Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Alles durcheinander – Transpositionschiffren

Skytale

Vor über 2500 Jahren nutzten die Spartaner Skytalen zur Übermittlung von geheimen Nachrichten. Sender und Empfänger besaßen je einen dieser Zylinder. Der Sender wickelte ein schmales Band aus Leder spiralförmig um seine Skytale und schrieb dann der Länge nach die Nachricht auf das Band. War das Band abgewickelt, konnte die Nachricht nur von einer Person gelesen werden, die eine Skytale genau desselben Radius hatte.

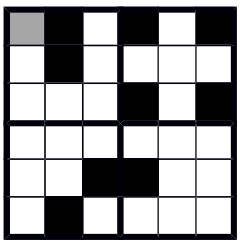
1) Finde die Skytale, mit der du den gegebenen Geheimtext entschlüsseln kannst.
2) Erläutere eine Strategie, um den Geheimtext auch ohne Skytale zu knacken.

Muster und Raster

Den Klartext entlang bestimmter Muster oder in bestimmte Raster zu schreiben, waren bis in die 1950er Jahre beliebte Variante der Verschlüsselung. Zur besseren Lesbarkeit der Texte wurden diese in Fünferblöcke gegliedert. Die Leerzeichen beim Entschlüsseln ignorieren.

3) Entschlüssle `VAENZ LELID OERSB HNSTC EOTEI HNRAN KRUIL X` mit der 6x6-Quadrat-Matrixverschlüsselung. Nutze ein leeres FLEISSNER-Raster.
4) `ZCTMC EUIAK NSIDS HAGAN CZNNI HETEJ EZKEC UNR` entstand durch Anwendung der Methode ZickZack mit dem Schlüssel 4. Was schreibt der Absender?

Schablonen (FLEISSNERsche Schablone)



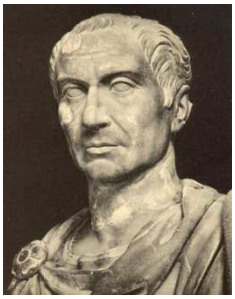
JULES VERNE verwendet in seinem Roman Mathias Sandorf die Kunst der Ver- und Entschlüsselung mithilfe einer FLEISSNER-Schablone. Auf dieser, 1881 vom österreichischen Oberst EDUARD FLEISSNER VON WOSTROWITZ entwickelten 6x6-Matrix-Schablone befinden sich an bestimmten Stellen (schwarz markiert) Löcher. Die Schablone wird mit der grauen Ecke oben links auf ein Blatt gelegt und in die Löcher die Buchstaben des Klartextes eingetragen. Dann wird die Schablone um neunzig Grad nach rechts gedreht und es weiteren Buchstaben eingetragen usw.

5) Verschlüssele `HAB KENNWORT IN ALTEN BAUM GELEGT AGENT OO X.`
6) `CSHCE HLLSA MOSRT UAERG MEBNE NSSIQ TEBCU A`
   Was schreibt der Absender?

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Die Geheimsprache von Julius Caesar



GAIUS JULIUS CAESAR (*100 v. Chr.; † 44 v. Chr.) war ein römischer Staatsmann, Feldherr und Autor. Nach Überlieferung des römischen Schriftstellers SUETON übermittelte CAESAR seine militärische Korrespondenz stets verschlüsselt. Er gilt als Begründer der klassischen Kryptologie. Aus heutiger Sicht ist das Caesar-Verfahren zwar primitiv, ist aber der Urvater aller Verfahren, bei die Zeichen des Klartextes durch andere Zeichen oder Symbole ausgetauscht werden. Solche Verfahren bezeichnet man als **Substitutionsverfahren**.

CAESAR ersetzte jeden Buchstaben im Klartext mit einem Buchstaben, der 3 Stellen zyklisch weiter hinten im Alphabet steht, also mit dem Schlüssel A → D:

Geheimtextalphabet:	DEFGHIJKLMNOPQRSTUVWXYZABC
Klartextalphabet:	ABCDEFGHIJKLMNOPQRSTUVWXYZ

1) Entschlüssle CAESARS Ausspruch: `LFK NDP, VDK XQG VLHJWH.`
2) Verschlüssle mit Hilfe der Caesar-Scheibe und dem Schlüssel `T` den lateinischen Caesar-Spruch: „Lacta alea est“.
3) Versuche folgende Nachricht zu knacken:
   a) `SQUIQH MQH ISXBQK`
   b) `EWFV EWCCISF`

CAESAR mit Schlüsselwort

Zum Brechen des einfachen CAESAR-Verfahrens mit Schlüsselbuchstabe muss man nur maximal 25 Möglichkeiten probieren. Das Prinzip ist also nicht sicher. Eine bessere Anordnung des Geheimalphabets erhält man mit Hilfe eines Schlüsselwortes und Startbuchstaben, wie in Aufgabe 3 b).

