Track B
INFA723 Homework 3

The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.

- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.

- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

Note: For all the programming assignments, you can choose any operating systems to develop your code. A README.txt is required to submit any programming assignments. In the README.txt, you need to provide the following information:

1) How to compile your program?
2) How to run your program?
3) What is the output and the results when I run your program?
4) Any descriptions which can help me understand, compile, run, and verify your answers. (FYI: I check every programming assignment turned in!)

Zip all you source code, project files, supporting files, and README.txt and submit the all-in-one zip file together to the D2L Dropbox.

(50 points) 1. A self-signed certificate (cert.cer) and its corresponding private key (prikey.pem) are provided in this question. The certificate includes information such as the certificate version number, the signature hash algorithm, the public key algorithm, the public key, etc. Answer the following questions:

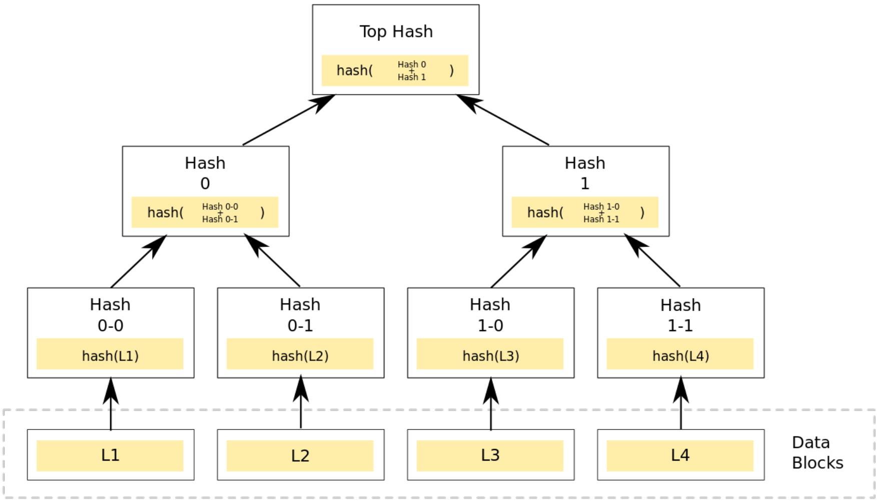
a) What is the signature hash algorithm used to create the certificate?
b) What is the public key algorithm used in the certificate?
c) What is the public key size?
d) trackbcipher.txt is a cipher file encrypted using the certificate. The command line used to encrypt the plaintext file trackb.txt is shown below:

```
> openssl smime -encrypt -binary -aes-256-cbc -in trackb.txt -out trackbcipher.txt -outform DER cert.cer
```

Decrypt the trackbcipher.txt and enclose a plaintext in your solution.

Note that you can use any tools (e.g., openssl) to help you answer the questions. Writing your own program is not necessary.

(50 points) 2. A Merkle tree (hash tree) is a tree of hashes in which the leaves are hashes of data blocks in, for instance, a file or set of files. Nodes further up in the tree are the hashes of their respective children. For example, in the picture hash 0 is the result of hashing the result of concatenating hash 0-0 and hash 0-1. That is, hash 0 = hash(hash 0-0 + hash 0-1) where + denotes concatenation.



Merkle trees can be used to verify any kind of data stored, handled and transferred in and between computers. Currently the main use of hash trees is to make sure that data blocks received from other peers in a peer-to-peer network are received undamaged and unaltered, and even to check that the other peers do not lie and send fake blocks. Suggestions have been made to use hash trees in trusted computing systems.

Answer the following questions:

a) Give a specific scenario in which the Merkle tree is used to protect the integrity of the data and explain how Merkle tree is used to protect the security of the message. (I have enclosed a paper in which the Merkle tree is used to protect data security in wireless sensor networks. It is ok to use the paper as an example to answer the question a) and explain how Merkle tree works. However, you are always encouraged to look for other solutions using Merkle tree other than the example given in the paper.)

b) For the same scenario, think about a single hash function solution, such as SHA-2. Can you replace the Merkle tree using the single hash function in the scenario given in a)? Why or why not?