Leistungsnachweis Fachdidaktik I
Grundlagen der Informatik für Maturitätsschulen

Eingereicht bei Prof. Dr. Juraj Hromkovič und Regula Lacher

Eingereicht von Lea Sarah Boesinger am 30. Dezember 2022

Einleitung

An einem Langzeitgymnasium in Zürich wird Informatik ab kommendem Schuljahr bereits in der ersten Klasse (7. Schuljahr) unterrichtet werden. Das Thema «Geheimschriften und Kryptographie» eignet sich besonders gut, grundlegende Informatikansätze auf spielerische und lustvolle Art weiterzugeben und die SuS neugierig auf weiterführende Inhalte zu machen. Eine Unterrichtseinheit zu diesem Thema eignet sich also hervorragend gerade für diese Schulstufe.
Um den SuS bewusst zu machen, dass das für sie neue Fach Informatik viele Verknüpfungen zu anderen Fächern und Lebensbereichen hat, wird der Fokus darauf liegen, dass die SuS an bekannte Dinge anknüpfen und in weiterführenden Schritten daraus neue Erkenntnisse gewinnen können, andererseits soll aber auch herausgearbeitet werden, dass das Thema «Geheimschrift und Kryptographie» (und Informatik im Allgemeinen) keine moderne Erfindung ist, sondern bereits in der Antike die Menschen beschäftigt hat. Da der Lateinunterricht in der oben genannten Schule obligatorisch ist, ist die Ausgangslage der Schüler:innen geradezu ideal, da die Klasse bereits Kenntnisse in der Sprache und Geschichte der Römer hat.
Die SuS sollen abstrakte Konzepte selbst erfahren und Erkenntnisse möglichst selbst entdecken, deshalb wurde bei dieser Planung der Kreativität und der individuellen SuS-Arbeit bewusst viel Platz eingeräumt. Dadurch bedingt beruht der Unterricht an verschiedenen Stellen explizit auf Ergebnissen aus der Klasse, was dazu führen wird, dass die Planung stets flexibel an diese Ergebnisse angepasst werden muss.

Im ersten Teil findet sich die Planung der Sequenzen 1: «Einführung in Geheimschriften», 2: «Einführung in Kryptosysteme». und 3: «Antikes Kryptosystem und eigenes Kryptosystem». Daran anschliessend sind im Anhang einerseits alle Aufträge, die in der Planung erwähnt und beschrieben werden, nochmals ausformuliert angefügt, andererseits findet sich dort auch ein Begriffslexikon aller Fachbegriffe, das sich die SuS während dieser Einführung selbständig erstellen, und das sie nach dieser Einführung kennen sollen.

