

Gruppenpuzzle zu Substitutionsverfahren

In Klasse 11 haben Sie die Substitution als eine Möglichkeit der Verschlüsselung kennengelernt. Wenn jedem Klartextzeichen genau ein Geheimtextzeichen zugeordnet wird, wie z. B. beim Caesar-Verfahren oder bei der Verwendung einer eindeutigen Zuordnungstabelle, spricht man von einer monoalphabetischen Substitution. Solche Verfahren sind für längere Texte nicht sehr sicher, da sie mithilfe einer Häufigkeitsanalyse geknackt werden können.

Ziel des Gruppenpuzzles ist es nun weitere Beispiele für Substitutionsverfahren dahingehend zu untersuchen, ob sie eine Verbesserung im Vergleich zu einer einfachen monoalphabetischen Verschlüsselung darstellen.

Stammgruppen:

Jeder erarbeitet zunächst in der Expertengruppe ein Substitutionsverfahren zur Verschlüsselung. Teilen Sie dazu die folgenden Verfahren unter sich auf:

- homophone Substitution*
- Polybios-Verfahren*
- Rotoren**
- Vigenère-Verfahren**

Hinweis: Die Sternchen geben Ihnen eine Orientierung hinsichtlich der Komplexität der Verfahren.

Expertengruppen:

- Erarbeiten Sie in der Expertengruppe anhand der bereitliegenden Materialien¹ das Verschlüsselungsverfahren, das Sie sich ausgesucht haben.
- Bereiten Sie sich darauf vor, Ihrer Stammgruppe das Verfahren anhand eines Beispiels zu erläutern.

¹ Hinweis für Lehrkräfte: Die Materialien für die homophone Substitution, das Polybios-Verfahren und das Vigenère-Verfahren befinden sich in diesem Dokument. Für das Verfahren „Rotoren“ wird auf Materialien aus dem Spioncamp der Uni Wuppertal¹ zurückgegriffen. Die Rotoren sollten im Vorfeld vorbereitet werden. Die Materialien stehen über die folgenden Links zur Verfügung:

- https://ddi.uni-wuppertal.de/website/repoLinks/v277_substitution-p-rotor-station.pdf
- https://ddi.uni-wuppertal.de/website/repoLinks/v249_substitution-p-rotor-mat0.pdf
- https://ddi.uni-wuppertal.de/website/repoLinks/v299_substitution-p-rotor-ab1.pdf

Stammgruppen:

- Stellen Sie sich die Verschlüsselungsverfahren, die Sie in den Expertengruppen erarbeitet haben, gegenseitig vor. Beginnen Sie dabei mit der homophonen Substitution und dem Polybios-Verfahren.
- Klären Sie für jedes Verfahren, bei welcher Information es sich um den Schlüssel handelt.
- Gehen Sie davon aus, dass ein Geheimtext gefunden wird und bekannt ist, mit welchem der vier Verschlüsselungsverfahren er verschlüsselt wurde. Untersuchen Sie für jedes Verfahren, ob sich der Geheimtext mithilfe einer Häufigkeitsanalyse knacken ließe.
- Erläutern Sie den Unterschied zwischen einer einfachen monoalphabetischen, einer homophonen und einer polyalphabetischen Substitution. Ordnen Sie die Abbildungen 1 bis 3 passend zu. Ordnen Sie auch die untersuchten Verfahren entsprechend zu.

