Praktikumsbericht
- Schulpraktische Übungen (SPS III) -
Fach Informatik

Vorgelegt von: Marie Herrmann

Matrikelnummer: 3728824

Semester: 7. Fachsemester

Schule:	Schule am Weißeplatz	
Anschrift:	Ferdinand-Jost-Straße 33, 04299 Leipzig	
Telefonnummer:	0341/241 677 50	
Zeitraum (von - bis)	28.04.2022	09.06.2022
Mentor:	Frau Mandy Menschner	
Vertreter der Fachdidaktik:	Herr Jörg Erbsmehl	

Universität Leipzig

Fakultät für Mathematik und Informatik
Professur für Didaktik der Informatik

31.07.22

Inhaltsverzeichnis

1. Analysen 3
1.1. Schulsituation 3
1.2. Klassensituation 3
1.3. Darstellung der technischen Unterrichtsbedingungen 4
1.4. Lehrplan – Lernzielebenen 6
1.5. Sach-/Fachanalyse 7
2. Planungsentwurf einer Unterrichtseinheit 10
2.1. Ziele der Unterrichtsstunde vom 12.05.2022 10
2.2. Vorüberlegungen zum Stundenverlauf 10
2.3. Didaktisch-methodische Vorüberlegungen 11
3. Tabellarische Verlaufsplanung der Unterrichtsstunde vom 12.05.2022 12
4. Schriftliche Nachbereitung 16
4.1. Reflektion über den Unterrichtsversuch 16
4.2. Ausblick 17
Anhang Eingesetzte Unterrichtsmittel / Medien i
I. Arbeitsblatt Kryptografie i
II. Stundenthema Schlüssel iv
III. Präsentation iv
Literaturverzeichnis viii
Quellenverzeichnis viii
Eigenständigkeitserklärung ix

1. Analysen

1.1. Schulsituation

Die *Schule am Weißeplatz*, ist eine Oberschule der Stadt Leipzig und liegt im Stadtteil Stötteritz. Zwei sich gegenüberstehende Häuser bilden den Rahmen für den Schulhof und das Schulgelände. 2015 wurde der Anbau zur Vergrößerung der Schule fertig gestellt und im Laufe der Jahre, wurde das Schulgelände immer weiter modernisiert. Außerdem besitzt sie eine eigene Turnhalle und einen Sportkäfig an der frischen Luft. Die Jahrgänge sind zweizügig und gehen von der 5. bis zur 10. Klasse.
Eine Besonderheit der Schule ist, dass sie eine von vier M.I.T.-Schulen in Leipzig ist. Die anderen Schulen, sind das Gerda-Taro-Gymnasium, die 68. Oberschule und die Lene-Voigt-Oberschule. M.I.T.-Schulen verfolgen ein Schulkonzept, dass ein erweitertes Angebot mit den Schwerpunkten digitale **M**edien, **I**nformatik und digitale **T**echnik anbietet. Anfang 2021 ist die erste fünfte Klasse mit dem M.I.T.-Zweig gestartet und bis Ende 2027 soll der Vollausbau der Sekundarstufe 1 für alle Klassenstufen erfolgreich fertiggestellt sein.
Der Stundenplan, geht von der 1. bis zur 10. Stunde. Die 2. und 3. Stunde können als Blockstunde gehalten werden, ebenso wie die 4. und 5. Stunde. Alle weitern Stunden sind als Einzelstunden angelegt. Für die heißen Tage im Jahr, gibt es verkürzte Unterrichtszeiten, bei denen alle Unterrichtsstunden (45 Minuten) auf 30 Minuten gekürzt werden.
Ab der 7. Stunde gibt es für die Schüler:innen die Möglichkeit an Ganztagsangeboten teilzunehmen. Neben den diversen Sportangeboten wie Kraftrainung und Fußball, gibt es unter anderem auch Angebote wie Töpfern, DJ School, Betreute Lernzeit und Robotik. Insgesamt gibt es ca. 31 verschiedene GTAs die besucht werden können. Es gibt keine Pflicht an einer GTA teilzunehmen, aber wenn man sich nach den Schnupperterminen für eine entscheidet, ist die wöchentliche Teilnahme Pflicht.
Um das Lehrangebot zu unterstützen, sind Klassenräume mit interaktiven Tafeln (nicht alle) ausgestattet, es stehen Beamer zur Verfügung, es gibt zwei PC-Pools, einen Klassensatz Tablets und einen Klassensatz Laptops. Außerdem gibt es in den Räumen Internet über LAN und WLAN.

1.2. Klassensituation

Während der Schulpraktischen Übung durften wir in der 8a unsere Unterrichtsversuche halten. Da im Informatikunterricht die Klassen halbiert werden, waren es 11 Schüler:innen die wir unterrichten durften, sechs Mädchen und fünf Jungen.
Alle Annahmen, die in diesem Abschnitt getroffen werden, beruhen auf eigenen Beobachtungen, die in den vergangenen Wochen gemacht werden konnten und auf dem Austausch mit den Kommilitonen und Betreuern.
Das Fachinteresse scheint im Allgemeinen in meinen Augen normal ausgeprägt zu sein, sie finden es nicht uninteressant aber ihr Lieblingsfach scheint es auch nicht zu sein. Die Schüler Julian, Jason und Felix, zeigen ein etwas größeres Interesse.
Beim Leistungsniveau lässt sich sagen, dass die Schüler:innen alle ein sehr ähnliches Level haben. Yana und Fabian, stechen hier insofern etwas raus, als das Yana aus einer ehemaligen

DAZ-Klasse (Deutsch als Zweitsprache) kommt, ihre Aufgaben gut und ordentlich machen möchte und deshalb etwas mehr Zeit benötigt. Bei Fabian sind es Konzentrationsschwierigkeiten, bei etwas längeren komplexen Aufgaben, verliert er leicht die Aufmerksamkeit und lässt sich vom Internet oder den Mitschülern ablenken.
Die Einschätzung des sozialen Verhaltens und der Sozialkompetenzen der Schüler:innen fällt etwas schwer. Unteranderem, weil es sich nur um eine Hälfte der Klasse handelt. Die Jungs und Mädchen bleiben mit ihren Gesprächen und Hilfestellungen eher unter sich. Alle gehen so weit in dem Alter erwartbar respektvoll miteinander um.

