Problem 1:

a) Confidentiality – Copying home work

b) **Availability** – system unavailability

c) Integrity – changing the amount affects the integrity of the system

d) Integrity – compromising the signature

e) Availability - Not allowing others to use

Integrity – false belief of trusted websites

f) Confidentiality – credit card number obtained

Availability – couldn't access the account

Integrity – acting as another person

g) Confidentiality – data access without permission

Integrity – acting as another person.

Problem 2:

If a virus can delete the files out of all its actions, What security service of computer will get affected with the US law of banning deletion of files?

- ➔ If the scenario of US legislation passing the law that strictly prohibits user from deleting files from computer disks occurs, the it will have a major impact on the security policies of **Availability and Integrity** .
- ➔ This is because if a computer containing important files is affected by a virus, then it might get deleted from the disk permanently or it might get corrupted causing in the loss of data.
- ➔ So deletion of file lead to breach of **availability** service of the computer and, the corruption of file can cause the **integrity** of the file to be questioned.
- ➔ So passing this law might lead to greater economic loss and it will be easy for hackers to affect any corporation or sector since the bulk files can be easily affected .

Problem 3:

The answer to the question is **Yes it is flawed.**

Lets consider TWO persons Alice and Bob.

Alice wants to send a message to **Bob**. Alice encrypts the message with a key **K** using XOR operation and sends it in the channel.

Alice ➔ (plaintext) XOR (K) = ciphertext ➔ BOB

At this time EVE (a third person –hacker) can see the cipher text in the channel and stores it.

Bob receives the ciphertext and he decrypts it with his key and obtains the plaintext. Bob sends the plaintext to Alice for verification. And Alice get the text and verifies it is the same plaintext she sent to Bob.

Bob ➔ (ciphertext) XOR (K) =plaintext ➔Alice

BUT, Eve who is monitoring the channel can see the plain text and she will store the plaintext too. Now she has the plain text and the cipher text. She can perform XOR operation on the these two and she can get the key. Which makes the communication between Alice and Bob vulnerable and it loses its confidentiality.

Eve ➔ (ciphertext) XOR (Plaintext) = K

PROBLEM 4 & 5 NEXT PAGE

Problem 5:

Cipher text : CSYEVIXIVQMREXIH

Plaintext : YOUARETERMINATED

Key : 4

PROGRAM:

```
public class Decrypt {
        public static void main(String a[])
        {       String ALPHABET="abcdefghijklmnopqrstuvwxyz";
                String cipherText="CSYEVIXIVQMREXIH";
                String ans="";
                int shiftKey;
                 cipherText = cipherText.toLowerCase();
            String plainText = "";
            for (int i = 0; i < cipherText.length(); i++)
            {       int charPosition = ALPHABET.indexOf(cipherText.charAt(i));
                                int keyVal = (charPosition - 4) % 26;
              if (keyVal < 0)
              {             keyVal = ALPHABET.length() + keyVal;
              }
              char replaceVal = ALPHABET.charAt(keyVal);
              plainText += replaceVal;
            }
            System.out.println(plainText);
        }
}
```

Output : youareterminated

Problem set 2:

Problem 4:

a, b, c are bits

$$a \oplus b = c$$

Let consider the value for a and b to be

a	b	c
0	0	0
0	1	1
1	0	1
1	1	0

1. $a \oplus a$

$= a a' + a' a$

$= 10 + 01$

$= 0 + 0$

$= 0$

2. $a \oplus a'$

$= aa + a'a'$

if $a = 1$ $= 1 + 0 = 1$

if $a = 0$ $= 0 + 1 = 1$

$\therefore a \oplus a' = 1$

3. $a + b'$

$= a'b' + ab$

a	b	b'	c
0	0	1	1
0	1	0	0
1	0	1	0
1	1	0	1

Answer $\Rightarrow$

④ $a'+b'$

a	b	a'	b'	c
0	0	1	1	0
0	1	1	0	1
1	0	0	1	1
1	1	0	0	0

$\therefore a' \oplus b' = a \oplus b$

⑤. $a \oplus b \oplus a$

$a \oplus b = c$

$\therefore a \oplus b \oplus a = c \oplus a$

c	a	$c \oplus a$
0	0	0
1	0	1
1	1	0
0	1	1

$c \oplus a = b$

⑥. $b \oplus c$

b	c	$b \oplus c$
0	0	0
1	1	0
0	1	1
1	0	1

$b \oplus c = a$