertis weiter: Das Vigenère-Verfahren verwendet ein Schlüsselwort, dessen Buchstaben die Verschiebung der Geheimtextbuchstaben bestimmen. Jeder Buchstabe des Schlüsselworts verweist auf ein anderes Geheimtextalphabet im Vigenère-Quadrat.[39] Bei einem Schlüsselwort der Länge sechs kommen also sechs verschiedene Geheimtextalphabete zur Anwendung. Soll beispielsweise der Klartext „CAESAR“ mit dem Schlüsselwort „ENIGMA“ verschlüsselt werden, so wird dem ersten Klartextbuchstaben „C“ über die C-Spalte des Vigenèrequadrats mit dem ersten Buchstaben „E“ des Schlüsselwortes über die E-Zeile der Geheimbuchstabe „G“ zugeordnet. Nach diesem Schema wird für alle Klartextbuchstaben der Geheimbuchstabe in der Zelle der Tabelle ermittelt, in der sich Spalte und Zeile kreuzen. Aus „CAESAR“ wird so „GNMYMR“ (siehe Tabelle).

| A | B | **C** | D | E | .. |
|---|---|---|---|---|---|
| B | C | D | E | F | .. |
| C | D | E | F | G | .. |
| D | E | F | G | H | .. |
| **E** | F | **G** | H | I | .. |
| F | G | H | I | J | .. |
| .. | .. | .. | .. | .. | .. |

| Klartext | **C** | A | E | S | A | R |
|---|---|---|---|---|---|---|
| Schlüssel | **E** | N | I | G | M | A |
| Geheimtext | **G** | N | M | Y | M | R |

**Tabelle 4: Ausschnitt aus dem Vigenère-Quadrat und Verschlüsselungsbeispiel mit dem Vigenère-Verfahren**

[38] Singh 2002, S. 66.
[39] Das Quadrat besteht aus 26 Spalten (A-Z) und 26 Zeilen in denen 26 mal das Alphabet jeweils um 1 verschoben dargestellt ist.

Bei einem Vergleich der drei vorgestellten Verfahren wird deutlich, dass die Komplexität der Verschlüsselung in chronologischer Reihenfolge steigt: Während eine nach dem Caesar-Verfahren verschlüsselte Nachricht durch die einfache Analyse der Buchstabenhäufigkeit dechiffriert werden kann, ist für die Vigenère-Verschlüsselung zunächst die Länge des Schlüsselwortes und dann die gleitende Häufigkeit zu ermitteln. Die Sicherheit der polyalphabetischen Verfahren steigt mit der Länge des verwendeten Schlüssels.[40]

#### 2.6.2.2. Mechanische Verfahren

Das erste kryptografische Gerät wurde im 15. Jahrhundert von dem bereits genannten Leon Battista Alberti entworfen: Eine aus einer inneren und einer äußeren Scheibe bestehende drehbare Chiffrierscheibe. Jedem Klartextbuchstaben auf der äußeren Scheibe steht ein Buchstabe auf der inneren gegenüber. Das gewählte Geheimtextalphabet wird durch Drehen der Scheiben zur gewünschten Position festgelegt und kann für polyalphabetische Verfahren nach jedem Buchstaben geändert werden. Die Chiffrierscheibe vereinfachte das Erstellen des Geheimtextes – das Prinzip und die damit verbundene Sicherheit der Vigenèreverschlüsselung blieben jedoch gleich.
Im 20. Jahrhundert entwickelte der deutsche Elektrotechniker und Erfinder Arthur Scherbius die Enigma, eine elektromechanische Chiffrier-Maschine, die eine wesentlich verbesserte Verschlüsselung ermöglichte. Die Enigma wurde in großer Stückzahl produziert und im Zweiten Weltkrieg vom deutschen Militär zur Verschlüsselung des Funkverkehrs eingesetzt. Dem britischen Geheimdienst gelang mit einem Team von Spezialisten um Alan Turing in Bletchley Park schließlich dennoch die Entschlüsselung.[41]
Der Bauplan der Chiffrier-Maschine beinhaltet eine Tastatur für die Klartexteingabe, ein Steckerbrett, drei Walzen und einen Reflektor, der zur Stromumlenkung dient. Die Walzen können zum einen in der Reihenfolge getauscht, zum anderen jeweils in eine von 26 (A-Z) möglichen Positionen gestellt werden. Sechs Steckerkabel können im Steckerbrett so gesteckt werden, dass Buchstabenpaare kreuzweise vertauscht werden.[42]
Die Originalmaschine ordnete jedem eingegebenen Buchstaben einen verschlüsselten

[40] Vgl. Witten (1998) Teil II: Wird ein Schlüsselwort verwendet, das mindestens so lang wie der Klartext ist, ist der Geheimtext praktisch nicht zu entschlüsseln.
[41] Spannend nachzulesen bei Singh, 2002: „Die Entschlüsselung der Enigma." S. 179-234.
[42] Eine sehr anschauliche Enigma-Simulation ist in das Programm CrypTool eingebunden.

Buchstaben zu, indem sie einen, sich nach jedem Buchstaben wieder neu konfigurierenden, Stromkreis schloss.[43]
Um dem Empfänger die Dechiffrierung des Geheimtextes zu ermöglichen, muss auch bei diesem Verfahren der Schlüssel, bestehend aus Walzenreihenfolge, Walzenpositionen sowie Steckerverbindungen, auf sicherem Weg übermittelt werden.

#### 2.6.2.3. Kryptologie heute

Die über die Jahrhunderte zu verfolgende ständige Weiterentwicklung der Verschlüsselungsalgorithmen erklärt sich ganz einfach: Eine Verschlüsselung gilt nur solange als sicher, als *Chiffre indéchiffrable,* bis sie dechiffriert ist. Dann wird ein verbessertes Verfahren benötigt. Allerdings gibt es noch ein weiteres Problem: Bei den vorgestellten klassischen und mechanischen Verfahren erfolgen Ver- und Entschlüsselung jeweils paarweise mit demselben Schlüssel, weshalb man diese auch als symmetrische Verfahren bezeichnet. Ein wesentliches Problem dieser symmetrischen Kryptografie ist die Schlüsselübermittlung, die so sicher erfolgen muss, dass nur der Empfänger Kenntnis des Schlüssels erlangt.
Seit den 1970er Jahren begannen Kryptografen daher, nach einer Alternative zu suchen. Die Public-Key-Kryptografie, deren bekanntestes Verfahren die RSA-Verschlüsselung[44] darstellt, löst das Schlüsselaustauschproblem zwischen Sender und Empfänger indem Ver- und Entschlüsselung nicht mit demselben Schlüssel geschehen. Die Verschlüsselung wird vom Sender mit einem öffentlichen, nicht geheimen Schlüssel durchgeführt, während die Entschlüsselung durch den Empfänger mit seinem privaten, geheimen Schlüssel erfolgt.
Wie geht das? Prinzipiell mit Einwegfunktionen, also Funktionen, bei denen die eine Richtung leicht, die andere sehr schwierig oder gar nicht auszurechnen ist. Der RSA-Algorithmus verwendet dazu die Multiplikation zweier großer Primzahlen. Das Produkt N zweier großer Primzahlen (p und q) ist leicht zu erstellen, die Faktorisierung von N aber ist bei genügend großen Primzahlen entsprechend schwieriger.[45] Aus p,q und deren Produkt N werden zwei Zahlen d und e so bestimmt, dass gilt:

$$d * e \equiv 1 \bmod (p - 1)(q - 1)$$

Ein zu verschlüssender Klartext M wird als Folge von ASCII-Zahlen dargestellt und durch den Sender mit Kenntnis des öffentlichen Schlüssels (N,e) nach der Formel:

[43] CrypTool. Aufbau und Funktionsweise der Enigma.
[44] 1978 von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt (vgl. Singh, S.329)
[45] vgl. RSA Factoring Challenge

$$C \equiv M^e \pmod{N}$$

als Geheimtext C chiffriert. Für die Entschlüsselung verwendet der Empfänger den nicht-öffentlichen Schlüssel d und die Formel:

$$M \equiv C^d \pmod{N}$$

Bei der Public-Key-Verschlüsselung werden, wie gezeigt, für Ver- und Entschlüsselung jeweils verschiedene Schlüssel eingesetzt, womit sich der Name asymmetrische Kryptografie erklärt.

| | **Verschlüsselung** | **Entschlüsselung** |
|---|---|---|
| **Symmetrisches Verfahren**: | Schlüssel: 3 | |
| Beispiel Caesar | c = m+3<br>Buchstabe A wird verschlüsselt: D = A+3 | m = c-3 // (Subtraktion als zur Addition inverse Funktion)<br>Buchstabe D wird entschlüsselt: A = D-3 |
| **Asymmetrisches Verfahren**: | Schlüssel: N,e | Schlüssel: N,d |
| Beispiel RSA | $C \equiv M^e \pmod{N}$ | $M \equiv C^d \pmod{N}$ |

**Tabelle 5: Asymmetrische vs. symmetrische Kryptografie (c steht für code/Geheimtext, m steht für message/Klartext)**

In der Praxis werden heute neben der assymetrischen Kryptografie weiterhin symmetrische Verfahren verwendet. Vor allem im Internet wird die Verschlüsselung durch Hybridverfahren realisiert, die den Zielkonflikt zwischen sicher und schnell wie folgt lösen: Der Sitzungsschlüssel wird asymmetrisch verschlüsselt übermittelt (sicherer), die eigentliche Verschlüsselung erfolgt dann symmetrisch (schneller).[46]

### 2.6.3. Sicherheit kryptografischer Verfahren: Zwei Ansätze

Es lassen sich zwei grundsätzliche Ansätze unterscheiden, welche die Frage, ob die Kenntnis des verwendeten Verfahrens die Sicherheit der Verschlüsselung beeinträchtigt, unterschiedlich beantworten.

[46] vgl. Witten, 2006, S. 46 und Schneier, S.90.

Kerckhoffs' Prinzip beantwortet die Frage mit einem klaren Nein. Es wurde 1883 von dem niederländischen Linguisten und Kryptologen Auguste Kerckhoffs formuliert und lautet:

> Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.[47]

Diesem Prinzip folgen die modernen Public-Key-Verfahren, z.B. das vorgestellte RSA-Verfahren.

Ein gegenteiliges Prinzip folgt dem Grundsatz „Security by obscurity" (Geheimhaltung durch Verschleiern). Diesen Ansatz benennt das Bundeamt für Sicherheit in der Informationstechnik in folgendem Zitat:

> Im Hochsicherheitsbereich wird man auf die zusätzliche Sicherheit, die ein geheim gehaltenes und dann notwendigerweise eigenentwickeltes Kryptoverfahren bietet, nicht verzichten können, da jede Offenlegung der Designprinzipien einen potentiellen Angreifer von vornherein in eine günstigere Position brächte und somit sich von selbst verbietet.[48]

Kritiker des Prinzips „Security by obscurity" merken an, dass mit einem durch die Geheimhaltung bedingten fehlenden Expertendiskurs, die Qualität des geheim gehaltenen Algorithmus zweifelhaft ist. Schneier argumentiert in diese Richtung, wenn er feststellt, dass die beste Art, Krytografie zu prüfen, die jahrelange öffentliche Kryptoanalyse ist: „Ein selbstgebackener Algorithmus kann unmöglich den hunderttausenden von Stunden an Kryptoanalyse unterzogen werden, die DES und RSA durchlaufen haben."[49]

[47] Quelle: http://de.wikipedia.org/wiki/Kerckhoffs_Prinzip
[48] BSI- Broschüre
[49] Schneier, S. 111.