Werden die Buchstaben so durcheinander gewürfelt, ergeben sich für einen Angreifer $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 - 1 = 403291461126605635583999999$ Varianten. Diese können selbst von modernen Rechnern nicht in einer vernünftigen Zeit durchprobiert werden (350 Millionen Versuche pro Sekunde per Brute Force). Zum Brechen der Verschlüsselung müssen statistische Methoden, die aus der Analyse der Sprache resultieren, eingesetzt werden.

4) Berechne die maximale Zeit für das Finden des korrekten Geheimtextalphabets mit 26 Buchstaben bei einem unbekannten Substitutionsverfahren.

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Die Verschlüsselungsverfahren von POLYBIOS und PLAYFAIR

POLYBIOS

	α	β	γ	δ	ε
α	A	B	Γ	Δ	E
β	Z	H	Θ	I	K
γ	Λ	M	N	Ξ	O
δ	Π	P	Σ	T	Y
ε	Φ	X	Ψ	Ω	

Archäologen fanden bei Ausgrabungen verschiedene Papyrusrollen des Griechen POLYBIOS (* 200 v. Chr.; † 120 v. Chr.). Diese enthielten unter anderem das nebenstehende Quadrat als auch den Geheimtext αεδεδββββεααεεαγδεδβγεδγ. Ihnen war schnell klar, dass es sich um ein Verschlüsselungsverfahren handeln muss.

1) Versuche den **griechischen** Klartext zu bestimmen.
2) Beschreibe das Verschlüsselungsverfahren.
3) Übertrage das Verfahren ins Deutsche. Nutze als Bezeichner die Zahlen 1 bis 5.
4) Verschlüssle den griechischen Ausspruch „Arzt, heil dich selbst“.

Um eine Entschlüsselung zu erschweren, kann man die Reihenfolge der Buchstaben durch ein Schlüsselwort verändern.

5) Einige Dich mit deinem Nachbarn auf ein Schlüsselwort, füge es in das deutsche POLYBIOS-Quadrat ein und fülle mit den verbliebenen Buchstaben systematisch auf.
6) Sendet Euch nun verschlüsselte Nachrichten mit der Angabe zu den geplanten Wochenendaktivitäten.

PLAYFAIR

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

Fast 2000 Jahre nach POLYBIOS entwickelt der englische Physiker CHARLES WHEATSTONE das nach seinem Bekannten BARON PLAYFAIR VON ST. ANDREWS benannte PLAYFAIR-Verfahren. WHEATSTONE ordnet die Buchstaben ebenfalls in einem Quadrat, ggf. mit Schlüsselwort an. Der Klartext wird in Zweierbuchstabenpaare zerlegt. Dabei müssen Paare mit gleichen Buchstaben oder übrig gebliebene Buchstaben mit Füllzeichen verändert werden. Anschließend kann die paarweise Verschlüsselung beginnen.

Beispiel:

Klartext: `TREFFPUNKT GASSE → TR EF FP UN KT GA SX SE`

Geheimtext: `US AK KL SP IU FB XC UC`

7) Ermittle die Verschlüsselungsregeln für PLAYFAIR. Unterteile in die Fälle A) beide Buchstaben stehen in der gleichen Zeile, B) beide Buchstaben stehen in der gleichen Spalte, C) die Buchstaben stehen in unterschiedlichen Zeilen und Spalten.
8) Entschlüssle den Geheimtext `PB UG YM SU CA PS UY CP` und erläutere die Bedeutung des Klartextes.

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

VIGENÈRE – polyalphabetische Verfahren

Der Angriffspunkt aller Verfahren, die nur ein Geheimtextalphabet verwenden, ist die Häufigkeit des Auftretens bestimmter Buchstaben und Buchstabengruppen. Der französischer Diplomat BLAISE DE VIGENÈRE (* 1523; † 1596) entwickelte auf der Grundlage der Idee eines Benediktinermönches ein Verfahren, das einem Klartextbuchstaben verschiedene Geheimtextbuchstaben zuordnet. Dazu benötigen wir für einen Buchstaben des Schlüsselworts eine eigene Caesar-Scheibe.

