

Anwendung des Vigenère-Verfahrens

Aufgabe 1: Verschlüsseln Sie den Klartext P F E F F E R M I N Z T E E mit dem Vigenère-Verfahren und dem Schlüsselwort BLUME.

Aufgabe 2: Entschlüsseln Sie den Geheimtext L C E T T R X N Y E K T T N A mit dem Vigenère-Verfahren und dem Schlüsselwort TAXI.

Aufgabe 3: Machen Sie an den Beispielen aus Aufgabe 1 und 2 deutlich, dass es sich bei dem Vigenère-Verfahren, um ein polyalphabetisches Substitutionsverfahren handelt.

Vigenère-Quadrat:

klar	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
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
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
26	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

Abbildung 1: Vigenère-Quadrat

Aufgabe 4*:

- a) Implementieren Sie das Caesar-Verfahren: Erstellen Sie ein Programm, das die Eingabe eines Klartextes und eines Schlüssels als Zahl erlaubt und den entsprechenden Caesar-verschlüsselten Geheimtext ausgibt. Ergänzen Sie auch die Möglichkeit der Entschlüsselung.
Tipp: Verwenden Sie den ASCII-Code der Klartextzeichen, um die Caesar-Verschiebung als Addition zu realisieren.
- b) Implementieren Sie das Vignère-Verfahren: Erstellen Sie ein Programm, das die Eingabe eines Klartextes und eines Schlüsselwortes erlaubt und den entsprechenden Vigenère-verschlüsselten Geheimtext ausgibt. Ergänzen Sie auch die Möglichkeit der Entschlüsselung.
Tipp: Überlegen Sie zunächst, wie Sie aus dem ASCII-Code des Schlüsselbuchstabens, die Schlüsselzahl für das Caesar-Verfahren berechnen können. Erweitern Sie dann Ihre Implementierung aus a) zu einer Implementierung des Vigenère-Verfahrens.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.

* Aufgabe zur Verknüpfung von Kryptologie und Algorithmik