1.a Section 1.12

Problem 4 (points: 7)
When someone steals the secret information such as password (a compromise of confidentiality) (for example Snooping, the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information.), then they can enter to our system with that password. After entering in our system, they can change any information in our system that leads to the incorrectness of information (a compromise in integrity) in our system. (Suronapee Phoomvuthisarn)

Problem 5 (points: 7)

Disclosure – confidentiality
Deception – integrity, availability
Disruption – integrity, availability
Usurpation – confidentiality, integrity, availability

Problem 9 (points: 7)
a. secure
b. precise
c. broad

Problem 11 (points: 7)
Laws protecting privacy of users might impact the ability of system administrators to monitor user activity by preventing them from reading certain private files without permission or prohibiting even tracking the behavior of the user. These examples show that monitoring a user can be restricted up to a certain point depending on the specific law. This restriction itself, however, can in turn restrict the ability of the administrator to provide system security, since he might be unable to track unauthorized behavior of users or detect intruders by monitoring the private files of users. (Dominik Pozny)

An old solution
Laws protecting privacy forbid the collection of some types of data. The goal of these laws is to prevent an organization, or individuals, from inferring information about individuals’ beliefs, behavior, or other personal characteristics from the data being transmitted. When monitoring user activity, privacy laws affect system administrators because they cannot observe certain data relating to user activity. For example, a user
may read private e-mail from her spouse. The contents of that e-mail, if protected by privacy laws, must be suppressed when the system administrator records network traffic. So the system administrators must devise a method to conceal or scramble the information (called sanitization). The problem becomes more complex when the information is relevant to a security analysis. For example, consider a sweep of a network looking for HTTP servers. That this is a sweep will be obvious when the IP addresses are correlated: every IP address on the network will have been probed. But the IP addresses may tie machine use to an individual user, so a law restricting the ability of the system administrator to tie actions to specific users may prevent the recording of the IP addresses. This would hinder the security analysis of the user activity, because some of those activities could not be recorded.

1.b Section 2.8

Problem 1 (Points: 6)

a) Set of rights is \{own, execute, write, read\}

<table>
<thead>
<tr>
<th></th>
<th>alicec</th>
<th>bобrс</th>
<th>cyndvrc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>own, execute</td>
<td>read</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>read</td>
<td>own, execute</td>
<td></td>
</tr>
<tr>
<td>Cyndy</td>
<td>read</td>
<td>read, write</td>
<td>own, read, write, execute</td>
</tr>
</tbody>
</table>

b) New access control matrix:

<table>
<thead>
<tr>
<th></th>
<th>alicec</th>
<th>bобrс</th>
<th>cyndvrc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>own, execute</td>
<td>read</td>
<td>read</td>
</tr>
<tr>
<td>Bob</td>
<td>own, execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyndy</td>
<td>read</td>
<td>read, write</td>
<td>own, read, write, execute</td>
</tr>
</tbody>
</table>

Problem 4

Set of rights is \{read, write, execute, append, list, modify, own\}

```
command delete_all_rights(p,q,s)
(a)
    delete read from a[q,s];
delete write from a[q,s];
delete execute from a[q,s];
delete append from a[q,s];
delete list from a[q,s];
delete modify from a[q,s];
delete own from a[q,s];
end

command delete_all_rights(p,q,s)
if modify in a[p,s]
then
    delete read from a[q,s];
delete write from a[q,s];
delete execute from a[q,s];
delete append from a[q,s];
delete list from a[q,s];
delete modify from a[q,s];
delete own from a[q,s];
end
```
2.1 Exercise 34.4

Problem 2b (Points: 5)
- p: have potato for dinner
- q: have rice for dinner

\((p \land \neg q) \lor (\neg p \land q)\)

Problem 2c (Points: 5)
- p: do all homework
- q: read text
- r: study lecture notes
- s: prepared for exam

\((p \land q \land r) \leftrightarrow s\) OR \((p \land q \land r) \rightarrow s\) \land \((s \rightarrow (p \land q \land r))\)

Problem 4b (Points: 5)
- C(x): x is child
- M(x, y): y is mother of x
- Y(x, y): x is younger than y

\[ \forall x, y \ [ C(x) \land M(x,y) \rightarrow Y(x, y) ] \]

Problem 4c (Points: 5)
- S(x): x is Sue
- M(x): x is Mary
- PGF(x, y): y is x’s parental grandfather

\[ \exists x, y, z \ [ S(x) \land M(y) \rightarrow PGF(x, z) \land PGF(y, z) ] \]

2.2 Prove by induction (Points: 10)
Base Case:
\( n=1: \ (n^3 + 2 \cdot n) = (1^3 + 2 \cdot 1) = 3 \)
\( 3 \mod 3 = 0 \)
Because 3 is divisible by 3 the base case holds.

Induction Hypothesis:
It is assumed that \( (n^3 + 2 \cdot n) \) is divisible by 3 and holds for all \( n \in \mathbb{N} \).

Induction Steps
\[
\left((n+1)^3 + 2 \cdot (n+1)\right) = (n+1)^3 (n+1)^2 + 2^3 (n+1) = (n+1)^3 \left((n+1)^2 + 2\right) = (n+1)^3 (n^2 + 2n + 3)
\]
\[
= n^3 + 2n + 3n + 3n^2 + 3 = n^3 + 2n + 3(n+n^2+1)
\]
The induction hypothesis holds. The first term \( n^3 + 2n \) has already been proved to be divisible by 3 in the base case. The term \( 3(n+n^2+1) \) is a multiple of 3 due to the multiplication of the term in the brackets with 3. Therefore it is divisible by 3 as well. Due to the fact that both terms \( n^3 + 2n \) and \( 3(n+n^2+1) \) are divisible by 3 you can use the distributive law and factor out 3. You get a term which is a multiple of 3 and therefore divisible by 3.

(Dominik Pozny)

3. **Exercise on Lattice**
(Dominik Pozny)

**Problem 1**

The relation \( \preceq \) forms a partial order as shown by the Hasse diagram:
Problem 2a

$S$ and $\leq$ form a lattice because all criteria for a lattice are met:

$\leq$ is reflexive since $a \leq a$ for all $a \in S$, e.g. $12 \leq 12$ since $1 \leq 1$ and $2 \leq 2$
$\leq$ is anti-symmetric since $a \leq b$ and $b \leq a$ imply $a = b$ for all $a, b \in S$ due to the partial order
$\leq$ is transitive since $a \leq b$ and $b \leq c$ imply $a \leq c$ for all $a, b, c \in S$ due to the partial order

Furthermore each two elements of $S$ have a common greatest lower bound and lowest upper bound.

Problem 2b

$S-\{21\}$ and $\leq$ form a lattice, since the properties of the relation stay the same (reflexive, anti-symmetric, transitive) and the boundary criterion is still met for $S-\{21\}$.

Problem 2c

$S-\{21, 22\}$ and $\leq$ form a lattice, since the properties of the relation stay the same (reflexive, anti-symmetric, transitive) and the boundary criterion is still met for $S-\{21, 22\}$.