Examination Paper

Spring Session 2016

Part A

1) Examples of each of the main authentication bases are password, PIN, or secrete for what a subject knows, a card, badge, or device for what a subject has, biometrics such as fingerprints or retinal characteristics for what a subject is, and in front of a particular terminal or in a specific room for where an entity is.

Part A

2) Two security properties of a cryptographic hash function are one-way, that is, it is infeasible to generate the preimage from the hash digest, and collision resistance, that is, it is infeasible to have two different messages with the same hash value.

Part A

3) “Online” and “offline” attacks differ in that
online require the connection to be active which
may impose certain restriction while attempting to
break the password while offline attack have
unlimited chances to break the password.

Part A

4) Two possible consequences of a buffer overflow are exploitation by attacker to inject malware to cause an attack against availability such as denial of service and run some arbitrary code to modify data (attack data integrity) as well as stealing information (attack on data confidentiality).

Part A

5) The principle of least privilege is reflected via
a partial order ≤ (generally a reflexive,
antisymmetric, and transitivity relation), so that for
every two elements a, b ∈ L there exists a least
upper bound u ∈ L and a greatest lower bound l
∈ L in a lattice.

Part A

7) Each row of the authorization table of Sandhu & Samarti contains access triplet (Subject, Object, Action). It is also known as the capabilities which is from the point of view of the subject's action on the various objects.

Part A

8) Two resources that can be targeted in a DOS attack are _network bandwidth (for network)__ and _______ memory storage as well as processor capacity (for computer).

Part A

9) Random seeding a password generator with time alone is a bad idea because __if an attacker knows the time, the attacker can use the same time as the seed to the random generator to regenerate the same sequence of password.__

SIM-2016-S3-CSCI262-S3a, Slide 34, 37

Part A

10) Inference is the derivation of Sensitive
information from non-sensitive, typically
aggregate data.

Part A

11) Spear phishing differs from general phishing in that

Spear phishing is targeting a specific person while general phishing is targeting all the people and expecting some to be fooled.

Part A

12) Error-based SQL injection uses Error messages
thrown by the database server to obtain
information about the structure of the database.

Part A

13) An event being “Not known to be bad” likely refers to not being on a event description of activities considered to be violating security policies in the context of Intrusion detection system.

Part A

14) To be stateless means a server has not committed any resources and is relevant in the context of client puzzle connection protocol.

Part A

15) A chain of custody provides assurances that evidences collected during digital forensics are un-altered???

Part A

16) Units are relevant in digital forensics and logging because ___________________________________

Part B – Question 1 …1

1) Describe three distinct types of attacks against password systems. Briefly discuss appropriate countermeasures against one of those types of attacks.

SIM-2016-S3-CSCI262-S2a, Slide21

Part B – Question 1 …2

- The three distinct attacks are dictionary attack, brute-force attack and hybrid attack. A dictionary attack uses a “dictionary” of all known words and try to find the password. Brute-force attack is trying all the possible combination of the password until it is correct. Hybrid attack is combination of brute-force and dictionary attack where we use dictionary as the basis but take variants on each of the words tested. We can protect against dictionary attack if we use words that are not commonly found in the dictionary or random words. Alternatively, use salt and regularly change the password.

Part B – Question 2 …1

2) Describe in detail how the one-time password system of Lamport works.

One-time password refers to a password that can be used only for one session or one transaction. Lamport's one-time password is one example of such password. Lamport's one-time password consists of two parts, the setup and the process as follows:

Setup:

- In the setup process, a user is selecting a password that is secret to him/her.
- The system will then use this password, together with some value, say n, generate a sequence of passwords $p_1, p_2, \dots p_n$.

Part B – Question 2 ...2

Process:

- A user, let's say Alice, request for connection to a server.
- The server issues a challenge n;
- The user responds with one-time password which is generated as $h^{n-1}(password)$
- The server checks if $h\left(h^{n-1}(password)\right) = h^{n}(password)$
- If it matches, then server accepts the communication request. If it does not, the server rejects the communication request.
- Once the user has been authenticated, the server needs to update its information.

Part B – Question 2 ...3

Process: (cont...)

