Part B – Question 1 …1

1) Briefly explain the three basic components in an access control triplet. Describe how these triplets relate to an ACM. Give an example of an ACM, and the two related representations based on it, to illustrate your answer.

The three basic components of access control triplets are (S, O, A) where

- S: a set of subjects
- O: a set of objects
- A: an access control matrix, A[S, O] with entries a(s,o)

Part B – Question 1 …2

- A triplet describes the state and state transitions of an access control matrix (ACM).
- The following is one example of an access control matrix

Part B – Question 2 …1

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

- 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.

Part b – Question 3 …1

3) Consider a BLP lattice system with multilevel classifications $C = \{X, Y\}$ and multilateral categories $K = \{A, B\}$. Sketch a diagram to illustrate the relationship between the security levels in this system. Explain, with reference to your diagram, the concept of partial ordering. State the BLP rule and give an example, based on your diagram, to explain each aspect of it.

Part B – Question 4 …1

4) Describe the relevance of the Principle of Least Privilege in the context of Buffer Overflows. You will need to briefly explain the Principle and the possible relevant effects of Buffer Overflows, but not the details of Buffer Overflows themselves.

- Principle of least privilege in the context of buffer overflow is that we limit the access an attacker can have hence even if he identify a way to launch a buffer overflow attack. Effect of buffer overflow would be that the attacker may install a malicious code and then input the address of the code to the return address of the program, hence when the actual program returns, it actually runs the malicious code.

Part B – Question 5 …1

5) Briefly explain the difference between logging and auditing. Describe two specific considerations when determining what should be logged and audited, and explain how they may influence your decisions.

- Logging is recording of events or statistics to provide information of the system use, misuse and performance. Auditing is the analysis of the log events provided by logging and to provide the information of the system in a more readable and understandable manner. The two considerations are, we need to consider how the attempts that violate the security policies can be made and we need to consider how to detect those attempts. This may influence my decision as there is no point of detecting a problem if we do not know the indicating effect.

Part B – Question 6 …1

6) Garfinkel stated … “Something you had once, something you’ve…, or something ….”. Complete the quote and explain the significance of it, in particular of this version.

Something you had once, something you have **known**, or something **you are**.

Part B – Question 7 … 1

7) Describe two general “good practices in coding”. For each of these explain why they are appropriate and give an example of what could go wrong if that practice is not followed.

The two general “good practices in coding” are:

- Never store secret in code
- Set default to deny instead of default to allow.

Part B – Question 1 …1

1) Describe the three main bases of authentication. Give an example of each. Describe an advantage and a disadvantage of each, either generally or for the specific example given.

The three main bases of authentication are:

- **Something you know**, e.g., password. Advantage of this base is a user can set his/her own desired password. The disadvantage is that password can be forgotten.
- **Something you have**, e.g., a “device” or key card. Advantage of this base is that authentication is easy. The disadvantage is the device may be lost.

Part B – Question 1 …2

- Something you are, e.g., fingerprint or any other biometric data. The advantage is this token cannot be lost or forgotten. The disadvantage is that the body part that is associated to the biometric information may be damaged, for example, finger may be accidentally cut (injured), and hence may affects the fingerprint.

Part B – Question 2 …1

2) Describe the use of access control matrices and how they relate to capabilities and access control lists. Give an example to illustrate your explanation.

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.

Part B – Question 2 …2

Access control matrix:

	x	y	z	
Alice		rw	r	e
Bob		r	rw	

Access control list:

x : (Alice, rw), (Bob, r)

y: (Alice, r), (Bob, rw)

z: (Alice, x)

Capabilities:

Alice: (x, rw), (y, r), (z, e)

Bob: (x, r), (y, rw)

Part B – Question 3 …1

3) Explain what a Trojan Horse is. 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 B – Question 3 …2

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 B – Question 3 …3

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 B – Question 4 …1

4) Name and describe the two types of errors that occur in authentication systems and in intrusion detection systems. Give an example of each. Explain how the interpretation of each differs between authentication systems and intrusion detection systems.

Part B – Question 4 …2

False negative and false positive.

From authentication perspective, false negative and false positive concerns the likelihood of getting a result which is wrong, that is, an invalid user but falsely identify as valid (false negative) and a valid user but falsely identify as invalid (false positive). From intrusion detection perspective, false negative is when we do not make a match, but we should have, that is, there is an intrusion take place, but the system did not manage to identify/recognize it. A false positive is when make a match, but we should not have, that is, the system identify an intrusion, which is actually not.

Part B – Question 5 …1

5) A company has two department, A and B and has determined that it is appropriate to have three levels of sensitivity, in increasing order X, Y and Z. Draw a BLP lattice system to represent this scenario. Using examples, explain the three BLP rules, 2 mandatory and 1 discretionary.

ss-property only can read below, *-property only can write up, ds-property – permission may be passed from an authorised person to a another, level authorized person

Part B – Question 6 …1

6) In the third assignment for this subject you looked at detecting intrusions in an event based scenario. An example of the information your program was to initially generate was a follows:

Event	Average	Stdev	Weight
Logins	4.50	1.25	2
Total time online	287.15	42.12	1
Emails sent	65.40	30.71	1
Orders processed	150.73	20.13	1
Pizza’s ordered online	2.03	1.06	0.5

Part B – Question 6 …2

Explain what each of these columns represent. How such values would be generated in practice, and how they are used in the detection of intrusions. You do not need to give numerical calculations but if it helps you to explain you can.