Beispiel

Schlüssel UNI → drei Caesar-Scheiben mit den Schlüsseln U, N und I

Schlüssel: `UNIUNIUNI`

Klartext: `SUEDSTADT`

Geheimtext: `MHMXFBUQB`

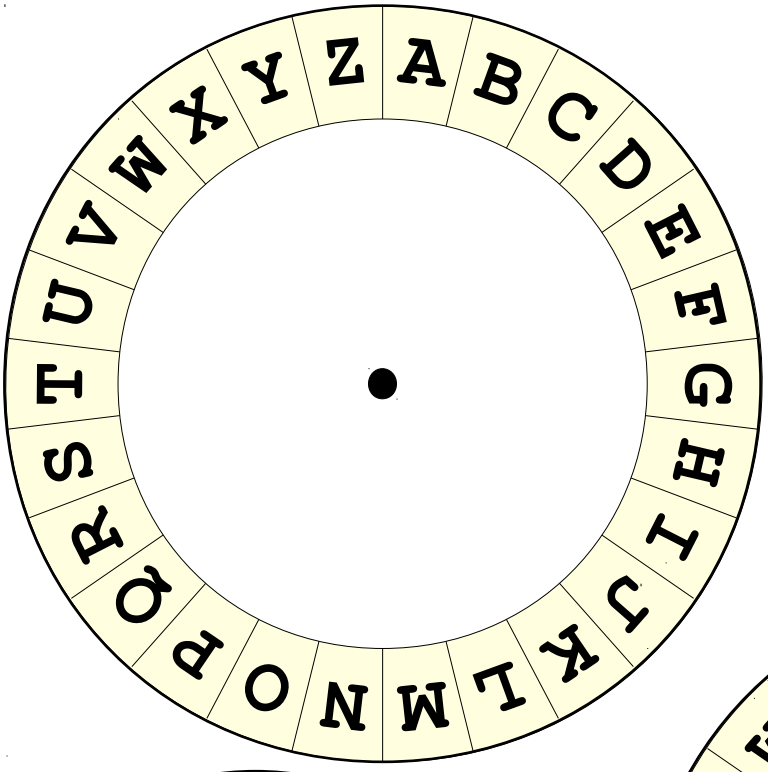
Jeder Klartextbuchstabe wird mit der Caesar-Scheibe verschlüsselt, die der Schlüsselbuchstabe angibt.

1) Prüfe das Beispiel nach.
2) Beschreibe die Auswirkung des Verfahrens auf die Häufigkeit der Buchstaben.
3) Entschlüssle den Text `FNVXRANNOOAO` mit dem Schlüssel `UNI`?

100% sicher

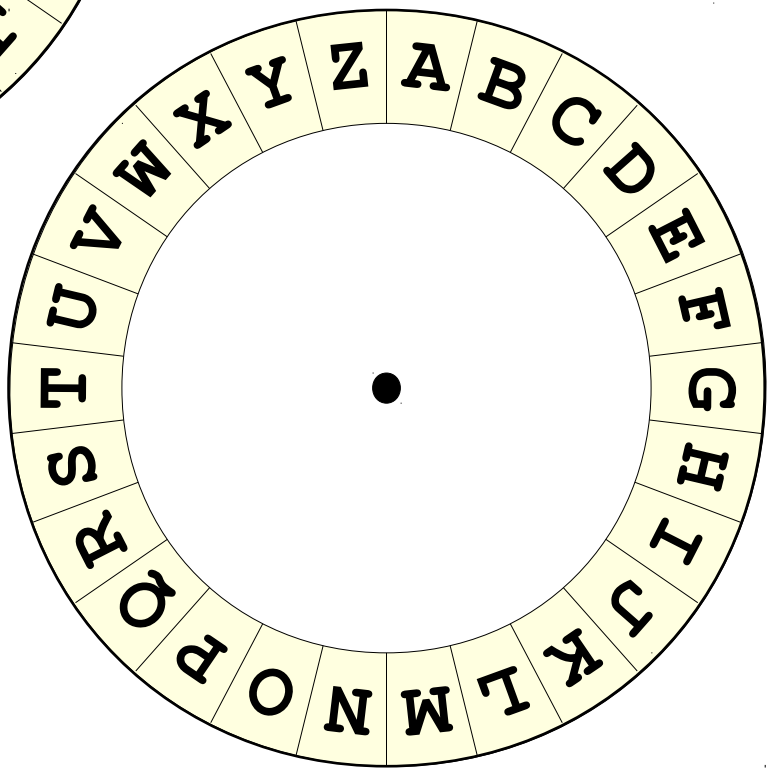
4) Der Geheimtext `MHOAYU` wurde mit dem VIGENÈRE-Verfahren verschlüsselt.
   a) Zeige, dass sich sowohl der Klartext `SCHULE` als auch der Klartext `PAUSEN` in den Geheimtext überführen lassen.
   b) Finde einen weiteren Klartext, der sich aus dem Geheimtext rekonstruieren lässt.
5) Wann ist das VIGENÈRE-Verfahren sicher?