Sequenz 1: Einführung in die Geheimschriften

Motivation & Ziele	Unterrichtsbeschreibung	Erwartungen	Begriffe	Arbeitsauftrag
Motivation: Als Einstieg in dieses Thema dient eine Art der paradoxen Intervention, i.e. man verhält sich so, wie es die SuS *nicht* erwarten. Durch das Zeigen einer chiffrierten Botschaft zu Beginn der Sequenz sind die SuS medias in res, und ohne viele einleitende Worte kann sofort am Inhalt gearbeitet werden. Ziele: Es soll deutlich werden, dass «die Zahlen für Buchstaben stehen», also die Buchstaben durch Zahlen ersetzt wurden. Es muss klar werden, dass man das System für die Chiffrierung und Dechiffrierung kennen muss, um zur Nachricht zu gelangen. Die SuS verstehen die Polybios-Chiffrierung und können sie aktiv anwenden	**1.1. Einstiegsgespräch im Plenum:** Der Klasse wird eine «wichtige» Nachricht unter dem Visualiser präsentiert: 323442221533 431323453121421524 *morgen schulfrei* Bei der Nachfrage, ob es sich alle notiert haben, wird es Proteste geben, da die SuS die Nachricht nicht verstehen. Mit diesem Aufhänger soll die Diskussion geführt werden, warum das so ist, und was benötigt wird, damit die Nachricht verstanden werden kann. **1.2. Knobelarbeit: Echt Antik!** Ausgehend von der Diskussion bei 1.1. wird erläutert, dass die Nachricht mit einem System chiffriert wurde, das in der griechischen Antike angewendet worden war. Die SuS erhalten nun die Polybios-Tabelle, es soll kurz im Plenumsgespräch geklärt werden, wie diese funktioniert. Nun kann zunächst die «wichtige» Nachricht dechiffriert werden, und zur spielerischen Vertiefung bekommt jede:r folgenden Auftrag: Auftrag an die Klasse (Einzelarbeit): • Verfasse eine kurze Botschaft an deine:n Nachbar:in. Chiffriere den Klartext dann in einen Geheimtext, indem du die Polybios-Codierung anwendest! • Dechiffriere die Nachricht, die du von deiner Nachbarin, deinem Nachbarn erhalten hast!	Es wird erwartet, dass die SuS rasch darauf kommen, dass die Zahlen stellvertretend für Buchstaben stehen. Die SuS werden verstehen, dass es ein System geben muss, damit eine Chiffrierung zuverlässig erstellt werden kann. Die Begriffe sollen in die Diskussion eingeflochten werden, die SuS sollen sich diese notieren mit der entsprechenden Definition, die vorgegeben wird (z.B. an der Wandtafel oder mit dem Visualiser). Die SuS werden bei der Sichtung der Poybios-Tabelle das System rasch durchschauen. Das Plenumsgespräch soll sicherstellen, dass die Funktionsweise von allen SuS verstanden wurde.	Klartext Geheimtext chiffrieren dechiffrieren Geheimschrift Substitution	1.2.

Sequenz 2: Einführung in Kryptosysteme

Motivation & Ziele	Unterrichtsbeschreibung	Erwartungen	Begriffe	Arbeitsauftrag

Motivation:
Nachdem die SuS das Prinzip der Geheimschrift anhand Polybios verstanden haben, sollen nun die Schwachstellen daran erkannt werden:
▪ Ist die Geheimschrift (also die Chiffrierung und die dazugehörige Dechiffrierung) bekannt, wird sie nutzlos, da sie nur eine Möglichkeit der Substitution eines Buchstabens bietet (monoalphabetisch).
▪ Da jeder Buchstabe im Klartext mit demselben Zeichen und in derselben Reihenfolge im Geheimtext abgebildet wird, kann eine Geheimschrift recht einfach geknackt werden.
▪ Das Geheimnis ist einzig das Wissen um die Chiffrierung.
 	
Der nächste Schritt soll deshalb hinführen zum Kryptosystem und zur Methode der Ver- und Entschlüsselung anhand von Caesar.
Um einen Lehrer:innen-Monolog zu ver–meiden, soll am Anfang der Sequenz durch einen kreativen Auftrag an die SuS *implizit* die Frage im Raum stehen, wie eine Geheimschrift gestaltet werden kann, damit sie nicht so einfach zu durchschauen ist: Die SuS selbst sollen eine Chiffrierungsmethode formulieren.
 	
Ziele:
▪ Die SuS verstehen den Unterschied zwischen «einem Buchstaben einen neuen Wert bzw. ein neues -geheimes- Zeichen zuordnen» und «den Klartext durch Substitution verschlüsseln».
	2.1. Geheimschrift unerwünscht...
	Im einführenden Klassengespräch soll die Frage nach der Sicherheit der Geheimschrift des Polybios gestellt werden; es sollen also die Schwachstellen besprochen werden.
	
	Kreativer Auftrag an die Klasse (Teamarbeit):
	• Jedes Team bekommt eine geheime Nachricht (zeigt sie niemandem!).
	• Überlegt euch zu zweit eine Methode, wie ihr diese Nachricht vor fremden Augen schützen könnt!
	• Wendet eure Methode auf die Nachricht an und schreibt das Ergebnis auf einen Zettel.
	• Es gelten folgende Regeln:
	  ○ Erlaubt sind alle Grossbuchstaben des lateinischen Alphabets.
	  ○ Es gibt keine Hilfsmittel wie Schere, Papier, Schachteln oder Ähnliches.
	  ○ Es muss möglich sein, aus dem Geheimtext eindeutig zum Klartext zu gelangen.
	
