**CSCI 563 Assignment 1**

**Instruction**:

* Show your work (40% penalty otherwise)
* Submit **a single PDF document** containing all your answers (10% penalty otherwise)
* Make sure if you submitted the intended one. It is recommended that you download what has been uploaded and double-check if the correct document has been submitted.
* You can submit as many times as you want, but the last submission will only be graded. If the last submission is made after the deadline, there should be a late submission penalty.
* Please **type** your answers. The only acceptable handwritten part is figure diagram. Don’t forget to convert the document to a PDF file to submit.
* **No plagiarism: Do not copy and paste any from textbooks and other resources to answer questions (Zero will be given otherwise).**
* Extensions can only be negotiated before the deadline.

**Problem 1. Access Control (60 pts., 20 pts. each)**

Assumption:

* Privileges: read (“R”), write (“W”), execute (“X”)
* Resources:
  + Document files: syllabus.doc, ch1.ppt
  + Image files: trees.jpg, jkim.png, csci563.gif
  + Binary files: prog1.exe, chrome.exe, wireshark.exe
* Access permissions (for users A, B, and C):
  + A has privilege to read all image files.
  + C has privilege to read and write all document files.
  + A and B have privilege to read “syllabus.doc”
  + A and C have privilege to read and execute “prog1.exe”, “chrome.exe”.
  + B and C have privilege to read csci563.gif.

1. Construct the corresponding access control matrix. To answer, use the format in Table 1.1 in the textbook.
2. Construct the corresponding access control list. To answer, use the format in Figure 1.5 in the textbook.
3. Construct the corresponding capabilities list. To answer, use the format in Figure 1.6 in the textbook.

**Problem 2. Vernam Cipher (40 pts., 20 pts. each)**

Suppose the following table for encoding and decoding.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Letter | A | E | Y | M | O | R | H | L |
| Binary | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

1. Assume a message M is ‘MORAL’ and the key is ‘HELLO’. What is the ciphertext C? Show your work.
2. Now assume a ciphertext C is ‘HYMYR’ and the key is ‘HELLO’. What is the plaintext P? Show your work.