Schriftliche Ausarbeitung

einer Unterrichtsreihe zum Thema

Kryptologie

HUMBOLDT-UNIVERSITÄT ZU BERLIN

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT

INSTITUT FÜR INFORMATIK

Seminar: Ausgewählte Kapitel der Didaktik der Informatik

Sommersemester 2015

Dozent: Dr. Nguyen-Thinh Le

Verfasserin: Mina Ghomi

Inhaltsverzeichnis

1. Einleitung 1

2. Bedingungsanalyse 2

2.1 Lernvoraussetzungen der Schüler 2

2.2 Einordnung der Stunden in die Unterrichtseinheit 4

2.3 Lehrvoraussetzungen der Lehrperson 7

3. Lernziele 10

3.1 Hauptziel der Unterrichtsreihe 10

3.2 Hauptziel und Teilziele der Unterrichtsstunden 10

4. Didaktische Strukturierung 13

5. Ausführliche Stundenentwürfe 37

5.1 Codierung und Steganographie 37

5.1.1 Alle Materialien der Station: Morsealphabet 39

5.1.2 Alle Materialien der Station: Braille-Schrift 43

5.1.3 Alle Materialien der Station: Winkeralphabet 47

5.1.4 Alle Materialien der Station: Semagramme 49

5.1.5 Alle Materialien der Station: Punktchiffren 53

5.1.6 Alle Materialien der Station: Musikalische Botschaften 58

5.1.7 Alle Materialien der Station: Computerbasierte Steganographie 62

5.2 Kryptographie: Transposition und monoalphabetische Substitution 64

5.2.1 Arbeitsblätter für das Thema Caesar-Chiffre 65

5.2.2 Arbeitsblätter für das Thema Freimaurer 70

5.2.3 Arbeitsblätter für das Thema Pflügen 73

5.2.4 Arbeitsblätter zum Thema Schablonen 76

5.2.5 Test 81

5.3 Kryptoanalyse 83

5.3.1 Arbeitsblatt für das Thema Kryptoanalyse 84

5.4 Kryptographie: Polyalphabetische Substitution 87

5.4.1 Arbeitsblätter für die Vigenère-Verschlüsselung 89

6. Abbildungsverzeichnis 95

7. Tabellenverzeichnis 96

8. Literaturverzeichnis 97

1. Einleitung

Im Seminar „Ausgewählte Kapitel der Didaktik der Informatik“ des Lehramtsmasters für Informatik habe ich zum Unterrichtsthema Kryptologie eine Unterrichtsreihe konzipiert, welche im Folgenden ausführlich beschrieben und didaktisch begründet wird.

In der Bedingungsanalyse werden, gemäß Hilbert Meyer, die für diese Unterrichtseinheit wesentlichen Einflussfaktoren erfasst und didaktisch bewertet. Anschließend werden im 3. Kapitel die angestrebten Lernziele der Unterrichtsreihe und der einzelnen Unterrichtsstunden formuliert.

Im 4. Kapitel folgt die didaktische Strukturierung, welche sowohl die Sachanalyse, die didaktische Analyse, als auch die methodische Analyse der Unterrichtsstunden integriert. Abschließend werden die ausführlichen Stundenentwürfe und Arbeitsblätter dargelegt.

2. Bedingungsanalyse

Bei der Analyse wird, auf Empfehlung von H. Meyer[1], eine Unterscheidung in vier Bedingungsfeldern vorgenommen. In Kapitel 2.1 werden die für die Unterrichtsreihe nötigen Lernvoraussetzungen der Schüler dargelegt. Kapitel 2.2 befasst sich mit der Einordnung der Stunden in die Unterrichtseinheit und fasst die Richtlinien- und Fachvorgaben zusammen, bevor dann im dritten Feld die Lehrvoraussetzungen der Lehrperson thematisiert werden. Die institutionellen Rahmenbedingungen, die von der Schule selbst auf den Unterricht einwirken, werden als viertes Feld im Laufe der Beleuchtung der drei anderen Felder ebenfalls dabei dargestellt.

2.1 Lernvoraussetzungen der Schüler

Diese Unterrichtsreihe besteht aus insgesamt sechs Unterrichtsblöcken von je 90 Minuten und dient zur erstmaligen Einführung in die Kryptologie, wobei verwandte Themen wie die Codierung und die Steganographie ebenfalls behandelt werden und somit keine fachlichen Inhalte bekannt sein sollten. Die aufeinander aufbauenden Unterrichtsblöcke sind für Schüler einer beliebigen Klassenstufe der Sekundarstufe I konzipiert, welche noch keine Vorkenntnisse über steganographische, kryptographische oder kryptoanalytische Verfahren haben.

Neben neuen Inhalten vermitteln die sechs Unterrichtblöcke den Schülern auch gezielt Methoden- und Sozialkompetenzen. „Soziale Kompetenz bezeichnet den Komplex all der persönlichen Fähigkeiten und Einstellungen, die dazu beitragen, das eigene Verhalten von einer individuellen auf eine gemeinschaftliche Handlungsorientierung hin auszurichten. Sozial kompetentes Verhalten verknüpft die individuellen Handlungsziele von Personen mit den Einstellungen und Werten einer Gruppe.“[2] Durch den abwechslungsreichen Einsatz verschiedener, meist kooperativer und kollaborativer, Unterrichtsmethoden werden

---

[1] MEYER: *Leitfaden Unterrichtsvorbereitung*, Seite 130.

[2] RIPPLINGER: *Lernziel Sozialkompetenz,* Seite 2.

vor allem die Teamfähigkeit, Kommunikationsfähigkeit und Konfliktfähigkeit der Schüler gefördert.

Angelehnt an Hilbert Meyers „pragmatischen Kompetenzstufenmodells“[3] und den Konstruktionsregeln wird in der nachfolgenden Tabelle ein Kompetenzstufenmodell für die Unterrichtsreihe dargelegt, nach welchem man die Leistungen der einzelnen Schüler einordnen kann. Alle Schüler befinden sich hierbei mindestens auf Stufe 1.

Stufe	**Kompetenzdimensionen**
1	Die Schüler können Informationen naiv verstecken oder verheimlichen.[4]
2	Die Schüler können Codierungen z.B. mithilfe des Morsealphabets nachvollziehen und nach Vorgabe ausführen.
3	Die Schüler können (auch codierte) Nachrichten in Bildern und Schriften verstecken, entdecken und ver- bzw. entschlüsseln.
4	Die Schüler können die Vorgehensweise von Transpositionsverfahren, monoalphabetischen und polyalphabetischen Substitutionsverfahren erläutern und ausgewählte Verfahren zur Ver- bzw. Entschlüsselung von Informationen anwenden.
5	Die Schüler können einen gegebenen Geheimtext, welcher mit Transpositions- oder monoalphabetischen Substitutionsverfahren verschlüsselt wurde, bei einer „Known Ciphertext Attack“ knacken.

Tabelle 1: Kompetenzstufenmodell für die Leistungen der Schüler

Die „Kompetenzstufen können je nach Komplexität des Inhalts, nach Alter und Leistungsvermögen der Schülerinnen und Schüler auf unterschiedlichen Entfaltungsniveaus

[3] MEYER: *Leitfaden Unterrichtsvorbereitung*, Seite 157.

[4] Oftmals lernen die Schüler bereits in der Grundschule aus eigenem Antrieb mit „unsichtbarer Tinte“ (z.B. mithilfe von Zitronensaft) zu schreiben oder die „Löffelsprache“ zu sprechen, welche eine Geheim- bzw. Spielsprache ist und auf dem Austausch der Vokale eines Wortes durch festgelegte Kürzel beruht. Um die Sprache zu entschlüsseln, zu lernen bzw. zu sprechen müssen die festgelegten Kürzel bekannt sein.

entwickelt werden. Der Aspekt zunehmender Selbstständigkeit im Denken und Handeln der Schüler wird über die Stufenfolge definiert."[5]

2.2 Einordnung der Stunden in die Unterrichtseinheit

Jede Unterrichtsstunde wird in dem Dreischritt „Einstieg, Erarbeitung und Ergebnissicherung" gegliedert, welcher von Hilbert Meyer als „methodischer Grundrhythmus des Unterrichts"[6] bezeichnet wird.

1. Schritt: In der *Einstiegsphase* muss die Lehrerin/der Lehrer dafür sorgen, dass eine gemeinsame Orientierungsgrundlage für den zu erarbeitenden Sach-, Sinn- oder Problemgegenstand hergestellt wird. Dies legt oft, aber nicht immer eine führende Rolle des Lehrers nahe. **2. Schritt:** In der *Erarbeitungsphase* sollen sich die Schülerinnen und Schülerin den Sach-, Sinn- oder Problemzusammenhang einarbeiten. Dies ist ohne ein hohes Maß an Eigentätigkeit nicht zu schaffen. Sie erhalten deshalb eine führende Rolle. **3. Schritt:** In der *Phase der Ergebnissicherung* sollen sich die Lehrerin/der Lehrer und die Schülerinnen und Schüler darüber verständigen, was bei der Unterrichtsarbeit herausgekommen ist und wie die Arbeit in der nächsten Stunde weitergehen kann. Darüber hinaus sollen die neu erworbenen Kenntnisse und Fähigkeiten geübt und gegebenenfalls angewandt werden. Dies legt eine gemeinsame Unterrichtsführung durch Lehrer sowie Schülerinnen und Schüler nahe.

Tabelle 2: Methodischer Grundrhythmus des Unterrichts von Hilbert Meyer

In dieser Unterrichtseinheit werden besonders drei methodische Grundformen des Unterrichts[7] verstärkt eingesetzt. Zum einen wird der lehrgangsförmige Unterricht eingesetzt, welcher „gut geeignet ist, um Sach-, Sinn- und Problemzusammenhänge aus der Sicht des Lehrenden zu vermitteln und dadurch Sach- und Fachkompetenz der Schüler aufzubauen"[8]. Dabei ist der Einbau kurzer Phasen selbstregulierten Lernens - z.B. in Form von Tandem- und Einzelarbeit - möglich. Zum anderen wird der individualisierende

---

[5] MEYER: *Einführung in die Arbeit mit unterrichtsmethodischen Kompetenzstufenmodellen,* Seite 6.

[6] MEYER: *Unterrichtsmethoden,* Seite 7.

[7] Hilbert Meyer definiert die drei Ebenen Mikro-, Meso- und Makromethodik, welche die Methodenvielfalt in drei Dimensionen einordnet. Die Makromethodik erfasst die institutionell fest verankerten methodischen Großformen: Freiarbeit, Lehrgänge, Projektarbeit und gemeinsamer Unterricht. Nachzulesen ist dieses Modell in MEYER: *Was ist guter Unterricht?,* Seite 74 ff.

[8] MEYER: *Was ist guter Unterricht?*, Seite 79.

Unterricht eingesetzt, welcher für selbst organisiertes Lernen steht und besonders geeignet ist, um individuelle Lernschwerpunkte herauszubilden und Methodenkompetenzen aufzubauen. Mit einem hohen Anteil an Gruppenarbeit wird auch die dritte Grundform, der sogenannte kooperative Unterricht, in die Unterrichtseinheit integriert. Typische Lehrer- und Schülertätigkeiten sind das gemeinsame Planen von kleinen Vorhaben und großen Projekten, die Arbeit an diesen Vorhaben in Kleingruppen, die Präsentation der Arbeitsergebnisse und die gemeinsame Reflexion und Kontrolle des Erreichten.[9]

Im Folgenden werden die Themen der Unterrichtsblöcke und die jeweils den einzelnen Unterrichtsphasen zugeordneten Methoden tabellarisch dargestellt.

Unterrichts-block	**Thema**	**Unterrichtsmethoden**
1. und 2. Block	Codierung und Steganographie	**Einstieg**: Brainstorming **Erarbeitung**: Doppelzirkel **Ergebnissicherung:** Schülerpräsentationen
3. Block	Transposition und monoalphabetische Substitution	**Einstieg**: Lehrervortrag **Erarbeitung**: Gruppen-Puzzle **Ergebnissicherung**: Test
4. Block	Kryptoanalyse	**Einstieg**: Lehrervortrag und fragend-entwickelnder U. **Erarbeitung**: Wettbewerb **Ergebnissicherung**: Schülerpräsentationen
5. und 6. Block	Polyalphabetische Substitution	**Einstieg**: Filmeinsatz **Erarbeitung 1**: Kugellager-Methode **Ergebnissicherung 1**: Lehrer-Schüler-Gespräch im Plenum **Erarbeitung 2**: Partnerarbeit **Ergebnissicherung 2**: Lehrer-Schüler-

[9] KÖLLER & MEYER: *Was ist eine gute Lehrerin/ein guter Lehrer?*, Seite 11.

		Gespräch im Plenum **Erarbeitung 3:** Einzelarbeit **Ergebnissicherung 3:** Schüler-Schüler-Gespräch im Plenum **Ergebnissicherung 4:** Redekette

Tabelle 3: Überblick über die Themen und Methoden der Unterrichtsreihe

Im aktuellen Berliner Rahmenlehrplan der Sekundarstufe I für Informatik gibt es keine explizite Nennung der Begriffe „Steganographie", „Kryptologie" oder „Verschlüsselung". Einzig im thematischen Modul „ITG4 Leben mit vernetzten Systemen" wird folgende Kompetenz genannt, welche entfernt auf Verschlüsselungsverfahren hindeutet: „Die Schülerinnen und Schüler kennen Formen des bargeldlosen Bezahlens in Geschäften und im Netz und entwickeln eine begründete Einschätzung der Sicherheit der verschiedenen Verfahren"[10]

Betrachtet man dagegen den Informatik-Lehrplan der Sekundarstufe I des Bundeslandes Rheinland-Pfalz, so wird explizit im Inhaltsbereich „Grundlagen der Informationsverarbeitung", welcher sich gezielt mit der Darstellung von Informationen in Form von Daten und mit Informatiksystemen zur Verarbeitung von Daten auseinandersetzt, die Verschlüsselung von Daten als verbindlicher Inhalt genannt.

Dabei werden auch, wie in der nachfolgenden Tabelle zu sehen ist, die Konzepte des Senders, Empfängers, der Nachricht und des Protokolls in Kommunikationsvorgängen (z.B. beim Codieren durch das Morsealphabet) behandelt. Die Entwicklung von Verschlüsselungsverfahren als Problemlösung für Sicherheitsprobleme wird hierbei als Hinweis nahegelegt.

[10] Berliner Rahmenlehrplan der Sekundarstufe I, 1. Auflage 2006, Seite 23.

Grundlagen der Kommunikation in Rechnernetzen beschreiben (optional im Wahlfach)	
Verbindliche Inhalte	**Hinweise für eine mögliche Umsetzung**
Sender, Empfänger, Nachricht, Protokoll	➢ Einfache Kommunikationsvorgänge experimentell durchführen (z.B. Morsen, Lichtsignale, Handzeichen) und dabei die Konzepte „Sender", „Empfänger", „Nachricht" und „Protokoll" erarbeiten ➢ Protokolle als Summe aller Vereinbarungen zwischen Sender und Empfänger zur Abwicklung von Kommunikationsvorgängen beschreiben ➢ Historische Verfahren (z.B. optische Telegrafie) und Kommunikationsvorgänge aus dem Alltag (z.B. Telefonieren, Briefversand) mit Hilfe der Konzepte beschreiben
Kommunikationsvorgänge im Internet	➢ Kommunikationsvorgänge des Internets simulieren (z.B. durch Rollenspiele) und dabei ein erstes Verständnis für Client-Server-Struktur, Authentifizierung, paketorientierte Datenübertragung und Routing entwickeln
Datensicherheit im Internet	➢ Sicherheitsprobleme bei Kommunikationsvorgängen aufzeigen (z.B. durch einsehbare Nachrichten bei den oben erwähnten Rollenspielen) ➢ Die Gefahren, die hiervon ausgehen, diskutieren
Verschlüsselung von Daten	➢ Erste Ansätze zur Lösung von Sicherheitsproblemen anhand einfacher (monoalphabetischer) Verschlüsselungsverfahren entwickeln

Tabelle 4: Auszug aus dem Lehrplan Informatik der Sekundarstufe I in Rheinland-Pfalz[11]

2.3 Lehrvoraussetzungen der Lehrperson

Laut Hilbert Meyer sind Lehrvoraussetzungen die geistigen, körperlichen und materiellen Grundlagen des zielorientierten, effektiven und ethisch akzeptablen Lehrerhandelns im Unterricht. Die Medienausstattung eines Klassenraumes nennt er als ein Beispiel für die materiellen Grundlagen, die personenbezogenen Anteile hingegen definiert H. Meyer als Lehrkompetenz: „Lehrkompetenz bezeichnet die durch Erfahrung und Lernen erworbene Fähigkeit eines Lehrers, in immer wieder neuen, nicht genau planbaren

[11] Lehrplan Informatik an Gymnasien und Integrierten Gesamtschulen in Rheinland-Pfalz, Seite 17.

Unterrichtssituationen kreativ, situationsangemessen und auf der Grundlage eines mit den Kollegen geteilten Berufsethos zu arbeiten.“ [12]

Bezogen auf diese Unterrichtsreihe ist ein umfangreiches Fachwissen zur Codierung, Steganographie, Kryptographie und Kryptoanalyse notwendig, wobei die moderne Kryptologie vorerst nicht behandelt wird. Es gibt zahlreiche Quellen, sowohl Bücher als auch Internetseiten[13]. In der folgenden Tabelle werden vier Internetseiten mit Materialien für den Unterrichtseinsatz empfohlen.

Internetseite	**Inhalte**
https://www.cryptoportal.org/	• Unterrichtsmaterial und Linksammlungen (vor allem für die Sekundarstufe II),
http://ddi.uni-wuppertal.de/material/spioncamp.html	• Unterrichtsmaterialien zur Codierung, Steganographie sowie Kryptographie mit Arbeitsblättern, Lösungen und Vorlagen zum Ausdrucken, welche fürs Stationenlernen ausgelegt sind.
http://www.cryptool-online.org/	• Verschlüsselungs- und Analysetools direkt im Browser, • Erläuterung zu vielen verschiedenen Verschlüsselungsverfahren, Codierungen und zur Kryptoanalyse
http://www.austromath.at/medienvielfalt/materialien/krypto/lernpfad/	• Lernpfad zur asymmetrischen Verschlüsselung mit Anwendungen z.B. zur RSA-Verschlüsselung

Tabelle 5: Empfohlene Internetseiten mit Unterrichtsmaterialien

Die Methodenvielfalt dieser geplanten Unterrichteinheit zur Kryptologie setzt sich zusammen aus dem genutzten Reichtum der Inszenierungstechniken (z.B. Impuls geben, provozieren, zeigen, verlangsamen), der Vielfalt an Handlungsmustern und der variabel gestalteten Verlaufsform des Unterrichts (siehe Tabelle 3: Überblick über die Themen und Methoden der Unterrichtsreihe). Hinzu kommt das ausbalancierte Auftreten der

[12] MEYER: *Leitfaden Unterrichtsvorbereitung*, Seite 162.

[13] Bitte schauen Sie für explizite Quellen auch ins Literaturverzeichnis.

Grundformen des Unterrichts, wobei jede Grundform eine andere Lehrerrolle nahelegt, welche als Lehrvoraussetzung entsprechend angenommen werden sollte. Beispielsweise dominiert die traditionelle Rolle des Lehrers beim lehrgangsförmigen Unterricht mit einem hohen Ausmaß an Lehrerlenkung. Typische Lehrertätigkeiten sind das Vortragen, das Zeigen, Erläutern und Fragenstellen. Im individualisierenden Unterricht ist der Lehrer verantwortlich für die pädagogisch gestaltete, anregungsreiche Lernumgebung. Er ist der Mentor im Hintergrund, der beobachtet und nur eingreift, wenn die Selbstorganisation des Lernens nicht funktioniert. Er achtet auf die gruppendynamischen Prozesse und das soziale Miteinander.[14] Im kooperativen Unterricht übernimmt der Lehrer meist die Rolle des Moderators. Er hilft bei der Planung, warnt vor überzogenen Hoffnungen und sorgt für die Leistungskontrollen.

[14] MEYER: Unterrichtsmethoden, Seite 8.

3. Lernziele

3.1 Hauptziel der Unterrichtsreihe

Die Schüler sollen die Teilgebiete Kryptographie und Kryptoanalyse der Kryptologie, sowie die Codierung und die Steganographie als verschiedene Wissenschaften definieren können und ausgewählte Verfahren anwenden oder zumindest erläutern können.

Die Schüler sollen Methoden- und Sozialkompetenzen aufbauen und in Zusammenarbeit mit anderen ihre Kommunikationsformen, ihr Einfühlungsvermögen und ihre Problemlösestrategien erweitern.

3.2 Hauptziel und Teilziele der Unterrichtsstunden

1. Unterrichtsthema: Codierung und Steganographie

Hauptziel	Die Schüler sollen mindestens zwei Codierungsarten und zwei steganographische Verfahren anwenden können.
Teilziele	Die Schüler sollen ... • sich in Morsezeichen verständigen können. • Nachrichten, welche in der Braille-Schrift verfasst wurden, lesen können. • Nachrichten in der Braille-Schrift verfassen können. • sich über das Winkeralphabet verständigen können. • den Unterschied zwischen Codierung und Steganographie nennen können. • Semagramme erstellen können. • das Verfahren der Punktchiffren erläutern und anwenden können. • einen gegebenen Musik-Code anwenden können. • eine Methode der computerbasierten Steganographie anwenden können. • Arbeitsschritte und Ziele bestimmen und koordinieren können.

Tabelle 6: Haupt- und Teilziele des 1. und 2. Unterrichtsblocks

2. Unterrichtsthema: Transposition und monoalphabetische Substitution

Hauptziel	Die Schüler sollen mithilfe von zwei Transpositionsverfahren und zwei monoalphabetischen Substitutionsverfahren Nachrichten chiffrieren und dechiffrieren können.
Teilziele	Die Schüler sollen ... • beschreiben können, wie man mit der Skytale verschlüsseln kann. • das Schablonen-Verfahren lehren und zur Verschlüsselung und Entschlüsselung von Nachrichten anwenden können. • das Pflügen-Verfahren beschreiben und zum Ver- und Entschlüsseln von Nachrichten anwenden können. • die Freimaurer Substitution erläutern und für die Ver- und Entschlüsselung von Nachrichten anwenden können. • die Caesar-Chiffre lehren und zum Ver- und Entschlüsseln von Nachrichten anwenden können. • den Unterschied zwischen Transpositions- und Substitutionsverfahren erläutern können. • respektvoll mit anderen Personen umgehen können. • sich ausdrücken, Fragen stellen und aktiv zuhören können. • neu erworbenes Wissen in Handeln und Kommunikation widerspiegeln können.

