Aufgabe 1)

a) Gegeben sei der folgende Caesar verschlüsselte Text:

> „AIRR WMI ZIVWYGLIR, MLVI WCWXIQI MHMSXIRWMGLIV DY QEGLIR, AMVH IW MQQIV IMRIR MHMSXIR KIFIR, HIV IMRJEPPWVIMGLIV MWX EPW WMI." – OIZMR QMXRMGO

Entschlüssele den Text mit Hilfe eines Brute-Force-Angriffs!
(Bei einem Brute-Force-Angriff handelt es sich um eine Methode, die versucht Passwörter oder Schlüssel durch automatisiertes, wahlloses Ausprobieren herauszufinden.)

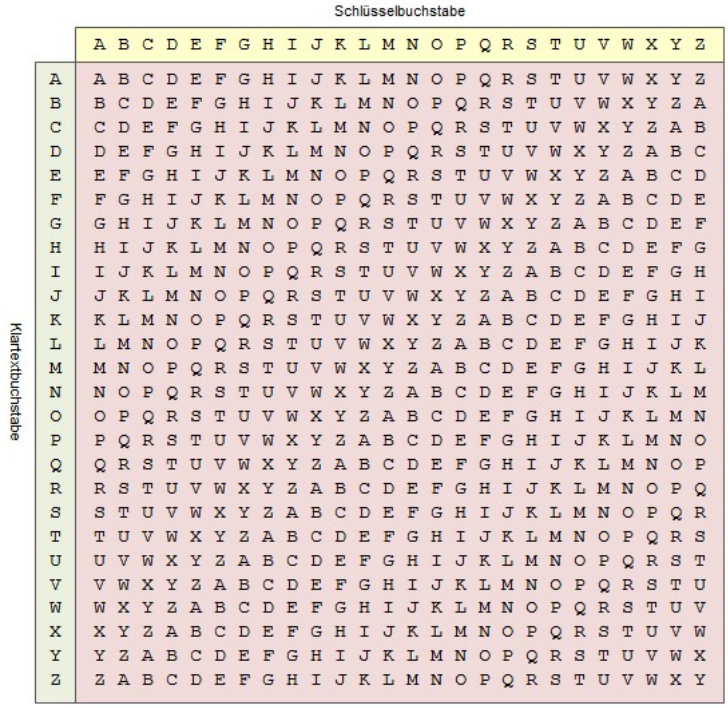
b) Gegeben sei der folgende Caesar verschlüsselte Text:

> „FQIIMÖHJUH IYDT MYU KDJUHMÄISXU. TK TQHVIJ IYU AUYDUD IUXUD BQIIUD, CKIIJ IYU HUWUBCÄßYW MUSXIUBD KDT IEBBJUIJ IYU DYSXJ CYJ VHUCTUD JQKISXUD." - SXHYI FYHYBBE

Entschlüssele den Text mit Hilfe einer Häufigkeitsanalyse (Frequenzanalyse)!

Aufgabe 2)

Das Vigenère-Verfahren beruht auf einem sogenannten Vigenère-Quadrat, das aus 26, Zeile um Zeile jeweils um einen Buchstaben verschobenen Versionen des Alphabets besteht.



	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Beim Vigenère-Verfahren wird zunächst ein Schlüsselwort vorgegeben - z.B. das Schlüsselwort 'HUND'. Mit Hilfe des Schlüsselworts und des Vigenère-Quadrats erfolgt jetzt die Erzeugung des Geheimtextes aus einem gegebenen Klartext. Hier ein Beispiel.

Schlüssel:	H	U	N	D	H	U	N	D	H
Klartext:	G	E	H	E	I	M	N	I	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓
Geheimtext:	N	Y	U	H	P	G	A	L	Z

a) Kannst du anhand des Beispiels das Verfahren erschließen?

b) Erstelle mit Hilfe des Vigenère-Verfahrens in CrypTool einen Geheimtext! Verwende hierfür einen von dir frei gewählten Schlüssel.

