Vigenére-Verschlüsselung

Die Vigenére-Verschlüsselung entstand im 16. Jahrhundert und galt damals lange als nicht entzifferbar. Heute stimmt das nicht mehr, sie ist jedoch eine recht sichere Verschlüsselungsmethode und durch einige Variationen kann man sie sogar noch sicherer machen.

Grundlegendes Prinzip:

Die Verschlüsselungsmethode funktioniert ähnlich wie die Caesar-Verschlüsselung. Es ist also hilfreich, wenn du schon weißt, wie diese Methode angewendet wird. Jeder Buchstabe des Textes, den wir verschlüsseln wollen, wird durch einen anderen Buchstaben ersetzt. Die entscheidende Neuheit an der Vigenére-Verschlüsselung war jedoch, dass man nicht jeden Buchstaben nach demselben Schema ersetzt, sondern ein Codewort als Schlüssel verwendet. Der erste Buchstabe des Textes wird also mit dem Caesar Code, der sich aus dem ersten Buchstaben des Codeworts ergibt, verschlüsselt, der zweite Buchstabe des Textes mit dem Caesar Code, der sich aus dem zweiten Buchstaben des Codeworts ergibt, usw. Ist man am Ende des Codeworts angelangt, beginnt man wieder mit dem ersten Buchstaben. Damit du nicht jedes Mal die Caesar-Verschlüsselung anwenden musst, gibt es als Hilfsmittel das sogenannte Vigenére-Quadrat. Hier werden einfach alle Caesar Alphabete untereinander angeordnet. Das sieht dann so aus:

	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	Z	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	A	B	C	D	E	F	G
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

Wenn wir jetzt einen Text verschlüsseln wollen, zum Beispiel „Geheimcodes lernen ist kinderleicht“, benötigen wir zusätzlich ein Codewort, zum Beispiel „Krimifest“. Als erstes ordnen wir jedem Buchstaben des Textes einen Buchstaben des Codeworts zu.

```
GEHEIMCODES LERNEN IST KINDERLEICHT
KRIMIFESTKR IMIFES TKR IMIFESTKRIMI
```

Jetzt benutzen wir unser Vigenére-Quadrat für die Verschlüsselung. Dabei stehen oben in der ersten Zeile die Buchstaben des Textes und links in der ersten Spalte die Buchstaben des Codeworts. Wir suchen also für unser Beispiel oben das G und links das K. In dem Feld, in dem sich nun die Spalte des G und die Zeile des K treffen, steht der Buchstabe für unsere Verschlüsselung, das ist ein Q. In diesem Bild haben wir das mal eingezeichnet:

	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	Z	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	A	B	C	D	E	F	G
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

Der ganze Satz verschlüsselt sieht dann so aus: „QVPQQRGGWOJ TQZSIF BCK SUVIIJEOZKTB“. Manchmal lässt man auch die Leerzeichen weg, um die Entschlüsselung für Uneingeweihte noch schwieriger zu machen.

Für die Entschlüsselung schreiben wir zuerst wieder das Codewort unter den verschlüsselten Text.

```
QVPQQRGGWOJ TQZSIF BCK SUVIIJEOZKTB
KRIMIFESTKR IMIFES TKR IMIFESTKRIMI
```

Nun suchen wir in der linken Spalte den Buchstaben des Codeworts und gehen dann die Spalte solange entlang, bis wir den Buchstaben des verschlüsselten Textes finden. Geht man die zugehörige Spalte nach oben, erhält man den Buchstaben des entschlüsselten Textes. Probier's doch gleich mal aus. Schaffst du es den Text „KOEII JY OEAF VYC GFJI NISZSWZX" zu entschlüsseln? Das Codewort ist „Supergeheim".

Varianten der Verschlüsselung:

Statt eines Codeworts, kannst du auch eine zufällige Zahlenfolge verwenden. Hierfür tauschen wir in der Spalte ganz links einfach die Buchstaben durch Zahlen von 1 bis 26 aus. Das Ver- und Entschlüsseln funktioniert nach demselben Prinzip. Es ist jedoch sicherer, da man eine beliebige Zahlenfolge schwerer erraten kann als ein Codewort.

Tipps für mehr Sicherheit:

Die Sicherheit lässt sich sehr einfach durch ein möglichst langes Codewort erhöhen. Je länger das Codewort ist, desto seltener muss es wiederholt werden. Durch eine Zeichenwiederholung erhält man nämlich auch in der verschlüsselten Botschaft Wiederholungen, woraus sich Rückschlüsse auf die Länge das Codewortes ziehen lassen. Hat man diese festgestellt, kann man die Botschaft in einen Caesar Code umwandeln und dadurch entschlüsseln.
Eine extreme Variante dieser Verlängerung des Codewortes ist die sogenannte One-Time-Pad-Methode, also die Einmalschlüssel-Methode. Hier ist der Schlüssel genauso lang wie der zu verschlüsselnde Text und sollte aus einer zufälligen Buchstaben- oder Zahlenabfolge bestehen. Diese Methode ist deshalb so sicher, weil sich durch die zufällige Abfolge keine Rückschlüsse auf den Schlüssel ziehen lassen. Durch die unendlich vielen Möglichkeiten ist es nahezu unmöglich den richtigen Schlüssel zu erraten. Selbst wenn man einen sinnvollen Text herausbekommt, hat man keine Sicherheit, dass dies tatsächlich die ursprüngliche Nachricht ist. Hier ein Beispiel dazu: Unser Ausgangstext ist „Krimis finden wir super", unser Schlüssel ist die zufällig generierte Buchstabenfolge „ZAUMGUOWGTHAWDGDKITD". Für mehr Sicherheit schreiben wir sowohl Botschaft als auch Verschlüsselung zusammen. Der verschlüsselte Text ist dann „JRCYOMTETWLNSLXVEXXU". Versuchen wir nun diese Nachricht zu entschlüsseln, könnten wir zum Beispiel durch den Schlüssel „KXXYDBMACWRVMHSBRUTH" zu dem Ergebnis „Zufall herausgefunden" kommen. Auch dies ist ein (einigermaßen) sinnvoller Text, jedoch nicht der, den wir verschlüsselt haben. Der Schlüssel sollte jedoch nur einmal verwendet werden, da es mithilfe moderner Analysetechniken möglich ist, diesen herauszufinden.