- The first column, “Event” contains the list of events being monitored.
- The second column, “Average” contains the average or mean that a particular event has under a normal situation.
- The third column, “Stdev” contains the standard deviation a particular events may be deviated from the mean. This can be the basis for specifying an anomaly, e.g., a measure as being more than a certain number of standard deviations away may be identified as anomaly.
- The fourth column, “weight” contains a factor to adjust the important or criticality of an event to the intrusions to be identified.

Part B – Question 7 …1

7) Explain what tailored attacks are. Give some specific examples in two different domains and explain how they perform relative to other attacks in those other domains.

Tailored phishing attack is where the attack is done on all people who are known to be customers to a particular banks etc. it is similar to tailored dictionary attack where we use what we know about the person to increase the likelihood of successful attack.

Part B – Question 1 …1

(SIM-2016-S3-CSCI262-S9b, slides 16 – 28)

1) Explain what inference is in the context of statistical databases. Explain the difference between direct and indirect attacks, using appropriate examples. Describe one method of protecting against inferential attacks against statistical interfaces and a potential problem with that method.

   Inference means the derivation of sensitive information from non-sensitive, typically aggregate, data.

   Direct attack is an attack where the aggregates are over small enough samples that information about individual elements of data can be obtained. Indirect attack is an attack where information external sources is combined with the results of aggregate queries.

Part B –Question 1 …2

An example of direct attack is an average salary of all employees older than 60 discloses an exact value of salary if exactly one employee older than 60 is employed.

An example of indirect attack is that we know, independent of the database, who lives in which suburb and who is a member of which department, the query …

```
SELECT SUM(SALARY), COUNT(*)
FROM EMPLOYEE
WHERE GROUP BY DEPTNAME, SUBURB;
```

… may then disclose the salaries of the employees who are the only people employed in a department and living in a particular suburb.

Part B – Question 1 …3

- One of the method of protecting inference attack is to design the database in such a way that inference is reduced. This approach removes an inference channel by altering the database structure or by changing the access control regime to prevent inference. One potential problem with this technique is the unnecessarily stricter access controls that may reduce availability.

Part B – Question 2 …1

2) Explain why positive validation of user input is important, and usually more appropriate than negative validation of user input. 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 2 …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 3 …1

3) Part of your first assignment related to implementing a form of two factor authentication. Explain how such authentication works, generally and in the example modelled in the assignment. Specify carefully the requirements of the “device”.

Two-factor authentication implies the use of two independent means of evidence, such as a password or PIN and a device which is able to provide one-time type passwords, to assert an entity. This two-factor authentication system is based on smartcard technology and is successor to the old sign the imprint of the card type mechanism or swipe the magnetic stripe.

Part B – Question 3 …2

- The assignment simulates an authentication process using two factors. The first factor is the password, which is something one knows, and the second factor is the device, which is something one has. The authentication process works as follows:
  - To connect to a server, the server requests the user to present some evidence of his/her identity such as userid, and a one-time password that is generated by a device that the user has. (In the assignment, the device was simulated using a program.)
  - From the device, the user gets the one-time password and enters the one-time password together with a userid to complete the authentication.

Part B – Question 3 …3

- Upon receiving the one-time password and the userid from the user, the server will generate another one-time password based on the userid and the device id that was associated to the user. If this one-time password matches, the connection request is established, otherwise the connection request is rejected.

- The two-factor authentication seeks to decrease the probability that the requestor (in our example, the user) is presenting false evidence of its identity. For example, if the user does not possess the device, the user cannot generate the required one-password and hence the server cannot authenticate the user correctly.

Part B – Question 4 …1

(SIM-2016-S3-CSCI262-S4a, SIM-2016-S3-CSCI262-S4b)

4) There are various methods of protecting against denial of service attacks. Syncookies are a specific method while client puzzles describe a general protection methodology. Explain how syncookies and client puzzles are similar, and how they differ. Describe the main properties desirable for client puzzles. Use examples as appropriate.

   Both are used as countermeasures to TCP SYN flooding attack. Syncookies avoid dropping connections when the SYN queue fills up. Severs uses a carefully constructed sequence number in the second message but discards the SYN queue entry. If the Server receives a “correct” ACK from the client, the Server can reconstruct the SYN queue entry and then connection proceeds as usual.

Part B – Question 4 …2

- As for the Juels and Brainard Client puzzles, puzzles will be presented when the Server detects a possible attack. When there is no evidence of a denial of service attack taking place, the Server accepts connections normally. However, when an attack on the Server is detected, perhaps through an intrusion detection system, the Server accepts connections selectively using puzzles.
- A client puzzle could be a cryptographic problem formulated using time and a server secret. The client needs to submit the correct solution to gain a connection. To be sure that very little work is required before the appropriate response is received, the generation of puzzle should not be too difficult and solving the puzzle should not be too tough either.

Part B – Question 4 …3

- One particularly important aspect of creating client puzzle is the flexibility and scalability. It is recommended that we treat the client puzzle as a number of independent sub-puzzles. The sub-puzzles may have different difficulties. With multiple sub-puzzles, we are able to maintain the total expected difficulty the same to that of a single puzzle and keep the standard deviation low.

Part B – Question 5 …1

5) A company has two department, A and B, and has determined that it is appropriate to have three levels of sensitivity, in increasing order: X, Y and Z. Draw a BLP lattice system to represent this scenario. Using examples, explain the three BLP rules, 2 mandatory and 1 discretionary.