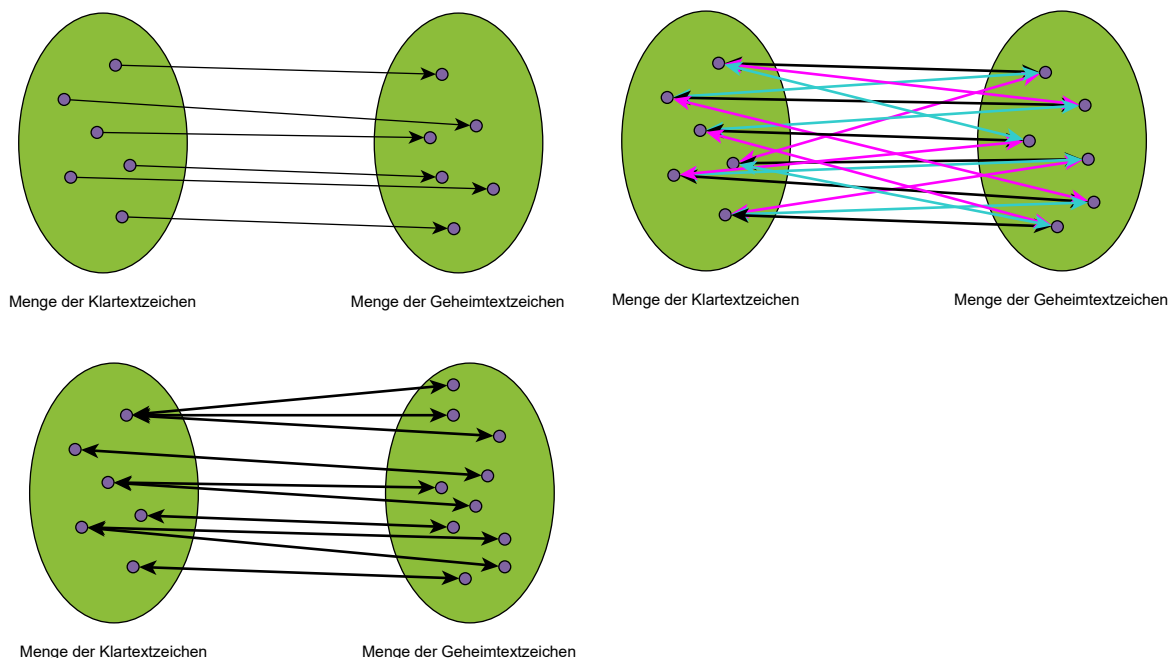


Abbildung 1: Abbildungen zu Aufgabenteil d)

- Untersuchen Sie, inwieweit die Verschlüsselung mithilfe eines Polybios-Quadrats sicherer wird, wenn zusätzlich eine Transposition durchgeführt wird. Sollte die Transposition vor oder nach der Substitution mithilfe des Polybios-Quadrats durchgeführt werden?

Homophone Substitution

Bei der *homophonen Substitution* werden häufiger auftretenden Klartextzeichen mehrere Geheimtextzeichen zugeordnet. Bei der Verschlüsselung wird für diese Klartextzeichen zufällig eines der zugeordneten Geheimtextzeichen ausgewählt.

Eine Zuordnungstabelle könnte z. B. so aussehen:

Klartext- zeichen	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheim- textzeichen	D W	5	N	M ?	A F T 1 S &	6	B	8 @	O Q	U	J	7	V	C 2 =	X	P	E	Z 3	G K	Y 4	R \$	H	0	L	9	I

Tabelle 1: Zuordnung für homophone Substitution

Verwendet man als Geheimtextzeichen die Zahlen 00 bis 99 kann die unterschiedliche Häufigkeit der Buchstaben noch besser berücksichtigt werden²:

