Erwartungshorizont / Bewertungsbogen für den Prüfling: _____

(BE: vom o. a. Prüfling erreichte Bewertungseinheiten)

Aufgabe	Erwartete Schülerleistungen	Anforderungsbereiche Bewertung			
		I	II	III	BE
Aufg. 1					
a)	Daten für Achteck-Codierung ergänzen	3			
	Achteck-Code mit genau 6 Einsen angeben	1	1		
	Nicht-Existenz von Codes mit mehr als 6 Einsen begründen	1	1		
	Rekonstruktion bei genau 2 fehlenden Bits begründen		1	1	
	Mindestanzahl für Rekonstruktion untersuchen		1	1	
b)	Fehlererkennung und -korrektur analysieren	3	2		
	Achteck-Code mit (7,4)-Hamming-Code vergleichen		3		
c)	Verarbeitung von 1011 in einer Tracetabelle darstellen	3	1		
	Fehlerhaftigkeit erläutern		2		
	Korrektur des Algorithmus durch Dokumentieren und Erläutern entwickeln		1	2	
	Eingeschränkte Eignung des ADT Schlange begründen		2		
	Summe: 30	11	15	4	

Aufg. 2					
a)	Verschlüsselung protokollieren	3			
	Rekursion am Beispiel erläutern	2	1		
	Struktogramm für eine iterative Operation entwickeln		3	1	
b)	Gemeinsamkeiten und Unterschiede der ADTs nennen	3			
	Prinzip der Entschlüsselung beschreiben	2	2		
	Funktion der ADTs für die Entschlüsselung erläutern		3		
	Auswirkung einer Vertauschung analysieren		3	1	
c)	Entscheidung anhand der Häufigkeitsverteilung erläutern	1	3	2	
	Summe: 30	11	15	4	

Aufg. 3					
a)	Eingabewerte und Verhalten des Motors beschreiben	2			
	Verhalten der Motorsteuerung erläutern		1	1	
	Schaltterm zur Schaltwerttabelle angeben	1			
	Minimierten Schaltterm bestimmen		2		
	Schaltnetz zeichnen	2			
b)	Schaltnetz vervollständigen		2		
	Vorgehen erläutern		2		
	Funktionalität des Multiplexers beschreiben	2	1		
	Ausgabe der Schaltung analysieren und vergleichen		1	3	
c)	Zustandsgraph zeichnen		4		
	Ausgaben angeben	2			
	Unterschiede zwischen Mealy und NEA erläutern	2	2		
	Summe: 30	11	15	4	

Gesamtsumme: 90	**33**	**45**	**12**	

Aufgabe 2

zu a)

Protokollierung der Verschlüsselung mittels Tracetabelle

Das Ergebnis ist „ARBUIT“.

`text`	`geheimtext`
ABITUR	A
BITUR	AR
BITU	ARB
ITU	ARBU
IT	ARBUI
T	ARBUIT

Abbildung 2.1: Tracetabelle

Erläuterung der Rekursion

Ein Grundprinzip einer Rekursion ist, dass sich eine Operation selbst aufruft. Im Beispiel wird das in der letzten Zeile des Struktogramms durch `verschluesseln(text)` realisiert. Damit daraus keine endlose Abfolge von Selbstaufrufen entsteht, ist ein weiteres Grundprinzip einer Rekursion das Vorhandensein einer Abbruchbedingung. Im Beispiel wird `verschluesseln` auf eine kürzere Zeichenkette angewendet und vor jedem Selbstaufruf ausgewertet, ob die Textlänge größer als null ist. Damit enden die Selbstaufrufe, sobald die Textlänge null ist.

Struktogramm einer iterativen Operation

verschluesseln_iterativ(text: Zeichenkette)

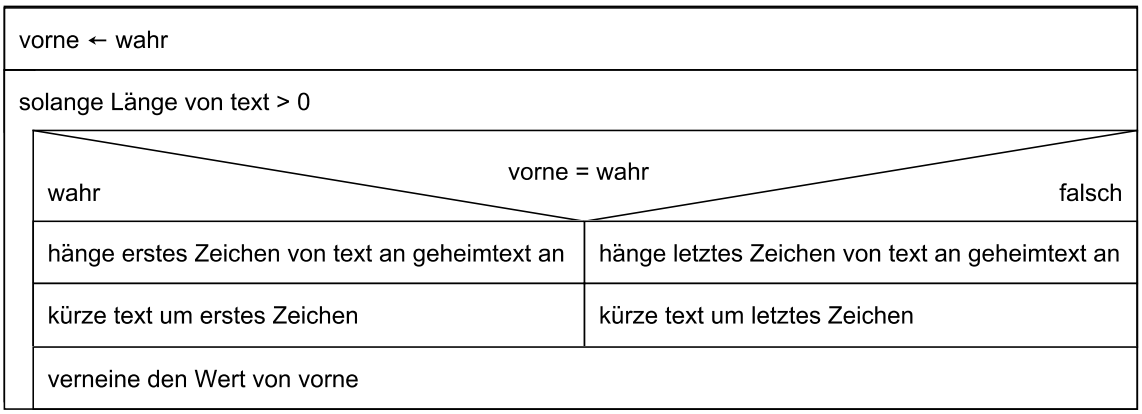

Abbildung 2.2: Struktogramm einer iterativen Operation

zu b)