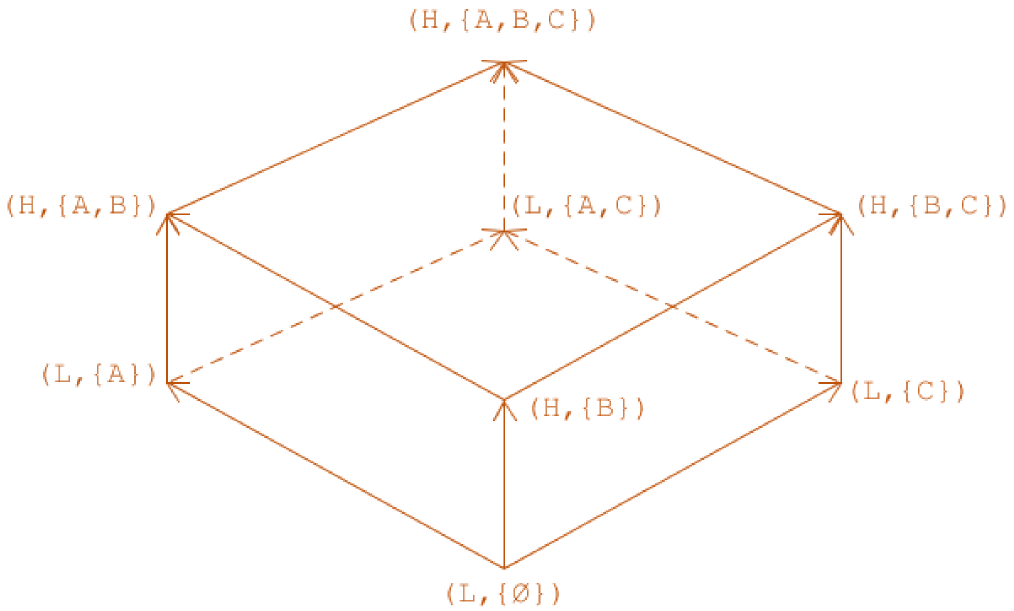
- The system will then replace $x_n = h^n(password)$ with the one-time password sent by the user's, that is, $x_{n-1} = h^{n-1}(password)$.
- The value n is replaced by $n - 1$.
- When n reaches 0, the system will have run out of passwords in the hash chain and will have to run a new setup process, with a new base password.

Part B – Question 2 …4

- Lamport’s one-time password works because the system define p_i to be $H^{n-1}(p)$ where H is a hash function known to all, e.g., MD5() in our Assignment 1. In this way, attacker cannot derive future password from a past password. For example, after p_6, which is equals $H^{n-6}(p)$, the attacker can compute $H(p_6)$, which equals $H^{n-5}(p)$, the already used password p_5. The attacker cannot compute p_7 because p_7 equals $H^{n-7}(p)$, and computing $H^7(p)$ from $H^6(p)$ would require the attacker to computer the inverse of H or to know p, but H is a cryptographic hash function.

Part B – Question 3

3) A company has three departments A, B and C, and has determined that it is appropriate to have two levels of sensitivity, in increasing order: L and H. Draw a BLP lattice system to represent this scenario.



Part B – Question 4 …1

4) Explain what positive validation of user input is and why positive it is important, and usually more appropriate than negative validation of user input. You need to explain what is meant by positive validation and negative validation. Give examples to support your argument.

Positive validation concern a situation where we try to distinguish between authorized and unauthorized entities. A true positive and false positive may be the result of positive validation. A true positive refers to a situation when we make a match, and it is correct. A false positive refers to a situation when we make a match (a positive match) but which is actually not. Positive validation, in particular, a false positive, of user input is important because it affects the false acceptance rate.

Part B – Question 4 …2

A false acceptance rate is the proportion of authentication attempts resulting in false acceptances, which means the number of matches is accepted which we should not.

In a negative validation, of course there are true negative and false negative. A true negative refers to a situation when the match should be rejected and we did. A false negative, on the other hand, refers to a situation when we did not make a match, but we should have. A negative validation, in particular false negative, affects the false rejection rate, which means the number of matches is rejected which we should not.

Part B – Question 5

5) Pharming is considered to be more technical and social engineering than deceptive phishing. Explain how pharming and phishing are related and why this statement is reasonable. You should note both the technical and social engineering aspects of each.

Part B – Question 6

6) Explain how the three classes of IDS attacker: clandestine, masquerade and misfeasor, differ from each other. Give example illustrating how the methods used to detect a masquerade might differ from those used to detect a misfeasor.

Masqueraders are those illegitimate users who are trying to imitate legitimate users while misfeasor are those authorized user who misuse their power.
Clandestine refers to someone who try to avoid the intrusion detection or auditing system.