Bei den Kompetenzen werden im Folgenden nur die Zusammenhänge erwähnt, die besonders herausstechen, da sich die Schüler:innen alle auf einem annähernd gleichen Niveau befinden. Beginnend mit der Fachkompetenz, das Thema was behandelt wurde, war für alle Schüler:innen neu, somit konnten sie nicht viel Vorwissen vorzeigen. Anhand einer Rechercheaufgabe zu den Verschlüsselungsverfahren, war es möglich einen kleinen Einblick in die Methodenkompetenz zu bekommen, da teilt sich die Klasse etwas. Einigen fällt es leichter, die wichtigsten Informationen aus einem Text zu ziehen und in geeigneter Form zu präsentieren, anderen fällt dies ein wenig schwerer. Zur Sozialkompetenz lässt sich sagen, dass alle auf einem recht ähnlichen Level sind, auf Grund der pubertären Entwicklung versuchen alle ihre Stimme zu finden. Einige sind ruhiger und zurückhaltender (Julie, Diana, Angeline, Yana, Fabian), andere sind ein wenig dominanter und Mitteilungsfreudiger (Marvin, Vianne, Lilly). In Punkto Selbstkompetenz sticht (zumindest verbal) Marvin heraus der, sobald er eine Aufgabenstellung nicht verstanden hat, gleich in die Defensive geht. Nach dem Motto, bevor ich hier was falsch mache, mach ich es lieber gar nichts. Positiv hervorgehoben werden kann an der Stelle Jason, der sowohl bei der Selbstkompetenz als auch bei der Sozialkompetenz, seinen Mitschüler:innen etwas voraus scheint. Er hat einen höflichen Umgang mit alles, ist hilfsbereit, auch wenn nicht gerade nett mit ihm gesprochen wird, nimmt sich aber auch zurück oder wehrt sich angemessen, wenn es Zuviel wird.

1.3. Darstellung der technischen Unterrichtsbedingungen

Der PC-Pool in dem unterrichtet wurde ist mit 16 Computerarbeitsplätzen für Schüler:innen und einem Computerarbeitsplatz für die Lehrperson ausgestattet. Dabei sitzen die Schüler:innen seitlich zur Lehrperson. Im Raum stehen außerdem noch ein Beamer und ein Whiteboard zur Verfügung.
Auf den Computern läuft Windows 10 und als pädagogische Software kann INES benutzt werden. Über INES ist es möglich die PCs der Schüler:innen zu steuern, zum Beispiel um das Internet an den einzelnen Geräten ein und auszuschalten, alle oder einzelne Bildschirme zu sperren oder Dateien an die Schüler:innen zu verteilen. Um Dateien an die Lernenden auszugeben, gibt es zwei Möglichkeiten. Eine ist, diese im LernSax in die entsprechende Gruppe hochzuladen oder sie über das Schulnetzwerk mit INES in den *incoming* Ordner zu laden. In beiden Fällen laden die Jugendlichen die Datei herunter und speichern sie in ihrem eigenen Ordner ab. Außerdem steht noch ein Klassensatz Tablets zur Verfügung, falls für Aufgaben ein weiteres digitales Endgerät benötigt wird.


Withboard und
Beamerfläche
Schrank
Garderobe
Schrank mit
Drucker
Regal für
Schultaschen

1.4. Lehrplan – Lernzielebenen

Die Schule am Weißeplatz hat bereits in diesem Schuljahr 2021/22 nach dem ab 01. August 2022 geltenden Lehrplan unterrichtet. Auf diesen werde ich mich in meinem Bericht beziehen. Die Jahresziele werden im Lehrplan in fünf Kategorien unterteilt und lauten wie folgt.

Modellieren und Implementieren

> Die Schüler erkennen Algorithmen anhand ihrer Eigenschaften. An Beispielen erfassen sie die Grenzen der Algorithmierbarkeit und Berechenbarkeit.
>
> Die Schüler modellieren Lösungen zu einfachen Problemen mit Hilfe von verschiedenen Darstellungen eines Algorithmus und implementieren diese in einer didaktisch reduzierten Programmierumgebung. Dabei nutzen sie die Phasen des Problemlöseprozesses.
>
> Die Schüler modellieren einfache Netzwerke.

Begründen und Bewerten

> Die Schüler analysieren ihre entwickelten Modelle bezüglich Realisierbarkeit. Sie gehen zielgerichtet mit Fehlermeldungen des Systems um.
>
> Die Schüler begründen die Funktionsfähigkeit von Netzwerken und bewerten deren Bedeutung für die gegenwärtige und zukünftige Gesellschaft.

Strukturieren und Vernetzen

> Die Schüler übertragen ihr Wissen zu algorithmischen Grundstrukturen auf die Lösung einfacher Probleme in didaktisch reduzierten Programmierumgebungen.
>
> Sie kennen den Aufbau und die Struktur einfacher technischer Datennetzwerke.

Kommunizieren und Kooperieren

> Die Schüler arbeiten während des Problemlöseprozesses kooperativ zusammen. Sie erkennen, wie die Nutzung von Informatiksystemen das gesellschaftliche Umfeld verändert und beziehen dabei ökologische, ökonomische und soziale Aspekte ein.

Darstellen und Interpretieren

> Die Schüler nutzen bei der Beschreibung eines Algorithmus verschiedene Darstellungsformen.
>
> Sie präsentieren die Ergebnisse ihrer implementierten Lösung unter Nutzung geeigneter informatischer Werkzeuge. [LA22a]

Die zwei gehaltenen Informatikstunden, waren Teil des Lernbereich 2 *Netzwerke in der Informatik* und behandelten das Thema *Kryprografie*. Die Ziele dafür sind in dem Lernbereich sind wie folgt formuliert.

