ECE 518 Homework 4/5

Alan Palayil

Due Date: 11/30/2022

A1:

a)

$S_A = (A_0+A_1+A_0) \bmod 32$

$= (7+17+7) \bmod 32$

$= 31$

$S_B = (B_0+B_1+B_0) \bmod 32$

$= (3+19+3) \bmod 32$

$= 21$

b)

Encryption function $e_{k1}||_{k2}$ (x) = $(k_1+k_2+x) \bmod 32$. Considering Alice chooses a=1.

Alice’s input:

$e_1(1) = (1 + 1 + 0) \bmod 32 = 2$

$e_2(1) = (1 + 1 + 1) \bmod 32 = 3$

c)

Bob's input:

$e_1(0) = (1 + 1 + 0) \bmod 32 = 2$

$e_2(0) = (1 + 1 + 0) \bmod 32 = 2$

d)

Bob decrypts his input:

$d_1(2) = (2 + 5 + 0) \bmod 32 = 7$

$d_2(2) = (2 + 5 + 0) \bmod 32 = 7$

He then computes: NAND (7, 7) = 0

e)

Suppose Alice chooses a = 0 and sends Bob the garbled circuit and inputs. Since Alice chose a = 0, Bob's input is encrypted as

$e_1(0) = (1 + 1 + 0) \bmod 32 = 2$

$e_2(0) = (1 + 1 + 0) \bmod 32 = 2.$

These values are not equal to 7, so Bob cannot decrypt his input and compute NAND (7, 7) = 0. Therefore, Bob cannot decide Alice's choice of a.

If Alice had chosen a = 1, A0 = 17, A1 = 7 while sending Bob the same garbled circuit and inputs then Bob would have been able to decrypt his input and compute NAND (7, 7) = 0.

A2:

a)

	alicerc	bobrc	cyndyrc
Alice	ox	r	
Bob	r	ox	
Cyndy	r	rw	orwx

b)

	alicerc	bobrc	cyndyrc
Alice	ox	r	r
Bob		ox	
Cyndy	r	rw	orwx

A3:

From the given data, TOP SECRET --> Priority 1, SECRET --> Priority 2, CONFIDENTIAL --> Priority 3, UNCLASSIFIED --> Priority 4. Assume A's partition be (L_A, C_A) and B's partition be (L_B, C_B). From discretionary access controls allows, If $L_A \geq L_B$ and $C_B \subseteq C_A$ then A can read B. If $L_B \geq L_A$ and $C_A \subseteq C_{B,}$ then A can write B.

a)

Paul cannot write or read the document because Paul's clearance level does not dominate categories B.

b)

Anna has clearance of Priority 3 in category C and wants to access a document in category B. Thus, Anna cannot read or write this document.

c)

Jesse can read a document because his clearance level is higher than the classification level of the document, but he is unable to write to the document because the classification level of the document is lower than the clearance level of the document.

d)

Sammi can read a document because the classification level of the document is higher than Sammi's clearance level; however, Sammi is unable to write to the document because the classification level of the document is lower than Sammi's clearance level.

e)

Robin cannot read a document because the classification level of the document is higher than Robin's clearance level, but Robin can write to the document because the classification level of the document is higher than Robin's clearance level.

A4:

Alice would like to read four objects in the order a, b, c, and d.

CD(a)=Citibank - Since Citibank a is the first object she is accessing in the first COI class; she can read Citibank a.

CD(b)=ARCO: Since Alice is accessing the first object in the second COI class, she can read ARCO b.

CD(c)=Citibank: Alice can read Citibank c because it comes from the same bank as the first COI and is related to Citibank.

CD(d)=Standard Oil: Alice is unable to read the Standard Oil d because it comes from the second COI and has already been read as CD(b)=ARCO.

A5:

a)

A file with the permission "rw-rw- r--" and Alice as group owner and owner. Bob had read and write permissions since he is also a group member of the group alice, whereas alice had read and write permissions at the owner and group levels.

b)

A file with the permission "rwxr-x---" in which Cyndy is the group owner and Alice is the owner. At the owner and group levels, Alice had read, write, and execute permissions. Because bob is also a group member of the group Alice, he had read and execute permissions at group as Cyndy was the owner of the group.

c)

A directory D, Alice was the owner, and Bob was the owner of the group, with permission "rwxr-x--x," Cyndy had read and execute permissions on the group. Bob had read, write, and execute permissions because he is also a member of the group that includes alice. However, alice had read, write, and execute permissions.