Part B – Question 6 …1

6) Explain the ideas of threshold models and statistical models in the context of an intrusion detection system. Give a specific example of applying a threshold. Explain the idea of data aging in the context of the statistical models.

Part B – Question 6 …2

Statistical model for anomaly detection is where statistic of past data is used to detect the anomaly and threshold model which is the simplest statistical model is where an alarm is triggered if more than the certain number of something happened or less than the certain number of something is happened. An example is login event. If there is more than 5 login per day, an alarm may be raised. We should not heavily rely on old statistic. If we are accumulating data over a period of time and taking it all into account, we should weight the data as a function of time.

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.

- 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 $p_1, p_2, \ldots p_n$.

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...)

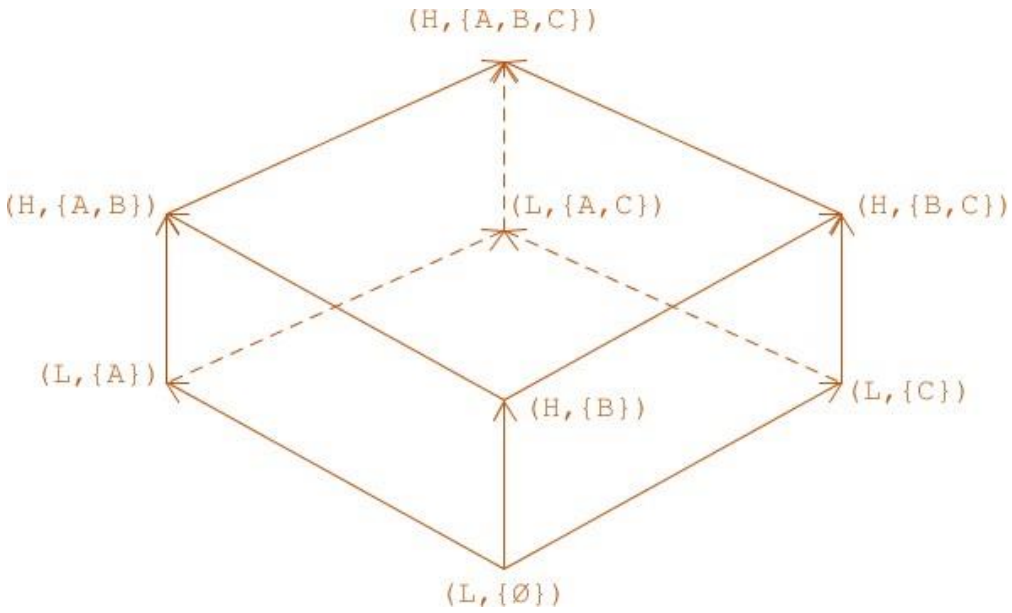
- The system will then replace $x_n = h^n(password)$ with the one-time password sent by the user's, that is, $x_{n-1} = h^{n-1}(password)$.
  - The value n is replaced by $n - 1$.
  - When n reaches 0, the system will have run out of passwords in the hash chain and will have to run a new setup process,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

1) For each of the following CWE's, explain what the problem is and the potentials 'bad thing' that could happen
   a. CWE-307: "Improper restriction of excessive authentication attempts."
   b. CWE-759: "Use of a One-Way Hash without a salt."
   c. CWE-306: "Use of Hard-coded Credentials."
   d. CWE-131: "Incorrect Calculation of Buffer Size."

Part C – Question 1 …2

a. CWE-307: “Improper restriction of excessive authentication attempts.”

   The problem is where there is not enough authentication restriction is being placed. If no restriction are placed then the attacker can use unlimited attempts to break the password.

Part C – Question 1 …3

b. CWE-759: “Use of a One-Way Hash without a salt.”

The problem is where salt is not used in hashing which makes the hash less secure. if salt is not used the adversary can just hash all the possible passwords and compare to break the password.

Part C – Question 1 ...4

c. CWE-306: “Use of Hard-coded Credentials.”

The problem is where sensitive credential like passwords are hard coded into the software used for internal authentication. This creates a loophole for the adversary to bypass the authentication process.

Part C – Question 1 ...5

d. CWE-131: “Incorrect Calculation of Buffer Size.”

The problem is where the buffer size of program is not computed properly the information is leaked out of bound of the buffer. This may cause buffer overflow where an adversary can place a malicious address in place of the return address to run the malicious code.

Part C – Question 2 …1

2) The following questions cover a range of topics:
   a. Sketch the process used within a state machine based security model to prove the security of an access control system.
   b. What is IDIP and what purpose does it serve? Explain briefly how it works.

Part C – Question 2 …2

c. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
    State = combine(state, container[i]);
```

A

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
    State = combine(state, container[i]);
```

Part C – Question 2 …3

a. Sketch the process used within a state machine based security model to prove the security of an access control system.

Part C – Question 2 ...4

b. What is IDIP and what purpose does it serve? Explain briefly how it works.

IDIP is known as Intrusion detection and isolation protocol is to stop an attack by blocking the connection. It works by detecting an attack and blocking the connection to the target from the source and inform the previous node about the attack which then blocks the connection and inform its previous node until which the connection is block from the source to the target.

Part C – Question 2 …5

c. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
    State = combine(state, container[i]);
```

B

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
    State = combine(state, container[i]);
```

Part C – Question 2 …6

Program A is defensive programming. Defensive programming is to guard against unexpected errors, but defensive programming is different from error handling. If a public variable is to accept and store integer, and you check if the value is integer is error handling as we know beforehand. If a private variable is to accept and store an integer and a program function is used to store the value and check are in place to make sure it is integer is defensive programming. Program A is defensive programming as the for loop is checking for I < elements, and as long as this condition is satisfied, the loop will run and eventually terminate, but program B has I != elements. There is a possibility that I is larger than elements outside the code hence it will lead to an indefinite loop.

