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

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 security engineer is designing a system. To ensure that no unauthorized user can log into the system, he implements an access control mechanism in which the decision to grant access depends on the state of the operative system. This state is composed by thousands of variables. A hacker takes advantage of inconsistencies between these variables to get access to the system. [10 pts]

b) A computer system uses the same port to serve access control and to download documents. When access control is not available for 10 minutes, the computer system allows users to access documents. A user starts the download of a very large file in order to gain access to the documents without valid credentials. [10 pts]

Question 2: [15pts]
Alice can read the files `xxx.sys` and `yyy.sys`, and can write and execute the file `zzz.sys`. Bob can read `yyy.sys`, and cannot access `zzz.sys` or `xxx.sys`. Charlie can execute `yyy.sys`, can write and read `xxx.sys` and cannot access `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 operation is very simple: 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 Bob (who belongs to the group Alice+Bob)?

a) Configuration A [10pts]

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

b) Configuration B [10pts]

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

Question 4: [15pts]
Consider a Bell-LaPadula (BLP) policy used in a hospital with classification labels public < restricted < confidential, and categories {administration, patient, finance}. Answer the following questions justifying your answers.

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

b) Can a principal with clearance (confidential, {administration}) write to a file with classification (restricted, {administration, finance})? Why? [5pts]

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

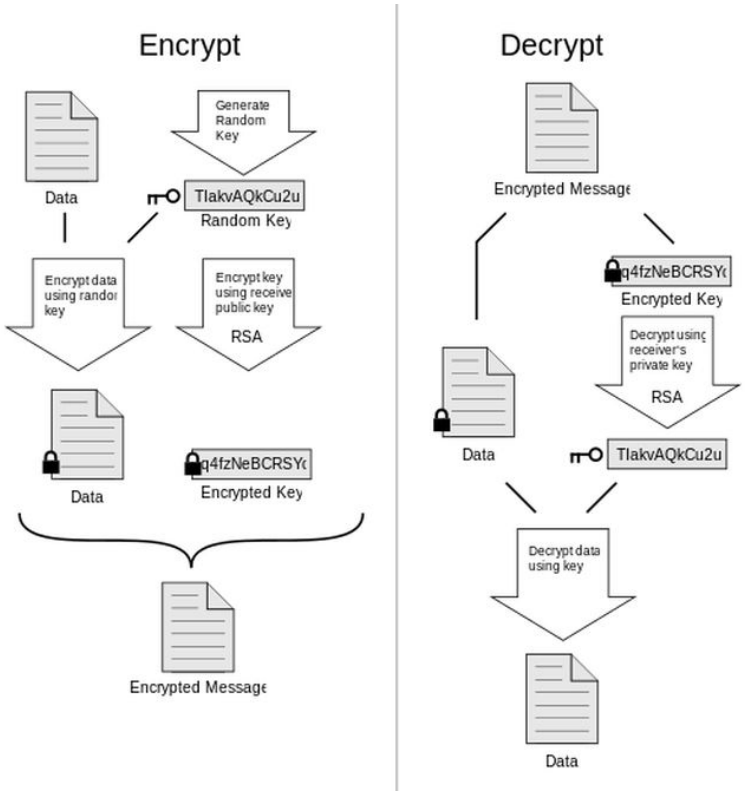
Name: **SCIPER:**

Question 5: [20pts]
In order to enter once a lab you need a signature of the professor on the message "permission to enter".

a) What properties of a hash function are necessary to ensure that signing a hash H("apt for entering") provides the same security as signing the message itself? [10pts]

b) Why would one want to add a nonce to the signature Sig(H("permission to enter", nonce)) [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. [5 pts]

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