# 3. Unterrichtsvoraussetzungen

## 3.1. Zeiten und Räume

### 3.1.1. Stundenplan

Der Grundkurs Informatik findet an der Luise-Henriette-Oberschule mit drei Wochenstunden jeweils montags als Doppelstunde (in der 1. und 2. Unterrichtsstunde) und dienstags als Einzelstunde (in der 7. Unterrichtsstunde) statt.

### 3.1.2. Fachräume

Der Informatikbereich der Luise-Henriette-Oberschule besteht aus zwei Fachräumen (Raum 310 und 312) unterschiedlicher Größe und Ausstattung. Sie befinden sich im dritten Stock des Hauptgebäudes und besitzen jeweils große Fenster nach Südwesten, was im Winter wegen der damit verbundenen Helligkeit sehr angenehm ist, jedoch im Frühling und Sommer die Raumtemperaturen schnell unangenehm macht. Leider ist die Gestaltung der Informatikfachräume von „Best-Case-Szenarien“[50] weit entfernt. Phasenweise unterrichte ich auch in einem dem Informatikbereich gegenüberliegenden Physikfachraum.

**Raum 310** ist offensichtlich als Schülerarbeitsraum konzipiert. Er steht den Schülerinnen und Schülern der Luise-Henriette-Oberschule auch außerhalb des Unterrichts zur Verfügung und wird sowohl von der Mittelstufe als auch von der Oberstufe in Freistunden zum Arbeiten, Spielen und Kommunizieren rege genutzt. Für die konkrete Durchführung des Informatikunterrichts mit einem Grundkurs ist der Raum schlecht geeignet, aufgrund der Kursgröße aber ohne Alternative. Raum 310 bietet Sitzplätze für 30 Schüler, es stehen dort 15 Computer zur Verfügung. Die Tische sind in fünf hintereinanderliegenden Reihen angeordnet und nur von einer Seite aus zugänglich. Da die Tische der ersten Reihe direkt an die Wand angrenzen, gibt es keinen Lehrertisch. Für Instruktionen und Ergebnispräsentationen ist an der Seitenwand ein Whiteboard montiert. Allerdings haben die Schüler der fünften Reihe – bedingt durch einen Vorsprung im ansonsten rechteckigen Raumschnitt – teilweise keine Sicht auf das Whiteboard. Für Diskussionen im Plenum ist die Sitzordnung ungeeignet, da die Schüler und Schülerinnen einander nur innerhalb ihrer eigenen Sitzreihe sehen können. Die Benutzung eines Beamers ist in diesem Raum nicht vorgesehen, als Notlösung kann ein Beamer in der zweiten Tischreihe aufgestellt werden, so dass die Projektionsfläche an der vorderen Wand

[50] vgl. Humbert S.113-115.

liegt. Dann müssen aber die Schüler der ersten Reihe, deren Tische an diese Wand grenzen, einen anderen Platz mit Sicht auf die Projektionsfläche finden.
**Raum 312** ist mit 18 Sitzplätzen, zehn Computern und einem Lehrertisch deutlich kleiner. Wie in Raum 310 sind die Tische in hintereinanderliegenden Reihen angeordnet, der Zugang durch einen Mittelgang lässt hier aber mehr Bewegung zu. Frontal steht ein Whiteboard zur Verfügung. Der Computer am Lehrertisch ist mit einem Beamer verbunden, dessen Projektionsfläche auf bzw. über dem Whiteboard liegt. Zusätzlich steht ein OH-Projektor zur Verfügung. Aufgrund der Kursgröße nutze ich diesen Raum nur in Unterrichtsphasen, in denen die Lerngruppe geteilt arbeitet.
In beiden Räumen sind die Computer mit dem Betriebssystem Windows 2000 ausgestattet, alle Computer sind über einen Router vernetzt und haben ständig Internetzugang.
**Der Physik-Fachraum** bietet mit 32 Sitzplätzen, Tafel und OH-Projektor die Möglichkeit, Phasen im Plenum durchzuführen, für die die Informatikräume zu klein (Raum 312) bzw. zu ungünstig ausgestattet (Raum 310) sind. Der Raum ist zu meinen Kurszeiten aber nicht immer frei, weshalb hier flexible Planung gefragt ist.

## 3.2. Lerngruppenanalyse

### 3.2.1. Die Schülerinnen und Schüler

Seit Beginn des laufenden Schuljahres 2007/08 erteile ich im Grundkurs Informatik des 1. Semesters selbstständig Unterricht. Mit 25 Teilnehmern – acht Schülerinnen und 17 Schülern – ist der Kurs in diesem Schuljahr relativ groß. In der Lerngruppe besteht eine gewisse Affinität zur Mathematik: Fünf Schülerinnen und zehn Schüler, das sind 60% der Gruppe, besuchen einen Leistungskurs Mathematik.
Alle Schüler und Schülerinnen der Lerngruppe arbeiten in Phasen der Rechnerarbeit in der Regel ruhig und konzentriert an den jeweiligen Aufgaben. In Phasen des Unterrichtsgesprächs fallen [*Schülernamen entfernt*] durch aktive Mitarbeit auf. [*Schülernamen entfernt*] beteiligen sich gelegentlich mit Beiträgen, während die anderen Schülerinnen und Schüler bisher nur nach Aufforderung eigene Beiträge zu Unterrichtsgesprächen beigesteuert haben. [*Schülername entfernt*] fehlte durch einen Krankenhausaufenthalt nach einem Motorradunfall für den Zeitraum von vier Wochen, konnte aber durch ihre engagierte Arbeit den Anschluss wieder finden.
Die Lerngruppe arbeitet insgesamt motiviert mit und zeigt sich interessiert an den angebotenen Inhalten und Methoden.

### 3.2.2. Inhaltliche Voraussetzungen

Der Einstieg in das erste Kurshalbjahr erfolgte für die Lerngruppe über den für die Informatik zentralen Begriff des Algorithmus.[51] Die Schüler und Schülerinnen übten sich in der strukturierten Planung und Dokumentation von Lösungswegen. In diesem Zusammenhang wurden Struktogramme als unterstützende Technik eingeführt und für verschiedene Problemstellungen verwendet: Dijkstras Kürzester-Weg-Algorithmus, Sieb des Eratosthenes, Euklidischer Algorithmus, „Aschenputtel-Algorithmus“[52].
Einen weiteren Themenblock bildeten Zahlensysteme mit dem Schwerpunkt auf Binär- und Hexadezimalzahlen, sowie das Rechnen in diesen Zahlensystemen. Als kontrastierendes Konzept zu den bekannten Stellenwertsystemen behandelten wir das Römische Zahlensystem. Ergänzend zu Zahlendarstellungen wurde die Codierung von Zeichen anhand verschiedener Umsetzungen (Morse, ASCII, Unicode) betrachtet. Es folgte die Behandlung des Themas Von-Neumann-Architektur.
Der Einstieg in das Programmieren erfolgte für die Lerngruppe über den variablenfreien Zugang mit der Minisprache Kara (Steuerung eines Marienkäfers durch eine zweidimensionale Welt).
Der Themenbereich Geschichte der Informatik wurde von mir an geeigneten Stellen integriert behandelt, z. B. Al-Chwarizmi als wegweisender arabischer Mathematiker auf den die Bezeichnungen Algebra und Algorithmus zurückgeführt werden, Gottfried Wilhelm Leibniz, der das Dualsystem in seiner Schrift „Explication de l’Arithmétique Binaire“ dokumentierte, sowie Von Neumann und Konrad Zuse.

### 3.2.3. Methodische Voraussetzungen

Um einerseits eine gewisse Einseitigkeit zu umgehen und andererseits deutlich zu machen, dass Informatikunterricht nicht gleichzusetzen ist mit Arbeiten am Computer, habe ich einzelne Sequenzen mit der Lerngruppe im Sinne eines „Hands-On!“-Ansatzes durchgeführt.[53] Beispielsweise haben die Schülerinnen und Schüler im Themenbereich Algorithmen in Partnerarbeit jeweils schriftlich ein Lösungsverfahren zur Herstellung eines Papierfliegers erarbeitet und parallel dazu im Praxistest die Flugfähigkeit ihrer Produkte erprobt.

---

[51] vgl. Schubert/Schwill, S. 5
[52] nach dem gleichnamigen Märchen mit der binären Auswahlentscheidung (gut → in’s Töpfchen, schlecht → in’s Kröpfchen)
[53] vgl. Gallenbacher: „Es ist meine feste Überzeugung, dass ein wissenschaftliches Thema sich am allerbesten erschließt, wenn man es buchstäblich ‚begreifen’ kann.“ S. IX.

Die Lerngruppe zeigt sich insgesamt aufgeschlossen für im Informatikunterricht ungewöhnliche Vorgehensweisen wie beispielsweise Rollenspiele.[54]
Für die Arbeitsphasen am Computer gilt Folgendes: Aufgrund der Rechneranzahl in den Fachräumen im Verhältnis zur Teilnehmerzahl des Kurses ist Einzelarbeit am Computer nur selten möglich.[55] Das sehe ich allerdings nicht als nachteilig und möchte an dieser Stelle auf die Ansätze des Extreme Programming verweisen, die „Programmieren zu zweit“ (Pair Programming)[56] als Standard – und nicht als Notlösung – verwenden.
Neben der genannten Partnerarbeit bei der Nutzung der Informatiksysteme habe ich mit dem Kurs verschiedene Formen der Gruppenarbeit durchgeführt:

- Inhaltsgleiche Gruppenarbeit: Dreier- und Vierergruppen erarbeiten das gleiche Thema, Mitglieder einer Gruppe präsentieren anschließend im Plenum
- inhaltsdifferente Gruppenarbeit: Dreier- und Vierergruppen erarbeiten verschiedene Themen, Mitglieder der verschiedenen Gruppen präsentieren anschließend im Plenum
- Gruppenarbeit nach dem Prinzip des Gruppenpuzzles.

Defizite bestehen in der Lerngruppe sowohl in Phasen der Erarbeitung in Gruppen als auch während der Auswertung von Arbeitsergebnissen im Plenum. Hier ist für einige Schüler festzustellen, dass ihre aktive Beteiligung in der Gruppe ebenso wie ihr Interesse an Beiträgen von Mitschülern nur sehr schwach ausgeprägt ist. Allerdings sehe ich, dass dieses Problem durch die räumlichen Gegebenheiten verstärkt wird und durch eine die Kommunikation stärker fördernde Anordnung des Mobiliars teilweise gelöst würde.