Tabelle 7: Haupt- und Teilziele des 3. Unterrichtsblocks

3. Unterrichtsthema: Kryptoanalyse

Hauptziel	Die Schüler sollen Kerckhoffs Prinzip erläutern, verschiedene Typen von Attacken der Kryptoanalytiker unterscheiden und zwei Verfahren zum Knacken von monoalphabetischen Substitutionsverfahren anwenden können.
Teilziele	Die Schüler sollen ... • Kerckhoffs Prinzip nennen können. • verschiedene Voraussetzungen, denen Kryptoanalytiker ausgesetzt sein können, aufzählen können • das Pflügen-Verfahren knacken können. • das Caesar-Verfahren durch das Ausprobieren aller möglichen Schlüssel knacken können.

	• das Caesar-Verfahren mithilfe der Häufigkeitsanalyse knacken können. • systematisch und zielgerichtet vorgehen können. • den Zeitrahmen bei der Planung und Durchführung von Aufgaben berücksichtigen können • die Vorgehensweisen und Methoden auf ihre Effektivität hin prüfen können.

Tabelle 8: Haupt- und Teilziele des 4. Unterrichtsblocks

4. Unterrichtsthema: Polyalphabetische Substitution

Hauptziel	Die Schüler sollen zwei polyalphabetische Substitutionsverfahren beschreiben können und das Vigenère-Verfahren anwenden können.
Teilziele	Die Schüler sollen ... • die Funktionsweise der ENIGMA erläutern können. • die Idee hinter der Turing Bombe von Alan Turing beschreiben können. • das Vigenère-Verfahren erläutern und zur Verschlüsselung und Entschlüsselung von Nachrichten anwenden können. • Informationsquellen erschließen können. • Medienangaben auch kritisch betrachten können. • verständlich reden können. • Rückmeldungen geben können. • Prioritäten setzen können.

Tabelle 9: Haupt- und Teilziele des 5. und 6. Unterrichtsblocks

4. Didaktische Strukturierung

Die Kryptologie wird laut Duden definiert als ein „Teilgebiet der Informatik, das sich mit der Lehre von der Entwicklung und der Bewertung von Verfahren zur Verschlüsselung von Daten im Rahmen des Datenschutzes befasst.“[15] Das Wort „kryptós“ stammt aus dem Griechischen und bedeutet „geheim“ bzw. „verborgen“. Die Kryptologie beinhaltet sowohl die Kryptographie, welche die Wissenschaft der Verschlüsselung von Informationen ist, als auch die Kryptoanalyse, welche die Wissenschaft der Entschlüsselung ohne Kenntnis des Schlüssels ist.

Die Schüler haben unterschiedliches Vorwissen und Assoziationen zur Kryptologie, daher eignet sich die Brainstorming-Methode als Einstieg in die erste Unterrichtsstunde der Unterrichtsreihe zur Kryptologie besonders gut. Dabei gibt der Lehrer einen Begriff, ein Thema oder eine Frage vor und lässt die Schüler sich innerhalb einer vorgegebenen Zeit dazu äußern. Die an die Tafel geschriebenen oder an die Pinnwand gehefteten Äußerungen werden weder bewertet, noch kommentiert, noch kritisiert.[16]

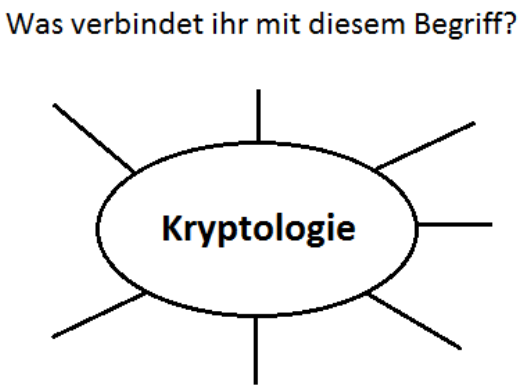


Abbildung 1: Tafelbild für die Einstiegsmethode Brainstorming

Die Methode aktiviert und fördert die Lernmotivation und verbindet die neuen Lerngegenstände mit bereits Bekanntem. Nach dem Einsatz der Methode sollte man sich

---

[15] http://www.duden.de/rechtschreibung/Kryptologie [Zugriffsdatum: 10.07.2015]

[16] MATTE*: Methoden für den Unterricht*, Seite 18.

auf die genannten Dinge verständigen, die im Unterricht weiterverfolgt werden sollen.[17] Beispielsweise kann im Anschluss die zukünftig verwendete Terminologie eingeführt werden. Mit „Klartext“ bezeichnet man die zu schützende Nachricht, mit „Geheimtext“ die verschlüsselte Nachricht und den Ver- bzw. Entschlüsselungsvorgang bezeichnet man auch als Chiffrieren bzw. Dechiffrieren. Einen weiteren unabhängigen und häufig mit der Kryptographie kombinierten Bereich bildet die Steganographie.

Die Steganographie bezeichnet die Wissenschaft des Versteckens von Informationen. Dabei wird die Existenz der Botschaft verheimlicht. Das Wort stammt ebenfalls aus dem Griechischen und bedeutet „verdecktes Schreiben“.

Ein steganographisches Verfahren ist beispielsweise die Punktchiffre. Klaus Schmeh beschreibt in seinem Buch „Versteckte Botschaften“ unter anderem die gebräuchlichste Form der Punktchiffre: „Man nehme ein Achsenkreuz und trage auf der y-Achse die Buchstaben von A bis Z ab. Auf der x-Achse werden die Zahlen 1, 2, 3 usw. abgetragen. Ist der erste Buchstabe des zu verschlüsselnden Texts ein S, dann zeichnet man an der Koordinate (1,S) einen Punkt. Ist der zweite Buchstabe ein T, dann folgt ein zweiter Punkt bei (2,T). Eine Punktchiffre lässt sich leicht tarnen. Beispielsweise kann der Absender die korrekte Beschriftung der x- und y-Achse weglassen und die Punkte stattdessen als Aktienkurse oder Temperaturverläufe deklarieren. Bettet man ein solches Diagramm in einen dazu passenden Text ein, dann wird kaum jemand Verdacht schöpfen. Der Text in Abbildung 2, den vermeintlich ein Enkel an seine Oma geschrieben hat, ist unerheblich. Die eigentliche Nachricht ist mit Hilfe der Bienen als Punktchiffre kodiert. Nimmt man die unter dem Bild abgetragene Buchstabenfolge als x-Achse, dann ergibt sich daraus folgende Nachricht: RENSEIGNEMENTS ARRIVENT. Das heißt: »Auskünfte kommen.«“[18]

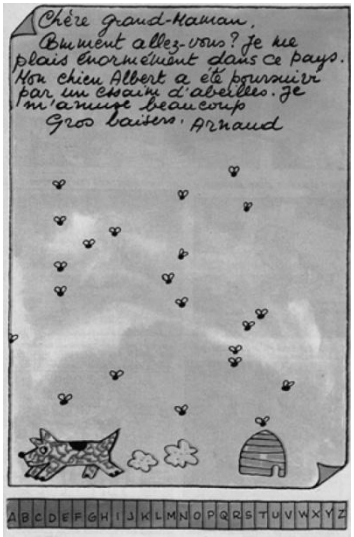


Abbildung 2: Punktchiffre in einem Kinderbrief

[17] MATTE: Methoden für den Unterricht, Seite 18.

[18] SCHMEH: *Verstecke Botschaften,* Seite 23-25.

Klaus Schmeh beschreibt in diesem Buch ebenfalls, wie verschiedene Komponisten wie beispielsweise Johann Sebastian Bach und Robert Schumann geheime Botschaften in ihren Kompositionen durch Noten einbetteten. „Den einflussreichsten Musik-Code veröffentlichte um das Jahr 1563 der Italiener Giovanni della Porta (1535–1615) in seinem Buch „De furtivis literarum notis“. Er legte elf Töne fest, die es in jeweils zwei Werten gab.“[19]

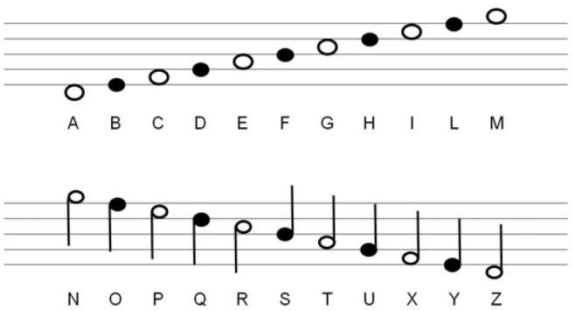


Abbildung 3: Musik-Code von Giovanni della Porta

Im Unterricht können die Schüler nach dem Lesen des dreiseitigen Buchausschnitts von Klaus Schmeh handelnd aktiv werden, indem sie selber ihre Namen in Tonfolgen notieren und spielen. Sollte es nicht möglich sein ein Keyboard mit Kopfhörern im Klassenraum zu platzieren, so kann man heutzutage auch kostenlose Piano-Apps[20] auf Tablets, Laptops oder Smartphones verwenden, um eine einhändige Abfolge von Noten zu spielen.

„Eine besondere Spielart der Steganographie ist das Akrostichon. Dabei muss man in einem Text jeweils nur den ersten Buchstaben jedes Wortes (oder eines jeden Satzes bzw. Absatzes) lesen, um die geheime Nachricht zu finden. Akrostichons wurden eher als ein Spiel, denn als echte Geheimhaltungsmaßnahme angesehen.“[21] Versteckt man die geheime Botschaft in Bildern oder in Schriften, so nennt man diese Semagramme. Der folgende Satz stellt ein Beispiel für ein Semagramm in einer unverfänglichen Nachricht dar:

Alle Studenten lernen wenig, aber sie haben dennoch Erfolg.

Man benötigt den folgenden Schlüssel 141241153, um die versteckte Nachricht lesen zu können. Markiert man nun nacheinander und in jedem Wort den Buchstaben an der jeweiligen, vom Schlüssel angegebenen Position, so erhält man folgendes Wort:

Alle Stu**d**enten **l**ernen w**e**nig, abe**r** **s**ie **h**aben denn**o**ch Er**f**olg → ADLERSHOF.

---

[19] SCHMEH: *Versteckte Botschaften*, Seite 28.

[20] Beispielsweise die App „Piano 10“.

[21] KLEIN: *Visuelle Kryptographie,* Seite 86.

Abbildung 4: Semagramm von US-Zensoren in San Antonio[22]

Die Abbildung 4 stellt ein Semagramm dar, welches zu Übungszwecken von US-Zensoren angefertigt wurde. In der Zeichnung wurde eine Morse-Nachricht in Form von Grashalmen entlang des Flussufers eingebettet. Ein langer Grashalm steht für einen Strich und ein kurzer Halm für einen Punkt. „Setzt man die Buchstaben zusammen und ergänzt an den richtigen Stellen Zwischenräume, dann entsteht folgende Nachricht: COMPLIMENTS OF CPSA MA TO OUR CHIEF COL HAROLD R SHAW ON HIS VISIT TO SAN ANTONIO MAY 11TH 1945.“[23]

Bevor man Schüler auffordern kann, verschiedene Morse-Nachrichten aus Semagrammen zu lesen, muss man die Codierung durch das Morsealphabet einführen. Der amerikanische Maler und Erfinder Samuel Morse entwickelte 1832 einen Schreibtelegraphen, mit dessen Hilfe man über Telegraphenmasten und Leitungen kurze und lange elektrische Impulse

---

[22] SCHMEH: *Versteckte Botschaften,* Seite 21.

[23] SCHMEH: Versteckte Botschaften, Seite 21.

übertragen konnte. Das daraufhin von ihm erfundene Morsealphabet ordnet jedem Buchstaben und jeder Zahl eine Kombination aus kurzen und langen Zeichen zu.

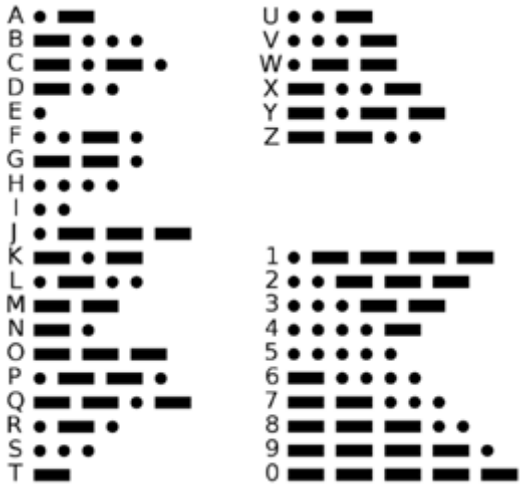


Abbildung 5: Morsealphabet

Im Gegensatz zur Steganographie möchte man bei der Codierung von Nachrichten nichts verstecken, denn Codierungen sind öffentlich. „Die Buchstaben bleiben wo sie sind, aber nicht was sie sind. Jeder kann nachschlagen, was sie bedeuten!“[24]

Eine weitere bekannte Codierung stellt die Braille-Schrift dar, welche von Blinden oder stark Sehbehinderten genutzt wird und daher auch Blindenschrift genannt wird.[25] Der in seiner frühen Kindheit erblindete Franzose Louis Braille erfand in seiner Jugend um 1825 diese Schrift und eröffnete blinden Menschen mit einem Schlag den Zugang zu Bildung und Wissen.[26] Bei der praktischen Durchführung des Schreibens wird eine ‘Schreibtafel’ verwendet, „eine Platte mit einem Raster von Löchern und ein darüber liegendes, aufklappbares Gitter, das den Blindenschriftzeilen angepasst ist. Nachdem dickes Papier zwischen dem Gitter und der Platte gelegt wird, können die Zeichen mit einem Griffel in

---

[24] http://ddi.uni-wuppertal.de/material/spioncamp/dl/codierung-codes-station.pdf [Zugriffsdatum: 21.07.15]

[25] https://de.wikipedia.org/wiki/Brailleschrift [Zugriffsdatum: 02.08.2015]

[26] https://www.cbm.de/aktiv-werden/interaktiv/Was-ist-eigentlich-Braille-407811.html [Zugriffsdatum: 02.08.2015]

das Papier gedrückt werden. Das Lesen geschieht durch das Abfühlen der erhabenen Punkte mit den Fingerspitzen."[27]

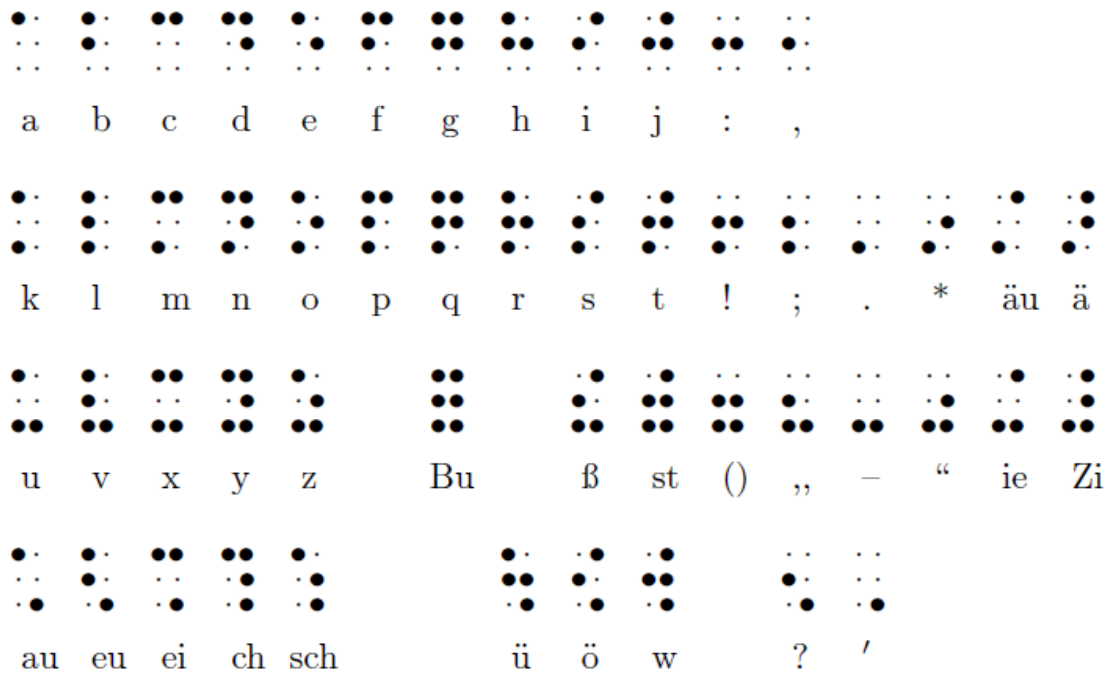


Abbildung 6: Braille-Schriftzeichen, entnommen aus BAUER: *Historische Notizen zur Informatik*, Seite 101.

Auch das Winkeralphabet stellt eine Codierung dar. Es dient z.B. der optischen Nachrichtenübermittlung zwischen Schiffen und wird heute vor allem militärisch genutzt, da es im Gegensatz zum Funkverkehr schwer abhörbar ist.[28] Dabei werden mithilfe von zwei rot-gelben Flaggen die Zeichen und Buchstaben durch verschiedene Stellungen der Arme angezeigt. Im Unterricht bietet es sich hier besonders an, die Schüler in Partner- oder Kleingruppenarbeit auf der enaktiven Ebene mit bereitgestellten Flaggen und dem Winkeralphabet (z.B. auf dem Schulflur oder –hof) kommunizieren zu lassen, sodass sie diesen Sachverhalt durch eigenes Handeln erfassen.

In der heutigen Zeit gibt es nun auch die computergestützte Steganographie, bei der die geheimen Botschaften in Textdateien, Bildern oder auch Audiodateien, den sogenannten Trägerdaten, versteckt werden. Nehls und Gleichmann beschreiben in ihrer Belegarbeit zur

---

[27] BAUER: *Historische Notizen zur Informatik,* Seite 102

[28] https://de.wikipedia.org/wiki/Winkeralphabet [Zugriffsdatum: 28.09.2015]

Steganographie verschiedene Verfahren wie beispielsweise die LSB[29]-Methode. „Bei diesem Verfahren wird die zu übermittelnde Nachricht in den niederwertigsten Bits der Farbwerte eines Bildpunktes versteckt, da hierbei die geringsten Veränderungen gegenüber dem Original-Bild entstehen.“ [30] Es gibt viele verschiedene Steganographie-Programme, welche jedoch teilweise viel Zeit in Anspruch nehmen und nicht immer kostenfrei erhältlich sind. Daher bietet die folgende Methode[31], geheime Daten in Dateien zu verstecken, einen erheblichen Vorteil, denn sie ist allein mithilfe von Windows-Bordmitteln und in wenigen Schritten ohne Einarbeitung nachvollziehbar durchführbar.

Durch die Tastenkombination `[WINDOWS]+[R]` und die Eingabe von `cmd` erreicht man die Konsole, wobei man mithilfe des Befehls `cd` in das entsprechende Verzeichnis der Trägerdatei bzw. der zu versteckenden Datei wechselt. Die Daten werden dann mithilfe des Befehls `copy` per Binärkopie hintereinander gehängt. Die Syntax dafür lautet:

`COPY /B` *Datei1* `+ /B` *Datei2 Ergebnisdatei*

Die neue „Ergebnisdatei“ stellt das Bild aus „Datei1“ dar, ohne z.B. den geheimen Text aus „Datei2“ anzuzeigen. Um an den geheimen Inhalt zu kommen, benennt man die „Ergebnisdatei“ entsprechend des Datei-Formats der „Datei2“ um und kann nun die „Ergebnisdatei“ als z.B. Textdatei öffnen. Ein erheblicher Nachteil dieser Methode ist, dass natürlich auch die Dateigrößen aufsummiert werden und die „Ergebnisdatei“ somit erheblich an Größe gewinnen kann.

Die Bergische Universität Wuppertal stellt ein SpionCamp[32] in Form von verschiedenen Arbeitsblättern, Stationsblättern, Materialien und Lösungen für mehrere Lernstationen zur Codierung, Steganographie und zu verschiedenen Verfahren der Kryptographie für Lehrer

---

[29] LSB ist die Abkürzung für Least Significant Bit.

[30] NEHLS: *Steganographie,* Seite 9.

[31] http://www.chip.de/bildergalerie/CHIP-Tipp-Geheimbotschaften-in-Dateien-verstecken-Galerie_32830336.html [Zugriffsdatum: 13.07.2015]

[32] http://ddi.uni-wuppertal.de/material/spioncamp.html [Zugriffsdatum: 14.07.2015]

bereit. Die Materialien können auch in anderen Unterrichtskontexten eingesetzt werden und unterliegen der Creative-Commons-Lizenz CC BY-NC-SA[33].

Angelehnt an die Idee des SpionCamps bietet es sich an, die von L. Humbert erläuterte Methode Doppelzirkel[34] für die Themen Codierung und Steganographie einzusetzen, um somit den vertieften Einstieg der Lernenden, von ihrem individuellen Vorwissen und persönlichem Interesse ausgehend, zu ermöglichen. Bei der Auswahl der Teilgebiete wird zwischen Wahl- und Pflichtstationen unterschieden, wobei grundlegendes Wissen an Pflicht- und spezielles Wissen an Wahlstationen erworben wird. In der folgenden Abbildung 7 sind die Themen des Doppelzirkels dargestellt, welche die Schüler selbstständig in Einzel-, Partner- oder auch Kleingruppenarbeit bearbeiten.

