Year - April 2024

TYBSc - IT

SEM - V

No. of Pages 14

TYBSc-IT Sem-V

(2½ Hours)

[Total Marks: 75]

N. B : (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt *any three* of the following: **15**

a. Define and explain the Internet of Things with 2 examples.
b. Explain calm and ambient technology using example of Live wire.
c. What is manufactured normalcy field? Explain.
d. Discuss the issue of Privacy in Internet of Things.
e. What is TCP and UDP ports? Explain with examples.
f. Define protocol. Explain the following application layer protocols: HTTP, HTTPS, SMTP, FTP,POP3, IMAP.

2. Attempt *any three* of the following: **15**

a. Explain microcontrollers and system-on-chips with respect to embedded computing.
b. Describe the difficulties encountered during the transition from a prototype to mass production?
c. How can one tap into the community for promoting IOT devices? Explain.
d. Describe Beagle bone Black with a focus on the following aspects: Operating System, Programming Language, Debugging, Hardware and Openness.
e. Compare python characteristics with C++.
f. Write a short note on Electric Imp.

3. Attempt *any three* of the following: **15**

a. Explain the sketch, iterate and explore process in prototyping.
b. What are laser cutters? Explain the main features to consider while choosing a laser cutter.
c. What is CNC Milling? Explain.
d. Explain the following terms with respect to APIs: (a) Scraping, (b) Mashing up APIs.
e. What is comet? Explain.
f. Explain the following protocols suited to Internet of Things applications: Message Queying telemetry transport (MQTT), Extensible Messaging & Presence Protocol(XMPP), Constrained Application Protocol

4. Attempt *any three* of the following: **15**

a What are the concerns regarding performance and battery life while writing code for embedded systems?
b Write a short note on long tail of Internet.
c Explain different types of libraries for embedded systems which works with limited memory.
d Discuss the business model canvas for Internet of Things.

[*Contd…*

X51Y4F7B99X51Y4F7B99X51Y4F7B99X51Y4F7B99

e Explain the following business models
   i Provide infrastructure
   ii Take a percentage
   iii Be a Key Resource
f What is venture capital? How can one exit?

5. Attempt any three of the following:
a Explain the steps for manufacturing PCBs. 15
b Discuss different environmental issues in Internet of Things.
c Write a short note on mass-producing the case and other fixtures.
d Explain in detail the process of designing kits.
e Discuss the issues in scaling up the software for large scale IOT devices.
f Explain the five critical requirements for sensor commons project.

X51Y4F7B99X51Y4F7B99X51Y4F7B99X51Y4F7B99

(2½ Hours)

[Total Marks: 75]

N. B. (1) **All** questions are **compulsory**
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made
(3) Answers to the **same question** must be **written together**
(4) Numbers to the **right** indicate **marks**
(5) Draw **neat labeled diagrams** wherever **necessary**
(6) Use of **Non-programmable** calculators is **allowed**

1. Attempt *any three* of the following: 15

a What are different technologies provided by Java EE platform?
b Explain 2-tier System Architecture, its advantage and disadvantage.
c Explain the Life cycle of Servlet with diagram.
d What is JDBC? Explain architecture of JDBC in Detail?
e Write short notes on JDBC Drivers?
f Write a program to accept details of a person and using servlet and store those details in database.

2. Attempt *any three* of the following: 15

a. Explain Request Dispatcher Interface with its methods.
b. What is Cookies? Explain setting sending and reading of Cookie in java Servlet.
c. What is session? Explain lifecycle of Http Session?
d. Write a short note on session management using servlet.
e. Explain the working of Non-Blocking I/O.
f. Write a program to create a servlet application to download a file.

3. Attempt *any three* of the following: 15

a. Distinguish between Servlet and JSP.
b. Explain lifecycle of JSP with diagram.
c. Explain different types of JSP tags with example.
d. Explain different core tags in JSTL.
e. List and explain any 4 JSP Implicit objects with their methods.
f. Explain different scopes of JSP objects.

4. Attempt *any three* of the following: 15

a What are the different types of beans? Explain.
b Explain lifecycle of stateful session beans.
c What is an interceptor? How an interceptor is defined and how aroundInvoke() is added to it?
d Explain the Benefits of Enterprise Java Beans.
e Explain lifecycle of message driven beans.
f Explain naming and directory service with example.