	2.2. Auswertung (Gruppenarbeit)
	Nachdem alle Teams eine Strategie entwickelt haben, soll diese nun getestet werden.
	Auftrag an die Klasse (Gruppenarbeit [zwei Teams]):
	• Übergebt eure «bearbeitete» Nachricht an das andere Team.
	• Erklärt die Methode, die ihr angewendet habt.
	• Versucht, die ursprüngliche Nachricht wiederherzustellen und übersetzt die Nachricht ins Deutsche.
		Es wird erwartet, dass die SuS erkennen, dass die Geheimschrift des Polybios nur solange den Inhalt der Nachricht schützen kann, wie das Geheimnis gewahrt ist; ist dieses einmal durchschaut, ist die Geheimschrift nutzlos.
		Wichtig ist, dass sie erkennen, dass die Geheimschrift nur eine Möglichkeit der Chiffrierung bietet.
				2.1.
				
				2.2.

▪ Die SuS verstehen somit den Unterschied zwischen einer Geheim–schrift und einem Kryptosystem. ▪ Die SuS formulieren Chiffrierungs–algorithmen und wenden sie an. ▪ Die SuS erproben Dechiffrierungs–algorithmen anhand eines Geheim–textes.	**2.3. Sicherung der Ergebnisse** (Klassengespräch) *Die SuS haben auf verschiedenste Weise ihre Nachrichten bearbeitet, wahrscheinlich mit unterschiedlichem Erfolg. Im Klassengespräch und mit einem Wandtafelbild sollen nun die erfolgreichen Strategien gesammelt und visualisiert werden (mit Stichworten).* Im Plenum soll die Frage gestellt werden, bei welcher Gruppe die Wiederherstellung der Nachricht besonders gut geklappt hat; die Gruppe soll ihre Strategie kurz vor der Klasse erläutern.	Erwartet wird, dass sich die SuS eine Strategie überlegt haben, die über das blosse Ersetzen eines Buchstabens durch ein neues Zeichen hinausgeht. Es wäre aber auch möglich, dass sie lediglich eine anders gestaltete Tabelle entwerfen als die des Polybios und den Chiffrierungsalgorithmus nur leicht anpassen. Im Idealfall gibt es eine Gruppe, die sich die Substitution durch eine Verschiebung im Alphabet mit einer bestimmten Zahl überlegt hat. An dieser Stelle kann der Unterschied Geheimschrift - Kryptosystem thematisiert und erläutert werden. Wenn es sich anbietet, sollen im Gespräch die Begriffe eingeflochten und definiert werden, die die SuS wiederum in ihr Begriffslexikon über–nehmen. Sinnvollerweise kann an dieser Stelle eine Hinführung zur Caesar-Verschlüsselung erfolgen.	Kryptosystem Schlüssel verschlüsseln entschlüsseln	

