Beruf:

- Fachinformatiker/-in Anwendungsentwicklung

**FA 228** 

Lösungsvorschläge:

Lösungsvorschläge sind in der Regel Vorschläge der einreichenden Schulen; sie sind im Wortlaut nicht bindend.
Anderslautende, aber zutreffende Antworten sind ebenfalls als richtig zu werten.

Nur für die Hand des Prüfers! Faktor

## Aufgabe 1 Softwareentwicklung

2

```
abstract class SymmetrischeCodierverfahren
{
        protected string klarText;
        protected string privateKey;
        public SymmetrischeCodierverfahren()
            klarText = "DIESISTEINEBOTSCHAFT";
            privateKey = "GEHEIM";
        }
        public void setPrivateKey(string key)
            privateKey = key;
        }
        public string getKlarText()
            return klarText;
        }
        public void setKlarText(string klarText)
            this.klarText = klarText;
        public abstract string codieren();
}
class Vigenere : SymmetrischeCodierverfahren
        public override string codieren()
            string geheim = "";
            int k = 0;
            char zeichen = 'A';
            for (int i = 0; i < klarText.Length; i++)
                zeichen = klarText[i];
                geheim += (char)((zeichen + privateKey[k] - 2 * 'A') % 26 + 'A');
                k = k % (base.privateKey.Length);
            return geheim;
        }
}
```

```
1.2
      class Program
              static void Main(string[] args)
              {
                  Vigenere crypto = new Vigenere();
                   crypto.setPrivateKey("PRUEFUNG");
                   string klartext = "DERADLERISTGELANDET";
                   crypto.setKlarText(klartext);
                   string codierterText = crypto.codieren();
                   Console.WriteLine("Klartext: {0}", klartext);
                   Console.WriteLine("verschlüsselt: {0}", codierterText);
                   Console.ReadKey();
              }
      }
```

## Aufgabe 2 IT-Systemtechnik

1

2.1.1 Asymmetrische Verschlüsselungsverfahren arbeiten mit zwei Schlüsseln, einem öffentlichen Schlüssel (Public Key) und dem privaten Schlüssel (Private Key).

Person A verschlüsselt mit dem Public Key von Person B.

Diese verschlüsselte Nachricht kann nun nur mit dem privaten Schlüssel (Private Key) von Person B entschlüsselt werden.

Person B ist Besitzer des Schlüsselpaares.

Person A verschlüsselt mit seinem privaten Schlüssel (Private Key). 2.1.2

Person B entschlüsselt die digitale Nachricht mit dem öffentlichen Schlüssel (Public Key) von Person A. Dadurch wird sichergestellt, dass die Nachricht von Person A ist.

2.1.3

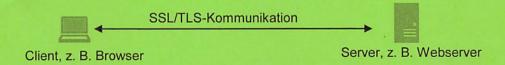
Keine riskante Schlüsselübergabe, bei vielen Kommunikationspartnern sind deutlich weniger Schlüssel in Umlauf.

## Nachteil:

Um die gleiche Berechnungssicherheit zu erreichen, ist gegenüber symmetrischer Verschlüsselung eine deutlich größere Schlüssellänge erforderlich, somit ist die Ver- und Entschlüsselung auch deutlich rechenaufwändiger.

Datenträger werden aufgrund des Rechen- bzw. Zeitaufwandes meist symmetrisch verschlüsselt.

Typische SSL/TLS Verbindung, am Beispiel eines Users, der mit seinem Browser eine Webseite auf ei-2.1.4 nem Webserver aufruft.



- 1. Browser verbindet sich mit dem Webserver (https://www...) und fordert diesen auf sich zu identifizie-
- 2. Webserver sendet zusammen mit dem Public Key sein SSL-Zertifikat an den Browser.
- 3. Browser prüft Gültigkeit des Zertifikates und generiert einen Session Key. Der Session Key wird mit dem Public Key des Webservers asymmetrisch verschlüsselt und an den Webserver zurückgeschickt.
- 4. Webserver entschlüsselt den Session Key asymmetrisch mit seinem Private Key und bestätigt dies dem Browser um die verschlüsselte Verbindung zu starten.
- Browser und Webserver verschlüsseln und entschlüsseln nun alle Daten über den Session Key mit symmetrischen Verschlüsselungsverfahren.

Bei hybriden Verschlüsselungsverfahren erfolgt der Schlüsselaustausch mit asymmetrischen- und der Datenaustausch mit symmetrischen-Verschlüsselungsverfahren.

- 2.2.1 Global Unicast: Weltweit gültig, in allen Netzen routebar Link Local: Nur lokal (LAN) gültig, nicht routebar
- 2.2.2 2001:1:2ac5::87c:0:a0 → 2001:0001:2ac5:0000:0000:087c:0000:00a0

Aufgabe 3 BWL 1

- 3.1 A-Kunden sind Kunden, die bezogen auf den Gesamtumsatz einen hohen prozentualen Umsatzanteil aufweisen.
   C-Kunden sind Kunden, mit denen ein geringer prozentualer Umsatzanteil erzielt wird.
- 3.2 Siehe Datei Aufgabe\_3\_Lösung.xls
- 3.3 Siehe Datei Aufgabe\_3\_Lösung.xls
- 3.4 Behandlung von A-Kunden:

Eigener fester Ansprechpartner/Kundenbetreuer
Bessere Konditionen (Rabatte, Skonti, Boni, ...)
Bessere Preise
Bevorzugung bei der Terminvergabe, schnelle Auftragsabwicklung
Gezielte Werbemaßnahmen und Informationen über neue Produkte, Sonderangebote usw.
Aufmerksamkeiten wie Werbegeschenke
Erhöhung der Kundenkontakte