Part C – Question 3 …1

3) The following questions relate to access control and authentication:
   a. What is the primary assumption we make about analysing the strength of a method of choosing a password? Why do we make this assumption?
   b. Based on your assumption from previous question, 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 five digit number.
      B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 3 …2

c. What does the “No write up” rule in the context of Biba imply? Give a simple example to illustrate your answer.
d. Should the password strength for an account be tied to the clearance level of a user? Justify your answer.

Part C – Question 4 …1

4) These questions relate to a variety of topics:
   a. What is honeypot?
   b. What role might a honeypot play in the detection and management of instructions?
   c. Give an example to illustrate how particular data within a real system might be considered to be a honeytoken.
   d. Explain why an when it is a bad idea to seed a random number generator with time only.
   e. What is XSS and what does it exploit?

Part C – Question 4 …2

a. What is honeypot?

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.

Part C – Question 4 …3

b. What role might a honeypot play in the detection and management of instructions?

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 4 ...4

c. Give an example to illustrate how particular data within a real system might be considered to be a honeytoken.

A honey token is a non-computer honeypot. Example fake data in database. This fake data are similar to the real data but to encourage the attacker to be in the system long enough to respond to the attack.

Part C – Question 4 ...5

d. Explain why an when it is a bad idea to seed a random number generator with time only.

It is a bad idea if the random number generator is used to generate password. This is because if the adversary knows the approximate time the password was generated, then the adversary can execute the random number generator a period of time frame close to the actual time and may obtain the random password.

Part C – Question 4 ...6

e. What is XSS and what does it exploit?

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 5 …1

5) One of the client puzzles we considered contained the statement h(C, Ns, Nc, X) = 000…000Y.
   a. Describe each of the components in the expression above.
   b. How does the selection of Ns and Nc differ, and what significance does this have?
   c. How much work is required to “solve” the puzzle, in the context of this statement?
   d. Explain how the puzzle would differ if the right hand side of the statement was Y000…00 rather than 000…000Y?
   e. Describe how we could modify this to generate sub-puzzles.
   f. What does the term resource disparity refer to in the context of puzzles?

Part C – Question 6 …1

6) These questions relate to a variety of topics:
   a. Describe how virus and worm propagation differs.
   b. How does a stateful inspection firewall differ from the traditional packet filters?
   c. Describe a typical phishing process.
   d. Explain the role a sandbox might play in the detection and analysis of malware.

Part C – Question 6 …2

a. Describe how virus and worm propagation differs.

   Virus propagate by manual transferring of infected files while worm propagate using only network connection.

Part C – Question 6 …3

b. How does a stateful inspection firewall differ from the traditional packet filters?

   Stateful inspection firewall allows a more dynamic structure such as authentication is required before an “allow” entry for a particular connection while traditional packet only deal with individual packets.

Part C – Question 6 ...4

c. 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 ...5

d. Explain the role a sandbox might play in the detection and analysis of malware.

sandbox plays an import role as if a software is suspected that to be a malware and it is a malware, the vector of damage caused by the infection is limited to that vector and it cannot affect the main environment keeping the main environment safe.

Part C – Question 7 …1

7) These question relate to inference:
   a. Describe and give examples of two different types of disclosure we might want to avoid in the context of a statistical database.
   b. Explain the difference between direct and indirect attacks. Use an example to assist in your explanation.
   c. 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.

Part C – Question 7 …2

a. Describe and give examples of two different types of disclosure we might want to avoid in the context of a statistical database.

The two types of disclosure are:

i. Disclosure of exact data, for example, Adam is 27 years old.
ii. Disclosure of bound, for example, Adam is younger than 30 years old.

Part C – Question 7 …3

b. Explain the difference between direct and indirect attacks. Use an example to assist in your explanation.

Direct attack is an attack where the aggregates are over small enough samples that information about individual elements of data can be obtained. Indirect attack is an attack where information external sources is combined with the results of aggregate queries.

Part C – Question 7 ...4

An example of direct attack is an average salary of all employees older than 60 discloses an exact value of salary if exactly one employee older than 60 is employed.

An example of indirect attack is that we know, independent of the database, who lives in which suburb and who is a member of which department, the query …

```
SELECT SUM(SALARY), COUNT(*)
FROM EMPLOYEE
WHERE GROUP BY DEPTNAME, SUBURB;
```

… may then disclose the salaries of the employees who are the only people employed in a department and living in a particular suburb.

Part C – Question 7 …5

- One of the method of protecting inference attack is to design the database in such a way that inference is reduced. This approach removes an inference channel by altering the database structure or by changing the access control regime to prevent inference. One potential problem with this technique is the unnecessarily stricter access controls that may reduce availability.

Part C – Question 7 ...6

c. 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.

Part C – Question 1 …1

1) One of the client puzzles we considered contained the statement $h(C, Ns, Nc, Y) = 000 \ldots 000X$.
   a. Describe each of the components in the expression above.
   b. How much work is required to “solve” the puzzle, in the context of this statement?
   c. What is the purpose of such a puzzle?
   d. Describe how we could modify this to generate sub-puzzles.
   e. What advantage do we obtain by using many sub-puzzles rather than just one single large puzzle?