Kennen der Grundlagen der Kryptografie und Verschlüsselung im historischen Kontext

- Begriff Kryptografie
- Klartext, Geheimtext und Schlüssel

- einfache symmetrische Verschlüsselungsverfahren Substitution

Anwenden von Kryptografie und Verschlüsselung in der Gegenwart. [LA22a]

1.5. Sach-/Fachanalyse

Kryptografie ist die Wissenschaft der Verschlüsselung (altgriechisch *kryptós* = verborgen oder geheim und *gráphein* = schreiben). Ihre Ursprünge liegen schon im Mittelalter in der Verschlüsselung der Nachrichten von Diplomaten und Gelehrten. Damals ging es rein um die Vermeidung des unbefugten Lesens von Nachrichten und deren Manipulation.

Die Kryptografie ist mit eine der Wissenschaften, die sich mit der Weiterentwicklung der Technik und der Digitalisierung, ebenfalls immer wieder neu gedacht werden muss. So beschäftigt sich die moderne Kryptographie nicht mehr nur mit der Verschlüsselung von Nachrichten, sondern im Allgemeinen mit der Konzeption, Definition und Konstruktion der sicheren Verarbeitung und Speicherung von Informationen (Informationssicherheit). Die detaillierten Ziele, lassen sich in vier Punkte unterteilen.

1. Vertraulichkeit durch Zugriffsschutz: Ausschließlich bestimmte, berechtigte Personen beziehungsweise Empfänger dürfen in der Lage sein, Nachrichten oder Daten zu erhalten und zu lesen.
2. Integrität bedeutet Schutz vor Änderung: Es muss sichergestellt sein, dass die Daten vollständig und unverändert beim Adressaten eingetroffen sind.
3. Authentizität und Fälschungsschutz: Der Absender der Daten beziehungsweise der Nachricht muss eindeutig und nachprüfbar identifizierbar sein.
4. Verbindlichkeit: In der Konsequenz von Punkt 3 darf der Datenabsender keine Möglichkeit haben, seine Urheberschaft abzustreiten. Es geht hierbei um den grundsätzlichen und eindeutigen Nachweis der Urheberschaft.
   [LA22b]

Im Wesentlichen gibt es zwei Arten von Verschlüsselungsverfahren, symmetrische und asymmetrische. Bei der symmetrischen Verschlüsselung wird die Ver- und Entschlüsselung zwischen Empfänger und Sender mit demselben Schlüssel durchgeführt. Bis in die 1970er Jahren wurden ausschließlich symmetrische Verfahren verwendet. Anders als bei den symmetrischen Verfahren gibt es bei den asymmetrischen ein Schlüsselpaar. Vereinfacht gesagt, wird ein Schlüssel (public key) zum Verschlüsseln und ein anderer Schlüssel (private key) zum Entschlüsseln verwendet. Damit wird sichergestellt, dass nur der rechtmäßige Empfänger die Daten und Nachrichten lesen kann.

Um den Kern der Kryptografie in meiner Unterrichtsstunde zu erfassen, den Schüler:innen Verfahren an die Hand zu geben, mit denen sie selbst Nachrichten verschlüsseln können und die Lernziele aus dem Lernplan mit einzubinden, muss das Thema deutlich reduziert werden. Ich habe mich dabei hauptsächlich auf drei einfache historische Verschlüsselungsverfahren, sowie die Definition, die wichtigsten Begriffe und die Ziele (wie weiter oben bereits beschrieben) der Kryptographie beschränkt.

Definition Kryptografie:

- altgriechisch *kryptós*, deutsch -> verborgen, geheim und g*ráphein*, deutsch -> schreiben

Ursprünglich die *Wissenschaft der Verschlüsselung* von Informationen. Heute befasst sie sich auch allgemein mit dem Thema *Informationssicherheit*, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.

Die wichtigsten Begriffe:

Der *Schlüssel* wird zum Ver- und Entschlüsseln der Nachricht benötigt. Er definiert wie die Nachricht verschlüsselt und damit auch entschlüsselt wird.

Der *Geheimtext* ist die verschlüsselte Nachricht, die verschickt wird, damit kein Unbefugter die Nachricht lesen kann.

Der *Klartext* ist die unverschlüsselte Nachricht, die der Empfänger lesen soll.

Historische Verschlüsselungsverfahren

Skytale:

Woher kommt dieses Verschlüsselungsverfahren?

Die Spartaner (ca. 500 v. Chr.) nutzten eine Skytale (griechisch für «Stock» oder «Stab»), um wichtige militärische Botschaften zu übermitteln.

Wie wird verschlüsselt?

Der Absender wickelte einen Streifen aus Pergament oder Leder spiralförmig um die Skytale und schreibt die Nachricht längs auf das aufgewickelte Band. Auf dem abgewickelten Streifen, steht nun eine scheinbar sinnlose Buchstabenfolge.

Wie wird entschlüsselt?

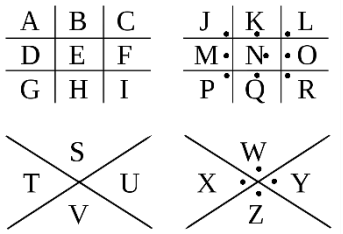
Der Empfänger bekommt den Pergament- oder Lederstreifen und kann die Botschaft mit einer Skytale vom selben Durchmesser, auf dem die Nachricht geschrieben wurde, wieder entziffern.

Freimaurer Code:

Woher kommt dieses Verschlüsselungsverfahren?

Der wahre Ursprung ist unbekannt. Es wird angenommen, dass sie bereits in der Antike benutzt wurde. Es gibt auch Hinweise, dass die Tempelritter sie während der christlichen Kreuzzüge im Mittelalter verwendet haben. Einige Freimaurer benutzten bis in die Neuzeit die Chiffren, um Aufzeichnungen, Riten und Nachrichten privat zu halten

Wie wird verschlüsselt?



Die Kernelemente dieses Systems sind die Raster und Punkte, in die das Alphabet verteilt wir. Es gibt unterschiedliche Varianten der Verteilung der Buchstaben, wobei die Struktur und Elemente gleichbleiben. Der Schlüssel besteht aus einem Gitter (siehe Grafik links). Beim Verschlüsseln wird das Umfeld des Buchstaben abgeschrieben.

