Di., 15.10.2013 Informatik Q2 M (Kr)

1. Klausur 13/I (Q2.1)

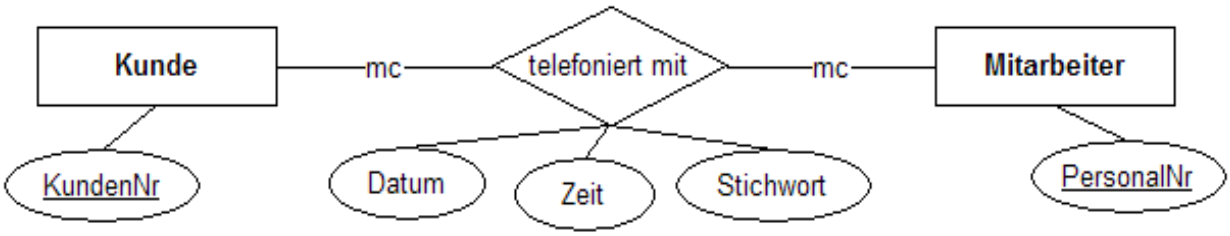
Dauer: 4·45 min (10:45 bis 13:45 Uhr) Name: ___www.r-krell.de_____

Hilfsmittel: einfacher Taschenrechner, Geodreieck

* *Achte auf sorgfältige Darstellung mit vollständigem, nachvollziehbarem Lösungsweg!* *
* *Kommentiere deine Programme!* *

1 Die Firma XYZ stellt Süßwaren her und verkauft sie.

a) Gelegentlich gibt es Telefonate zwischen Kunden und Mitarbeitern der Firma XYZ. Viele Kunden rufen nie an, andere öfter. Anrufe werden nur von den sieben Mitarbeitern der Kundendienstabteilung angenommen, nicht von Mitarbeiteren anderer Abteilungen. Bei jedem Telefonat werden neben den Beteiligten auch Datum und Zeit sowie in einem Stichwort der Grund des Anrufs (z.B. „Reklamation“, „Lob“,..) in der Datenbank erfasst. Dazu ist das ER-Diagramm gegeben:



a1) Erläutere die Multiplizitäten der Beziehung „telefoniert mit“.

a2) Erläutere kurz, warum (in der 2.NF) eine zusätzliche Tabelle Telefonat (oder auch Kunde_Mit-arbeiter) für die „telefoniert mit“-Beziehung nötig ist und notiere für die Telefonat-Tabelle alle Spaltenüberschriften mit Typen und markiere Primär- und ↑Fremdschlüssel.

a3) Jeder Mitarbeiter gehört zu einer Abteilung (oben nicht eingezeichnet). Erkläre, wie und warum die Beziehung zwischen Mitarbeiter und Abteilung ohne Zusatztabelle realisiert werden kann.

b) Auch für die Warenherstellung bzw. Warenbeschaffung der Firma XYZ soll eine Datenbank erstellt werden. Dabei wird von folgenden Sachverhalten ausgegangen:

> Alle Waren bestehen aus Rohstoffen. Eine Ware kann aus mehreren Rohstoffen bestehen, ein Rohstoff kann in mehreren Waren vorhanden sein. Die Datenbank soll speichern können, welcher Rohstoff in welcher Ware mit welchem Gewicht enthalten ist.
>
> Ein Rohstoff kann von mehreren Lieferern (=Lieferanten) geliefert werden. Selbstverständlich kann ein Lieferer mehrere verschiedene Rohstoffe liefern. Einige Rohstoffe werden von XYZ selbst erzeugt und werden daher nicht von einem fremden Lieferer bezogen. Die Datenbank soll speichern können, welcher Lieferer welchen Rohstoff zu welchem Preis je Kilogramm liefern kann.
>
> Alle Waren gehören jeweils einer Warengruppe mit einer Warengruppennummer an.
>
> Alle Waren sind verpackt. Es gibt Waren mit gleicher Verpackung. Für jede Verpackung wird die Verpackungsnummer erfasst.

