

## Gruppenpuzzle zu Substitutionsverfahren

### **Stammgruppen:**

Jeder erarbeitet zunächst in der Expertengruppe ein Ersetzungsverfahren zur Verschlüsselung. Teilt dazu die folgenden Verfahren unter euch auf:

- homophone Substitution\*
- Polybios-Verfahren\*
- Enigma/Rotoren\*\*
- Vigenère-Verfahren\*\*

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

### **Expertengruppen:**

- a) Erarbeitet in der Expertengruppe anhand der bereitliegenden Materialien das Verschlüsselungsverfahren, das ihr euch ausgesucht habt.
- b) Bereitet euch darauf vor, eurer Stammgruppe das Verfahren anhand eines Beispiels zu erläutern.

### **Stammgruppen:**

- a) Stellt euch die Verschlüsselungsverfahren gegenseitig vor.
- b) Klärt für jedes Verfahren, bei welcher Information es sich um den Schlüssel handelt.
- c) Stellt euch vor, ihr findet einen Geheimtext und wisst, mit welchem der vier Verschlüsselungsverfahren er verschlüsselt wurde. Diskutiert, für jedes Verfahren, ob sich der Text mit einer Häufigkeitsanalyse knacken ließe.
- d) Erläutert den Unterschied zwischen einer monoalphabetischen und einer polyalphabetischen Substitution.

## 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	5	N	M	A	6	B	8	O	U	J	7	V	C	X	P	E	Z	G	Y	R	H	0	L	9	I
	W			?	F			@	Q					2				3	K	4	\$					
				T	1									=												
				S																						
				&																						

Tabelle 1: Zuordnung für homophone Substitution

Verwendet man als Geheimtextzeichen die Zahlen 00 bis 99 kann die unterschiedliche Häufigkeit der Buchstaben noch besser berücksichtigt werden<sup>1</sup>:

Häufigkeit 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	00	16	06	02	15	03	28	14	45	94	19	97	22	01	20	07	23	05	04	08	78	99	37	49	24	
	38		18	44	09	70	10	69	34			35		26	12			40	11	48	25						
	57			58	17		29	79	42			59		39				47	13	61	32						
	65			80	21				50					46				60	36	67	41						
	72				27				63					62				74	86	87							
	98				30				68					66				77	91	90							
					33				76					75				93	96								
					43				83					84													
					56									85													
					64									89													
					71																						
					73																						
					81																						
					82																						
					88																						
					92																						
				95																							

Tabelle 2: Zuordnung für homophone Substitution

### Aufgaben:

- Verschlüssele deinen Vornamen mit Tabelle 1 oder Tabelle 2.
- Entschlüssele den Geheimtext 31157033220038620664 mithilfe von Tabelle 2.
- Begründe, warum die Zahlen 0 bis 9 in Tabelle 2 in der Form 00, 01, 02, ..., 09 aufgeschrieben werden müssen.

<sup>1</sup> nach einer Idee aus Beutelspacher, A. (2009). *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. (9. Aufl.) Vieweg + Teubner.

## Polybios-Verfahren

Bei der Verschlüsselung mithilfe eines Polybios-Quadrats wird jeder Buchstabe durch eine Kombination aus zwei Ziffern ersetzt.

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

Nummeriere die Spalten und Zeilen mit 1 bis 5. Für das Schlüsselwort *informatik* erhältst du so das Polybios-Quadrat in Abbildung 1.

Ersetze nun beim Verschlüsseln jedes Zeichen durch die Kombination aus *Zeilennummer* und *Spaltennummer*. Das *t* wird z. B. zu *23* und das *v* zu *51*.

### Aufgaben:

- Entschlüssele den Geheimtext 13 15 33 11 23 22 34 mithilfe des Polybios-Quadrats in Abbildung 1.
- Erstelle das Polybios-Quadrat für das Schlüsselwort *regenschirm*. Verschlüssele damit deinen Vornamen.

	1	2	3	4	5
1	i	n	f	o	r
2	m	a	t	k	b
3	c	d	e	g	h
4	l	p	q	s	u
5	v	w	x	y	z

Abbildung 1: Polybios-Quadrat  
für das Schlüsselwort  
*informatik*

## 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 einem Geheimtextalphabet 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. „TIGER“. 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 „I“ verschlüsselt. Für das „e“ im Klartext ergibt sich daher an dieser Stelle ein „M“ im Geheimtext usw.

Als Hilfsmittel kannst du 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 benötigte Zeile und Spalte für die Verschlüsselung des Klartextzeichens „g“ mit dem Schlüsselbuchstaben „T“ gelb markiert.

### Beispiel:

Schlüssel	T	I	G	E	R	T	I	G		E	R	T	I	G	E	R		T	I		G	E	R	T
Klartext	g	e	h	e	i	m	e	s		t	r	e	f	f	e	n		u	m		a	c	h	t
Geheimtext	Z	M	N																					M

### Aufgabe 1:

- Verschlüssele den Klartext im obigen Beispiel vollständig.
- Beschreibe das Vorgehen bei der Verschlüsselung mithilfe des Vigenère-Quadrats.

### Aufgabe 2:

- Entschlüssele den Geheimtext „JIC TILLUF MDU HIT FMSY“. Das Schlüsselwort ist GELB.

Schlüssel	G	E	L		B																			
Klartext	d																							
Geheimtext	J	I	C		T																			

- Beschreibe das Vorgehen bei der Entschlüsselung mithilfe des Vigenère-Quadrats.

**Aufgabe 3:** Mache 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-Quadrat:

klar	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Abbildung 1: Vigenère-Quadrat

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](https://creativecommons.org/licenses/by-nc-sa/4.0/). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.

