

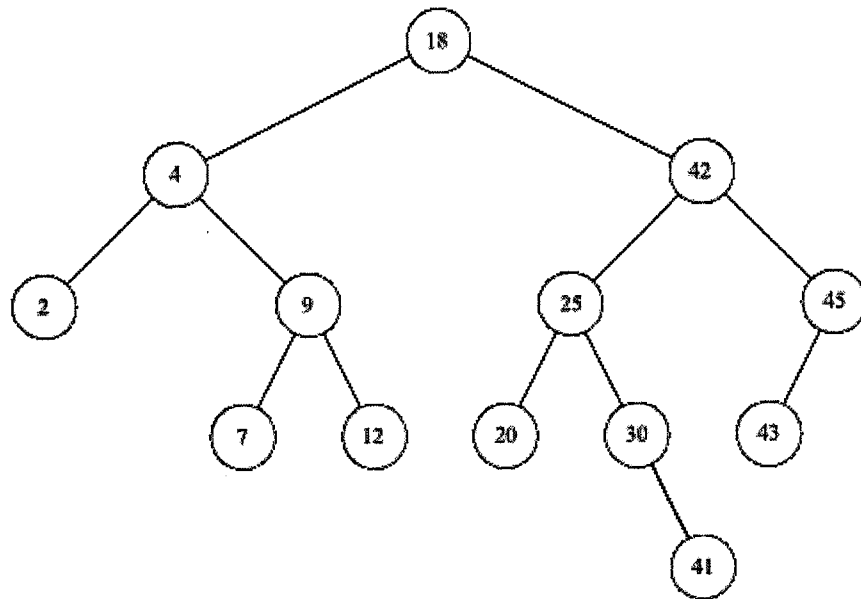
Nur für die Hand des Lehrers!

Teilaufg.	Aufgabe 1	Pkte												
1.1.1	<table><tr><td>TVektor</td></tr><tr><td>x1 : Real</td></tr><tr><td>x2 : Real</td></tr><tr><td>x3 : Real</td></tr><tr><td>add(v : TVektor): TVektor</td></tr><tr><td>sub(v : TVektor): TVektor</td></tr><tr><td>mult(r : Real): TVektor</td></tr><tr><td>skalarprodukt (v : TVektor) : Real</td></tr><tr><td>vektorprodukt (v : TVektor) : TVektor</td></tr><tr><td>betrag() : Real</td></tr><tr><td>istOrthogonalZu (v : TVektor) : Boolean</td></tr><tr><td>istParallelZu (v : TVektor) : Boolean</td></tr></table>	TVektor	x1 : Real	x2 : Real	x3 : Real	add(v : TVektor): TVektor	sub(v : TVektor): TVektor	mult(r : Real): TVektor	skalarprodukt (v : TVektor) : Real	vektorprodukt (v : TVektor) : TVektor	betrag() : Real	istOrthogonalZu (v : TVektor) : Boolean	istParallelZu (v : TVektor) : Boolean	3
TVektor														
x1 : Real														
x2 : Real														
x3 : Real														
add(v : TVektor): TVektor														
sub(v : TVektor): TVektor														
mult(r : Real): TVektor														
skalarprodukt (v : TVektor) : Real														
vektorprodukt (v : TVektor) : TVektor														
betrag() : Real														
istOrthogonalZu (v : TVektor) : Boolean														
istParallelZu (v : TVektor) : Boolean														
1.1.2	<p>Delphi:</p> <pre>function TVektor.skalarprodukt(v:TVektor): Real; begin result := x1*v.x1 + x2*v.x2 + x3*v.x3; end; function TVektor.istOrthogonalZu(v:TVektor): boolean; begin result := skalarprodukt(v) = 0; end;</pre> <p>Java:</p> <pre>float skalarprodukt(TVektor v) { return x1*v.x1 + x2*v.x2 + x3*v.x3; } boolean istOrthogonalZu(TVektor v) { return (skalarprodukt(v) == 0); }}</pre>	<div>2</div> <div>2</div>												

Nur für die Hand des Lehrers!