[54] So veranschaulichte eine Schülergruppe im Rahmen des Themas Zahlendarstellung in einem Rollenspiel einen Vier-Bit-Zähler, indem vier Schüler das Bit $2^0$, $2^1$, $2^2$ und $2^3$ darstellten (stehend: Bit ist auf eins gesetzt, sitzend: Bit ist auf null gesetzt), während ein weiterer Schüler als Impulsgeber durch Anstoßen des Einerbits den Takt für das Zählen von 1 bis 15 angab.
[55] Nämlich nur dann, wenn die Schülerinnen und Schüler beide Informatikräume parallel nutzen können und mindestens ein Schüler fehlt.
[56] siehe dazu den Absatz zu Pair Programming auf der Extreme Programming-Homepage. <http://www.extremeprogramming.org/rules/pair.html>

# 4. Planung und didaktische Entscheidungen

Bruce Schneier, Autor des Buches *Secrets and Lies, IT-Sicherheit in einer vernetzten Welt*, behauptet: „Digitale Sicherheit ist so ziemlich das Coolste, mit dem man sich heute befassen kann [...].“[57] Natürlich gibt es jenseits dieser Behauptung weitere Gründe, das Thema Computersicherheit als inhaltlichen Schwerpunkt der Unterrichtsreihe zu wählen. In diesem Abschnitt werde ich zunächst den Bezug des Themas zum Rahmenlehrplan Informatik für die gymnasiale Oberstufe herausstellen und dann den Bezug zur Schülerwelt sichtbar machen.

## 4.1. Bezug zum Rahmenlehrplan

An der Luise-Henriette-Oberschule wird derzeit vor der Jahrgangsstufe 12 kein Informatikunterricht erteilt. Daher ist Informatik für die Schüler und Schülerinnen meines Grundkurses ein neu beginnendes Fach. Der Berliner Rahmenlehrplan für die gymnasiale Oberstufe sieht für Informatik als neu beginnendes Unterrichtsfach im ersten Kurshalbjahr der Qualifikationsphase den Kurs in-Z1 mit den beiden Inhaltsbereichen „Rechner und Netze“ sowie „Datenbanken und Datenschutz“ vor.[58]

**1. Kurshalbjahr (in-Z1): Einführung in die Informatik**
**Rechner und Netze**
- Schichtenarchitektur
- VON-NEUMANN-Architektur
- Client-Server-Struktur
- Protokolle
- Einblicke in die Geschichte der Informatik

**Datenbanken und Datenschutz**
- Überblick zu Datenbanksystemen (DBS)
- Benutzung eines einfachen relationalen DBS
- Datenschutz und Datensicherheit
- Datenschutzgesetz mit Fallbeispielen

**Abbildung 2: Auszug aus dem Berliner Rahmenlehrplan für die gymnasiale Oberstufe**

Meine Unterrichtsreihe zur Computersicherheit bezieht sich auf Inhalte des zweiten genannten Bereichs und dort auf den Unterpunkt „Datenschutz und Datensicherheit“. Mit dem Thema Kryptologie setze ich den Schwerpunkt auf einen Teilbereich der Datensicherheit, der sich als Vertiefungsgebiet im Rahmenlehrplan wiederfindet. Der Rahmenlehrplan sieht Vertiefungsgebiete vor, welche es ermöglichen, „exemplarisch

[57] Schneier, S. xi
[58] Rahmenlehrplan S. 24

klassische und/oder aktuelle Themenbereiche der Informatik zu erarbeiten, um die Einsichten und Kompetenzen der Lernenden zu erweitern“.[59] Das Themengebiet „Kryptologie und Datensicherheit“ ist ein mögliches Vertiefungsgebiet (V2).[60]

## 4.2. Bezug zur Lebenswelt der Schülerinnen und Schüler

### 4.2.1. Computersicherheit und Lebenswelt

Die Schüler nutzen nicht nur im Fachunterricht sondern auch zuhause den Computer als Kommunikationsmedium und Arbeitsmittel. Sicherheitsrisiken wie Viren, Würmer oder Trojaner sind ihnen, wenn auch nicht in den technischen Details, so doch zumindest als Schlagworte bekannt. Ebenso kennen und verwenden sie gewisse Schutzmaßnahmen: Auf den Schulrechnern besitzt jeder Schüler einen eigenen, passwortgeschützten Bereich; die Eingabe des Namens und des Passwortes zur Authentifizierung im Rechnernetz der Schule ist für die Schüler Routine. Auch zuhause werden Dateien auf dem Computer vor dem Zugriff Unbefugter (Eltern, Geschwister, ...) geschützt. Firewalls schotten die Computer in der Schule wie zuhause gegen Angriffe aus dem Internet ab. Die Tatsache, dass digitale Sicherheitsrisiken im Alltag der Schüler allgegenwärtig sind, macht das Wissen über und das Anwenden von Schutzmaßnahmen zu einem für jeden Einzelnen relevanten Thema.
In der ersten Unterrichtsstunde des neu beginnenden Grundkurses Informatik hatte ich die Schülerinnen und Schüler aufgefordert, stichwortartig auf Zettel zu schreiben, welche inhaltlichen Erwartungen sie an das Schulfach Informatik mitbringen. Wir haben die Zettel anschließend an der Tafel gesammelt, sortiert und geclustert.[61] In Verbindung mit der Unterrichtsreihe zur Computersicherheit sind es zwei Nennungen, die mir hier erwähnenswert scheinen. Auf einem Zettel wurde genannt: „Passwörter knacken“, ein anderer Zettel nannte: „Ich will Hacker werden!“.

### 4.2.2. Kryptologie und Lebenswelt

Viele Schülerinnen und Schüler können auf spielerische Erfahrungen im Bereich Kryptologie zurückgreifen: Als Grundschüler haben sie Nachrichten in Geheimtinte geschrieben, dann Kryptogramme in einem Harry-Potter-Roman entziffert und später mit dem „Meisterdieb Artemis Fowl“ in den Büchern Eoin Colfers Geheimcodes entschlüs-

[59] Rahmenlehrplan, S. 20
[60] Rahmenlehrplan, S. 27
[61] nach der Kartenmethode als Metaplantechnik zur Gesprächsmoderation

selt. Kinder- und Jugendliteratur steckt voller Möglichkeiten, die eigenen detektivischen Fähigkeiten zu erproben, dabei Aha-Effekte zu erfahren und Erfolgserlebnisse zu gewinnen, und ganz allgemein Spaß am Rätseln zu entwickeln.

## 4.3. Inhaltliche Entscheidungen

Im Rahmen der Unterrichtsreihe werden folgende kryptografische Verfahren behandelt:

1. Als Vertreter der „klassischen“ Verfahren Caesar, Alberti und Vigenère.
2. Als (elektro-)mechanisches Verfahren die Verschlüsselung der Chiffrier-Maschine Enigma.
3. Als Beispiel für moderne asymmetrische Kryptografie das RSA-Verfahren.

Die Verfahren werden in der Reihenfolge ihrer zeitlichen Entstehung erarbeitet, was sich aus zwei Gründen anbietet: Erstens können die Schülerinnen und Schüler so die Geschichte der Kryptografie als ständige Weiterentwicklung und Verbesserung von Verfahren im Wettstreit zwischen Kryptografen und Angreifern erleben. Zweitens wächst bei dieser Ordnung vom Einfachen zum Komplizierten schrittweise die an die Schülerinnen und Schüler gestellte Leistungsanforderung.
Die „Handreichungen zum Berliner Rahmenlehrplan Informatik“ schlagen vor, den RSA-Algorithmus in den Mittelpunkt zu stellen.[62] Diese Idee wurde hier im Prinzip aufgegriffen, indem der Algorithmus als derzeitiger „Höhepunkt der Verschlüsselungskunst“ den Abschluss der Reihe darstellt. Die besondere Bedeutung der RSA-Verschlüsselung in Bezug auf Computersicherheit in der Praxis steht im Fokus der 10. und 11. Reihenstunde „Sicherheit mit RSA?“: Dort werden Anwendungen des RSA-Verfahrens beim E-Banking betrachtet, die Übereinstimmung mit Kerckhoffs’ Prinzip hervorgehoben, sowie der *RSA Factoring Challenge* kennengelernt.

## 4.4. Methodische Entscheidungen

Vor dem Hintergrund, dass Mitverantwortung und Mitgestaltung von Unterricht im Rahmenlehrplan der Sekundarstufe II festgeschriebene Prinzipien sind, [63] erscheinen mir ausgewählte Methoden des SOL geeignet, die Schüleraktivität zu steigern und damit genau diese Leitziele anzubahnen.

[62] Handreichungen, S. 13
[63] siehe Einleitung.

Die einzelnen SOL-Methoden werden ausführlich auf der Homepage des baden-württembergischen Kultusministeriums vorgestellt und anhand von Beispielen erläutert.[64] Im Rahmen meiner Unterrichtsreihe zur Computersicherheit habe ich folgende Methoden des SOL-Ansatzes verwendet, die ich in den folgenden Abschnitten kurz vorstellen werde:

Gruppenpuzzle

Sortieraufgabe mit Begriffskarten

Strukturlegen mit Begriffskarten

### 4.4.1. Gruppenpuzzle

Im SOL-Ansatz ist das Gruppenpuzzle ein zentraler Bestandteil: „Organisatorisches Grundprinzip ist das Gruppenpuzzle.“[65] Das Gruppenpuzzle wird in der Erarbeitungsphase eingesetzt, indem ein vom Lehrer in mehrere Teilthemen zerlegtes Thema von den Schülerinnen und Schülern in arbeitsteiligen Gruppen selbstständig erarbeitet wird. Der Wechsel von Phasen in themendifferenten Stammgruppen zu Phasen in themengleichen Expertengruppen ist das Merkmal dieser Methode. Konkret werden die folgenden Arbeitsphasen durchlaufen:[66]

1. Themenverteilung in der **Stammgruppe**: Zunächst werden in den sogenannten Stammgruppen die zu erarbeitenden Teilthemen auf die Mitglieder verteilt. Die Stammgruppengröße ist jeweils so groß, wie die Zahl der zu verteilenden Unterthemen (in den Beispielen drei oder vier).
2. Erarbeitung in der **Expertengruppe**: In neuen themengleichen Gruppen gleicher Gruppengröße wie zuvor, den sogenannten Expertengruppen, erarbeiten die Mitglieder gemeinsam ihr Thema und überlegen sich, wie sie den Stoff später präsentieren wollen.
3. Wissensvermittlung in der **Stammgruppe**: In diesem Schritt kehren die Experten wieder in ihre Stammgruppen zurück und geben dort in Form einer Kurzpräsentation das erarbeitete Wissen an die anderen Gruppenmitglieder weiter, so dass nach Abschluss dieser Phase jedes Gruppenmitglied die Informationen zu allen Teilthemen besitzt.

[64] Herold, Martin. Lehrerfortbildung. Internet: <http://sol-mlf.lehrerfortbildung-bw.de > [08.01.2008]
[65] SOL-Broschüre, S.4
[66] Herold und Landherr, S.78-79.

Interessanterweise ist das Gruppenpuzzle die einzige SOL-Methode, die in den ersten Monaten meines Referendariats in allen drei Seminaren (Allgemeines Seminar, Fachseminar Englisch und Fachseminar Informatik) sowohl vorgestellt als auch mit der Seminargruppe ausprobiert wurde. Ein aktueller Artikel über „Die Jigsaw-Methode“ stellt fest: „Das Gruppenpuzzle ist der Klassiker unter den kooperativen Arbeitsmethoden.“[67] Daher will ich kurz erläutern, wie und wo diese Lernform entstanden ist.
Das Gruppenpuzzle wurde erstmals 1971 in Austin, Texas verwendet „as a matter of absolute necessity“, wie der Erfinder dieser Methode, der Psychologie-Professor Elliot Aronson rückblickend schreibt.[68] Mit dem Ende der Rassentrennung fanden sich erstmals weiße, afro-amerikanische und hispanische Jugendliche gemeinsam im Klassenzimmer. Aronson beschreibt, wie sich gegenseitiges Misstrauen, Vorurteile und Rassismus in Gewalt ausdrückten und die Schüler nicht miteinander klar kamen. Anhand von Unterrichtshospitationen analysierte Aronson gemeinsam mit seinen Studenten die Situation und entwickelte den *Jigsaw Classroom* als Antwort auf die existierenden Probleme. Das Ziel, nämlich „to help students get along with each other”, wurde durch diese kooperative Lernform erreicht.