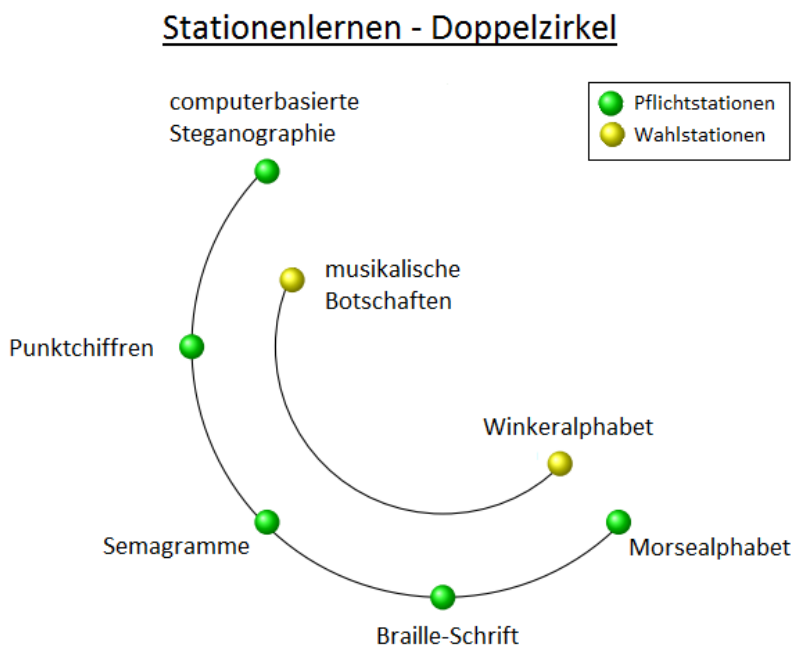


Abbildung 7: Stationenlernen zum Thema Codierung und Steganographie

„Zu jedem inhaltlichen Schwerpunkt werden verschiedene Arbeits- und Lernangebote bereitgestellt, die die unterschiedlichen Lernvoraussetzungen der Schülerinnen und Schüler im Hinblick auf Lernerfahrungen, Wissensstände sowie individuelle Aneignungs- und

---

[33] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.de [Zugriffsdatum: 14.07.2015]

[34] http://ddi.uni-wuppertal.de/ddi-sommersemester-2008/Sommersemester_2008-DdI-7_Ausdruck.pdf [Zugriffsdatum: 14.07.2015]

Bearbeitungsmethoden berücksichtigen.“[35] Die Reihenfolge ist insoweit vorgegeben, dass vor der Station „Semagramme“ die Station „Morsealphabet“ besucht werden sollte. Ansonsten ist die Reihenfolge der Stationen sowie die Bearbeitungszeit der einzelnen Stationen frei. In einer Vorbesprechung sollten, vor allem bei Klassen die noch unerfahren mit der Freiarbeit sind, feste Verhaltensregeln gemeinsam im Klassenverband aufgestellt werden. Auch die Zeitplanung dieser Erarbeitungsphase sollte, vor allem beim erstmaligen Durchführen von Stationenlernen, großzügig bemessen sein, da nach den Stationswechseln der Lautstärkepegel wieder gesenkt werden muss. Die Ergebnissicherung kann durch eine Besprechung der einzelnen Stationen im Plenum stattfinden. Mithilfe von kurzen Erläuterungen der Sachverhalte und Präsentationen der Ergebnisse und Erfahrungen können noch offene Fragen dabei im Plenum diskutiert werden.

Nun ist eine thematische Grundlage geschaffen, um kryptographische Verfahren einzuführen, welche häufig mithilfe von steganographischen Verfahren kombiniert werden. Dabei ist ein Bezug zur Geschichte der Kryptologie sinnvoll, um den Schülern die Motivation für die Entstehung dieser jahrhundertealten Verfahren nahezulegen.

404 v. Chr. entwickelten und verwendeten die Spartaner das älteste bekannte Verschlüsselungsverfahren. „Die Spartaner waren in ihren zahlreichen Schlachten immer wieder darauf angewiesen, Befehle und Nachrichten zu übermitteln, die vor dem Gegner geheim gehalten werden mussten. Dazu verwendeten die Spartaner als Kryptosystem die Skytale. Dieses System setzt voraus, dass Sender und Empfänger jeweils in Besitz eines Holzstabes mit genau demselben Durchmesser sind. Um eine Nachricht zu verschlüsseln wickelt der Sender einen schmalen Papierstreifen spiralartig um den Holzstab. Die Spartaner haben damals Papyrus oder Pergament benutzt. “[36] Nun kann das Papier

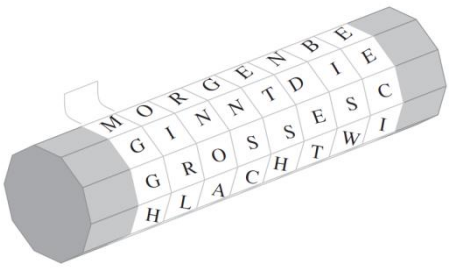


Abbildung 8: Skytale

[35] http://ddi.uni-wuppertal.de/ddi-sommersemester-2008/Sommersemester_2008-DdI-7_Ausdruck.pdf [Zugriffsdatum: 14.07.2015]

[36] FREIERMUTH: *Einführung in die Kryptologie,* Seite 19.

mit der geheimen Nachricht beschrieben werden, und zwar von links nach rechts, ohne Leer- und Satzzeichen, so dass auf jeder Windung nur genau ein Buchstabe steht. „Die einzigen Leerzeichen, die nach dem Verschlüsseln übrig bleiben, sind die Leerzeichen am Schluss des Textes, wenn die letzte Zeile auf der Skytale nicht mehr gefüllt werden kann.“[37] Ausschließlich ein Empfänger mit einer Skytale mit dem gleichen Durchmesser kann durch das Umwickeln des Papierstreifens den Klartext wiederherstellen.

Die Skytale gehört zu den Transpositionsverfahren, bei denen die Klartextzeichen erhalten bleiben und lediglich ihre Position verändert wird. „Das Wort Transposition ist abgeleitet vom lateinischen Wort „transponere“ = verschieben.“[38] Weitere Transpositionsverfahren sind die Schablone und das Pflügen.

Bei der Pflügen-Verschlüsselung wird zuvor ein Schlüssel n mit $n \in \mathbb{N}$ festgelegt, welcher angibt, wie viele Buchstaben in eine Zeile geschrieben werden sollen. Anschließend schreibt man nacheinander in jede Zeile n Buchstaben des Textes, wobei die letzte Zeile mit beliebigen Buchstaben aufgefüllt werden kann. Nun notiert man den Geheimtext angefangen bei den Buchstaben der letzten Spalte von unten nach oben, hinüber zur vorletzten Spalte von oben nach unten und so weiter, wie beim Pflügen eines Feldes.[39]

Beispiel Der Text **DER SCHATZ LIEGT UNTER DEN PALMEN** soll verschlüsselt werden. Du wählst als Schlüssel zum Beispiel die **6** und schreibst die Buchstaben so auf:

D	E	R	S	C	H
A	T	Z	L	I	E
G	T	U	N	T	E
R	D	E	N	P	A
L	M	E	N	X	X

D	E	R	S	C	H
A	T	Z	L	I	E
G	T	U	N	T	E
R	D	E	N	P	A
L	M	E	N	X	X

Du schickst die Nachricht **XAEEHCITPXNNNLSRZUEEMDTTEDAGRL** ab.

Abbildung 9: Ein Beispiel für das Transpositionsverfahren Pflügen entnommen aus dem SpionCamp

---

[37] FREIERMUTH: Einführung in die Kryptologie, Seite 20.

[38] http://ddi.uni-wuppertal.de/material/spioncamp/dl/transposition-skytale-station.pdf [Zugriffsdatum: 01.09.2015]

[39] http://ddi.uni-wuppertal.de/material/spioncamp/dl/transposition-pfluegen-station.pdf [Zugriffsdatum: 01.09.2015]

Für die Schablonen-Verschlüsselung benötigen sowohl der Sender als auch der Empfänger dieselbe Lochschablone; eine Schablone, die an bestimmten Stellen Löcher aufweist. Die Lochschablone wird auf ein leeres Papier gelegt und die ersten Buchstaben der Nachricht werden nacheinander einzeln in die Löcher eingetragen. Anschließend wird die Schablone im Uhrzeigersinn um 90 Grad gedreht und die nächsten Buchstaben in die Löcher eingetragen. So fährt man fort bis alle vier Stellungen der Schablone genutzt wurden. Ist die Nachricht länger, beginnt man mit einem neuem Quadrat. Ist die Nachricht kürzer, werden die übrigen Felder mit irgendwelchen Buchstaben gefüllt.[40]

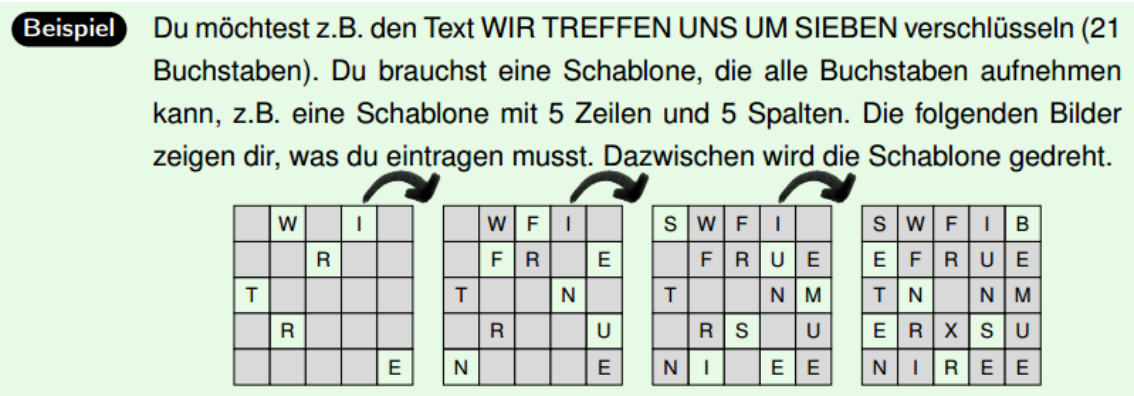


Abbildung 10: Beispiel für die Schablonen-Verschlüsselung, entnommen aus dem SpionCamp

Im Gegensatz zum Transpositionsverfahren werden bei Substitutionsverfahren die Klartextzeichen ersetzt und ihre Position nicht geändert. Das Wort Substitution ist abgeleitet vom lateinischen Wort „substituere“ und bedeutet „ersetzen“.[41] Zu den bekanntesten monoalphabetischen Substitutionsverfahren gehören das Freimaurer- und die Caesar-Verschlüsselung.

---

[40] http://ddi.uni-wuppertal.de/material/spioncamp/dl/transposition-schablone-station.pdf [Zugriffsdatum: 01.09.2015]

[41] http://ddi.uni-wuppertal.de/material/spioncamp/dl/substitution-m-caesar-station.pdf [Zugriffsdatum: 01.09.2015]

Die Freimaurer sind ein Geheimbund[42], welche die Freimaurer-Verschlüsselung im 18. Jahrhundert nutzten. Dafür werden alle Buchstaben des Alphabets, wie in Abbildung 11 zu sehen, in einer beliebigen Reihenfolge in vier bestimmte Muster geschrieben. Zum Verschlüsseln wird jeder Buchstabe des Klartextes durch die Linien und Punkte ersetzt, die den jeweiligen Buchstaben umgeben.

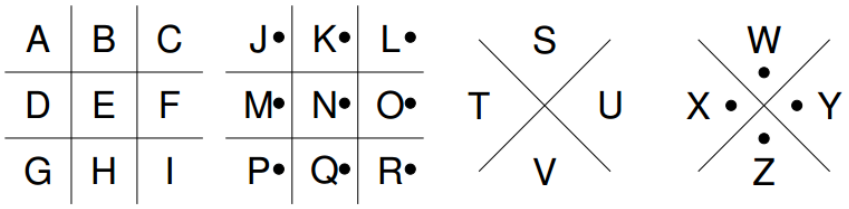


Abbildung 11: Freimaurer-Alphabet

Auf einem Arbeitsblatt des SpionCamps zum Thema Freimaurer ist die Entschlüsselung des folgenden Textes gefordert:

Der Klartext dazu lautet: „VERSUCH DEIN GLUECK“.

In der Antike (ca. 50 v. Chr.) verschlüsselte der römische Feldherr Gaius Julius Caesar militärische Nachrichten mithilfe des nach ihm benannten Substitutionsverfahrens Caesar-Verschlüsselung. Bei diesem Verfahren wird das Klartext-Alphabet um n Stellen zyklisch verschoben, so dass jeder Buchstabe immer auf den gleichen anderen abgebildet wird, wobei Leerzeichen und Sonderzeichen nicht berücksichtigt werden. Verschlüsselt man beispielsweise den Klartext „ADLERSHOF“ mit dem Schlüssel n = 3, so erhält man den Geheimtext „dgohuvkri“.

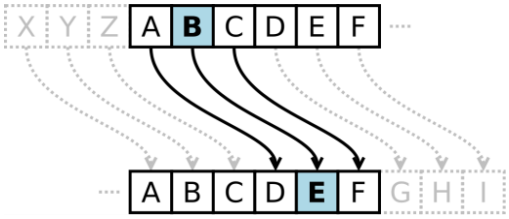


Abbildung 12: Caesar-Chiffre mit n = 3

[42] „Die Freimaurer haben sich der Verschwiegenheit und insbesondere dem Grundsatz verpflichtet, freimaurerische Bräuche und Logenangelegenheiten nicht nach außen zu tragen.“ https://de.wikipedia.org/wiki/Freimaurerei [Zugriffsdatum: 01.09.2015]

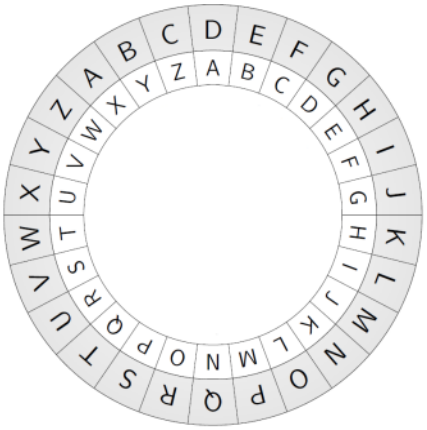


Abbildung 13: Chiffrierscheibe

Eine sogenannte Chiffrierscheibe, wie sie in Abbildung 13 zu sehen ist, kann zur erleichterten Ver- und Entschlüsselung verwendet werden. Die innere Scheibe stellt das Alphabet des Klartextes dar, die äußere Scheibe die des Geheimtextes. Bei einem Schlüssel von n = 3 entspricht das A des Klartextalphabets dem um drei Stellen verschobenen Buchstaben D. Verschiebt man nun die innere Scheibe dementsprechend, so sieht man auf einen Blick das zum Klartext-Alphabet zugeordnete Geheimtext-Alphabet auf der äußeren Chiffrierscheibe.

Wie bereits die Römer in der Antike, können auch die Schüler im heutigen Klassenzimmer mithilfe der Caesar-Verschlüsselung und der Chiffrierscheibe verschlüsseln. Aufgrund der Aufteilung in mehrere Verschlüsselungsverfahren ist die kooperative Gruppen-Puzzle-Methode prädestiniert für die Erarbeitung dieser Unterrichtsthemen.

Zuvor werden in der Einstiegsphase der Unterrichtsstunde, anhand eines Lehrervortrags, die Begriffe der Steganographie und Codierung wiederholt, sowie die der Kryptologie, Kryptographie und Kryptoanalyse definiert und die Geschichte der Kryptologie durch einen Vortrag über die Skytale eingeleitet. Es ist durchaus sinnvoll, den Lehrervortrag mit einer mitgebrachten Skytale (Holzstab) und einem Papierstreifen zum Ausprobieren und Demonstrieren zu untermauern. Für die Erarbeitungsphase werden anschließend vier heterogene Expertengruppen gebildet. In Abbildung 14 sind zwei Expertenthemen zu den Transpositionsverfahren Schablone und Pflügen und zwei weitere zu den Substitutionsverfahren Freimaurer- und Caesar-Verschlüsselung dargestellt.

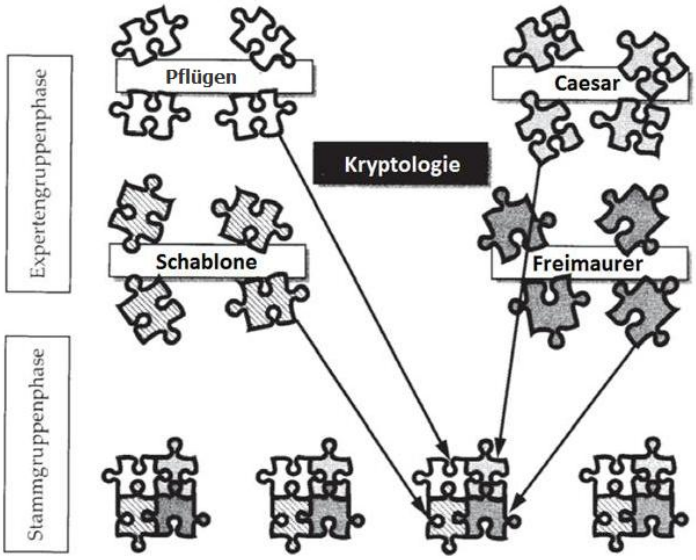


Abbildung 14: Gruppen-Puzzle für zwei Substitutions- und zwei Transpositionsverfahren

Nachdem sich die Expertengruppen in einer vorgegebenen Zeit mit ihrem jeweiligen Teilgebiet, mithilfe von Materialien, auseinandergesetzt haben, werden Stammgruppen gebildet, in denen mindestens ein Experte aus jedem Teilgebiet enthalten ist. In dieser Phase werden alle Teilgebiete den jeweils anderen Schülern der Stammgruppe gelehrt. Am Ende sollten alle Schüler einen Überblick über den kompletten thematischen Zusammenhang haben. Die Ergebnissicherung erfolgt durch einen maximal zehn minütigen Test, in dem alle Teilthemen ungefähr gleichgewichtet abgeprüft werden. „In der Auswertung werden die Stammgruppen im Kollektiv bewertet; es gibt also keine Einzelsieger, sondern nur Gruppensieger. Somit kann nur jenes Team gewinnen, in dem alle Teammitglieder bereit und in der Lage sind, sich gegenseitig zu belehren und einander zuzuhören.“[43]

Da die Schüler nun erste Erfahrungen mit Verschlüsselungsverfahren gemacht haben und im Zuge der Bearbeitung der Arbeitsblätter beim Gruppen-Puzzle erste Überlegungen zum Dechiffrieren der Verfahren mit und auch ohne Schlüssel angestellt haben, ist eine Überleitung zur Kryptoanalyse angemessen.

---

[43] MEYER: *Gruppen-Puzzle,* Seite 3.

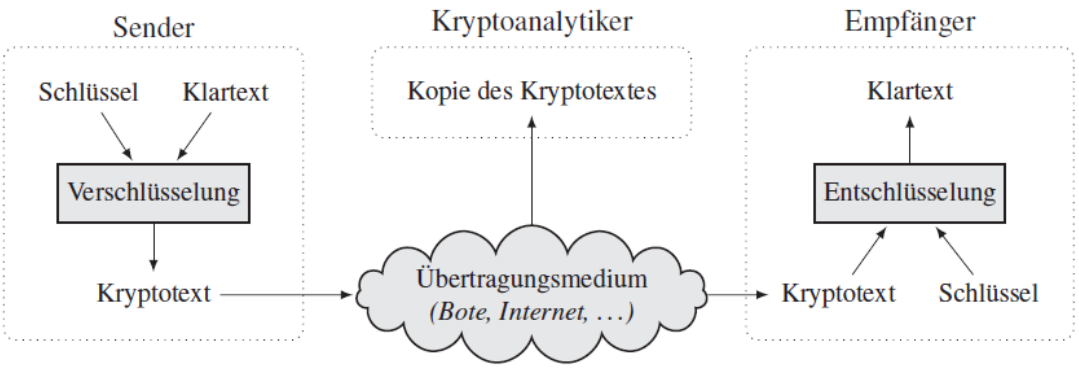


Abbildung 15: Kommunikationsschema, entnommen aus Freiermuth: *Einführung in die Kryptologie,* S. 29

Sowohl der Sender einer Nachricht als auch der Empfänger jener Nachricht müssen damit rechnen, dass der verschickte Text einem Gegner, dem sogenannten Kryptoanalytiker, in die Hände fallen kann. „Damit ist die ganze Kryptologie ein intellektuelles Spiel zwischen Kryptosystemdesignern und Kryptoanalytikern. Die Designer versuchen clevere Kryptosysteme zu bauen, und die Kryptoanalytiker versuchen eines nach dem anderen zu knacken.“[44]

„Die „Philosophie“ der modernen Kryptoanalyse wird durch das Prinzip von Kerckhoffs beschrieben; dies wurde erstmals in dem Buch „La cryptographie militaire“ (1883) des niederländischen Philologen Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwenhof (1835 bis 1903) formuliert, wie sein Name in vollem barockem Glanze lautet.“[45]

Kerckhoffs Prinzip besagt, dass die Sicherheit eines Verschlüsselungssystems nicht von der Geheimhaltung des Algorithmus abhängen darf. Die Sicherheit gründet einzig auf der Geheimhaltung des Schlüssels.[46] Demnach sollte das Ziel der modernen Kryptographie sein, Verfahren zu entwickeln, die auch dann noch sicher bleiben, wenn der Algorithmus bekannt und öffentlich diskutiert wurde.

---

[44] Freiermuth: *Einführung in die Kryptologie*, S. 30.

[45] BEUTELSPACHER: *Kryptologie,* Seite 19.

[46] BEUTELSPACHER: Kryptologie, Seite 19.

Albrecht Beutelspacher beschreibt in seinem Buch „Kryptologie“ in Kapitel 1.7 die unterschiedlichen Voraussetzungen, denen ein Kryptoanalytiker gegenüber stehen kann. Man unterscheidet folgende Typen von Attacken:

- Angriff mit bekanntem Geheimtext (known ciphertext attack):
  Der Kryptoanalytiker kennt ein relativ großes Stück Geheimtext.
- Angriff mit bekanntem Klartext (known plaintext attack):
  Der Kryptoanalytiker kennt ein (vergleichsweise kleines) Stück vom zusammengehörigen Klartext/Geheimtext.
- Angriff mit frei gewähltem Klartext (chosen plaintext attack):
  Wenn der Kryptoanalytiker Zugang zum Verschlüsselungsalgorithmus (mit dem aktuellen Schlüssel) hat, so kann er, um den Schlüssel zu erschließen, auch selbstgewählte Stücke Klartext verschlüsseln und versuchen, aus dem erhaltenen Geheimtext Rückschlüsse auf die Struktur des Schlüssels zu ziehen. Er könnte etwa der Maschine besonders regelmäßige Klartexte zum Verschlüsseln geben, zum Beispiel Folgen aus demselben Buchstaben (aaa . . .), mit dem Auftrag, diese zu verschlüsseln.

In der Einstiegsphase stellt der Lehrer im Lehrervortrag Kerckhoffs Prinzip vor. Durch die fragend-entwickelnde Methode bindet der Lehrer daraufhin die Schüler mit ein und stellt ihnen beispielsweise Fragen wie: „Welche Voraussetzungen könnte ein Kryptoanalytiker haben?“, um so die drei verschiedenen Typen von Attacken im Plenum herauszuarbeiten. Da die Schüler bereits die Caesar-Chiffre kennen, liegt es nahe, nun dieses Verfahren zu knacken. Auch hier wird fragend-entwickelnd herausgearbeitet, dass es beispielsweise die Möglichkeit gibt, alle 25 möglichen Schlüssel auszuprobieren[47]. Eine weitere Möglichkeit wäre es, eine Häufigkeitsanalyse durchzuführen, bei der der am häufigsten vorkommende Buchstaben des Geheimtextes durch den statistisch am häufigsten vorkommenden Buchstaben der (deutschen) Sprache ersetzt wird und so weiter.