Part B – Question 7

7) Describe factors used in differentiating between types of malware. Specify the main types of malware and illustrate how those factors apply to them.

Part C – Question 1 …

1. The following questions relate to authentication and access control:
    a. Explain what salting is, where we use it, and why we use it.
    b. Assuming the attacker knows the method we use to choose a password, which of the following two methods of generating a password is better? Justify your answer. In every instance the choosing is uniformly random.
        A. Choosing a six digit number.
        B. Choosing a lower case letter, followed by two digits, followed by an upper case letter, followed by two digits.

Part C – Question 1 …

c. Name and describe two list representations corresponding to an access control matrix. If we want to efficiently determine all the actions available to a subject, which of the two list representation is appropriate and why?

d. Name and describe the two types of error rates that occur in authentication systems.

Part C – Question 1 …

a. Explain what salting is, where we use it, and why we use it.

The “Salt” is a value randomly generated. It is used in hashing where instead of only the password is hashed, the password is combined with the salt and then hashed. The salt it stored somewhere too. This is used so that the adversary have many combination to try the password with many salts and delays the adversary from finding the correct password hash.

Part C – Question 1 …

b. Constructing a password by choosing a seven digit number.

$$Entropy = log_2 N^l$$

$$= log_2 10^6 = 6 log_2 10 = 6 \times \frac{log_{10} 10}{log_{10} 2} = 19.93\ bits$$

$$Complexity\ of\ the\ password = \ 2^{19.93} \approx 998{,}913.34$$

Part C – Question 1 …

B. Constructing a password by choosing a lower case letter, followed by two digits, followed by an upper case letter, and followed by two digits

- One lower case letter: $26^1 = 26$
- One digit: $10^2 = 100$
- One upper case letter: $26^1 = 26$
- Two digits: $10^2 = 100$

$Entropy$

$$= 1 \times \frac{log_{10}(26 \times 100 \times 26 \times 100)}{log_{10}2}$$

$$= 1 \times \frac{log_{10}(6760000)}{log_{10}2} = 22.69$$

$$Complexity\ of\ the\ password = \ 2^{22.69} \approx 6{,}766{,}601.52$$

Part C – Question 1 …

- From the previous computation, it is concluded that method one provide a stronger password. Although the second methods seem more complex, but because the pattern of creating a password is know to an attacker, this actually reduce the entropy of the password, and hence the complexity.

Part C – Question 1 …

c. Name and describe two list representations corresponding to an access control matrix. If we want to efficiently determine all the actions available to a subject, which of the two list representation is appropriate and why?

Access control matrix is used to restrict subject from accessing objects that the subject is not authorized to act on.
Capabilities is from the perspective of subject, and access control list is from the perspective of objects.
If we want to efficiently determine all the available to a subject, the capabilities list is more efficient because capabilities list shows/list all the objects the subject is able to access and the operations/authorization to access those objects.

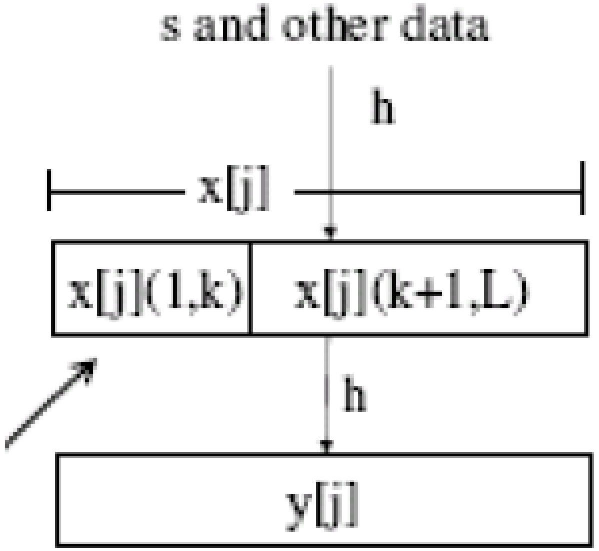
Part C – Question 7 …2

d. Name and describe the two type of error rates that occur in authentication systems.

- The two type of error rates that occur in authentication systems are **False Acceptance Rate (FAR)** and **False Rejection Rate (FRR)**. False Acceptance Rate (FAR) is the proportion of authentication attempts resulting in false acceptances, and False Rejection Rate (FRR) is the proportion of authentication attempts resulting in false rejections.

