Aufgabe 1: Gesellschaftliche Grundlagen *(9 Punkte)*

a) Warum ist Datenschutz wichtig für die persönliche Handlungsfreiheit? *(3 Punkte)*

b) Welcher Zusammenhang besteht zwischen Demokratie und Datenschutz? *(3 Punkte)*

c) Warum steht heute beim Datenschutz der Schutz personenbezogener Daten im Vordergrund, und nicht mehr die Abgrenzung zwischen privater Sphäre und öffentlicher Sphäre? *(3 Punkte)*

Aufgabe 2: Anonymitätsmaße *(12 Punkte)*

Gegeben ist folgende Tabelle. A und B sind die Quasi-Identifier, S ist ein sensitives Attribut. Die beiden letzten Spalten gehören zu Aufgabenteil b.

A	**B**	**S**	angreifbar	nicht angreifbar
a	b	1	☐	☐
a	b	2	☐	☐
a	b	3	☐	☐
b	c	4	☐	☐
b	c	4	☐	☐
b	d	5	☐	☐
b	d	6	☐	☐
c	d	7	☐	☐
c	d	8	☐	☐
c	d	8	☐	☐

a) Welche k-Anonymität erfüllt die Tabelle? *(1 Punkt)*

☐ keine
☐ 1-Anonymität
☐ 2-Anonymität
☐ 3-Anonymität

b) Benennen Sie einen der in der Vorlesung vorgestellten Angriffe auf die k-Anonymität, mit dem sich die Privatheit einiger der in dieser Tabelle gespeicherten Personendaten aufheben lässt. Markieren Sie in in den mit " ☐ " vorgegebenen Feldern rechts neben der Tabelle alle Datensätze, die Sie mit diesem Verfahren angreifen können. *(4 Punkte)*

c) Geben Sie die *minimale Menge* von Dummy-Datensätze an, die Sie *mindestens* in die Tabelle einfügen müssen, damit diese 4-anonym wird. *(4 Punkte)*

d) Erfüllt eine Datenbank, die l-Divers ist, zugleich die t-Closeness-Eigenschaft? Begründen Sie Ihre Antwort. *(3 Punkte)*

Aufgabe 3: Datenschutz im Internet *(14 Punkte)*

a) **Wann** beim Webseitenabruf treten Web-Bugs in Aktion, und **wo** in der technischen Infrastruktur des Internets werden die Daten über den Anwender gespeichert, die durch den Einsatz von Web-Bugs entstehen? *(2 Punkte)*

b) Welche Informationen kann ein Webseitenbetreiber über den Anwender erhalten, wenn er Web-Bugs einsetzt? Nennen Sie nur Daten, die nicht beim normalen Webseitenabruf ohnehin anfallen. *(2 Punkte)*

c) Welche Datenschutzprobleme können dem Anwender durch den Einsatz von Web-Bugs entstehen? *(2 Punkte)*

d) Gegeben ist folgende Mix-Kaskade:

Der Sender möchte eine anonyme Nachricht an den Empfänger übermitteln. Wie sieht das Datenpaket aus, das der **Mix1** an **Mix2** schickt? Verwenden Sie dazu die passenden Symbole aus der folgenden Aufstellung. *(8 Punkte)*

Msg	Nachricht vom Sender an den Empfänger
A_S, A_1, A_2, A_3, A_E	Adresse von Sender, Mix1...3, Empfänger
S_S, S_1, S_2, S_3, S_E	symmetrischer Schlüssel von Sender, Mix1...3, Empfänger
K_S, K_1, K_2, K_3, K_E	öffentlicher Schlüssel von Sender, Mix1...3, Empfänger
P_S, P_1, P_2, P_3, P_E	privater Schlüssel von Sender, Mix1...3, Empfänger
R_0, R_1, $\cdots R_n$	statistisch unabhängige Zufallszahlen

