Fachinformatiker/-in FA 228

Anwendungsentwicklung

Ganzheitliche Aufgabe I

Bearbeitungszeit: 90 Minuten

Verlangt:	Alle Aufgaben

Hilfsmittel: Nicht programmierter Taschenrechner,
PC mit entsprechender Softwareausstattung:
Office-Paket, Programm zur grafischen Darstellung von Prozessen,
Programmentwicklungsumgebung, Internet-Browser, Reader für PDF-Files,
HTML-Nachschlagewerk in digitaler Form und textbasierter HTML-Editor

Bewertung: Die Bewertung der einzelnen Aufgaben ist durch Faktoren näher vorgegeben.

Zu beachten: Die Prüfungsunterlagen sind vor Arbeitsbeginn auf Vollständigkeit zu überprüfen.

Der Aufgabensatz zur Ganzheitlichen Aufgabe I besteht aus:

- den Aufgaben 1 bis 3
- der Anlage 1: Prinzip symmetrischer Verschlüsselungsverfahren zu Aufgabe 1
- der Anlage 2: Prinzip der Vigenère-Codierung zu Aufgabe 1.1
- der Datei: „Kundenumsätze.xls“ zu Aufgabe 3

Bei Unstimmigkeiten ist sofort die Aufsicht zu informieren.

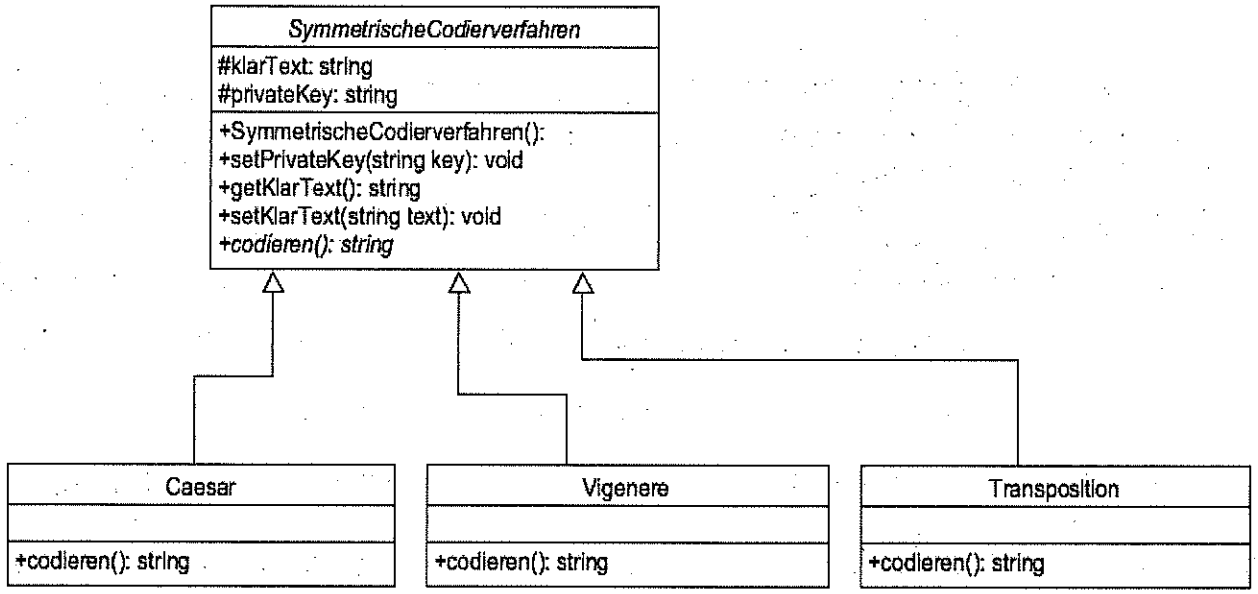
Klare und übersichtliche Darstellung der Rechengänge mit Formeln und Einheiten wird entscheidend mitbewertet.

