Klassische Kryptographie

Blais de Vigenère

Blaise de Vigenère lebte von 1523 bis 1596 in Frankreich und war nach dem Studium bei verschiedenen Herren im diplomatischen Dienst. Bei einer diplomatischen Mission in Rom entdeckte er in einem Archiv die Arbeiten von Alberti und von anderen Kryptologen. Schnell wurde aus dem anfangs nur praktischen Interesse ein Lebensziel: diese Schriften alle zu studieren und ein neues, mächtigeres Chiffriersystem zu entwickeln. 1570 gab er den Dienst auf und widmete sich seinen Interessen. 1580 veröffentlichte es sein Werk Traictè de Chiffres. Das Buch gibt einen genauen Stand der Kryptographie seiner Zeit wieder und enthält außerdem Goldmacherrezepte, Alchemie und japanische Ideogramme.

Die Stärke des neuen Verfahrens beruht darauf, dass nicht nur ein, sondern mehrere verschiedene Geheimtextalphabete genutzt werden. Dazu braucht man im ersten Schritt ein so genanntes Vigenere- Quadrat. Unter dem Klartextalphabet sind 26 Geheimtextalphabete aufgelistet, jedes um einen Buchstaben gegenüber dem vorhergehenden vorschoben. Die Auswahl des jeweiligen Alphabets erfolgte über das Schlüsselwort. Da die Vigenère - Methode mehrere Geheimtextalphabete verwendet, um eine Nachricht zu verschlüsseln, bezeichnet man dieser Verfahren als polyalphabetische Verschlüsselung.

Vigenère-Chiffrierung

Die Vigenère-Chiffrierung ist im Gegensatz zur Caesar-Chiffrierung eine *polyalphabetische Substitution*. Dies bedeutet, daß sie, anstatt jedem Buchstaben nur 1 Zeichen zuzuordnen, jedem Buchstaben mehrere Zeichen zuordnet. Dies erhöht die Sicherheit immens, da der Angriff über die Häufigkeitsverteilung der Zeichen (fast) unmöglich gemacht wird.

Das Verfahren: Zunächst wird ein Schlüssel festgelegt. Dieser Schlüssel besteht nicht, wie bei der Caesar-Chiffrierung, aus einer Zahl, sondern aus einem Wort, einem Satz oder einem ganzen Text – kurz, einer Zeichenfolge von *n* Zeichen Länge. Zur Chiffrierung des Klartextes wird dieser Schlüssel nun hintereinander über den Klartext gelegt, dann werden die einzelnen Zeichen des Schlüssels und des Klartextes addiert. Dies hat zur Folge, dass ein und derselbe Klartext-Buchstabe mehrere Substitutionen besitzen kann.

Beispiel: Gegeben sei ein Klartext mit

s = DIES IST EIN SATZ.

Nun wählen wir einen Schlüssel mit

k = KEY

Nun legen wir den Schlüssel hintereinander über den Klartext:

K	E	Y	K		E	Y	K		E	Y	K		E	Y	K	E
D	I	E	S		I	S	T		E	I	N		S	A	T	Z

Nun haben wir nichts weiter zu tun, als die einzelnen Zeichen, die übereinander stehen, zu addieren. Heraus kommt das Chiffre mit

c = NMCCMQDIGXWDD

Auch hier werden den Buchstaben die Zahlen von 0 bis 25 zugewiesen. Die Formel zur Berechnung der Zeichen ist $c = (s + k) \bmod 26$

Wie man sieht, ist dies die gleiche Formel, die auch zur Caesar-Chiffrierung angewandt wurde. Der Unterschied besteht darin, dass sich *k* ständig ändert und somit eine bessere Verteilung der Häufigkeiten der Zeichen erreicht wird.

Schwachstelle: Trotz der besseren Verteilung der Häufigkeiten der Buchstaben wiederholen sich kleinere Wörter, anhand derer man das Schlüsselwort errechnen kann. Dies ist vor allem bei kurzen Schlüsseln der Fall. Allgemein gilt: Je länger der Schlüssel, desto sicherer die Vigenère-Verschlüsselung.

Verwendung dieses Quadrates:
Man schreibt die zu verschlüsselnde Botschaft auf und darunter immer wieder das Schlüsselwort hintereinander (Leerzeichen werden dabei ignoriert). Nun sucht man sich den Buchstaben der Botschaft, der gerade verschlüsselt werden soll in der ersten Zeile des Vigenère-Quadrates. Von dort aus geht man in dieser Spalte soweit hinunter, bis man ganz links den Buchstaben des Schlüsselwortes, der unter dem zu verschlüsselnden Buchstaben steht, gefunden hat. So ergibt sich nach und nach die verschlüsselte Botschaft. Diese Art von Verschlüsselung lässt sich nicht so einfach entschlüsseln, da die Häufigkeit der einzelnen Buchstaben viel gleichmäßiger verteilt ist, als bei einer monoalphabetischen Verschlüsselung, denn ein Buchstabe der zu verschlüsselnden Botschaft kann auf alle anderen 25 Buchstaben des Alphabets abgebildet werden.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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