Fachdidaktik I, Studienleistung im HS 23

Sequenz 1: Grundlagen der Informatik für Maturitätsschulen

Eingereicht bei Prof. Dr. Juraj Hromkovič und Regula Lacher
Eingereicht von Marco Lichtsteiner am 9. Dezember 2023

Einleitung

Bei diesem Dokument handelt es sich um eine Studienleistung, erbracht im Rahmen der Fachdidaktik I, GymInf, 2023.
Die vorliegende Unterrichtssequenz eignet sich dank der Rätsel- und Knobelaufgaben, deren Lösung zwar Ausdauer und Fantasie, aber keine fortgeschrittenen Mathematikkenntnisse erfordern, speziell, aber nicht nur, für Klassen *ohne* MINT-Profil. Sie stellt einen Einstieg in den Unterrichtsblock *Kryptografie* dar und ist für die Dauer von mindestens drei Lektionen konzipiert. Die starke Verzahnung mit dem Kapitel 2 *Geheimschriften und Datensicherheit* des Buches **INFORMATIK – Data Science und Sicherheit** (Barot et al., 2022) ist beabsichtigt und ermöglicht bei Bedarf das Kombinieren mit anderen Buchkapiteln/kapitelteilen.
Da der Autor im eigenen vorausgegangenen Programmier-Unterricht die Fibonacci-Reihe thematisierte, wird sie hier bewusst wieder aufgegriffen. Sollte dies nicht erwünscht sein, empfiehlt es sich bei der Aufgabe 1 andere einfache Transpositionschiffren und bei der Aufgabe 4c) die Variante «Latein» zu verwenden.

Rahmenlehrplan Informatik

- «Verschiedene Codierungen und Darstellungen von Informationen kennen
- Eigene und fremde Lösungswege formal beschreiben und kritisch analysieren
- Algorithmen entwerfen, beurteilen [und in einer Programmiersprache umsetzen]

(EDK, 2017)

Eigene Lernziele

Die SuS…

- verwenden die Begriffe Alphabet, Klartext, Geheimtext, Geheimschrift, Chiffrierung und Dechiffrierung und setzen sie korrekt zueinander in Beziehung.
- kennen die Skytale-Geheimschrift und die Geheimschrift von Polybios.
- unterscheiden zwischen Transpositionschiffre und Substitutionschiffre und wenden sie an.

Jahrgangsstufe

9. oder 10. Schuljahr, Grundlagenfach

Vorwissen aus der Informatik und der Mathematik

- Intuitive Vorstellung von Algorithmen als Lösungsmethoden
- Fibonacci-Reihe

Ablauf / Zeitaufwand

- Lektion 1: Aufgabe 1, Theorieinput *Neue Konzepte und Begriffe*, Aufgabe 2
- Lektion 2*: Theorieinput *Chiffrieren mit Tabellen (Skytale)*, Aufgabe 3, Aufgabe 4, Hausaufgaben auf übernächste Lektion
- Lektion 3*: Theorieinput *Codieren von Buchstaben (Polybios)*, Aufgabe 5, Aufgabe 6

* idealerweise als Doppellektion zu unterrichten

Geheimschriften der Antike

⇒ Aufgabe 1 *(adaptiert von Barot et al., 2022, S. 51)*

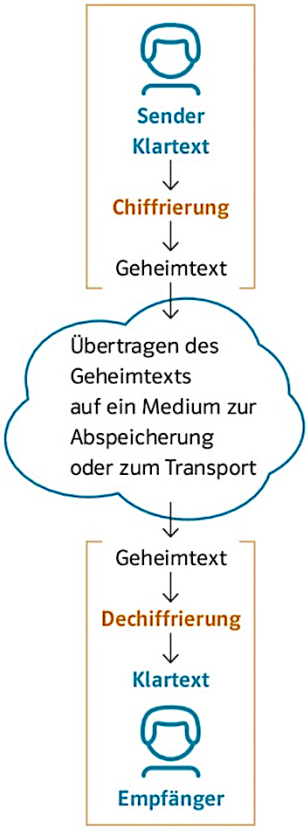
Das Geheimnis der folgenden zwei verwendeten (unterschiedlichen) Geheimschriften liegt im Austausch beziehungsweise der Verschiebung der Positionen der Buchstaben. Versuche aus den Geheimtexten die beiden ursprünglichen Texte wiederherzustellen.
Hinweis: Nutze in beiden Fällen die ersten sechs Fibonacci-Zahlen (0, 1, 1, 2, 3, 5).

a) H U E E T H E G U E S T I G E H E M M C S R H T F I N E

b) G H E I E S C M R I F H E N S I N T D E H T U D A E T H E S A M

Neue Konzepte und Begriffe *(adaptiert von Barot et al., 2022, S. 49)*

Jede Schrift ist ein System von grafischen Zeichen, und die Grundlage dafür bildet ein **Alphabet** – eine endliche Menge von Zeichen, die zur Informationsdarstellung dienen. Die Zeichen eines Alphabets werden auch als **Buchstaben** bezeichnet. Wörter und Texte als Darstellungen von Informationen sind die Folgen von Buchstaben des entworfenen Alphabets.



