Answer Sheet for Homework 1 (selected from submissions)
Course IS-2150/TEL-2810 Introduction to Computer Security [Fall 2006]

1 Section 1.11

Exercise 1 (points: 5)

a. confidentiality
b. availability
c. integrity
d. integrity
e. availability
f. availability & integrity
g. confidentiality & integrity

Exercise 4 (points: 5)
If you can get the username and password of someone’s email account, that would result in those compromises. You will be able to send messages to exchange data as if you are him.

(Farqad Moshili)

Problem 5 (points: 5)

Unauthorized access to information is *disclosure*. For instance, snooping which is the unauthorized interception of information, is a form of disclosure. Confidentiality services counter this threat.

Acceptance of false data is called *deception*. For instance, the man-in-the-middle attack is a kind of deception, where the receiver and sender do not realize that an intruder is reading the sent information and possibly sending false information to the receiver. Integrity services counter this threat.

Interruption or prevention of correct operation is called *disruption*. Denial of service is an instance of disruption. The attacker may prevent the server from providing service to the requesting client. Availability services take care of this threat.

Unauthorized control of some part of the system is called *usurpation*. Masquerading or pretending to be someone else to control a system is a kind of usurpation. Integrity services (called “authentication services”, in this context) counter this threat.

Therefore, three security services-confidentiality, integrity and availability- are sufficient to deal with the threats of disclosure, disruption, deception and usurpation.

(Vikrant Khenat)

Problem 7 (points: 5)

a. Prevention is more important than detection and recovery.

Example: Prevention of Virus Infection in a computer is more important than its detection and recovery. If a computer is already infected with a virus, it may corrupt and delete data, which may not be recoverable.

b. Detection is more important than prevention and recovery.

Example: Although prevention is always better than cure, Detection would be more important in cases when it is very hard to prevent a certain type of attack. This is true in Intrusion Detection Systems. For example, if a service is to be provided, there is always a threat of a Denial-of-Service attack. Such attacks should be detected first to prevent the unavailability of the service.

c. Recovery is more important than prevention and detection.

Example: In a hard disk crash, recovery of the users files and other information is more important. All Hard disks are probable to crash after some time, so it is hard to prevent such crashes, but a recovery plan should be put in force before hand by using RAID arrays and weekly backups.

(Summit Tuladhar)

Problem 9 (points: 5)

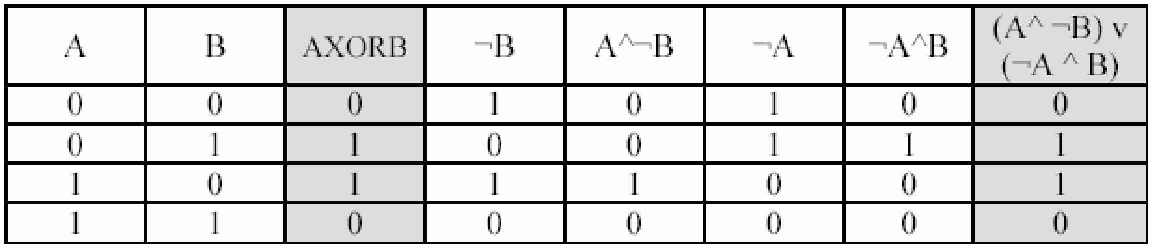
a. secure
b. precise
c. broad

Problem 15 (points: 5)

a. Security mechanism in a company depends on who is responsible for the company's security. The power to implement appropriate controls must reside with those who are responsible. If management determines what programs are to be on the system, then the system administrators who are responsible for the security, who see the need for security measures will be unable to implement the appropriate security measures. Since management is not aware of the technical aspects of security as much as system administrators it's possible for management to make some poor choices with regard to cost, resources, security measures. Also coordination among the system coordinators is also pivotal in an organization and this coordination might be compromised if management makes the key security decisions.

b. The problem can be fixed by providing system administrators (knowledgeable people) with more control and sufficient resources for administering computer systems. Management should consult the system administrators before making any decision on security issues. If the company has several divisions each should have separate system administrator then the company can have one security head who is knowledge about security issues and who heads all the systems administrators. Management should leave all the key security decisions to him. Security head should take care of delegating the appropriate security tasks to the concerned system administrators. Part of the management role requires them to know about the cost, resources, security polices etc, management can get up to date about these by consulting the security head.

2.a (Points: 10)



A	B	AXORB	¬B	A^¬B	¬A	¬A^B	(A^ ¬B) v (¬A ^ B)
0	0	0	1	0	1	0	0
0	1	1	0	0	1	1	1
1	0	1	1	1	0	0	1
1	1	0	0	0	0	0	0

(Yazeed Taiseer Hamid)

2.b (Points: 10)

(i) S=The sun shines
H=We can make hay

$S \rightarrow H$

(ii)
p: do all homewok
q: read text
r: study lecture notes
s: prepared for exam

$(p \wedge q \wedge r \rightarrow s)$

2.c (Points: 10)

