Alex Hortin
Computer Security Assignment 3

1:Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it.

a Create the corresponding access control matrix.

Files(below)/Users ->	Alice	Bob	Cyndy
alicerc	READ/WRITE/OWN	READ	READ
bobrc	READ	READ/WRITE/OWNS	READ/WRITE
cyndyrc			READ/WRITE/OWN

b Cyndy gives Alice permission to read cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix.

Files(below)/Users ->	Alice	Bob	Cyndy
alicerc	READ/WRITE/OWN		READ
bobrc	READ	READ/WRITE/OWNS	READ/WRITE
cyndyrc	READ/		READ/WRITE/OWN

15 Pts Why is Theorem 3-2 an important and basic theoretical result in the field of Computer and Network Security?

Theorem 3-2

It is undecidable whether a given state of a given protection system is safe for a given generic right.

This theorem is very important since it essentially says that as many rights and safeguards we put in a system to isolate and obscure certain things from users it can never be officially declared safe according to the rules that we laid out for the system. This theorem states that there may always be a leaking of rights to users or processes that should not possess those rights.

The result is that a given system may not always be entirely safe since the safety problem for non trivial systems in undecidable, but security is the study of those systems to help ensure the highest level of safety possible.

30 Pts Using the algorithms given in the proof of Theorem 3-2, specify the access control matrixthat will result after five steps of the following Turing machine on the given tape configuration,with the read head on the left-most 'A'.

```
Tape Configuration:     A B B A b b …
                       ^
                       p
```

Turing Machine:

K = { p, q, r } initial state = p, halt state = r
M = { A, B } ∪ { b }
δ= δ (p, A) = (p, A, R)
δ (p, B) = (q, A, L)
δ (q, A) = (p, A, R)
δ (q, B) = (r, A, R)

Note: The algorithms in the book assume an initially blank tape. Therefore, given the four initial input characters on this Turing machine tape, you may start with a "pre-loaded" 4 x 4access control matrix that corresponds to the initial tape configuration.

```
.......................................................
A B B A b b ...                    State 0
^
p = δ (p, A) = (p, A, R)
........................................................
A B B A b b ...                    State 1
  ^
  p = δ (p, B) = (q, A, L)
........................................................
A A B A b b ...                    State 2
^
q = δ (p, A) = (p, A, R)
........................................................
A A B A b b ...                    State 3
  ^
p = δ (p, A) = (p, A, R)
........................................................
A A B A b b ...                    State 4
    ^
p = δ (p, B) = (q, A, L)
........................................................
A A A A b b ...                          State 5
  ^
p = δ (p, A) = (p, A, R)
```

	s1	s2	s3	s4
s1	A	Own		
s2		B	Own	
s3			A	Own
s4				A Own

4.3A noted computer security expert has said that without integrity, no system can provide confidentiality.

Do you agree? Justify your answer.

As defined in the book: **Confidentiality** is the concealment of information or resources.
Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change

I completely agree with this statement. Confidentiality is nothing without data integrity. If there is no data integrity, than data can be altered rendering any confidentiality completely useless. Since loss of integrity can also reveal details of the system confidentiality is lost that way as well.

Can a system provide integrity without confidentiality? Again, justify your answer.

Definitely. Take the online version of Magic the Gathering for example. I can set my collection to public, removing the confidentiality of my collection, however any user viewing it will not be able to alter it, due to the integrity of the system in place.

4.4A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.

I do not agree with this claim. The problem is there will need to be a security mechanism to protect the keys. In all cases these keys must be protected by other keys, or by some non cryptographic type of security mechanism. Even if the key were only stored on one flash drive that was read only and the system didn't allow copying that key, you would still need some physical level of security to see who had access to that key.