Die Kunst des Lesens und Schreibens war ursprünglich nur wenigen Menschen vorbehalten, weshalb die ersten Schriften als "Geheimschriften" angesehen werden können. Mit der Zunahme der Lese- und Schreibkompetenz stieg der Bedarf an der Geheimhaltung von schriftlich festgehaltenen Informationen. Die ersten Versuche, Geheimschriften zu entwickeln, sind bereits etwa 4'000 Jahre alt und basierten auf dem geordneten Austausch der Reihenfolge von Buchstaben in Texten.

Ein **Klartext** in einer natürlichen Sprache ist die Ausgangsinformation, die einer geheimen Transformation unterzogen werden soll. Die Umwandlung eines Klartextes in einen Geheimtext wird als **Chiffrierung** bezeichnet. Die Rückumwandlung des Geheimtexts in den Klartext ist die **Dechiffrierung**. Eine Geheimschrift ist so gestaltet, dass die Dechiffrierung eindeutig zum ursprünglichen Klartext führt.

Bei der Kommunikation gibt es immer einen **Sender** und einen **Empfänger**. Wenn eine Geheimschrift verwendet wird, chiffriert der Sender seinen Klartext in einen Geheimtext, und der Empfänger dechiffriert diesen Geheimtext, um den ursprünglichen Klartext zu erhalten. Die Wahl des Alphabets und die Art der Chiffrierung bestimmen die Sicherheit der Geheimschrift.

Die Grundlage jeder Schrift und Geheimschrift sind somit die Alphabete, die die Zeichen für die Informationsdarstellung festlegen. Die Reihenfolge und Kombination dieser Zeichen spielen eine entscheidende Rolle in der Welt der Kodierung und Decodierung, sei es für künstlerische, kommunikative oder geheime Zwecke. Es können dabei verschiedene Alphabete für Klartexte und Geheimtexte zum Einsatz kommen.

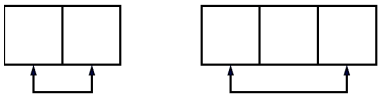
⇒ **Aufgabe 2** *(adaptiert von Barot et al., 2022, S. 50)*

a) Die beiden Vorgehensweisen bei der Chiffrierung und Dechiffrierung in Aufgabe 1 kann man grafisch sehr einfach und anschaulich beschreiben. Für **a** sieht die grafische Darstellung, sowohl für die Chiffrierung wie für die Dechiffrierung, wie folgt aus.

a

für n = 1 für n = 2

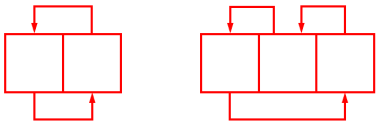
Chiffrierung und Dechiffrierung



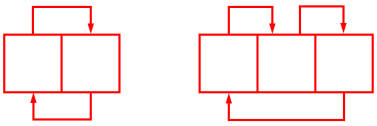
b

für n = 1 für n = 2

Chiffrierung:



Dechiffrierung:



Ergänze rechts die grafischen Darstellungen für **b**.

Bei **a** handelt es sich um eine Vertauschung, bei **b** um eine Verschiebung. Beides sind Beispiele für eine **Transposition** (Austausch der Positionen von Buchstaben).

b) Formuliere Algorithmen für die Chiffrierung und die Dechiffrierung der Texte nach den oben gezeichneten Mustern.

a – **Vertauschung**

H | E U | T E | G E H | T E S U | M G E H E I | M | S C | H R | I F T | E N
H | U E | E T | H E G | U E S T | I G E H E M | M | C S | R H | T F I | N E
0 1 1 2 3 5 0 1 1 2 (3)

Chiffrierung:

1. Unterteile den Klartext wiederholend in Abschnitte der Länge 18.
2. Beginne links in jedem Abschnitt und vertausche den ersten Buchstaben mit dem um die erste Fibonacci-Zahl (0) weiter rechtsstehenden Buchstaben.
3. Wiederhole 2. mit dem Buchstaben rechts von dem letzten vertauschten Buchstaben und der nächsten Fibonacci-Zahl, solange bis die 6. Fibonacci-Zahl (5) verwendet wurde.

Dechiffrierung:

1. Unterteile den Klartext wiederholend in Abschnitte der Länge 18.
2. Beginne links in jedem Abschnitt und vertausche den ersten Buchstaben mit dem um die erste Fibonacci-Zahl (0) weiter rechtsstehenden Buchstaben.
3. Wiederhole 2. mit dem Buchstaben rechts von dem letzten vertauschten Buchstaben und der nächsten Fibonacci-Zahl, solange bis die 6. Fibonacci-Zahl (5) verwendet wurde.

b – **Verschiebung**

G | E H | E I | M S C | H R I F | T E N S I N | D | H E | U T | E D A | S T H E | M A
G | H E | I E | S C M | R I F H | E N S I N T | D | E H | T U | D A E | T H E S | A M
0 1 1 2 3 5 0 1 1 2 3 (5)

Chiffrierung:

1. Unterteile wiederholend den Klartext von links nach rechts in Abschnitte der Längen $n + 1$. Wähle dabei für n alternierend die ersten sechs Fibonacci-Zahlen.
2. Verschiebe in jedem Abschnitt den ersten Buchstaben an dessen letzte Stelle.