Für den Einsatz der Methode des Gruppenpuzzles habe ich mich in der 1./2. und 10./11. Reihenstunde entschieden, da sich die in diesen Stunden behandelten Themen gut in verschiedene Aspekte zerlegen lassen und mir eine selbstständige Erarbeitung der Teilthemen innerhalb der Expertengruppen realistisch erscheint.
In der 1./2. Reihenstunde erarbeiten sich die Schülerinnen und Schüler mit Caesar, Alberti und Vigenère drei historische Beispiele symmetrischer Verschlüsselungsalgorithmen, die sich in Komplexität und Umfang nur geringfügig unterscheiden. Da das Caesar-Verfahren das simpelste dieser drei Verfahren ist, erhalten die Caesar-Experten die zusätzliche Aufgabe, Chiffrierscheiben aus vorbereiteten Bögen[69] herzustellen.
In der 10./11. Reihenstunde lässt sich das Thema „Sicherheit mit RSA?“ in drei sich ergänzende Teilaspekte zerlegen. Die inhaltlichen Aspekte der Expertengruppen bieten jeweils unterschiedliche Blickwinkel auf das RSA-Verfahren, die in den Stammgruppen zu einer Gesamteinschätzung des Verfahrens zusammengetragen werden sollen.

[67] Avci-Werning, Meltem. „Die Jigsaw-Methode.“ In: Lernchancen. Heft Nr. 56, Berlin: Friedrich-Verlag, 2007. S. 48.
[68] Aronson, Elliot. “History of the Jigsaw”. Internet: <http://www.jigsaw.org/history.htm> [08.01.2008]
[69] Verwendung fanden die Kopiervorlagen von Gallenbacher, Anhang Kapitel 9 (ohne Seitenzahl)

### 4.4.2. Sortieraufgabe mit Begriffskarten

Sowohl die Sortieraufgabe als auch das Strukturlegen eignen sich am Ende einer Unterrichtsreihe zur Wiederholung und Festigung des Gelernten. Das benötigte Arbeitsmaterial für beide Methoden sind Begriffskarten. Die Begriffskarten enthalten jeweils einen aus einer Menge (vorgeschlagen wird die Zahl 30)[70] von Fachbegriffen, die für das unterrichtete Thema relevant sind. Diese Begriffe werden auf ein Blatt Papier gedruckt, jeder Schüler erhält eine Kopie und schneidet die Begriffe aus. Nachdem jeder Schüler einen Satz Begriffe (die Begriffskarten) vor sich liegen hat, wird sortiert.
Das Sortieren funktioniert folgendermaßen:

1. In Einzelarbeit sortieren die Schülerinnnen und Schüler die Begriffe auf zwei Stapel: den „Weiß-ich"-Stapel und den „Weiß-ich-nicht"-Stapel. Auf den ersten Stapel kommen die Begriffe, die den Schülern bekannt sind, auf den zweiten entsprechend die unbekannten Begriffe, also die, deren Bedeutung sie momentan nicht zuordnen können.
2. In Dreier- oder Vierergruppen klären die Schüler gemeinsam die Begriffe Ihrer „Weiß-ich-nicht"-Stapel. Bei Unklarheiten sind sowohl Nachschlagen in den Unterlagen (Hefter, Lehrbuch) als auch Rückfragen an die Lehrerin erlaubt.

### 4.4.3. Strukturlegen mit Begriffskarten

Strukturlegen wird in der Regel zunächst in Einzelarbeit ausgeführt. Da bei dieser Methode, wie bei der Sortieraufgabe, mit Begriffskarten gearbeitet wird, und ein sinnvolles Strukturieren nur machbar ist, wenn die Begriffe zuvor verstanden worden sind, bietet sich eine Unterrichtssequenz an, in der die Schüler zuerst die Sortieraufgabe und dann das Strukturlegen ausführen.
Das Strukturlegen wird folgendermaßen durchgeführt:

1. Der Schüler/die Schülerin legt die Begriffskarten vor sich auf dem Tisch zu einer Struktur zusammen. Die Begriffe können hin- und hergeschoben werden, bis die Struktur (für den jeweiligen Schüler!) passt.
2. Nach Fertigstellung können die Begriffe auf ein Blatt Papier geklebt und mit Überschriften, Verbindungslinien, Pfeilen etc. ergänzt werden.

Es gibt hier keine Master-Lösung, denn „Strukturlegen dient der individuellen Ordnung und nachhaltigen Speicherung neuer Fachinhalte."[71] Die auf dem Tisch visualisierten Strukturen spiegeln zwar alle einen inhaltlich-logischen Zusammenhang der Begriffe

[70] Herold und Landherr, S. 73
[71] Herold, S. 74

wider, dieser ist aber nicht eindeutig, sondern wird sich in Abhängigkeit von den individuellen Ordnungskriterien der Schüler unterscheiden.
Nachdem alle Schülerinnen und Schüler ihre Strukturen gelegt haben, kann die Lerngruppe aufgefordert werden, sich die Lösungen anderer anzusehen und sich diese erklären zu lassen. Dafür bleibt zum Beispiel die eine Hälfte der Lerngruppe bei ihren gelegten Strukturen sitzen, während die andere Hälfte der Gruppe umhergeht. Nach einiger Zeit wird gewechselt.
In der 12. und letzten Reihenstunde verwendete ich die Sortieraufgabe mit Begriffskarten zur Kryptografie und daran anschließend das Strukturlegen mit diesen Begriffskarten. Der Einsatz dieser Methoden diente der weiteren Vernetzung der behandelten Fachinhalte sowie der nachhaltigen Speicherung des erworbenen Fachwissens.

### 4.4.4. Weitere Entscheidungen

In zwei Unterrichtsstunden habe ich mich für den Einsatz englischsprachiger Texte entschieden. Erstens: Die Entschlüsselung des Kryptogramms aus *Der Goldkäfer* ist nur im englischen Original möglich. Zweitens: Die Bekanntmachung der erfolgreichen Faktorisierung von RSA200 liegt nur in der *Lingua franca* Englisch vor.
Diese Entscheidung fällte ich, nachdem ich mich in einem Grundkurs Englisch, den neun meiner Informatikschülerinnen und -schüler besuchen, bei Hospitationen vom Leistungsniveau der Schüler überzeugen konnte. Da außerdem vier weitere Kursteilnehmer einen Leistungskurs Englisch belegt haben, konnte ich von ausreichenden Englischkenntnissen für mein Vorhaben ausgehen.
Eine weitere Methode namens „Think-Pair-Share“/ „Ich-Du-Wir“ [72], die weder zum SOL-Repertoire noch zum konventionellen Unterricht gehört, verwende ich in der 5./6. Reihenstunde bei der erwähnten Kryptoanalyse aus *Der Goldkäfer*. Diese Entscheidung fiel aufgrund folgender Überlegungen: Die Methode fördert zunächst die intensive individuelle Auseinandersetzung mit einem Problem, anschließend werden Ideen mit dem Partner besprochen und weiter entwickelt, bevor sie dann in der Gruppe gemeinsam zusammengetragen werden. Think-Pair-Share ist besonders geeignet für die arbeitsgleiche Erarbeitung einer Problemlösung, bei der das Problem offen und zugänglich ist und das Ergebnis vom Ideenreichtum der ganzen Lerngruppe abhängt.
Für die Verwendung des E-Learning-Programms CrypTool (das ich im folgenden Abschnitt kurz vorstelle) sprechen die anschaulichen Simulationen, die in der ersten Erar-

[72] Bärzel, S. 118-121.

beitungsphase eines neuen Algorithmus das Verstehen fördern. Weiter lassen die interaktiven Möglichkeiten des Lernprogramms in Phasen des Anwendens und Übens ein aktives, exploratives Lernen zu. Die aktuelle Version CrypTool 1.4.10. ist in den beiden Informatikräumen der Luise-Henriette-Oberschule auf allen Rechnern installiert.

## 4.5. CrypTool

CrypTool ist ein Lernprogramm zur Kryptologie mit der Zielsetzung, für Sicherheit in der Informationstechnologie zu sensibilisieren. Ursprünglich von der Deutschen Bank für Mitarbeiterschulungen entwickelt, wird CrypTool seit 1998 von Teams der Universitäten Siegen und Darmstadt weiterentwickelt und beschränkt sich nicht mehr auf den Einsatz in der betrieblichen Weiterbildung. Inzwischen ist das Programm CrypTool in der Version 1.4.10 als Freeware verfügbar und wird auch in der schulischen Lehre eingesetzt.[73] Ein Einsatz im Informatikunterricht wird in den „Handreichungen zum Berliner Rahmenplan Informatik“ explizit empfohlen.[74]

Mit CrypTool können Schülerinnen und Schüler moderne und klassische kryptografische Verfahren nachvollziehen. Mithilfe interaktiver Programme werden die einzelnen Verfahren und die dahinter liegenden Algorithmen schrittweise veranschaulicht. Es kann auch experimentiert werden: CrypTool bietet die Möglichkeit, eigene Texte gemäß eines gewählten Verfahrens mit einem selbstgewählten bzw. -generierten Schlüssel zu chiffrieren.

Die nachfolgende Abbildung zeigt die Verschlüsselung der Nachricht: „Morgen um sieben vor der Kirche“ mit dem selbstgewählten Schlüssel D, also einer Caesar-Verschiebung um drei Buchstaben im Alphabet.

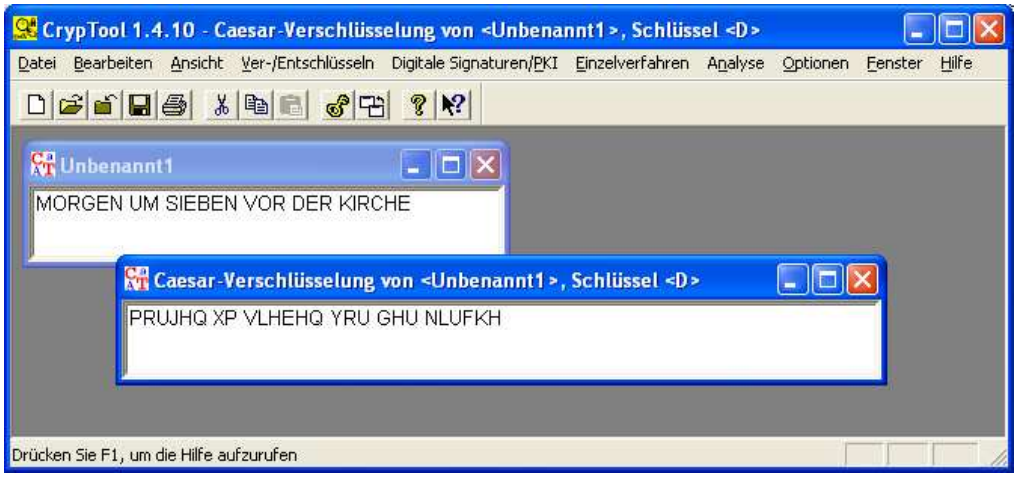



**Abbildung 3: Caesar-Verschlüsselung mit CrypTool**

[73] Esslinger, 2007, S.2
[74] Handreichungen zum RLP, S. 13

Ergänzend bietet das Programm auch Funktionen für die Kryptoanalyse sowohl klassischer als auch moderner Verfahren. Beispielsweise können verschlüsselte Textdokumente bezüglich der Häufigkeit einzelner Buchstaben und n-Gramme analysiert werden, ein hilfreiches Werkzeug bei der Entschlüsselung monoalphabetisch chiffrierter Dokumente. Aber auch moderne Verfahren können mit CrypTool dechiffriert werden: Das Programm bietet verschiedene Algorithmen zur Faktorisierung.