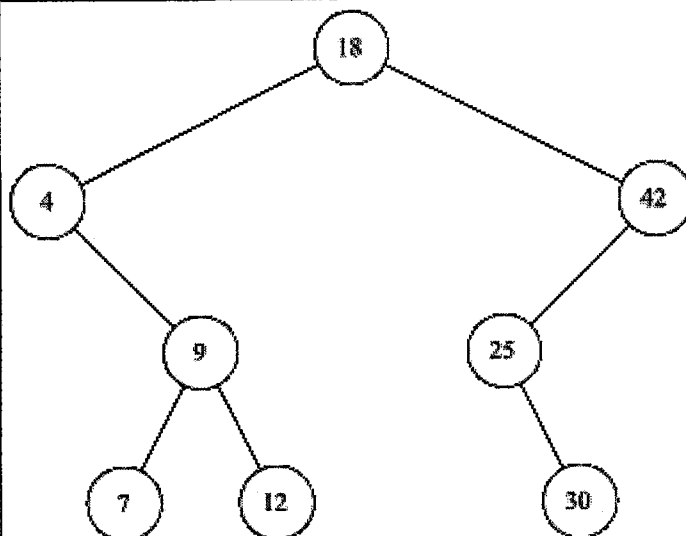
1.2.1

2



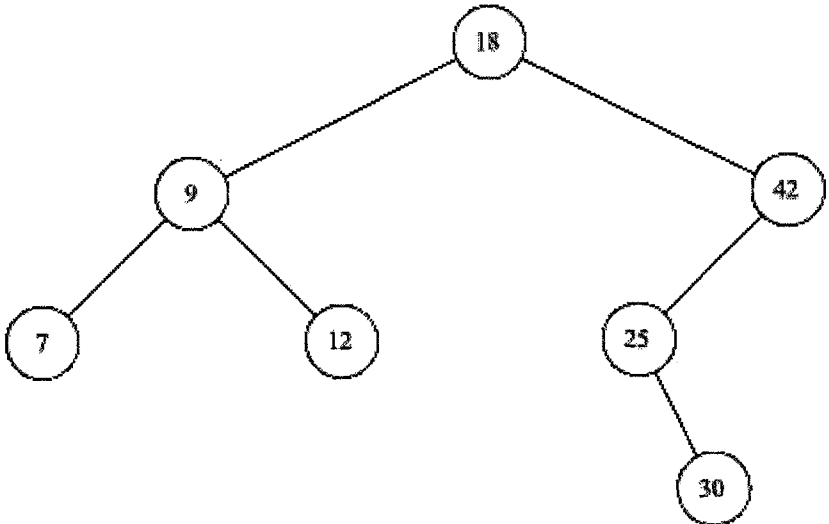
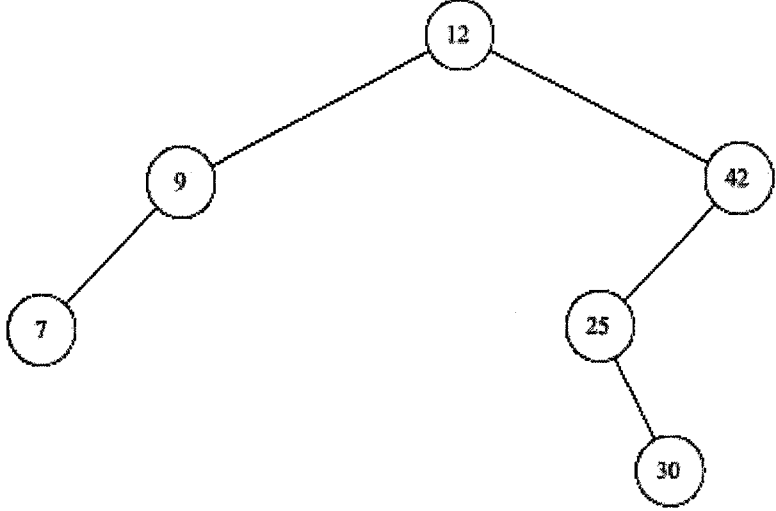
1.2.2