Zeichne zu den eingerahmten Informationen das ER-Diagramm und beschrifte die Relationen in mc-Notation. Nur die im Text ausdrücklich genannten Attribute sind aufzuführen.

c) Auch für die Belieferung ihrer Kunden verwendet die Firma XYZ eine Datenbank. U.a. gibt es die folgenden 4 Tabellen (Primärschlüssel sind unterstrichen und Fremdschlüsseln ist ein ↑ vorangestellt):

Ware
<u>BestellNr</u> Bezeichnung Gewicht Verkaufspreis ↑WarengruppenNr ↑VerpackungsNr

Kunde
<u>KundenNr</u> Nachname Vorname Straße PLZ Ort eMail

Lieferschein
<u>LieferscheinNr</u> ↑KundenNr Bestelldatum Lieferdatum

Lieferposition
<u>↑LieferscheinNr</u> <u>↑BestellNr</u> Menge

c1) Erkläre kurz allgemein die Aufgaben von Primär- und Fremdschlüsseln.
c2) Begründe kurz: Neben den 4 genannten muss es mindestens 2 (!) weitere Tabellen geben.
c3) Notiere jeweils den SQL-Befehl
  (1) zum Erstellen der Tabelle Lieferposition (mit Schlüsseln; für Typen siehe c3)(2))
  (2) zum Füllen der Tabelle Lieferposition mit dem Datensatz (436, 80910, 4), wobei du davon ausgehen darfst, dass es in der Lieferschein-Tabelle bereits einen Lieferschein mit der LieferscheinNr 436 gibt und dass 80910 eine gültige Bestellnummer aus der Warentabelle ist.
c4) Notiere nun die SQL-Select-Befehle für folgende Abfragen. Gesucht sind:
  (1) Kundennummer und eMail-Adresse aller Kunden mit Postleitzahl 40227
  (2) Bestellnummer und Bezeichnung aller Waren, deren Bezeichnung mit „Schoko...“ anfängt
  (3) Bestellnummer und Bezeichnung aller Waren mit einem Gewicht zwischen 100 und 500 Gramm
  (4) der Sortimentsumfang, d.h. die Anzahl aller Waren, die XYZ anbietet.
  (5) Bezeichnung und Verkaufspreis des/der teuersten Artikel(s). Nenne zunächst eine einfache Abfrage, die reicht, wenn es nur einen teuersten Artikel gibt. Notiere dann, wie man eine Liste aller passenden Artikel-Bezeichnungen erhalten kann, wenn es mehrere verschiedene Artikel gibt, die alle den gleichen höchsten Preis haben.
  (6) Name und Kundennummer aller Kunden, die am 14.10.2013 bestellt haben. Nenne sowohl eine geschachtelte *select*-Anweisung als auch eine *select*-Anweisung mit Join (egal, ob letzterer durch Komma oder mit dem Schlüsselwort *inner join* bewerkstelligt wird).
  (7) Name und Kundennummer aller Kunden, die von irgendeiner Ware auf einmal (=in einer Lieferposition) mehr als 10 Exemplare geliefert bekommen haben.

(2) Kryptologie I

a) Bei der Steganografie werden zu übermittelnde Textnachrichten z.B. in einem Bild oder in einer Musikdatei so versteckt, dass sich Bild oder Musik noch im Grafik-Programm bzw. im mp3-Player öffnen und ansehen/abspielen lassen. Nenne 2 Vor- und 2 Nachteile der Steganografie gegenüber dem erkennbaren Versenden verschlüsselter Nachrichten!

b) Bei der Skytale wird der Nachrichtentext auf ein um einen Stab gewickeltes Papierband geschrieben. Passen 3 Buchstaben auf den Umfang des Stabes, so wird der Klartext „Informatikarbeit“ zum Geheimtext „Iarntbfieokiratm“.