Aufgabe 4: Lokationsbasierte Dienste *(11 Punkte)*

Beantworten Sie die folgenden Fragen zum Mix-Zones-Verfahren:

a) Welche Systemarchitektur nutzt das Mix-Zones-Verfahren? *(1 Punkt)*
- ☐ Anonymisierung auf zentralem Server
- ☐ dezentrale Anonymisierung durch Zusammenarbeit mehrerer Rechner
- ☐ lokales Verfahren zur Selbstanonymisierung auf dem Rechner eines Teilnehmers

b) Welche Informationen gibt das Mix-Zones-Verfahren aus, also welche Daten erhalten die Datenempfänger von den Teilnehmern in den Mix Zones? *(2 Punkte)*

c) Beschreiben Sie das Mix-Zones-Verfahren. Gehen Sie bei Ihrer Beschreibung darauf ein, welche Arten von Zonen es gibt, welche Bedeutung diese haben und was passiert, wenn ein Teilnehmer sie betritt oder verlässt. *(5 Punkte)*

d) Nennen Sie drei Situationen, in denen *das Verfahren* die Privatheit der Teilnehmer nicht schützen kann. *(3 Punkte)*

Aufgabe 5: Datenschutz in Datenbank-Szenarien *(14 Punkte)*

Im Folgenden geht es um das Verfahren "Fragmentation". Gegeben ist folgendes Beispiel:

Klartext-Tabelle db

Name	Datum	Arzt	Diagnose	Behandlung
Alice	2012	Dr. Brown	Schnupfen	Kamillentee
Bob	2013	Dr. Brown	Schnupfen	Fencheltee
Carol	2012	Dr. Red	Heiser	Kamillentee

Constraints

C_0	{Name}
C_1	{Arzt, Diagnose}
C_2	{Arzt, Behandlung}

Die Klartext-Datenbank *db* wurde gemäß der Constraints C_0 bis C_2 in zwei Fragmente überführt. Verschlüsselte Daten wurden mit "XXX" abgekürzt:

Fragment1

Salt	Enc	Datum	Arzt
115	XXX	2012	Dr. Brown
322	XXX	2013	Dr. Brown
502	XXX	2012	Dr. Red

Fragment2

Salt	Enc	Diagnose	Behandlung
742	XXX	Schnupfen	Kamillentee
193	XXX	Schnupfen	Fencheltee
121	XXX	Heiser	Kamillentee

a) Markieren Sie in der folgenden Liste die korrekten Aussagen. *(3 Punkte)*

wahr	*falsch*	*Aussage*
☐	☐	Beim Honest-but-Curious-Angreifermodell hat der Angreifer Zugriff auf alle Daten, die die Datenbank an den Nutzer schickt.
☐	☐	Für SUM-Anfragen muss immer ein ganzes Fragment zum Client übertragen und dort entschlüsselt werden.
☐	☐	Constraints sind wohldefiniert, wenn kein Constraint die Teilmenge eines anderen Constraints ist.

b) Schreiben Sie folgende Anfragen so um, dass sie der Dienstleister auf den Fragmenten ausführen kann. Geben Sie dabei an, wieviele Datensätze Ihre Anfrage an den Client übermittelt, die nicht zum Anfrageergebnis gehören. *(4 Punkte)*

```
1.) SELECT Diagnose FROM db WHERE Name = ‘‘Alice’’
    (Gib alle Diagnosen für Alice aus)

2.) SELECT count(*) FROM db WHERE Diagnose = ‘‘Schnupfen’’
    (Zähle, wie oft Schnupfen diagnostiziert wurde)

3.) SELECT * FROM db WHERE Diagnose = ‘‘Schnupfen’’
      MINUS SELECT * FROM db WHERE Name = ‘‘Bob’’
    (Suche alle Datensätze von Leuten mit Schnupfen, die nicht Bob sind.)

4.) SELECT Diagnose, count(Diagnose) FROM db GROUP BY Diagnose
    (Zähle, wie oft jede Diagnose gestellt wurde)
```

c) Geben Sie das *optimale* Set von Fragmenten an, das die an den Client übertragenen Daten für folgende Anfrage minimiert und die Constraints C_0 bis C_2 erfüllt: *(4 Punkte)*

```
SELECT Name FROM db WHERE Diagnose = ‘‘Schnupfen’’ AND Datum = 2012
```

d) Erläutern Sie, warum "Maximale Sichtbarkeit" ein wichtiger Bestandteil einer optimalen Fragmentierung ist. *(3 Punkte)*