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 gibt die Möglichkeit über einen Index oder über einen Iterator eine Sammlung zu durchlaufen. 2.
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)

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.

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?

7) Was versteht man unter einer Schnittstelle?

Einführung

Beschreibe den Unterschied zwischen Steganographie und Kryptographie anhand eines Beispiels.

Beschreibe den Unterschied zwischen Transposition und Substitution anhand eines Beispiels.

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

1) Beschreibe was man darunter versteht.

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

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

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

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

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!

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

4) Verschlüssele die Botschaft „Dieser Code ist nicht zu knacken“ mit Hilfe einer Caesar-Verschiebung. Verwende einen beliebigen Schlüssel ungleich 0 und 26.

5) Verschlüssele die Botschaft „Dieser Code ist nicht zu knacken“ mit Hilfe einer Vigenere-Verschlüsselung und den Schlüsselwort „info“.

6) Wie lautet die Auguste Kerckhoffs Ratschlag, wie man ein Verschlüsselungssystem sicher gestaltet?