K2Info2	Klausur (12.5.2015)	Raum 0x04

1. Aufgabe **(6 Punkte)**

Der folgende LaTeX-Code wurde mit dem Editor *Kile* erstellt:

```
\documentclass[11pt]{article}

\usepackage{graphicx}

\begin{document}

 \begin{picture}(100,100)
  \put(10,70) {\line (1,0) {100}}
  \put(0,0) {\vector (1,1) {100}}
 \end{picture}

\end{document}
```

a) Erläutere anhand des Codes den grundlegenden Aufbau einer LaTeX-Datei.
b) Erläutere, was der oben gezeigte Code für eine Ausgabe erzeugt, wenn man ihn kompiliert.
c) Vergleiche LaTeX mit gewöhnlicher Textverarbeitungssoftware wie Microsoft Word.

2. Aufgabe **(12 Punkte)**

RSA-Verschlüsselung oder „Ich weiß etwas, was du nicht weißt...“

a) Erläutere den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungen. Gib je ein Beispiel.
b) Erkläre die beiden Begriffe „private key“ und „public key“.
c) Erläutere die Bedeutung von Einwegfunktionen für das RSA-Verfahren. Gib ein (Alltags-)Beispiel für eine Einwegfunktion an.

Seien p und q zwei Primzahlen und N=pq. Die Zahlen e (encipher) und d (decipher) seien sinnvoll gewählt. Sei M der Klartext und C der verschlüsselte Text.

d) Wie schafft man es, einen Klartext in eine Zahl M zu überführen?

e) Darf M > N sein? Begründe deine Antwort kurz.

f) Erläutere, wie man folgende Schritte aus den obigen Zahlen üblicherweise bildet:
- Schlüsselerzeugung (private und public key)
- Verschlüsseln
- Entschlüsseln

g) Notiere ein Programm in Pseudocode, welches in der Lage ist, für eine Zahl N, die ein Produkt zweier Primzahlen p und q ist, die beiden Faktoren p und q zu bestimmen.

3. Aufgabe **(6 Punkte)**

Im Parkhaus am Darmstädter Hof wird ein neuer Ticketautomat aufgestellt. Du bist für dessen Programmierung zuständig.

a) Gib die nötigen Methoden an, die ein solcher Ticketautomat besitzen sollte, um für seinen Zweck funktionsfähig zu sein. Du kannst diese jeweils in Stichworten erläutern.

Nachdem du den Ticketautomaten in ein Java-Programm umgesetzt hast, sollst du dem zuständigen Projektleiter den Aufbau eines Java-Programmes erläutern. Im Zuge dessen musst du ihm die folgenden Begriffe näher bringen:

- **Zusatz: Datenfeld (+1 Punkt)**
- Konstruktor
- Zuweisung
- Sondierende / verändernde Methode
- Lokale Variable

b) Erläutere obige Begriffe anhand des folgenden Codes:

```
public class Ticketautomat
{
   private int preis;                  private int bisherGezahlt;                  private int gesamtsumme;

   public Ticketautomat(int ticketpreis)
   {     preis = ticketpreis;              bisherGezahlt = 0;                        gesamtsumme = 0;              }

   public int gibPreis()
   {     return preis;                                                                                             }

   public int gibBisherGezahltenBetrag()
   {     return bisherGezahlt;                                                                                     }

   public void geldEinwerfen(int betrag)
   {     if (betrag > 0)   {     bisherGezahlt = bisherGezahlt + betrag;                                         }
         else              {     System.out.println("Bitte nur positive Beträge verwenden: " + betrag);         }
   }

   public void ticketDrucken()
   {
      if (bisherGezahlt >= preis)
         {     System.out.println("####################");     System.out.println("# Die BlueJ-Linie");
               System.out.println("# Ticket");                 System.out.println("# " + preis + " Cent.");
               System.out.println("####################");     System.out.println();                              }
      else {     System.out.println("Sie müssen noch mindestens " + (preis - bisherGezahlt) + " Cent einwerfen."); }
   }

   public int wechselgeldAuszahlen()
   {     int wechselgeld;     wechselgeld = bisherGezahlt;     bisherGezahlt = 0;     return wechselgeld;     }
}
```

Zusatzaufgabe **(+2 Punkte)**

Erläutere, was im sogenannten „Hackerparagraphen“ festgeschrieben ist und welche Probleme dies für Informatiker mit sich bringt.