Häufigkeit in Prozent ca.	6	2	2	5	17	2	3	5	8	1	1	3	2	10	2	1	1	7	7	6	4	1	1	1	1	1
Klartext- zeichen	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheim- textzeichen	31 38 57 65 72 98	00 18 58 80 27 30 33 43 56 64 71 73 81 82 88 92 95	16 44 17 21 17 27 21 29 30 33 43 56 64 71 73 81 82 88 92 95	06 09 09 17 21 27 30 33 43 56 64 71 73 81 82 88 92 95	02 09 17 21 27 30 33 43 56 64 71 73 81 82 88 92 95	15 70 29 50 63 68 76 83	03 10 29 50 63 68 76 83	28 69 79 50 63 68 76 83	14 34 42 50 63 68 76 83	45 94 19 97 22 01 20 07 23 05 04 08 78 99 37 49 24	94 19 97 22 01 20 07 23 05 04 08 78 99 37 49 24	19 97 22 01 20 07 23 05 04 08 78 99 37 49 24	97 22 01 20 07 23 05 04 08 78 99 37 49 24	22 01 20 07 23 05 04 08 78 99 37 49 24	01 20 07 23 05 04 08 78 99 37 49 24	20 07 23 05 04 08 78 99 37 49 24	07 23 05 04 08 78 99 37 49 24	23 05 04 08 78 99 37 49 24	05 04 08 78 99 37 49 24	04 08 78 99 37 49 24	08 78 99 37 49 24	78 99 37 49 24	99 37 49 24	37 49 24	49 24	24

Tabelle 2: Zuordnung für homophone Substitution

Aufgaben:

- Verschlüsseln Sie das Wort „entenrennen“ mit Tabelle 1.
- Entschlüsseln Sie den Geheimtext 702132822399647794 mithilfe von Tabelle 2.
- Begründen Sie, dass die Zahlen 0 bis 9 in Tabelle 2 in der Form 00, 01, 02, ..., 09 dargestellt werden müssen.
- Erläutern Sie, inwieweit die homophone Substitution eine Verbesserung einer einfachen monoalphabetischen Substitution darstellt.

² nach einer Idee aus Beutelspacher, A. (2009). *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. (9. Aufl.) Vieweg + Teubner.

Polybios-Quadrate

Verschiedene Verschlüsselungsverfahren basieren auf der Verwendung von Polybios-Quadraten. Bei der Verschlüsselung mithilfe eines Polybios-Quadrats wird jeder Buchstabe durch eine Kombination aus zwei Zeichen ersetzt.

Für das Erstellen eines Polybios-Quadrats benötigen Sie zunächst ein Schlüsselwort, z. B. *informatik*. Tragen Sie dieses Wort in eine Tabelle mit 5 Spalten und 5 Zeilen ein. Lassen Sie dabei wiederholt auftretende Buchstaben weg. Aus *informatik* wird also *informatk*. Füllen Sie die restlichen Plätze mit den fehlenden Buchstaben des Alphabets in alphabetischer Reihenfolge auf. Da die Tabelle nur 25 Plätze hat, lässt man den im Deutschen selten auftretenden Buchstaben j weg und ersetzt ihn im Klartext ggf. durch ein i.

	A	D	F	G	X
A	i	n	f	o	r
D	m	a	t	k	b
F	c	d	e	g	h
G	l	p	q	s	u
X	v	w	x	y	z

Abbildung 1: Polybios-Quadrat
für das Schlüsselwort
informatik

Je nach Verfahren werden die Zeilen und Spalten nummeriert oder mit Buchstaben versehen. Das ADFGX-Verfahren verwendet z. B. für die Beschriftung der Zeilen und Spalten die Zeichen A, D, F, G und X. Für das Schlüsselwort *informatik* erhält man so das Polybios-Quadrat in Abbildung 1.

Beim Verschlüsseln wird jedes Zeichen durch die Kombination aus *Zeilennummer* und *Spaltennummer* ersetzt. Das *t* wird z. B. zu *DF* und das *v* zu *XA*.

Aufgaben:

- Entschlüsseln Sie den Geheimtext XAFFAXAXDDDF mithilfe des Polybios-Quadrats in Abbildung 1.
- Erstellen Sie das Polybios-Quadrat für das Schlüsselwort *seifenblase*. Verschlüsseln Sie damit den Vornamen *annabel*.
- Untersuchen Sie, ob es sich bei dem ADFGX-Verfahren um eine monoalphabetische Substitution handelt.

