Nicht klausurrelevant sind: BEALE-Papers, Enigma

Aufgabensammlung

Algorithmik

1) Was versteht man unter einer While-Schleife? Gib ein Beispiel an! (Kapitel 4.7.1)

Es wird ein Programmteil wiederholt, bis eine Bedingung erfüllt ist.

```
Pseudocode:

int a=0;
while (a!=5) {
  a sei Zufallszahl zwischen (0,10)...
}

// wie oft a eine Zahl bekommt lässt sich nicht genau sagen
// vielleicht beim ersten mal, vielleicht nie?
```

Es gibt die Möglichkeit über einen Index oder über einen Iterator eine Sammlung zu durchlaufen.
2) Welche Methoden benötigt ein Objekt der Klasse Iteratur, damit eine Sammlung durchlaufen werden kann? (Kapitel 4.7.2)

3) Wie wird eine Sammlung mithilfe eines Index durchlaufen? (Kapitel 4.7.3)

```
Die Sammlung, z.B. ein Array, besitzt oft einen Index, der bei der
Variable direkt mit angegeben wird, z.B. a[5]=5;

durchlaufen wir die gesamte Sammlung z.B. mit einer for-Schleife
for (int i=0; i<a.length(); i++){
    if (a[i]==5)
}
```

4) Beschreibe, was man unter einem Array versteht, welche Vor- und Nachteile ergeben sich im Vergleich mit einer ArrayList? (Kapitel 4.10)

5) Erzeuge ein Programm, das ein Array mit dem Namen Anzahl erstellt, 26 Einträge vom Typ „integer“ hat und jedem Eintrag einen Startwert von -1 gibt.

```
int[] Anzahl=new int[26];
for (int i=0; i<26; i++) Anzahl[i]=-1;
```

6) Java ist deshalb so gut, weil es so viele Bibliotheksklassen hat. Was versteht man unter Bibliotheksklassen. Geben Sie ein Beispiel, warum dies ein so bedeutender Vorteil dieser Programmiersprache ist! Warum ergänzt sich „Objektorientierte Programmierung“ und eine umfangreiche Klassenbibliothek so hervorragend? Kapitel 5

7) Was versteht man unter einer Schnittstelle?
Die Schnittstelle einer Klasse beschreibt, was eine Klasse leistet und wie sie benutzt werden kann, ohne dass ihre Implementierung sichtbar wird.

Einführung

Beschreibe den Unterschied zwischen Steganographie und Kryptographie anhand eines Beispiels.
Bei der Steganographie wird die Nachricht nur verborgen, wird sie entdeckt so ist sie lesbar.
Z.B. wird eine Nachricht auf die Innenseite eines Gürtels geschrieben.

Bei der Kryptographie wird die Nachricht verschlüsselt, selbst wenn sie gefunden wird, kann der Sinn nicht ohne weiteres herausgefunden werden.

Beschreibe den Unterschied zwischen Transposition und Substitution anhand eines Beispiels.
Bei der Transposition werden die Buchstaben eines Textes durcheinandergewürfelt, z.B. zuerst alle ungeraden Buchstaben augelistet und dann alle geraden, aus hallo wird hloal. Bei der Substituion wird jeder Buchstabe durch ein anderes Zeichen ersetzt, z.B. um eines Stelle weiter im Alphabet, aus hallo wird ibmmp.

Eine Möglichkeit, eine monoalphabetische Verschlüsselung zu knacken, liegt in der Häufigkeitsanalyse.

1) Beschreibe was man darunter versteht.

Bei der Häufigkeitsanlayse werden die Buchstaben eines Textes gezählt, da in jeder Sprache bestimmte Buchstaben mit einer gewissen Häufigkeit vorkommen. Im Deutschen ist das z.B. der Buchstabe E. Bei einer Substituion kann ein Buchstabe also entschlüsselt werden, indem der häufigste Buchstabe „abgezält" wird.

2) Schreibe ein Programm, das für einen Text eine Häufigkeitsanalyse durchführt. Auch Pseudocode ist erlaubt!

```
Pseudocode:
// Array für alle Buchstaben
int[] alphabet = new int[26];
// Wiederholung für alle Buchstaben
wiederhole so oft, wie es Buchstaben im Text gibt{
    char a ist nächster Buchstabe;
    // erhöhe dort den Array, welcher Buchstabe gelesen wurde
    alphabet[ord(a)]++;
}
```

3) Beschreibe, warum sich die Häufigkeitsanlayse bei Verwendung einer polyalphabetischen Verschlüsselung nicht mehr anwenden lässt.

Werden mehr als ein Alphabet zum Verschlüsseln eingesetzt, zwischen denen gewechselt wird, so wird nicht immer ein Buchstabe nur durch einen anderen substituiert, ermittelt man z.B. den Buchstaben a in einem Text als den häufigsten, so kann dieser im Klartext viele verschiedene Buchstaben repräsentieren.

Auch Polyalphabetische Verschlüsselungen wurden schon geknackt, z. B. die Vigenére-Verschlüsselung.

1) Beschreibe, wie sich bei kleiner Schlüssellänge eine Vigenére-Verschlüsselung knacken lässt.

Bestimmte Textfolgen tauchen häufig auf, es könnte sein, dass sise dasselbe bedeuten. Nun zählt man den Abstand zwischen diesen Folgen und ermittelt alle Teiler. In einer Übersicht wird wahrscheinlich, um welche Schlüssellänge es sich handelt. Ist diese bekannt, so lässt sich die Häufigkeitsanlayse für jedes Teilalphabet durchführen.

2) Eine Lösungsmöglichkeit des Problems in Teilaufgabe 1) könnte die Verwendung von sehr langen Schlüsseln sein, also z.B. die Verwendung von Schlüsseln, die so lange sich wie der Text selbst. Auch sehr lange Schlüssel wurden schon geknackt, indem man vermutet, dass der lange Schlüssel bestimmte Schlüsselwörter enthält. Beschreibe diese Art der Entschlüsselung!
Ist der Schlüssel sehr lang, so kann man vermuten, dass ein bestimmtes Wort im Klartext vorhanden ist, z.B. das Wort „die". Nun prüfe man an allen Stellen des Klartextes, ob hier durch Einsetzen der Teil des Schlüssels einen Sinn ergibt. Aus Teilen eines Worten z.B. ypt könnte man das Wort Agypten testen. usw.

3) Beschreibe ausgehend der Teilaufgabe 1) und 2), wie eine Vigenére-Verschlüsselung beschaffen sein muss, dass sie relativ sicher ist.
man benötigt lange aber zufällige Schlüssel...

4) Verschlüssele die Botschaft „Dieser Code ist nicht zu knacken" mit Hilfe einer Caesar-Verschiebung. Verwende einen beliebigen Schlüssel ungleich 0 und 26.
... siehe Internet
http://www.manuel-friedrich.net/ab/2Inf1/caesar.php

5) Verschlüssele die Botschaft „Dieser Code ist nicht zu knacken" mit Hilfe einer Vigenere-Verschlüsselung und den Schlüsselwort „info".
http://www.manuel-friedrich.net/ab/2Inf1/vigenere_quadrat.php
LVJGMEHCLRNGBANQPGEISAFQSRS

6) Wie lautet die Auguste Kerckhoffs Ratschlag, wie man ein Verschlüsselungssystem sicher gestaltet?
Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.