Arbeitsauftrag 3
Kryptographie: Blaise de Vigenère

INF-11 Zeit: 1 UE
Fach: Informatik

„Mit 24 Jahren arbeitete er als Sekretär für den Herzog von Nevers. Nachdem dieser starb, wurde Vigenère 1549 von einem Gericht beauftragt, für zwei Jahre nach Rom zu gehen, um dort diplomatische Aufgaben zu erfüllen. Dort kam er erstmals mit Kryptologie in Kontakt. 1570 schied er aus dem diplomatischen Dienst aus und widmete sich nach seiner Heirat mit Marie Varé ausschließlich des Schreibens und der Kryptologie.
Er verfasste mehr als 20 Bücher, die bekanntesten sind: Traicte de Cometes (1580) und Traicte de Chiffres (1586).

Basierend auf den Ideen des Benediktinermönches Johannes Trithemius (1462–1516) beschrieb er unter anderem die nach ihm benannte Vigenère-Verschlüsselung. Diese galt lange Zeit als unknackbar, und erst um 1850, fast 300 Jahre nach Vigenère, konnte Charles Babbage Vigenère-Chiffrierungen systematisch entziffern. Schließlich veröffentlichte Friedrich Wilhelm Kasiski 1863 ein nach ihm benanntes Verfahren für die Bestimmung der Schlüsselwortlänge und Entzifferung des Algorithmus. „- Wikipedia

Die Vigenere Verschlüsselung benutzt einen längeren Schlüssel, um nachfolgende Buchstaben unterschiedlich zu verschlüsseln. Bei einer Schlüssellänge von 1 wäre es die Cäsar Verschlüsselung.
Die Vigenere Verschlüsselung ist eine polyalphabetische Verschlüsselung, weil die mehr als eine Verschiebung nutzt. Benutzt https://studio.code.org/s/vigenere/lessons/1/levels/1 als Hilfe.

Arbeitsauftrag 1 (Pflichtaufgabe):

Wende die Vigenere Verschlüsselung an, um den folgenden Text mit dem Schlüssel „**SCHOKOLADENEIS**“ zu verschlüsseln. Benutze dafür das untenstehenden Vigenere Quadrat.

Meine Oma faehrt im Huehnerstall Motorrad
Motorrad Motorrad
Meine Oma fährt im Huehnerstall Motorrad
Meine Oma ist eine ganz patente Frau

Arbeitsauftrag 2 (Pflichtaufgabe):

Wende die Vigenere Verschlüsselung an, um den folgenden Text mit dem Schlüssel „**ERDBEEREIS**“ zu entschlüsseln. Benutze dafür das untenstehenden Vigenere Quadrat.

GYDSPIJ FITFRJF LEK HQW ZVUTGLCYMKWVOVRK XISFETNU

Arbeitsauftrag 3:

Recherchiere, warum die Vigenere Verschlüsselung sicherer als eine monoalphabetische Verschlüsselung ist.

Arbeitsauftrag 4:

Recherchiere wie man die Vigenere Verschlüsselung knacken kann.

	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

Vigenere Quadrat