In der Erarbeitungsphase bietet sich die Methode „Wettbewerb“ an, um die Schüler selbst als Kryptoanalytiker tätig werden zu lassen. Es ist eine Gruppenarbeit, die besonders in der

[47] Diese Methode bezeichnet man auch als „brute-force attack“.

Sekundarstufe I beliebt ist und sich für entdeckendes Lernen ebenso wie für Übungen oder für das Wiederholen eignet. Der Lehrer bildet heterogene Schülerteams von drei bis vier Schülern. Alle Schülerteams erhalten dieselben Aufgaben mit unterschiedlichen Schwierigkeitsstufen. Jedes Team muss alle Aufgaben bearbeiten und anschließend die Ergebnisse auf einem Blatt mit dem sich selbst gegebenen Teamnamen abgeben. „Während ein Schüler an der Tafel die Aufgaben vorrechnet und alle Schüler die Lösungswege mitschreiben, schaut der Lehrer zügig die Lösungen an. Gewinnen kann die Gruppe mit den meisten, aber mindestens 75% richtigen Lösungen. Gibt es mehrere Gruppen mit der gleichen Anzahl richtiger Lösungen, dann ist die schnellste dieser Gruppen der Sieger.“[48]

Die Schüler können und wissen bereits, dass man das monoalphabetische Substitutionsverfahren von Caesar durch das Ausprobieren von 25 möglichen Schlüsseln knacken kann. Da liegt es nahe, dieses Verschlüsselungsverfahren „weiterzuentwickeln“.

1586 veröffentlichte der französische Diplomat Blaise de Vigenère die nach ihm benannte Vigenère-Verschlüsselung. Die Idee ist es, die Caesar-Verschlüsselung mehrmals anzuwenden, sodass „ein Klartextbuchstabe nicht stets zu demselben Geheimtextbuchstaben verschlüsselt“[49] wird. Da nicht nur ein sondern mehrere Geheimtextalphabete dem Klartextalphabet zugeordnet werden, gehört die Vigenère-Verschlüsselung zu den polyalphabetischen Substitutionsverfahren.

Man benötigt für die Verschlüsselung mit dem Vigenère-Verfahren neben einem Schlüsselwort auch ein Vigenère-Quadrat. Wie in der Abbildung 16 dargestellt, besteht es aus allen 26 möglichen Alphabet-Verschiebungen. Das Schlüsselwort kann jede beliebige Buchstabenfolge sein. „Man verschlüsselt einen Buchstaben, indem man den über ihm stehenden Schlüsselwortbuchstaben bestimmt. Der Geheimtextbuchstabe ist der Schnittpunkt derjenigen Zeile, die mit dem Schlüsselwortbuchstaben beginnt und mit derjenigen Spalte, deren erstes Element der Klartextbuchstabe ist.“[50]

---

[48] ISB: *Zusammenspiel von Unterrichtsmethoden,* Seite 33.

[49] BEUTELSPACHER: *Kryptologie,* Seite 34.

[50] BEUTELSPACHER: *Kryptologie*, Seite 36.

Klartext

Schlüsselbuchstaben	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Abbildung 16: Vigenère-Quadrat entnommen aus SpionCamp

Das folgende Beispiel aus dem Buch „Kryptologie“ von A. Beutelspacher veranschaulicht das Vorgehen. Dabei ist das Schlüsselwort „VENUS“ und der Klartext „polyalphabetisch“. „Um den ersten Geheimtextbuchstaben zu erhalten, muss man (im Vigenère-Quadrat) in dem Alphabet, das mit V beginnt, nachsehen, was in der Spalte p steht; dies ist der Buchstabe K. Um den zweiten Buchstaben zu verschlüsseln, sucht man in der Zeile E den Buchstaben in der Spalte o; dieser ist S. Und so weiter.“[51]

Schlüsselwort:	V	E	N	U	S	V	E	N	U	S	V	E	N	U	S	V
Klartext:	**p**	**o**	**l**	**y**	**a**	**l**	**p**	**h**	**a**	**b**	**e**	**t**	**i**	**s**	**c**	**h**
Geheimtext:	**K**	**S**	**Y**	**S**	**S**	**G**	**T**	**U**	**U**	**T**	**Z**	**X**	**V**	**M**	**U**	**C**

Abbildung 17: Beispiel für die Vigenère-Verschlüsselung, entnommen aus Beutelspacher: *Kryptologie,* S.35

Für die Entschlüsselung eines Geheimtextbuchstabens benötigt man ebenfalls das Schlüsselwort und das Vigenère-Quadrat. Man bestimmt als erstes den über dem Geheimtextbuchstaben stehenden Schlüsselwortbuchstaben. Anschließend sucht man in

[51] BEUTELSPACHER: *Kryptologie*, Seite 34-35.

der Zeile, welche mit dem Schlüsselwortbuchstaben beginnt, den Geheimtextbuchstaben. Der Buchstabe, mit dem die Spalte beginnt, entspricht dem Klartextbuchstaben.

Auch dieses Verfahren wurde bereits 1854 (allerdings unveröffentlicht) von Charles Babbage geknackt. Der erste veröffentlichte Angriff stammt von dem preußischen Infanteriemajor Friedrich Wilhelm Kasiski, der diesen 1863 publiziert hat. Eine zweite Methode geht auf Colonel William Frederick Friedman zurück. Beide Methoden dienen dazu, die Schlüsselwortlänge zu bestimmen.[52] Auf die Vorstellung der Methoden sollte in der Sekundarstufe I aufgrund der (mathematischen) Komplexität verzichtet werden.

In Partnerarbeit können sich die Schüler anhand eines Arbeitsblattes das Vigenère-Verfahren aneignen, sich gegenseitig aufkommende Fragen beantworten, gemeinsam diskutieren und mithilfe von Übungsaufgaben ihr Wissen erproben. Nach einer kurzen Zusammenfassung des Vigenère-Verfahrens im Plenum bekommt jeder einzelne Schüler einen mit der Vigenère-Chiffre verschlüsselten (einzigartigen) Geheimtext, mit dem Auftrag diesen mit dem Schlüsselwort „Sonne“ zu dechiffrieren. Diese kurzen Geheimtexte ergeben aneinandergereiht einen sinnvollen Text, der beispielsweise einer guten Nachricht entspricht, wie der folgende Geheimtext[53]:

Wbqymuv vfx Kczzij iaq has Iötid njvxkqurvf! Rn qek Krgxwf uryls fb wuvöa vwl iaq ee Kbplwbrahw krvxwfuvr vwr Fsfbr fgzsvax, oweq Jjoh Tlgav hrk vrhxw yrvrw Vnhwsistetsa nyxuroif.

Wenn jeder Schüler (je nachdem wie viele in der Klasse sind) einen etwa gleichgroßen Anteil an Buchstaben entschlüsselt und die Schüler dann reihum hintereinander ihren entschlüsselten Textabschnitt vorlesen, dann ergibt dieser zusammengesetzt die folgende gute Nachricht:

---

[52] BEUTELSPACHER: *Kryptologie*, Seite 36.

[53] Es gibt zahlreiche Tools zum Verschlüsseln im Internet, beispielsweise folgende Internetseite für die Vigenère-Verschlüsselung: https://gc.de/gc/vigenere/ [Zugriffsdatum: 02.09.2015].

„Endlich ist Sommer und die Vögel zwitschern! Da das Wetter heute so schön ist und am Wochenende weiterhin die Sonne scheint, wird Frau Ghomi uns heute keine Hausaufgaben aufgeben."

Bevor die Schüler diese erfreuliche Nachricht am Ende der Unterrichtsreihe zur Kryptologie von einander vorgelesen bekommen, werden sie zuvor in der Einstiegsphase diesen letzten Blockes einen Filmausschnitt zu einem berühmten polyalphabetischen Substitutionsverfahren des 20. Jahrhunderts schauen.

„Der deutsche Ingenieur Arthur Scherbius (1878–1929) baute ein kryptographisches Gerät, das verschiedene mechanische und elektrische Elemente auf raffinierte Art und Weise zu einer Verschlüsselungsmaschine kombinierte. Die sogenannte ENIGMA wurde zum gefürchtetsten Kryptosystem der Geschichte."[54] Es gibt zahlreiche Bücher und auch Filme rund um die ENIGMA, wie zum Beispiel der 2014 erschienene Hollywood-Film „The Imitation Game", denn die ENIGMA war die Verschlüsselungsmaschine der deutschen Wehrmacht im Zweiten Weltkrieg und hat damit eine große historischen Bedeutung. Eine empfehlenswerte, freiverfügbare ARTE Dokumentation von Denis van Waerebeke, welche 2014 veröffentlich wurde, trägt den Titel „Wie ein Mathegenie Hitler knackte" und ist derzeit auf Youtube unter folgendem Link in HD verfügbar:

https://www.youtube.com/watch?v=LHY3ugWiqBQ.

Im Vordergrund dieser Dokumentation steht der britische Kryptoanalytiker Alan Turing, welcher im Dienst der Alliierten die ENIGMA knackte und durch die Entschlüsselung der Funksprüche der Deutschen maßgeblich am Sieg der Alliierten im zweiten Weltkrieg beteiligt war. „Er war einer der Gründer der Informatik, denn er legte unter anderem den Begriff des Algorithmus exakt mathematisch fest. Mit seiner Definition von Algorithmen im Jahr 1936 datiert man die Entstehung der Informatik als eigenständige Wissenschaftsdisziplin."[55]„Den Briten gelang es nicht nur, das ENIGMA-System zu

---

[54] FREIERMUTH: *Einführung in die Kryptologie,* Seite 164.

[55] FREIERMUTH: *Einführung in die Kryptologie,* Seite 29.

knacken, sondern sie konnten diese Tatsache auch bis zum Ende des zweiten Weltkriegs vor den Deutschen geheim halten.“[56]

In der Einstiegsphase sollte der Klasse mindestens die Hälfte des Lehrfilmes und somit ca. 28 Minuten Filmmaterial gezeigt werden.[57] Die Faszination des Mediums soll zur Information, Motivation und vor allem zur Veranschaulichung genutzt werden. Der kreative Filmeinsatz kann Lernprozesse auslösen, jedoch nicht ersetzen. „Filme dosiert, didaktisch wohl überlegt und methodisch kreativ eingesetzt, beleben den Unterricht und steigern seine Wirkung. Entscheidend für die unterrichtliche Qualität des Filmeinsatzes sind immer die Phasen, die auf die Filmbetrachtung folgen.“[58] Daher wird in der Erarbeitungsphase die Kugellager-Übung verwendet, um den Filminhalt intensiv zu rekapitulieren.

Die Kugellager-Übung ist eine Form der Partnerarbeit und wird auch „Doppelter Sitzkreis“ genannt, da sich die Schüler in einem Innen- und Außenkreis einander gegenübersitzen. Nach dem Betrachten des Filmausschnittes beginnt die erste Runde dieser Übung, indem die im Außenkreis sitzenden Schüler ihrem jeweils im Innenkreis gegenübersitzenden Partner den Inhalt des Filmes erzählen. Dafür ist ein Fragenkatalog von Vorteil, sodass die Schüler auf konvergente Fragen wie „Aus welchen Bestandteilen ist die ENIGMA aufgebaut?“, aber auch auf divergente Fragen wie „Was fand ich besonders interessant?“ antworten. In der zweiten Runde fasst der zuhörende Partner zusammen, was sein Gegenüber erzählt hat, und fügt hinzu, was ihm noch aufgefallen ist. Anschließend werden neue Partnerschaften gebildet, indem sich die Schüler in einem der beiden Kreise um mehrere Plätze weiter bewegen. „Nun berichten die im Innenkreis Sitzenden denen im Außenkreis, was sie gesehen haben und was sie besonders interessant fanden. Wiederum fasst der nun zuhörende Schüler zusammen, was sein Gegenüber gesagt hat.“[59] „Die Übung trainiert das aktive Sprechen ebenso wie das aktive Zuhören. Sie fördert in besonderer Weise die Speicherung des Gelernten im Gedächtnis.“

---

[56] BEUTELSPACHER: *Kryptologie,* Seite VIII.

[57] Bis zu Minute 27:56.

[58] MATTES: *Methoden für den Unterricht,* Seite 66.

[59] MATTES: *Methoden für den Unterricht,* Seite 20.

Die ENIGMA, welche in der Abbildung 18 zu sehen ist, besteht grob aus drei Bestandteilen:

- einer Tastatur mit den Buchstaben A bis Z,
- einem Lampenfeld mit selbigen Buchstaben
- und einer Verschlüsselungseinheit, die wiederum aus drei Walzen, einer Umkehrwalze und einem Steckerbrett besteht.

Abbildung 18: ENIGMA, Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr.

„Das wichtigste Element der Verschlüsselungseinheit sind die Walzen. Eine Walze ist eine Scheibe, die mit Hilfe eines Zahnrades mechanisch gedreht werden kann. Die Verschlüsselung, die durch die drei hintereinander geschalteten Walzen zusammen mit der Umkehrwalze entsteht, entspricht jedoch nur einer monoalphabetischen Verschlüsselung. Die große Sicherheit der ENIGMA basiert darauf, dass sich die Walzen nach jedem eingegebenen Buchstaben abhängig voneinander drehen. So ergibt sich eine sehr komplexe polyalphabetische Verschlüsselung. Die erste Walze wird nach jedem eingegebenen Buchstaben um eine Position im Uhrzeigersinn gedreht. Die zweite Walze dreht sich erst, wenn die erste Walze eine volle Umdrehung gemacht hat. Die dritte Walze wird erst nach einer vollen Umdrehung der zweiten Walze gedreht, ähnlich wie bei einem

Kilometerzähler. Dadurch wiederholt sich die Verschlüsselung erst nach insgesamt 26 · 26 · 26 = 17 576 Buchstaben.“[60]

„Die Verschlüsselung eines Klartextes mit der ENIGMA läuft nun folgendermaßen ab: Der Operateur schaut in der Schlüsseltabelle nach, welche Einstellungen für den aktuellen Tag gelten. Dann wählt er die entsprechenden Walzen aus und bringt sie der Walzenlage folgend in den drei Walzenbuchten unter. Danach dreht er die drei Walzen, so dass die in der Grundstellung erwähnte Einstellung vorliegt. Schließlich steckt er die Steckerverbindungen entsprechend den Angaben in der Schlüsseltabelle.“[61] Um eine Nachricht zu verschlüsseln, drückt der Operateur der Reihe nach die Tasten, die den Buchstaben des Klartextes entsprechen. Durch elektrische Signale, die durch die Verschlüsselungseinheit fließen, werden dann die Lampen der entsprechenden Geheimtextbuchstaben zum Leuchten gebracht. Für die Entschlüsselung benötigt der Empfänger dieselben Einstellungen der ENIGMA und gibt anschließend die Buchstaben des Geheimtextes ein. Die Lampen der Buchstaben des Klartextes leuchten nun auf, denn die Umkehrwalze führt dazu, dass die Entschlüsselung gleich wie die Verschlüsselung funktioniert.

Alan Turings Idee war es, eine elektromechanische Maschine zu bauen, die systematisch alle Schlüssel durchprobierte. Sie bestand aus über hundert hintereinander geschalteten ENIGMA-Geräten, mit der die Alliierten alle Walzenlagen und Grundstellungen durchprobieren konnten. Die Maschine wird als Turing-Bombe bezeichnet und konnte alle Möglichkeiten in rund sechs Stunden testen. Bis zum Ende des Zweiten Weltkrieges waren über 210 Turing-Bomben verdeckt im Einsatz.

Bislang haben der Sender und der Empfänger der verschlüsselten Nachrichten denselben Schlüssel zum Ver- bzw. Entschlüsseln verwendet, daher spricht man auch von einer „symmetrischen Verschlüsselung“. Doch dieser Sachverhalt führt zwangsläufig zu einem Problem: Was soll man tun, wenn ein manueller Schlüsselaustausch nicht möglich ist?

---

[60] MATTES: Methoden für den Unterricht, Seite 169.

[61] MATTES: Methoden für den Unterricht, Seite 171.

Die Lösung für dieses Schlüsselaustauschproblem ist die asymmetrische Verschlüsselung.

Bei asymmetrischen Verschlüsselungsverfahren wird ein öffentlicher Schlüssel für das Verschlüsseln und ein zweiter privater Schlüssel für das Entschlüsseln verwendet. 1976 begründeten Diffie und Hellman mit ihrem Diffie-Hellman-Schlüsselaustausch-Verfahren die asymmetrische Kryptographie, auf der die modernen kryptographischen Verfahren, wie RSA, beruhen. Aufgrund der hohen mathematischen Voraussetzungen ist die Behandlung der asymmetrischen Verfahren vorzugsweise in der Sekundarstufe II zu behandeln.

Die Unterrichtsreihe zur Kryptologie wird mit der Redekette-Methode im Klassenverband beendet. Die Redekette beginnt mit einer offenen Frage oder einem Impuls des Lehrers. In diesem Fall eignet sich die Frage: „Was haben wir in den letzten sechs Blöcken Neues gelernt?" Der daraufhin aufgerufene Schüler äußert seine Antwort und nimmt anschließend einen weiteren Schüler dran, „sodass eine Kette von Beiträgen entsteht."[62] Im Vorfeld kann man sich auf Regeln einigen. Eine Regel sollte sein, dass jede Schülerantwort nur zu einem Teilthema sein darf und nur einen zeitlichen Umfang von beispielsweise 2 Minuten[63] haben darf. Außerdem sollten bevorzugt Schüler aufgerufen werden, die noch keine Gelegenheit hatten sich zu äußern, auch wenn diese sich nicht gemeldet haben. Der Lehrer sollte nur eingreifen, wenn die Regeln missachtet werden. Die Schüler sitzen vorzugsweise einander zugewandt. „Die Methode erzeugt eine mitbestimmte, stressfreie, angenehme Atmosphäre"[64] und bildet ein zusammenfassendes und schönes Ende der Unterrichtsreihe.

---

[62] MATTES: *Methoden für den Unterricht,* Seite 22.

[63] Je nach zur Verfügung stehender Zeit und Schüleranzahl ist die Minutenanzahl anzupassen.

[64] MATTES: *Methoden für den Unterricht,* Seite 22.

5. Ausführliche Stundenentwürfe

5.1 Codierung und Steganographie

Thema: Codierung und Steganographie (2 x 90 min)

Zeit	**Phasen**	**Unterrichtsschritte/Lehrer-Schülerinteraktion**	**Sozialform & Handlungs-muster**	**Medien**
20 min	Einstieg	L. beginnt Brainstorming an der Tafel (oder am interaktiven Whiteboard) mit dem ersten mittleren Kreis „Kryptologie“ und fragt: „Was verbindet ihr mit diesem Begriff?“. Der Lehrer bittet die Schüler ihre Assoziationen und ihr Vorwissen dazu anzuschreiben. Falls S. nichts anschreiben, stellt L. konkretere Fragen wie: „Was verbindet ihr mit dem Begriff Verschlüsselung/Codierung/Morsealphabet?“ oder „Hat jemand von euch schon mal in einer Geheimsprache kommuniziert?“ Besondere Interessen/Fragen der S. notiert sich der L. und greift sie später wieder auf.	Brainstorming Methode Plenum Schüler-Schüler-Gespräch bzw. Lehrer-Schüler-Gespräch	Tafel oder interaktives Whiteboard oder Pinnwand
115 min	Erarbeitung	L. vereinbart mit S. Verhaltensregeln. S. arbeiten selbstständig an verschiedenen Stationen in Einzel-, Partner- oder auch Kleingruppenarbeit. Es gibt fünf Pflichtstationen, wobei das Morsealphabet vor der Station zu	Stationenlernen im Doppelzirkel Einzel-, Partner- und Kleingruppen-	Arbeits- und Stationen-blätter, Piano-App, Taschen-lampen-App,

		Semagrammen bearbeitet werden sollte: • Morsealphabet (Stationsblatt 1, Material 1: Morsealphabet-Tabelle, AB 1, Lösung von AB 1) • Braille-Schrift (Stationsblatt 2, AB 2.1, Lösung von AB 2.1 und AB 2.2) • Semagramme (Stationsblatt 4, Lösung 4, AB 4, Lösung zu AB 4) • Punktchiffren (Stationsblatt 5, AB 5, Lösung zu AB 5) • Computerbasierte Steganographie (Stationsblatt 7, Lösung 7) und zwei Wahlstationen im Doppelzirkel: • Winkeralphabet (Stationsblatt 3, AB 3) • Musikalische Botschaften (Stationsblatt 6, AB 6)	arbeit	Taschen-lampen, Stecknadeln, Mindestens 2 paar Flaggen, leeres Papier, Stifte zum Zeichnen, Windows-PCs
45 min	Ergebnis-sicherung / Präsentationen	Jede Pflichtstation wird besprochen, indem S. von L. aufgefordert werden, das Themengebiet zu erläutern und ggf. ihre erstellten Werke zu präsentieren. Falls genügend Zeit vorhanden ist, werden auch die Wahlstationen von S. erläutert und ggf. präsentiert.	Plenum Schülervortrag	Beamer, Laptop, Lautsprecher, Magnete zum Befestigen der Werke an der Tafel

5.1.1 Alle Materialien der Station: Morsealphabet

Stationsblatt 1:

SPIONCAMP

Morse-Alphabet

Codierung

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

1832, noch vor der Erfindung des Telefons, erfand der Amerikaner Samuel Morse einen Apparat, den Morsetelegraphen. Mit dessen Hilfe konnten Nachrichten über große Entfernungen hinweg übermittelt werden. Dazu wurden so genannte Telegraphenmasten aufgestellt und Leitungen durch das ganze Land gespannt. Es konnten allerdings keine gesprochenen Worte übertragen werden, sondern lediglich kurze und lange elektrische Impulse.

Deshalb dachte sich Samuel Morse ein Alphabet aus, das nur aus kurzen und langen Signalen bestand:

A	• —	U	• • —
B	— • • •	V	• • • —
C	— • — •	W	• — —
D	— • •	X	— • • —
E	•	Y	— • — —
F	• • — •	Z	— — • •
G	— — •		
H	• • • •		
I	• •		
J	• — — —		
K	— • —	1	• — — — —
L	• — • •	2	• • — — —
M	— —	3	• • • — —
N	— •	4	• • • • —
O	— — —	5	• • • • •
P	• — — •	6	— • • • •
Q	— — • —	7	— — • • •
R	• — •	8	— — — • •
S	• • •	9	— — — — •
T	—	0	— — — — —

Für die Übertragung von Morsezeichen kann man auch Lichtzeichen verwenden. Zwischen den Buchstaben wird eine kurze Pause gemacht. Zwischen den Wörtern eine etwas längere.

