Name: _____

Abiturprüfung 2009

Informatik, Leistungskurs

Aufgabenstellung:

Ein Jugendtreff möchte seine interne Verwaltung von einem Karteikartensystem auf ein computerbasiertes System umstellen und an alle angemeldeten Jugendlichen einen elektronisch lesbaren Mitgliedsausweis austeilen. Mit Hilfe dieses Ausweises können sich die Jugendlichen zu verschiedenen Arbeitsgemeinschaften (kurz „AGs“) anmelden. Die Anmeldung ist notwendig, um die Zuordnung zu den AGs (zum Beispiel bei begrenzter Teilnehmerzahl) planen zu können. Von jedem Jugendlichen werden der Name und die Adresse verwaltet, von jeder AG eine Bezeichnung, der Name des Betreuers sowie eine Höchstteilnehmerzahl. Jeder Mitgliedsausweis ist nur bis zum 31.12. eines bestimmten Jahres gültig.

Das neue Computersystem soll auf einem relationalen Datenbanksystem basieren.

a) Modellieren Sie das Datenbanksystem, indem sie die Entitäten und Beziehungen graphisch in einem Entity-Relationship-Diagramm darstellen, und bestimmen Sie dabei auch die Kardinalitäten. Begründen Sie Ihre Entscheidungen bezüglich der Kardinalitäten.

   Überführen Sie Ihr Modell in ein normalisiertes relationales Datenbankschema der 3. Normalform.

   Beschreiben Sie allgemein die Bedingungen für die erste, zweite und dritte Normalform.
   (22 Punkte)

b) Im Folgenden sind drei Abfragen dargestellt. Erläutern Sie Ihre Lösungsansätze jeweils zunächst umgangssprachlich und entwickeln Sie anschließend für Ihr Datenbankschema geeignete SQL-Anweisungen.

   1. Die Bezeichnungen aller angebotenen Aktivitäten zusammen mit deren Betreuern
   2. Die Ausweisnummer und das letzte Gültigkeitsjahr des Ausweises von „Peter Müller“
   3. Die Ausweisnummern aller Jugendlichen, die die AG „Handball“ aber nicht die AG „Tischtennis“ gewählt haben *(12 Punkte)*

Name: _____

c) In dieser Teilaufgabe wird auf das folgende relationale Datenbankschema Bezug genommen:

Aktivitäten (AktivitätNr, Bezeichnung)
bucht (AusweisNr, AktivitätNr)

Analysieren und erläutern Sie die folgende SQL-Anweisung.

```
1  SELECT Aktivitäten.Bezeichnung
2  FROM bucht INNER JOIN Aktivitäten ON bucht.AktivitätNr =
3       Aktivitäten.AktivitätNr
4  WHERE
5     (SELECT count(*) FROM bucht
6     WHERE bucht.AktivitätNr = Aktivitäten.AktivitätNr) >= 10
7  GROUP BY Aktivitäten.Bezeichnung;
```

(6 Punkte)

d) Zum Zwecke eines Datenabgleichs sollen die Daten des Jugendtreffs über das Internet an einen Sachbearbeiter der Stadtverwaltung übertragen werden. Aus Sicherheitsgründen werden die Daten vor der Übertragung mit dem Vigenère-Verfahren verschlüsselt. Zum Beispiel werden die Bezeichnungen der AGs ohne Trennungszeichen direkt hintereinandergeschrieben und dann mit einem Schlüsselwort verschlüsselt.

AG-Namen: `HANDBALLTISCHTENNIS`
Schlüsselwort: `SPORT`

Bestimmen Sie die Verschlüsselung des Textes mit Hilfe des Vigenère-Verfahrens (siehe Vigenère-Quadrat im Anhang). *(4 Punkte)*

e) Der Datenschutzbeauftragte merkt an, dass das Vigenère-Verfahren nicht in allen Fällen sicher ist, und schlägt vor, die Daten nach dem RSA-Verfahren zu verschlüsseln.

Nehmen Sie Stellung zu diesem Vorschlag, indem sie die Sicherheit beider Verfahren unter Bezugnahme auf die Verschlüsselungsalgorithmen miteinander vergleichen.

(6 Punkte)

Zugelassene Hilfsmittel:

- Wörterbuch zur deutschen Rechtschreibung
- Taschenrechner

Name: _____

Anlage

Das Vigenère-Quadrat:

Schlüssel-Zeichen \ Quelltext-Zeichen	**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**
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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