Part C – Question 2 ..1

2) These questions relate to intrusion detection systems:
   a. Explain the difference between masqueraders and misfeasors.
   b. Explain the difference between anomaly detection and misuse based detection. Give an example to help illustrate each.
   c. Explain what Unified Threat Management Systems are. Given an advantage and a disadvantage of using one.

Part C – Question 2 ..2

a. Masqueraders are those illegitimate users who are trying to imitate legitimate users while misfeasor are those authorized user who misuse their power.

Part C – Question 2 ..3

b. Anomaly detection refers to detection where observed behaviour differs from a typical behaviour of a user while misuse based detection refers to detection where observed behaviour indicates an attempt to inappropriately use resources.

An example of anomaly detection: A particular user, let's say user A logs in only on week days, but suddenly user A logs in on Sunday mid-night for three different occasions.

An example of misuse based detection: A user trying to access resources that her or she is not authorized to.

Part C – Question 2 ..4

c. Unified Treat Management System is a system where different threat management services like anti-virus, firewall, intrusion prevention, intrusion detection etc. features unified together. Advantage of Firewall: Can filter out packet based on the rules, Disadvantage: Firewall cannot prevent attack those bypass the firewall like internal attackers or connection that bypass the firewall like VPN.

Part C – Question 3 …1

3) These questions relate to malware and problematic code:
   a. Describe how virus and worm propagation differs.
   b. Describe the difference between direct action and memory residence.

Part C – Question 3 …2

a. Virus propagates on the manual transfer of virus infected files while work propagate using network connection.
b. Viruses install themselves into the memory of the host computer when the original virus program is executed. Even when the original virus program is closed, new object can still be infected without having to run anything else. These are called memory residence. Direct action viruses are only active when an infected object is active.

Part C – Question 3 …2

c. Consider the following piece of code and answer the subsequent questions. Assume x is a private key w-bits bong. The $function\ modexp(s[k], y, n)$ involves determining the result of raising $s[k]$ to the power of y, and taking $mod\ n$ of the result.

```
s[0] = 1;
for ( k=0; k<w; k++) {
    if ( x[k] == 1)
        R[k] = modexp(s[k], y, n);
    else
        R[k] =  s[k];
    s[k+1] = R[k]*R[k] mod n
}
return R[w-1];
```

i. What attack is the code vulnerable to?
ii. Explain how you would carry out such an attack.
iii. Explain how you could protect against such an attack.

Part C – Question 4 …1

4) Explain briefly what potential problem and domain each of the statements or code fragments is associated with, and what a likely effect would be. The syntax may not be precise.
   a. For k while for k
   b. strcpy (variable, “Polymorphic”);
   c. int N; cin << N; new char[N];
   d. system(user_input);

Part C – Question 5 …1

5) The following questions cover a range of topics:
   a. One major component of access control representations is the grouping together of entities. Explain why this is done and give examples illustrating two significant but distinct types of grouping that are possible.
   b. Explain what salting is, where we use it, and why we use it.
   c. Would Biba or BLP be more appropriate for protecting a file system against unauthorized modification of data? Justify your answer.

Part C – Question 5 …2

a. One major component of access control representations is the grouping together of entities. Explain why this is done and give examples illustrating two significant but distinct types of grouping that are possible.

Grouping is where the user are place into a group. Permission granted to a group will allow the users of that group to enact that right.

Two distinct grouping may be “Employee” and “Non-Employee”.

Part C – Question 5 …3

b. 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 5 …4

c. Would Biba or BLP be more appropriate for protecting a file system against unauthorized modification of data? Justify your answer.

Biba is more appropriate as it is an integrity based access control model. The policy of Biba is “No write up, No Read Down”. Hence a subject of a low level cannot modify “write” to an object of higher level.

Part C – Question 6 …1

6) The following questions cover a range of topics:
   a. CWE/SANS classify the top problems into three categories: Insecure interaction between components, risky resource management and porous defences. Name and briefly describe an example from each of these categories.
   b. Explain what buffers, buffer overflows and shell coding are. Use an example to illustrate how they are related.
   c. What is the aim of inference, in the context of statistical databases?

Part C – Question 6 …2

a. Examples:
   - Insecure Interaction with components
     - Injection, XSS etc.
   - Risky Resource Management
     - Buffer overflow, limited pathname restriction, uncontrolled format string
   - Porous Defences
     - Missing or incorrect authentication or authorization, no encryption

Part C – Question 6 ...3

b. Explain what buffers, buffer overflows and shell coding are. Use an example to illustrate how they are related.

In computing, a buffer is a memory location where data is stored. Buffer overflow is an effect where data is not limited by bounds of its allocated memory and overflows to other memory location. Shell coding is insertion of own code into the buffer.

How buffer, buffer overflow and shell code are related is best described using the following example. A buffer stores data but if an inefficient function such as strcpy() is used, the function does not check for bound and it may overflow into other memory location. If the return address of the program is found, an adversary may insert his/her malicious code in place of the return address and when the program hits to the return address, the malicious code is executed.

Part C – Question 6 ...4

c. What is the aim of inference, in the context of statistical databases?

The aim of inference is to derive sensitive data from non-sensitive data such as aggregated data. By doing a sequence of aggregated queries it is possible to find the value of the sensitive data.

Part C – Question 7 …1

7) The following questions cover a range of topics:
   a. How do two-channel and two-factor authentication differ?
   b. Describe a typical phishing process.
   c. Explain one example to illustrate the role of sandbox environments in the security of mobile code or in the detection of malware.
   d. Briefly describe how the three primary components of a virus are related.

