Final Exam

CS252A

November 25, 2017

Duration: 3 hours

Name: ____

Roll No. _______________________________

Section I: Basic Cryptography (25 points)

1. **[7 points]** *Public Key cryptography* requires a *public* and a *private* key. You never have to share your secret private key with anyone. In symmetric cryptography you must share the secret key with the party communicating with you. That gives an impression that public key cryptosystems are superior to symmetric key cryptosystems. Why is it that we still use both types of cryptosystem?

   [Your answer must be based on computational argument and not social arguments – such as "we want to give both equal chance" or some such illogical statement.]

The only answer that is expected and gotten full marks is regarding efficiency of symmetric key systems. All other reasons provided seem to indicate that Public Key System should not even be used.

Model Answer: Symmetric crypto is much more efficient, especially when implemented in hardware, and public key systems require complex mathematical operations over a finite field, and hence much slower. However, symmetric key is harder to distribute, whereas public key distribution problem has multiple solutions.

Thus, these two systems co-exist – public key cryptosystem is used to negotiate the symmetric key first, and then for more voluminous data transfer, symmetric key algorithms are used – often implemented in hardware.

2. **[7 points]** Given a message text ***M*** which is few megabytes in size, describe how would one create a digital signature to go along with ***M,*** to prove the authenticity of the sender? Assume that the sender has a public key ***p,*** and private key ***q,*** and a signature function ***S.***

Your answer must consider the fact that the size of the signature should be much smaller than the text itself. Normally a digital signature should be in kilobytes or less.

If you have not used hash – you cannot reduce size. So if you skipped hash or did not show the equational form as below – you would lose some points.

Model Answer: You first hash the message M into a fixed length bitstring, and then use private key q to sign as follows. Say b = hash(M) and signature = S(b,q).

Receiver takes the signature, applied public key p of the sender, and obtain b'. It also computes hash(M). If hash(M) == b', then it knows that the message was signed using q. Since q is supposed to be secret and only possessed by the sender, it can be sure that the message came from who claims it to be.

3. ***[2 + 3 + 2 = 7 points]*** If you want to send a message ***M*** (encrypted or unencrypted), you may want to send something additional to prove the integrity of the message *(i.e. to show that the message has not been altered during transmission*). What is this additional information called in the cryptographic parlance? What kind of function is used to create this additional information? Name one such standard function which is widely used in SSL/TLS based communication.

Model Answer: You need to use a hash function that is collision resistant and difficult to invert.

Message digest or cryptographic digest, or message authentication code.

SHA 256, SHA 512, SHA3 -- any one of them will do.

4. **[2 + 1 + 1 = 4 points]** What is **PKI**? Why do we need **PKI**? What is the most common **PKI** system in use today?

Model Answer: Public key infrastructure. Public key of an entity has to be known by others in order to send encrypted messages to that entity or to check digital signature done by the entity. In order for everyone to find the public key of the entity from an authenticated source, a PKI has to be designed.

Digital Certificate (X.509) based or PGP (Pretty Good Privacy) based.

Section II: Java Programming Concepts (60 points)

5. **[5 points]** What are the differences between JVM, JRE, and JDK?

   Model Answer: JVM = Java Virtual Machine – the software emulator that runs byte code.
   JRE = Java run time environment – that has libraries in bytecode form and various auxiliary functions that allow a Java program to run on a JVM.
   JDK = Java Development Kit – a software development environment and corresponding Javac, JVM, JRE etc.

6. **[5 points]** Explain difference between a static method and a regular method in Java class with code example.

   Not too much was expected here. If your answer made the following point, only then you got full points.

   Model Answer: Static method is class specific. Regular method is instance specific.

