Name: Rama Krishna Kamma
CWID: 50321021

CSCI 563 Assignment 1

Problem 1. Access Control

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.

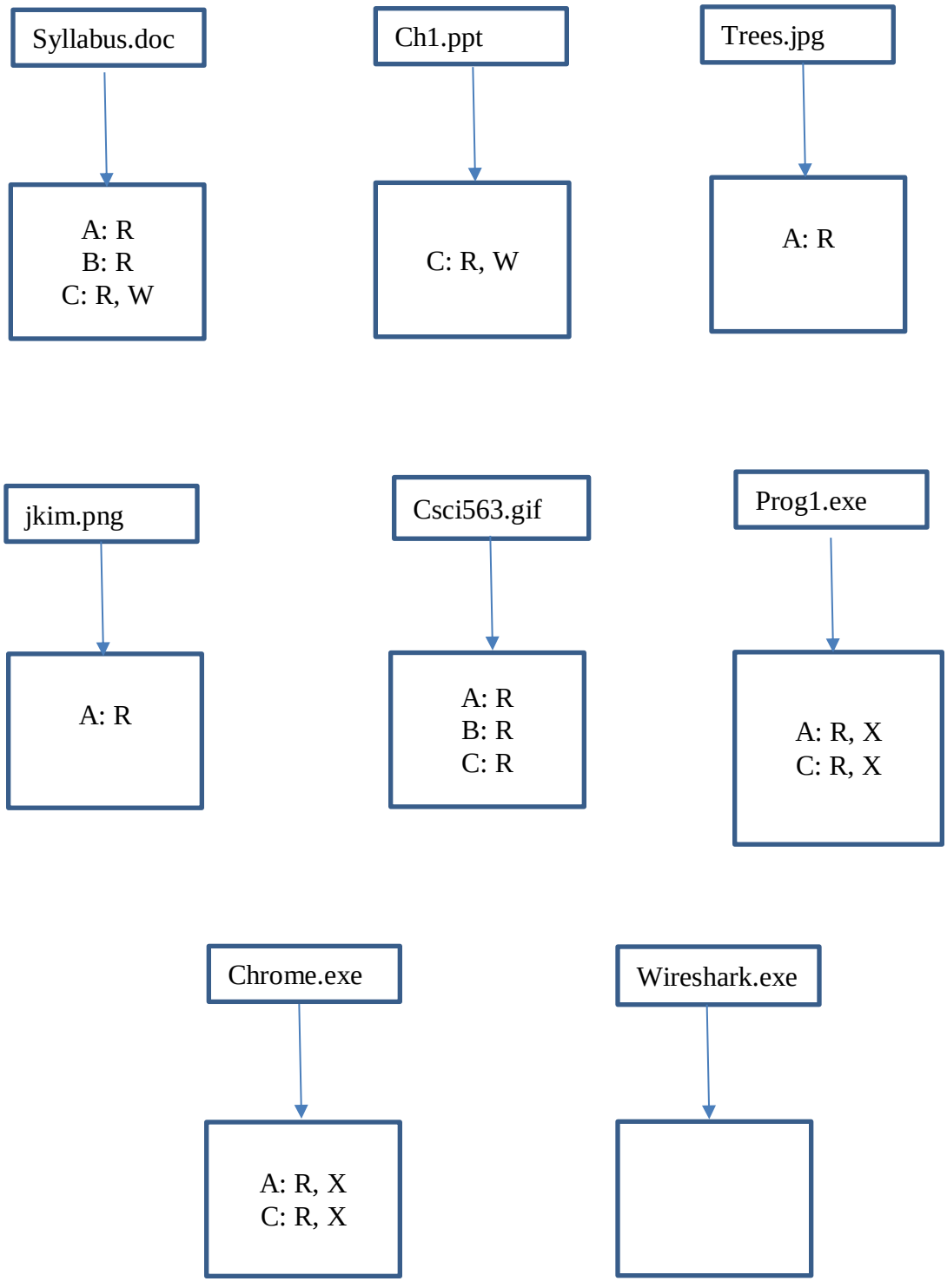
a. Construct the corresponding access control matrix. To answer, use the format in Table 1.1 in the textbook.