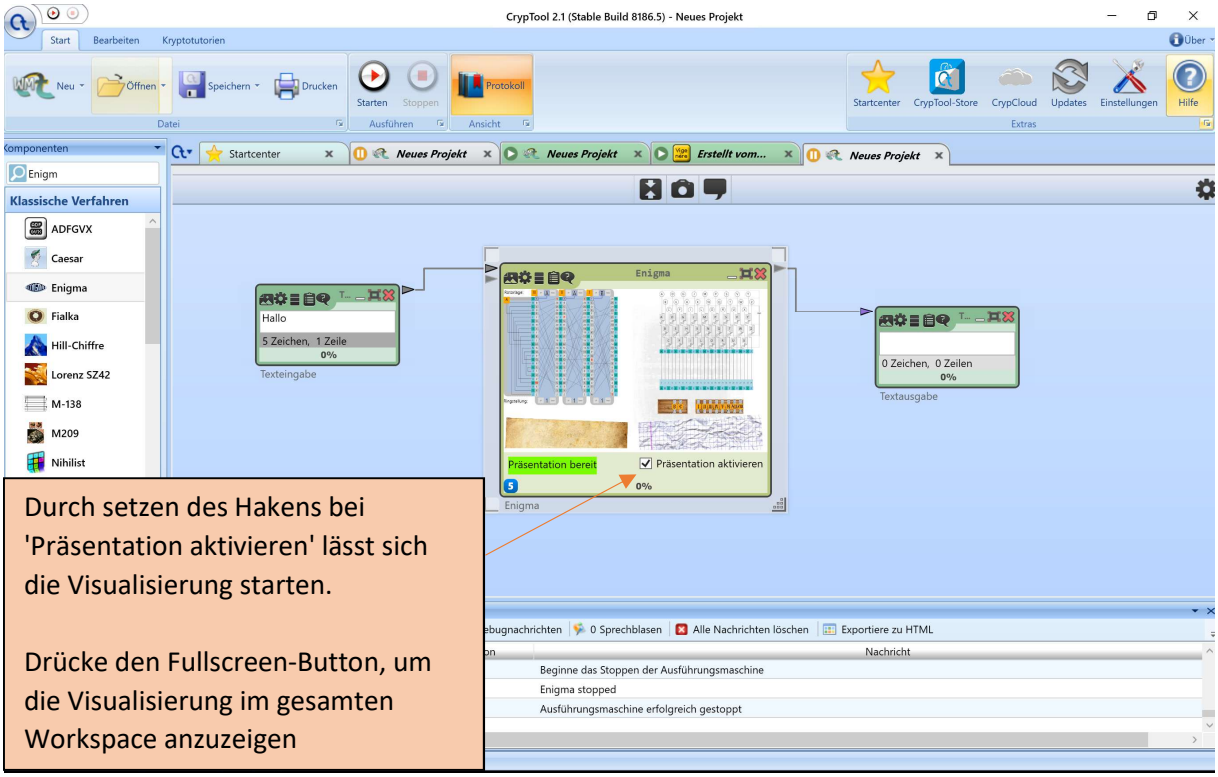
c) Übergib deinem/-er Nachbar(-in) den in Aufgabenteil b) erstellten Geheimtext und den dazugehörigen Schlüssel. Lass sie/ihn mit Hilfe von CrypTool den Klartext entschlüsseln!

Tobias Gries

Aufgabe 3)

In CrypTool 2 lassen sich komplexe Verschlüsselungssysteme, wie beispielsweise die Enigma-Verschlüsselung visuell darstellen.

Starte hierzu ein neues Projekt, welches eine *Texteingabe*, eine *Textausgabe* und die *Enigma-Verschlüsselung* enthalten.



Durch setzen des Hakens bei 'Präsentation aktivieren' lässt sich die Visualisierung starten.

Drücke den Fullscreen-Button, um die Visualisierung im gesamten Workspace anzuzeigen