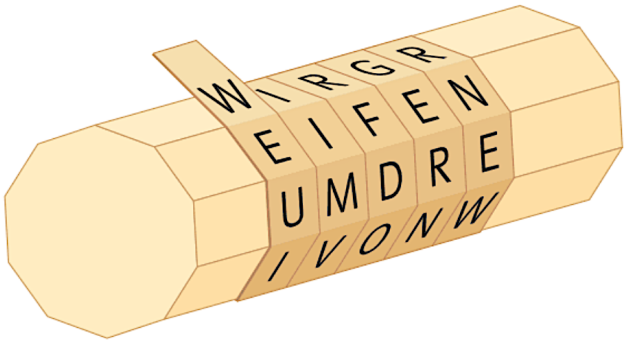
Dechiffrierung:

1. Unterteile wiederholend den Geheimtext von links nach rechts in Abschnitte der Längen $n + 1$. Wähle dabei für n alternierend die ersten sechs Fibonacci-Zahlen.
2. Verschiebe in jedem Abschnitt den letzten Buchstaben an dessen erste Stelle.

c) ⇒ **Partnerarbeit**
Überlege dir ein anderes kurzes Muster zur Chiffrierung der Texte auf der Basis des Austauschens der Positionen der Buchstaben. Chiffriere damit einen Klartext und gib den erzeugten Geheimtext deiner Nachbarin/deinem Nachbarn zur Dechiffrierung.

Chiffrierung mit Tabellen

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



In Sparta hat man vor 2500 Jahren eine Geheimschrift, genannt SKYTALE, verwendet, die man am anschaulichsten mit einer Tabelle beschreiben kann. Man schreibt einen Klartext zeilenweise in eine Tabelle, auch **Matrix** genannt, von links nach rechts. Den Geheimtext erzeugt man, indem man die Buchstaben spaltenweise von oben nach unten liest und die Spalten von links nach rechts liest. Zum Beispiel betrachten wir die Tabelle (8 × 12) wie folgt:

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

Wenn die Tabelle nicht vollständig gefüllt ist, schreibt man beliebige (am besten zufällig gewählte) Buchstaben in die letzten freien Felder. Wenn ein Text mehr Buchstaben umfasst als die Anzahl Felder der Tabelle, schneidet man den Text in Stücke der Länge, die der Anzahl der Felder der Tabelle entspricht. Dann chiffriert man jedes Stück mit der Tabelle auf die gleiche Art und Weise. Das Geheimnis der Geheimschrift ist die Tabellengrösse (Zeilen mal Spalten) und die Reihenfolge der Positionen, in der man die Tabelle bei der Erzeugung des Geheimtextes durchläuft.
Wenn man diese Tabelle spaltenweise von links nach rechts und innerhalb der Spalten von oben nach unten liest, entsteht der folgende Geheimtext:

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

Bei der Dechiffrierung muss man den Geheimtext in die Tabelle spaltenweise von oben nach unten eintragen und danach wird der Klartext wie üblich zeilenweise lesbar.
Bei der Verwendung der ursprünglichen SKYTALE war es ein bisschen einfacher. Das Geheimnis war nur eine Zahl i, und zwar der Umfang eines Holzstabes (die Anzahl der Zeilen der Tabelle). Egal, wie lang der Text war, man hat den Text in i Zeilen geschrieben. Somit konnte man die Anzahl der Spalten selbst bestimmen als

$$\frac{\text{Länge des Textes}}{i}$$ nach oben aufgerundet.

⇒ Aufgabe 3 *(adaptiert von Barot et al., 2022, S. 51)*

Notiere alle Möglichkeiten für die Chiffrierung des Klartextes `GEHEIM` mit einer 2 x 3-Tabelle, wenn:
- nur „zeilenweise“ oder „spaltenweise“ (ganze Zeile oder ganze Spalte in gleicher Richtung) gelesen werden kann und
- beim zeilenweisen Lesen alle Zeilen einheitlich von links nach rechts oder von rechts nach links gelesen werden und
- beim spaltenweisen Lesen alle Spalten einheitlich von unten nach oben oder von oben nach unten gelesen werden.

Man hat zuerst zwei Möglichkeiten S und Z, den Geheimtext spaltenweise oder zeilenweise zu erzeugen. Wenn man spaltenweise chiffriert, kann man die Spalten von links nach rechts (→) oder von rechts nach links (←) nehmen. Innerhalb der Spalte könnte man von unten nach oben (↑) oder von oben nach unten (↓) eintragen. Analog muss man beide, die vertikale und die horizontale Richtung, bei einer zeilenweisen Chiffrierung bestimmen. Dadurch entstehen 2 * 2 * 2 = 8 Möglichkeiten, die man mit folgenden Triples bezeichnen kann.