Sequenz 3: Antikes Kryptosystem und eigenes Kryptosystem

Motivation & Ziele	Unterrichtsbeschreibung	Erwartungen	Begriffe	Arbeitsauftrag
Ziele: Die SuS sollen verstehen, dass ein Kryptosystem ein grösseres Mass an Sicherheit bietet als eine blosse Geheimschrift, da ein Kyptosystem per Definition eine Sammlung von Geheimschriften ist, und so die Möglichkeiten der Chiffrierung vervielfältigt werden, abhängig von der Grösse der Schlüsselmenge. Aber auch wenn die Sicherheit des Caesar-Systems auf den ersten Blick sehr hoch erscheint, soll erkannt werden, dass es mit Leichtigkeit geknackt werden kann.	**3.1. Wettbewerb** Alle Schüler:innen bekommen einen «Alphabetstreifen» und die verschlüsselte Nachricht (siehe Auftrag) Auftrag an die Klasse (Einzelwettkampf): • Entschlüssle Caesars Nachricht! • Wenn du es geschafft hast, stehe auf und lies die Nachricht laut vor! (eventuell gibt es einen kleinen Preis für die Gewinnerin oder den Gewinner) *Anm. Es wird bewusst auf eine «Drehscheibe» verzichtet, um die Aufgabe des Wettbewerbs etwas schwieriger zu gestalten und das Abstraktionslevel zu erhöhen.*	Es wird erwartet, dass die SuS aufgrund des vorab erworbenen Wissens in der Lage sind, Caesars Nachricht zu entschlüsseln. Allenfalls kann darauf aufmerksam gemacht werden, dass es sich wirklich um eine Verschlüsselung handelt, und dass der Alphabetstreifen von Nutzen ist. Erfahrungsgemäss lassen sich SuS dieser Altersstufe eifrig auf Wettkämpfe ein, eventuell wäre es auch sinnvoll, sie in Teams arbeiten zu lassen (je nach Klasse).	*Wiederholung:* *Kryptosystem* *Schlüssel* *verschlüsseln* *entschlüsseln*	3.1.
	3.2. Auswertungen 3.2.1. Der/die Gewinner:in soll kurz erklären, wie er:sie vorgegangen ist. Anhand der Ausführungen sollen die SuS überlegen, wieviele Möglichkeiten es für die Caesar-Verschlüsselung gesamthaft gibt. (Eventuell kann die Frage als kurze Teamaufgabe gestellt werden, aber ein Plenumsgespräch eignet sich wohl ebensogut dafür, da die SuS sehr rasch zur Lösung finden werden.)	Es wird angenommen, dass die SuS recht schnell darauf kommen, dass das Kryptosystem aus 25 Geheimschriften besteht. An dieser Stelle kann der Begriff «Schlüsselmenge» eingeführt und besprochen werden.	Schlüsselmenge	
zu 3.2.2. Es soll verstanden werden, dass sich die Häufigkeit einzelner Buchstaben des Klartextes im Kryptotext wiederspiegelt und dort eins zu eins abgebildet wird.	3.2.2. Haben die SuS verstanden, dass es 25 verschiedene Schlüssel gibt, sollen sie zu zweit Überlegungen anstellen, welche Strategien grundsätzlich zur Entschlüsselung angewendet werden können; dafür wird ihnen die Leitfrage visualisiert, die Antworten sollen im Plenumsgespräch ausgewertet werden. An dieser Stelle soll (nochmals) der Unterschied zwischen Geheimschrift und Kryptosystem angesprochen werden, damit der letzte Auftrag gut verstanden wird.	Da die SuS «alle Möglichkeiten durchprobieren» sicherlich als Antwort formulieren würden, wurde dies bereits in der Fragestellung vorweggenommen (siehe Auftrag 3.2.2.). (Erfahrungsgemäss schadet eine Repetition nicht...)		3.2.2.