BERGISCHE UNIVERSITÄT WUPPERTAL

CC BY NC SA
v3 – 5. Juli 2013

Material 1: Morsealphabet-Tabelle

SPIONCAMP

Morse-Alphabet
Codierung

Morsealphabet-Tabelle

A	• —	U	• • —
B	— • • •	V	• • • —
C	— • — •	W	• — —
D	— • •	X	— • • —
E	•	Y	— • — —
F	• • — •	Z	— — • •
G	— — •		
H	• • • •		
I	• •		
J	• — — —		
K	— • —	1	• — — — —
L	• — • •	2	• • — — —
M	— —	3	• • • — —
N	— •	4	• • • • —
O	— — —	5	• • • • •
P	• — — •	6	— • • • •
Q	— — • —	7	— — • • •
R	• — •	8	— — — • •
S	• • •	9	— — — — •
T	—	0	— — — — —

BERGISCHE UNIVERSITÄT WUPPERTAL

v3 5. Juli 2013

AB 1:

SPIONCAMP

Arbeitsblatt

Morse-Alphabet

Codierung

Aufgabe 1 Könnt ihr folgende Nachricht verstehen?

.... .- .-.. .-.. - - -

Aufgabe 2 Wie lautet das Morse-Signal für SOS? (Das ist das internationale Hilfesignal.)

Aufgabe 3 An der Station findet ihr eine Taschenlampe. Stellt euch zu zweit mit ein paar Metern Entfernung gegenüber auf, jeder mit einem Morse-Alphabet. Buchstabiert euch mit der Taschenlampe gegenseitig jeweils ein Wort.

A	• —	U	• • —
B	— • • •	V	• • • —
C	— • — •	W	• — —
D	— • •	X	— • • —
E	•	Y	— • — —
F	• • — •	Z	— — • •
G	— — •		
H	• • • •		
I	• •		
J	• — — —		
K	— • —	1	• — — — —
L	• — • •	2	• • — — —
M	— —	3	• • • — —
N	— •	4	• • • • —
O	— — —	5	• • • • •
P	• — — •	6	— • • • •
Q	— — • —	7	— — • • •
R	• — •	8	— — — • •
S	• • •	9	— — — — •
T	—	0	— — — — —

BERGISCHE UNIVERSITÄT WUPPERTAL

v3 5. Juli 2013

Lösung von AB 1:

SPIONCAMP

Lösungen

Morse-Alphabet
Codierung

Lösung 1 **HALLO**

Lösung 2 . . . – – – . . . ist das Zeichen für SOS.
In Not wird aber nicht »SOS SOS . . . « gefunkt, sondern immer »S« und »O« abwechselnd.

v3 5. Juli 2013

5.1.2 Alle Materialien der Station: Braille-Schrift

Stationsblatt 2:

SPIONCAMP

Braille-Schrift

Codierung

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

Louis Braille (geboren 1808 in Frankreich) wurde im Alter von 3 Jahren nach einem Unfall blind. Mit 14 Jahren entwickelte er eine Schrift, die auch Blinde lesen können. Sie besteht aus erhöhten Punkten, die mit den Fingern zu ertasten sind.
Es gibt für Blinde viele Bücher in Blindenschrift. Für den Computer gibt es spezielle Braille-Zeilen, mit denen auch Blinde z. B. im Web surfen können.
Obwohl es auch noch andere Schriftarten mit erhöhten Zeichen gibt, ist die Braille-Schrift heute am weitesten verbreitet.

Tafel mit Braille-Zeichen

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
1	2	3	4	5	6	7	8	9	0			

Dir ist vielleicht aufgefallen, dass z. B. »1« und »A« durch dasselbe Braille-Zeichen dargestellt werden. Damit man weiß, was gemeint ist, wird einer Zahl ein bestimmtes Zeichen vorangestellt. Geht es danach mit Buchstaben weiter, wird das Zeichen für »Buchstabe« geschrieben. Diese vorangestellten Zeichen heißen auch **Präfixe**. Du findest die Zeichen in der Abbildung rechts.

Zahl	Buchstabe

Beispiel

21 Äpfel

Es gibt auch Zeichen für Klammern, Umlaute, Groß- und Kleinschrift und andere spezielle Zeichen. Diese wurden hier weggelassen.

BERGISCHE UNIVERSITÄT WUPPERTAL

v3 – 5. Juli 2013

AB 2.1:

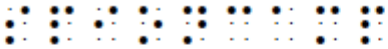
SPIONCAMP

Arbeitsblatt

Braille-Schrift

Codierung

Aufgabe 1 Kannst du folgende Nachricht verstehen?



Aufgabe 2 Aufgabe 1 war ziemlich leicht. Kannst Du auch das hier »lesen«?

Aufgabe 3 An der Station findet ihr ein Blatt, auf dem ihr selbst Nachrichten »schreiben« könnt. Arbeitet im Team. Eine(r) schreibt ein Wort durch Stecken der Nadeln auf das Brett. Die/der andere liest dann wie ein Blinder — Augen schließen. Nicht schummeln! — und versucht, die Nachricht zu ertasten. Beschreibt eurem Partner Buchstabe für Buchstabe, welche Punkte erhöht sind. Zum Beispiel für ein **N**:

oben links, oben rechts, mitte rechts, unten links

Der Sehende kann dann nachschauen, welcher Buchstabe das ist. Wechselt nach dem Wort die Rollen.

v3 – 5. Juli 2013

Lösung zu AB 2.1:

SPIONCAMP

Lösungen

Braille-Schrift
Codierung

Lösung 1 **SPIONCAMP**

Lösung 2 **DIE ANTWORT IST 42**

BERGISCHE UNIVERSITÄT WUPPERTAL

v1

AB 2.2:

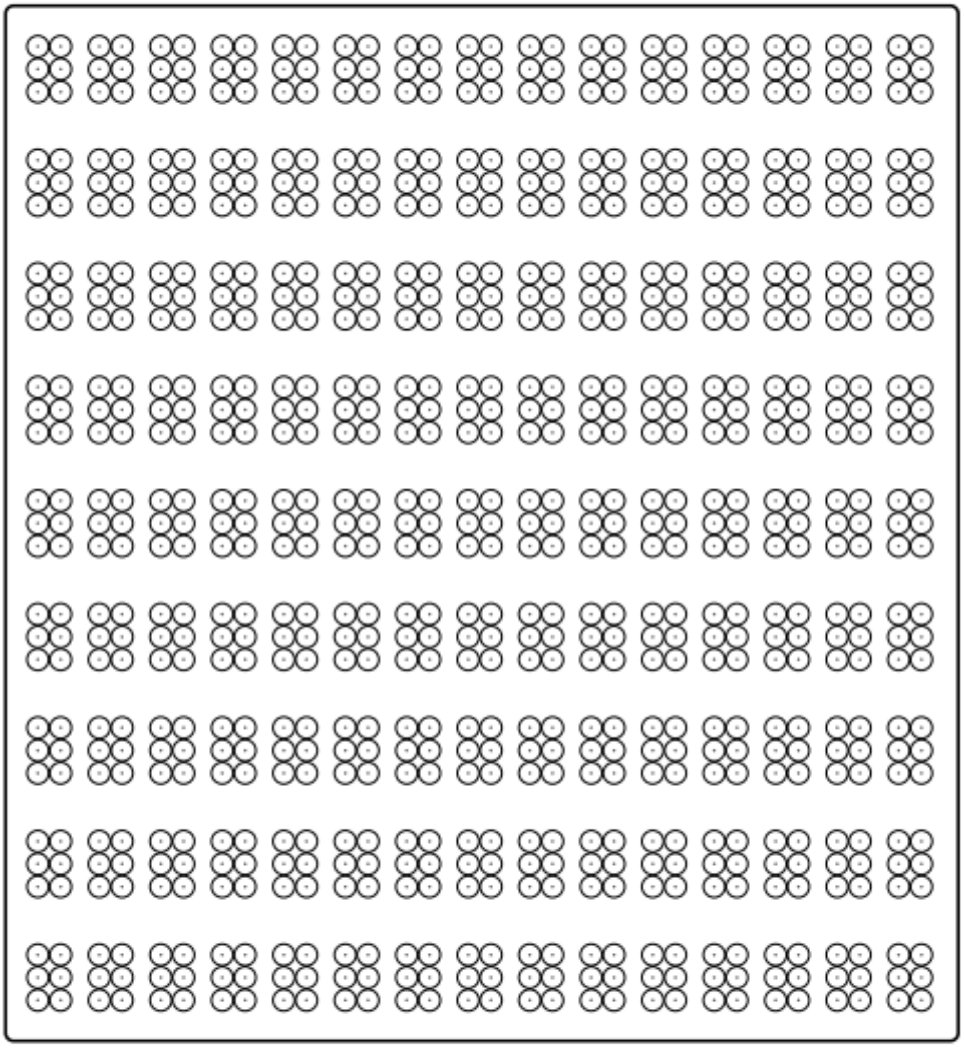
SPIONCAMP

Arbeitsblatt

Braille-Schrift

Codierung

Stecke einen Text. Probiert zu zweit aus, ob die/der jeweils andere den Text mit dem Finger erfühlen kann. Nimm die Tabelle auf dem Stationsblatt für die Buchstabencodes hinzu.



Du brauchst Stecknadeln (nicht zu lang!) zum Stecken der Braille Schrift.

BERGISCHE UNIVERSITÄT WUPPERTAL

v3 – 10. Juli 2013

5.1.3 Alle Materialien der Station: Winkeralphabet

Stationsblatt 3:

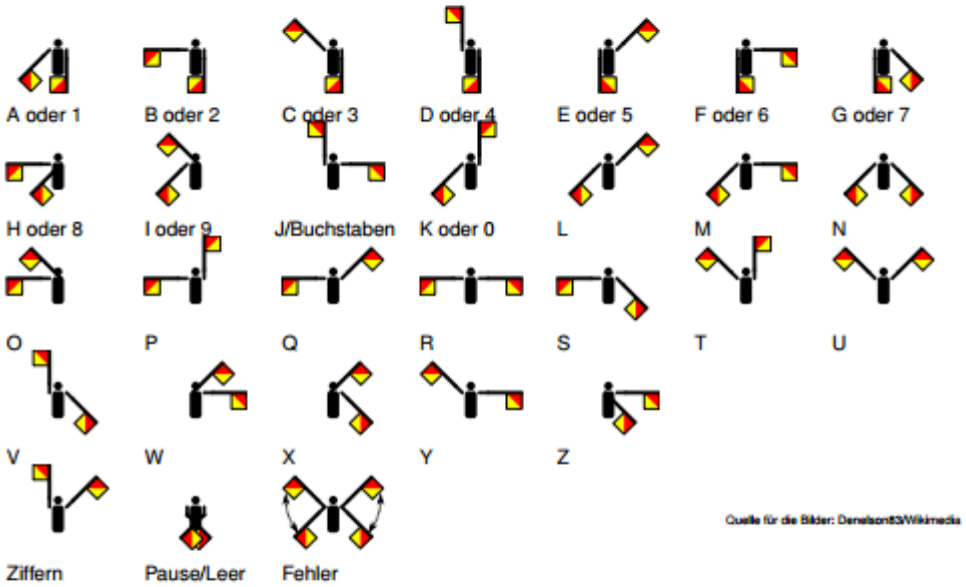
SPIONCAMP

Winkeralphabet

Codierung

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

Das Winkeralphabet stammt aus der Seefahrt. Man kann sich damit verständigen, wenn man sich in Sichtweite aber außer Hörweite voneinander befindet. Man nimmt zwei Flaggen in die Hände und zeigt durch Stellung der Arme bestimmte Zeichen an.



Quelle für die Bilder: Denelson83/Wikimedia

Einige Zeichen sind doppelt belegt: das erste Zeichen kann zum Beispiel »A« oder »1« bedeuten. Möchtest du eine Ziffern senden, winkst du einmal das Zeichen für »Ziffern«. Für Buchstaben nach Ziffern, das Zeichen »J«.

Kennt ihr dieses Zeichen?

Es wurde 1958 erfunden und soll *atomare Abrüstung* symbolisieren. Atomare Abrüstung heißt auf Englisch *Nuclear Disarmament*. Die Zeichen für N und D aus dem Winkeralphabet wurden zu diesem Zeichen kombiniert. (Der senkrechte Strich ist das D, die beiden schrägen das N.)

BERGISCHE UNIVERSITÄT WUPPERTAL

v2 5. Juli 2013

AB 3:

SPIONCAMP

Arbeitsblatt

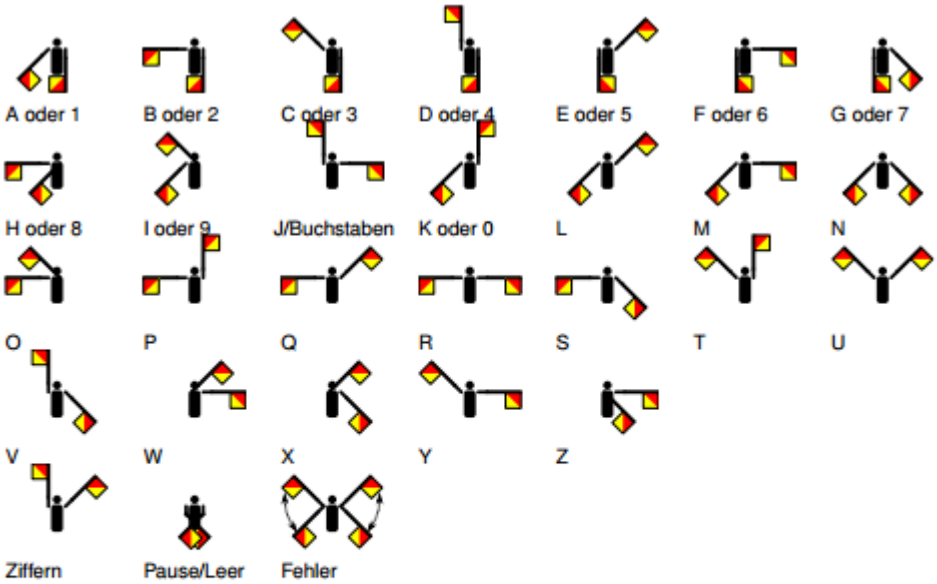
Winkeralphabet

Codierung

Aufgabe 1 Entschlüssele folgende Nachricht!

Aufgabe 2 An der Station findet ihr Flaggen. Nehmt jeder zwei und stellt euch mit ein paar Metern Entfernung gegenüber auf. Buchstabiert euch mit den Flaggen gegenseitig jeweils ein Wort.

Das Winkeralphabet



BERGISCHE UNIVERSITÄT WUPPERTAL

v2 5. Juli 2013

5.1.4 Alle Materialien der Station: Semagramme

Stationsblatt 4:

SPIONCAMP

Bild
Steganographie

Die Buchstaben bleiben **was** sie sind, aber man erkennt nicht, **wo** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das **Steganographie**. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)

Bei der Steganographie werden Nachrichten in Medien versteckt, z.B. in Bildern. Wenn du dir das Bild nur kurz ansiehst, fällt dir gar nicht auf, das hier eine Nachricht enthalten sein könnte.
Texte oder Bilder, in denen Nachrichten versteckt wurden, heißen *Semagramme*.

Aufgabe 1 Kannst du die Nachricht in dem folgenden Semagramm lesen?
Es ist nicht ganz einfach, da die Nachricht vor dem Verstecken codiert wurde.
Tipp: Sieh dir die Stationen zur Codierung nochmal an.

Bild: Emma, 3 Jahre (dem Bild wurde dann die (codierte) Nachricht hinzugefügt)

BERGISCHE UNIVERSITÄT WUPPERTAL

v3 5. Juli 2013

Lösung zum Stationsblatt 4:

SPIONCAMP

Lösungen

Bild
Steganographie

Lösung 1 Das Bild enthält eine Nachricht im Morsecode. Die Grashalme haben lange und kurze Stengel und sind zu Büscheln (= Buchstaben) zusammengefasst. Die Nachricht lautet also:

(LEHRER SIND DOOF)

BERGISCHE UNIVERSITÄT WUPPERTAL

v2 5. Juli 2013

AB 4:

Arbeitsblatt zur Station: Semagramme

1. Aufgabe:

Welche Nachricht verbirgt sich in diesem Bild?

Bildquelle: Schmeh: *Versteckte Botschaften*, Seite 23. Ursprünglich aus der französischen Zeitschrift Spirou.

2. Aufgabe:

Zeichne ein Bild und verbirg eine kurze Nachricht von maximal drei Wörtern darin. Lass das Bild bei der Station liegen, sodass ein Mitschüler versuchen kann, es zu entschlüsseln.

3. Aufgabe:

Nimm ein Bild eines Mitschülers und versuche seine verborgene Nachricht zu entdecken.

Lösung zu AB 4:

1. Aufgabe

Die Raben auf dem Baum stehen für VW, die Blumen für VOLVO und die Latten des Zauns für BUICK.

5.1.5 Alle Materialien der Station: Punktchiffren

Stationsblatt 5:

Literaturquelle: Schmeh, Klaus: *Versteckte Botschaften - Die faszinierende Geschichte der Steganografie*, 1. Auflage, Heise Verlag Hannover, 2009.

Punktchiffren

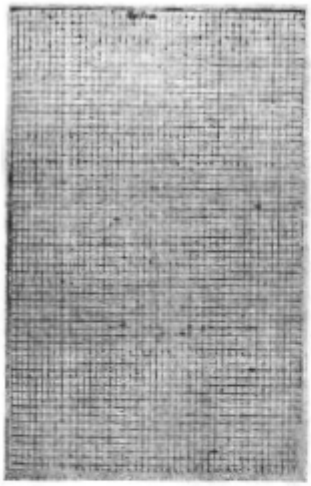
1977 berichtete der US-Historiker Albert C. Leighton in einer Fachzeitschrift über einen interessanten Fund.[10] In einem Archiv in München war er auf ein aus 20 Blättern bestehendes Manuskript gestoßen, das mit von Hand aufgetragenen Karolinien sowie mit zahlreichen Punkten und ein paar wenigen Symbolen beschrieben war. Das Manuskript war offensichtlich um das Jahr 1583 entstanden und erfüllte keinen unmittelbar erkennbaren Zweck. Da die Blätter im Archiv zusammen mit einigen Verschlüsselungsunterlagen aufbewahrt wurden, vermutete er, dass die seltsamen Punkte eine geheime Nachricht darstellten.

Leighton hielt es für wahrscheinlich, dass er auf eine Punktchiffre gestoßen war. Eine Punktchiffre ist ein steganografisches Verfahren, das (in seiner gebräuchlichsten Form) wie folgt funktioniert: Man nehme ein Achsenkreuz und trage auf der y-Achse die Buchstaben von A bis Z ab. Auf der x-Achse werden die Zahlen 1, 2, 3 usw. abgetragen. Ist der erste Buchstabe des zu verschlüsselnden Texts ein S, dann zeichnet man an der Koordinate (1,S) einen Punkt. Ist der zweite Buchstabe ein T, dann folgt ein zweiter Punkt bei (2,T). Weitere Punkte wären beispielsweise (3,E), (4,G), (5,A), (6N), (7,O), (8,G), (9,R), (10,A), (11,F), (12,I) und (13,E).

Eine Punktchiffre lässt sich leicht tarnen. Beispielsweise kann der Absender die korrekte Beschriftung der x- und y-Achse weglassen und die Punkte stattdessen als Aktienkurse oder Temperaturverläufe deklarieren. Bettet man ein solches Diagramm in einen dazu passenden Text ein, dann wird kaum jemand Verdacht schöpfen. Auch die anfangs erwähnten Kreuze unter einem Liebesbrief können eine Punktchiffre bilden.

Im Falle des Manuskripts aus dem Münchner Archiv hatte der Autor ganz auf ein Achsenkreuz verzichtet und seine Punkte einfach auf das Karomuster geschrieben. Eine weitere Tarnung gab es nicht. So stand Albert C. Leighton vor einem Stapel Karopapier, auf dem sich pro Blatt ein paar Dutzend Punkte ohne zusätzliche Information verloren. Die Bedeutung dieser Punktesammlung zu ermitteln, war keine einfache Aufgabe. Notizen auf den Zetteln zeig-

10) Albert C. Leighton: *The earliest use of a dot cipher.* Cryptologia 2/1977



Auf diesem Karopapier aus dem 16. Jahrhundert fand der Historiker Albert C. Leighton eine getarnte Nachricht.

ten, dass schon zuvor (wahrscheinlich irgendwann im 19. Jahrhundert) jemand einen Entzifferungsversuch unternommen hatte – vermutlich ohne Erfolg.

Doch Leighton hatte das Glück des Tüchtigen. An anderer Stelle im Archiv fand er vier Papierstreifen, auf denen Buchstaben sowie einige Wörter (hauptsächlich Namen und Orte) notiert waren. Eine Prüfung ergab, dass sich diese Streifen tatsächlich als Achsenkreuze für die Entschlüsselung der Punktchiffre nutzen ließen. Das erste Wort, das Leighton – 400 Jahre nach der Verschlüsselung – zum Vorschein bringen konnte, hieß ANFANG. Ohne größere Mühe entzifferte Leighton auch den Rest der Punktchiffre. Diese erwies sich als in deutscher Sprache verfasst (obwohl damals noch Latein die vorherrschende Schriftsprache war) und enthielt beispielsweise folgenden Absatz:

Die babstlich heiligkeit hat noch als vil uns bewyst nyt mer dan zehen tausend kronen zu hilff hiher geschichkt, die ist man khnehten zuvor schan schultig gewest, wie E.L. selb zu erwegen, das mit so schlehter somma nit vil krieg zu feyrn.

Der Absender beklagte sich also, dass ihm der Papst nur 10.000 Kronen zur Verfügung gestellt hatte, was für kriegerische Zwecke nicht besonders viel war. Historiker Leighton hatte keine Mühe, den Text richtig einzuordnen. Er stammte aus der Zeit der Gegenreformation, als die katholische Kirche versuchte, gegen den in Deutschland um sich greifenden Protestantismus vorzugehen. Zu den Protagonisten, die auf der Seite des Papsts kämpften, gehörte der Freisinger Bischof Ernst von Bayern (1554–1612), der um 1577 auch Erzbischof von Köln werden wollte. Ein Vertrauter Ernsts, der an den dortigen Verhandlungen teilnahm, war offensichtlich der Absender der getarnten Botschaft. Sie war an Ernsts Bruder adressiert, aber offenbar vor allem für ihn

selbst bestimmt. Gemäß dem Inhalt der Nachricht hätte der Vertraute gerne mehr finanzielle Unterstützung durch den Papst erhalten.