Wie wird entschlüsselt?

Beim Entschlüsseln wird das geschriebene Symbol gesucht und der Klartext-Buchstabe aufgeschrieben.

Caesar Chiffre:

Woher kommt dieses Verschlüsselungsverfahren?

Der Namen kommt vom römischen Herrscher Julius Caesar, der so seine geheimen Botschaften versendet hat.

Wie wird verschlüsselt?

- Alphabet wird um einen bestimmten Wert verschoben
- Der Klartext-Buchstabe wird einem Geheimbuchstaben zugeordnet und aufgeschrieben

Wie wird entschlüsselt?

- Alphabet wird um einen bestimmten Wert verschoben (gleicher Wert wie bei der Verschlüsselung)
- Geheimbuchstaben suchen und den zugeordneten Klartext-Buchstaben aufschreiben

Beispiel: Verschiebung um 5 (k = 5)

Klartext-Alphabet: 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
Geheim-Alphabet: 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

Klartext: GUTEN MORGEN
Geheimtext: BPOZI HJMBZI

2. Planungsentwurf einer Unterrichtseinheit

2.1. Ziele der Unterrichtsstunde vom 12.05.2022

In den Bildungsstandards der Informatik, kommt die Kryprografie im speziellen nicht mit vor. Was aber mit ihr Hand in Hand geht, ist der Datenschutz. Unter dem Inhaltsbereich Informatik, Mensch und Gesellschaft ist folgende Kompetenz zu finden: Schülerinnen und Schüler (verwenden und) beschreiben Verfahren zur Sicherung von Vertraulichkeit, Authentizität und Integrität von Daten. [GE16, S. 12]
Wobei es sich hier um den Prozessbereich *Kommunizieren und Kooperieren*, mit Anforderungsbereich I Reproduktion handelt. Die Schülerinnen und Schüler erschließen aus leicht erfassbaren Texten und Diagrammen Informationen mit informatischem Gehalt und geben einfache informatische Sachverhalte unter Benutzung der Fachsprache schriftlich oder mündlich wieder. [GE16, S. 8]

Die Lernziele für diese Einführungsstunde zum Thema Kryptografie, wurden wie folgt formuliert.

Kognitive Ziele

Schüler:innen lernen den Begriff Kryptographie kennen.

Schüler:innen bekommen einen Einblick in die Notwenigkeit von Kryptographie.

Schüler:innen lernen verschiedene Kryptographie-Verfahren kennen.

Psychomotorische Ziele

Schüler:innen vertiefen den Gebrauch von Maus und Tastatur.

Schüler:innen vertiefen das Navigieren im Dateiverzeichnis der Schule.

Schüler:innen vertiefen das Öffnen und Abspeichern von Dateien.

Affektive Ziele wurden keine formuliert.

2.2. Vorüberlegungen zum Stundenverlauf

Zuvor ging es um die Themen *Übertragungsgeschwindigkeiten* und *Wie funktioniert das Internet*. Von allen SPÜ-Stunden, die in dieser Klasse gehalten wurden, war das die Erste und mit ihr hat der neue Themenkomplex *Kryptografie* begonnen. Damit konnte in die Stunde neu gestartet werden und es gab keinen Zwang Inhalte der letzten Stunde aufzugreifen und weiterzuführen. Außerdem sollte die nächste Stunde dieses Thema weiterführen. In der dritten und vierten Stunde soll es dann weiter um sichere Passwörter und sichere Netzwerke gehen. Eine Lernerfolgskontrolle wurde am Ende dieser Stunde und auch am Ende der SPÜ-Stunden nicht geplant.

2.3. Didaktisch-methodische Vorüberlegungen

Im Kern geht es bei der Kryprografie darum, dass Nachrichten nur von bestimmten Personen(gruppen) gelesen werden sollen. Um das zu erreichen, werden die Nachrichten verschlüsselt und Personen mit dem richtigen Schlüssel können dann den Klartext lesen. Zum Unterstreichen dieser Tatsache habe ich mich dazu entschieden das Stundenthema zu verschlüsseln und nur ausgewählten Schüler:innen den Schlüssel zugeben. Diese Schüler:innen können dann relativ einfach das Thema entschlüsseln, wo hingegen die anderen mehr überlegen müssen oder gar nicht auf die Lösung kommen. In einem Unterrichtsgespräch, soll gemeinsam die Lösung besprochen werden und warum es einige leichter hatten als andere das Wort zu entziffern.

Es folgt eine Mischung aus Frontalunterricht und Unterrichtsgespräch. Ziel des Unterrichtsgesprächs ist es herauszufinden, welches Vorwissen die Schüler:innen mitbringen. Nach dem kurzen Gespräch folgt ein kurzer Lehrervortrag zur Definition und Nutzung der Kryptografie. Die Form des Lehrervortrags wurde hier gewählt, um den Schüler:innen einen schnellen prägnanten Überblick zu geben. Alternativ wäre es an der Stelle auch möglich gewesen, dass einer der Lernenden viel Vorwissen hat und mit den eigenen Worten Kryptografie erklären kann. In diesem Fall hätte die Präsentationsfolie anschließend als Zusammenfassung oder Ergänzung gedient.