Gemeinsamkeiten und Unterschiede der ADTs Schlange und Stapel

Stapel und Schlange sind abstrakte Datentypen, mit denen Daten dynamisch verwaltet werden. Sowohl Stapel als auch Schlange merken sich die Reihenfolge der eingefügten Inhalte. Es kann immer nur auf einen Inhalt zugegriffen werden.

Beim ADT Schlange werden Elemente am Ende angefügt und vorne wieder entnommen. Elemente, die zuerst eingefügt wurden, werden zuerst entnommen.

Beim ADT Stapel werden Elemente oben abgelegt und auch nur dort wieder entfernt. Das Element, das zuletzt eingefügt wurde, wird als erstes wieder entnommen.

Beschreibung des Prinzips der Entschlüsselung

Bei der Entschlüsselung werden immer die ersten zwei Zeichen des Geheimtextes betrachtet. Das erste Zeichen wird in einer Schlange abgelegt und das zweite auf einem Stapel. Danach werden beide Buchstaben aus dem Geheimtext entfernt. Dieses Vorgehen wird solange wiederholt, bis der Geheimtext keine Zeichen mehr enthält.

Der Klartext wird schrittweise vom ersten bis zum letzten Buchstaben aufgebaut. Dazu werden zuerst alle Elemente der Schlange entnommen und an den Klartext angehängt. Danach wird der Stapel buchstabenweise abgebaut, wobei jeder entnommene Buchstabe zum Geheimtext hinzugefügt wird.

Erläuterung der Verwendung zweier verschiedener ADTs

Die Reihenfolge der ersten Hälfte der Zeichen des Klartextes bleibt beim Erstellen des Geheimtextes erhalten. Diese Zeichen befinden sich an den ungeraden Stellen im Geheimtext. Beim Entschlüsseln muss folglich die Reihenfolge weiterhin erhalten bleiben, was durch die Schlange gewährleistet wird.

Beim Verschlüsseln der zweiten Hälfte des Geheimtextes wird die Reihenfolge der Zeichen umgekehrt: Das letzte Zeichen wird als erstes angehängt, das vorletzte als zweites und so weiter. Deswegen muss beim Entschlüsseln die Reihenfolge erneut umgekehrt werden, was durch einen Stapel realisiert werden kann.

Wegen der unterschiedlichen Reihenfolgen wurden zwei verschiedene ADTs verwendet.

Analyse der Auswirkung einer Vertauschung

Wenn statt der Schlange ein Stapel verwendet wird, ergibt sich für diesen Stapel die Buchstabenfolge „BRA“. Allerdings wird durch den Stapel die Reihenfolge der Buchstaben umgekehrt. Dies ist für die Entschlüsselung falsch.

Für die Schlange ergibt sich durch die Vertauschung die Buchstabenfolge „TIE“. Bei den Buchstaben auf einer geraden Position muss die Reihenfolge zur Entschlüsselung umgekehrt werden. Die Schlange leistet dies jedoch nicht, also bleiben die Buchstaben in der Reihenfolge des Geheimtextes.

Als Klartext entsteht das Wort „BRATIE“.

zu c)

Erläuterung zur Entscheidung des Verfahrens

Alle Verfahren liefern unterschiedliche Ergebnisse der Häufigkeitsanalyse. Je nach Ergebnis kann dann entschieden werden.

Beim OwnCrypt-Verschlüsselungsverfahren werden die Buchstabenhäufigkeiten nicht verändert, man erhält also eine der Sprache entsprechende Häufigkeitsverteilung der Buchstaben, wenn der Text ausreichend lang ist.

Durch die Caesar-Chiffre wird die in jeder Sprache ungleiche Verteilung der Buchstabenhäufigkeit nicht verborgen. Allerdings ist die Häufigkeit der einzelnen Buchstaben entsprechend des gewählten Schlüssels verschoben.

Für das Vigenère-Verfahren mit einem Schlüsselwort der Länge größer gleich zwei wird die Häufigkeit durch die polyalphabetische Vorgehensweise stark verändert. Dadurch werden die Unterschiede zwischen den Buchstabenhäufigkeiten in der Regel geringer.