5. Attempt *any three* of the following: 15

a. Explain Persistency in Java.
b. Explain JPA Architecture with diagram.
c. Explain hibernate with advantages.
d. Explain architecture of hibernate.
e. What is Impedance Mismatch? How it can be solved?
f. What are different components of Hibernate? Explain.

58025BDD15AA89D6DF7312BFADD3DA4B

TYBSC-IT - Sem V

(2½ Hours) [Total Marks: 75]

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt *any three* of the following: 15

a. Explain the duty of linux system administrator in monitoring and tuning Performance of a system.

b. Explain with the help of an example,
   i) How pipe can be used to add functionality to a command.
   ii) How the result of a command can be sent to a file.

c. What is a linux distribution? State in brief the Linux support offered by Red Hat.

d. With the help of an example, explain how backup can be scheduled and automated using cron.

e. State the features of the two types of links. Show how a deleted file can be restored using a link.

f. Discuss how yum overcomes the limitations of a tar ball and rpm.

2. Attempt *any three* of the following: 15

a. What is the difference between a partition and a logical volume? Highlight in brief the features of the different types of partitions.

b. Discuss the steps to create an encrypted volume.

c. Briefly explain the ifcfg configuration file variables.

d. With the help of an example, explain how to setup SSH port forwarding.

e. Explain the purpose and contents of the following files:
   i. /etc/group
   ii. /etc/shadow

f. State the commands to do the following. Give an example for each.
   i. Display ownership of file or directory
   ii. Change group ownership
   iii. Change user ownership
   iv. Set file permissions for user, group, and others using absolute mode
   v. Set file permissions for user, group, and others using relative mode

3. Attempt *any three* of the following: 15

a. What are tables, chains and rules in a firewall?

b. Enlist the steps to setup iptables logging.

c. State the reasons for which public/private keys are typically used. With the help of an example explain how public/private keys are used to encrypt traffic that is sent to a server.

d. What is GPG signing? State the commands to sign a file using GNU Privacy Guard.

e. Discuss the configuration of NFS server and client.

f. Discuss the generic Samba parameters in the global section of the samba configuration file.

[Contd...

4A200F3A17E7C68AB1CD4CE9789E1364

(5)

4. **Attempt *any three* of the following:**

a Write the steps to setup a secondary DNS server.

b Explain in brief the most relevant parameters from the dhcpd.conf file.

c Briefly discuss the three components play a role in the process of Internet mail.

d Name and explain the parameters that should be configured for a mail server handling messages from the Internet.

e List and explain the various performance parameters for Apache modes.

f Explain the steps to setup a Protected Web Server.

5. **Attempt *any three* of the following:**

a. What is a shell script? State the elements of a good shell script.

b. Demonstrate the use of pattern matching operators in a shell script.

c. Explain the steps to create an iSCSI target configuration.

d. Discuss the steps to troubleshoot a nonoperational cluster.

e. Explain the steps to perform a Virtual Machine Network Installation Using a Kickstart File.

f. List the steps to configure TFTP server for PXE boot.

4A200F3A17E7C68AB1CD4CE9789E1364

TYBSc-IT sem-V

(2½ Hours)

[Total Marks: 75]

N B (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt *any three* of the following: **15**

a. Explain .NET framework's architecture in brief.
b. Explain for each loop with suitable example.
c. Write a C# program to demonstrate the use of Multicast delegates.
d. Compare: value types and reference types in C#.
e. Give details about type conversion.
f. What is String class in C#? Write any 3 properties and methods.

2. Attempt *any three* of the following: **15**

a. Write a short note on ASP.NET page life cycle.
b. Write a short note on page class.
c. Explain any five properties of List Box and Drop Down List controls.
d. Explain AdRotator control in ASP.NET.
e. What is meant by validation of data? How to use the ASP.NET validation control to validate the user input?
f. Explain any two website navigation controls in ASP.NET.

3. Attempt *any three* of the following: **15**

a. Explain exception handling mechanism in C# with example.
b. Define session state management. What are the modes of storing session state data?
c. Elaborate cookie with suitable code snippet.
d. What is cross-page posting? Explain with an example.
e. Explain Master Page with its uses and working.
f. What is Theme? Explain Global theme.