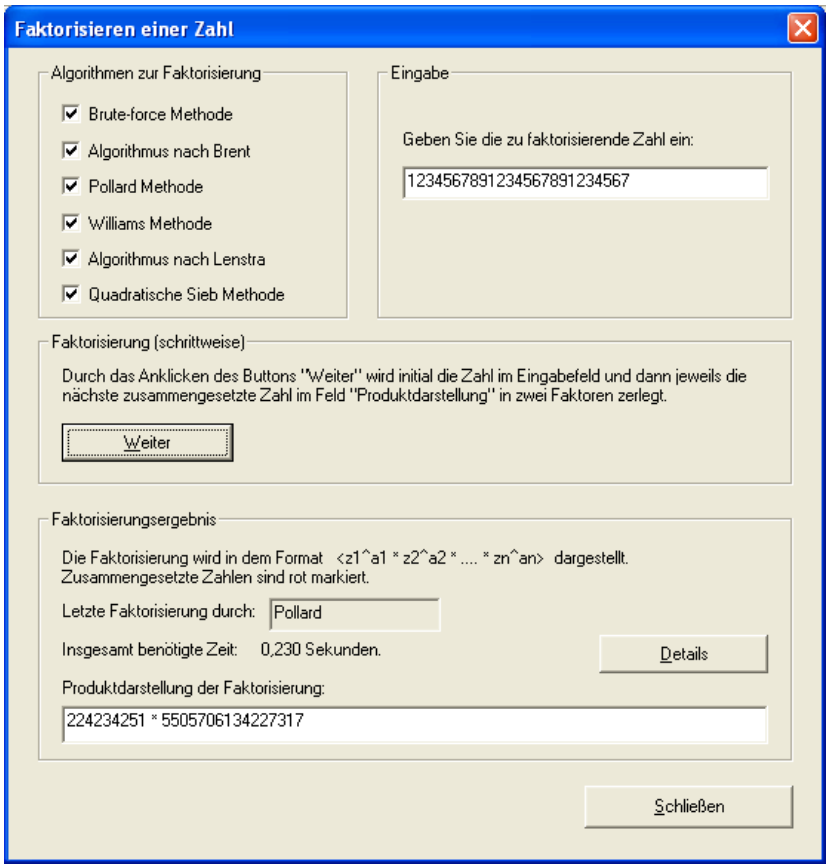



**Abbildung 4: Faktorisieren einer Zahl mit CrypTool**

In der Abbildung wurde eine 25-stellige Zahl in nur 0,23 Sekunden in ihre Primfaktoren zerlegt.

Da CrypTool als E-Learning Programm konzipiert ist, kann es sowohl für die selbstständige Erarbeitung neuer Lerninhalte eingesetzt werden als auch zur Wiederholung und Vertiefung vorhandener Kenntnisse. Darüber hinaus existiert seit Ende 2007 ein das E-Learning-Programm ergänzendes Portal, auf dem Lehrerinnen und Lehrer geeignete Unterrichtsentwürfe und -materialien im Themenfeld Kryptologie veröffentlichen.

# 5. Synopse

Die Durchführung der Unterrichtsreihe umfasste insgesamt zwölf Unterrichtsstunden im Zeitraum vom 19. November bis 18. Dezember 2007. In der Mitte der Reihe lag die an der Luise-Henriette-Oberschule durchgeführte Projektwoche in der Zeit vom 3. bis 6. Dezember, wodurch sich der folgende Ablauf ergab: Zwei Wochen Durchführung der Unterrichtsreihe, eine Woche Mitarbeit bei der Projektwoche, zwei Wochen Durchführung der Unterrichtsreihe. In der Übersicht sind die Unterrichtssequenzen, die in „Darstellung und Analyse“ näher betrachtet werden grau hinterlegt.

| **Reihen-stunde** | **Fachinhalte und Unterrichtsform** | **Kompetenzen**[75] |
|---|---|---|
| **Thema: Klassische Verfahren der Kryptografie** | | |
| **1. und 2. Montag, 19. 11.** | Grundbegriffe der Kryptologie (Schlüssel, Ver- und Entschlüsselung, Geheimtextalphabet, Klartextalphabet)<br>Historische mono- und polyalphabetische Verfahren der Verschlüsselung: Caesar/Alberti/Vigenère | Grundbegriffe der Kryptologie kennen und verwenden.<br>Das Caesar-Verfahren als typische monoalphabetische Verschlüsselung kennen und anwenden.<br>Das Alberti-Verfahren als einfache polyalphabetische Verschlüsselung kennen und anwenden.<br>Das Vigenère-Verfahren als typische polyalphabetische Verschlüsselung kennen und anwenden.<br>Mit Information umgehen:<br>Recherchieren in globalen Informationsräumen (Wikipedia).<br>Ausgewählte Funktionen des E-Learning-Programms CrypTool nutzen.<br>Kommunizieren und Kooperieren:<br>Aktive Mitarbeit in Stamm- und Expertengruppe. |
| | Gruppenpuzzle | |
| **3. Dienstag, 20.11.** | Anwenden und Üben:<br>Caesar/Vigenère | Das Caesar-Verfahren als typische monoalphabetische Verschlüsselung kennen und anwenden.<br>Das Vigenère-Verfahren als typische polyalphabetische Verschlüsselung kennen und anwenden.<br>Ausgewählte Funktionen des E-Learning-Programms CrypTool nutzen. |
| | Partnerarbeit unter Verwendung des E-Learning Programms CrypTool | |

[75] Kompetenzen gemäß Rahmenlehrplan Informatik und Handreichungen zum Berliner Rahmenlehrplan Sek. II für Informatik.

| Reihen-stunde | Fachinhalte und Unterrichtsform | Kompetenzen[75] |
|---|---|---|
| **Thema: Entziffern des Kryptogramms aus *The Gold-Bug*** | | |
| **4. und 5. Montag, 26.11.** | Kryptoanalyse des Kryptogramms aus *The Gold-Bug / Der Goldkäfer* von Edgar Allan Poe.<br>Think-Pair-Share (Ich-Du-Wir) | Entschlüsselung eines monoalphabetisch verschlüsselten englischen Textes mithilfe von Häufigkeitstabellen (Histogrammen).<br>Die Sicherheit einer monoalphabetischen Verschlüsselung beurteilen.<br>Erfahren, dass die Kryptoanalyse im Team schneller zum Erfolg führt. |
| **Thema: Enigma-Verschlüsselung** | | |
| **6. Dienstag, 27.11.** | Enigma: Informationsrecherche Simulation der Enigma-Maschine<br>Arbeitsteilige Gruppenarbeit Partnerarbeit unter Verwendung des E-Learning Programms CrypTool | Mit Information umgehen:<br>Recherchieren in globalen Informationsräumen (Wikipedia).<br>Kommunizieren und Kooperieren:<br>Arbeitsergebnisse in geeigneter Form präsentieren.<br>Ausgewählte Funktionen des E-Learning-Programms CrypTool nutzen. |
| **Thema: Das RSA-Verfahren** | | |
| **7. und 8. Montag, 10.12.** | Chiffrierung durch modulares Potenzieren.<br>Schlüsselgenerierung beim RSA-Verfahren<br>Einzel- und Partnerarbeit | Die Einweg-Eigenschaft der Multiplikation großer Primzahlen erfassen.<br>Die Generierung von Schlüsselpaaren durchführen.<br>Den RSA-Algorithmus verstehen und anwenden. |
| **9. Dienstag, 11.12.** | RSA-Wettbewerb<br>Inhaltsgleiche Gruppenarbeit | Ver- und Entschlüsselung nach dem RSA-Verfahren durchführen.<br>Die Sicherheit des RSA-Verfahrens beurteilen.<br>Ausgewählte Funktionen des E-Learning-Programms CrypTool nutzen. |

<table>
<tr><th>Reihen-<br>stunde</th><th>Fachinhalte<br>und Unterrichtsform</th><th>Kompetenzen[75]</th></tr>
<tr><td colspan="3">Thema: Sicherheit mit RSA?</td></tr>
<tr><td rowspan="2">10. und 11.<br>Montag, 17.12.</td><td>RSA und Sicherheit<br>Anwendungen und Probleme des RSA-Verfahrens</td><td rowspan="2">Die Sicherheit des RSA-Verfahrens beurteilen, Bedeutung für Sicherheit im Internet erkennen:<br>Kerckhoffs’ Prinzip benennen und erkennen, dass das RSA-Verfahren diesen Grundsatz erfüllt.<br>Erkennen, dass digitale Zertifikate das RSA-Verfahren verwenden<br>Informationen über den RSA Factoring Challenge auswerten und dabei erkennen, dass die Schwierigkeit des Faktorisierens von N die Sicherheit des RSA-Algorithmus ausmacht.<br>Kommunizieren und Kooperieren:<br>Aktive Mitarbeit in Stamm- und Expertengruppe.</td></tr>
<tr><td>Gruppenpuzzle</td></tr>
<tr><td colspan="3">Thema: Begriffskarten zur Kryptografie</td></tr>
<tr><td rowspan="2">12.<br>Dienstag,<br>18.12.</td><td>Begriffe zur Kryptografie und Geschichte der Kryptografie</td><td rowspan="2">Die Schülerinnen und Schüler strukturieren die in der Unterrichtsreihe erworbenen neuen Fachinhalte im Sinne einer individuellen Ordnung zur nachhaltigen Speicherung des Wissens.</td></tr>
<tr><td>Sortieraufgabe und Strukturlegen mit Begriffskarten</td></tr>
</table>

**Tabelle 6: Übersicht über die durchgeführte Unterrichtsreihe**

# 6. Darstellung und Analyse ausgewählter Sequenzen

## 6.1. Zur Auswahl der Sequenzen

Die ausgewählten Sequenzen dienen der genauen Betrachtung und Analyse der unter 1.2.3. genannten Aspekte. Als erste Unterrichtssequenz werde ich eine Doppelstunde zur Erarbeitung dreier klassischer kryptografischer Verfahren vorstellen. Die zweite dargestellte Unterrichtssequenz ist eine Doppelstunde zur Beurteilung der Sicherheit des RSA-Verfahrens. Abschließend stelle ich eine Unterrichtsstunde zur Vernetzung der erworbenen Fachinhalte vor.