Ein weiteres Ziel für die Stunde ist, dass die Schüler:innen verschiedenen einfache Verschlüsselungsverfahren kennen lernen. Damit die Lernenden selbst aktiv werden und die Lehrperson nicht alles vorträgt, ist dafür eine Recherchearbeit geplant. In einer abgewandelten Form des Gruppenpuzzles. Damit nicht jeder alles Recherchieren muss, gibt es drei Gruppen die zu den Themen Freimaurer Code, Caesar Chiffre und Skytale Fragen auf einem Arbeitsblatt beantworten müssen. Damit alle arbeiten, ist die Recherche als Einzel- und Stillarbeit angelegt. Das heißt die Gruppen arbeiten nicht direkt zusammen, sondern die Einteilung dient nur zur Orientierung wer welches Thema bearbeitet. Um das Verantwortungs- und Pflichtbewusstsein der Schüler:innen anzusprechen, sind sie dafür verantwortlich ihr Thema gut zu bearbeiten, um ihren Mitschüler:innen dieses anschließend ordentlich und strukturiert erklären zu können. Die Verschlüsselungsverfahren, die nicht selbst bearbeitet wurden, sollen ergänzt werden, während die Mitschüler:innen sie erklären. Der Rechercheteil, soll das Erfassen, Kürzen und Wiedergeben von Texten und Sachverhalten schulen. Ziel ist es auch die Schüler:innen dahingehend zu fordern, dass sie sich Informationen auch mal selbst beschaffen müssen und nicht von der Lehrperson vorgegeben bekommen was wichtig und richtig ist. Beim Vorstellen der Verschlüsselungsverfahren durch die Schüler:innen geht es auch darum in einer entspannteren Atmosphäre (nicht sehend vor der Klasse, sondern sitzend am Platz), Wissen strukturiert an die anderen weiterzugeben. Alternativ wäre es auch möglich gewesen eine „*Hands on“* Variante zu erstellen bei der anhand eines Beispiels die Ver- und Entschlüsselung erarbeitet werden soll. Ich habe mich aktiv gegen diese Möglichkeit entschieden, da zum einen die zweite Stunde eine aktivere werden soll und zum anderen ich die Schüler:innen damit herausfordern will.

3. Tabellarische Verlaufsplanung der Unterrichtsstunde vom 12.05.2022

Uhr-zeit	Unterrichts-schritt	Lehrerin und Schüler:innen Handlung	Methode, Sozialform	Mittel	Bemerkungen
13:15 0'	Vor dem Unterricht	Lehrerin Handlung • verteilt an einen Teil der Schüler:innen einen "Schlüssel" • öffnet die Präsentation • verteilet die Dokumente im Laufwerk an die Schüler:innen-PCs Schüler:innen Handlung • hängen ihre Jacken auf • stellen ihre Taschen hinten ins Regal • packen einen Stift und das Hausaufgabenheft aus • lassen die Rechner ausgeschaltet		Schlüssel, Beamer, USB-Stick, Word-Datei	
13:15 3'	Begrüßung	Lehrerin Handlung • fordert die Schüler:innen auf sich ruhig an ihren Platz zu stellen. • begrüßt die Schüler:innen und lässt sie sich hinsetzten • stellt sich vor Schüler:innen Handlung • sehen nach vorn und hören zu	Lehrervortrag		

13:18 3'	Ausrichtung	Lehrerin Handlung • öffnet die nächste Folie der Präsentation • fragt die Schüler:innen wer die Überschrift lesen kann Schüler:innen Handlung • sehen nach vorn auf die Präsentation • versuchen die Überschrift zu lesen • ein Teil kann die Überschrift lesen mit Hilfe des Schlüssels (vor der Stunde bekommen)	Frontalunterricht, Unterrichtsgespräch	Beamer, Präsentation, "Schlüssel"	
13:21 5'	Information	Lehrerin Handlung • löst den Inhalt der Überschrift auf • Fragen: Was versteht ihr unter Kryptographie? Woher kennt ihr Verschlüsselungen? • deckt mit den Antworten der Schüler:innen die Präsentation nach und nach auf • Definition Kryptographie • Nutzen von Kryptographie Schüler:innen Handlung • sehen nach vorn • versuchen die Fragen der Lehrperson zu beantworten	Frontalunterricht, Unterrichtsgespräch, Lehrervortrag	Beamer, Präsentation	

13:26 3'	Vorbereiten für Stillarbeit	Lehrerin Handlung • Handlungsablauf der Schüler:innen über Beamer anzeigen (Rechner starten -> Anmelden -> Datei aus Verzeichnis öffnen -> Datei im Informatikordner Speichern -> Datei offen halten -> warten wie weiter) Schüler:innen Handlung • folgen dem Handlungsablauf	Stillarbeit	Schüler:innen Rechner, Präsentation, Word-Datei	
13:29 10'	Information, Verarbeitung	Lehrerin Handlung • Hinweis auf die Wichtigkeit des Word-Dokuments, wichtig für die folgende Stunde • teilt den Schüler:innen Verschlüsselungsverfahren zu, zu denen Sie recherchieren sollen und die Word-Datei füllen sollen (Skytale, Freimauerchiffre, Caesar-Chiffre) Schüler:innen Handlung • recherchieren zu dem ihnen zugeteilten Verschlüsselungsverfahren • ergänzen die Word-Datei mit den von ihnen gefundenen Informationen Woher kommt das Verschlüsselungsverfahren? Wie wird verschlüsselt? Wie wird entschlüsselt?	Stillarbeit, Recherche	Internet, Word-Datei	In der Word-Datei gibt es vorgegebene Links zu Webseiten für die Recherche. Zusatz Recherche: Häufigkeitsanalyse, Enigma

13:39 15'	Auswertung	Lehrerin Handlung • Hinweis auf die Wichtigkeit des Word-Dokuments, wichtig für die folgende Stunde • 3x - wählt mit Würfel Schüler:in aus (präsentiert Verschlüsselungsmethode am Platz) • über INES Kontrolle ob mitgeschrieben wird Schüler:innen Handlung • eine(r) präsentiert die recherchierten Informationen (am Platz) • Schüler:innen die das Thema nicht hatten notieren die wichtigsten Informationen mit • Schüler:innen gleichen den Vortrag mit ihren Informationen ab	Schülervortrag	Word-Datei, Präsentation, Würfel, INES	Bei zu wenig Zeit: • nächste Stunde nochmal drauf eingehen Bei übriger Zeit (unwahrscheinlich): • anreißen von symmetrischer und asymmetrischer Verschlüsselung
13:54 2'	Ausblick	Lehrerin Handlung • Word-Datei auf Vollständigkeit Kontrolle (rumgehen) • Schüler:in die Freigabe zum Speichern der Datei und runterfahren des Rechners geben Schüler:innen Handlung • warten auf Lehrperson • speichern Datei und Herunterfahren des Rechners • wer nicht mitgeschrieben hat, HA Verschlüsselungsverfahren recherchieren	Frontalunterricht, Lehrervortrag	Schüler:innen Rechner, Word-Datei	Schüler:innen sind für Inhalt verantwortlich Kontrolle nur, ob etwas zu den Verschlüsselungs-verfahren geschrieben wurde