(S, →, ↓)

G	H	I
E	E	M

(S, →, ↑)

E	E	M
G	H	I

(S, ←, ↓)

I	H	G
M	E	E

(S, ←, ↑)

M	E	E
I	H	G

(Z, →, ↓)

G	E	H
E	I	M

(Z, →, ↑)

E	I	M
G	E	H

(Z, ←, ↓)

H	E	G
M	I	E

(Z, ←, ↑)

M	I	E
H	E	G

Die Möglichkeit (Z, →, ↓) chiffriert den Klartext in den gleichen Klartext, also kann man sie nicht zur Geheimhaltung verwenden.

Somit gibt es 7 sinnvolle Möglichkeiten mit Tabellen Klartexte zu chiffrieren:

⇒ Aufgabe 4

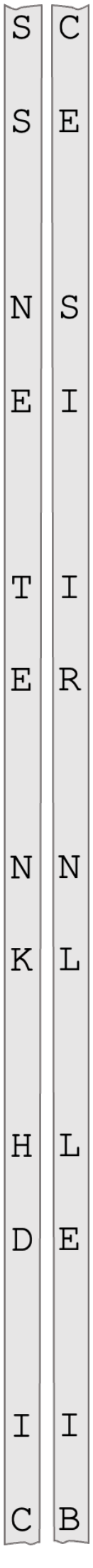
Rechts siehst du zwei Bänder mit Buchstaben darauf, die einen Geheimtext darstellen, der mit einer Skytale erstellt wurde. Dein Ziel ist es, den Geheimtext zu dechiffrieren.

Hier ist wichtig, dass neben Scheren **auch bereits Streichholzschachteln auf dem Lehrerpult bereitliegen**. Letztere bzw. die darin aufbewahrten Streichhölzer werden erst für die Aufgabe 5 benötigt. Die Streichholzschachteln selbst dienen hier aber als Skytalai (Skytale ist ein Substantiv im Femininum im Altgriechischen und die Pluralform wird durch die Endung "-ai" gebildet.), um welche die beiden Geheimtext-Bänder gewickelt werden. So wird klar, dass die Matrix eine 4 x 6-Tabelle ist und der Geheimtext zeilenweise von unten nach oben und innerhalb der Zeilen von rechts nach links zu lesen ist.

a) Da du leider die passende Skytale nicht hast, überlege (und notiere)...

- welche Tabellen (Anzahl Zeilen?/Anzahl Spalten?) es gibt, in welche du den Geheimtext übertragen kannst.

- Der Geheimtext umfasst 24 Buchstaben.
- Es kommen somit folgende Tabellen in Frage:
  2 x 12,
  3 x 8,
  4 x 6,
  5 x 5 (mit 1 Leerfeld),
  6 x 4,
  8 x 3,
  12 x 2 (was den beiden Bändern entspricht, sofern an derselben Stelle gestartet wird)



- wie du die Skytale finden und für das Erstellen der passenden Tabelle nutzen kannst.

- Die Abstände zwischen den Buchstaben sind abwechselnd kurz und lang.
- Das könnte auf eine Skytale mit abwechseln schmalen und breiten «Zeilen» hindeuten.
- Dies wiederum könnte bedeuten, dass die Skytale im Querschnitt rechteckig ist.
- Auf dem Lehrerpult liegen Streichholzschachteln.
- Die Bänder müssen ausgeschnitten und um eine Streichholzschachtel gewickelt werden.
- Es resultiert eine 4 x 6-Tabelle.

b) Erstelle die passende Tabelle und dechiffriere den Geheimtext. Wie lautet der Klartext?

4 x 6-Tabelle (Z, ←, ↑)

Klartext: BLICKE INS INNERE DES LICHTS

S	T	H	C	I	L
S	E	D	E	R	E
N	N	I	S	N	I
E	K	C	I	L	B

c) Verwende den Klartext, um das versteckte Rätsel zu lösen.

- Der Klartext fordert die SuS auf, einen «Blick ins Innere des Lichts» zu werfen. Das «Innere des Lichts» ist hier eine Umschreibung der Innenseite der Streichholzschachtel.

Variante «Latein»
- Dort findet sich der Hinweis «2. Zeile, Latein!».
- Die zweite Zeile der 4 x 6-Tabelle lautet, von links nach rechts gelesen, SEDERE.
- Sedere ist das lateinische Wort für das Verb «sich hinsetzen».
- **SICH HINSETZEN** ist somit das finale Lösungswort.
- Wer das als erste/r klar (durch Aussprechen oder durch Ausführen) kommuniziert, gewinnt einen kleinen Preis.

Variante «Fibonacci»
- Dort findet sich der Hinweis «3. – 8. Fibonacci, H → N», was auf die 3. bis 8. Zahlen der Fibonacci-Reihe hindeutet, also auf die Zahlen 1, 2, 3, 5, 8, 13.
- In der 4 x 6-Tabelle können nun die Buchstaben an ebendiesen Positionen herausgelesen werden: S(1), T(2), H(3), I(5), E(8), N(13), wobei das H zu einem N verändert werden muss.
- Mit diesen Buchstaben kann das Lösungswort **TENNIS** gebildet werden.
- Wer das Rätsel als erste/r löst, gewinnt einen kleinen Preis.