Bei seiner weiteren Suche im Archiv entdeckte Leighton noch eine zweite Punktchiffre, die mit dem gleichen Verfahren verschlüsselt wurde. Diese wurde offensichtlich von Ernst selbst verfasst. Der Adressat und die genaue Entstehungszeit sind nicht bekannt. Darin berichtet Ernst über ein Bündnis, das er mit anderen Bischöfen geschlossen hat, um seine Interessen durchzusetzen. Zwar waren diese Informationen Historikern bereits bekannt, doch immerhin brachten die entschlüsselten Quellen ein paar neue Facetten ans Licht.

Die von Leighton aufgefundene Punktchiffre ist die älteste bekannte ihrer Art. Leider weiß man heute nicht mehr, wer auf die Idee kam, sie zu nutzen, und wie die Nachrichten übertragen wurden. Die Idee, die Botschaften zu verschlüsseln und zu verstecken, ist angesichts der damaligen Machtspiele sicherlich nachvollziehbar. Allerdings sind keine weiteren Punktchiffren aus dem Umfeld des Ernst von Bayern überliefert. Vermutlich hatte der Bischof mit dem üblichen Problem zu kämpfen: Ein Semagrammverfahren ist für längere Nachrichten oft zu umständlich und nicht praktikabel.

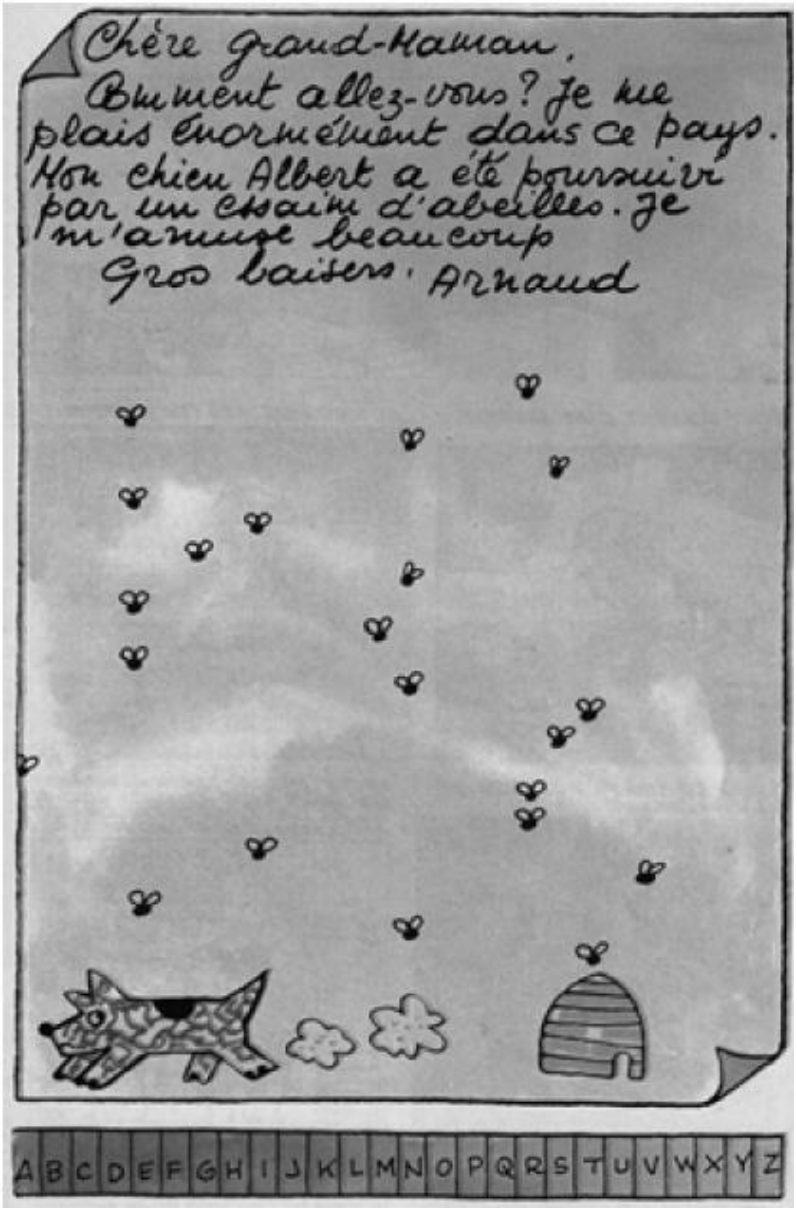
Erst etwa 50 Jahre nach Ernst von Bayern ist die nächste Punktchiffre belegt. Sie findet sich in einem Buch des englischen Geistlichen und Wissenschaftlers John Wilkins (1614–1672), der sich ausführlich mit der Steganografie beschäftigte. Allerdings beschreibt Wilkins dieses Verfahren nur, ohne dass es zu einem praktischen Einsatz gekommen wäre. Auch die meisten anderen bekannten Beispiele sind eher Spielereien als ernst zu nehmende Werkzeuge für die geheime Kommunikation.

AB 5:

Arbeitsblatt zur Station: Punktchiffren

1. Aufgabe

Dieser Kinderbrief aus der französischen Zeitschrift Spirou enthält eine versteckte Nachricht. Wie lautet diese Nachricht?



Die versteckte Nachricht lautet:

Lösung von AB 5:

Der Text den vermeintlich ein Enkel an seine Oma geschrieben hat, ist unwichtig. Die eigentliche Nachricht ist mit Hilfe der Bienen als Punktchiffre kodiert. Nimmt man die unter dem Bild abgetragene Buchstabenfolge als x-Achse, dann ergibt sich daraus folgende Nachricht: RENSEIGNEMENTS ARRIVENT. Das heißt: »Auskünfte kommen.«

5.1.6 Alle Materialien der Station: Musikalische Botschaften

Stationsblatt 6:

Literaturquelle: Schmeh, Klaus: *Versteckte Botschaften - Die faszinierende Geschichte der Steganografie*, 1. Auflage, Heise Verlag Hannover, 2009.

Musikalische Botschaften

Zu den nächstliegenden Dokumenten, in die sich eine geheime Botschaft einkodieren lässt, gehören Notenblätter. Wenn jede Note für einen bestimmten Buchstaben steht, dann kann ein Datenschmuggler problemlos einen längeren Text als Musikstück notieren und unauffällig versenden. Allerdings fällt die Tarnung schnell auf, sobald jemand versucht, das Werk zu spielen. Für diesen Fall sollte der Besitzer vorsichtshalber vorgeben, Anhänger einer besonders progressiven Musikrichtung zu sein.

Die Idee, mit Noten Buchstaben darzustellen, ist schon sehr alt.[12] Bereits Johann Sebastian Bach verewigte seinen Nachnamen in zahlreichen Werken, indem er die Tonfolge B-A-C-H einbaute. Bach hatte das Glück, dass es zu jedem der vier Buchstaben einen gleichnamigen Ton gibt. Mindestens 300 andere Komponisten (darunter so bekannte Namen wie Beethoven, Schumann und Liszt) übernahmen in den folgenden Jahrhunderten diese Tonfolge und setzten Bach damit ein Denkmal.

Vor allem im 19. Jahrhundert war es unter Komponisten eine verbreitete Praxis, den eigenen Namen oder sonstige Buchstabenkombinationen mit Noten zu kodieren. So stellte beispielsweise der deutsche Violinist Friedrich Fesca (1789–1826) die Tonfolge F-E-Es-C-A an den Anfang eines Streichquartetts. Ähnliches versuchte Fescas Kollege und Zeitgenosse Louis Spohr (1784–1859) in einem seiner Werke. Da es zu den Buchstaben P, O und R jedoch keine passenden Noten gibt, musste er tricksen. Er begann seine Tonfolge mit einem Es, gefolgt von den Buchstaben »po«, die für »piano« stehen. Darauf folgte ein H und schließlich eine mit dem Hals nach unten dargestellte Viertelnote, die eine gewisse optische Ähnlichkeit mit einem »r« hat. Besonders elegant wirkt dies zwar nicht, aber immerhin.

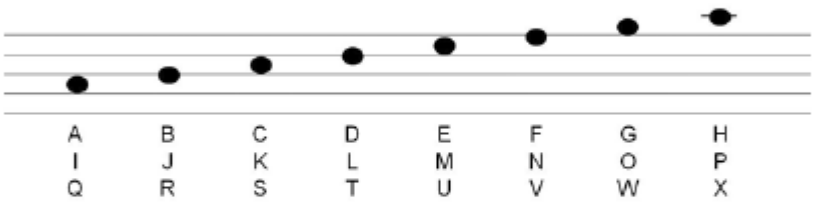
12) Eric Sams: *Musical Cryptography*. Cryptologia 3/1979

26 Punkt, Punkt, Komma, Strich – Semagramme

Der irische Komponist John Field (1782–1837) wollte dem offenbar nicht nachstehen. Anstatt seinen Namen in Musikform zu pressen (was nicht wirklich funktioniert hätte), versuchte er es mit den Tonfolgen B-E-E-F (Rindfleisch) und C-A-B-B-A-G-E (Kohl). Diese Melodien waren seiner Haushälterin gewidmet, die ihn offensichtlich mit guten Mahlzeiten versorgte. Falls Sie derartige Tonfolgen nachspielen wollen, sollten Sie beachten, dass die Note B im Englischen eine andere Bedeutung hat als im Deutschen. Hierzulande ist das B ein vermindertes H und daher klanglich mit dem Ais identisch. International kennt man dagegen kein H, sondern bezeichnet diesen Ton als B. Mit anderen Worten: Das deutsche B klingt einen Halbton tiefer als das englische.

Die bisherigen Beispiele wirken recht harmlos im Vergleich zu den Tonspielereien, die Robert Schumann in seine Kompositionen einbaute. Mehrfach kommen in seinen Stücken die Töne Es-C-H-A vor, wobei es sich um die spielbaren Buchstaben seines Nachnamens handelt. Teilweise variierte er auch die Reihenfolge. Weitere von ihm verwendete Folgen sind A-B-E-G (Name eines Freunds), G-A-D-E (ebenfalls der Name eines Freunds), F-A-E (frei aber einsam), A-D-E, A-C-H und B-Es-D-H (Name eines Freunds, eigentlich Bezeth). Schumanns steganografisches Meisterwerk lautet zweifellos LASSDASFADEFASSDASAECHDE, was für »Lass das Fade, fass das Echte« steht.

Ende des 19. Jahrhunderts reichte es einigen Komponisten offenbar nicht mehr aus, nur mit den Buchstaben A bis H zu arbeiten. Einige der Tonmeister entwickelten daher Codes, die jedem Buchstaben eine Note zuordneten. Das Beispiel in der folgenden Abbildung stammt von dem französischen Komponisten Francis Poulenc. Dieser nutzte den Code, um in seinem Stück *Pièce brève sur le nom d'Albert Roussel* (»Kurzes Stück über den Namen Albert Roussel«) den Namen seines Kollegen Albert Roussel zu verarbeiten. Bekannte Komponisten, die mit ähnlichen Codes arbeiteten, waren Claude Debussy, Arthur Honegger und Maurice Ravel.

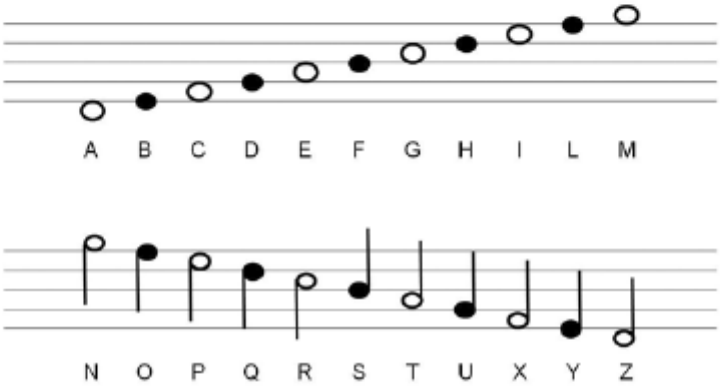


Dieser Notencode stammt von dem französischen Komponisten Francis Poulenc.

Neben Musikern beschäftigten sich auch Verschlüsselungsexperten mit Noten-Codes. Entsprechende Aktivitäten sind erstmals für das 16. Jahrhundert belegt. Unter anderem experimentierte Philipp II. von Spanien damit. Im Vatikan entstand 1596 ein ähnliches System. Dieses sah neun Noten vor, die

jeweils acht Werte annehmen konnten, wodurch 72 unterschiedliche Symbole zur Verfügung standen. Leider ist nicht bekannt, in welchem Umfang die päpstlichen Verschlüsselungsexperten dieses System nutzten.

Den einflussreichsten Musik-Code veröffentlichte um das Jahr 1563 der Italiener Giovanni della Porta (1535–1615) in seinem Buch *De furtivis literarum notis*. Er legte elf Töne fest, die es in jeweils zwei Werten gab (siehe Abbildung unten). Damit konnte er die 22 für die lateinische Sprache relevanten Buchstaben kodieren (J, K, V und W ließ er weg). Dieser Code fand in den folgenden Jahrhunderten den Weg in zahlreiche Musik- und Verschlüsselungsbücher. Es gab mehrere Abwandlungen und Erweiterungen. Michael Haydn (1737–1806), der Bruder des bekannteren Komponisten Joseph Haydn, zählt zu den prominentesten Personen, die sich mit diesem Thema befassten.



Der Italiener Giovanni della Porta entwickelte im 16. Jahrhundert diesen Code, mit dem sich ein Text als Musikstück tarnen ließ.

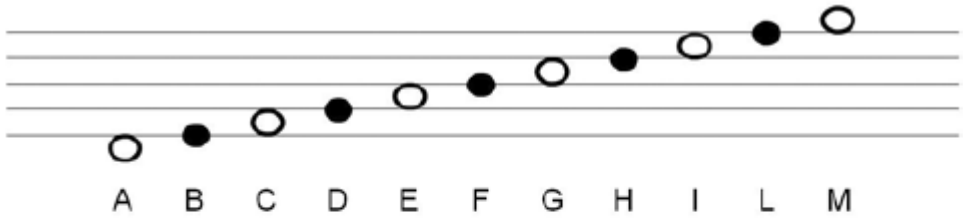
Musikalische Steganografie fand jedoch nicht nur in Büchern, sondern auch in der Praxis statt. So verwendeten um das Jahr 1800 zwei französische Diplomaten eine Porta-ähnliche Technik, um miteinander zu kommunizieren. Leider ist nicht bekannt, ob dieses System seinerzeit jemandem auffiel und ob es gebrochen wurde. Für das Jahr 1950 ist ein weiterer Fall belegt. Damals fing die Polizei in New York ein Notenblatt ab, dessen Inhalt sich als nicht spielbar erwies. Eine Überprüfung zeigte, warum: Es handelte sich um einen illegalen Wettschein.

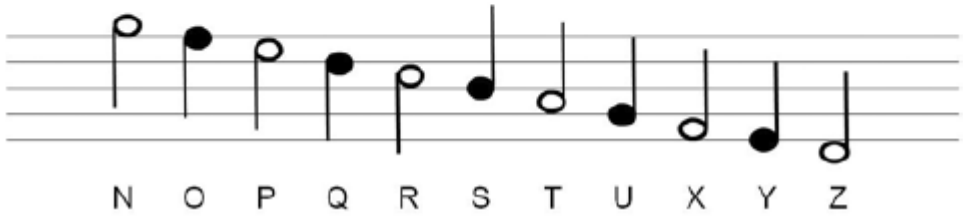
AB 6:

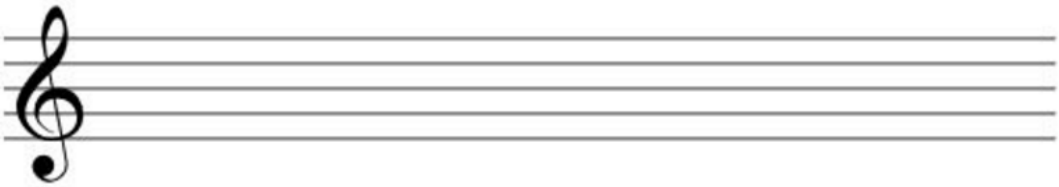
Arbeitsblatt zur Station: Musikalische Botschaften

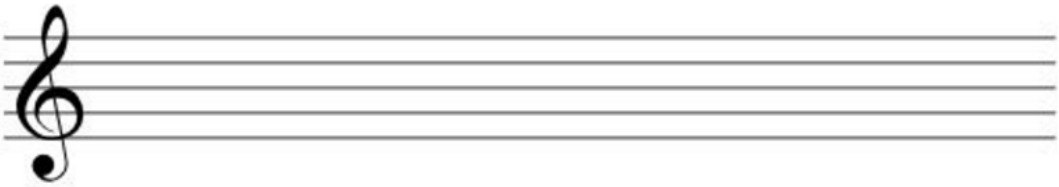
1. Aufgabe:

Notiere mithilfe des Musik-Codes von Giovanni della Porta deinen Vor- und Nachnamen als Musikstück.









2. Aufgabe:

Verwende die Piano App und Kopfhörer, um deine notierten Noten zu spielen.

5.1.7 Alle Materialien der Station: Computerbasierte Steganographie

Arbeitsblatt zur Station: Computerbasierte Steganographie

1. Aufgabe:

Verstecke Geheimbotschaften in Dateien. Folge dafür der Schritt für Schritt Anleitung am Windows-PC:

(1) Wähle ein Träger-Bild im JPG-Format aus. Achte bei der Wahl darauf, dass die versteckten Daten den Überbringer aufblähen. Wer eine 100-MByte-Botschaft in einem 100x100 Pixel großen JPG-Bild versteckt, macht schnell auf sich aufmerksam.

(2) Schreibe eine geheime Nachricht in den Text-Editor von Windows und speichere diese beispielsweise auf dem Desktop.

(3) Öffne die Konsole über die Tastenkombination `[WINDOWS]+[R]` und die Eingabe von „`cmd`".

(4) Navigiere mithilfe von „`cd`" in das richtige Verzeichnis:

```
C:\Users\Mina>cd Desktop

C:\Users\Mina\Desktop>
```

(5) Der simple Trick der geheimen Botschaft besteht darin, die Daten per Binärkopie hintereinander zu hängen. Die Option `/B` sagt dem Programm, dass wir die Daten im Binärformat aneinanderhängen wollen. Die Syntax lautet:

COPY /B *Datei1* **+ /B** *Datei2 Ergebnisdatei*

```
C:\Users\Mina>cd Desktop

C:\Users\Mina\Desktop>COPY /B Baum.jpg + /B geheim.txt neuerBaum.jpg
Baum.JPG
geheim.txt
        1 Datei(en) kopiert.

C:\Users\Mina\Desktop>_
```

(6) Ein Doppelklick auf die neue Datei zeigt das unveränderte Bild. Um an den geheimen Inhalt zu kommen, benennt man die Datei neuerBaum.jpg einfach in eine TXT-Datei um. Anschließend kann man die Daten wie gewohnt extrahieren.

2. Aufgabe:

Nenne einen Vor- und einen Nachteil dieser Methode.

Vorteil:_____

Nachteil:_____

Lösung zu Stationsblatt 7:

2. Aufgabe:

Nenne einen Vor- und einen Nachteil dieser Methode.

Vorteil:

- Man benötigt keine Software, die Daten werden mit Windows-Bordmitteln in Dateien versteckt.
- Man kann mehrere geheime Botschaften übermitteln, indem man ein Archiv (ZIP-Ordner) anstelle einer TXT-Datei mit einem Trägerbild verknüpft.

Nachteil:

- Die Dateigröße summiert sich auf, d.h. wenn das Bild eine Größe von ca. 3 MB hat und die geheime Botschaft eine Größe von ca. 1 MB, dann hat die neue Datei eine Größe von ca. 4 MB.
- Sensible Daten sollten Sie auf diesem Weg nicht übermitteln. Ein Blick mit einem Hex-Editor in die präparierte JPG-Datei, offenbart die typische ZIP Datei-Signatur zusammen mit den im Archiv vorhandenen Dateinamen.

5.2 Kryptographie: Transposition und monoalphabetische Substitution

Thema: Transpositions- und monoalphabetische Substitutionsverfahren

Zeit	**Phasen / Methode**	**Unterrichtsschritte/Lehrer-Schülerinteraktion**	**Sozialform & Handlungs-muster**	**Medien**
10 min	Einstieg	L. führt die Begriffe Kryptologie, Kryptographie und Kryptoanalyse ein und beginnt die Geschichte der Kryptologie mit dem ältesten bekannten Verfahren: der Skytale.	Plenum Lehrervortrag	Tafel oder interaktives Whiteboard, Skytale und Papierband
70 min	Erarbeitung	L. teilt die S. in vier leistungsheterogene Gruppen auf, welche in der ersten Gruppen-Puzzle-Phase jeweils Expertengruppen für Caesar-Chiffre, Freimaurer, Pflügen oder Schablone werden. In der Stammgruppenphase setzen sich jeweils ein S. aus jeder Expertengruppe in Stammgruppen zusammen und lehren einander ihr erlerntes Verfahren.	Gruppen-Puzzle bzw. Gruppenarbeit Schüler-Schüler-Gespräch	AB zu den vier Themen, Scheren zum Ausschneiden des Materials
10 min	Ergebnis-sicherung	S. schreiben einen (kurzen) angekündigten Wissenstest zu allen vier Themen: Skytale, Schablone, Caesar-Chiffre und Freimaurer-Chiffre. Es gewinnt die Stammgruppe mit der höchsten aufsummierten Punktzahl.	Test Einzelarbeit	Test

5.2.1 Arbeitsblätter für das Thema Caesar-Chiffre

SPIONCAMP

Caesar

Substitution (monoalphabetisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

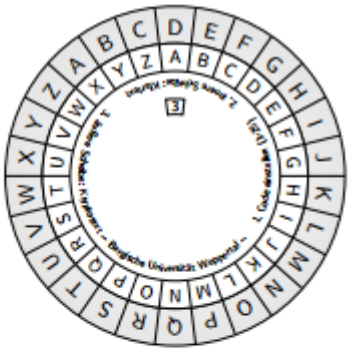
Der römische Feldherr Julius Caesar (100 bis 44 v. Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Diese Anzahl der Stellen heißt **Caesar-Schlüssel**.