## 6.2. Thema: Klassische Verfahren der Kryptografie

### 6.2.1. Stundenziel

Die Schülerinnen und Schüler kennen und verwenden die Grundbegriffe Schlüssel, Ver- und Entschlüsselung, Geheimtextalphabet und Klartextalphabet. Sie recherchieren in globalen Informationsräumen (Wikipedia). Sie kennen drei klassische Verfahren der Verschlüsselung: Caesar, Alberti und Vigenère.

### 6.2.2. Darstellung und Analyse

Diese Doppelstunde bildete den Einstieg in die vierwöchige Unterrichtsreihe zur Computersicherheit. In dieser Unterrichtssequenz arbeiteten die Schülerinnen und Schüler nach der Methode des Gruppenpuzzles, der zeitliche Ablauf war wie folgt geplant:

Einstieg/Stammgruppen: 15 Minuten
Expertengruppen: 30 Minuten
Pause: 5 Minuten
Stammgruppen: 30 Minuten
Plenum: 15 Minuten

Nach einer kurzen Lehrerinfo über Inhalte und Methoden der neu beginnenden Unterrichtsreihe erfolgte die Einteilung in Stammgruppen lehrergesteuert nach Sitzordnung. Aus der Anzahl von 23 anwesenden Kursteilnehmern und drei Teilthemen ergaben sich sowohl für die Stammgruppen als auch für die Expertengruppen fünf Dreier- und zwei Vierergruppen. Für die Einteilung der Experten waren die Schülerinnen und Schüler selber verantwortlich, d.h. die Verteilung der drei Themen innerhalb der Stammgruppen wurde selbstständig ausgehandelt. Für die beiden Viererstammgruppen ergab sich die

unvermeidliche Situation, dass durch die Doppelbelegung eines der drei Themen eine gewisse Redundanz existierte.

Damit in den Expertenrunden konzentriert gearbeitet werden konnte, stellte ich für diese Phase beide Informatikräume zur Verfügung: Die Caesar-Expertenrunden nutzten Raum 312, während die Expertengruppen zu Alberti und Vigenère Raum 310 nutzten.

Auf den Arbeitsblättern (im Anhang die Arbeitsblätter Alberti und Vigenère) waren als Quelle für die Informationsrecherche zum einen Seiten der deutschsprachigen Wikipedia angeführt, zum anderen wurde auf Visualisierungen verwiesen, die das E-Learning-Programm CrypTool bereithält.

Was ich nicht vorhergesehen hatte war, dass an diesem Tag das Internet nicht zur Verfügung stehen würde.[76] Für die Caesar- und Vigenère-Expertenrunden war das kein substanzielles Problem: Da CrypTool ausreichende Informationen zu den Verfahren zur Verfügung stellt, konnte auf dieses Offline-Programm zurückgegriffen werden. Anders sah dies für die Alberti-Experten aus. Da das Alberti-Verfahren in CrypTool nicht visualisiert wird, wurde auf dem Arbeitsblatt dieser Gruppe ausschließlich auf Internetquellen verwiesen, die jetzt aber nicht zu erreichen waren. Ich entschied daher spontan, mich selber als Alberti-Experten zur Verfügung zu stellen. Diese inhaltliche Einbindung meiner Person hatte allerdings nachteilig zur Folge, dass ich dadurch die zuvor geplante Beobachterrolle in dieser Phase nicht wahrnehmen konnte.

Die anschließende Synthese in den Stammgruppen erfolgte wieder für alle Gruppen in Raum 310. Bevor die Experten in ihren Stammgruppen berichteten, regte ich als sinnvolle Rednerreihenfolge den Verlauf Caesar-Alberti-Vigenère an. In der Stammgruppenphase konnte ich mich als Beobachterin davon überzeugen, dass die jeweiligen Experten „ihr“ Verfahren sachkundig und verständlich vorstellten und dabei die Grundbegriffe (Schlüssel, Ver- und Entschlüsselung, Geheimtextalphabet, Klartextalphabet) korrekt verwendeten.

In einem abschließenden Unterrichtsgespräch im Plenum nannten einzelne Schüler die Bereiche Diplomatie/Militär sowie Kirche/Päpstlicher Hof als Einsatzfelder für Kryptografie. Weiter erläuterten die Schüler die Begriffe mono- und polyalphabetisch und konnten sie den vorgestellten Verfahren zuordnen. Sie äußerten und begründeten ihre Vermutungen über die Sicherheit der behandelten Verfahren.

[76] Eine Situation, die (so der Systemadministrator) „extrem selten, eigentlich fast nie“ auftritt.

Der Umgang mit Information beim Recherchieren in globalen Informationsräumen konnte in dieser Sequenz aus den oben genannten Gründen nicht wie geplant geübt werden .

### 6.2.3. Alternativen

Da die Ziele dieser Stunde insgesamt erreicht wurden, scheint die Methode des Gruppenpuzzles in dieser Lerngruppe grundsätzlich geeignet zu sein, klassische Verfahren der Kryptografie zu erarbeiten. Teile der Planung lassen sich aber optimieren: Denkbar (und vorausschauend hinsichtlich des beschriebenen Netzausfalls) wäre die Bereitstellung der zu dem Alberti-Verfahren benötigten Informationen entweder in digitaler Form oder in gedruckter Form auf Papier. Grundsätzlich ließe sich diese Stunde sogar ganz ohne Computer durchführen, da alle drei Verfahren mit Papier und Bleistift nachvollzogen werden können.
Allerdings spricht für den Einsatz von CrypTool zur Veranschaulichung des Caesar- und des Vigenère-Verfahrens die ansprechende Visualisierung dieser Algorithmen. Vor diesem Hintergrund plädiere ich, bei aller Sympathie für „Papier und Bleistift“-Informatik, in dieser Unterrichtssequenz für den Einsatz des Programms.

## 6.3. Thema: Sicherheit mit RSA?

### 6.3.1. Vorausgegangener Unterricht

Wie aus der Synopse ersichtlich, war dieser Unterrichtssequenz eine eher mathematikzentrierte Doppelstunde zur Erarbeitung des RSA-Algorithmus vorausgegangen, sowie eine Einzelstunde, in der die Schlüsselgenerierung in Form eines RSA-Wettbewerbs vertiefend geübt wurde.

### 6.3.2. Stundenziel

Die Schülerinnen und Schüler benennen Kerckhoffs’ Prinzip und erkennen, dass das RSA-Verfahren diesen Grundsatz erfüllt. Sie erkennen die Bedeutung von RSA-Verfahren für die Sicherheit im Internet. Sie werten Informationen über den *RSA Factoring Challenge* aus und erkennen dabei, dass die Schwierigkeit des Faktorisierens von N die Sicherheit des RSA-Algorithmus ausmacht.

### 6.3.3. Darstellung und Analyse

In dieser Doppelstunde arbeiteten die Schülerinnen und Schüler nach der Methode des Gruppenpuzzles. Die Einteilung in Stammgruppen erfolgte wie unter Sequenz 1 beschrieben, diesmal entsprach die Anzahl der Anwesenden aber mit 24 einer Zahl, die (mod 3) = 0 ergibt.[77] Die Einteilung der Experten erfolgte innerhalb der Gruppen wieder eigenverantwortlich. Der zeitliche Ablauf im Überblick:

Einstieg/Stammgruppen: 5 Minuten

Expertengruppen: 40 Minuten

Pause: 5 Minuten

Stammgruppen: 30 Minuten

Plenum: 15 Minuten

Diesmal hatten die Schüler wegen des größeren Umfangs der Arbeitsaufträge für die Expertenphase 40 Minuten zur Verfügung, die meinen Beobachtungen zur Folge auch weitgehend zur Erarbeitung und Diskussion der Inhalte benötigt wurde. Der Umgang mit Informationen beim Recherchieren in globalen Informationsräumen konnte in dieser Sequenz wie geplant geübt werden.

Der Einsatz englischsprachiger Texte für Thema 2 (*RSA Factoring Challenge*) erwies sich, wie vermutet, nicht als Hürde. Ich konnte in den Expertenrunden beobachten, dass die Schülerinnen und Schüler die Inhalte des fremdsprachlichen Textes problemlos aufnehmen und zusammenfassen konnten.

Die anschließende Synthese in den Stammgruppen erfolgte in allen von mir beobachteten Gruppen sachkundig und verständlich. Der für diese Phase vorgesehene Zeitrahmen erwies sich als realistisch.

In der abschließenden Phase im Plenum wurde insbesondere Kerckhoffs' Prinzip von der Lerngruppe kontrovers diskutiert. Ist ein Verfahren wirklich sicherer, weil es über lange Zeit öffentlich geprüft wurde? Oder erhöht die Offenlegung des Algorithmus das Sicherheitsrisiko? Ein Schüler formulierte eine weitere Frage zur Sicherheit des RSA-Verfahrens: Wird es bald Quantencomputer geben, die auch ein großes N in kurzer Zeit faktorisieren können?

Offensichtlich traf das gewählte Stundenthema in der Lerngruppe auf große Resonanz.

[77] also einer Zahl, die sich bei ganzzahliger Division ohne Rest durch drei teilen lässt.

### 6.3.4. Alternativen

Um die Bedeutung des RSA-Verfahrens für die Sicherheit im Internet einschätzen zu können, wurde in dieser Stunde als Beispiel Internet-Banking gewählt. In der vorbereitenden Planung dieser Sequenz hatte ich, unter dem Aspekt Schülernähe, auch den Bereich E-Commerce mit entsprechenden Internet-Auftritten einzelner Firmen in Erwägung gezogen. Meine Entscheidung, exemplarisch einen Teil des Sicherheitskonzepts des Online-Auftritts einer Berliner Bank zu wählen, fiel letzlich aufgrund der überschaubaren Darstellung dieser Bank.

## 6.4. Thema: Begriffskarten zur Kryptografie

### 6.4.1. Stundenziel

Die Schülerinnen und Schüler strukturieren mithilfe von Begriffskarten die in der Unterrichtsreihe erworbenen neuen Fachinhalte im Sinne einer individuellen Ordnung zur nachhaltigen Speicherung des Wissens.

### 6.4.2. Darstellung und Analyse

Diese Einzelstunde bildete den Abschluss der vierwöchigen Unterrichtsreihe zur Computersicherheit und war gleichzeitig die letzte Informatikstunde vor Weihnachten.
Die Schülerinnen und Schüler arbeiteten mit Begriffskarten zur Kryptografie nach den Methoden Sortieren und Strukturlegen. Die verwendeten Begriffe beinhalten sowohl Namen als Anker für die nach diesen Männern benannten Verschlüsselungsverfahren als auch Grundbegriffe der Kryptografie (siehe Tabelle).

| | | |
|---|---|---|
| Adi Shamir | geheimer Schlüssel | monoalphabetisch |
| Arthur Scherbius | Geheimtext | öffentlicher Schlüssel |
| asymmetrisch | Histogramm | polyalphabetisch |
| Blaise de Vigenère | Internet | Primzahlen |
| Caesar | Klartext | Ronald Rivest |
| digitales Zertifikat | Kryptologie | RSA |
| Diplomatie | Leon Alberti | Sicherheit |
| Enigma | Leonard Adleman | Substitution |
| Entschlüsselung | Militär | symmetrisch |
| Faktorisieren | modulo | Verschlüsselung |

**Tabelle 7: Begriffe zur Kryptologie**

Die Stunde war in zwei Phasen geteilt: Nach einer kurzen Lehrerinfo über Vorgehensweise und Ziel der verwendeten Methode, erfolgte in den ersten 20 Minuten das individuelle Ausschneiden und Sortieren der Begriffskarten mit anschließender Klärung der Begriffe des „Weiß-nicht“-Stapels in Dreiergruppen. In den weiteren 25 Minuten folgte die Durchführung des Strukturlegens in Einzelarbeit. Eine anschließende Kommunikationsphase, in der die Strukturen der Mitschüler betrachtet und diskutiert werden sollten, war als Eventualphase angedacht, konnte aber aus Zeitgründen nicht mehr durchgeführt werden.