Sequenz 3: Antikes Kryptosystem und eigenes Kryptosystem				
Motivation & Ziele	Unterrichtsbeschreibung	Erwartungen	Begriffe	Arbeitsauftrag
Von der bei Caesar erlangten Erkenntnis ausgehend sollen die SuS ein «eigenes» Kryptosystem ertüfteln, indem sie die Polybios-Tabelle als Ausgangslage nehmen und ein Schlüsselwort zur Hilfe nehmen. Die SuS verstehen die Verwendung eines Schlüsselwortes und begreifen, dass dadurch die Schlüsselmenge des Kryptosystems nicht -wie bei Caesar- auf <u>einen</u> Wert limitiert ist.	**3.3. Polybios 2.0** Nachdem sich sowohl die Geheimschrift des Polybios, als auch das Kryptosystem des Caesar als zu leicht zu knacken herausgestellt haben, sollen die SuS nun «das Beste aus beiden Systemen vereinen». 3.3.1. Vorbereitende Fragestellung Zunächst soll in der Klasse besprochen werden, was bei der Polybios-Geheimschrift verändert/ verbessert werden müsste, damit aus der Geheimschrift ein Kryptosystem wird. Auch hier sollen sich - wie schon bei Auftrag 3.2.2.- die SuS zunächst selbst besprechen und die Antworten sollen dann in einer kurzen Plenumsdiskussion ausgewertet werden. *Anm. Die SuS sind aufgefordert, sich selbständig Notizen zu machen; obwohl eine Lösung visualisiert wird, wird diese nicht als Kopie an die Klasse ausgehändigt.* Auftrag an die Klasse (Gruppenarbeit): Wie könnt ihr aus der Polybios-Geheimschrift ein Kryptosystem machen? Hilfreiche Hinweise: Überlegt euch, • wie ihr die Buchstaben in der Tabelle anordnet, • wie ihr einen Schlüssel verwenden könnt. Wichtig: Ein:e Empfänger:in muss mit dem Schlüssel dieselbe Buchstabenanordnung erhalten und eine verschlüsselte Botschaft entschlüsseln können!	Es wird erwartet, dass die SuS verstehen, dass es nicht eine feste Anordnung der Buchstaben in der Tabelle geben kann, damit aus der Geheimschrift ein Kryptosystem wird. Wie ein Schlüssel verwendet werden kann, ist wohl die spezielle Herausforderung an dieser Fragestellung.	Schlüsselwort	3.3.1.

Sequenz 3: Antikes Kryptosystem und eigenes Kryptosystem				
Motivation & Ziele	Unterrichtsbeschreibung	Erwartungen	Begriffe	Arbeitsauftrag
Die SuS sollen mit dem letzten Auftrag das Gelernte anwenden und vertiefen, mit dem Erstellen des Lernvideos sollen sie die neuen Begriffe verwenden und festigen. Diese Aufgabe dient einerseits den Lernenden zur selbständigen und kreativen Anwendung, andererseits auch der Lehrperson als Überprüfung des Lernstandes: Die SuS müssen in der Lage sein, schriftlich und mündlich die Vorgehensweise des Kryptosystems verständlich zu formulieren und dabei die neuen Begriffe korrekt zu verwenden.	3.3.2. Eigenes Kryptosystem Die SuS sollen nun mit dem neu erworbenen Wissen als letzte Aufgabe ein eigenes Kryptosystem entwickeln. Auftrag an die Klasse (Gruppenarbeit): 1. Beschreibt euer Verfahren schriftlich und wendet es an auf den Text «Diesen Text kann niemand lesen». 2. Erstellt ein kurzes «Lernvideo», in dem ihr euer Verfahren vorstellt (maximal zwei Minuten).	Es wird erwartet, dass die SuS nun in der Lage sind, selbständig ein Kryptosystem auf der Grundlage des Erarbeiteten zu erstellen, und dass sie diese Aufgabe selbständig umsetzen können.		3.3.2.

Anhang 1: Aufträge

Auftrag 1.2.

Mach es wie Polybios!

1. Schreibe eine kurze Nachricht an deinen Nachbarn/ deine Nachbarin.
2. Chiffriere den Klartext in einen Geheimtext, indem du die Polybios-Codierung anwendest.
3. Dechiffriere die Nachricht, die du von deinem Nachbarn/ deiner Nachbarin erhalten hast.

	1	2	3	4	5
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I/ J**	**K**
3	**L**	**M**	**N**	**O**	**P**
4	**Q**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Auftrag 2.1.

Geheimdienst!

Die Geheimschrift des Polybios wurde leider geknackt. Da ihr im Geheimdienst arbeitet, ist es eure Aufgabe, eine neue Methode zu entwickeln, die der Senat in Zukunft verwenden kann, um wichtige Botschaften vor Spionen zu schützen!

Aufgaben:
1. Denkt euch eine Methode aus, wie ihr eine Nachricht chiffrieren könnt, damit fremde Augen sie nicht verstehen können.
2. Chiffriert mit eurer Methode die geheime Nachricht.