Part C – Question 7 …2

a. How do two-channel and two-factor authentication differ?

In two factor authentication, the authentication system uses password/pin and a device (token system) which is able to produce one time password. In two-channel authentication, two different channels are used; one channel is from the client to the server and the second channel is from server to client using a different channel e.g. telephone etc. to give targeted authentication

Part C – Question 7 …3

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 7 …4

c. Explain one example to illustrate the role of sandbox environments in the security of mobile code or in the detection of malware.

Sandbox plays an import role as if a software is suspected to be a malware and it is a malware, the vector of damage caused by the infection is limited to that vector and it cannot affect the main environment keeping the main environment safe.

Part C – Question 7 …5

d. Briefly describe how the three primary components of a virus are related.

The three components of a virus are infection vector, payload and trigger. The infection vector is the structure of the virus allowing it to duplicate, payload is what the virus does beside spreading and trigger is the condition which the virus has to meet to activate the payload.

Part C – Question 1 …1

1) For each of the following CWE's, explain what the problem is and the potential "bad thing" that could happen.
   a. CWE-89: "Improper Neutralization of Special Elements used in an SQL Command"
   b. CWE-190: "Integer Overflow or Wraparound."
   c. CWE-131: "Incorrect Calculation of Buffer Size."
   d. CWE-306: "Missing Authentication for Critical Function."
   e. CWE-807: "Reliance on Untrusted Inputs in a Security Decision."

Part C – Question 2 …1

2) The following questions cover a range of topics:
   a. 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.
   b. Describe the base rate fallacy problem. Explain where it is likely to occur, why it occurs, and what the potential effect is. Sketch an example to explain your answer. You do not need to give or use the formula in answering this question.
   c. Describe how virus and worm propagation differs.

Part C – Question 2 …2

- Viruses infect files on the infected host, or in the boot area, to help aid replication.
- Worms replicate themselves to spread with minimal user interaction. Worms typically use widely available applications such as email to spread.

Part C – Question 2 …3

3) These questions relate to a variety of topics:
   a. What are honeypots? What role do they have in detecting and managing intrusions?
   b. What is XSS and what does it exploit?
   c. What are race conditions? Use an example to help your explanation
   d. 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.

Part C – Question 3a ...1

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.

Part C – Question 3a …2

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

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 3b …1

What is XSS and what does it exploit?

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 3c …1

What are race conditions? Use an example to help your explanation

A race condition is a situation in which two or more threads or processes are reading or writing some shared data, and the final result depends on the timing of how the threads are scheduled. Race conditions can lead to unpredictable results and subtle program bugs. A thread can prevent this from happening by locking an object. When an object is locked by one thread and another thread tries to call a synchronized method on the same object, the second thread will block until the object is unlocked.

Part C – Question 3c …2

What are race conditions? Use an example to help your explanation

Classical example of Race condition is incrementing a counter.

Incrementing a counter is not an atomic operation and can be further divided into three steps like read, update and write. If two threads try to increment count at a same time and if they read the same value because of interleaving of read operation of one thread to update operation of another thread, one count will be lost when one thread overwrite increment done by other thread.

Part C – Question 3d …1 (SIM-2016-S3-CSCI262-S6a)

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 3d …2

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 3d …2

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 4 ..1

4) The following questions relate to access control and authentication:
   a. Describe in detail how the one-time password system of Lamport works.
   b. Consider the following statements and answer the subsequent questions:

      Alice can jump fences and climb walls.

      Bob can paint fences, paint walls and roll barrels.

      Chris can climb walls and climb barrels.

      Dan can paint barrels and push Bob.

      i. What are the subjects, objects and actions for this scenario?

      ii. Draw an access control matrix for this scenario. Name and give an example of each of the list representations. Be sure to label all parts of your answer.

Part C – Question 4.2

c. 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 seven digit number.

B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 4 ...3

a. 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 $p_1, p_2, \ldots p_n$.

Part C – Question 4 ...4

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 C – Question 4 ...4

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 C – Question 4 ...5

- 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 C – Question 4 ...6

b. Consider the following statements and answer the subsequent questions:

   Alice can jump fences and climb walls.

   Bob can paint fences, paint walls and roll barrels.

   Chris can climb walls and climb barrels.

   Dan can paint barrels and push Bob.

   i. What are the subjects, objects and actions for this scenario?

   ii. Draw an access control matrix for this scenario. Name and give an example of each of the list representations. Be sure to label all parts of your answer.

Part C – Question 4 ...7

Subject: Alice Bob Chris Dan

Object: Fence Wall Barrel Bob

Actions: Jump Climb Paint Roll push

Control Access Matrix:

Object / Subject	Fence	Wall	Barrel	Bob
Alice	Jump	Climb		
Bob	Paint	Paint	Roll	
Chris		Climb	Climb	
Dan			Paint	Push

Access Control List:

Fence: (Alice, jump), (Bob, paint)
Wall: (Alice, climb), (Bob, paint), (Chris, climb)
Barrel: (Bob, roll), (Chris, climb), (Dan, paint)
Bob: (Dan, push)

Part C – Question 4 - 8

c. 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 seven digit number.