⇒ Hausaufgaben *(zitiert aus Barot et al., 2022, S. 51/52)*

a) Beschreibe die Dechiffrierung der Geheimschriften. Wie geht man vor und wo ist der Unterschied zur Chiffrierung?

Man schreibt bei der Dechiffrierung den Geheimtext in die Tabelle genauso ein, wie man den Geheimtext aus der Tabelle gelesen hat.

b) Ist es möglich, den Geheimtext zeilenweise in eine Tabelle einzutragen und dann den Klartext spaltenweise zu lesen?

Man nimmt statt der ursprünglichen Matrix 8 x 12 die Matrix 12 x 8 und fügt den Geheimtext zeilenweise von links nach rechts ein.
Jetzt kann man den Klartext spaltenweise von oben nach unten innerhalb der Spalten und von links nach rechts lesen.
Wenn man also die Matrix a x b in eine mit den Dimensionen b x a umwandelt, läuft die Dechiffrierung genauso wie die Chiffrierung.

c) Gibt es Tabellengrössen, in denen der Algorithmus für die Chiffrierung identisch mit dem Algorithmus für die Dechiffrierung sein kann?

Falls a = b, d.h. wenn die Tabelle quadratisch ist, sind die Algorithmen für die Chiffrierung und für die Dechiffrierung identisch.

d) Lies den Text *Geschichtlicher und gesellschaftlicher Kontext*.

Geschichtlicher und gesellschaftlicher Kontext

Zeichen (Buchstaben, Symbole) sind die atomaren Bausteine einer Schriftsprache. Bevor die Schriftsprache entstand, dienten vereinfachte Abbildungen von Tieren, Menschen oder Dingen als Zeichen. Ein solches Zeichen entsprach ursprünglich einem Konzept (einem Wort).
Die ältesten archäologischen Funde sind rund 20 000 Jahre alt (z. B. die Höhlenzeichnungen von Lascaux in Frankreich). Solche abbildenden Zeichen entwickelten sich im Verlauf der kulturellen Entwicklung von konkreten Abbildungen mit ikonischem Charakter zu abstrakten Zeichen mit symbolischem Charakter.

Die ältesten Schriftfunde sind ungefähr 6000 Jahre alt (Irak und Mesopotamien) und es waren **Bilderschriften**. Das bedeutet, dass einzelne Objekte zeichnerisch durch ihre Formen dargestellt wurden. Werden die Zeichen abstrakter und entsprechen inhaltlich immer noch einem Objekt bzw. dem Wort für dieses Objekt, so bezeichnen wir solche Schriften als **Wortschriften**. Der Nachteil dieser Schriftart lag in der ständig wachsenden Anzahl der Zeichen, da man für jedes neue Wort ein neues Zeichen brauchte. Das führte zu der Idee, die grosse Anzahl von Wörtern als Folgen von Zeichen aus einem begrenzten Zeichenrepertoire darzustellen und damit die Anzahl der notwendigen Zeichen zu reduzieren.

Der nächste Schritt in der Entwicklung waren die **Silbenschriften**, in denen ein einzelnes Zeichen einer bestimmten Silbe entspricht (z. B. Ägypten, Mayas). Man vermutet den Ursprung in den einsilbigen Wörtern, bei denen das Zeichen nicht mehr für das Wort, sondern für die Silbe des Wortes (Wortlaut) umgenutzt wurde. Diese phonetische Art der Schriftentwicklung hat sich in vielen Kulturen durchgesetzt und führte letztendlich zur **Buchstabenschrift**, die heute meistverbreitete Schriftart. Hier entspricht jedem Zeichen ein bestimmter Laut. Zuerst entstanden unterschiedliche Mischformen. Die erste reine Buchstabenschrift wurde vor ungefähr 4000 Jahren unter dem Einfluss von ägyptischen Hieroglyphen entwickelt. Die meisten europäischen Alphabete (Zeichensysteme) haben ihren Ursprung im griechischen Alphabet, das die Etrusker nach Italien gebracht hatten und so die Grundlage für die Entwicklung des lateinischen Alphabets legten.

Im Unterschied zu natürlichen Sprachen entwickelt man in der Informatik Schriften, die nichts mit den Phonemen der gesprochenen Sprache oder der visuellen Darstellung von Objekten gemeinsam haben. Das bekannteste Beispiel ist das binäre Alphabet {0,1}, mit dem man beliebige Texte darstellen (kodieren) kann.

Es ist interessant zu beobachten, dass die ältesten Funde von Geheimsprachen ungefähr so alt sind wie die Buchstabenschriften. Diese Geheimschriften basierten auf dem Austausch der Positionen der Buchstaben in den Originaltexten oder -botschaften. Über die Richtung des Schreibens und des Lesens (die Zeichen von links nach rechts und die Zeilen von oben nach unten wie in unserer Kultur) bestand und besteht kein Konsens, weshalb unterschiedliche Kulturen auch unterschiedliche «Schreibrichtungen» entwickelten (z. B. die Zeichen von rechts nach links oder von oben nach unten). Innerhalb eines Schriftsystems ist die Schreibrichtung aber festgelegt und die natürlichste Idee für die «Verschleierung» von Texten ist die Änderung der Schreibrichtung.