b1) Verschlüssele ebenso (mit dem gleichen Stab vom Umfang=3, aber möglichst wenig Windungen/kurzem Papierband) von Hand die beiden Klartexte „Alles gelernt“ und „Erfolgreiches Entschlüsseln“.
b2) Entschlüssele von Hand den Geheimtext „Ashl elgieem“ mit dem gleichen Stab.
b3) Ein abgefangener Geheimtext lautet „Tsstah n dii‘b!“. Versuche ihn systematisch zu entschlüsseln, indem du nacheinander von Hand Stäbe von 2, 3, 4 und 5 Buchstaben Umfang

verwendest/simulierst und jeweils den erhaltenen Klartext notierst. Welcher Umfang liefert am ehesten eine Lösung?

b4) Stelle Überlegungen zur Sicherheit des Verfahrens an. Kann die Sicherheit erhöht werden oder wird sie verschlechtert, wenn man zum Übermitteln etwa einer Nachricht aus 25 Zeichen einen möglichst dünnen (Umfang=1) oder einen möglichst dicken Stab (Umfang > 20) verwendet oder wenn man ein längeres Papierband nimmt (z.B. für 40 oder 120 Zeichen) und das 10-mal bzw. 30-mal um einen Stab vom Umfang=4 wickelt?

c) Der rechte Teil des Bildes zu b) legt nahe, für die Programmierung der Skytale in Java eine zweidimensionale Reihung (2-dim. Array) zu verwenden (siehe Kasten).

c1) Erläutere den Programmtext, in dem du auf die Berechnung der *windungszahl*, die Bedeutung der *tabelle*, den Sinn der beiden Doppelschleifen und den Sinn des ‚#'-Zeichens eingehst, das auch in der zweiten Doppelschleife wieder auftaucht!

c2) Schreibe eine passende Methode *entschlüssele* (der der Geheimtext und der Umfang übergeben werden) in Java oder als Struktogramm!

```
public String verschlüssele (String klartext, int umfang)
{                                                    // zu Aufgabe 2c)
 int windungszahl = (klartext.length()+umfang-1)/umfang;
 char[][] tabelle = new char[windungszahl][umfang];
 int pos = 0;
 for (int y = 0; y < umfang; y++) // Doppelschleife 1
 {
  for (int x = 0; x < windungszahl; x++)
  {
   if (x*umfang + y < klartext.length() )
   {
    tabelle[x][y]=klartext.charAt(pos);
    pos++;
   }
   else
   {
    tabelle[x][y]='#';  // Füllen mit '#'-Zeichen
   }
  }
 }
 String geheimtext = "";
 for (int x = 0; x < windungszahl; x++)  // Doppelschleife 2
 {
  for (int y = 0; y < umfang; y++)
  {
   if (tabelle[x][y]!='#')
   {
    geheimtext = geheimtext + tabelle[x][y];
   }
  }
 }
 return (geheimtext);
}
```

3 Kryptologie II

Zweidimensionale Reihungen/Tabellen spielen auch bei folgendem anderen Verschlüsselungsverfahren eine Rolle: Ein 5x5-Quadrat enthält innen die Buchstaben des (Klartext-)Alphabets. Zum Verschlüsseln wird jeder Klartextbuchstabe durch zwei Buchstaben, nämlich die Randbeschriftung des Quadrats, ersetzt. Nennt man wie in Mathe die Rechtsachse zuerst, wird *a* durch *im*, *b* durch *nm*, *s* durch *fi* und *z* durch *rk* ersetzt. Ein *j* im Klartext wird wie *i* als *oa* verschlüsselt.
Beispiel: Der Klartext „okay" wird zum Geheimtext „otraimok".

	i	n	f	o	r
m	a	b	c	d	e
a	f	g	h	i	k
t	l	m	n	o	p
i	q	r	s	t	u
k	v	w	x	y	z

a) Ver- bzw. entschlüssele von Hand:

a1) Verschlüssele den Klartext „so geht es".