In der ersten Phase konnte ich beobachten, dass in einigen Gruppen für die Klärung der Begriffe auf die Unterlagen im Hefter zurückgegriffen und angeregt diskutiert wurde. Ebenso wurden aus den Gruppen vereinzelt Rückfragen an mich gestellt, wobei es in erster Linie um Bestätigung von Vermutungen ging, z.B. „Adleman, das war doch der von RSA, oder?“

In der zweiten Phase war eine sehr heterogene Herangehensweise an die Aufgabe zu beobachten. Einige Schülerinnen und Schüler arbeiteten intensiv an ihren Strukturen, während andere doch eher abwartend auf ihre Begriffskarten blickten. Dies wird auf dem Foto, das ich für das Deckblatt ausgewählt habe, deutlich. Der Schüler in der Mitte des Fotos ist gerade damit beschäftigt, eine Struktur zu legen, seine Nachbarin zur rechten Seite, von der wir auf dem Bildausschnitt nur den linken Arm sehen, hat vor sich auf dem Tisch bereits Ansätze einer Struktur liegen, während der Nachbar auf der linken Seite auf seine als lange Liste ausgelegten Begriffskarten blickt.

Zwei Schüler äußerten den Wunsch, das Strukturlegen als Partnerarbeit durchführen zu dürfen. Ich erklärte ihnen, warum dieses Vorgehen dem Ziel der Methode, eine individuelle Ordnung herzustellen, widerspricht. Da sie aber offensichtlich weder einsichtig noch bereit waren, sich umstimmen zu lassen, zeigte ich mich flexibel und erlaubte schließlich das veränderte Vorgehen für diese beiden Schüler. Die anderen Schülerinnen und Schüler führten das Strukturlegen planmäßig in Einzelarbeit aus. Im weiteren Stundenverlauf zeigte sich, dass auch die genannte Zweiergruppe eine ordentlich durchdachte Struktur anfertigte.

Insgesamt zeigten die Ergebnisse, dass die Möglichkeiten der Methode zur Rückschau und Reflexion von allen Schülerinnen und Schülern genutzt wurden. Besonders in Erinnerung geblieben ist mir die positive Rückmeldung einer Schülerin, die nach dem Strukturlegen sagte: „Das funktioniert wirklich, ich kann mir die Sachen so besser merken!“

### 6.4.3. Alternativen

Da die Ziele dieser Stunde insgesamt erreicht wurden, scheinen die verwendeten Methoden für diese Lerngruppe geeignet zu sein, Fachinhalte in ihren logischen Zusammenhängen zu begreifen.

Dennoch möchte ich Alternativen hinsichtlich der Zeitplanung und der Sicherung erwähnen. Optimierungen sind bei der Zeitplanung erforderlich: Auf die Durchführung einer anschließenden Kommunikationsphase, in der die Strukturen der Mitschüler betrachtet und diskutiert werden, sollte meines Erachtens nicht verzichtet werden. Zum einen werden so die einzelnen Tätigkeiten der Schülerinnen und Schüler gewürdigt, zum anderen bietet sich beim Vergleich alternativer Strukturen die Möglichkeit, eigene Schemata zu überdenken. Diese Optimierung könnte erreicht werden durch:

- einen größeren Zeitrahmen (etwa 60 Minuten)
- weniger Begriffskarten
- bereits ausgeschnittene Begriffskarten, um so die Phase des Ausschneidens zu sparen.

In Bezug auf die Ergebnissicherung sind Alternativen denkbar. Die Strukturen können nach Fertigstellung auf ein entsprechend großes Blatt Papier geklebt und dadurch für die Zukunft fixiert werden. Ein derartiges Produkt kann dann in Kleingruppen oder im Plenum präsentiert oder ausgestellt werden.

Allerdings zeigen Untersuchungen von Herold, dass einmal konstruierte Strukturen noch Wochen später aus dem Gedächtnis wieder hergestellt werden können,[78] und daher eine Sicherung an dieser Stelle nicht unbedingt erforderlich ist. Darüber hinaus betont die in meiner Stunde gewählte Vorgehensweise den Prozesscharakter bei der Anwendung der Methoden und lässt den Schülern den Weg für eine Wiederholung des Strukturlegens (etwa zur Klausurvorbereitung) offen.

[78] Herold, S.74

# 7. Reflexion

## 7.1. Zusammenfassende Analyse

Insgesamt bin ich mit den inhaltlichen Ergebnissen der Unterrichtsreihe zufrieden. Die Schülerinnen und Schüler sind zwar durch diese zwölf Unterrichtsstunden keine Kryptoexperten geworden, konnten aber für Belange der Computersicherheit sensibilisiert werden und dabei Einblicke in die Geschichte und Gegenwart der Kryptografie gewinnen.

Doch steigerte der Einsatz von SOL-Methoden tatsächlich die Schüleraktivität?

Beim Einsatz des Gruppenpuzzles konnte ich eine Steigerung der Schüleraktivität besonders für diejenigen Schülerinnen und Schüler feststellen, die in konventionellen Unterrichtsstunden keine Wortbeiträge beisteuern. Durch den besonderen Aufbau des Wechsels zwischen Experten- und Stammgruppen sind auch Schülerinnen und Schüler, die sich in konventioneller Gruppenarbeit eher passiv verhalten, gefordert aktiv mitzuarbeiten. Mit der Methode des Gruppenpuzzles ist zumindest für die Synthesephase in der Stammgruppe eine etwa gleiche Verteilung der Redeanteile aller Gruppenmitglieder gewährleistet. Für die in dieser Reihe erprobte Methode des Sortierens mit Begriffskarten konnte ich für die gesamte Lerngruppe eine hohe Aktivität feststellen. Für die Methode Strukturieren gilt: Die Aktivität liegt in der Verantwortung des Einzelnen. Das beinhaltet aber auch die Verantwortung für die Konsequenz: Wer in dieser Phase nicht aktiv ist, kann am Ende der Phase auch kein Ergebnis vorlegen. Insgesamt überzeugte mich bei der Arbeit mit Begriffskarten der hohe Aufforderungscharakter dieser Karten.

Bei einer direkten Gegenüberstellung der analysierten SOL-Sequenzen zu den Unterrichtssequenzen ohne SOL-Methoden, ist eine höhere Schüleraktivität in allen SOL-Stunden der durchgeführten Unterrichtsreihe ersichtlich. Tatsächlich bedingt die Steigerung der Schüleraktivität eine Rücknahme der Aktivität der Lehrerin während der Unterrichtssequenzen. Hier möchte ich folgende Veränderungen hervorheben: Einerseits nimmt die Erstellung der Arbeitsblätter für die Expertengruppen im Vorfeld sehr viel Zeit in Anspruch, andererseits steht dann während der Durchführungsphasen im Unterricht ausreichend Freiraum zur Verfügung, um die Lerngruppe zu beobachten, oder dort, wo es Schwierigkeiten gibt, unterstützend einzugreifen.

Der Einsatz von Methoden des SOL bietet also, unter Einbeziehung motivierender Fachinhalte, sehr gute Möglichkeiten zur Steigerung der Schüleraktivität.

## 7.2. Ausblick

Für den weiteren Informatikunterricht in der Qualifikationsphase werde ich, ausgehend von den in dieser Reihe gewonnenen Erfahrungen, verstärkt SOL-Methoden verwenden. Die Realisierung einer anderen in dieser Zeit entstandenen Idee werde ich jedoch auf die Zeit nach dem Referendariat verschieben müssen: Fächerverbindendes Lernen in einer Unterrichtsreihe, die für das Fach Englisch „Entstehung des Genres Detektivroman in der englischsprachigen Literatur des 19. Jahrhunderts“ mit Inhalten aus der Informatik „Computersicherheit durch Kryptografie“ zusammenbringt.

# 8. Anhang

GK Informatik 19.11.2007

## Verfahren zur Verschlüsselung

## Gruppe Vigenère

Blaise de Vigenère
(Bildquelle: http://de.wikipedia.org/wiki/Bild:Vigenere.jpg)

**Bearbeiten Sie folgende Aufgaben:**

1. **Informieren Sie sich über das Vigenère-Verfahren zur Verschlüsselung!**

   Öffnen Sie CrypTool (gelbes Logo auf dem Desktop). → Einzelverfahren → Visualisierung von Algorithmen → Vigenère

   Internet: http://de.wikipedia.org (Blaise de Vigenère)

2. **Notieren Sie Stichworte zu Vigenères Leben: Beruf, Geburts-, Todesjahr, Nationalität.**

3. **Klären Sie in Ihrer Gruppe die Funktionsweise des Verfahrens.**

4. **Verschlüsseln Sie eine (kurze) Nachricht nach dem Vigenère-Verfahren. Notieren Sie sich den Geheimtext und den verwendeten Schlüssel.**

# Verfahren zur Verschlüsselung

# Gruppe Alberti

Leon Battista Alberti
(Bildquelle: http://de.wikipedia.org/wiki/Bild:LeonBattistaAlberti.jpg)

**Bearbeiten Sie folgende Aufgaben:**

5. **Informieren Sie sich über das Alberti-Verfahren zur Verschlüsselung!**

   Internet:
   http://www.schulmodell.de/info/unterricht/kl10/alberti.htm
   http://de.wikipedia.org/wiki/Leon_Battista_Alberti

6. **Notieren Sie Stichworte zu Albertis Leben: Beruf, Geburts-, Todesjahr, Nationalität.**

7. **Klären Sie in Ihrer Gruppe die Funktionsweise des Verfahrens.**

8. **Verschlüsseln Sie eine (kurze) Nachricht nach dem Alberti-Verfahren! Notieren Sie sich den Geheimtext und den verwendeten Schlüssel.**

**Thema 1**

**Sicherheit mit RSA?**

## Arbeitsauftrag 1:

Wie Sie wissen, zählt das RSA-Verfahren zu den sogenannten asymmetrischen Verfahren. Informieren Sie sich über asymmetrische Verfahren, z.B. auf der Website von Wikipedia.
Notieren Sie dabei Stichworte, um später in einem Kurzreferat folgende Fragen beantworten zu können:

1. Worin unterscheiden sich asymmetrische Verfahren der Verschlüsselung von symmetrischen Verfahren?
2. Erklären Sie anhand des RSA-Verfahrens die Begriffe
   a. öffentlicher Schlüssel
   b. privater Schlüssel

3. Nennen Sie Vorteile und Nachteile asymmetrischer Verfahren!
4. Was sind Hybridverschlüsselungsverfahren? Nennen Sie Anwendungsbeispiele!