1

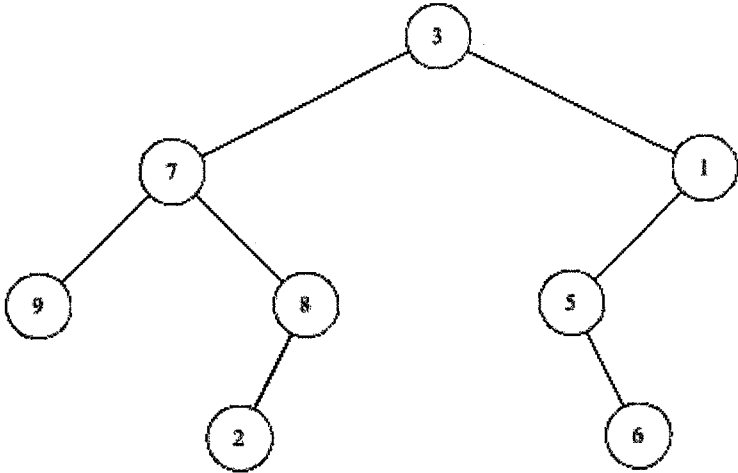


Die 2 steht in einem Blatt, dieses kann also einfach entfernt werden.

Nur für die Hand des Lehrers!

		1,5
	<p>Der Knoten mit der 4 hat nun ein Kind, wird also durch dieses ersetzt.</p>  <p>Der Knoten mit der 18 hat zwei Kinder. Also wird die größte Zahl des linken Teilbaums (12) in diesen Knoten geschrieben und anschließend aus dem linken Teilbaum entfernt.</p>	1,5
1.2.3	2 7 12 9 4 30 25 42 18	2

Nur für die Hand des Lehrers!

1.2.4	 <pre> graph TD 3((3)) --- 7((7)) 3 --- 1((1)) 7 --- 9((9)) 7 --- 8((8)) 8 --- 2((2)) 1 --- 5((5)) 5 --- 6((6)) </pre>	3
1.2.5	Minimale Höhe: 8, maximale Höhe: 299	2

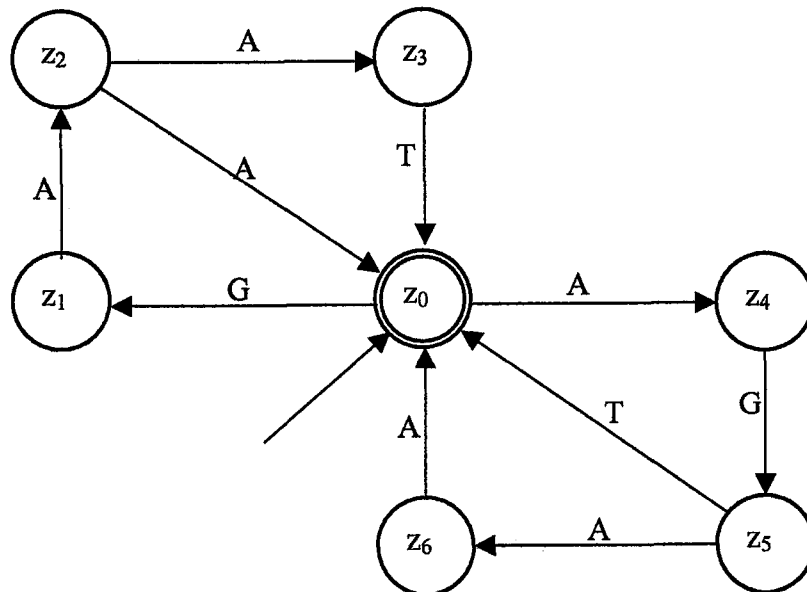
Teilaufg.	Aufgabe 2	Pkte
2.1.1	<p>GAATTTAG ist keine gültige Sequenz, da GAA oder GAAT am Beginn des Wortes stehen, aber die darauf folgenden Zeichen TTT... oder TTA... kein Bestandteil eines gültigen Teilwortes einer DNA-Sequenz sind.</p> <p>GAATAGTGAA ist eine gültige DNA-Sequenz bestehend aus den Teilworten GAAT, AGT und GAA.</p>	2

Nur für die Hand des Lehrers!