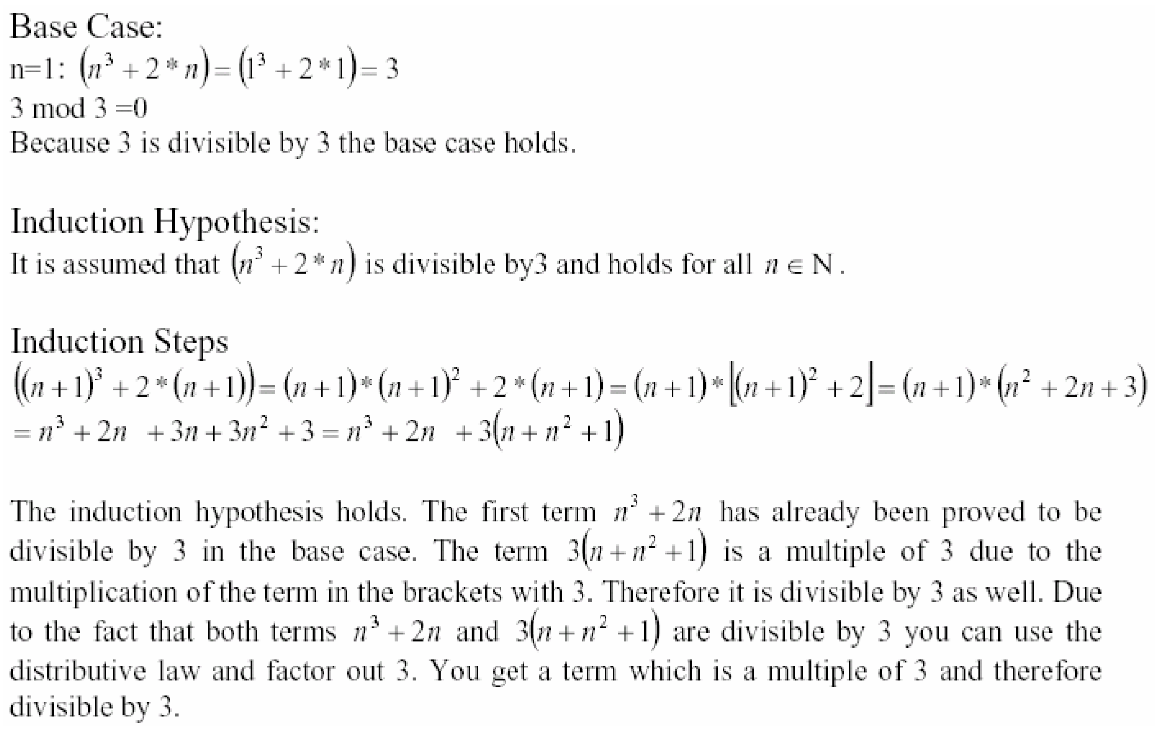
(i) IsBird(x): x is a bird
CanFly(y): y can fly

$\neg [\ \forall x\ \ \text{IsBird}(x) \rightarrow \text{CanFly}(x)]$

(ii)
C(x): x is child
M(x, y): y is mother of x
Y(x, y): x is younger than y

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

3. (Points: 10)



Base Case:

n=1: $(n^3 + 2 * n) = (1^3 + 2 * 1) = 3$

3 mod 3 =0

Because 3 is divisible by 3 the base case holds.

Induction Hypothesis:

It is assumed that $(n^3 + 2 * n)$ is divisible by3 and holds for all $n \in \mathrm{N}$.

Induction Steps

$$((n+1)^3 + 2*(n+1)) = (n+1)*(n+1)^2 + 2*(n+1) = (n+1)*[(n+1)^2 + 2] = (n+1)*(n^2 + 2n + 3)$$
$$= n^3 + 2n \quad + 3n + 3n^2 + 3 = n^3 + 2n \quad + 3(n + n^2 + 1)$$

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.

<u>4.a</u> (Points: 10)

Relation “subset” is:

<u>Reflexive</u>: $\because \forall x \in S, x \subseteq x.$

$\therefore$ relation “subset” is reflexive.

<u>Antisymmetric</u>: $\because \forall x, y \in S, (x \subseteq y) \wedge (y \subseteq x) \Rightarrow (x = y).$

$\therefore$ relation “subset” is antisymmetric.

<u>Transitive</u>: $\because \forall x, y, z \in S, (x \subseteq y) \wedge (y \subseteq z) \Rightarrow (x \subseteq z).$

$\therefore$ relation “subset” is transitive.

Existence of greatest lower bound and lowest upper bound:

$(\forall x, y \in S) \wedge (x \subseteq y)$, the greatest lower bound is x, the lowest upper bound is y;

$(\forall x, y \in S) \wedge (x \not\subset y)$, the greatest lower bound is $(x \cap y)$ (including $\{\phi\}$), the lowest upper bound is $(x \cup y)$(including S).

$\therefore S$ forms a lattice under the relation “subset”.

(Xin Zhou)

<u>4.b</u>

(1) (Points: 10)

Relation $\lesssim$ generate a **partial order** on the elements of D.

For example 13 and 21 are not related under the relation.

Hasse diagram:

```
         33
       /    \
    32       23
   /    \   /   \
31       22      13
   \    /   \   /
     21      12
       \    /
         11
```

(2) (Points: 10)

a. Answer:

S and ≲ form a lattice. Because the relation is reflexive, antisymmetric, and transitive and any pair of element a, b have a least upper bound and a greatest lower bound.

b. Answer:

If remove element 21 from set S, the resulting *S* and ≲ form a lattice. Because the relation is reflexive, antisymmetric, and transitive and any pair of element a, b have a least upper bound and a greatest lower bound.

If further remove 22 from the previous set S, the resulting *S* and ≲ form a lattice. Because the relation is reflexive, antisymmetric, and transitive and any pair of element a, b have a least upper bound and a greatest lower bound.