Substitution – Teil 1

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Substitution* beschreiben. Bei der Substitution werden Buchstaben oder sogar ganze Wörter des Klartextes durch andere Buchstaben, Wörter oder auch Symbole ersetzt. Ein Beispiel, das euch vielleicht bereits bekannt ist, stellt die Caesar-Verschlüsselung dar. Es gibt jedoch auch noch die Verschlüsselung nach Atbash und mittels Polybius-Tafel.

Atbash- und Ceasar-Verschlüsselung

Bei beiden Verschlüsselungen werden die Buchstaben des Alphabetes durch andere Buchstaben ausgetauscht. Dies kann jedoch auf auf verschiedene Arten erfolgen.

So wird bei Atbash der erste Buchstabe des Alphabetes mit dem Letzten, der Zweite mit dem Vorletzten und so weiter ausgetauscht.

Klaralphabet																								
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
Z	Y	X	W	V	U	Z	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
Atbash Geheimalphabet																								

Anders erfolgt bei Caesar eine Verschiebung des Alphabetes. Hier wird jeder Buchstabe mit dem Buchstaben ersetzt, der um einen festen Wert später im Alphabet auftaucht.

Klaralphabet																								
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
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
Caesar Geheimalphabet mit einer Verschiebung von 6																								

Aufgabe 1

Verschlüssle die folgende Nachrichten mit Atbash:

TREFFEN UM DREI

Aufgabe 2

Entschlüssle die folgende Nachricht mit Atbash:

WVI TVRVI SZG WRV YVFGV

Verschlüsselung mittels Polybius-Tafel

Die Buchstaben eines Klartextes müssen jedoch nicht immer nur durch Buchstaben ersetzt werden. Es ist auch möglich sie durch Zahlen zu ersetzen, wie das Verfahren mittels Polybius-Tafel zeigt.

Die Polybius-Tafel stellt eine Art Tabelle (oder auch Matrix genannt) dar, in der jeder Buchstaben des Alphabets eingetragen wird und eine X- und Y-Koordinate erhält.

		Y				
		1	**2**	**3**	**4**	**5**
X	**1**	A	B	C	D	E
	2	F	G	H	I/J	K
	3	L	M	N	O	P
	4	Q	R	S	T	U
	5	V	W	X	Y	Z

Die Anzahl der Zeilen und Spalten kann dabei beliebig angepasst werden. Im obigen Beispiel wird nun das A mit „1 1“, „11“ bzw. „1,1“ oder B mit „1 2“, „12“ bzw. „1,2“ verschlüsselt (für die Schreibweise der Koordinaten gibt es noch etliche weitere Möglichkeiten).

Aufgabe 3

Verschlüssle die Nachricht aus Aufgabe 1 mittels der obigen Polybius-Tafel.

Aufgabe 4

Entschlüssle die folgende Nachricht:

14 15 42

43 13 23 31 45 15 43 43 15 31

31 24 15 22 44

11 32

21 31 45 43 43