Es gelten folgende Regeln:

- Erlaubt sind alle Grossbuchstaben des lateinischen Alphabets (keine Interpunktion).
- Ihr dürft keine Hilfsmittel wie Schere, Papier, Schachteln, ... benutzen.
- Der Geheimtext muss eindeutig wieder in den Klartext umzuwandeln sein.

zu 2.1.

Liste der geheimen Botschaften:
dominus in casam revenit.
servus numquam laborat.
mercatores valde gaudent.
dominus amicos exspectat.
dei homines adiuvant.
equos non reperiunt.
servi ad aedificium properant.
servus senatorem salutat.
dominus servos laudat.
servus verba audire vult.
senator ante tabernam exspectat.
populus equos spectat.

Auftrag 2.2.

Dechiffrierung!

Eure neu entwickelte Chiffrierung muss nun getestet werden!

Aufgaben:

1. Erklärt dem anderen Team die Methode, die ihr zur Chiffrierung verwendet habt.

2. Übergebt eure chiffrierte Nachricht dem anderen Team.

3. Dechiffriert die Nachricht und übersetzt sie ins Deutsche; fragt beim anderen Team nach, ob die Nachricht korrekt ist!

Auftrag 3.1.

Wettbewerb!

Es ist euch gelungen, Caesars Nachricht abzufangen! Du musst die Botschaft, möglichst schnell an den Senat weiterleiten, damit du eine Belohnung erhälst – wie schnell bist du?

Aufgabe: Entschlüssle Caesars Nachricht!
Geschafft? Stehe auf und lies die Nachricht laut vor!

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

J D O O L H Q E H V W H K W D X V G U H L W H L O H Q

Tipp: Die Botschaft ist in Deutsch verfasst!

Lösung:

«GALLIEN BESTEHT AUS DREI TEILEN»

Auftrag 3.2.2.

Wie gehts schneller?

Überlegt euch zu zweit folgende Frage und macht schriftliche Notizen dazu:

Wie kann ich Caesar entschlüsseln, wenn ich nicht alle 25 möglichen Varianten durchprobieren will?

Tipp: Überlege, was die deutsche Sprache für Auffälligkeiten hat!

Mögliche Lösungsfolie zu 3.2.2.:

1. Häufigkeit beachten!
   «e» ist der Buchstabe, der im Deutschen am häufigsten vorkommt, gefolgt von «n», «i» und «s».
   Man kann also den häufigsten Buchstaben im Kryptotext suchen und ihn dem «e» zuweisen: Der Abstand im Alphabet zwischen den Buchstaben ist dann der Schlüssel! *(«e» kommt 6x vor im Rätseltext!)*

2. Doppelbuchstaben erkennen!
   Man kann sich überlegen, welche Buchstaben im Deutschen als Doppelfolge vorkommen können und diese durchprobieren. *(«ll» im Rätseltext)*

3. Kombinationen erkennen!
   Im Deutschen kommen verschiedene Buchstabenkombinationen sehr häufig vor, z.B. «sch», «st» oder «ei». Bei längeren Texten kann sich wiederholende Wortfolgen erkennen und wiederum gezielt Codierungen ausprobieren.

Auftrag 3.3.1.

Wie wird aus Polybios' Geheimschrift ein Kryptosystem?

Überlegt euch in der Gruppe folgende Frage und macht schriftliche Notizen dazu:

Wie muss ich die Geheimschrift des Polybios erweitern, damit daraus ein funktionierendes Kryptosystem entsteht?

Überlegt euch dabei,

- wie ihr die Buchstaben in der Tabelle anordnet,
- wie ihr einen Schlüssel verwenden könnt.

Wichtig: Ein:e Empfänger:in muss mit dem Schlüssel dieselbe Buchstaben–anordnung erhalten und eine verschlüsselte Botschaft entschlüsseln können!