7. **[8 + 7 = 15 points]** I want to create a java class with class name "Singleton". The property of this class must be that ***if an instance is created for this class, another instance of the same class cannot be created until this instance has been deleted or gone out of scope***. My friend wrote the following code for this class. Does this class implementation have the property mentioned above? If not, why not – explain in detail. How will you fix the problem?

```
Class
Singleton
{
                 private static Singleton instance;
                 public String str;
                 private Singleton() {
                 }
                 static Singleton getSingleInstance() {

                      if (instance == null) {
                                       instance = new Singleton();
                           }
                      ~~}~~
                      return instance;
```

```
            }
        }
```

Those who think private constructors are not allowed – they are wrong. Private constructors are used when you have a factory method like "getSingleInstance" but in any case, the point was to find logically why this will not work as an implementation of "singleton" property. The (instance == null) check and the instance creation are not atomic. As a result, when two threads will call "getSingleInstance()" there is a chance, that two instances might be created. One more point, those who thought a delete() function is missing – are confusing between C++ and Java. Java has garbage collection. Also, note that returning instance even when instance is not null is ok – as you are not returning a new instance – you are giving back the old instance – so that was not the problem either.

Model Answer: No this will have race condition, or it will have concurrency problems. If getSingleInstance() is called from two threads, and one thread checks the nullity of the instance and gets true answer, it may be preempted and another thread will create an instance. When the original thread is scheduled back, it will also create an instance.

You need to use synchronized blocks to make the checking of the instance's nullity, and creation of the instance atomic.

```
Synchronized{
            if (instance == null) {
                        instance = new Singleton();
                }
}
```

8. **[25 points]** Consider the following Java code snippet: (a class named **Data** is defined first, and later used in the main by various threads).

```
public class Data {
public Data(){ value = 0;}
private int value;
public int getValue() {
return value;
}
7. public void setValue(int value) {
8. this.value = value;
9. }
10.  }

In the main() we have:

11.  Data data = new Data();
12.  for (int i = 0; i < numberOfThreads; i++) {
13.  final Thread thread = new Thread(new Runnable() {
             i.  public void run() {
            ii.  int value = data.getValue();
           iii.  data.setValue(value + 1);
            iv.  }
14.  });
15.  thread.start();
16.  }
```

Now answer the following questions based on this code snippet:

A. **[5 points]** If the parameter numberOfThreads = 3, what will be the value of the variable **data.value** at the end of executing the for loop in the main ()?

Model Answer: 1, 2 or 3 depending on scheduler. It will be nondeterministic, since there will be race condition.

B. **[5 points]** Will there be any concurrency problem in this code? What is such a concurrency problem known as?

Model Answer: Yes, there will be. It is called a Data Race condition or race condition or violation of mutual exclusion.

C. **[8 points]** If there is a concurrency problem, how will you fix it? You can just write down the modified lines of the code (with the line number) here.

Model Answer: reading of value and setting the value by its increment are not atomic, leading to nondeterminism. The following change in Like 13 (ii – iv) will fix it.

```
synchronized (data) {

              final int value = data.getValue();
```

```
                  data.setValue(value + 1);

                }
```

D. **[3 points]** Explain the utility of the ‘**final**’ key word on **line 13**.

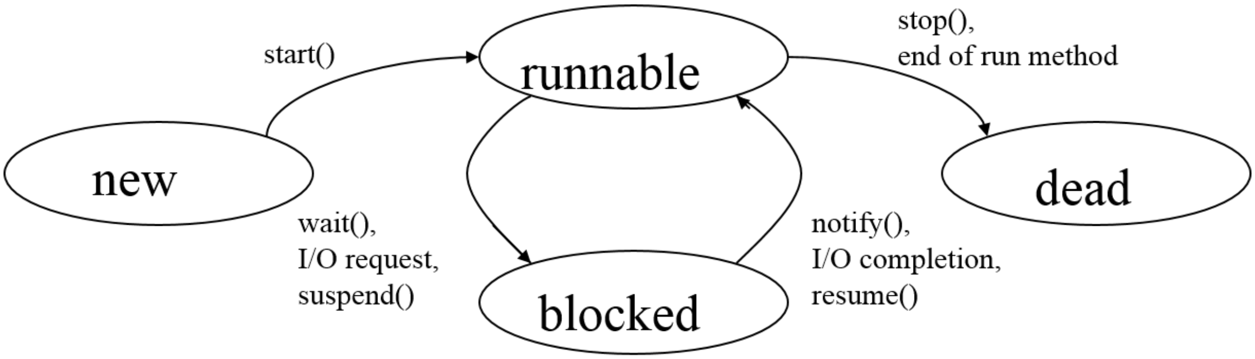
Model Answer: final modifier indicates to the compiler to ensure that the variable cannot have another assignment. For example, the variable thread cannot be assigned a different instance of the class that is implementing runnable in this example code.

