CSCI 563 Assignment 1
Due by: 11:59PM on Feb. 7, 2024 (Wednesday)

Instruction:

- Provide your name and CWID on top in the first page of your submission
- Show your work (at least 50% penalty otherwise)
- Submit a single PDF document containing all your answers to the associated folder under Assignments (at least 50% penalty otherwise)
- Make sure that 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.
- Plagiarism: Any violation causes a zero score for the assignment and may result in a failing grade (Do not copy and paste anything from this document to your document submitted)
- Hand-written answers (including showing work) will not be accepted and graded.
- No extension/resubmission request will be accepted.

Problem 1. Vernam Cipher (20 pt., 10 pt. 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

a. Assume a message M is 'EMORY' and the key is 'HELLO'. What is the ciphertext C? Show your work.

b. Now assume a ciphertext C is 'RRYLM' and the key is 'HELLO'. What is the plaintext P? Show your work.

Problem 2. Access Control (30 pt., 10 pt. each)

Consider the following:

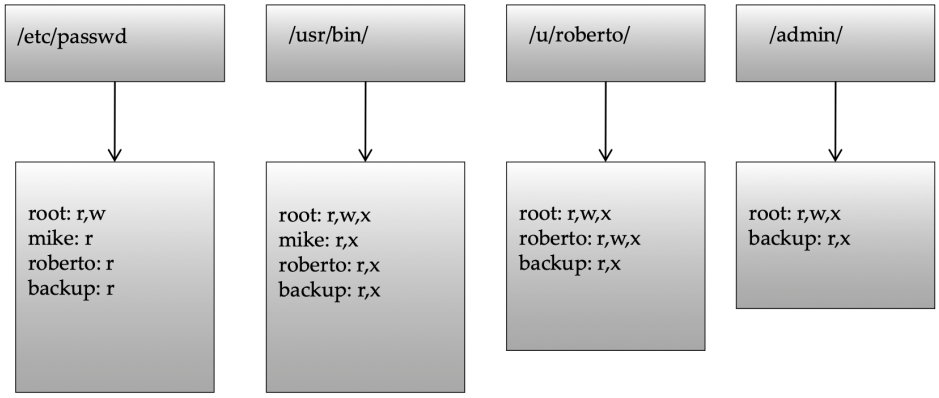
- Privileges: read ("r"), write ("w"), execute ("x")
- Resources:
  - Document files: D1.doc, D2.ppt
  - Image files: D3.jpg, D4.png, D5.gif
  - Binary files: D6.exe, D7.exe, D8.exe
- Access permissions (for users of A, B, and C):
  - A has privilege to read and write all document files.
  - B has privilege to read all image files.
  - A and C have privilege to read "D4.png"

- B and C have privilege to read “D1.doc”
- B has privilege to read, write and execute “D8.exe”
- Everyone has privilege to read and execute “D6.exe”

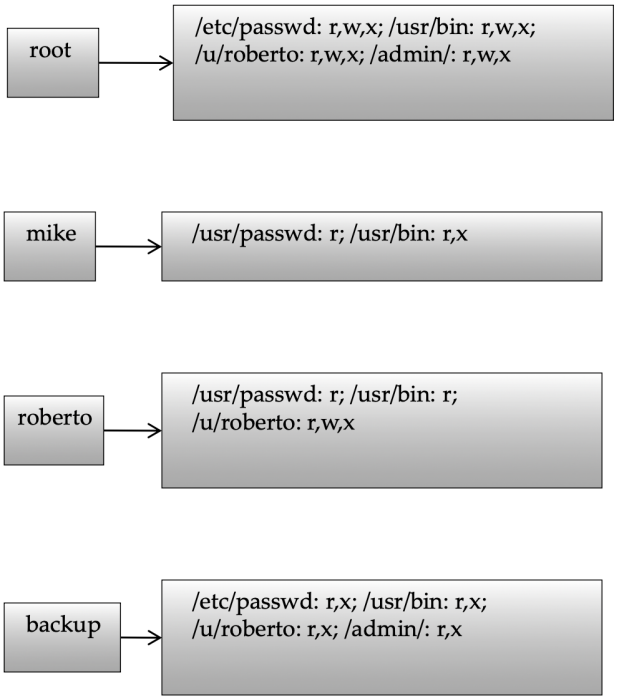
a. Construct the corresponding access control matrix. To answer, use the format in Table 1.1 in the textbook (seen below).

	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
. . .	. . .	. . .	. . .	. . .

b. Construct the corresponding access control list. To answer, use the format in Figure 1.5 in the textbook (seen below).



c. Construct the corresponding capabilities list. To answer, use the format in Figure 1.6 in the textbook (seen below).


root
/etc/passwd: r,w,x; /usr/bin: r,w,x;
/u/roberto: r,w,x; /admin/: r,w,x
mike
/usr/passwd: r; /usr/bin: r,x
roberto
/usr/passwd: r; /usr/bin: r;
/u/roberto: r,w,x
backup
/etc/passwd: r,x; /usr/bin: r,x;
/u/roberto: r,x; /admin/: r,x