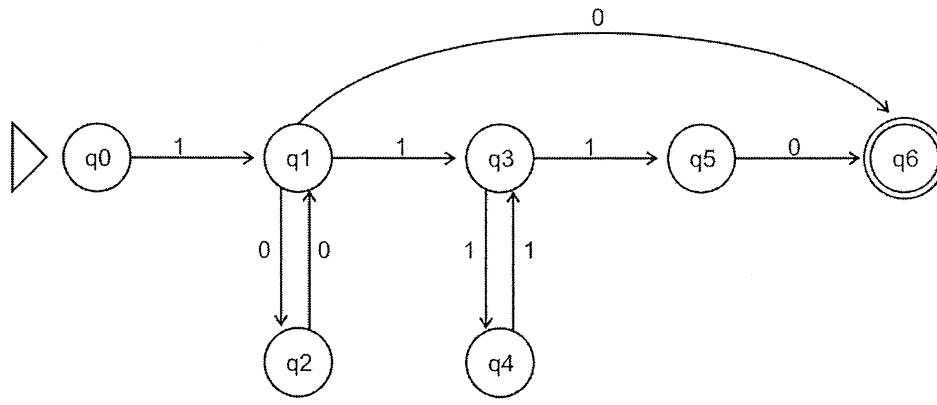


Teilaufg.	Aufgabe 1	Pkt
1.1.1	<p>Lösung in Java:</p> <pre> int mult1(int a, int b){ int sum=0; int i; for(i=1;i<=a;i=i+1){ sum=sum+b; } return sum; } </pre> <p>Lösung in Delphi:</p> <pre> function mult1(a,b:integer):integer; var i:integer; begin result:=0; for i:=1 to a do result:=result+b; end; </pre>	3
1.1.2		
a)	$3 \cdot 7 = 7 + 2 \cdot 7 = 7 + 7 + 1 \cdot 7 = 7 + 7 + 7 + 0 = 21$	1
b)	<p>Lösung in Java:</p> <pre> int mult2(int a, int b){ if(a>0){ return b+mult2(a-1,b); } else{ return 0; } } </pre> <p>Lösung in Delphi:</p> <pre> function mult2(a,b:integer):integer; begin if a>0 then result:=b+mult2(a-1,b) else result:=0; end; </pre>	3

1.1.3	<p>Lösung in Java:</p> <pre>int mult3(int a, int b){ if(a>=0){ return mult2(a,b); } else{ return -mult2(-a,b); } }</pre> <p>Lösung in Delphi:</p> <pre>function mult3(a,b:integer):integer; begin if a<0 then result:=-1*mult2(-1*a,b) else result:=mult2(a,b); end;</pre> <p>Korrekt ist auch die Betrachtung einer anderen Fallunterscheidung.</p>	3
1.2.1	<p>Lösung in Java:</p> <pre>class Knoten{ public int data; public Knoten next; }</pre> <p>Lösung in Delphi:</p> <pre>type TZeiger=^TKnoten; TKnoten=record data:integer; next:TZeiger; end;</pre>	2
1.2.2		
a)	<p>Lösung in Java:</p> <pre>L=L.next;</pre> <p>Lösung in Delphi:</p> <pre>L:=L^.next;</pre>	1
b)	<p>Lösung in Java:</p> <pre>Knoten kneu=new Knoten(); kneu.data=45; kneu.next=L.next; L.next=kneu;</pre> <p>Lösung in Delphi:</p> <pre>new(pneu); pneu^.data:=45; pneu^.next:=L^.next; L^.next:=pneu;</pre>	3

1.2.3	<p>Lösung in Java:</p> <pre> int summe(Knoten k){ Knoten kneu=new Knoten(); int erg=0; kneu=k; while(kneu!=null){ erg=erg+kneu.data; kneu=kneu.next; } return erg; } </pre> <p>Lösung in Delphi:</p> <pre> function summe(pL:TZeiger):integer; var paktuell:TZeiger; begin result:=0 paktuell:=pL; while paktuell<>nil do begin result:=result+paktuell^.data; paktuell:=paktuell^.next; end; end; </pre>	4
-------	---	---

Teilaufg.	Aufgabe 2	Pkt
2.1.1	Es ist $R = 1(00)^*(11)^*0$	2
2.1.2	Eine mögliche Grammatik lautet: $P = \{S \rightarrow 1A; A \rightarrow 00A \mid B; B \rightarrow 11B \mid 0\}$	2,5
2.1.3	 <pre> graph LR start(()) --> q0((q0)) q0 -- 1 --> q1((q1)) q1 -- 0 --> q2((q2)) q2 -- 0 --> q1 q1 -- 1 --> q3((q3)) q3 -- 1 --> q4((q4)) q4 -- 1 --> q3 q3 -- 1 --> q5((q5)) q5 -- 0 --> q6(((q6))) q1 -- 0 --> q6 style start fill:none,stroke:none </pre>	3,5