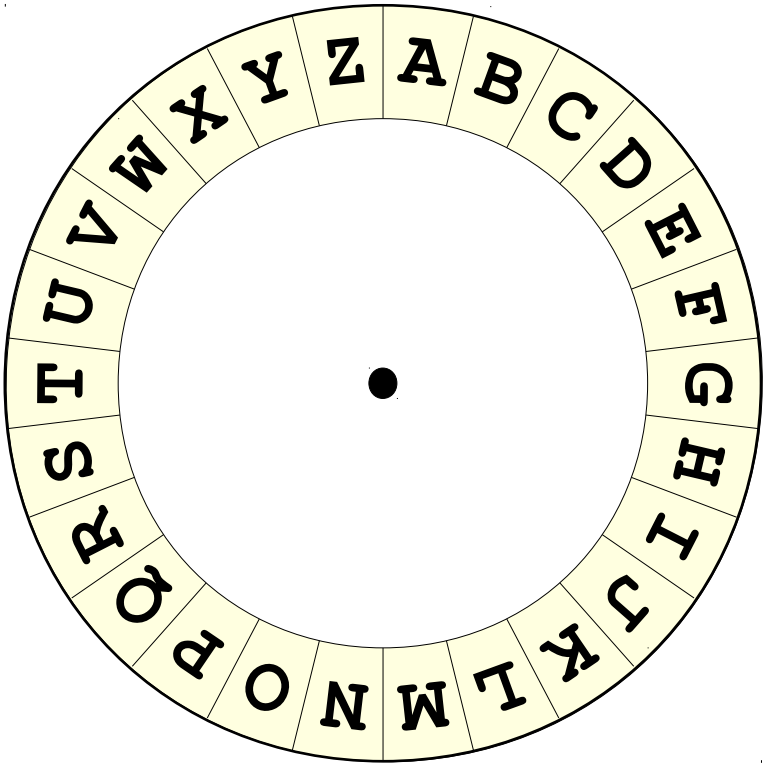
Die Erhöhung der Sicherheit geht mit der Verlängerung und der Einmaligkeit des Schlüssels einher. Hat der Schlüssel eine zufällige Buchstabenreihung, die gleiche Länge wie der Klartext und wird nur einmal benutzt, so entsteht das einzige, mathematisch beweisbar nicht knackbare Verfahren: **One Time Pad**. Der diplomatischen Dienst in der Weimarer Republik, der sog. „Heiße Draht“ zwischen den Regierungen während des kalten Kriegs und CHE GUEVARA benutzten One Time Pads.

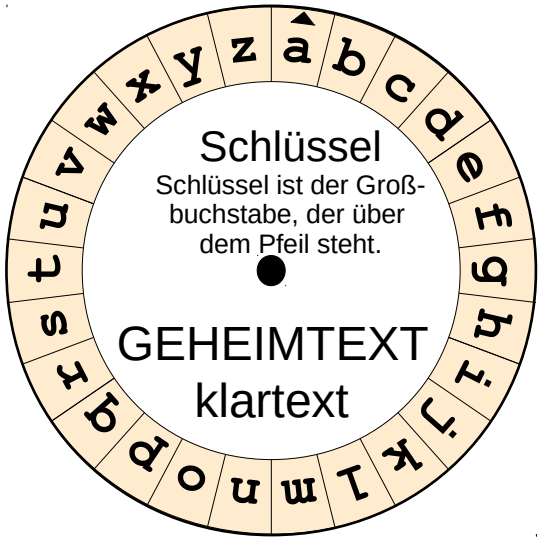

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z


a b c d e f g h i j k l m n o p q r s t u v w x y z
Schlüssel
Schlüssel ist der Groß-
buchstabe, der über
dem Pfeil steht.
GEHEIMTEXT
klartext


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
Schlüssel
Schlüssel ist der Groß-
buchstabe, der über
dem Pfeil steht.
GEHEIMTEXT
klartext


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


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


a b c d e f g h i j k l m n o p q r s t u v w x y z
Schlüssel
Schlüssel ist der Groß-
buchstabe, der über
dem Pfeil steht.
GEHEIMTEXT
klartext