Kodierung von Buchstaben

Vor mehr als 2500 Jahren begann sich eine neue Methode für das Chiffrieren durchzusetzen. Man ersetzte unabhängig von deren Position im Klartext einzelne Buchstaben des Alphabets durch festgelegte Kodierungen. Am häufigsten «kodierte» (chiffrierte) man die Buchstaben, indem man sie durch andere Symbole ersetzte, manchmal auch durch Symbolfolgen. Die älteste bekannte Geheimschrift dieser Art stammt vom griechischen Geschichtsschreiber Polybios (ungefähr 2200 Jahre alt). Für das Chiffrieren und Dechiffrieren nutzte er die folgenden Tabellen (links angewandt auf das griechische Alphabet mit 24 Buchstaben und rechts auf das auf 24 Buchstaben reduzierte lateinische Alphabet).

	1	2	3	4	5
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

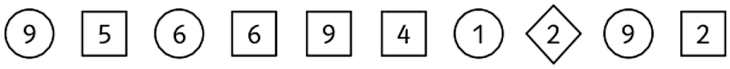
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U / V
5	W	X	Y	Z	

In seiner Tabelle wurde jeder Buchstabe des Alphabets durch eine Folge von zwei Ziffern kodiert. Die erste Ziffer entsprach der Nummerierung der Zeile und die zweite Ziffer der Nummerierung der Spalte. Somit wurde beim lateinischen Alphabet A durch 11 chiffriert, M durch 32, Y durch 53 usw.

Diese Idee führte im Raum des alten Palästina zur Entwicklung ganz neuer Zeichen für die Chiffrierung. Eine Verallgemeinerung dieser Idee zeigt die folgende Tabelle. Für jeden Buchstaben der Schrift wird ein neues Zeichen zusammengesetzt, das durch die Position des Buchstabens in der Tabelle bestimmt wird.

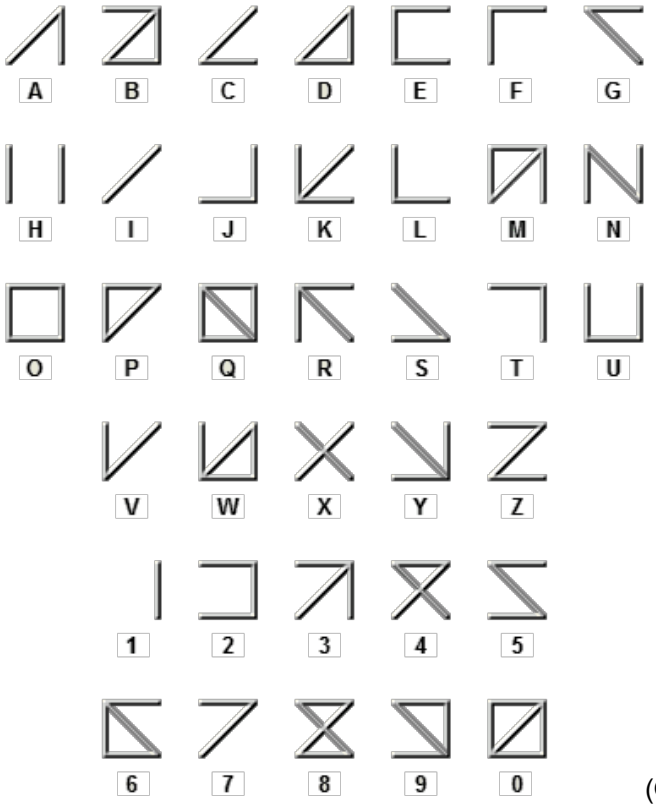
	1	2	3	4	5	6	7	8	9
○	A	B	C	D	E	F	G	H	I
□	J	K	L	M	N	O	P	Q	R
◇	S	T	U	V	W	X	Y	Z	

Das Zeichen für die entsprechende Zeile (Kreis, Quadrat, Raute) wird mit dem Zeichen der entsprechenden Spalte zu einem neuen Zeichen kombiniert. Somit wird der Klartext INFORMATIK wie folgt chiffriert.



Das Quadoo-Alphabet

(zitiert aus https://kryptografie.de/kryptografie/chiffre/quadoo.htm)
Das Quadoo-Alphabet ist eine Quadratschrift für Sehbehinderte, die Ähnlichkeit zur normalen lateinischen Schrift hat. Allerdings ist diese stark vereinfacht, jeder Buchstabe setzt sich aus lediglich bis zu 6 Geraden zusammen:



(Quelle: https://fakoo.de/quadoo.html)

Diese Geraden sind reliefartig, also erhaben ausgeführt und ermöglichen so ein Ertasten des Buchstabens auch für Blinde. Gleichzeitig sind die Buchstaben dem normalen Alphabet so ähnlich, dass sie auch für Sehende mit minimalem Lernaufwand lesbar ist.
Mit den sechs Geraden der Quadoo-Schrift, die entweder gesetzt oder nicht gesetzt sein können ergeben sich insgesamt zwei hoch sechs, also 64 Kombinationsmöglichkeiten. 36 entfallen auf bereits definierte Buchstaben und Ziffern. Es bleiben also noch genügend offene Kombinationen für Sonderzeichen. Die gesamte Definition aller Zeichen findet sich auf der Website von Alexander Fakoó.