E. **[4 points]** Note that in **line 13** and **lines (13.i- 13.iv)** we have defined the **run()** method and defined a new **Runnable** object and a new class implementing the **Runnable** interface at the same time. What is such a class defined on-the-fly called? What is the advantage of such a class?

Model Answer: Inner class and anonymous class.

Advantage: You limit the scope of the class as objects of its type seem to be only necessary within the scope within which it is defined. Also, it does not require naming the class which often helps in reducing namespace congestion.

9. **[10 points]** Java Threads usually have four states, **new**, **runnable**, **blocked**, and **dead**. In the lecture slides, we showed a state diagram where these four states were represented with circles, and arrows were annotated with the method calls that would change the thread’s state from one state to another. Draw the Java thread life cycle state diagram with these four states, and arrows showing state transitions along with the names of the method calls that would create those transitions.



Note that if you missed some of the arrows, or the method names or the reason for the transition from one state to the other (such as I/O request) – you lose a few points depending on how much you miss.

Section III: Block Chain and Bit Coins (15 points)

10. [**5 x 2 = 10 points]** Please select the correct answer for each of the following: (There may be more than one correct choices in some cases. Unless you select all correct choices, you will not get any points.)

    1. **A bit coin Wallet address is:**

a. An IP address of the user

b. Wallet identifier given by the administrator

c. Public key generated from a public-private key pair generation by user

d. A private key

e. None of the above

2. **If more than 51% bitcoin users collude, they can do the following easily:**

a. Steal bitcoins from other wallets (Not possible without knowing private key of owners)

b. **Invalidate valid transactions**

c. Mine more bit coins than the maximum bit coins possible in the system (Not possible as the code base is not maintained by the miners and the max minable coins is fixed by the code base maintainers).

d. None of the above

3. **Which of the following is not a relevant term while describing blockchain?**

a. Distributed

b. peer to peer

c. Public Ledger

d. Tamper-resistant

f. None of the above

4. **In bitcoin block chain, the longest path wins based on the logic that:**

a. Longest path means cryptographically secure

b. Longest path means more proof of work computation

c**. Forked paths by malicious users cannot go faster than longest path computed by more than 51% honest users**

d. All the above

e. None of the above

(In this one, all of the above has been given points as well although statement a is strictly not fully valid).

5. **The need for a block chain based naming service arises due to the fact:**

a. **Standard DNS is controlled by a few corporations and governmental entities**

b. Standard DNS can be manipulated by a few in authority and ban certain domains

c. The Blockchain based name service is robust to tampering due to 51% consensus requirement

d. The block chain based name service such a NameCoin is fault tolerant

(In this one, subset of a,b,c,d fetched points as well).

11. **[5 points]** Explain why is it that a bitcoin transaction takes about 1 hour to get confirmed. (Please write brief and relevant argument only. Write only relevant logically consistent explanation.)

Any answer that closely resemble the following even without the exact intent – has been given points.

Model Answer: In the current bitcoin network, It takes about 10 minutes to be mined into a block. However, unless other blocks are built on top of this block, this block may not remain in the longest chain. To make sure that this block is extended into the longest chain, as a rule of thumb, one waits for at least 6 subsequent mined blocks to extend this block – so on an average that takes about 6 x 10 = 60 minutes. We assume that once 6 blocks have been mined and connected into a chain from this block, it will be hard for hashpower less than 50% to compete and create a longer chain.