COM-301 : Computer Security
MIDTERM - 25th October
Group A

Name: **SCIPER:**

Question 1: [20 pts]
Here are two scenarios where the security of the system is violated. Name one computer security principle that has been violated to get to this situation. Justify your answer.

a) A professor wants to run an online exam. Students must authenticate to the server before proceeding to the exam. To avoid the exam, some unprepared students flood the server with authentication requests. While handling these requests, the server cannot handle the requests for the exam page. [10pts]

b) A lazy programmer decides that every time a user requests reading access to a file she will also receive write and execution access. A malicious user takes advantage of this fact to change the password of other users. [10pts]

Question 2: [15pts]
Alice can read and write to the file `xxx.sys`, can read the file `yyy.sys`, and can execute the file `zzz.sys`. Bob can read and write to `yyy.sys`, and cannot access `zzz.sys` or `xxx.sys`. Charlie can execute `yyy.sys`, can write and read `xxx.sys` and only write `zzz.sys`.

a) Write the associated access control matrix? [5pts]

b) Write the set of access control lists for this situation. [5pts]

c) Write the set of capabilities for this situation. [5pts]

Name: **SCIPER:**

Question 3: [20pts]
In the class we saw how a user, say Alice, can write a small application `msg` to allow other users to leave messages for her. The application works such that executing '`msg string`' writes `string` into `msgfile.txt`, as described by this pseudocode:

```
Program msg(string input)
{
   file = open("msgfile.txt","a");   // open messages log with append rights
   write(input+'\n',file);           // write input in messages log
   close(file);                      // close messages log
   exit;
}
```

Why are these permission configurations problematic when the script is called by Charlie (not Alice, not in the group Alice+Bob)? [10pts each]

a) Configuration A

```
-rwx--x--x   Alice Alice+Bob msg
-rwxr-x-wx   Alice Alice+Bob msgfile
```

b) Configuration B

```
-rwx--x--x   Alice Alice+Bob msg
-rwxrw---x   Alice Alice+Bob msgfile
```

Question 4: [15pts]
Consider a BIBA policy used in a bank with classification labels public < verified < certified, and categories {administration, investments, finance}. Answer the following questions justifying your answers.

a) Explain which subject classification, if any, gives a principal the most privileges for writing and for reading? [5pts]

b) Can a principal with classification (verified, {administration,finance}) read from a file with classification (verified, {administration})? Why? [5pts]

c) How is the process of upgrading a document from public to certified called? What precautions must be taken when doing this? [5pts]

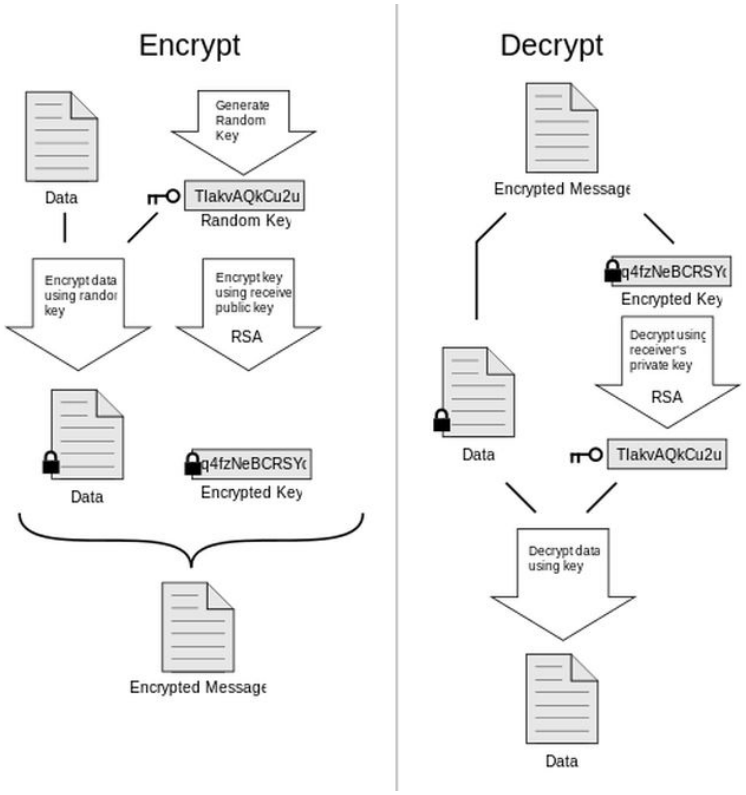
Name: **SCIPER:**

Question 5: [20pts]
Let us assume that we have an adversary that has the capability to steal a password database.

a) What properties of a hash function are used to secure the storage of passwords? [10pts]

b) What is the role of a salt when storing H(password || salt)? [10pts]

Question 6: [10pts]
The following picture explains how PGP (Pretty Good Privacy) used to encrypt emails.



a) What types of encryption are used to obtain confidentiality? Explain how they are used, and the reasons why we use this combination. [5pts]

b) If you also need to provide integrity, what would you need to add? Justify your answer. [5pts]