a2) Entschlüssele den Geheimtext „firirtrm raitimni".

b) Entwirf wahlweise ein Programm zum Ver- oder zum Entschlüsseln (in Java oder als Struktogramm). Du darfst voraussetzen, dass die Variable *char[][] zeichen = new char[6][6]* bereits in der 0. Zeile und 0. Spalte die Randbeschriftung und in den Zeilen und Spalten 1 bis 5 das Alphabet enthält, d.h. dass z.B. *zeichen[2][1] = 'b', zeichen[2][0]='n'* und *zeichen[0][1] ='m'* ist.

c) Ordne das Verfahren richtig ein (Steganografie/echte Verschlüsselung, Transposition/Substitution, Chiffre/Code, mono-/polyalphabetisch).

d) Beurteile die Sicherheit dieses Verfahrens.

4 Kryptologie III

Gegeben ist die Verschlüsselungstafel nach Vigenère.

a) Verschlüssele von Hand den Klartext MATHEMATIK mit dem Schlüsselwort HUND

b) Entschlüssele von Hand den Geheimtext ZHBKSNEGCVYN mit dem Schlüssel KATZE.

c) Ein anderer Geheimtext heißt „VMBKI RIFDI WRQZEBDX NMBDI - RIFULBF“. Prüfe in den vier folgenden Kästen, wie oft trotz Verschiebung gleiche Geheimbuchstaben übereinander stehen (Autokorrelation) und gib auf Grund der Werte eine begründete Vermutung für die Länge des Vigenère-Schlüsselworts ab! (Keine Entschlüsselung verlangt!)

Vigenère-Quadrat

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

+1	VCQKYD NQPN AMF YUFY TYUKJUWFLWCXW WVCQKYD NQPN AMF YUFY TYUKJUWFLWCX
+2	VCQKYD NQPN AMF YUFY TYUKJUWFLWCXW XWVCQKYD NQPN AMF YUFY TYUKJUWFLWC
+3	VCQKYD NQPN AMF YUFY TYUKJUWFLWCXW CXWVCQKYD NQPN AMF YUFY TYUKJUWFLW
+4	VCQKYD NQPN AMF YUFY TYUKJUWFLWCXW WCXWVCQKYD NQPN AMF YUFY TYUKJUWFL

d) Außer dem Autokorrelationsverfahren (wie in c)) gibt es den ursprünglichen Kasiski-Test („Kasiski-I“), bei dem mehrfach auftretende längere Buchstaben-Kombinationen im Geheimtext gesucht werden. Beschreibe diesen Ansatz mit der dahinter liegenden Vermutung und erläutere den Entschlüsselungs- bzw. Analyseversuch bis einschließlich der Anwendung der Häufigkeitsanalyse! (Angriffs-Verfahren beschreiben, nicht durchführen).

e) Erläutere den Begriff ‚One-Time-Pad‘ und stelle eine Beziehung zum Vigenère-Verfahren her. Beurteile auch hier die Sicherheit des Verfahrens.

5 Kryptologie IV

Bei den symmetrischen Verfahren müssen sich Sender und Empfänger nicht nur auf ein gemeinsames Verfahren einigen, sondern normalerweise auch den gleichen Schlüssel benutzen. Die sichere Weitergabe des Schlüssels ist nicht leicht.

Eine Abhilfe versucht Shamir's *no key algorithm* zu schaffen, wo beide Partner A (Alice) und B (Bob) jeweils nur mit ihrem eigenen Schlüssel ver- und entschlüsseln, ihren Schlüssel aber nie weitergeben.
Beschreibe das abgebildete Verfahren und erläutere notwendige Eigenschaften geeigneter Verschlüsselungsverfahren (nenne dabei auch ein geeignetes Verfahren). Beurteile die Sicherheit des Gesamtverfahrens.