Quadoo wurde von Alexander Fakoó im April 2008 erfunden.

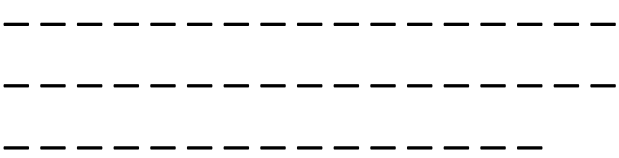
⇒ Aufgabe 5

a) Was spricht für / gegen die Verwendung von Quadoo als Geheimschrift?

- Pro:
  - Jeder Buchstabe des Alphabets hat eine eindeutige Kodierung.
  - Die Symbole sind einfach und klar gehalten → Schablone!

- Kontra:
  - Die Kodierung ist bewusst darauf ausgelegt, dass die Symbole einfach mit dem entsprechenden Buchstaben des Alphabets in Verbindung gebracht werden und somit leicht auswendig gelernt werden können.
  - Buchstaben und die sie kodierenden Symbole sehen sich i.d.R. sehr ähnlich.
  - Aus der Häufigkeit der Symbole kann leicht darauf geschlossen werden, welches Symbol welchen lateinischen Buchstaben kodiert.

b) Auf den ersten Blick sehen die Symbole des folgenden Geheimtextes aus wie diejenigen des Quadoo-Alphabets. Bei genauerem Hinsehen werden aber Unterschiede erkennbar. Wir nennen die verwendete Geheimschrift deshalb **Secret-Quadoo**.



Der Geheimtext wurde mit einer 3 x 9-Tabelle chiffriert. Die Bezeichnungen für Zeilen und Spalten sind aber unbekannt. Das einzig Bekannte ist, dass im ursprünglichen Klartext die am häufigsten vorkommenden Buchstaben E und N sind, und dass die Buchstaben B, C, F und G genau dreimal vorkommen.

Versuche, den Geheimtext zu dechiffrieren und die Chiffrierungstabelle komplett herzustellen.

	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	

Lösung, schrittweise:

Wenn man eine ähnliche Strategie wie in Beispiel oben in Betracht zieht, bestimmen die Zeilen das Innere und die Spalten das Äussere der neuen Zeichen. Das sieht so aus, weil man drei unterschiedliche Zeichen für das Innere ／ ＼ ╳ und neun unterschiedliche für das Äussere hat. Die Frage ist nur, welche der Zeilenbezeichnungen zu welcher Zeile und welche der Spaltenbezeichnungen zu welcher Spalte gehören.

Das häufigste Zeichen ist ◸ und das zweithäufigste ◤. Somit ist klar (rot in der Tabelle), dass wenn ◸ den Buchstaben E und ◤ den Buchstaben N kodiert, muss ┌ die Bezeichnung der fünfte Spalte sein. Die Verteilung der Bezeichnungen für die Zeilen (rot in der Tabelle) ist somit auch klar. Jetzt kennen wird die Chiffrierung der drei Buchstaben E, N und W.

					┌				
／	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	

Wenn wir sie einsetzen, erhalten wir den folgenden Lückentext:

\- - - - - - E N - E - - E - - E N
\- - - - - - - - - E N - - - N E -
\- - E - - - E N - - - - - E N

Wenn man in einem nächsten Schritt die Häufigkeit der Symbole analysiert, sieht man:

／ ↗ ／ ◺ kommen je 3x vor, genau wie, laut Aufgabenstellung, die Buchstaben B, C, F und G.

Die Zweierkombi ／◺ kommt 2x vor, ausserdem je 1x ⧖／◺ (könnte SCH sein) bzw. ／|＼

Das Symbol ／ steht somit wohl für den Buchstaben C, die Zweierkombis könnten CH und CK sein, die Dreierkombi könnte für SCH stehen, was alles auch zu den Zeilenbeschreibungen passt:

	¯	|	|		┌			┘	
／	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	

C H - - - - E N - E - - E - - E N
\- - - S C H - - - E N - - - N E -
\- - E - - - E N - - - C K E N

Damit sind auch die Symbole für A und J (Spalte 1), B und T (Spalte 2), L und U (Spalte 3) und Q und Z (Spalte 8) bekannt. Der Geheimtext ist nun wie folgt dechiffriert:

```
C H - - - - E N - E - B E - - E N
B - T S C H A - T E N - - - N E U
- - E - - - E N B L - C K E N
```

Ab hier lässt sich am Anfang der zweiten Zeile Lückentextes das Wort «Botschaften» erahnen. Somit steht ◹ für O und ◹ für F:

	‾	|	|		⌜	⌜		⌟	
╱	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	

```
C H - F F - E N - E - B E - - E N
B O T S C H A F T E N - O - N E U
- - E - - - E N B L - C K E N
```

Sucht man nach einer logischen Reihe in der Symbolik der Spaltenbeschreibungen und/oder komplettiert den Klartext (→ «Chiffren verbergen Botschaften…»), kann man die drei fehlenden Spaltenbezeichnungen ergänzen. Die Chiffrierungstabelle sieht wie folgt aus:

	⌜	⌜	⌜	‾	⌜	⌜	‾	⌟	⌜
╱	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	

Bei solchen Dechiffrierungsaufgaben ist es hilfreich, gleichzeitig mit der noch unvollständigen Klartext-Tabelle (dem Lückentext) und den bisher erkannten Teilen der Chiffrierungstabelle zu arbeiten. Die bekannten Bezeichnungen von Zeilen und Spalten geben uns wichtige Informationen darüber, welche Symbole welche Buchstaben kodieren können und welche nicht.

