§ 7. Die Vigenère–Chiffre

(7.1) Das Vigenère–Quadrat

In dem Vigenère–Quadrat sind alle 26 Verschiebe–Chiffren der Reihe nach aufgelistet:

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	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

(7.2) Die Vigenère–Chiffre

Bei der Vigenère–Chiffre werden mehrere Verschiebe–Chiffren im regelmäßigen Wechsel benutzt. Dieser Wechsel wird durch ein Schlüsselwort $\overline{\boldsymbol{w}}$ aus beliebigen Buchstaben geregelt.

Verschlüsselung: Das Schlüsselwort wird hintereinander über den gesamten Klartext geschrieben, so dass über jedem Buchstaben des Klartextes ein Buchstabe des Schlüsselwortes steht. Steht über einem Buchstaben $\boldsymbol{\nu}$ des Klartextes der Schlüsselwortbuchstabe $\boldsymbol{\Sigma}$, so wird $\boldsymbol{\nu}$ durch die Verschiebechiffre $\boldsymbol{a} \longmapsto \boldsymbol{\Sigma}$ verschlüsselt. Den entsprechenden Geheimtextbuchstaben kann man aus dem Vigenère–Quadrat ablesen.

Entschlüsselung: Das Schlüsselwort wird hintereinander über den gesamten Geheimtext geschrieben, so dass über jedem Buchstaben des Geheimtextes ein Buchstabe des Schlüsselwortes steht. Steht über einem Buchstaben $\boldsymbol{\Gamma}$ des Geheimtextes der Schlüsselwortbuchstabe $\boldsymbol{\Theta}$, so wird $\boldsymbol{\Gamma}$ durch die Umkehrabbildung der Verschiebechiffre $\boldsymbol{a} \longmapsto \boldsymbol{\Theta}$ entschlüsselt. Den entsprechenden Klartextbuchstaben kann man aus dem Vigenère–Quadrat ablesen.

(7.7) BEISPIEL: Entschlüsselung einer Vigenère–Chiffre

(Beispiel aus Beutelspacher: Kryptologie)

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

Mit dem Schlüsselwort B U E R O läßt sich dieser Geheimtext entschlüsseln.

Blaise de Vigenère (1523 – 1596)

(7.3) SATZ: Vigenère–Chiffre

Gegeben seien ein Klartext

$$\alpha_1\alpha_2\alpha_3\ldots\alpha_s \text{ mit } \alpha_i \in \mathfrak{a} \quad (i \in \{1,2,\ldots,s\})$$

und ein Schlüsselwort

$$\overline{w} = B_1B_2\ldots B_l \text{ mit } B_k \in \mathfrak{A} \quad (k \in \{1,2,\ldots,l\})\,.$$

Dann gilt für die Verschlüsselung $V(\alpha_i)$ $(i \in \{1,2,\ldots,s\})$ eines Klartextbuchstabens α_i durch die Vigenère–Chiffre mit dem Schlüsselwort $\overline{w}$

$$V(\alpha_i) = \Omega^{-1}\left((\Omega(B_j) + \omega(\alpha_i)) \bmod 26\right)\,,$$

wobei der Index j definiert ist durch

$$j = \begin{cases} i \bmod l & , \text{ falls } i \bmod l \neq 0 \\ l & , \text{ falls } i \bmod l = 0 \end{cases}$$

Der Kasiski–Test

Friedrich Wilhelm Kasiski (1805 – 1881)

Mit dem Kasiski–Test versucht man, die Schlüsselwortlänge eines Vigenère–verschlüsselten Geheimtextes herauszufinden.

(7.4) DEF: Der **Abstand zweier Buchstaben** in einem beliebigen Text

$$\alpha_1\alpha_2\alpha_3\alpha_4\ldots\alpha_s$$

ist definiert als der Betrag der Differenz ihrer Indizes.

(7.5) SATZ: Ist der Abstand zweier gleicher Wörter in einem Klartext ein Vielfaches der Schlüsselwortlänge, so werden sie durch die Vigenère–Chiffre in dasselbe Geheimtextwort verschlüsselt.

(7.6) Der Kasiski–Test

In einem Vigenère–verschlüsselten Geheimtext suche man zwei gleiche Folgen aus mindestens 3 Geheimtextbuchstaben und bestimme deren Abstand. Dieser Abstand ist vermutlich ein Vielfaches der gesuchten Schlüsselwortläge.

Hat man mehrere solcher Folgen gefunden, so ist die gesuchte Schlüsselwortläge wahrscheinlich ein Vielfaches des ggT's der gefundenen Abstände, wobei man "Ausnahmefälle" unberücksichtigt läßt.