Projektbeschreibung

Das Softwarehaus SecurelTy ist auf den Bereich Sicherheitssoftware spezialisiert.
Das örtliche Jugendforschungszentrum möchte für interessierte Schüler einen Aktionstag zum Thema Verschlüsselung anbieten und fragt die Firma SecurelTy diesbezüglich an.
Sie werden als Auszubildender mit der Durchführung des Aktionstages beauftragt.

Aufgabe 1 Softwareentwicklung (Anlage 1 und Anlage 2) 2

Sie haben entschieden, ein objektorientiertes Programm zur Vigenère-Verschlüsselung zu realisieren, welches zu den symmetrischen Verschlüsselungsverfahren zählt (siehe Anlage 1).
Ein Kollege hat bereits folgendes UML-Klassendiagramm für Sie entworfen:



1.1 Implementieren Sie lediglich die Klassen „SymmetrischeCodierverfahren“ und „Vigenère“, sowie die Methoden der beiden Klassen gemäß obigem UML-Klassendiagramm.
Verwenden Sie, die an Ihrer Schule unterrichtete Programmiersprache.

Das Prinzip der Vigenère-Codierung, welches Sie in der Methode **codieren()** implementieren sollen, wird in Anlage 2 erklärt.

Hinweis: Sie können davon ausgehen, dass im Klartext nur Großbuchstaben, keine Umlaute, keine Sonderzeichen und keine Leerzeichen enthalten sind.

1.2 Schreiben Sie ein Hauptprogramm, mit dem Sie die Klasse „Vigenère“ mit folgenden Daten prüfen können.

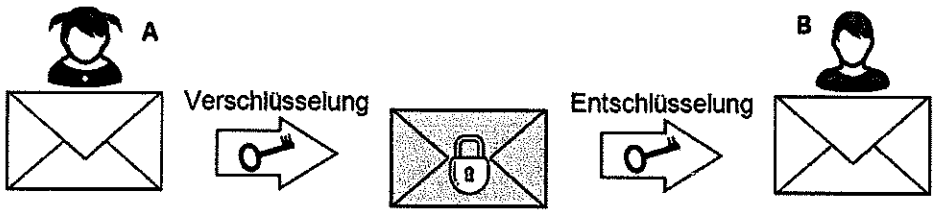
klarText: “DERADLERISTGELANDET“
privateKey: “PRUEFUNG“

Zur Überprüfung: der codierte Text lautet: “SVLEIFRXXJNKJFNTSVN“

Aufgabe 2 IT-Systemtechnik 1

2.1 Ihr Auftraggeber bittet Sie um eine Erklärung verschiedener Verschlüsselungsverfahren.

2.1.1 Person A möchte an Person B eine verschlüsselte Nachricht versenden.
Erklären Sie den Ablauf der asymmetrischen Verschlüsselung. Gehen Sie dabei auch auf die verwendeten Schlüssel ein.



2.1.2 Erklären Sie, wie das asymmetrische Verfahren zur Signatur von digitalen Inhalten eingesetzt werden kann.

2.1.3 Nennen Sie je einen Vor- und Nachteil der asymmetrischen gegenüber der symmetrischen Verschlüsselung und begründen Sie, welches Verfahren für die Verschlüsselung eines umfangreichen Datenträgers besser geeignet ist.

2.1.4 Beim SSL- bzw. TLS-Protokoll werden symmetrische und asymmetrische Verschlüsselungsverfahren miteinander kombiniert.
Erklären Sie das SSL/TLS-Verfahren mit Hilfe der Begriffe „Public Key", „Private Key" und „Session Key".

2.2 Sie erhalten den Auftrag, die Software OPENVPN auf zwei Rechnern zu installieren.
Bei der Konfiguration eines der Netzwerkinterfaces erhalten Sie folgende Ausgabe:

```
Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix:
   IPv6-Adresse. . . . . . . . . . . . : 2001:1:2ac5::87c:0:a0
   Verbindungslokale IPv6-Adresse  . . : fe80::106d:f7:355:1ce5
   Standardgateway . . . . . . . . . . : fe80::1
```

2.2.1 Geben Sie den Scope (Geltungsbereich) und die Routebarkeit der beiden Adresstypen "Global Unicast" (2001:xyz) und "Link Local" (fe80:xyz) an.