4. Attempt *any three* of the following: **15**

a Explain ADO.NET architecture.
b What is DataReader? Give suitable example.
c Write short note on Data Source Controls.
d What is data binding? Explain its types.
e What are the attributes of GridView control?
f Compare: Data Adapter and Data Reader.

5. Attempt *any three* of the following: **15**

a. Explain the working of AJAX.
b. Write short note on the XML Text Reader class.
c. What do you mean by authentication and authorization? What are its types?
d. Explain ScriptManager and Timer controls.
e. Explain AJAX with its advantages and Disadvantages.
f. How to configure web.config for implementing Forms authentication?

X51YAFE88BX51YAFE88BX51YAFE88BX51YAFE88B

(7)

(2½ Hours) [Total Marks: 75]

N. B.: (1) **All** questions are **compulsory**.
(2) Numbers to the **right** indicate **marks**.
(3) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(4) Answers to the **same question** must be **written together**.
(5) **Mixing** of Sub-Questions is not allowed.
(6) Draw **neat labelled diagrams** wherever **necessary**.

1. Attempt any three of the following: 15
a. What is Big Data? State its characteristics.
b. Discuss the challenges of Big data.
c. Describe the current analytical architecture for data scientists.
d. Explain the ACID property in RDBMS.
e. What are different phases of the Data Analytics Lifecycle? Explain in detail.
f. Write a short note on Classification of Analytics.

2. Attempt any three of the following: 15
a. What is clustering? State its advantages & disadvantages.
b. State the applications of Association Rules.
c. Write a short note on Diagnostics.
d. Explain the concept of K-means clustering algorithm.
e. Write a brief note on Apriori algorithm.
f. What is Logistic regression? Explain in detail.

3. Attempt any three of the following: 15
a. Write a short note on Decision trees.
b. Describe the ARIMA Model technique.
c. Explain a probabilistic classification method based on Naive Bayes' theorem.
d. Explain Time Series Analysis in detail.
e. How to predict whether customers will buy a product or not? Explain w.r.t decision tree.
f. What is tokenization? Explain how it is used in text analysis.

4. Attempt any three of the following: 15
a. Describe the concept of MapReduce.
b. State the components of Spark Stack.
c. Explain the concept of Resilient Distributed Datasets.
d. Write a short note on Hadoop Distributed File System.
e. Explain in detail the Hadoop Architecture.
f. Write a short note on Job Chaining in advanced MapReduce context.

5. Attempt any three of the following: 15
a. What are the Distributed Analysis and Patterns?
b. What is the functionality of the filter mapper? Explain in detail with example.
c. Write a short note on Data Ingestion.
d. State & explain different Design Patterns.
e. Explain with example Relations, tuples and Filtering in context of Pig.
f. Write the entire procedure with appropriate commands for importing data from MySQL to HDFS.

****

(8)

TY/BSC

(2 ½ Hours) [Total Marks: 75]

N.B. (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labelled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

Q. 1 Attempt the three of the following. **15**

a. Explain Mesos, Akka and Cassandra as data science processing tools.
b. Explain the basics of Business layer.
c. List and explain different programming languages using in data science processing.
d. What is data vault? Explain hubs, links and satellite with respect to data vault.
e. Explain the Rapid Information Factory ecosystem.

Q. 2 Attempt the three of the following. **15**

a. Give an overview of the functions of Audit, Balance, and Control Layer.
b. Explain the following shipping terms: i. Seller ii. Carrier iii. Port, iv. Ship, v. Terminal, Named Place.
c. Explain the fundamental data science process steps.
d. Explain Data Lakes and Data Swamps.
e. List and explain the different data stores used in data science.

Q. 3 Attempt the three of the following. **15**

a. Explain the different ways to deal with errors.
b. How you will handle missing values in Pandas? Explain
c. Write a python program to keep Only the Rows That Contain a Maximum of Two Missing Values.
d. Explain the principles of data analysis.
e. Write a python program to Drop the Columns Where All Elements Are Missing Values.

Q. 4 Attempt the three of the following. **15**

a. How to Complete the 5 Whys?
b. What are pareto charts? What information can be obtained from pareto charts?
c. Explain the Time section of TPOLE.
d.. Explain hypothesis testing, t-test and chi-square test with respect to data science.
e. Write a short note on data valut.