Part C – Question 2 …1

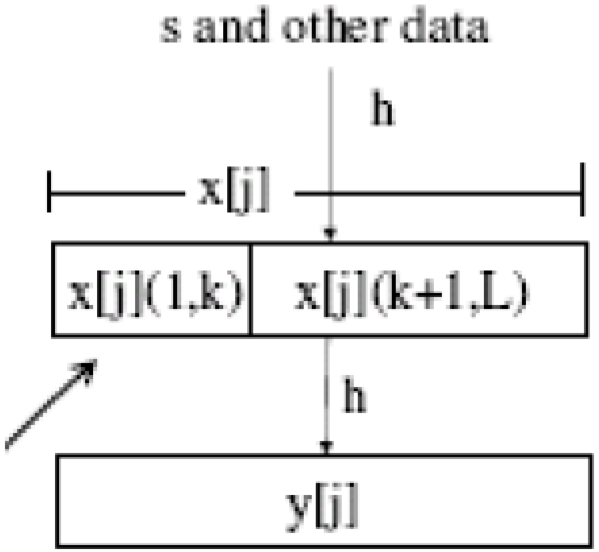
2) Consider the diagram to the right and answer the following questions:
   a. What is the context of this diagram?
   b. What is sent to the client and how is this generated?
   c. What should the client respond with?
   d. What is the role of k?
   e. How much work would we expected the client to do?
   f. Is the answer from the client unique? Justify your answer.



Part C – Question 2 …2

a. What is the context of this diagram?

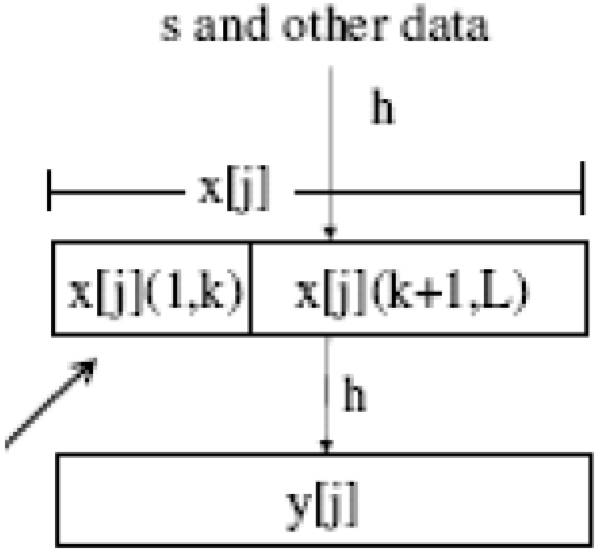
The diagram refers to the construction of client puzzles.



Part C – Question 2 ...3

b. What is sent to the client and how is this generated?

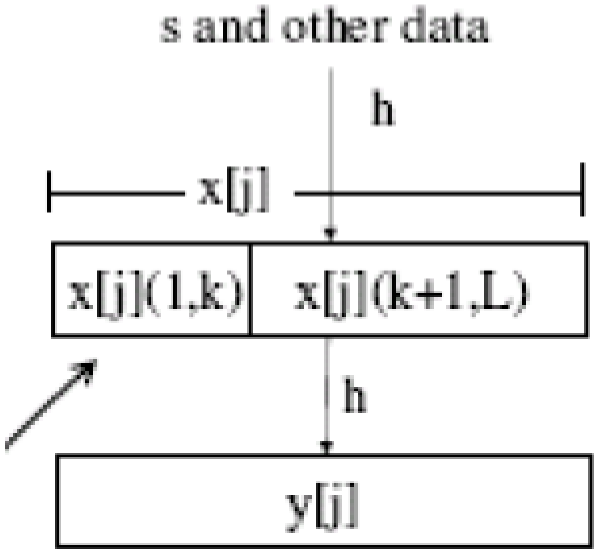
X[j](k+1,L) is sent to the client. This is generated by taking a sub-puzzle and taking k bit as the solution of the puzzle



Part C – Question 2 …4

c. What should the client respond with?