2.1.2

Übergangsdiagramm:

5



2.2.1

 $(A|G|T)^* AGT (A|G|T)^*$

2

2.2.2

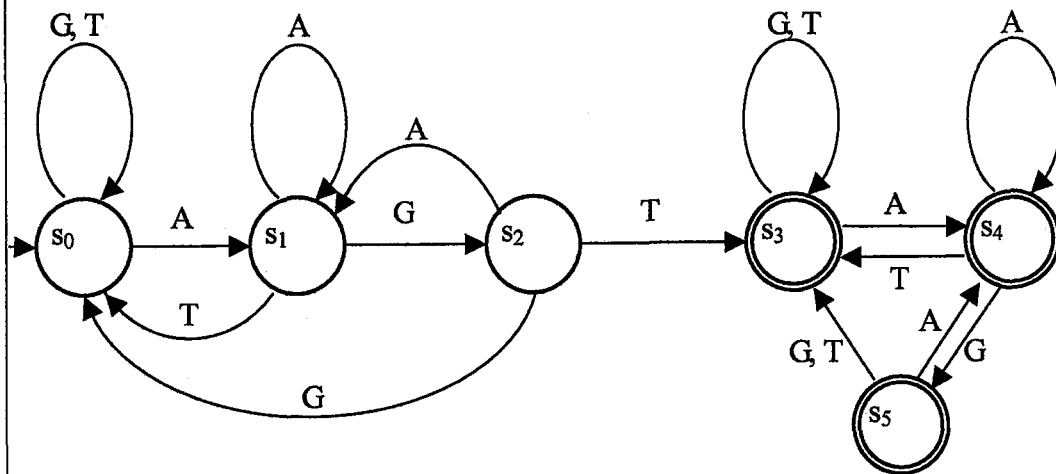
	A	G	T
$s_0 = \{z_0\}$	$s_1 = \{z_0, z_1\}$	$s_0 = \{z_0\}$	$s_0 = \{z_0\}$
$s_1 = \{z_0, z_1\}$	$s_1 = \{z_0, z_1\}$	$s_2 = \{z_0, z_2\}$	$s_0 = \{z_0\}$
$s_2 = \{z_0, z_2\}$	$s_1 = \{z_0, z_1\}$	$s_0 = \{z_0\}$	$s_3 = \{z_0, z_3\}$
$s_3 = \{z_0, z_3\}$	$s_4 = \{z_0, z_1, z_3\}$	$s_3 = \{z_0, z_3\}$	$s_3 = \{z_0, z_3\}$
$s_4 = \{z_0, z_1, z_3\}$	$s_4 = \{z_0, z_1, z_3\}$	$s_5 = \{z_0, z_2, z_3\}$	$s_3 = \{z_0, z_3\}$
$s_5 = \{z_0, z_2, z_3\}$	$s_4 = \{z_0, z_1, z_3\}$	$s_3 = \{z_0, z_3\}$	$s_3 = \{z_0, z_3\}$

6

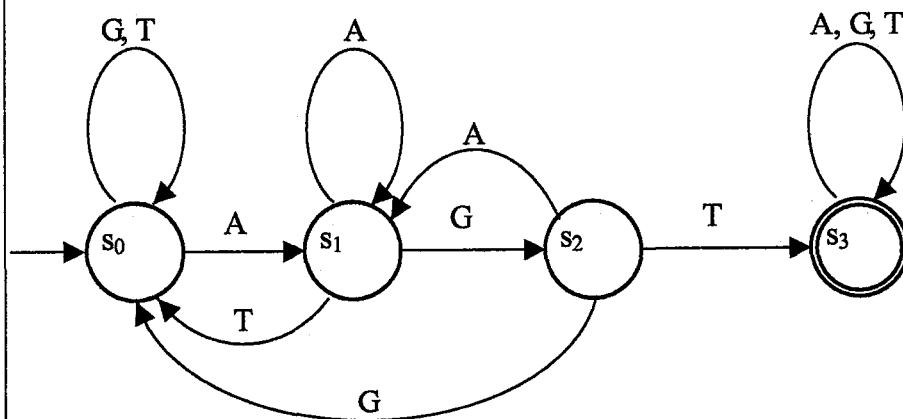
Zustände $\{s_0, s_1, s_2, s_3, s_4, s_5\}$, Alphabet $\{A, G, T\}$, Startzustand s_0 , Menge der Endzustände $\{s_3, s_4, s_5\}$

Nur für die Hand des Lehrers!