Q. 5 Attempt the three of the following. **15**

a. What is organize superstep? Explain in brief.sss
b. Where is chi square test used?
c. Explain regression and its types?
d. Why is report superstep important? Explain its importance.
e. Explain Pricipal Component Analysis in details.

****

X51Y7BACD7X51Y7BACD7X51Y7BACD7X51Y7BACD7

(2 ½ Hours) [Total Marks: 75]

N. B. (1) **All** questions are **compulsory**
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made
(3) Answers to the **same question** must be **written together**
(4) Numbers to the **right** indicate **marks**
(5) Draw **neat labelled diagrams** wherever **necessary**
(6) Use of **Non-programmable** calculators is **allowed**

Q. 1 Attempt the three of the following. **15**

a Explain Mesos, Akka and Cassandra as data science processing tools.
b Explain the basics of Business layer.
c List and explain different programming languages using in data science processing.
d What is data vault? Explain hubs, links and satellite with respect to data vault.
e Explain the Rapid Information Factory ecosystem.

Q. 2 Attempt the three of the following. **15**

a Give an overview of the functions of Audit, Balance, and Control Layer.
b. Explain the following shipping terms: i. Seller ii. Carrier iii. Port, iv. Ship, v. Terminal, Named Place.
c. Explain the fundamental data science process steps.
d. Explain Data Lakes and Data Swamps.
e List and explain the different data stores used in data science.

Q. 3 Attempt the three of the following. **15**

a. Explain the different ways to deal with errors.
b. How you will handle missing values in Pandas? Explain
c. Write a python program to keep Only the Rows That Contain a Maximum of Two Missing Values.
d. Explain the principles of data analysis.
e. Write a python program to Drop the Columns Where All Elements Are Missing Values.

Q. 4 Attempt the three of the following. **15**

a. How to Complete the 5 Whys?
b. What are pareto charts? What information can be obtained from pareto charts?
c. Explain the Time section of TPOLE.
d. Explain hypothesis testing, t-test and chi-square test with respect to data science.
e. Write a short note on data valut.

Q. 5 Attempt the three of the following. **15**

a. What is organize superstep? Explain in brief.sss
b. Where is chi square test used?
c. Explain regression and its types?
d. Why is report superstep important? Explain its importance.
e. Explain Pricipal Component Analysis in details.

****

X51Y7BACD7X51Y7BACD7X51Y7BACD7X51Y7BACD7

(2 ½ Hours) [Total Marks: 75]

N. B. (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labelled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

Q. 1 Attempt the three of the following. 15

a. Explain Mesos, Akka and Cassandra as data science processing tools.
b. Explain the basics of Business layer.
c. List and explain different programming languages using in data science processing.
d. What is data vault? Explain hubs, links and satellite with respect to data vault.
e. Explain the Rapid Information Factory ecosystem.

Q. 2 Attempt the three of the following. 15

a. Give an overview of the functions of Audit, Balance, and Control Layer.
b. Explain the following shipping terms: i. Seller ii. Carrier iii. Port, iv. Ship. v. Terminal, Named Place.
c. Explain the fundamental data science process steps.
d. Explain Data Lakes and Data Swamps.
e. List and explain the different data stores used in data science.

Q. 3 Attempt the three of the following. 15

a. Explain the different ways to deal with errors.
b. How you will handle missing values in Pandas? Explain
c. Write a python program to keep Only the Rows That Contain a Maximum of Two Missing Values.
d. Explain the principles of data analysis.
e. Write a python program to Drop the Columns Where All Elements Are Missing Values.

Q. 4 Attempt the three of the following. 15

a. How to Complete the 5 Whys?
b. What are pareto charts? What information can be obtained from pareto charts?
c. Explain the Time section of TPOLE.
d. Explain hypothesis testing, t-test and chi-square test with respect to data science.
e. Write a short note on data valut.

Q. 5 Attempt the three of the following. 15

a. What is organize superstep? Explain in brief.sss
b. Where is chi square test used?
c. Explain regression and its types?
d. Why is report superstep important? Explain its importance.
e. Explain Pricipal Component Analysis in details.