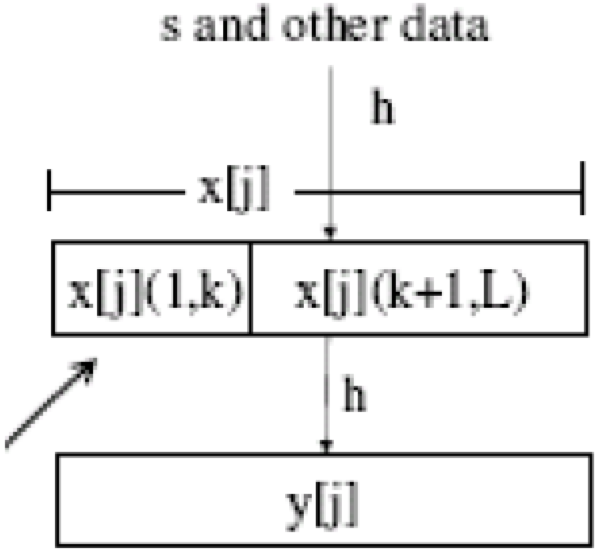
The client should respond with x[j](1,k) to be joined with x[j](k+1,L) to get y[j].



Part C – Question 2 …5

d. What is the role of k?

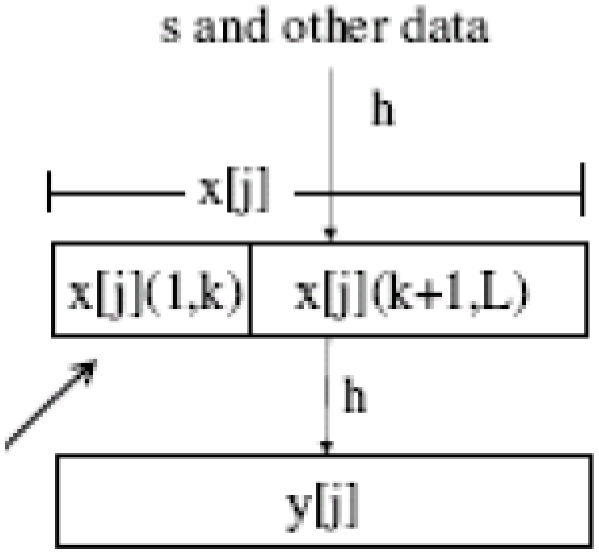
k is the number of bits that are missing from the puzzle. It determines the complexity (efforts) that a client needs to put in to solve the puzzle.



Part C – Question 2 …6

e. How much work would we expected the client to do?

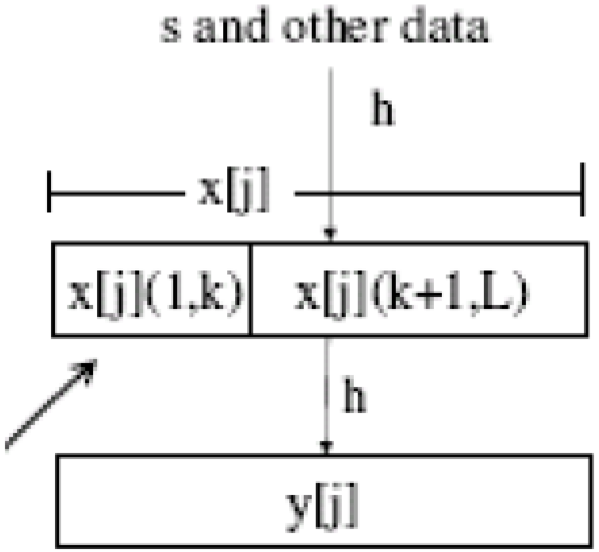
The client is expected to do minimal work so that the authentication can be fast.



Part C – Question 2 …7

f. Is this process stateless? Explain your answer.

Yes, the puzzle stores no information. The solution itself contains all the information the server needs other than their own server secret.



Part C – Question 3

3. The following questions relate to DoS attacks:
    a. What are the possible consequences or damages caused by a DoS attack?
    b. Describe the difference(s) between a quantity attack and a quality attack.
    c. Which DoS attack does Syncookie aim to resist? Briefly describe how Syncookie works.
    d. Describe 2 common techniques use by amplification attacks.

Part C – Question 4

4. Explain what each of the following is/are, explaining the motivation and/or context for each as part of your answer:
   a. Master passwords
   b. CAPTCHA
   c. XSS
   d. TOCTOU

Part C – Question 4 …

a. Master password:

Master password is a single password where all the properties are applied to that password instead of many other passwords that are less secured. Typically it is used as the main password used to protect sensitive information such as other passwords and certificates.