Beispiel Beim Schlüssel **3** nahm Caesar immer den Buchstaben, der im Alphabet drei Stellen weiter rechts steht.
Dazu schrieb er das Alphabet zweimal untereinander. Das untere Alphabet schrieb er allerdings um drei Stellen verschoben.

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

Caesar ersetzte also in seinem Text jedes **A** durch ein **D**, jedes **B** durch ein **E** usw. Beachte, dass **X** durch **A** ersetzt wird, also das Alphabet nach dem Z einfach mit A weitergeschrieben wird.

Damit nicht jedesmal die beiden gegeneinander verschobenen Alphabete aufgeschrieben werden müssen, kann auch eine sogenannte Chiffrierscheibe benutzt werden. In der Abbildung ist wie im Beispiel der Schlüssel 3 eingestellt.
Mit der Scheibe kannst du nun sowohl Texte verschlüsseln als auch entschlüsseln. Möchtest du verschlüsseln, dann suchst du den Buchstaben auf der inneren Scheibe und schreibst den entsprechenden Buchstaben auf der äußeren Scheibe auf. Entschlüsseln geht entsprechend umgekehrt: Hier suchst du den Buchstaben außen und schreibst den entsprechenden Buchstaben auf der inneren Scheibe auf.



v4 5. Juli 2013

Caesar

Substitution (monoalphabetisch)

Die »normale« Caesar-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird.

Diese Verschlüsselung funktioniert so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort.
- Dieses Wort schreibst du unter ein normales Alphabet. Buchstaben, die doppelt vorkommen, lässt du dabei weg.
- Anschließend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt. Kein Buchstabe darf doppelt vorkommen.

Beispiel Schlüsselwort: GEHEIMSCHRIFT. Dieses Schlüsselwort wird unter das Alphabet geschrieben, doppelte Buchstaben werden dabei weggelassen.

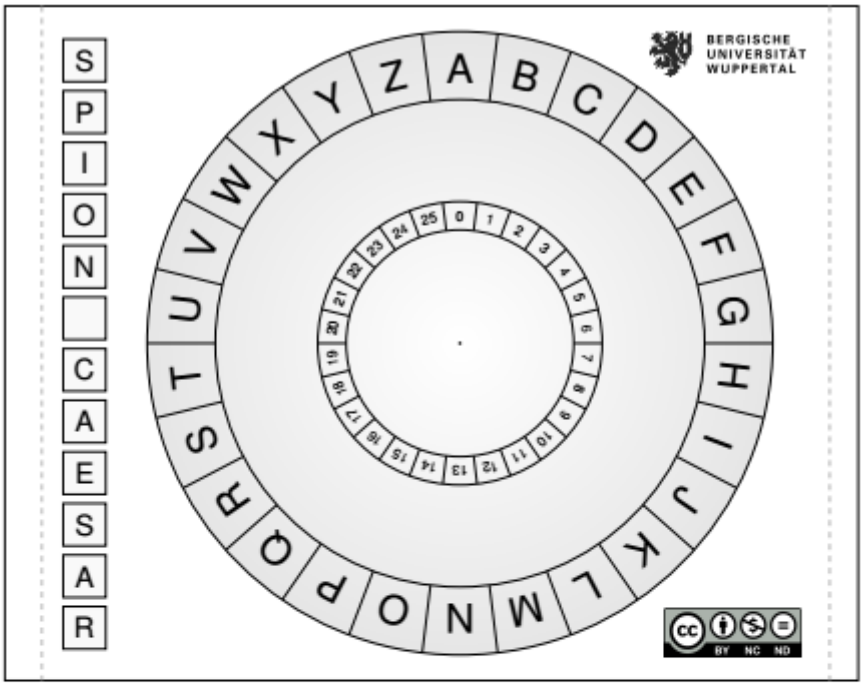
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
wird ersetzt durch	G	E	H	I	M	S	C	R	F	T																

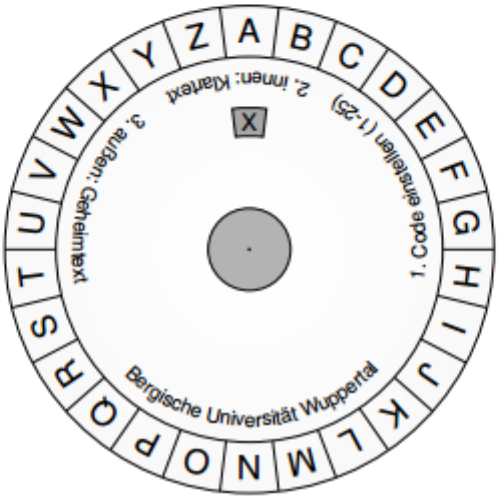
Nun wird mit den restlichen Buchstaben aufgefüllt.

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

Mit dieser Tabelle wird dann ver- und entschlüsselt.

v4 5. Juli 2013


BERGISCHE UNIVERSITÄT WUPPERTAL
S P I O N
C A E S A R
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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
BY NC ND


1. Code ersteller (1-25)
2. innen: Klartext
3. außen: Geheimtext
X
Bergische Universität Wuppertal
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

Aufgabe 1 Könnt ihr die Nachricht ohne bekannten Schlüssel entschlüsseln?
YHQL YLGL YLFL

Aufgabe 2 Entschlüsselt mit der Chiffrierscheibe die folgenden Nachrichten. Mögliche Schlüssel sind: **2**, **7**, **10**, **13**. Einer ist jeweils der richtige Schlüssel. Das heißt, dass man bei Verschiebung um diese Zahl die Nachricht erhält.

a) **SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU?**

b) **YVRORE PNRFNE, VPU JREQR QN FRVA.**

Aufgabe 3 Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

Aufgabe 4 Fällt dir eine Möglichkeit ein, wie du einen Text entschlüsseln kannst, ohne alle Schlüssel durchzuprobieren? *Tipp:* Nutze dabei eine bestimmte Eigenschaft einer Sprache (z. B. Deutsch) aus.

v3 5. Juli 2013

Lösung 1 **VENI VIDI VICI** (Lateinisch: Ich kam, ich sah, ich siegte. Dies schrieb Julius Caesar in einem Brief an Gaius Matius, nachdem er die Truppen Pharnakes II. von Pontus in nur vier Stunden besiegte.)

Lösung 2

a) Schlüssel 7:
LIEBE KLEOPATRA, TREFFEN WIR UNS BEI DEN PYRAMIDEN?

b) Schlüssel 13:
LIEBER CAESAR, ICH WERDE DA SEIN.

Lösung 3 Man muss höchstens 25 Schlüssel durchprobieren, um die Lösung zu erhalten.

Lösung 4 Häufigkeitsanalyse: In der Deutschen Sprache ist der häufigste Buchstabe das »E«. Der häufigste Buchstabe im Geheimtext könnte also dem E entsprechen.

v3 5. Juli 2013

5.2.2 Arbeitsblätter für das Thema Freimaurer

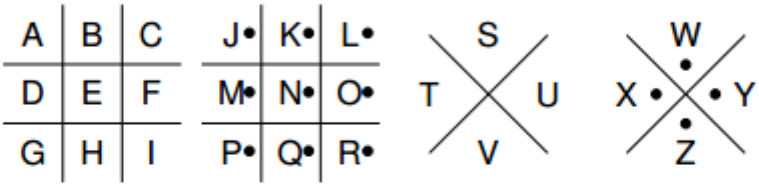
SPIONCAMP

Freimaurer

Substitution (monoalphabetisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Diese Verschlüsselung, die im 18. Jahrhundert von den Freimaurern - einem Geheimbund - benutzt wurde, funktioniert so:
Zunächst schreibt man eine beliebige Reihenfolge aller Buchstaben des Alphabets in vier bestimmte Muster. Im folgenden Bild wurde die Reihenfolge von A bis Z genommen.



Zum Verschlüsseln wird jeder Buchstabe durch die Linien und Punkte ersetzt, die ihn umgeben.

Beispiel Schau dir das Bild oben an. Die Linien und Punkte, die beim **N** stehen, sehen in etwa so aus: ⊡. **N** wird immer durch dieses Zeichen ersetzt.

v3 5. Juli 2013

SPIONCAMP

Arbeitsblatt

Freimaurer-Chiffre

Substitution (monoalphabetisch)

Aufgabe 1 Kannst du folgenden Text entschlüsseln?

Aufgabe 2 Schreibt euch eine Nachricht mit dem Freimaurer-Chiffre.

Aufgabe 3 Wie kann man ohne Schlüssel die Nachrichten entziffern?

v3 5. Juli 2013

Lösung 1 **VERSUCH DEIN GLUECK**

Lösung 3 Über eine Häufigkeitsanalyse. Man schaut nach, welches das häufigste Zeichen ist. Das könnte das »E« sein. Ebenso verfährt man mit dem zweithäufigsten Zeichen, und so weiter. Du brauchst dazu eine Tabelle, wie häufig jeder Buchstabe in einer bestimmten Sprache vorkommt. Ein Ausprobieren aller Kombinationen wäre viel zu aufwändig.

v3 5. Juli 2013

5.2.3 Arbeitsblätter für das Thema Pflügen

SPIONCAMP

Pflügen

Transposition

Die Buchstaben bleiben **was** sie sind, aber nicht **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Das Pflügen zeigt dir, wie man durch Anordnen und Neuordnen von Buchstaben verschlüsseln kann. Pflügen geht so:

- Lege fest, wieviele Buchstaben in eine Zeile geschrieben werden sollen. Das ist der Schlüssel.
- Schreibe deinen Text auf, aber in jede Zeile nur so viele Buchstaben, wie vorher festgelegt. Die letzte Zeile wird mit beliebigen Buchstaben aufgefüllt.
- Der verschlüsselte Text entsteht, indem du nun die letzte Spalte von unten nach oben aufschreibst, danach die vorletzte Spalte von oben nach unten und so weiter.

Beispiel Der Text **DER SCHATZ LIEGT UNTER DEN PALMEN** soll verschlüsselt werden. Du wählst als Schlüssel zum Beispiel die **6** und schreibst die Buchstaben so auf:

D	E	R	S	C	H
A	T	Z	L	I	E
G	T	U	N	T	E
R	D	E	N	P	A
L	M	E	N	X	X

Ist die Nachricht zu kurz, dann wird einfach mit beliebigen Buchstaben aufgefüllt, bis der Kasten voll ist. Wie der Pfeil zeigt, schreibst du die Buchstaben nun ab. Die Reihenfolge ähnelt dem Pflügen eines Felds.

D	E	R	S	C	H
A	T	Z	L	I	E
G	T	U	N	T	E
R	D	E	N	P	A
L	M	E	N	X	X

Du schickst die Nachricht **XAEEHCITPXNNNLSRZUEEMDTTEDAGRL** ab.

v4 – 5. Juli 2013

Aufgabe 1 Versuche, die folgende »gepflügte« Nachricht zu entschlüsseln. Der Schlüssel ist **6**.

X G C N E I T M I S R S E H I E H T C I D A H E

Aufgabe 2 Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (= Anzahl Buchstaben pro Zeile) entschlüsseln kannst.

Aufgabe 3 Schreibt euch gegenseitig eine Nachricht! Einigt euch auf den Schlüssel (= Anzahl Buchstaben pro Zeile)!

CC BY NC SA
v3 5. Juli 2013

Lösung 1 Der Schlüssel ist 6. Da der Text 24 Zeichen hat, ergibt sich daraus ein 6x4 Rechteck. Also fange ich nach dem Pflügen-Schema rechts unten mit dem »X« an und gehe von dort aus vier Zeichen nach oben, dann in Schlangenlinien die nächste Spalte nach unten, usw. So ergibt sich das folgende Schema:

```
D I E S E N
A C H R I C
H T I S T G
E H E I M X
```

Die Nachricht lautet: Diese Nachricht ist geheim.

Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Anhand des bekannten Schlüssels und der Nachrichtenlänge kann man die Größe des Rechtecks ermitteln. Der Schlüssel entspricht der Spaltenanzahl. Die Nachrichtenlänge geteilt durch den Schlüssel ergibt die Zeilenanzahl. In dieses Rechteck wird die verschlüsselte Nachricht nach folgendem Verfahren eingetragen: Man fängt nach dem Pflügen-Schema rechts unten mit dem ersten Buchstaben an und geht von dort aus die errechnete Zeilenanzahl nach oben, dann in Schlangenlinien die nächste Spalte nach unten und so weiter. Die Nachricht kann dann von links nach rechts und Zeile für Zeile gelesen werden.

Lösung 3 Allgemeine Lösung kann nicht vorgestellt werden.

v3 5. Juli 2013

5.2.4 Arbeitsblätter zum Thema Schablonen

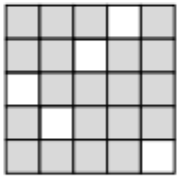
SPIONCAMP

Schablonen

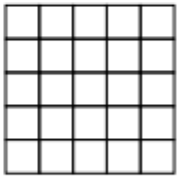
Transposition

Die Buchstaben bleiben **was** sie sind, aber nicht **wo** sie sind.
So eine Verschlüsselung heißt **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Du brauchst für die Schablonen-Verschlüsselung eine Lochschablone. Das ist ein Papier, das an bestimmten Stellen Löcher hat. Beide Personen, der Sender und der Empfänger, benötigen die gleiche Schablone.



Lochschablone

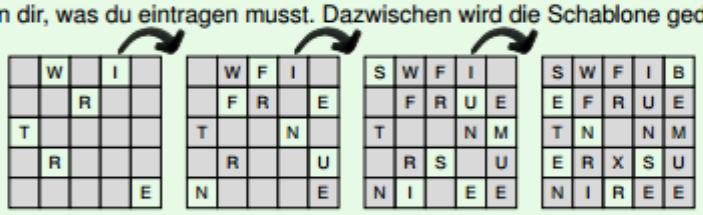


kariertes Papier

Mit dieser Art Schablone verschlüsselst du so:

- Du legst die Schablone auf ein leeres Papier und trägst die ersten Buchstaben der Nachricht in die Löcher ein.
- Danach drehst du die Schablone im Uhrzeigersinn um 90 Grad und trägst die nächsten Buchstaben der Nachricht ein.
- So fährst du fort, bis du alle vier Stellungen der Schablone benutzt hast. Ist die Nachricht länger, beginnst du mit einem neuen Quadrat. Ist sie kürzer, werden übrige Felder mit irgendwelchen Buchstaben gefüllt.
- Bei Schablonen mit ungerader Zeilen- und Spaltenanzahl bleibt immer ein Buchstabe in der Mitte frei. Dieser muss anschließend frei gewählt werden.

Beispiel Du möchtest z.B. den Text WIR TREFFEN UNS UM SIEBEN verschlüsseln (21 Buchstaben). Du brauchst eine Schablone, die alle Buchstaben aufnehmen kann, z.B. eine Schablone mit 5 Zeilen und 5 Spalten. Die folgenden Bilder zeigen dir, was du eintragen musst. Dazwischen wird die Schablone gedreht.



In der Mitte ist noch ein Buchstabe frei geblieben. Diesen kannst du beliebig setzen, z. B. »S«. Daraus ergibt sich dann der verschlüsselte Text SWFIBE-FRUETNSNMERXSUNIREE.

BERGISCHE UNIVERSITÄT WUPPERTAL

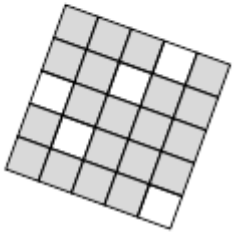
v3 – 5. Juli 2013

Aufgabe 1 Du findest an der Station einige verschlüsselte Nachrichten. Kannst du sie mit den Schablonen entschlüsseln?

Aufgabe 2 Schreibt euch gegenseitig eine Nachricht mit einer der Schablonen an der Station.

Aufgabe 3 Erkennst du das Muster, wie eine solche Schablone aufgebaut ist?
Überlege dir die Antwort anhand folgender Hilfsfragen: Wie dürfen die Löcher angeordnet sein? Wie viele Kästchen musst du ausschneiden, damit am Ende alle Kästchen komplett mit Buchstaben ausgefüllt sind? Wenn ein Kästchen ausgeschnitten ist, welche anderen Kästchen dürfen dann nicht ausgeschnitten werden?

Aufgabe 4 Entwirf selbst eine Schablone und verschlüssele mit deiner eigenen Schablone eine Nachricht.



v3 – 5. Juli 2013

Lösung 1

Text oben links:
DER BRIEF LIEGT IN DER UNTERSTEN SCHUBLADE (Schablone 3)
Text oben rechts:
DIE NACHRICHT ZERSTOERT SICH IN 5 SEKUNDEN (Schablone 1)
Text unten:
VORSICHT VOR DER EXPLOSION AUF DEM MARKT (Schablone 2)

Lösung 2

»eigene Lösung«

Lösung 3

Einen Vorschlag für die Lösung siehst du in der nachfolgenden Abbildung. Hier sind vier Ringe dargestellt. Du darfst bei der Schablonenproduktion aus jedem Ring jede Zahl nur einmal als Fenster verwenden.

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

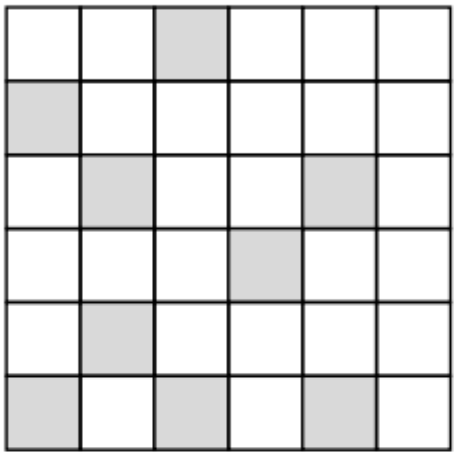
Du drehst die Schablone nach jedem Schritt um 90 Grad. D.h. du füllst viermal Kästchen aus oder liest diese aus. Also kannst du insgesamt ein Viertel der Kästchen ausschneiden.

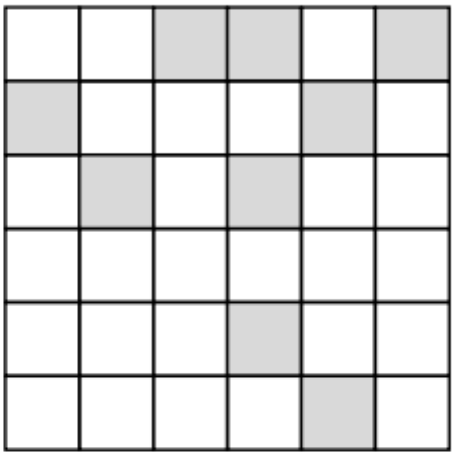
Lösung 4

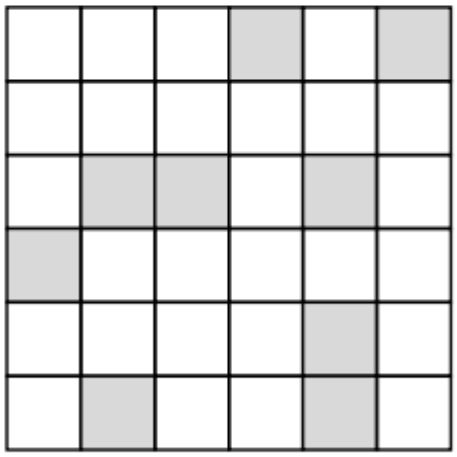
»eigene Lösung«

v3 – 23. September 2013

Vorlagen für Schablonen







CC BY NC SA v3

Texte zum Entschlüsseln

S	U	I	D	N	E	C	E	D	R	H	T
E	T	C	G	H	U	I	T	5	Z	S	S
B	R	B	T	R	E	E	E	I	E	N	R
I	R	L	S	T	I	K	C	S	A	H	U
N	D	A	E	E	D	T	C	N	O	D	I
E	F	N	E	L	R	H	E	R	N	I	N

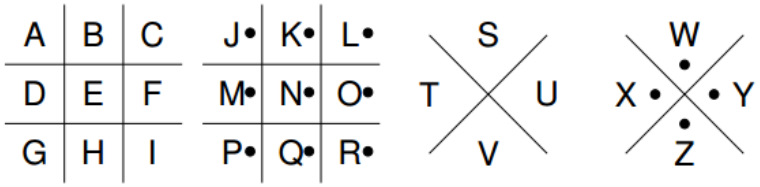
E	O	V	O	O	R
S	M	S	R	I	M
A	C	R	H	K	D
T	E	I	R	O	E
X	N	X	T	P	A
U	Y	F	D	V	L

v3 – 5. Juli 2013

5.2.5 Test

Test zu Transpositions- und Substitutionsverfahren

Aufgabe 1



Verschlüssele die folgende Nachricht mit der Freimaurer-Chiffre:

Klartext: WIR WERDEN SIEGEN

Geheimtext:_____

_____

Aufgabe 2

Der Caesar-Schlüssel entspricht n = 5. Chiffriere das folgende Wort:

Klartext: BONBON

Geheimtext:_____

Aufgabe 3

Wähle die wahren Aussagen zur Schablonen-Verschlüsselung aus.

- ☐ Empfänger und Sender benötigen dieselbe Lochschablone.
- ☐ Man dreht die Schablone im Uhrzeigersinn um 180 Grad.
- ☐ Übrige Felder dürfen nicht mit irgendwelchen Buchstaben gefüllt werden.
- ☐ Bei Schablonen mit ungerader Zeilen- und Spaltenanzahl bleibt immer ein Buchstabe in der Mitte frei.

Aufgabe 4

Verwende zum Transponieren das Pflügen-Verfahren. Es sollen 5 Buchstaben in eine Zeile geschrieben werden. Der Klartext lautet: SÜßIGKEITEN FÜR ALLE. Wie lautet der Geheimtext?

Geheimtext:_____

_____

Test - Lösung

Aufgabe 1

Geheimtext:

Aufgabe 2

Geheimtext: gtsgts

Aufgabe 3

Wahre Aussagen zur Schablonen-Verschlüsselung sind, die erste und vierte Aussage.

- Empfänger und Sender benötigen dieselbe Lochschablone.
- Bei Schablonen mit ungerader Zeilen- und Spaltenanzahl bleibt immer ein Buchstabe in der Mitte frei.

Denn:

- Man dreht die Schablone im Uhrzeigersinn um 90 Grad.
- Übrige Felder werden mit irgendwelchen Buchstaben gefüllt werden.