## Arbeitsauftrag 2:

Lesen Sie den folgenden Text über Kerckhoffs' Prinzip!

**Kerckhoffs' Prinzip** ist ein Grundsatz der modernen Kryptografie. Es wurde 1883 von dem niederländischen Linguisten und Kryptologen Auguste Kerckhoffs formuliert und lautet:

„Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels."

(Quelle für Text und Bild: http://de.wikipedia.org/wiki/Kerckhoffs_Prinzip)

1. Wie lautet Kerckhoffs' Prinzip? Erklären Sie!
2. Erfüllt das RSA-Verfahren dieses Prinzip? Begründen Sie Ihre Antwort!

Lesen Sie dann im Anhang den Auszug aus der **Broschüre „Sicherheit durch Verschlüsselung**“, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben hat und notieren Sie dabei Stichworte, um später folgende Frage beantworten zu können:

3. Decken sich die darin enthaltenen Anforderungen an Verschlüsselungssysteme mit **Kerckhoffs' Prinzip** ?

---

Anhang Thema 1

# Anforderungen an Verschlüsselungssysteme

Es sind im Wesentlichen fünf Kriterien, an denen der Sicherheitswert von Verschlüsselungssystemen zu messen ist. Hier kommen logische, technische und organisatorische Elemente zusammen:

- Sicherheit der mathematisch-kryptografischen Algorithmen
- verlässliches Schlüsselmanagement
- Fehlbedienungs- und Fehlfunktionssicherheit
- Vorkehrungen gegen sicherheitsmindernde Manipulationen
- Abwesenheit verdeckter kompromittierender Kanäle

Die Sicherheit der kryptografischen Algorithmen, die der eigentlichen Datenverschlüsselung oder der Schlüsselvereinbarung dienen, kann nur auf der Grundlage einer intensiven, zeitaufwendigen, sich an „worst-case“ Situationen orientierenden und von erfahrenen Fachleuten vorgenommenen Analyse beurteilt werden. Selbst ein Verfahren, das eine solche Untersuchung überstanden hat, ist angesichts des steten wissenschaftlichen Fortschritts immer wieder kritisch zu hinterfragen.

Im Hochsicherheitsbereich wird man auf die zusätzliche Sicherheit, die ein geheim gehaltenes und dann notwendigerweise eigenentwickeltes Kryptoverfahren bietet, nicht verzichten können, da jede Offenlegung der Designprinzipien einen potentiellen Angreifer von vornherein in eine günstigere Position brächte und somit sich von selbst verbietet. Dem Anspruch auf Geheimhaltung muss dann natürlich auch die Methode der technischen Umsetzung Rechnung tragen.

**Thema 2**

**RSA Factoring Challenge**

**ANNOUNCEMENT OF "RSA FACTORING CHALLENGE"**
**(3/18/91)**

RSA Data Security hereby announces that it is sponsoring an ongoing "factoring challenge" (with cash prizes) to encourage research in computational number theory and the pragmatics of factoring large integers. RSA Data Security specializes in cryptographic products, particularly those based on the RSA public-key cryptosystem. The results of this challenge will help users of the RSA public-key cryptosystem achieve the level of security they desire.

Auszug aus der Bekanntmachung des *RSA Factoring Challenge*.
(Quelle: http://groups.google.com/group/sci.crypt/msg/a20e42af47ec4a12 )

## Arbeitsauftrag 1:

Informieren Sie sich über den „RSA Factoring Challenge“, z.B. auf der Website von Wikipedia. Notieren Sie dabei Stichworte, um später in einem Kurzreferat folgende Fragen beantworten zu können:

1. Worum geht es bei diesem Wettbewerb?
2. Erklären Sie den Begriff „factoring“ (faktorisieren) im Zusammenhang mit RSA!
3. Seit wann gibt es den Wettbewerb?
4. Wer richtete diesen Wettbewerb aus?
5. Welche „Meilensteine“ gab es in der Geschichte des Wettbewerbs?
6. Wann wurde er beendet? Warum? (Offizielle Begründung und Ihre Vermutung)

## Arbeitsauftrag 2:

Lesen Sie den Text im Anhang. Es handelt sich um einen Auszug aus der Bekanntmachung einer erfolgreichen Faktorisierung aus dem Jahre 2005.
Notieren Sie sich Stichworte, um später folgende Fragen beantworten zu können:

1. Wie lange dauerte die Faktorisierung?
2. Wie viele Computer wurden eingesetzt?
3. Wie lange hätte es auf einem einzelnen Computer mit der verwendeten CPU gedauert?

(Sollten Sie sich für Details interessieren, können Sie den gesamten Artikel unter dieser Quelle lesen: http://www.crypto-world.com/announcements/rsa200.txt)

---

**Anhang Thema 2**:

```
Date: Mon, 9 May 2005 18:05:10 +0200 (CEST)
From: "Thorsten Kleinjung"
Subject: rsa200

We have factored RSA200 by GNFS. The factors are

35324619344027701212726049781984643686711974001976\
25023649303468776121253679423200058547956528088349

and

79258699544783330333470858414800596877379758573642\
19960734330341455767872818152135381409304740185467

[…]

Sieving has been done on a variety of machines. We estimate that
lattice sieving would have taken 55 years on a single 2.2 GHz
Opteron
CPU.
Note that this number could have been improved if instead of the
PIII-
binary which we used for sieving, we had used a version of the
lattice-siever optimized for Opteron CPU's which we developed in
the
meantime.
The matrix step was performed on a cluster of 80 2.2 GHz Op-
terons
connected via a Gigabit network and took about 3 months.

We started sieving shortly before Christmas 2003 and continued
until
October 2004. The matrix step began in December 2004.
Line sieving was done by P. Montgomery and H. te Riele at the
CWI, by
F. Bahr and his family.

More details will be given later.
```

F. Bahr, M. Boehm, J. Franke, T. Kleinjung

# 9. Verwendete Literatur

## Rahmenlehrplan und Schulgesetz

**Senatsverwaltung für Bildung, Jugend und Sport Berlin.**
„Rahmenlehrplan für die gymnasiale Oberstufe. Informatik." Berlin, 2006.
„Handreichungen zum Berliner Rahmenlehrplan Sek. II für Informatik." Berlin, 2005.
**Senatsverwaltung für Bildung, Wissenschaft und Forschung Berlin.**
„Schulgesetz für das Land Berlin (26. Januar 2004)." Berlin: 2007.

## Didaktik

**Barzel**, Bärbel; Büchter, Andreas: Leuders, Timo. *Mathematik Methodik. Handbuch für die Sekundarstufe I und II.* Berlin: Cornelsen, 2007.
**Gudjons,** Herbert. *Handlungsorientiert Lehren und Lernen. Schüleraktivierung, Selbsttätigkeit, Projektarbeit.* 4. Auflage. Bad Heilbrunn: Klinkhardt, 1994.
**Gudjons,** Herbert. *Pädagogisches Grundwissen.* 2. Auflage Bad Heilbrunn: Klinkhardt, 1994.
**Herold**, Martin; Landherr, Birgit. *SOL. Selbstorganisiertes Lernen. Ein systemischer Ansatz für den Unterricht*. 2. Auflage. Baltmannsweiler: Schneider-Verlag Hohengehren, 2003.
**Hubwieser**, Peter. *Didaktik der Informatik.* 3. Auflage. Berlin: Springer, 2007
**Humbert**, Ludger. *Didaktik der Informatik*. 2. Auflage. Wiesbaden: Teubner, 2006.
**Ministerium für Kultus, Jugend und Sport Baden-Württemberg** (Hg.). Broschüre **„**SOL. Selbst organisiertes Lernen.", 2003.
**Schubert**, Sigrid; Schwill, Andreas. *Didaktik der Informatik*. 1. Auflage. Heidelberg: Spektrum, 2004.

## Computersicherheit und Kryptologie

**Bauer**, Friedrich L. *Entzifferte Geheimnisse. Codes und Chiffren und wie sie gebrochen werden.* Berlin/Heidelberg: Springer, 1995
**Eckert**, Claudia. *IT-Sicherheit. Konzepte – Verfahren – Protokolle*. 4. Auflage. München: Oldenbourg Wissenschaftsverlag, 2003.
**Engelmann**, Lutz (Hg.). *Lehrbuch Informatik. Gymnasiale Oberstufe*. Berlin: Duden, 2006. Kapitel Datenschutz und Datensicherheit, S. 96–104.
**Gallenbacher**, Jens *Abenteuer Informatik*. *IT zum Anfassen. Von Routenplaner bis Online-Banking.* Heidelberg: Spektrum, 2007.
**Poe**, Edgar Allan. *The Gold-Bug and Other Tales*. Stuttgart: Reclam, 1984.
**Schneier**, Bruce. *Secrets and Lies. IT-Sicherheit in einer vernetzten Welt*. Heidelberg: Dpunkt-Verlag, 2000.
**Sgarro**, Andrea; Würmli, Markus. *Geheimschriften. Verschlüsseln und Enträtseln von Geheimtexten*. Augsburg: Weltbild Verlag, 1991.
**Singh**, Simon. *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* 3. Auflage. München: Dtv, 2002.

**Witten**, Helmut; Irmgard Letzner und Ralph-Hardo Schulz: „RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle."
Teil I: Sprache und Statistik. LogIn 18 (1998) Heft 3/4, S. 57–65.
Teil II: Von Caesar über Vigenère zu Friedman. LogIn 18 (1998) Heft 5, S. 31–39.
Teil III: Flußchiffren, perfekte Sicherheit und Zufall per Computer. LogIn 19 (1999) Heft 2, S. 50–57.
**Witten**, Helmut; Ralph-Hardo Schulz: „RSA & Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. Neue Folge."
Teil 1: RSA für Einsteiger. LogIn 140 (2006) S.45–54.
Teil 2: RSA für große Zahlen. LogIn 143 (2006) S. 50-58.

## Sonstiges

**Duden Band 7.** Das Herkunftswörterbuch. 3. Auflage. Mannheim: Dudenverlag, 2001.

### Internet-Quellen

(Die URLs wurden am 19. März 2008 überprüft.)

**Aronson**, Elliot: The Jigsaw Classroom. http://www.jigsaw.org/
**Bundesamt für Sicherheit in der Informationstechnik** BSI. Broschüre**:** „Sicherheit durch Verschlüsselung". http://www.bsi.bund.de/literat/faltbl/F27Verschluesselung.htm
**Chemnitzer Schulmodell**. http://www.schulmodell.de/info/unterricht/kl10/alberti.htm
**Deutschsprachige Wikipedia**:
Johann Heinrich Pestalozzi.
http://de.wikipedia.org/wiki/Johann_Heinrich_Pestalozzi
Kerckhoffs' Prinzip.
http://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip
RSA Factoring Challenge.
http://de.wikipedia.org/wiki/RSA_Factoring_Challenge
**Esslinger**, Bernhard. CrypTool. http://www.cryptool.de/
**Esslinger**, Bernhard; Hoelzner, Kai. „CrypTool. Ein E-Learning Programm zur Kryptologie." In: Deutsches Forschungsnetz. http://www.dfn.de/presse-information/ dfnmitteilungen/
**Extreme Programming**. http://www.extremeprogramming.org/rules/pair.html
**Herold**, Martin. Lehrerfortbildung. Internet: http://sol-mlf.lehrerfortbildung-bw.de