Übungsblatt 3 – Teil 2

Ausgabe: 15.05.2014
Abgabe: 21.05.2014

Aufgabe 3: FilterWriter und FilterReader am Beispiel der Caesar-Chiffre — 50 Punkte

Die Caesar-Chiffre ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert.
Bei der Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Geheimtextbuchstaben abgebildet. Diese Abbildung ergibt sich, indem man die Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch nach rechts verschiebt (rotiert). Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt.

Beispiel: Verschiebung um fünf Zeichen

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
Geheim:	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

Aus dem Klartext „Caesar“ würde also der Geheimtext HFJXFW.

Implementieren Sie die Klassen `CaesarWriter` und `CaesarReader`, welche folgende Anforderungen erfüllen sollen:

`CaesarWriter`

- Diese Klasse soll den zu schreibenden Text mittels Caesar-Chiffre *verschlüsseln*.
- Sie soll einen Konstruktor besitzen, dem die Anzahl der Verschiebungen übergeben werden kann. Dieser Konstruktor soll selbstverständlich ebenfalls die Verschachtelung verschiedener Writer-Implementierungen unterstützen.
- `CaesarWriter` soll von der Klasse `FilterWriter` aus dem Paket `java.io` erben. Überlegen Sie sich, welche Methoden Sie überschreiben müssen, sodass eine korrekte Verschlüsselung zu jeder Zeit garantiert ist.

`CaesarReader`

- Diese Klasse soll den zu lesenden Text mittels Caesar-Chiffre *entschlüsseln*.
- Sie soll einen Konstruktor besitzen, dem die Anzahl der Verschiebungen übergeben werden kann. Dieser Konstruktor soll selbstverständlich ebenfalls die Verschachtelung verschiedener Reader-Implementierungen unterstützen.
- `CaesarReader` soll von der Klasse `FilterReader` aus dem Paket `java.io` erben. Überlegen Sie sich, welche Methoden Sie überschreiben müssen, sodass eine korrekte Entschlüsselung zu jeder Zeit garantiert ist.

Es sollen nur Buchstaben (A-Z, a-z, Ä, Ö, Ü ,ä, ö, ü) verschlüsselt werden. Sonderzeichen und Leerzeichen sollen unverändert bleiben. Ihr Alphabet könnte also wie folgt aussehen:

0	1	…	25	26	27	…	51	52	53	54	55	56	57
A	B	…	Z	a	b	…	Z	Ä	Ö	Ü	ä	ö	ü

Beachten Sie: wird bei einer Verschiebung das Ende des Alphabets erreicht, wird wieder von vorne begonnen. Bei einer Verschiebung um 5 würde also beispielsweise Ü auf B abgebildet werden.