①

Institute of Information Technology

Jahangirnagar University

Professional Masters in IT

2nd Trimester Final Examination- Fall 2022
Duration: 3 Hours
Course Code: PMIT – 6104

Intake: Summer 2022, Spring 2022
Full Marks: 60
Course Title: Database Security

Do not write anything on the question paper.
There are **7 (Seven)** questions. Answer any **5 (Five)** of them.

1. a) What is meant by CIA triangle? [2]
b) How does *Polyinstantiation* occur in your database? [4]
c) Mention three well known security principles which are supported with RBAC. [3]
d) Explain *risk*, *vulnerability* and *threat*? [3]

2. a) Explain the role expression *re* = *(r,sc)* and define *sc* in Geospatial Data Authorization model. The symbols have their usual meaning. [4]
b) "*A senior manager is recorded as being in his office late one night. Subsequently at the time he was in his office the audit trail records several unsuccessful attempts to access database objects using a password of a member of clerical staff to objects to which the manager had no rights of access*". [5]
What are the threats in the above mentioned case? Explain the nature of the threats.
c) What is *capability list* in MAC policy? [3]

3. a) What is *Trust Negotiation in Trust Management System*? [2]
b) In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted? [3]
c) Many organisations have a choice to deploy their data resources and services either using their own IT infrastructure, or by choosing to have their data resources and services managed remotely by hosting databases on the 'Cloud'. [3]
Discuss the key strengths and limitations of these alternative approaches.
d) How do you secure statistical data by *controlling query set size and query overlap control method*? [4]

4. a) How does *micro aggregation* work in statistical database? [4]
b) Consider the following scenario: [4]
"*You have been asked to observe how data-entry clerks use new accounting software at a large accounting firm. As part of an observational study, the clerks are informed that they will remain anonymous. You install logging software on several clerks' computers, and your analysis of these logfiles reveals that many of the clerks are making a particular data entry error when using the new software. These errors will cause the firm to lose money, and company policy clearly dictates that workers salaries will be docked for mistakes leading to loss of company profit. You report the problem with the new software package to your boss. Your boss demands that you turn over your log files so the company can follow-up with more training for the employees and ensure that the company is reimbursed for the errors from the employees' pay*".
Identify an ethical framework and use it to argue why you should and should not turn over the logfiles to your boss.
c) How the query denial does lead to the information leakage in statistical data? Explain with necessary example. [4]

Question 4:

5. a) Rahim and Karim are having a debate about Public Key Infrastructure (PKI). Rahim says that it is simply a way of authenticating users. However, Karim argues that it is a type of encryption algorithm. They have asked you to decide who is correct. Briefly outline the purpose of PKI. Explain what is meant by a *certificate authority* and *digital certificate*.

   b) How do you hide a message into an image LSB steganography method? [5]

   c) Can steganography secure an encrypted database? Explain. [3]

6. a) What are the security challenges in Big Data ? [3]

   b) What is *MapReduce*? Illustrate a simple example of the working of MapReduce. [4]

   c) What are the main components of MapReduce Job? [2]

   d) Explain what is *JobTracker* in Hadoop? What are the actions followed by Hadoop? [3]

7. a) In order to facilitate the exchange of secret messages, Karim & Rahim have developed an image based steganography system. After a considerable investigative effort, you have learned that their system deploys an ASCII letter encoding scheme, shown in the below figure. You have also discovered that they use raw RGB images as their 'cover images', and that they embed their secret bits into these images by deploying the LSB scheme. In particular, they use the last 2 bits of each color channel (in each pixel) for embedding. This morning, you've seized one of their stego images. The image is of size 20x40 pixels. [4]

Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z

   i) How many secret letters, at most, could be contained in the given image?

   ii) Now, assume that instead of using the last 2 bits of each color channel in a pixel they decide to put all the secret bits into the LSB of only one channel while leaving the other channels intact. (The overall number of secret bits / pixel remains the same as in (i)). Would this approach be better or worse than the one originally described? Explain.

   b) What is *Inverse Document Frequency*? How does it work? [4]

   c) How does Privacy Homomorphism (PH) and Order-Preserving encryption techniques work to query on encrypted data in server side in DAS model. [4]

5. a) Rahim and Karim are having a debate about Public Key Infrastructure (PKI). Rahim says that it is simply a way of authenticating users. However, Karim argues that it is a type of encryption algorithm. They have asked you to decide who is correct. Briefly outline the purpose of PKI. Explain what is meant by a *certificate authority* and *digital certificate*. [4]

b) How do you hide a message into an image LSB steganography method? [5]

c) Can steganography secure an encrypted database? Explain. [3]

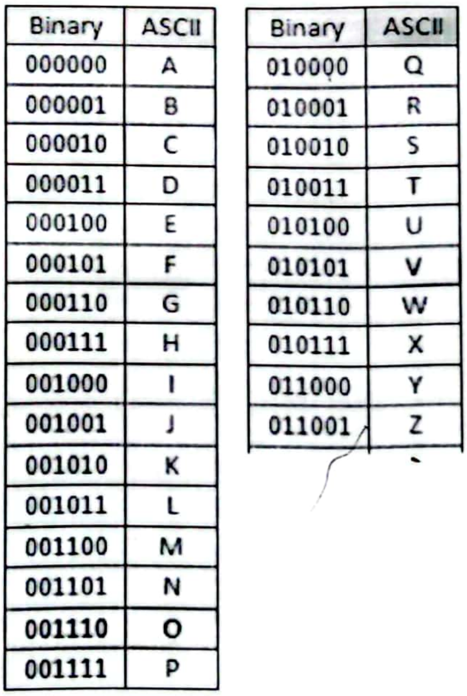
6. a) What are the security challenges in Big Data ? [3]

b) What is *MapReduce*? Illustrate a simple example of the working of MapReduce. [4]

c) What are the main components of MapReduce Job? [2]

d) Explain what is *JobTracker* in Hadoop? What are the actions followed by Hadoop? [3]

7. a) In order to facilitate the exchange of secret messages, Karim & Rahim have developed an image based steganography system. After a considerable investigative effort, you have learned that their system deploys an ASCII letter encoding scheme, shown in the below figure. You have also discovered that they use raw RGB images as their 'cover images', and that they embed their secret bits into these images by deploying the LSB scheme. In particular, they use the last 2 bits of each color channel (in each pixel) for embedding. This morning, you've seized one of their stego images. The image is of size 20x40 pixels. [4]



Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z

i) How many secret letters, at most, could be contained in the given image?

ii) Now, assume that instead of using the last 2 bits of each color channel in a pixel they decide to put all the secret bits into the LSB of only one channel while leaving the other channels intact. (The overall number of secret bits / pixel remains the same as in (i)). Would this approach be better or worse than the one originally described? Explain.

b) What is *Inverse Document Frequency*? How does it work? [4]

c) How does Privacy Homomorphism (PH) and Order-Preserving encryption techniques work to query on encrypted data in server side in DAS model. [4]