Solution:

Users	Syllabus.doc	Ch1.ppt	Trees.jpg	Jkim.png	Csci563.gif	Prog1.exe	Chrome.exe	Wireshark.exe
A	Read		Read	Read	Read	Read, Execute	Read, Execute	
B	Read				Read			
C	Read, Write	Read, Write			Read	Read, Execute	Read, Execute	

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

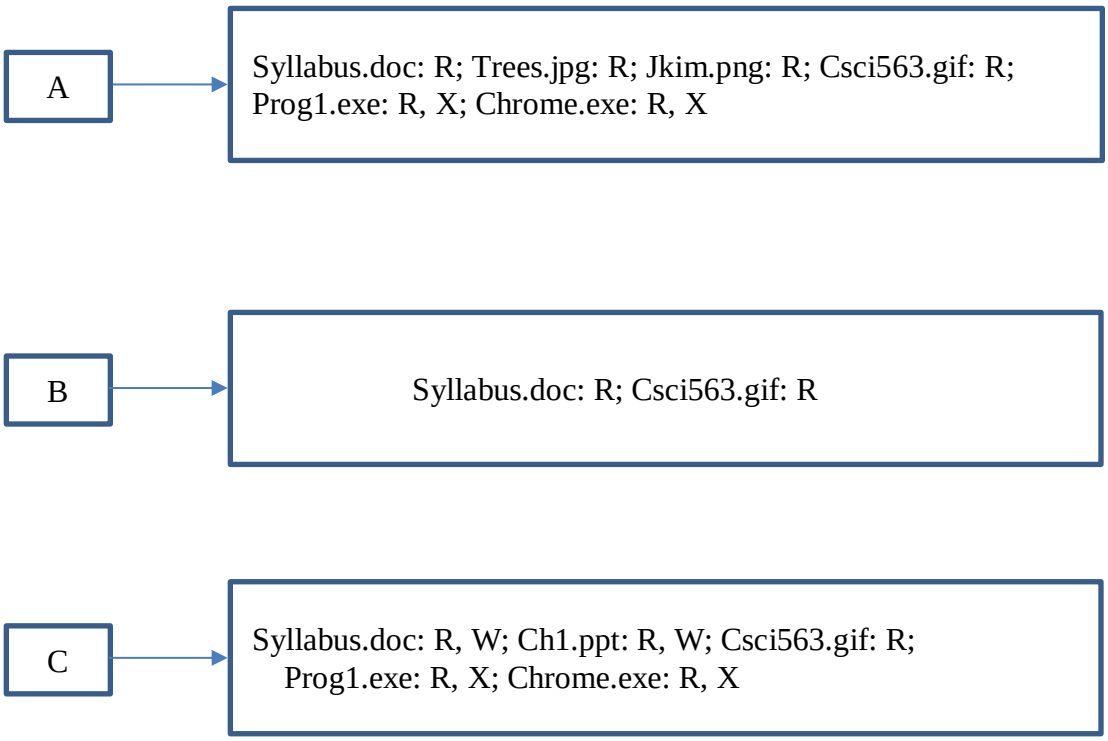
Solution:



Where R: Read, W: Write, X: Execute.

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

Solution:



Where

R: Read, W: Write, X: Execute.

Problem 2. Vernam Cipher:

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 'MORAL' and the key is 'HELLO'. What is the ciphertext C? Show your work.

Solution:

Given
Message = "MORAL"
Key = "HELLO"

Vernam Cipher = Message (XOR) Key

XOR Operation:

A	B	Result
0	0	0
0	1	1
1	0	1
1	1	0

Step-1: Convert given message into binary format according to the given table.

Message	M	O	R	A	L
Binary	011	100	101	000	111

Step-2: Convert given key into binary format according to the given table.

Key	H	E	L	L	O
Binary	110	001	111	111	100

Step-3: Performing XOR Operation

Message Binary	011	100	101	000	111
Key Binary	110	001	111	111	100
XOR	101	101	010	111	011

Step-4:

Cipher Text	R	R	Y	L	M

From the above vernam cipher the cipher text for given message and key is "RRYLM"

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

Solution:

Given
Ciphertext = "HYMYR"
Key = "HELLO"

Vernam Cipher = Cipher text (XOR) Key

XOR Operation:

A	B	Result
0	0	0
0	1	1
1	0	1
1	1	0

Step-1: Convert given cipher text into binary format according to the given table.

Ciphertext	H	Y	M	Y	R
Binary	110	010	011	010	101

Step-2: Convert given key into binary format according to the given table.

Key	H	E	L	L	O
Binary	110	001	111	111	100

Step-3: Performing XOR Operation

Ciphertext Binary	110	010	011	010	101
Key Binary	110	001	111	111	100
XOR	000	011	100	101	001

Step-4:

Plain Text	A	M	O	R	E

From the above vernam cipher the plain text for given message and key is "AMORE"