Vigenère-Verfahren

Das Vigenère-Verfahren wurde im 16. Jahrhundert von dem Franzosen Blaise de Vigenère entwickelt. Es basiert auf der Caesar-Verschlüsselung. Bei der Verschlüsselung eines Textes wird jedoch nicht nur eine Verschiebung verwendet. Stattdessen wechselt die Verschiebung von Zeichen zu Zeichen. Statt eines Geheimtextalphabets gibt es somit bis zu 26 verschiedene Geheimtextalphabete. Man spricht daher von einer **polyalphabetischen Substitution**.

Der Schlüssel beim Vigenère-Verfahren ist ein Wort, z. B. TULPE. Das Schlüsselwort wird immer wieder über den Klartext geschrieben. Der aktuelle Buchstabe im Schlüsselwort gibt an, mit welchem Buchstaben an dieser Stelle das A verschlüsselt wird und legt damit fest, um wie viele Stellen das Klartextzeichen für die Verschlüsselung verschoben wird. Wenn im Beispiel also bei dem ersten Klartextzeichen das A mit einem T verschlüsselt wird, ergibt sich eine Verschiebung um 19, so dass das G mit einem Z verschlüsselt wird. Beim zweiten Buchstaben wird das A mit einem U verschlüsselt. Für das R im Klartext ergibt sich daher an dieser Stelle ein L im Geheimtext usw.

Als Hilfsmittel können Sie eine Caesar-Scheibe oder das Vigenère-Quadrat in Abbildung 1 verwenden, das alle 26 möglichen Verschiebungen enthält. In der obersten Zeile steht das Klartextalphabet. In den Zeilen darunter stehen dann die Verschiebungen um eine, um zwei, um drei Stellen usw. In Abbildung 1 sind die Zeile und Spalte, die für die Verschlüsselung des Klartextzeichens G mit dem Schlüsselbuchstaben T benötigt werden, gelb markiert.

Beispiel:

Schlüssel	T	U	L	P	E	T		U	L	P	E	T		U	L		P	E	T	U
Klartext	G	R	O	S	S	E		P	A	R	T	Y		U	M		N	E	U	N
Geheimtext	Z	L	Z																	H

Aufgabe 1:

- Verschlüsseln Sie den Klartext im obigen Beispiel vollständig.
- Beschreiben Sie das Vorgehen bei der Verschlüsselung eines Klartextzeichens mithilfe des Vigenère-Quadrats.

Aufgabe 2:

- Entschlüsseln Sie den Geheimtext „COTGO ULE NYI VSYJD“. Das Schlüsselwort ist KURZ.

Schlüssel	K	U																		
Klartext	S																			
Geheimtext	C	O																		

- Beschreiben Sie das Vorgehen bei der Entschlüsselung eines Geheimtextzeichens mithilfe des Vigenère-Quadrats.

Aufgabe 3: Machen Sie an den Beispielen aus Aufgabe 1 und 2 deutlich, dass es sich um eine polyalphabetische Substitution handelt. Wie viele verschiedene Geheimtextalphabete werden in den Beispielen verwendet?

Vigenère-Quadrat³:

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

Abbildung 1: Vigenère-Quadrat

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Von der Lizenz ausgenommen ist das InfSII-Logo.

³ Die Darstellung des Vigenere-Quadrats entspricht der Darstellung in den Ergänzenden Hinweisen zum Kerncurriculum Informatik in Niedersachsen, die an 2027 als Hilfsmittel in zentralen Prüfungsaufgaben verwendet werden dürfen. (vgl. Niedersächsisches Kultusministerium (Hrsg.) (2025) *Ergänzende Hinweise zum Kerncurriculum Informatik für die gymnasiale Oberstufe am Gymnasium, an der Gesamtschule sowie für das Kolleg*. <https://cuvo.nibis.de/index.php?p=download&upload=736> [Datum des Zugriffs: 13.08.2025])