2.2.2 Wie lautet die Global Unicast-Adresse des Netzwerkinterfaces in ungekürzter Schreibweise?

Aufgabe 3 BWL (Datei: Kundenumsätze.xls) 1

Sie werden beauftragt eine ABC-Analyse zur Kundeneinteilung nach Umsätzen durchzuführen. Dazu stehen Ihnen die Daten der Datei „Kundenumsätze.xls" zur Verfügung.

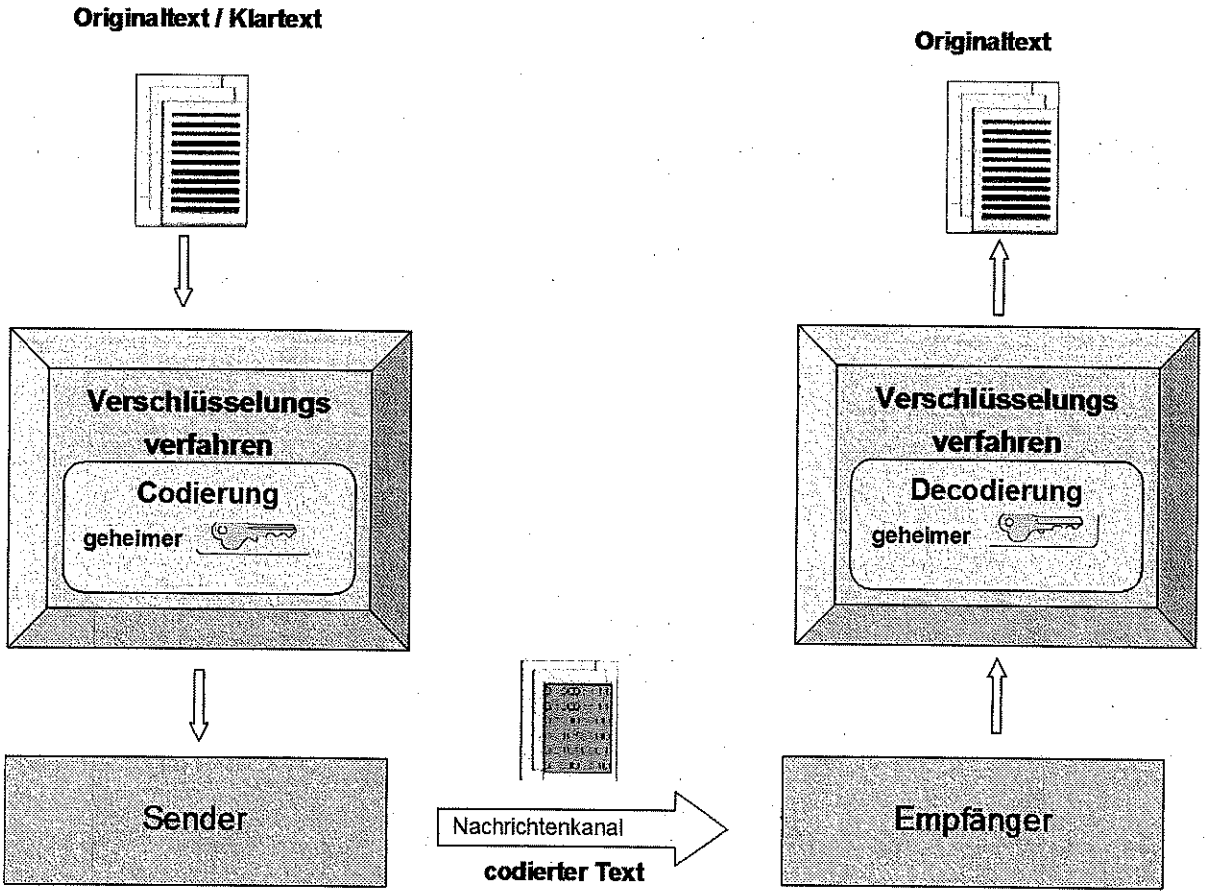
3.1 Erklären Sie den grundsätzlichen Unterschied zwischen A-Kunden und C-Kunden.