4. Schriftliche Nachbereitung

4.1. Reflektion über den Unterrichtsversuch

Die wichtigste Frage zuerst, konnten die Lernziele erfüllt werden?
Die Lernziele *„Schüler:innen lernen den Begriff Kryptographie kennen.“* und *„Schüler:innen bekommen einen Einblick in die Notwenigkeit von Kryptographie.“*, wurden meiner Einschätzung nach und der der Hospitanten und Betreuer erreicht. Das Lernziel *„Schüler:innen bekommen einen Einblick in die Notwenigkeit von Kryptographie.“*, konnte aus Zeitgründen nicht mehr erfüllt werden.

Einschätzung der Stunde in zeitlich chronologischer Reihenfolge.
Der Einstieg in die Stunde, mit dem Ansagen der Namen und der damit verbundenen Freigabe zum Hinsetzten, war aus meiner Sicht gut gelungen. Ich denke den Schüler:innen hat es gezeigt, dass ich die Stunden und sie erstnehme und mich mit ihnen beschäftige. Das hat mir auch das Feedback der Betreuer und Kommilitonen gespiegelt. Bei der Einführung ins Stundenthema, mit der verschlüsselten Überschrift und dem Schlüssel, der nur an die Hälfte der Schüler:innen ausgeteilt wurde, gingen die Meinungen zum Vorgehen etwas auseinander. Ich fand es vertretbar, dass einige Schüler:innen Leerlauf hatten. Dazu muss ich anmerken, dass ich die Hoffnung hatte das diejenigen ohne Schlüssel selbst mehr versuchen darauf zukommen was dort geschrieben steht. Das hat nicht so gut funktioniert und das hat das Feedback der anderen Parteien auch gespiegelt. Wenn ich die Stunde nochmal halten sollte, würde ich allen Schüler:innen einen Schlüssel geben und ein Teil würde zu einem falschen Ergebnis führen.
Den anschließenden Lehrervortrag habe ich eventuell zu schnell abgehandelt und habe zu schnell gesprochen, aber das ist eine Einschätzung, die im anschließenden Gespräch nicht bestätigt wurde.
Die Rechercheaufgabe finde ich nach wie vor eine gute Idee. Ich habe allerdings stark unterschätzt wie langsam die Schüler:innen schreiben und wie lange sie damit für die anschließende Ergänzung benötigen. Das Feedback der Betreuer, hat ebenfalls deutlich gemacht, dass es eine sehr anspruchsvolle Aufgabe war, die den Schüler:innen viel abverlangt. Von den Kommilitonen kam der Vorschlag für das nächste Mal ein Verfahren mit den Lernenden gemeinsam zu erarbeiten, damit der Arbeitsauftrag klarer wird und die übrigen Verfahren selbst erarbeiten zu lassen. Wichtig wäre außerdem noch gewesen die Inhalte, welche die Schüler:innen auf dem Arbeitsblatt notiert haben müssen, entweder auf den Präsentationsfolien vorbereitet zu haben oder sie anzuschreiben, während sie vorgetragen werden. Das hätte das mitschreiben und ergänzen vereinfacht.
Dadurch, dass die Schüler:innen beim Vortragen und mitschreiben länger gebrauchthaben als erwartet, hat mir zum Ende der Stunde die Zeit für die Folie „Ziele der Kryptografie“ gefehlt, was ich dann in die nächste Stunde schieben musste.

Zu meinem pädagogischen Auftreten fällt es mir immer schwer etwas zu sagen, da ich viel spontan handle und zwischenzeitlich das Gefühl hatte, ich übertreibe es mit den Zurechtweisungen der Schüler:innen. Auch mit der Strafarbeit für Fabian habe ich im Anschluss gehadert, ob sie nicht übertrieben war. Für die folgende Stunde hat sich diese aber ausgezahlt. Er hat versucht mitzumachen und sich seiner zwischenzeitlichen Langeweile gestellt ohne

Unsinn zu machen. Die für mich wichtigsten Punkte sind immer Offenheit den Schüler:innen gegenüber, konsequentes Handeln und jede Situation ohne Vorbelastung neu zu betrachten. Im Feedbackgespräch nach der Stunde, habe ich für mein Auftreten viel positive Rückmeldung bekommen. Von meinen Kommilitonen gab es positives Feedback zu meinem Auftreten und meiner Präsenz im Raum. Die Rückmeldung der Betreuer war ebenfalls positiv, vor allem gab es lob für meinen Umgang mit den Schülern. Dass ich ihnen immer wieder positive Zuwendung und Aufmerksamkeit gebe, sie ihnen aber auch genauso schnell entziehen kann.

4.2. Ausblick

Meine Schwäche liegt eindeutig darin das Aufgabenniveau für die Schüler:innen zu hoch anzusetzen. Ich neige dazu den Anforderungsbereich recht hoch an zusetzten, wobei ich inhaltlich nicht zu viel erwarte, sondern eher bei den „Softskills“ wie mit der Tastatur schreiben oder Inhalte vortragen. Das ist denke ich das wichtigste was ich im Hinterkopf behalten muss, die Schüler:innen sind langsamer als ich annehme und gerade in der Phase der Pubertät, fallen einigen soziale Interaktionen schwerer.

Meine Stärke ist mein pädagogisches Auftreten. Die Fähigkeit Situationen gut einschätzen zu können und mit einem guten Urteilsvermögen spontan auf diese zu reagieren.

Mir diese Schwäche und Stärke immer wieder vorzuhalten und zu berücksichtigen, wird mir zum einen die Möglichkeit geben meine Stunden besser an die Schüler:innen anzupassen und zum anderen im Klassenzimmer immer wieder das nötige Selbstvertrauen geben selbstbewusst in der Klasse aufzutreten.