B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 4 ...9

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

$$Entropy = log_2 N^l$$

$$= log_2 10^7 = 7log_2 10 = 7 \times \frac{log_{10} 10}{log_{10} 2} = 23.25\ bits$$

$$Complexity\ of\ the\ password = \ 2^{23.25} \approx 9{,}975{,}792.32$$

Part C – Question 4 ...10

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

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

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

$$= 1 \times \frac{\log_{10}(676000)}{\log_{10}2} = 19.37$$

$$Complexity\ of\ the\ password = 2^{19.37} \approx 677{,}565.08$$

Part C – Question 4 ...11

- 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 5 …1

5) These questions relate to a variety of topics:
   a. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You will need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
        state = combine(state, container[i]);
```

B

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
        state = combine(state, container[i]);
```

Part C – Question 5 …2

b. Various Windows operating systems make use of a Biba-based system. Explain why it would be inappropriate for them to use BLP-based system for similar purposes?
c. What is the relevance of the return address in the context of buffer overflows?
d. Briefly explain the purpose of polymorphism in virus construction, using an example to illustrate what happens in polymorphic viruses. (SIM-2016-S3-CSCI262-S6a, pg 41)
e. How does a security audit trail differ from a security audit? (SIM-2016S3-CSCI262-S8a,

Part C – Question 5 …3

- Program A is defensive programming. Defensive programming is to guard against unexpected errors, but defensive programming is different from error handling. If a public variable is to accept and store integer, and you check if the value is integer is error handling as we know beforehand. If a private variable is to accept and store an integer and a program function is used to store the value and check are in place to make sure it is integer is defensive programming. Program A is defensive programming as the for loop is checking for I < elements, and as long as this condition is satisfied, the loop will run and eventually terminate, but program B has I != elements. There is a possibility that I is larger than elements outside the code hence it will lead to an indefinite loop.

Part C – Question 6 …1

6) These questions relate to a variety of topics.
   a. Describe one of the three “normal system behaviour” characteristics of Denning.
   b. Explain the relevance of false positives and false negatives in the context of intrusion detection. Give an example of each.
   c. Explain why each of the following rules might or might not be used in limiting password choices.
      I. A minimum length of password of 10 characters.
      II. Must be based on an uncommon dictionary word.
      III. At lease one alphabetical, one numerical and one special character.
      IV. Password changes every 50 days.
      V. Password changes no more than every 10 days.

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.

$$Entropy = log_2 N^l$$

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

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

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.

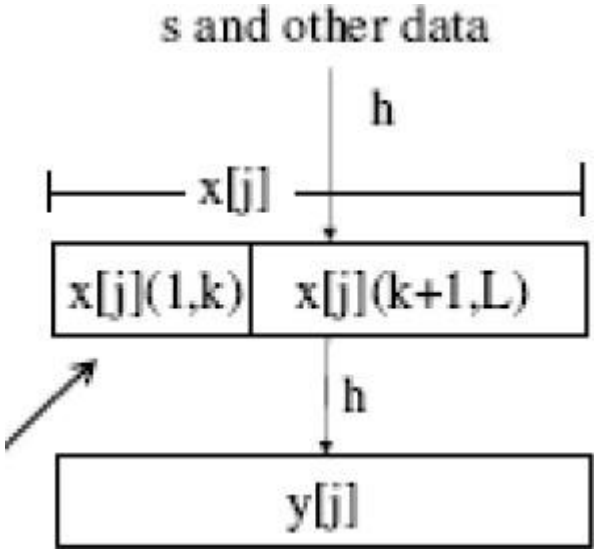
Part C – Question 7 …2

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

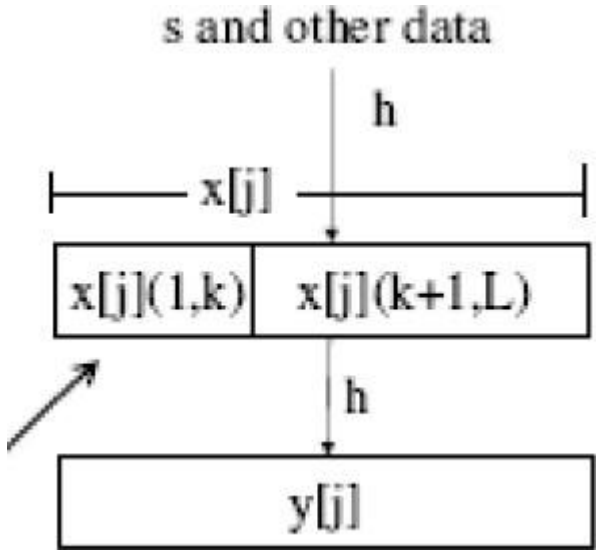
2) Consider the diagram to the right and answer the following questions:
   a. What is the context of this diagram?
   b. What is sent to the client and how is this generated?
   c. What should the client respond with?
   d. What is the role of k?
   e. How much work would we expected the client to do?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



Part C – Question 2 …2

a. What is the context of this diagram?

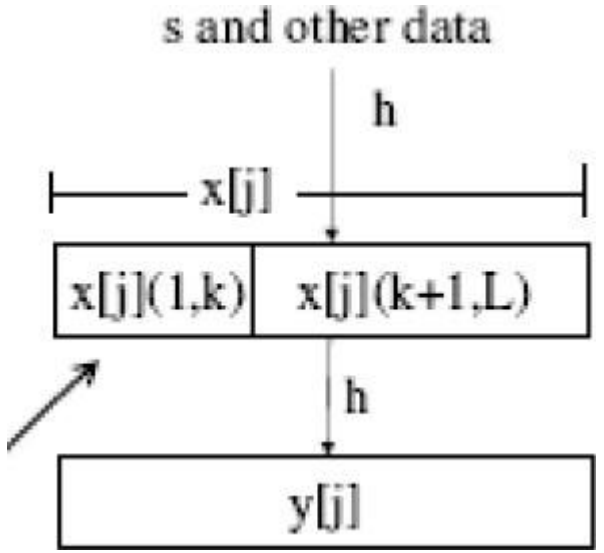
The diagram refers to the construction of client puzzles.