Darstellung als Übergangsdiagramm:



oder vereinfacht



2.3

Grammatik G mit

Terminalsymbole $\{A, G, T\}$,Nichtterminalsymbole $\{S, W, X, V, Y\}$

Startsymbol: S

Produktionensystem:

 $\{S \rightarrow SS|W|X|VSY|YSV|\epsilon, V \rightarrow AGT, W \rightarrow AGAA, X \rightarrow GAAT, Y \rightarrow GAA\}$ Die Produktionen $S \rightarrow VSY$ und $S \rightarrow YSV$ können nicht durch reguläre Produktionen ersetzt werden.

5

Nur für die Hand des Lehrers!

Teilaufg.	Aufgabe 3	Pkte
3.1.1	<p>Das Programm testet die eingegebene Zahl ob sie durch 7 teilbar ist. Der Ausgabewert 0 bedeutet, dass die Eingabe ohne Rest durch 7 teilbar ist, der Ausgabewert 1 bedeutet das Gegenteil. => Eingabe 28 liefert 0, Eingabe 19 liefert 1.</p>	3
3.1.2	<pre> 0 INM 21 1 LDA 21 2 JNP 10 3 LDA 22 4 ADD 21 5 STA 22 6 LDA 21 7 DEC 8 STA 21 9 JMP 1 10 OUT 22 11 END 21 DEF 0 //n 22 DEF 0 //Summe </pre>	4
3.2.1	<p>Symmetrische Verschlüsselung: Jedes Kommunikationspaar benötigt einen anderen Schlüssel. Es gibt $9+8+7+6+5+4+3+2+1=45$ Paare, also benötigt man 45 Schlüssel.</p> <p>Asymmetrische Verschlüsselung: Jede Person benötigt nur ein Schlüsselpaar, also benötigt man 10 Schlüsselpaare bzw. 20 Schlüssel.</p>	2 1
3.2.2	<p>Sobald das Verfahren öffentlich bekannt ist, ist es genauso sicher oder unsicher, wie das reine Substitutionsverfahren ohne zusätzliche Zeichen. Jeder kann, ohne Kenntnis des Schlüssel jedes zweite Zeichen streichen. Das Prinzip von Kerckhoffs wird somit verletzt.</p>	2

Nur für die Hand des Lehrers!

3.2.3

a) $n = p \cdot q = 1643$; $\varphi = (p-1) \cdot (q-1) = 1560$

Bestimmung von d mit Hilfe des erweiterten euklidischen Algorithmus:

q	g	v	d
	1560	1	0
	29	0	1
53	23	1	-53
1	6	-1	54
3	5	4	-215
1	1	-5	269

Ergebnis $d = 269$ b) Der Absender benutzt das öffentliche Schlüsselpaar (e,n) des Empfängers und codiert die Nachricht m zu $c = m^e \bmod n$.Der Empfänger decodiert die Nachricht c mit Hilfe seines geheimen Schlüssels (d,n) unter Verwendung der Gleichung $m' = c^d \bmod n$.c) Ein Angreifer muss - um $\varphi(n)$ errechnen zu können- den Modul n wieder in die Primfaktoren p und q zerlegen. Nur so kann er d als modulares Inverses des (öffentlichen) e berechnen. Die Faktorisierung von n ist bei großen Primzahlen nur mit sehr großen Rechenzeiten möglich.

4

2

2

Nur für die Hand des Lehrers!**Aufgabe 1:**

Aufgabe	1.1.1	1.1.2	1.2.1	1.2.2	1.2.3	1.2.4	1.2.5	Σ
Punkte	3	4	2	4	2	3	2	20
erreicht								

Aufgabe 2:

Aufgabe	2.1.1	2.1.2	2.2.1	2.2.2	2.3	Σ
Punkte	2	5	2	6	5	20
erreicht						

Aufgabe 3:

Aufgabe	3.1.1	3.1.2	3.2.1	3.2.2	3.2.3a	3.2.3b	3.2.3c	Σ
Punkte	3	4	3	2	4	2	2	20
erreicht								