Der Klartext lautet:

```
Chiffren verbergen Botschaften vor neugierigen Blicken
```

c) ⇒ **Partnerarbeit**
Chiffriere einzelne Wörter oder kurze Sätze mit Secret-Quadoo und nutze dazu die auf dem Lehrerpult bereitliegenden Streichhölzer. Gib die erzeugten Geheimwörter/-texte deiner Nachbarin/deinem Nachbarn zur Dechiffrierung.

d) ⇒ **Gruppenarbeit (3er- und/oder 4er-Gruppen)** *(adaptiert von Barot et al., 2022, S. 56)*
Entwickelt eine eigene einfache Geheimschrift. Nutzt dazu ebenfalls (nur) die auf dem Lehrerpult bereitliegenden Streichhölzer. Chiffriert mit eurer Geheimschrift einen Klartext.

Gebt nun die Beschreibung (Tabelle, Zeichnungen, …) der Geheimschrift für die Dauer von 1 – 2 Minuten der Gruppe rechts von euch zum Auswendiglernen. Nach der Rückgabe der Beschreibung übergebt ihr der Gruppe euren Geheimtext zum Dechiffrieren.

e) ⇒ **Zusatz-Partneraufgabe**
Das Quadoo-Alphabet wurde auch mit dem Ziel entwickelt, blinden oder sehbehinderten Menschen die Möglichkeit zu bieten, auf taktile und haptische Weise auf Texte zuzugreifen.

Testet, ob auch das Secret-Quadoo-Alphabet diesem Anspruch gerecht werden könnte. Holt beim Lehrerpult eine Augenbinde und versucht das Dechiffrieren mit verbundenen Augen.

⇒ Aufgabe 6

a) Fasse in einem Satz zusammen, was die Geheimschrift von Polybios und Secret-Quadoo gemeinsam haben.

Beide Geheimschriften basieren auf der Kodierung von Buchstaben durch andere Symbole oder Symbolfolgen. Der Fachbegriff dafür lautet **Substitution**.

b) Was ist der grundlegende, methodische Unterschied zwischen diesen beiden Geheimschriften und der Geheimschrift Skytale?

Die Geheimschrift Skytale basiert auf **Transpositionen** (dem Austausch der Positionen von Buchstaben), während die Geheimschrift von Polybios und Secret-Quadoo **Substitutionen** nutzen.

Was mit dieser Unterrichtseinheit bewirkt werden kann

Die Unterrichtseinheit "Geheimschriften der Antike" vermittelt den SuS grundlegende Kenntnisse über verschiedene Chiffriermethoden, die in der antiken Zeit verwendet wurden. Dabei lernen sie nicht nur die Funktionsweisen von Transposition (Skytale) und Substitution (Polybios und Secret-Quadoo) kennen, sondern auch die Bedeutung von Klartext- und Geheimtextalphabeten in diesen Verfahren.

Die SuS werden befähigt, Algorithmen zur Chiffrierung und Dechiffrierung anzuwenden, um Geheimtexte zu erstellen und zu entschlüsseln.

Durch Reflexion über die Vor- und Nachteile unterschiedlicher Chiffriermethoden gewinnen die SuS Einblicke in Sicherheitsaspekte und die Schwierigkeiten bei der Dechiffrierung. Dies ermöglicht es ihnen, die Bedeutung und Anwendung von Chiffriermethoden in der modernen Kommunikation und Sicherheit besser zu verstehen und zu evaluieren.

Literatur

Barot, M., Dorn, B., Fourny, G., Gallenbacher, J., Hromkovič, J., Lacher, R. (2022): *INFORMATIK – Data Science und Sicherheit.* Baar: Klett und Balmer.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Kratwohl, D. R. (1956). *Taxonomy of educational objectives: The classification of educational goals.* Vol. Handbook I: Cognitive domain. New York: David McKay Company.

EDK (2017): Rahmenlehrplan für die Maturitätsschulen: Informatik. Abgerufen am 11.10.2023 unter https://www.edk.ch/de/themen/gymnasium.

Fakoó, A. (2023). *Das Quadoo-Alphabet.* Abgerufen am 11.10.2023 unter https://fakoo.de/quadoo.html.

Kryptografie.de (2023). *Quadoo Schrift Code.* Abgerufen am 11.10.2023 unter https://kryptografie.de/kryptografie/chiffre/quadoo.htm.