Part C – Question 2 …3

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

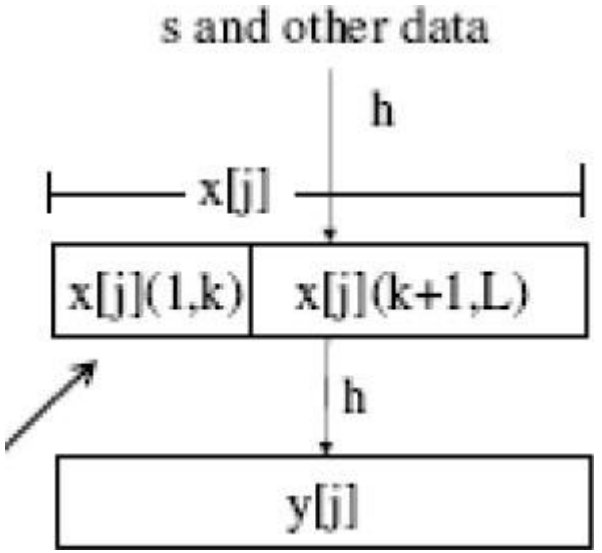
X[j](k+1,L) is sent to the client. This is generated by taking a sub-puzzle and taking k bit as the solution of the puzzle



Part C – Question 2 ...4

c. What should the client respond with?

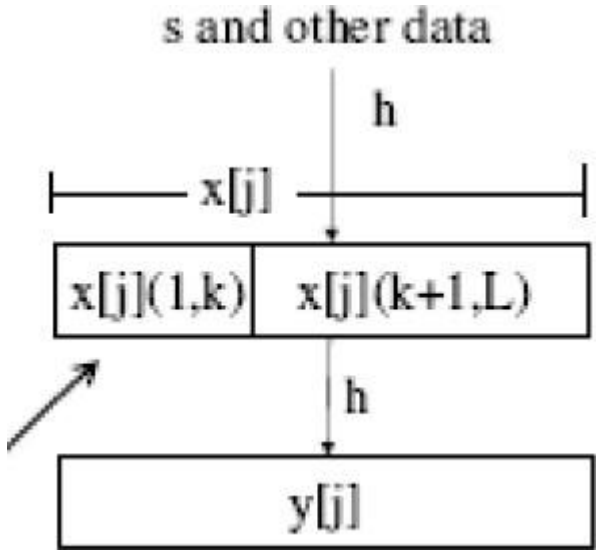
The client should respond with x[j](1,k) to be joined with x[j](k+1,L) to get y[j].



Part C – Question 2 …5

d. What is the role of k?

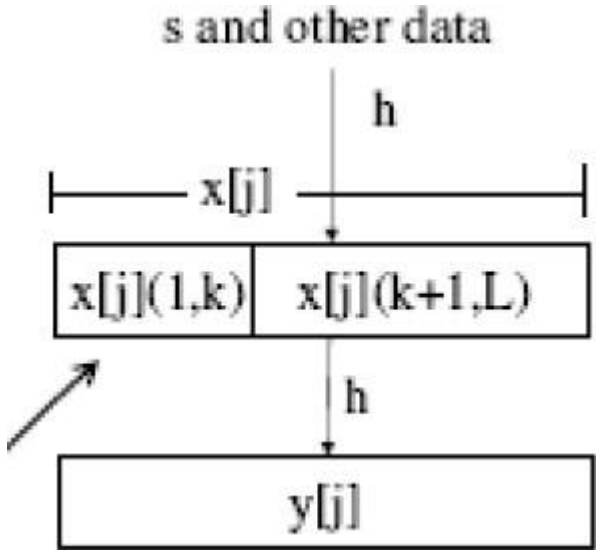
k is the number of bits that are missing from the puzzle. It determines the complexity (efforts) that a client needs to put in to solve the puzzle.



Part C – Question 2 …6

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

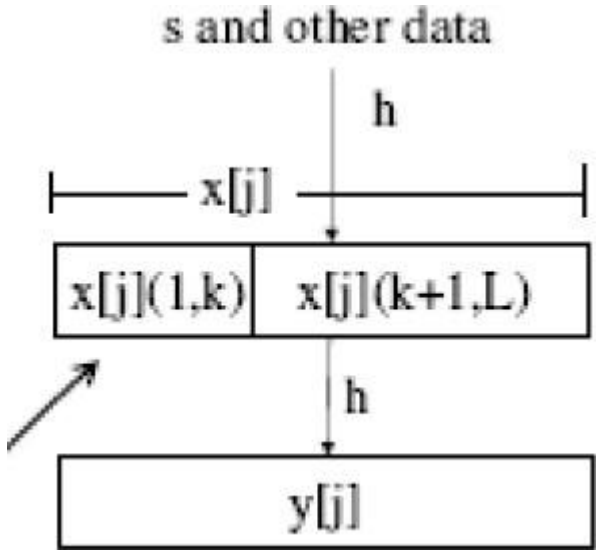
The client is expected to do minimal work so that the authentication can be fast.



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.