2.2	<table> <tr> <th>δ^*</th> <th>1</th> <th>2</th> </tr> <tr> <td>$z0 := \{q0\}$</td> <td>$\{q0, q1\}$</td> <td>$\{\}$</td> </tr> <tr> <td>$z1 := \{q0, q1\}$</td> <td>$\{q0, q1\}$</td> <td>$\{q0, q2\}$</td> </tr> <tr> <td>$z2 := \{q0, q2\}$</td> <td>$\{q0, q1\}$</td> <td>$\{\}$</td> </tr> </table> <p>Startzustand= $z0$, Endzustand= $\{z2\}$, Alphabet= $\{1, 2\}$, Zustände= $\{z0, z1, z2\}$, Übergangsfunktion δ^* s. Tabelle</p>	δ^*	1	2	$z0 := \{q0\}$	$\{q0, q1\}$	$\{\}$	$z1 := \{q0, q1\}$	$\{q0, q1\}$	$\{q0, q2\}$	$z2 := \{q0, q2\}$	$\{q0, q1\}$	$\{\}$	5				
δ^*	1	2																
$z0 := \{q0\}$	$\{q0, q1\}$	$\{\}$																
$z1 := \{q0, q1\}$	$\{q0, q1\}$	$\{q0, q2\}$																
$z2 := \{q0, q2\}$	$\{q0, q1\}$	$\{\}$																
2.3.1	<p>Eingangsalphabet= $\{a, b, c\}$, Ausgabealphabet= $\{x, y, z\}$, Startzustand= $q0$, Zustände= $\{q0, q1, q2\}$, Endzustände= $\{\}$, Übergangsfunktion δ^* s. Tabelle</p> <table> <tr> <th>δ^*</th> <th>a</th> <th>b</th> <th>c</th> </tr> <tr> <td>$q0$</td> <td>$q1 x$</td> <td>$q2 y$</td> <td>$q0 z$</td> </tr> <tr> <td>$q1$</td> <td>$q2 z$</td> <td>$q1 y$</td> <td>$q1 x$</td> </tr> <tr> <td>$q2$</td> <td>$q0 y$</td> <td>$q0 z$</td> <td>$q2 x$</td> </tr> </table>	δ^*	a	b	c	$q0$	$q1 x$	$q2 y$	$q0 z$	$q1$	$q2 z$	$q1 y$	$q1 x$	$q2$	$q0 y$	$q0 z$	$q2 x$	3
δ^*	a	b	c															
$q0$	$q1 x$	$q2 y$	$q0 z$															
$q1$	$q2 z$	$q1 y$	$q1 x$															
$q2$	$q0 y$	$q0 z$	$q2 x$															
2.3.2	$\rightarrow q0 \xrightarrow{x} q1 \xrightarrow{y} q1 \xrightarrow{x} q1 \xrightarrow{z} q2 \xrightarrow{z} q0 \xrightarrow{z} q0$	1,5																
2.3.3	<p>Das erste Zeichen ist ein z gewesen. <u>Da sich der Automat im Startzustand befindet, muss das Eingabewort mit einem c begonnen haben.</u> Der Automat befindet sich dann immer noch im Zustand $q0$.</p> <p>Das zweite Ausgabezeichen ist ein x, daher muss das Eingabezeichen ein a gewesen sein.</p> <p><u>Man fragt also rückwärts, wie ist die Ausgabe entstanden und in welchem Zustand befindet sich dann der Automat.</u> Man erhält insgesamt die folgende Rückübersetzung $w=cabaca$, denn</p> $\rightarrow q0 \xrightarrow{z} q0 \xrightarrow{x} q1 \xrightarrow{y} q1 \xrightarrow{z} q2 \xrightarrow{x} q2 \xrightarrow{y} q0$	2,5																

Teilaufg.	Aufgabe 3:	Pkt
3.1.1	<p>Gegeben ist eine zufällige Anordnung einer vorgegebenen Menge von n Zahlen. <u>In dieser Anordnung wird zunächst von vorne angefangen das größte Element gesucht, die Position und der Wert gespeichert und mit dem letzten Element der Anordnung getauscht.</u> Damit ist der 1. Durchlauf beendet und <u>das größte Element der Anordnung steht an letzter Stelle.</u></p> <p>Im 2. Durchlauf wird die neue Anordnung nur bis <u>zum vorletzten Element durchlaufen.</u> Auch hier wird nach dem <u>größten Element</u> gesucht und <u>mit dem Element an vorletzter Stelle vertauscht.</u> Damit verringert sich die zu durchlaufende Anzahl der Elemente jeweils um 1.</p> <p><u>Das Verfahren wiederholt man nun solange, bis nur noch die beiden ersten Elemente verglichen und evtl. vertauscht werden müssen.</u></p>	3