Aufgabe 4

Geheimtext: XAEGITRXEÜIßÜEFLLNKS

5.3 Kryptoanalyse

Thema: Kryptoanalyse

Zeit	**Phasen / Methode**	**Unterrichtsschritte/Lehrer-Schülerinteraktion**	**Sozialform & Handlungs-muster**	**Medien**
20 min	Einstieg	L. führt Kerckhoffs' Prinzip ein und arbeitet die verschiedenen Typen von Attacken mithilfe vom fragend-entwickelnder Unterricht heraus. L.: „Welche Voraussetzungen könnte ein Kryptoanalytiker haben?" Anschließend wird fragend-entwickelnd herausgearbeitet, wie man die Caesar-Chiffre knacken kann. → 25 Schlüssel ausprobieren & Häufigkeitsanalyse	Plenum Lehrervortrag und fragend-entwickelnder Unterricht	Tafel oder interaktives Whiteboard
50 min	Erarbeitung	L. teilt die S. in leistungsheterogene 3er-Gruppen auf. Alle Schülerteams erhalten dasselbe Arbeitsblatt.	Wettbewerbs-Methode Gruppenarbeit	AB, Stoppuhr
20 min	Ergebnis-sicherung	Mehrere Schüler erläutern den Lösungsweg an der Tafel → Fragen, Diskussionen Die Siegergruppe wird bekannt gegeben.	Plenum Schülervortrag	Tafel

5.3.1 Arbeitsblatt für das Thema Kryptoanalyse

Kryptoanalyse - Wettbewerb

Könnt ihr die folgenden Texte ohne bekannten Schlüssel entschlüsseln?

Aufgabe 1 (5 Punkte)

Ihr fangt eine Nachricht ab und möchtet herausbekommen, was darin steht. Ihr wisst, dass »Pflügen« als Verschlüsselungsverfahren verwendet wurde.

Hier ist die Nachricht:

H I H A N N K E G C E C A O I T K S A C S N S F N T R I A D

Schlüssel:_____

Klartext:_____

Aufgabe 2 (5 Punkte)

Der folgende Geheimtext wurde mit der Caesar-Chiffre verschlüsselt. Ermittelt den Schlüssel und den Klartext.

Geheimtext: **OTLUXSGZOQ**

Schlüssel:_____

Klartext:_____

Aufgabe 3 (10 Punkte)

Der folgende Geheimtext wurde ebenfalls mit der Caesar-Chiffre verschlüsselt. Ermittelt den Schlüssel und den Klartext. Tipp: Nutzt die Häufigkeitsverteilungen im Anhang.

Aiv vimxix ws wtäx hyvgl Reglx yrh amrh?
Iw mwx hiv Zexiv qmx wimriq Omrh.
Iv lex hir Orefir Aslp mr hiq Evq,
Iv jeßx mlr wmgliv, iv läpx mlr Aevq.

Schlüssel:_____

Klartext:_____

Anhang:

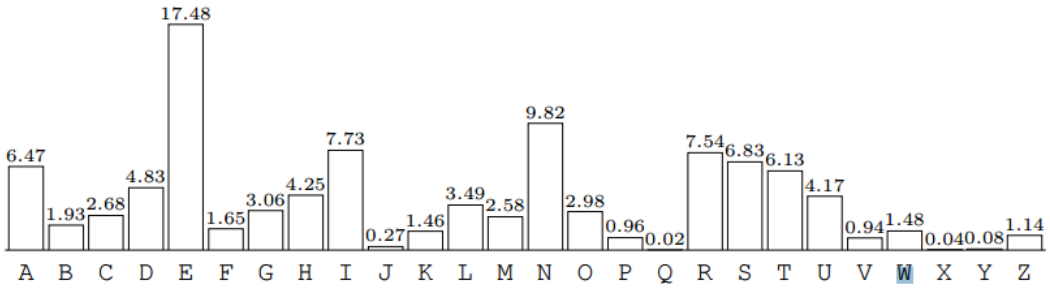


Abbildung 1 Häufigkeitsverteilung von Einzelbuchstaben im Deutschen (in %).

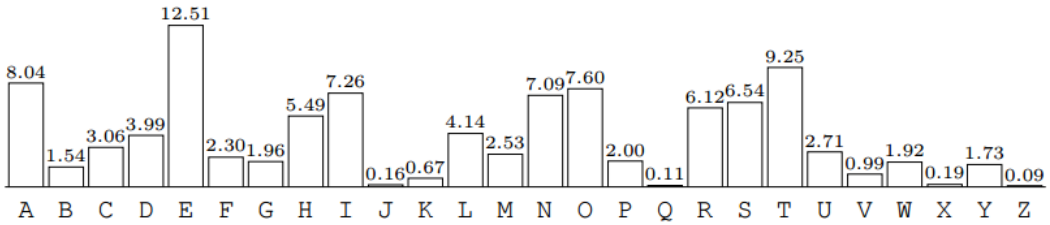


Abbildung 2 Häufigkeitsverteilung von Einzelbuchstaben im Englischen (in %).

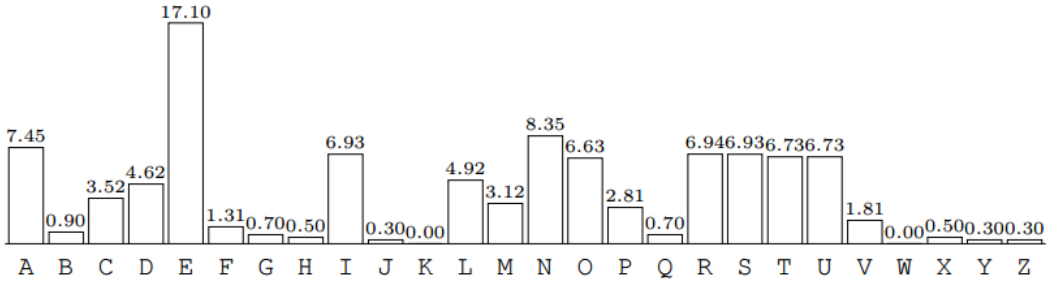


Abbildung 3 Häufigkeitsverteilung von Einzelbuchstaben im Französischen (in %).

Lösung

Aufgabe 1:

Es sind 30 Buchstaben, daher sind 5, 6 und 10 mögliche Schlüssel, welche man ausprobiert.

Schlüssel: 5

Klartext: DAS KNACKEN IST GAR NICHT SO EINFACH

Aufgabe 2:

Schlüssel: 6

Klartext: Informatik

Aufgabe 3:

Schlüssel:

Klartext:

Wer reitet so spät durch Nacht und Wind?

Es ist der Vater mit seinem Kind.

Er hat den Knaben wohl in dem Arm,

Er faßt ihn sicher, er hält ihn warm.

Ein Auszug aus dem „Erlkönig“ von Johann Wolfgang von Goethe.

5.4 Kryptographie: Polyalphabetische Substitution

Thema: Polyalphabetische Substitution

Zeit	**Phasen / Methode**	**Unterrichtsschritte/Lehrer-Schülerinteraktion**	**Sozialform & Handlungs-muster**	**Medien**
35 min	Einstieg	L. zeigt der Klasse die ARTE Dokumentation „Wie ein Mathegenie Hitler knackte“ bis zur Minute 27:56.	Filmeinsatz Plenum	PC mit Internet (Youtube), Beamer oder interaktives Whiteboard
40 min	Erarbeitung 1	Die S. sitzen im Doppelkreis. 1. Runde: die im Außenkreis sitzenden S. erzählen ihren im Innenkreis gegenübersitzenden Partner den Inhalt des Filmes. (12 min) 2. Runde: der zuhörende Partner fasst zusammen, , was sein Gegenüber erzählt hat, und fügt hinzu, was ihm noch aufgefallen ist. (8 min) Mit vertauschten Rollen und neuen Partnern wird die Übung wiederholt.	Kugellager-Übung Partnerarbeit	Stühle im Doppelkreis
15 min	Ergebnis-sicherung 1	Verschiedene S. werden aufgefordert, verschiedene Aspekte des Films zu erläutern. Wie ist die Funktionsweise der ENIGMA? Wer ist Alan Turing?	Plenum Lehrer-Schüler-Gespräch	

35 min	Erarbeitung 2	Alle Schülerpaare (die vorzugsweise leistungsheterogen sind) erhalten beide Arbeitsblätter zur Vigenère-Verschlüsselung. Sie lesen diese und eignen sich so das Verfahren an. Aufkommende Fragen und Diskussionen sollen erstmal untereinander geklärt werden. Anhand des zweiten Arbeitsblattes üben die S. das Verfahren.	Partnerarbeit	AB, Vigenère-Quadrat
15 min	Ergebnis-sicherung 2	S. wird aufgefordert, das Vigenère-Verfahren zu erläutern. Ein Beispiel wird gemeinsam an der Tafel chiffriert. Offene Fragen werden geklärt.	Plenum	Tafel, Vigenère-Quadrat
15 min	Erarbeitung 3	Jeder S. bekommt einen individuellen Abschnitt eines Geheimtextes, mit dem Auftrag diesen mit einem gegebenen Schlüsselwort zu dechiffrieren. Achtung: Beim Verteilen der Geheimtext-Abschnitte auf die Reihenfolge achten!	Einzelarbeit	Geheimtext-Schnipsel für jeden S., Vigenère-Quadrat
5 min	Ergebnis-sicherung 3	Die S. lesen ihre Klartexte nacheinander in der richtigen, vom Lehrer bestimmten, Reihenfolge vor.	Plenum	
20 min	Ergebnis-sicherung 4	Die Inhalte der Unterrichtsreihe sollen stichpunktartig mithilfe einer Redekette wiederholt und zusammengefasst. Der L. startet eine Redekette, indem er einen S. aufruft. 1) Codierung: Morsealphabet, Braille-Schrift, Winkeralphabet 2) Steganographie: Semagramme, Punktchiffren, musikalische Botschaften, computerbasiert Steganographie 3) Transposition: Skytale, Pflügen, Schablonen 4) Monoalphabetische Substitution: Freimaurer, Caesar-Chiffre 5) Polyalphabetische Substitution: ENIGMA, Vigenère-Chiffre	Redekette Plenum	

5.4.1 Arbeitsblätter für die Vigenère-Verschlüsselung

SPIQNCAMP

Vigenère

Substitution (polyalphabetisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. **Was** sie sind, ist immer wieder verschieden.
Solche Verschlüsselungen heißen **polyalphabetische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Poly* heißt *viel*.)

Der Franzose Blaise de Vigenère (1523 bis 1596, s. Bild) entwickelte ein Verschlüsselungsverfahren, das viele verschobene Alphabete verwendet. Dazu werden alle möglichen Alphabetverschiebungen untereinander geschrieben — das sind 26 Alphabete. Das Ganze heißt dann **Vigenère-Quadrat** (s. Material).

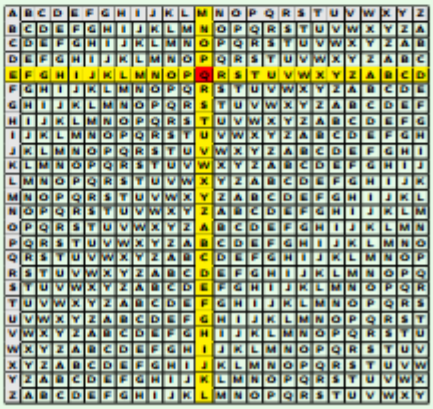
Verschlüsseln geht damit so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird unter die Nachricht geschrieben. Unter jeden Buchstaben der Nachricht wird ein Buchstaben des Schlüsselwortes geschrieben. Das Schlüsselwort wird dabei ständig wiederholt.
- Nun nimmt man sich jeweils einen Buchstaben der Nachricht und sucht ihn in der ersten Zeile des Vigenère-Quadrates. Von da aus geht man nach unten bis zu dem Alphabet, das ganz links mit dem entsprechenden Buchstaben des Schlüsselwortes beginnt.
- Der Buchstabe, den man dort findet, ist der verschlüsselte Buchstabe.

Beispiel

Nachricht:	MORGEN ABEND UM NEUN GEHTS LOS
Schlüsselwort:	EINFAC HEINF AC HEIN FACHE INF
Geheimtext:	QWELEP HFMAI UO UICA LEJAW TBX

(Bild: das erste **M** wird mit dem Schlüsselbuchstaben **E** verschlüsselt.)



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

CC BY NC SA

Aufgabe 1 Verschlüsselt euren Namen mit dem Schlüsselwort **HUT**.

Aufgabe 2 Entschlüsselt folgenden Text. Das Schlüsselwort ist **ROT**:
XIM XSFRQAK

Aufgabe 3 Beschreibe ähnlich zum Verschlüsseln, wie das Entschlüsseln funktioniert.

v3 5. Juli 2013

Vigenère-Quadrat

Nimm dir für die Ver- und Entschlüsselung ein Lineal oder Ähnliches zur Hilfe, damit du nicht in den Spalten und Zeilen verrutschst.

Klartext

Schlüsselbuchstaben

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

v1

Lösung 1 Z. B. **MARIE**:

```
MARIE
HUTHU
TUKPY
```

Lösung 2 **GUT GEMACHT**

Lösung 3 ...umgekehrt, wenn Buchstaben in einer Zeile/Spalte die Vorgänger...

Jedem Schüler wird ein anderer Abschnitt zum Dechiffrieren zugewiesen. Hier wurde der Text in 13 Abschnitte, also für 13 Schüler unterteilt.

Geheimtext-Abschnitte

Das Schlüsselwort ist „Sonne“.

1. Wbqymuv vfx
2. Kczzij iaq has
3. Iötid njvxkqurvf!
4. Rn qek Krgxwf
5. uryls fb wuvöa
6. vwl iaq ee
7. Kbplwbrahw
8. krvxwfuvr vwr
9. Fsfbr fgzsvax,
10. oweq Jjoh Tlgav
11. hrk vrhxw yrvrw
12. Vnhwsistetsa
13. nyxuroif.

Jeder Schüler trägt nacheinander seinen Klartext in der richtigen Reihenfolge vor.

Lösung der Geheimtext-Abschnitte

1. Endlich ist
2. Sommer und die
3. Vögel zwitschern!
4. Da das Wetter
5. heute so schön
6. ist und am
7. Wochenende
8. weiterhin die
9. Sonne scheint,
10. wird Frau Ghomi
11. uns heute keine
12. Hausaufgaben
13. aufgebenArbeitsblätter

6. Abbildungsverzeichnis

Abbildung 1: Tafelbild für die Einstiegsmethode Brainstorming 13

Abbildung 2: Punktchiffre in einem Kinderbrief 14

Abbildung 3: Musik-Code von Giovanni della Porta 15

Abbildung 4: Semagramm von US-Zensoren in San Antonio 16

Abbildung 5: Morsealphabet 17

Abbildung 6: Braille-Schriftzeichen, entnommen aus BAUER: *Historische Notizen zur Informatik*, Seite 101 18

Abbildung 7: Stationenlernen zum Thema Codierung und Steganographie 20

Abbildung 8: Skytale 21

Abbildung 9: Ein Beispiel für das Transpositionsverfahren Pflügen entnommen aus dem SpionCamp 22

Abbildung 10: Beispiel für die Schablonen-Verschlüsselung, entnommen aus dem SpionCamp 23

Abbildung 11: Freimaurer-Alphabet 24

Abbildung 12: Caesar-Chiffre mit n = 3 24

Abbildung 13: Chiffrierscheibe 25

Abbildung 14: Gruppen-Puzzle für zwei Substitutions- und zwei Transpositionsverfahren 26

Abbildung 15: Kommunikationsschema, entnommen aus Freiermuth: *Einführung in die Kryptologie,* S. 29 27

Abbildung 16: Vigenère-Quadrat entnommen aus SpionCamp 30

Abbildung 17: Beispiel für die Vigenère-Verschlüsselung, entnommen aus Beutelspacher: *Kryptologie,* S.35 30

Abbildung 18: ENIGMA, Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr. . 34

7. Tabellenverzeichnis

Tabelle 1: Kompetenzstufenmodell für die Leistungen der Schüler 3

Tabelle 2: Methodischer Grundrhythmus des Unterrichts von Hilbert Meyer 4

Tabelle 3: Überblick über die Themen und Methoden der Unterrichtsreihe..... 6

Tabelle 4: Auszug aus dem Lehrplan Informatik der Sekundarstufe I in Rheinland-Pfalz.... 7

Tabelle 5: Empfohlene Internetseiten mit Unterrichtsmaterialien 8

Tabelle 6: Haupt- und Teilziele des 1. und 2. Unterrichtsblocks 10

Tabelle 7: Haupt- und Teilziele des 3. Unterrichtsblocks 11

Tabelle 8: Haupt- und Teilziele des 4. Unterrichtsblocks 12

Tabelle 9: Haupt- und Teilziele des 5. und 6. Unterrichtsblocks 12

8. Literaturverzeichnis

Bauer, Friedrich L.: *Historische Notizen zur Informatik*, Springer-Verlag, 2009.

Beutelspacher: *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*, 10. Auflage, Springer Spektrum 2015.

Freiermuth, Hromkovic, Keller und Steffen: Einführung in die Kryptologie. Lehrbuch für Unterricht und Selbststudium, 2. Auflage, Springer Vieweg 2014.

Hartmann, W./ Näf, M./ Reichert, R.: *Informatikunterricht planen und durchführen,* Springer-Verlag Berlin Heidelberg, 2006.

Humbert, Ludger: *Didaktik der Informatik mit praxiserprobtem Unterrichtsmaterial*, 2. Auflage, Teubner Verlag Wiesbaden, 2006.

ISB: *Zusammenspiel von Unterrichtsmethoden – Methodiküberlegungen für den mathematisch-naturwissenschaftlichen Unterricht,* erarbeitet im Auftrag des bayerischen Staatsministeriums für Unterricht und Kultus, 1999.

Klein, Andreas: *Visuelle Kryptographie,* Springer-Verlag Berlin Heidelberg, 2007.

Köller, O. / Meyer, H.: *Was ist eine gute Lehrerin/ein guter Lehrer?*, Cornelsen Stiftung Lehren und Lernen, 2013.

Mattes, Wolfgang: *Methoden für den Unterricht - 75 kompakte Übersichten für Lehrende und Lernende,* Schöningh Verlag, 2004.

Meyer, Hilbert: *Einführung in die Arbeit mit unterrichtsmethodischen Kompetenzstufenmodellen, Ergänzung zur SECHSTEN LEKTION,* Abschnitt 3.4 (Seite 155-160 des LEITFADENS), Carl von Ossietzky Universität Oldenburg, 2007.

Meyer, Hilbert: *Leitfaden Unterrichtsvorbereitung*, 7. Auflage, Cornelsen Schulverlage, 2014.

Meyer, Hilbert: *Unterrichts-Methoden II: Praxisband*, 14. Auflage, Cornelsen Verlag Scriptor, 2008.

Meyer, Hilbert: *Unterichtsmethoden.* In: Kiper, H./ Meyer, H. / Topsch, W.: Einführung in die Schulpädagogik. Berlin 2002, S. 109-121.

Meyer, Hilbert: *Was ist guter Unterricht?,* 7. Auflage, Cornelsen Verlag Scriptor, 2011.

Nehls, U./Gleichmann, F.: *Steganographie,* Belegarbeit bei Prof. Dr. Blakowski, 2002.

Nuttelmann: *Geheime Mitteilungen? Ein Unterrichtsbeispiel zum Thema Kryptologie in einem Leistungskurs Informatik*, veröffentlicht in Schwill: Informatik und Schule: Fachspezifische und fachübergreifende didaktische Konzepte, Springer-Verlag, 1999, Seiten 219-230.

Ripplinger, Jürgen: *Wie Schulen soziales Lernen systematisch fördern können,* mehrwert gGmbH.

Schöningh: *Informatik 3*, Schöningh Verlag, 2013.

Singh*: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet,* 12. Auflage, Deutscher Taschenbuch Verlag GmbH 2014.

Spitz/Pramateftakis/Swoboda: *Kryptographie und IT-Sicherheit*, 2. Auflage, Vieweg+Teubner 2011

Schmeh, Klaus: C*odeknacker gegen Codemacher. Die faszinierende Geschichte der Verschlüsselung,* 3. Auflage, 2014.

Schmeh, Klaus: *Versteckte Botschaften - Die faszinierende Geschichte der Steganografie*, 1. Auflage, Heise Verlag Hannover, 2009.

Internetquellen[65]

Berliner Rahmenlehrplan der Informatik für die gymnasiale Oberstufe: (1. Auflage 2006) http://www.berlin.de/imperia/md/content/sen-bildung/unterricht/lehrplaene/sek2_informatik.pdf?start&ts=1429785405&file=sek2_informatik.pdf.

Lehrplan Informatik an Gymnasien und Integrierten Gesamtschulen in Rheinland-Pfalz, http://lehrplaene.bildung-rp.de/lehrplaene-nach-faechern.html?tx_abdownloads_pi1[action]=getviewcatalog&tx_abdownloads_pi1[category_uid]=260&tx_abdownloads_pi1[cid]=5786&cHash=8a1c0230bf08932ab529a9f0dcda7bda.

Humbert: Vorlesungsmaterialien zur Didaktik der Informatik – Sommersemester September 2008: http://ddi.uni-wuppertal.de/ddi-sommersemester-2008/

Carl von Ossietzky Universität Oldenburg, (Hilbert Meyer): Gruppen-Puzzle: http://www.staff.uni-oldenburg.de/hilbert.meyer/10643.html

SpionCamp von der Universität Wuppertal: http://ddi.uni-wuppertal.de/material/spioncamp.html

Grundlagen der Kryptologie, sowie Tools, Tutorials und Aktuelles: http://www.kryptowissen.de/

Anleitung für die klassischen Bsp. der Steganographie: http://www.blinde-kuh.de/geheim/geheimschrift.html

Berliner OSZ Handel, Fachbereich Informatik: http://www.oszhdl.be.schule.de/gymnasium/faecher/informatik/krypto/

Open-Source Lernprogramm: https://www.cryptool.org/de/

[65] Der letzte Zugriff auf alle Internetquellen war September 2015.

http://www.cryptool-online.org/, https://www.cryptoportal.org/

Einsteigerplattform: https://www.kryptographiespielplatz.de/index.php

Unterrichtsideen für alle Klassenstufen zum Thema Sicherheit (Microsoft): https://www.sicherheit-macht-schule.de/

Chiffrierscheiben zum Basteln: http://www.dtv-kinderbuch.de/_spiele_downloads/special_raetsel/Vorlage_Chiffrierscheibe.pdf?download=true

Aktuelles und Ratgeber über IT-Sicherheit für Unternehmen und Verbraucher: https://www.sicher-im-netz.de/

Kryptographie – RSA Lernpfad:
http://www.austromath.at/medienvielfalt/materialien/krypto/uebersicht.htm