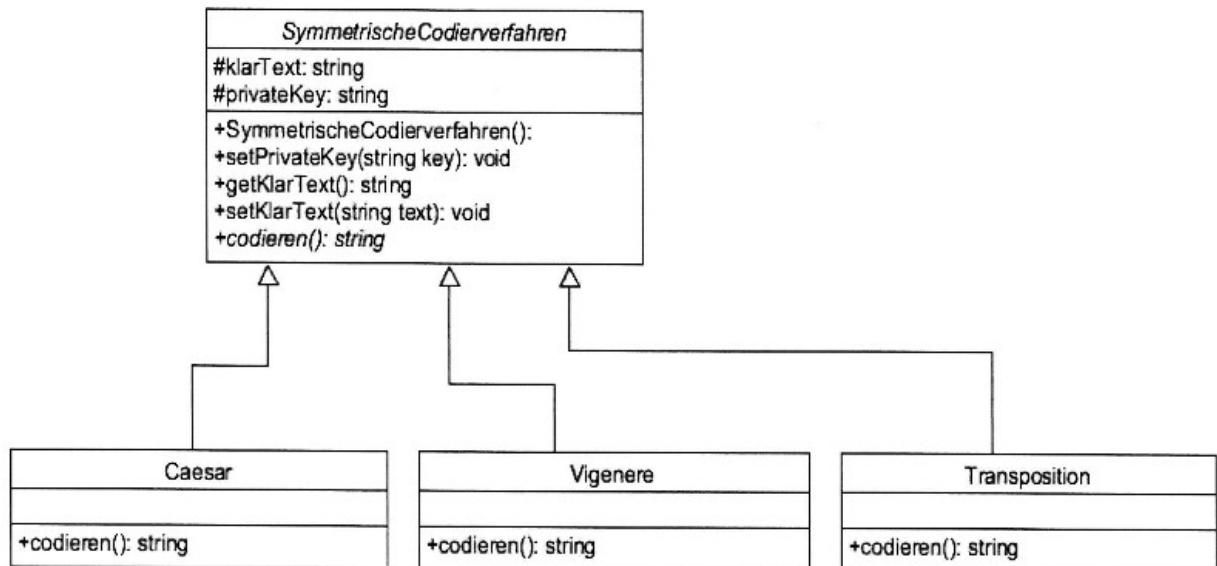


Elektronikschule Tettnang	Softwareentwicklung	Datum:	Klasse:
	Programm zur Verschlüsselung	Name:	

Sie haben entschieden, ein objektorientiertes Programm zur Vigenère-Verschlüsselung zu realisieren, welches zu den symmetrischen Verschlüsselungsverfahren zählt (siehe Anlage 1). Ein Kollege hat bereits folgendes UML-Klassendiagramm für Sie entworfen:



- 1.1 Implementieren Sie lediglich die Klassen „SymmetrischeCodierv Verfahren“ und „Vigenère“, sowie die Methoden der beiden Klassen gemäß obigem UML-Klassendiagramm. Verwenden Sie, die an Ihrer Schule unterrichtete Programmiersprache.

Das Prinzip der Vigenère-Codierung, welches Sie in der Methode **codieren()** implementieren sollen, wird in Anlage 2 erklärt.

Hinweis: Sie können davon ausgehen, dass im Klartext nur Großbuchstaben, keine Umlaute, keine Sonderzeichen und keine Leerzeichen enthalten sind.

- 1.2 Schreiben Sie ein Hauptprogramm, mit dem Sie die Klasse „Vigenère“ mit folgenden Daten prüfen können.

klarText: "DERADLERISTGELANDET"
privateKey: "PRUEFUNG"

Zur Überprüfung: der codierte Text lautet: "SVLEIFRXXJNKJFNTSVN"

Elektronikschule Tett nang	Softwareentwicklung	Datum:	Klasse:
	Programm zur Verschlüsselung	Name:	

Zum Verschlüsseln benötigt sowohl der Sender als auch der Empfänger einen gemeinsamen privaten Schlüssel. Der Klartext sowie der private Schlüssel wird ohne Leerzeichen, Umlaute, bzw. Sonderzeichen als Großbuchstaben angegeben:

Ist die Zeichenlänge des Schlüssels kleiner als die Zeichenlänge des Klartextes, wird der Schlüssel solange wiederholt bis die Schlüssellänge gleich der Länge des Klartextes ist (siehe unteres Beispiel).

Zeile 1: Klartext: DIESISTEINEBOTSCHAFT

Zeile 2: Schlüssel: GEHEIM

D	I	E	S	I	S	T	E	I	N	E	B	O	T	S	C	H	A	F	T
G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I	M	G	E

Nun wird jedem Buchstaben eine Zahl zugeordnet nach der folgenden Tabelle

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

Die Zahl 4 entspricht nach der obigen Tabelle dem Buchstaben E.

$A \rightarrow 0$, $B \rightarrow 1$, $C \rightarrow 2$, ... $Z \rightarrow 25$ diese Werte erhält man einfach über den ASCII-Code der Großbuchstaben:

'A' - 'A' = 0; 'B' - 'A' = 1; 'C' - 'A' = 2; ... 'Z' - 'A' = 25;

Die Codierung erfolgt, indem die zugeordneten Werte der einzelnen Buchstaben die übereinander stehen addiert werden.

Für den Wert des i-ten Buchstabens des codierten Textes ergibt sich die folgende Berechnung:

$\text{codewert}[i] = (\text{klartextwert}[i] + \text{keywert}[i]) \bmod 26$

Die Modulooperation wird verwendet, weil zwei Buchstabenwerte den Wert von 25 überschreiten könnten und so außerhalb des Alphabetes lägen.

Beispiel:

Zeile 1: Klartext: DIESISTEINEBOTSCHAFT

Zeile 2: Schlüssel: GEHEIM

Zeile 3: Der sich ergebende chiffrierter Text

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

Beispiel (grau markiert): 'S' + 'M' $\rightarrow 18 + 12 = 30 \rightarrow 30 \bmod 26 = 4$ (entspricht 'E')

$\text{codewert}[5] = (18 + 12) \bmod 26 \rightarrow \text{codewert}[5] = 4$.