3.2 Führen Sie mithilfe der Datei „Kundenumsätze.xls" und den dort angeführten Einteilungskriterien eine ABC-Analyse durch. Verwenden Sie dazu kopierfähige Formeln und beachten Sie, dass die Vergabe der einzelnen ABC-Klassen automatisiert erfolgen soll.

3.3 Ermitteln Sie mithilfe einer geeigneten Formel im Tabellenblatt „Diagramm" die Gesamtumsätze der einzelnen ABC-Klassen und stellen Sie Ihr Ergebnis in einem aussagekräftigen Diagramm dar.

3.4 Machen Sie vier unterschiedliche Vorschläge für den Umgang mit A-Kunden im Vergleich zu C-Kunden.

Abschlussprüfung Winter 2018/19 von Berufsschule und Wirtschaft (gewerblicher Bereich) in Baden-Württemberg	FA 228
Ganzheitliche Aufgabe I	Fachinformatiker/-in *Anwendungsentwicklung*
Anlage 1: zu Aufgabe 1, Prinzip symmetrischer Verschlüsselungsverfahren	



Abschlussprüfung Winter 2018/19 von Berufsschule und Wirtschaft (gewerblicher Bereich) in Baden-Württemberg	FA 228
Ganzheitliche Aufgabe I	**Fachinformatiker/-in** *Anwendungsentwicklung*
Anlage 2: zu Aufgabe 1.1, Prinzip der Vigenère-Codierung	

Zum Verschlüsseln benötigt sowohl der Sender als auch der Empfänger einen gemeinsamen privaten Schlüssel.
Der Klartext sowie der private Schlüssel wird ohne Leerzeichen, Umlaute, bzw. Sonderzeichen als Großbuchstaben angegeben:
Ist die Zeichenlänge des Schlüssels kleiner als die Zeichenlänge des Klartextes, wird der Schlüssel solange wiederholt bis die Schlüssellänge gleich der Länge des Klartextes ist (siehe unteres Beispiel).

Zeile 1: Klartext: DIESISTEINEBOTSCHAFT
Zeile 2: Schlüssel: GEHEIM

D	I	E	S	I	S	T	E	I	N	E	B	O	T	S	C	H	A	F	T
G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I	M	G	E

Nun wird jedem Buchstaben eine Zahl zugeordnet nach der folgenden Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Die Zahl 4 entspricht nach der obigen Tabelle dem Buchstaben E.

`A→0, B→1, C→2,.. Z→25` diese Werte erhält man einfach über den ASCII-Code der Großbuchstaben:
'A' - 'A' = 0; 'B' - 'A' = 1; 'C' - 'A' = 2; ... 'Z' - 'A' = 25;
Die Codierung erfolgt, indem die zugeordneten Werte der einzelnen Buchstaben die übereinander stehen **addiert** werden.

Für den Wert des `i-ten` Buchstabens des codierten Textes ergibt sich die folgende Berechnung:

```
codewert[i] = (klartextwert[i] + keywert[i]) mod 26
```

Die Modulooperation wird verwendet, weil zwei Buchstabenwerte den Wert von 25 überschreiten könnten und so außerhalb des Alphabetes lägen.

Beispiel:

Zeile 1: Klartext: DIESISTEINEBOTSCHAFT
Zeile 2: Schlüssel: GEHEIM
Zeile 3: Der sich ergebende chiffrierter Text

D	I	E	S	I	S	T	E	I	N	E	B	O	T	S	C	H	A	F	T
G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I	M	G	E
J	M	L	W	Q	E	Z	I	P	R	M	N	U	X	Z	G	P	M	L	X

Beispiel (grau markiert): 'S' + 'M' → 18 + 12 = 30 → 30 mod 26 = 4 (entspricht 'E')
`codewert[5] = (18 + 12) mod 26 → codewert[5] = 4.`