2. Infoblatt:

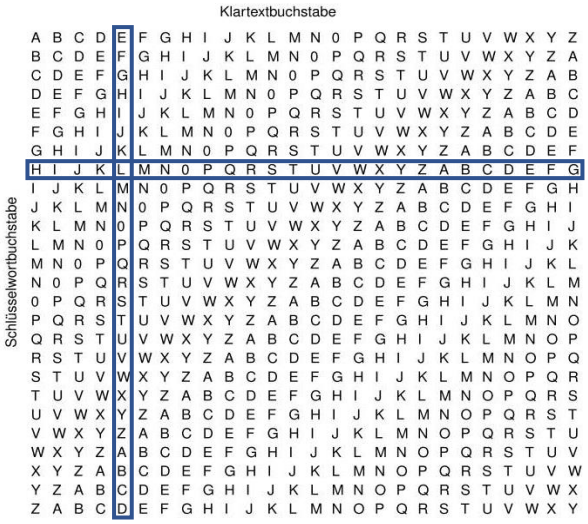
Vigenère

Wir haben auf dem ersten Aufgabenblatt gesehen, dass Geheimtexte, die mit einem monoalphabetischen Verfahren verschlüsselt sind, oft mit einer Häufigkeitsanalyse geknackt werden können. Bei einer **polyalphabetischen Substitution** wird ein Buchstabe in der Regel mit verschiedenen Buchstaben oder Zeichen verschlüsselt.

Ein polyalphabetisches Verfahren wurde von Blaise de Vigenère im 16. Jahrhundert entwickelt und nach ihm benannt. Dafür wird zunächst ein Schlüsselwort benötigt. In diesem Beispiel ist es GEHEIM. Wir schreiben es so oft über den Klartext, bis jedem Klartextbuchstaben ein Buchstabe des Schlüsselwortes zugeordnet ist.

Schlüssel:	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E
Klartext:	T	R	E	F	F	P	U	N	K	T	K	I	R	C	H	E
Geheimtext:	Z	V	L													

Nun wird jeder einzelne Buchstabe, wie bei der Cäsar-Verschlüsselung verschlüsselt. Um das T zu verschlüsseln, wird die Cäsar-Scheibe so eingestellt, dass das A mit dem Buchstaben über dem T, also dem G verschlüsselt wird. So wird aus dem T ein Z. Für das R muss die Scheibe so gedreht werden, dass das E unter dem A ist.



Damit nicht so viel gedreht werden muss, kann das **Vigenère-Quadrat** verwendet werden. Es ist ein Quadrat, das aus 26 Zeilen besteht. Jede Zeile besteht jeweils aus um einen Buchstaben verschobenen Versionen des Alphabets. Der Geheimtextbuchstabe steht in der Zeile des Schlüsselbuchstaben (H) und in der Zeile des Klartextbuchstaben (E).

So ergibt sich folgender Geheimtext: ZVLJNBARRXSUXGOI

Das Vigenere-Verfahren galt lange Zeit als unknackbar. Erst im Jahr 1854 gelang es Charles Babbage. Da dies aber nicht öffentlich gemacht wurde, ging der preußische Offizier Friedrich Kasiski mit seinem Lösungsverfahren im Jahr 1863 in die Geschichte ein. Das Verfahren wird **Kasiski-Test** genannt. Der Test besteht aus zwei Teilen:

1. **Schlüsselwortlänge** bestimmen
   1.1. Zeichenketten suchen, die mehrmals im Text vorkommen
   1.2. Abstände zwischen den Zeichenketten zählen
   1.3. gemeinsame Teiler der Abstände bestimmen
2. **Häufigkeitsanalysen** für die einzelnen Caesar-Verschlüsselungen zu jedem Buchstaben im Schlüsselwort

Vigenère

Definition Primzahl: Eine Primzahl ist eine Zahl größer als 1, die nur durch sich selbst und 1 teilbar ist.

Definition Primfaktorzerlegung: Die Primfaktorzerlegung ist eine Möglichkeit eine Zahl als eindeutiges Produkt von Primzahlen zu schreiben. Dabei wird eine Zahl so lange in Produkte aus Primzahlen zerlegt, bis sie nicht mehr weiter geteilt werden kann. Die Reihenfolge ist dabei egal.

Beispiele: $12 = 2 \cdot 2 \cdot 3$, $150 = 2 \cdot 3 \cdot 5 \cdot 5$

Die Primfaktorzerlegung ist ein wichtiger Zwischenschritt für viele mathematische Verfahren. Darüber lassen sich zum Beispiel gemeinsame Teiler bestimmen.

Vigenère-Quadrat:

Schlüsselwortbuchstabe \ Klartextbuchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	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	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	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	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	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	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	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	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	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	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	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	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