Anhang Eingesetzte Unterrichtsmittel / Medien

I. Arbeitsblatt Kryptografie

Kryptografie

Definition Kryptografie:

- altgriechisch *kryptós*, deutsch -> verborgen, geheim und *gráphein*, deutsch -> schreiben

Ursprünglich die **Wissenschaft der Verschlüsselung** von Informationen. Heute befasst sie sich auch allgemein mit dem Thema **Informationssicherheit**, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.

Ziele und Notwendigkeit:

Die Verschlüsselung, dient der **Geheimhaltung und** dem **Schutz** von übertragenen oder **gespeicherten Informationen**.

- **Zugriffsschutz:**
  Nur berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.
- **Integrität/Änderungsschutz:**
  Die Daten müssen nachweislich vollständig und unverändert sein.
- **Authentizität/Fälschungsschutz und Verbindlichkeit:**
  Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein und seine Urheberschaft zu bestreiten, d. h., sie sollte sich gegenüber Dritten nachweisen lassen.

Aufgabe

Öffne die Links zu dem dir zugeteilten Verschlüsselungsverfahren. Lies dir die Texte auf den Internetseiten durch und beantworte die untenstehenden Fragen, indem du die Antworten darunterschreibst.

Caesar-Chiffre

Links:
https://meinstein.ch/math/caesar-verschluesselung-in-der-schule/
https://de.serlo.org/informatik/48121/caesar-verschl%C3%BCsselung

Woher kommt dieses Verschlüsselungsverfahren?

Lösung: Der Namen kommt vom römischen Herrscher Julius Caesar, der so seine geheimen Botschaften versendet hat.

Wie wird verschlüsselt?

Lösung:

- Alphabet wird um einen bestimmten Wert verschoben
- Der Klartext-Buchstabe wird einem Geheimbuchstaben zugeordnet und aufgeschrieben

Wie wird entschlüsselt?

Lösung:

- Alphabet wird um einen bestimmten Wert verschoben (gleicher Wert wie bei der Verschlüsselung)
- Geheimbuchstaben suchen und den zugeordneten Klartext-Buchstaben aufschreiben

Beispiel: Verschiebung um 5 (k = 5)

Klartext-Alphabet: 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
Geheim-Alphabet: 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

Klartext: GUTEN MORGEN
Geheimtext: BPOZI HJMBZI

Wie sicher findest du dieses Verschlüsselungsverfahren?

1. Freimaurerchiffre/-code

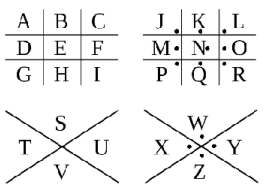
Links:
https://freimaurer-wiki.de/index.php/Geheimschrift
https://onyxframework.org/de/was-ist-die-freimaurerische-chiffre/#Wie_es_funktioniert

Woher kommt dieses Verschlüsselungsverfahren?

Lösung: Der wahre Ursprung ist unbekannt. Es wird angenommen, dass sie bereits in der Antike benutzt wurde. Es gibt auch Hinweise, dass die Tempelritter sie während der christlichen Kreuzzüge im Mittelalter verwendet haben. Bis ins 18. Jahrhundert waren die Freimauerchiffren verschwunden. Einige Freimaurer benutzten dann wieder die Chiffren, um Aufzeichnungen, Riten und Nachrichten privat zu halten.

Wie wird verschlüsselt?

Lösung:



Die Kernelemente dieses Systems sind die Raster und Punkte, in die das Alphabet verteilt wird. Es gibt unterschiedliche Varianten der Verteilung der Buchstaben, wobei die Struktur und Elemente gleichbleiben. Der Schlüssel besteht aus einem Gitter (siehe Grafik links). Beim Verschlüsseln wird das Umfeld des Buchstaben abgeschrieben.

Wie wird entschlüsselt?

Lösung: Beim Entschlüsseln wird das geschriebene Symbol gesucht und der Klartext-Buchstabe aufgeschrieben.

Wie sicher findest du dieses Verschlüsselungsverfahren?

2. Skytale

Links:
https://informatik.mygymer.ch/g23c/013.kryptologie-sicherheit/01.antik.html#skytale
https://www.inf-schule.de/kids/datennetze/verschluesselung/schritt5
https://de.wikipedia.org/wiki/Skytale

Woher kommt dieses Verschlüsselungsverfahren?

> Lösung: Die Spartaner (ca. 500 v. Chr.) nutzten eine Skytale (griechisch für «Stock» oder «Stab»), um wichtige militärische Botschaften zu übermitteln.

Wie wird verschlüsselt?

> Lösung: Der Absender wickelte einen Streifen aus Pergament oder Leder spiralförmig um die Skytale und schreibt die Nachricht längs auf das aufgewickelte Band. Auf dem abgewickelten Streifen, steht nun eine scheinbar sinnlose Buchstabenfolge.

Wie wird entschlüsselt?

> Lösung: Der Empfänger bekommt den Pergament- oder Lederstreifen und kann die Botschaft mit einer Skytale vom selben Durchmesser, auf dem die Nachricht geschrieben wurde, wieder entziffern.

Wie sicher findest du dieses Verschlüsselungsverfahren?

3. Zusatz Häufigkeitsanalyse

Links:
https://de.wikipedia.org/wiki/H%C3%A4ufigkeitsanalyse

Wo für benutzt man sie?

> Lösung:
>
> - Zur Entschlüsselung von Geheimtexten ohne vorhanden Schlüssel (bei Ersetzungsverfahren)

Wie funktioniert es?

> Lösung:
>
> - Mit Hilfe des Häufigkeitsvorkommen der Buchstaben in einem Text, z.B. e = 17% (häufigster Buchstabe in der deutschen Sprache)
>
> Beispiel: Wenn in einem verschlüsselten Text Q zu ca. 17% vorkommt, dann ist es entschlüsselt sehr wahrscheinlich der Buchstabe E

II. Stundenthema Schlüssel

Entschlüsselung:

1. Die Zahlen stehen für Buchstaben. Siehe Tabelle.

A	B	C	...	G	H	I	J	K	...
1	2	3	...	7	8	9	10	11	...

