1. Using Sandhu’s notation for separation-of-duty

- Describe a sequence in which different clerks must prepare a purchase order, receive a loading dock receipt, and then issue a check to pay for the order.
  *ans. assumes static SoD between clerk and loadingDockWorker otherwise they should all be clerk.*
  
  \[
  \begin{align*}
  \text{prepare} & : \text{clerk} \\
  \text{receive} & : \text{loadingDockWorker} \\
  \text{issue} & : \text{clerk}
  \end{align*}
  \]

- Describe a sequence in which a manager requests a purchase, a clerk gets bids and chooses a supplier, the order is approved by the purchasing manager, and then the original manager OKs the final issuance of the purchase order.
  *ans. assumes purchasingManager is different from manager.*
  
  \[
  \begin{align*}
  \text{request} & : \text{manager} \downarrow x \\
  \text{bids} & : \text{clerk} \\
  \text{approve} & : \text{purchasingManager} \\
  \text{final} & : \text{manager} \downarrow x
  \end{align*}
  \]

- Describe a sequence in which a Vice President or 2 managers can approve a promotion, after which a clerk enters the data, and then a second checks the data.
  *ans.*

  \[
  \begin{align*}
  2: \text{approve} & : \text{vp} = 2, \text{manager} = 1 \downarrow x \\
  \text{enter} & : \text{clerk} \\
  \text{check} & : \text{clerk}
  \end{align*}
  \]
2. Describe an approbability scenario in which Sandhu’s notation is insufficient to describe.

ans. The problem with Sandhu’s notation is that it does not allow branching in the approval process. So a process which consists of one of two alternatives (eg. one with 3 steps and one with 2) cannot be implemented.

3. Consider declassification in which a security officer reduces the level of a document, for example for top secret to secret. Can this be done with a lattice? If so, explain how. Otherwise describe a scheme how this scenario can be accommodated.

ans. The lattice rules do not allow for declassification. Hence, they must be augmented with declassification rules, for example declassify(topSecret, secret) by topSecretSecurityOfficer.

4. Can the integrity of a computer be ensured by its operating system? Explain the degree to which it can and cannot be ensured.

ans. There are three aspects of integrity: the user who makes the changes, the information flow (ie Biba), and the executable correctly modifies the object (ie Clark-Wilson). An OS can ensure the first two, but not the last (although it can control what executables update the objects).

5. The following techniques have been used to protect passwords. Describe against what attacks they are effective:

- shadow file ans. off-line attacks.
- one-way hash of the password ans. stealing or reading file containing passwords.
- PAM (Pluggable Authentication Modules) ans. weak password.
- trusted path ans. login spoofer.
- salt ans. requires separate dictionary attack for each user.

6. Consider a situation in which retina scans have been used as an authentication mechanism in the presence of an armed guard. As a cost cutting measure, management has decided to get rid of the guard. What effect will this have on security.

ans. someone may try to put up a picture of an retina, which the scanner might accept. The guard would have presumably objected to this.

7. Banks use 2-factor identification for ATMs (a card and a PIN). Describe the ways in which this is significantly more secure than single factor and why the PIN is so short.

ans. 1) If you lose your ATM card, an attacker does not have the PIN (unless you wrote it on the card) 2) If you let someone use your card once, they learn your PIN but must give you back the card (preventing further access) 3) The card is confiscated after 3 tries (given 4 digits its a 1 in 10000 shot) and there is a camera in the machine.
8. What is the advantage of the TCB? What is the disadvantage?

ans. The advantage of the TCB is it gives a means of identifying those components of the computer system on which integrity depends. The disadvantage is that the TCB does not distinguish large breaches from small ones, and hence integrity requirements can pull in the whole of the system into the TCB.

9. What parts of a computer system must be part of the TCB? Explain.

ans. The OS kernel. Any process with the ability to read and/or write any label. Any process which authenticates.

10. When considering integrity, do applications become part of the TCB? How can the size of the TCB be limited?

ans. Yes, anything that updates objects becomes part of the TCB. We need to consider what is critical, important, insignificant, whatever, and appropriately verify by category.

11. Which of the following actions are authorization or authentication (or both):

   - showing ID ans. authentication.
   - having a document notarized ans. authentication
   - withdrawing money from the bank ans. authorization
   - depositing money at the bank ans. authorization
   - adding a signatory to an account ans. authentication (from the owner or designee) and authorization (the bank agrees)