Der Friedman–Test

William F. Friedman (1891 – 1969)

Frage: Mit welcher Wahrscheinlichkeit besteht ein willkürlich aus einem Text herausgegriffenes Buchstabenpaar aus gleichen Buchstaben?

(7.8) DEF: In einem Text $\boldsymbol{T}$ mit $\boldsymbol{n \geq 2}$ Buchstaben komme der Buchstabe

$$\begin{array}{cc} \boldsymbol{a} & \boldsymbol{n_1} \text{ mal} \\ \boldsymbol{b} & \boldsymbol{n_2} \text{ mal} \\ \boldsymbol{c} & \boldsymbol{n_3} \text{ mal} \\ \vdots & \vdots \\ \boldsymbol{z} & \boldsymbol{n_{26}} \text{ mal} \end{array}$$

vor. Dann heißt die Zahl

$$\boldsymbol{I(T) := \sum_{i=1}^{26} \frac{n_i \cdot (n_i - 1)}{n \cdot (n-1)}}\,.$$

der **(Friedman'sche) Koinzidenzindex von $\boldsymbol{T}$**.

(7.9) BEM: Der Koinzidenzindex $\boldsymbol{I(T)}$ gibt die Wahrscheinlichkeit dafür an, dass ein zufällig aus dem Text $\boldsymbol{T}$ herausgegriffenes Buchstabenpaar aus gleichen Buchstaben besteht.

(7.10) SATZ: Es sei $\boldsymbol{T}$ ein Text mit mindestens 2 Buchstaben.

a) Kommt in $\boldsymbol{T}$ der $\boldsymbol{i}$–te Buchstabe des Alphabets mit der Wahrscheinlichkeit $\boldsymbol{p_i}$ vor ($\boldsymbol{i = 1, 2, \ldots, 26}$), so gilt für den Koinzidenzindex von $\boldsymbol{T}$

$$\boldsymbol{I(T) \;\approx\; p_1^2 + p_2^2 + p_3^2 + \ldots + p_{26}^2 \;=\; \sum_{i=1}^{26} p_i^2}\,.$$

b) Es gilt $\boldsymbol{\frac{1}{26} \leq I(T) \leq 1}$, falls $\boldsymbol{T}$ "genügend" viele Buchstaben besitzt.

c) Der Koinzidenzindex $\boldsymbol{I_D}$ der deutschen Sprache (d.h. der Koinzidenzindex eines "normalen" deutschen Textes) ist

$$\boldsymbol{I_D \;\approx\; 0,0762}\,.$$

d) Der Koinzidenzindex $\boldsymbol{I_G}$ eines Textes, in dem alle 26 Buchstaben gleichhäufig vorkommen, ist

$$\boldsymbol{I_G \;=\; \frac{1}{26} \;\approx\; 0,0385}\,.$$

(7.11) BEM: Ist der Koinzidenzindex eines Geheimtextes ungefähr gleich $\boldsymbol{I_D \approx 0.0762}$, so ist die Verschlüsselung wahrscheinlich monoalphabetisch. Ist er dagegen sehr viel kleiner als $\boldsymbol{0.0762}$, so ist der Text wahrscheinlich polyalphabetisch verschlüsselt.

(7.12) Der Friedman–Test

Es sei $\boldsymbol{GT}$ ein Vigenère–verschlüsselter Geheimtext aus $\boldsymbol{n}$ Buchstaben, der den Koinzidenzindex $\boldsymbol{I(GT)}$ hat. Dann gilt für die Schlüsselwortlänge $\boldsymbol{l}$ die Näherung

$$\boldsymbol{l \;\approx\; \frac{(I_D - I_G)\cdot n}{I(GT)\cdot(n-1) - n\cdot I_G + I_D}\;,}$$

wobei $\boldsymbol{I_D}$ de Koinzidenzindex der deutschen Sprache und $\boldsymbol{I_G}$ der Koinzidenzindex eines Textes aus gleichhäufigen Buchstaben ist.

(7.13) FOLGERUNG: Ist $\boldsymbol{GT}$ ein Vigenère–verschlüsselter Geheimtext aus $\boldsymbol{n}$ Buchstaben, der den Koinzidenzindex $\boldsymbol{I(GT)}$ hat, so ist die Schlüsselwortlänge $\boldsymbol{l}$ ungefähr

$$\boldsymbol{l \;\approx\; \frac{0,0377\cdot n}{I(GT)\cdot(n-1) - n\cdot 0,0385 + 0,0762}\;.}$$