Q	R	S	T	...	X	Y	Z
17	18	19	20	...	24	25	26

2. Das Wort wird von rechts nach links gelesen.

III. Präsentation

- Taschen bitte nach hinten stellen
- Packt einen Stift (Federmappe) und das Hausaufgabenheft aus
- Jacken an den Hacken hängen
- Rechner bleiben aus, Tastatur und Maus nach oben schieben

Stundenthema

E 9 F 1 R 7 O 20 P 25 R 11

Stundenthema

K R Y P T O G R A F I E

Definition:

- altgriechisch *kryptós*, deutsch -> verborgen, geheim
  gráphein, deutsch -> schreiben
- Ursprünglich die Wissenschaft der Verschlüsselung von Informationen
- Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit
  - Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind

Ablauf:

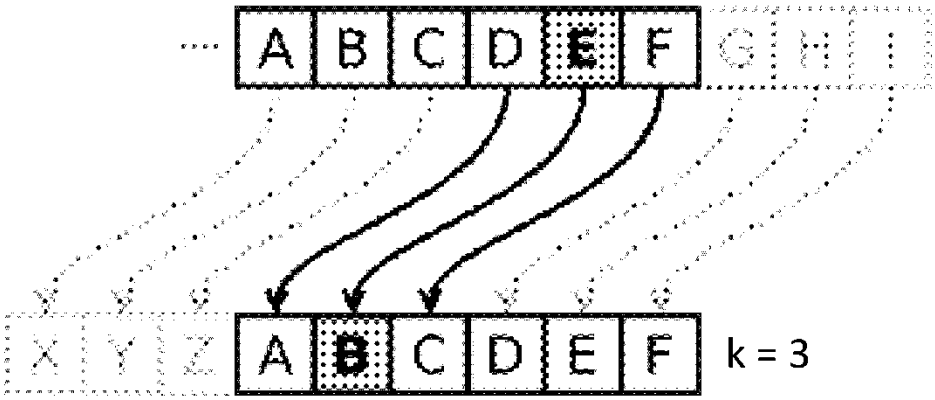
-> Rechner starten -> Anmelden

-> Dateiverzeichnis (Explorer) öffnen -> Laufwerk (H:) -> **incoming** Ordner öffnen -> Datei **Kryptografie** öffnen

-> Datei -> speichern unter … -> in deinem Schulorder/ Info-Ordner speichern

-> **Aufgabe** in Einzelarbeit bearbeiten

Caesar Chiffren

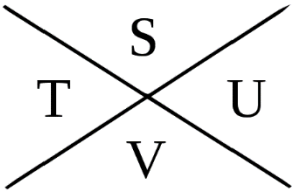


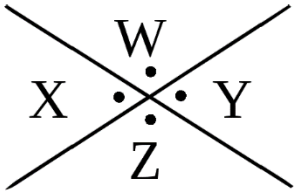
Skytale

Freimaurerchiffren/-code

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R





Ziele der Kryptografie:

- dient der Geheimhaltung und dem Schutz von übertragenen oder gespeicherten Informationen
  - Zugriffsschutz
  - Änderungsschutz
  - Fälschungsschutz und Verbindlichkeit

Literaturverzeichnis

[GE16] Bildungsstandards Informatik für die Sekundarstufe II, 2016.

[LA22a] Landesamt für Schule und Bildung (LaSuB): Lehrplan Oberschule Informatik, Dresden, 2022.

[LA22b] Lauterschlag, E.: Kryptographie. Definition, Ziele und geschichtliche Entwicklung. http://www.was-ist-malware.de/it-sicherheit/kryptographie/, Stand: 30.07.2022.

Quellenverzeichnis

Freimaurer Wiki: Geheimschrift. https://freimaurer-wiki.de/index.php/Geheimschrift, Stand: 30.07.2022.

Bildungsstandards Informatik für die Sekundarstufe II, 2016. https://informatikstandards.de/fileadmin/GI/Projekte/Informatikstandards/Dokumente/Bildungsstandards_SII.pdf

Hornet Security: Kryptographie. Von den Anfängen der Verschlüsselung, bis hin zur heutigen Zeit. Die Geschichte der Kryptographie und ein Blick in die Zukunft. https://www.hornetsecurity.com/de/wissensdatenbank/kryptographie/?_adin=11711554438, Stand: 30.07.2022.

Informatik G23c: Skytale. https://informatik.mygymer.ch/g23c/013.kryptologie-sicherheit/01.antik.html#buchstabenhaufigkeit-in-der-deutschen-sprache, Stand: 30.07.2022.

Keller-Buttell, M.: Skytale von Sparta. https://www.inf-schule.de/kids/datennetze/verschluesselung/schritt5, Stand: 30.07.2022.

Landesamt für Schule und Bildung (LaSuB): Lehrplan Oberschule Informatik, Dresden, 2022. http://lpdb.schule-sachsen.de/lpdb/web/downloads/3209_lp_os_informatik_2022.pdf?v2

Lauterschlag, E.: Kryptographie. Definition, Ziele und geschichtliche Entwicklung. http://www.was-ist-malware.de/it-sicherheit/kryptographie/, Stand: 30.07.2022.

onyxframework: Was ist die freimaurerische Chiffre? https://onyxframework.org/de/was-ist-die-freimaurerische-chiffre/#Wie_es_funktioniert, Stand: 30.07.2022.

Wikipedia: Kryptographie. https://de.wikipedia.org/wiki/Kryptographie#Geschichte_der_Kryptographie, Stand: 30.07.2022.

Wikipedia: Skytale. https://de.wikipedia.org/wiki/Skytale, Stand: 30.07.2022.

Eigenständigkeitserklärung

Hiermit erkläre ich, den vorliegenden Praktikumsbericht eigenständig und ausschließlich unter Verwendung der im Quellenverzeichnis angegebenen Literatur- und sonstigen Informationsquellen verfasst zu haben.

Unterschrift Studierender