Part C – Question 4 …

c. XSS:

XSS is an abbreviation for cross site scripting. It exploits vulnerabilities in using dynamic web content, in particular, it involves the use of those vulnerabilities to gather data from a user that should not be gathered. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

Part C – Question 4 …

d. TOCTOU

It is an abbreviation for Time Of Check, Time Of Use. It is an attack that targets a race condition occurring between the time of check (state) for a resource and the time of use of the resource. This attack is possible when two or more concurrent processes are operating on a shared file. For example, the first access is a check to verify some attribute of the file, followed by a call to use the file. An attacker can alter the file between the two accesses.

Part C – Question 5

5. The following questions relate to intrusion detection:
   a. Explain the ideas of threshold models in the context of an intrusion detection system. Use a specific example to help in explaining.
   b. The lecture notes describe the 5+1 related goals of intrusion detection, the +1 being assurance. State and briefly describe the 5 goals. For each of those goals, give an example of what may happen if the goal is not met.
   c. What are honeypots? What role do they have in detecting and managing intrusions?

Part C – Question 5

c. What are honeypots? What role do they have in detecting and managing intrusions?

A *honey pot* is a decoy that lures attackers away from production systems. It’s usually a computer attached to the network that runs special software to emulate services, applications, protocols. A honey pot should not contain any data other than the information specifically created to trick the attacker. Nor should it be allowed to connect to any other system except other honey pots, to prevent the attacker from using the honey pot to launch an attack. We can use honeypots to rule the attacker to stay on the system long enough for the administrators to respond to the attack. In this case, the honeypots act as decoys in the intrusion detection and prevention system.

Part C – Question 6

6. This is a collection of mixed questions.
   a. Describe what a timing side-channel attack is, illustrate how it might work, and describe a countermeasure to protect against such timing attacks.
   b. Describe a typical phishing process.
   c. What is Trojan Horse? Describe two distinct methods of identifying a Trojan Horse and explain when and why each of those methods might be appropriate.

Part C – Question 6

b. Describe a typical phishing process.

A typical phishing process involves deception where the user is fooled into believing that there are issue with his account and enter his account details to fix the issue but is actually stored and collected by the phisher to cause harm.

Part C – Question 6 …

c. What is a Trojan Horse? Describe two distinct methods of identifying a Trojan Horse and explain when and why each of those methods might be appropriate.

Trojan Horse are non-replicating program that openly exhibit one desirable behaviour, it might be a game for example, but have some real intent hidden from the user. This real intent could, for example, be to open ports on a machine to allow attackers access. A Trojan horse renames itself to the name of a valid system file. It can also be encrypted and polymorphic, and could install themselves in different ways to escape detection.

Part C – Question 6 …

Two methods of detecting Trojan Horses:

- Monitoring – Make use of virus monitors to monitor known methods of virus activities, such as attempts to write to a boot sector, modify interrupt vectors, write to system files, etc. and detect abnormal behaviour of the system. This technique is able to detect the Trojan Horse before complete infection. The disadvantages is that to detect a high percentage of viruses, the sensitivity of the monitor must be set high and this may generate many false alarms.

Part C – Question 6 …

Two methods of detecting Trojan Horses: (cont…)

- Signature scanning – the simplest and the most common approach to virus detection. With this technique, signature extraction is a non-trivial process. The infection is disassembled and the key portions are identified. Next, the key portions are combined to form a signature. The signature is then checked against a large library of programs to reduce the chance of false positives occurring when signature accidentally matches some library code. The advantage of this technique is that other than detecting Trojan Horse, it can also be used to detect logic bombs and other malicious software. The disadvantage is that scanning cannot find new viruses before their patterns are known. In addition, this technique is also ineffective against polymorphic viruses.

Part C – Question 7

7. This is a collection of mixed questions.
   a. Name and describe two methods of protecting, at the query level, against inferential attacks in statistical interfaces. For each of those methods describe a potential problem.
   b. Describe two distinct scenarios or applications domains where we may use reverse engineering for legitimate and distinct purposes. Be sure to explain how reverse engineering may help.
   c. A Biba based system is used in some Windows operating systems. What purpose does it’s use serve and why would a BLP based system be inappropriate?

Part C – Question 7 …6

a. Name and describe two methods of protecting, at the query level, against inferential attacks in statistical interfaces. For each of those methods describe a potential problem.

   i. Try to design a database in such a way that inferences is reduced.

   ii. Attempt to reject specific/sequence of queries which may lead to inference attack.