3.1.2									3
		1.	2.	3.	4.	5.	6.	7.	
	Ausgangsanzordnung	40	4	38	13	2	23	8	
	Nach dem 1. Durchlauf	4	38	13	2	23	8	40	
	Nach dem 2. Durchlauf	4	13	2	23	8	38	40	
	Nach dem 3. Durchlauf	4	2	13	8	23	38	40	
	Nach dem 4. Durchlauf	2	4	8	13	23	38	40	
	Nach dem 5. Durchlauf	2	4	8	13	23	38	40	
	Nach dem 6. Durchlauf	Schluss							
3.2.1									
a)	Es sind 7 Zahlen vorgegeben. Beim ersten Durchlauf müssen 6 Vergleiche durchgeführt werden. Beim 2. Durchlauf nur noch 5 Vergleiche, beim 3. Durchlauf dann 4, usw. Beim 6. Durchlauf ist dann nur noch ein Vergleich durchzuführen, so dass man folgende Summe erhält: $6+5+4+3+2+1=21$.								1
b)	Für eine große Anzahl von n Elementen werden nach dem Maxsort-Verfahren also $\sum_{i=1}^{n-1} i = (n-1) + (n-2) + \dots + 2 + 1 = \frac{n \cdot (n-1)}{2} = \frac{1}{2}(n^2 - n)$ Vergleiche durchgeführt. Daher ist die Laufzeit von der Ordnung $O(n^2)$.								2

3.2.2									
a)	Im <u>günstigsten Fall</u> ist die Anordnung in der <u>richtigen Reihenfolge</u> . Das Bubblesort-Verfahren läuft dann die Anordnung <u>nur ein Mal</u> durch. Es werden dann <u>(n-1) Vergleiche</u> durchgeführt. Das Laufzeitverhalten ist also <u>$O(n)$</u> . Im <u>ungünstigsten Fall</u> ist die Liste falsch herum sortiert. Dann werden zunächst <u>(n-1), dann (n-2), dann (n-3), ... Vergleiche pro Durchgang</u> durchgeführt. Es ergeben sich somit <u>n Durchläufe</u> und daher ein Laufzeitverhalten der Ordnung <u>$O(n^2)$</u> .								2
b)	Das Bubblesort-Verfahren hat in der Regel ein besseres Laufzeitverhalten als das Maxsort-Verfahren. <u>Nur wenn die Reihe „falschherum“ sortiert ist, stimmt das Laufzeitverhalten des Bubblesort-Verfahrens mit dem Laufzeitverhalten des Maxsort-Verfahrens überein.</u> Während eine <u>Vorsortierung</u> auf das Laufzeitverhalten des <u>Maxsortverfahrens keinen Einfluss hat</u> , denn es wird von jeder verringerten Anordnung jeweils das Maximum gesucht, <u>verbessert sich die Laufzeit beim Bubblesort-Verfahren.</u>								1,5

3.3.1		
a)	<u>Durch Vergleich der Häufigkeitsverteilungen kann jedem Buchstaben des kodierten Textes ein entsprechendes Zeichen des ursprünglichen Textes zugeordnet werden. Eventuell unklare Zuordnungen können dann noch aus dem Kontext heraus gebildet werden.</u>	1,5
b)	Jedem Geheimtextzeichen wird eindeutig ein Klartextzeichen zugeordnet und umgekehrt.	1
c)	Das RSA-Verfahren ist ebenfalls ein Substitutionsverfahren, da auch hier <u>bestimmte Zahlen durch andere Zahlen ersetzt werden</u> . Das RSA-Verfahren wehrt einen Angriff durch die Häufigkeitsanalyse durch die <u>Bildung von Blöcken B einer bestimmten Länge l ab</u> . Es sind die Blöcke, die dann durch andere Zeichen (andere Blöcke) <u>substituiert</u> werden. Durch die Blockbildung wird die Häufigkeitsanalyse zumindest erschwert.	2
3.3.2		
a)	Bei dem Automaten wird <u>jeder Buchstabe des Eingangsalphabets durch einen anderen Buchstaben des Ausgabealphabets ersetzt</u> . Daher stellt der Automat ein Substitutionsverfahren dar.	1
b)	Die Zuordnung der Buchstaben des Eingangsalphabets zu den Buchstaben des Ausgangsalphabets ist <u>abhängig von dem Zustand</u> , in dem sich der Automat gerade befindet. Es wird also <u>nicht immer einem Buchstaben des Eingangsalphabets derselbe Buchstabe des Ausgangsalphabets zugeordnet</u> .	2