(ANMERKUNG: I/J BESETZEN EIN FELD)

	1	2	3	4	5
1					
2					
3					
4					
5					

Mögliche Lösungsfolie zu 3.3.1.:

1. Schlüsselwort wählen: z.B. KRYPTOGRAPHIE
2. Schlüsselwort in die Tabelle schreiben, doppelt vorkommende Buchstaben bei zweiter Verwendung ignorieren.

	1	2	3	4	5
1	**K**	**R**	**Y**	**P**	**T**
2	**O**	**G**	~~**R**~~ **A**	~~**P**~~ **H**	**I/J**
3	**E**				
4					
5					

3. Die verbliebenen Buchstaben des Alphabets der Reihe nach in die Tabelle einfügen:

	1	2	3	4	5
1	K	R	Y	P	T
2	O	G	~~**R**~~ A	~~**P**~~ H	I/J
3	E	**B**	**C**	**D**	**F**
4	**L**	**M**	**N**	**Q**	**S**
5	**U**	**V**	**W**	**X**	**Z**

Auftrag 3.3.2.

Erstellt euer eigenes Kryptosystem!

Erweitert die Polybios-Tabelle nun zu eurem eigenen Kryptosystem, mit dem ihr Texte ver- und entschlüsseln könnt!

1. Beschreibt euer Verfahren schriftlich und wendet es an auf den Text «Diesen Text kann niemand lesen»; testet auch die Entschlüsselung!

2. Erstellt ein kurzes «Lernvideo», in dem ihr euer Verfahren vorstellt (maximal vier Minuten).

3. Ladet euer Video ins Teams hoch in den Ordner «Polybios 2.0»

Wichtig: Achtet darauf, dass ihr Begriffe korrekt verwendet!

	1	2	3	4	5
1					
2					
3					
4					
5					

Anhang 2: Begriffe & Definitionen[1] *(in der Reihenfolge ihrer Verwendung)*

Klartext:
Ein lesbarer Text in einer natürlichen Sprache.

Geheimtext:
Ein Klartext, auf den eine Chiffrierung angewendet wurde; wird auch Chiffre genannt.

chiffrieren/ Chiffrierung:
Umwandlung eines Klartextes in einen Geheimtext mit Hilfe einer Geheimschrift.

dechiffrieren/ Dechiffrierung:
Umwandlung eines Geheimtextes in den Klartext mit Hilfe einer Geheimschrift.

Geheimschrift:
Kombination aus Chiffrierung und dazugehöriger Dechiffrierung.
Eine Geheimschrift besteht aus einem Klartextalphabet, einem Geheimtextalphabet, einem Algorithmus zur Chiffrierung und einem Algorithmus zur Dechiffrierung.
Die Chiffrierung sollte dabei einer injektiven Funktion entsprechen.

Substitution:
Codierung von Buchstaben durch andere Symbole oder Symbolfolgen.

Kryptosystem:
Eine Sammlung von Geheimschriften, bei der jede Geheimschrift einen eindeutigen Namen hat.

Schlüssel:
Bezeichnet den eindeutigen Namen einer Geheimschrift eines Kryptosystems.

Kryptotext:
Synonym für Geheimtext im Rahmen eines Kryptosystems.

verschlüsseln:
Umwandlung eines Klartextes in einen Kryptotext mit Hilfe eines Kryptosystems und eines Schlüssels.

entschlüsseln:
Umwandlung eines Kryptotextes in den Klartext mit Hilfe eines Kryptosystems und des dazugehörigen Schlüssels.

Schlüsselmenge:
Anzahl möglicher Geheimschriften/ Schlüssel, über die ein Kryptosystem verfügt.

Schlüsselwort *(hier in Bezug auf die Polybios-Tabelle)*:
Beliebige Buchstabenfolge, anhand derer die Reihenfolge des Alphabets in der Tabelle -und damit die Zuweisung zur Zahlenkombination- festgesetzt wird.

[1] Informatik. Data Science und Sicherheit, 49ff. (Klett und Balmer Verlag).