Die Vigenère-Verschüsselung knacken

Nach der Erfindung der Vigenère-Verschlüsselung um 1550 durch Blaise de Vigenère dauerte es fast 300 Jahre, bis es dem exzentrischen britischen Genie Charles Babbage[1] (vgl. Abbildung) Mitte des 19. Jahrhunderts gelang die Vigenère-Verschlüsselung zu knacken. Er erkannte, dass der Schwachpunkt der polyalphabetischen Verschlüsselung beim Schlüsselwort lag und dass insbesondere kurze Schlüssel ein Knacken des Codes entscheidend vereinfachen.

Um die Vigenère-Verschlüsselung zu knacken sind folgende Schritte nötig:

1. Im Geheimtext werden Buchstabenfolgen gesucht, die mehrmals vorkommen.
2. Es wird die Länge des Schlüsselwortes ermittelt.
3. Das Schlüsselwort wird bestimmt.

In der Folge werden die einzelnen Schritte theoretisch erläutert. In der Aufgabe zum Kapitel soll dann diese Theorie in die Praxis umgesetzt und ein vigenère-verschlüsselter Text geknackt werden.

Schritt 1 – Mehrmals vorkommende Buchstabenfolgen finden

Der Geheimtext wird nach Buchstabenfolgen durchsucht, die mehrmals vorkommen. Diese Folgen sollten mindestens die Länge 3 haben. Gleiche Buchstabenfolgen können bei der polyalphabetischen Verschlüsslung auf zwei Arten entstanden sein. Entweder es wurde das gleiche Klartextwort mit den gleichen Stellen des Schlüsselwortes verschlüsselt oder es entstand zufällig die gleiche Folge von Buchstaben. Die zweite Möglichkeit ist bei Folgen von 3 und mehr Buchstaben sehr klein, was mit Hilfe der Wahrscheinlichkeitsrechnung belegt werden kann. Also ist es ziemlich sicher, dass gleiche Buchstabenfolgen vom gleichen Klartextwort herstammen.

Jede der mehrmals vorkommenden Buchstabenfolge wird aufnotiert. Zudem wird bei jeder Folge hinzugefügt in welchem Abstand zur identischen Folge sie im Geheimtext auftritt (Abstand 1. Buchstabe zu 1. Buchstaben). Daraus ergibt sich eine Tabelle mit Zahlen.

Schritt 2 – Schlüssellänge ermitteln

Wie oben erklärt kann man mit grosser Wahrscheinlichkeit davon ausgehen, dass die gleichen Buchstabenfolgen vom gleichen Klartextwort stammen, das mit dem gleichen Teil des Schlüsselwortes codiert wurde. Die logische Schlussfolgerung daraus ist, dass jeder der aufnotierten Abstände das Schlüsselwort eine ganzzahlige Anzahl Mal enthalten muss. Es muss also die Länge des Schlüsselwortes ein Teiler aller aufgelisteten Abstände sein! Dieser in allen Abstandszahlen vorkommende Teiler muss zwangsläufig die Länge des Schlüsselwortes sein.

Schritt 3 – Schlüsselwort bestimmen

[1] Charles Babbage lebte von 1792 bis 1871. Er war auch bekannt als Computerpionier und gilt als Erfinder er ersten automatischen Rechenmaschine. 1822 entwickelte er die „Difference Machine No.1“. 1833 die „Difference Machine No2“, welche aber aus Geldmangel nicht fertiggestellt wurde. Nachbildungen zeigten später, dass sie aber funktionsfähig gewesen wäre.

Mit der Kenntnis der Länge des Schlüssels sind wir einen entscheidenden Schritt weiter gekommen. Die polyalphabetische Verschlüsselung lässt sich nun in monoalphabetische Verschlüsselungen aufteilen.

Wir wissen nun, welche Buchstaben des Geheimtextes mit jeweils dem gleichen Buchstaben des Schlüsselwortes codiert wurden – sprich für welche Buchstaben jeweils die gleiche Spalte des Vigenère-Quadrates verwendet wurde. Ist beispielsweise das Schlüsselwort 5 Buchstaben lang, so wurde er 1., der 6., der 11., der 16. usw. Buchstaben des Geheimtextes immer mit der gleichen Spalte verschlüsselt. Entsprechend gilt das dann auch für den 2., den 7., den 12. etc.

Wir können jeden Buchstaben im Geheimtext einem Schlüsselwortbuchstaben zuordnen. Damit entsteht eine Aufteilung des Geheimtextes in sowiele Teile, wie das Schlüsselwort Buchstaben enthält. Jedem dieser Teile liegt eine monoalphabetische Verschlüsselung zugrunde, die sich in bekannter Manier mit Hilfe der Häufigkeitsanalyse knacken lässt. Damit lässt sich also für jeden der Teile herausfinden, mit welchem Geheimtextalphabet er verschlüsselt wurde.

Ist das Geheimtextalphabet für jeden Teil des Geheimtextes bekannt, so kann mit dem Vigenère-Quadrat jeweils der zum entsprechenden Alphabet gehörende Klartextbuchstaben des Schlüsselwortes abgelesen werden. Das Schlüsselwort kann bestimmt werden.

Mit der Kenntnis des Schlüsselwortes ist der Code vollständig geknackt.

Zum Schluss

Der Codierer kann das ungewollte Dechiffrieren seines Textes einfacher oder schwerer machen. Es ist insbesondere einfach einen Geheimtext zu knacken, wenn das gewählte Schlüsselwort kurz ist. Je länger das Schlüsselwort, umso weniger identische Buchstaben folgen werden auftreten (Wahrscheinlichkeitsrechnung!). Idealerweise wäre das Schlüsselwort gleichlang wie der Text selber, was aber wegen dem Schlüsseltausch in der Praxis nicht durchführbar ist.

Um einen polyalphabetisch verschlüsselten Text knacken zu können, muss er eine bestimmte Länge aufweisen. Ist er nur sehr kurz, z.B. einige Wörter, so werden kaum gleiche Buchstabenfolgen auftauchen und es ist damit nicht möglich das Schlüsselwort zu bestimmen.

Klartext-alphabet	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	
0	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	
1	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	
2	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	
3	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	
4	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	
5	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	
6	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	
7	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	
8	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	
9	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	
10	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	
11	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	Vigenère-
12	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	Quadrat
13	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	
14	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	
15	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	
16	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	
17	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	
18	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	
19	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	
20	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	
21	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	
22	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	
23	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	
24	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	
25	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	