VEERMATA JIJABAI TECHNOLOGICAL INSTITUTE

Matunga, Mumbai-400 019

Autonomous Institute affiliated to University of Mumbai

EXAMINATION	Mid Semester Examination (MST) Sept 2018	DATE OF EXAM	26th Sept 2018
SEMESTER & PROGRAM	Sem-VII, Final Year B Tech (Computer Engineering)	TIME	12.00 am to 1:30 am
TIME ALLOWED	**1.5 HRS.**	MARKS	**40**
COURSE NAME – (CODE)	Information Security(CO4003_T)		

Instructions
1. All questions carry equal marks.
2. Figures to the right indicate full marks.
3. Justify for objective type questions.

Q.1 a. A sender *S* sends a message *m* to receiver *R*, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place. (02)

(I) S can launch a birthday attack to replace m with a fraudulent message.

(II) A third party attacker can launch a birthday attack to replace m with a fraudulent message.

(III) R can launch a birthday attack to replace m with a fraudulent message.

(A)(I)and(II) only (B)(I)only

(C)(II)only (D)(II)and(III) only

b. Using public key cryptography, X adds a digital signature σ to message M, encrypts <M, σ>, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations? (02)

(A) Encryption: X's private key followed by Y's private key; Decryption: X's public key followed by Y's public key

(B) Encryption: X's private key followed by Y's public key; Decryption: X's public key followed by Y's private key

(C) Encryption: X's public key followed by Y's private key; Decryption: Y's public key followed by X's private key

(D) Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key

c. In a class of targeted malicious code in program security, briefly specify "Man in the middle attack and Salami Attack" ? (02)

d. Discuss about security issues in Multilevel databases? (04)

Q.2 a. Illustrate in detail, about the Vulnerabilities, Attacks and Defense mechanisms in Network security? (08)

b. Carol and Eav agree to use the prime p=5 and the primitive root g=2 . Carol chooses the secret key a=4 and Eav chooses the secret key b=3. Then, using Diffie-Hellman Key Exchange Protocol, Find the common secret key share between Carol and Eav. (02)

$R_A = 2^4 \bmod 5$
$= 1$
$R_B = 2^3 \bmod 5$
$= 3$
$k = 1^3 \bmod 5 = 1$
$k = 3^4 \bmod 5 = 1.$

Q.3 a. With examples explain some of the ways in which the following memory management techniques of the OS be exploited : (10)

1. Fence
2. Base Bound Register

Q.4 a. Elaborate with examples the SQL injection attack and its countermeasures. How you can protect your SQL queries? (08)

b. In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of Ais 35. Find the private key of A. (02)

$n = 221$
$\phi(n) = 192$

****

$e = 35$

$d = e^{-1} \bmod \phi(n)$
$= 35^{-1} \bmod 192$

$= 11.$

VEERMATA JIJABAI TECHNOLOGICAL INSTITUTE

Matunga, Mumbai-400 019

Autonomous Institute affiliated to University of Mumbai

EXAMINATION	Mid Semester Examination (MST) Sept 2018	DATE OF EXAM	27th Sept 2018
SEMESTER & PROGRAM	Sem-VII, Second B Tech (Computer Engineering)	TIME	12.00 pm to 01:30 pm
TIME ALLOWED	**1.5 HRS.**	MARKS	**40**
COURSE NAME – (CODE)	Data Mining and Data Warehousing (CO4003_T)		

Instructions
1. All questions carry equal marks.
2. Figures to the right indicate full marks.
3. Make assumptions wherever necessary.

Q.1. a. Find whether or not each of the tasks given below is a data mining task. Justify. (03)
1. Dividing each of the customers of the company according to their profitability.
2. Predicting the future stock price of a company using historical records.
3. Monitoring the heart rate of a patient for abnormalities.

b. Describe the steps involved in data mining when viewed as a process of knowledge discovery. (03)

c. Describe two challenges to data mining with respect to (04)
i) Data mining methodology
ii) Efficiency and scalability.

Q.2. a. Define the following data mining functions. (02)
1. Discrimination
2. Association

b. Classify the following attributes as binary, discrete, or continuous. Also classify them as nominal or ordinal,interval or ratio. Some cases may have more than one interpretation, so briefly indicate your reasoning if you think there may be some ambiguity. (03)
1. Brightness as measured by a light meter.
2. Bronze, Silver, and Gold medals as awarded at the Olympics.
3. Ability to pass light in terms of the following values: opaque, translucent ,transparent

c. List the different techniques for discretization. (03)

d. How do we calculate the dissimilarity between objects described by numeric attributes? Explain with example. (02)

Q.3. a. Use smoothing by mean with a bin depth of 3 for the following data (03)
130 ,115, 90 , 85, 120,110, 92 , 123, 118.
What are the other methods for data smoothing?

b. For the following data, find the mean , mode , median.and the outliers. Draw a boxplot for the data. (04)
22, 21, 23, 23, 24, 25, 29, 33, 49 , 6, 27

mean = 282/11 = 25.63
mode = 23
median = 24

Q1 22
Q2 = 24
Q3 29

1932 7

1.5 x 7 = 10.5

22 - 10.5 = 11.5
29 + 10.5 = 30.5

∴ 6 & 33, 49 are outliers

c. What technique is used to detect redundancy during data integration? (03)
Explain it when the attributes are nominal. 3 .

Q.4. a. Why is it not possible to use OLAP with operational databases? 4 (03)

b. Suppose that a data warehouse consists of the four dimensions *date*, *spectator*, *location*, and *game*, and the two measures *count* and *charge*, where *charge* is the fare that a spectator pays when watching a game on a given date. Spectators may be students, adults, or seniors, with each category having its own charge rate. 4 (07)

(a) Draw a *star schema* diagram for the data warehouse.

(b) Starting with the base cuboid [*date*, *spectator*, *location*, *game*], what specific *OLAP operations* should you perform in order to list the total charge paid by student spectators at *GM Place* in 2010?