Substitution – Teil 2

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Substitution* beschreiben. Weiter gibt es aber auch noch die Unterteilung in *Mono-* und *Polyalphabetisch*. Bei Ersterem findet nur ein Alphabet verwendung (siehe Caesar- oder Atbash-Verschlüsselung), was das „Knacken“ mittels einer Häufigkeitsanalyse einfach ermöglicht. Bei polyalphabetischen Verfahren werden mehrere Geheimalphabete verwendet und somit gleiche Buchstaben durch mehrere verschiedene Buchstaben ersetzt. Ein Beispiel für ein solches Verfahren ist die Vigenére-Verschlüsselung.

Vigenére-Verschlüsselung

Dieses Verfahren ähnelt der Caesar-Verschlüsselung, nur mit dem Unterschied, dass man hier nicht ein Geheimalphabet (das verschobene Alphabet) verwendet, sondern mehrere. Damit die Person, die die Nachricht verschlüsselt und die Person, die die Nachricht entschlüsselt, wissen welche und wieviele Geheimalphabete verwendet werden, einigen sie sich auf ein *Schlüsselwort*.

Die Positionen der einzelnen Buchstaben des Schlüsselwortes im Alphabet geben an, um wieviel das Alphabet verschoben wird. Die Anzahl der Geheimalphabete entspricht dabei der Länge des Schlüsselwortes. Wird zum Beispiel das Schlüsselwort *GEHEIM* verwendet, dann werden zum Verschlüssel des Klartextes sechs Geheimalphabete verwendet:

1. Geheimalphabet ist das Alphabet um **sechs** Buchstaben verschoben.
2. Geheimalphabet ist das Alphabet um **vier** Buchstaben verschoben.
3. Geheimalphabet ist das Alphabet um **sieben** Buchstaben verschoben.
4. Geheimalphabet ist das Alphabet um **vier** Buchstaben verschoben.
5. Geheimalphabet ist das Alphabet um **acht** Buchstaben verschoben.
6. Geheimalphabet ist das Alphabet um **zwölf** Buchstaben verschoben.

Die Tabelle auf der folgenden Seite veranschaulicht dies nochmal für alle Buchstaben.

Soll nun der Text *ICH MAG INFORMATIK* verschlüsselt werden, dann wir der erste Buchstabe (I) mit dem ersten Geheimalphabet verschlüsselt, der zweite mit dem zweiten und so weiter, bis man wieder beim ersten Geheimalphabet anfängt:

I	G →	O	I	G →	O	A	G →	G
C	E →	G	N	E →	R	T	E →	X
H	H →	O	F	H →	M	I	H →	P
M	E →	Q	O	E →	S	K	E →	O
A	I →	I	R	I →	Z			
G	M →	S	M	M →	Y			

Aus „ICH MAG INFORMATIK“ wird also „OGO QIS ORMSZYGXPO“.

Buchstabe des Schlüsselwortes	Buchstabe des Klartextes																								
	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

Aufgabe 1

Verschlüssle die folgende Nachricht mit der Vigenére-Verschlüsselung und dem Schlüsselwort GEHEIM:

TREFFEN UM DREI

Aufgabe 2

Entschlüssle die folgende Nachricht mit dem Schlüsselwort GEHEIM.

JIY KMUKV OEB POI IICFK