

## 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:

		Klartextbuchstabe																									
		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
Schlüsselbuchstabe	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	

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:** Beschränken Sie sich auf die Darstellung des Textes in Klein- oder in Großbuchstaben. 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. Verwenden Sie auch hier zur Vereinfachung ausschließlich Klein- oder ausschließlich Großbuchstaben.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Von der Lizenz ausgenommen ist das InfSII-Logo.

---

\* Aufgabe zur Verknüpfung von Kryptologie und Algorithmik