****

X51Y7BACD7X51Y7BACD7X51Y7BACD7X51Y7BACD7

T4BSC IT Sem - V

(11)

Paper / Subject Code: 53701 / Software Project Management

(2½ Hours)

[Total Marks: 75]

N. B. (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt *any three* of the following: 15

a. Define project. Describe the project management life cycle with the help of diagram and state the W5HH principle.
b. What is project product? Explain the product breakdown structure with the help of example.
c. Define Business Case. Explain business case document in detail.
d. How to evaluate and manage risk in software project management? Explain.
e. Describe the main steps of step wise approach to planning software projects overview with help of diagram.
f. Suppose a software development company has undertaken a project that is expected to cost £190,000 to execute and the expected inflow is £25,000 per quarter for the first year, £30,000 per quarter thereafter. What is the payback period for the project?

2. Attempt *any three* of the following: 15

a. Describe the spiral model with the help of diagram and give the advantages and disadvantages of it.
b. Define Atern/Dynamic Systems Development Method. State and explain eight core principles of it.
c. Explain briefly Albrecht/IFPUG function point and solve the following: For a organization, the following table summarizes the weightings to be used for computing function points measures of a software having the following characteristics : Number of user inputs : 10 (simple), Number of user outputs : 7 (simple), Number of user enquires : 3 (average) , Number of files : 6 (average), Number of External interfaces : 1 (complex), Calculate unadjusted function point measures of the size of the software system?
d. Discuss Agile and Scrum as a fast delivery approach of a project in detail.
e. Describe the COCOMO II and discuss its stages.
f. Describe the Capers Jones estimating rules of thumb with the help of relevant examples.

3. Attempt *any three* of the following: 15

a. Describe the nature of resources and their scheduling.
b. List and Describe Bohem's top ten software project risks and the different strategies for reducing it.
c. Explain the concept of forward pass, backward pass, and critical path.
d. Distinguish between PERT and CPM.

[*Contd...*

9BF3D1FF996635D692980B2145069950

e Suppose four risks namely R1, R2, R3 and R4 have been identified and assigned the probabilities of occurrence of 0.1, 0.2, 0.3 and 0.4 respectively. The likely damages due to the four risks are Rs. 60,000; Rs. 1,00,000; Rs. 70,000; Rs. 80,000 respectively. Calculate the risk exposure of all the risks.

f Create a precedence activity network using the following details:

Activity	Depends on	Duration (days)
A		5
B	A	7
C	B	6
D	A	5
E	D	10
F	B	15
G	B	8
H	G	8
I	C	4
J	G	4
K	E,F	7
L	I,H	5

Calculate the earliest and latest start and end dates and the float associated with each activity. From this identify the critical path.

4. Attempt *any three* of the following:

a. Define Contract. Explain fixed price contract with its' advantages and disadvantages. 15

b. Describe Vroom's expectancy theory of motivation.

c. Describe three important categories of stress management techniques.

d. How to control the change? Explain the change control process.

e. Describe the ethical and professional concerns as a member of any organization.

f. Suppose a project is budgeted to cost $150,000. The project is to be completed in 20 months. After two months, the project is 10% complete at an expense of £25,000. It was planned that after 2 months, 15% of the project work should have been completed. Compute the cost performance index and the schedule performance index. Interpret these values to assess the progress of the project.

5. Attempt *any three* of the following:

a. Explain five basic stages of Team development. Also state the different types of people needed to form a balanced team. 15

b. "Student fails in the project, if the projects are not closed properly". Justify this statement.

c. What is Testing? Give a brief explanation of the main activities involved in Software Testing.

d. What is the importance of Software quality? Discuss six major external software quality characteristics identified by ISO 9126.

e. Discuss reasons for project closure.

f. Explain CMM (Capability Maturity Model) with it's the various levels.

9BF3D1FF996635D692980B2145069950

(2 ½ Hours) [Total Marks: 75]

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 Attempt All.

(a) Multiple Choice Questions. **(10M)**

i. A typical stream cipher encrypts plaintext _____ byte at a time.
a) one b) two c) three d) multiple

ii. Rail fence is an example of _____.
a) Caesar cipher b) Transposition technique c) Substitution technique d) Steganography

iii. The _____ method provides a one-time session key for two parties. a) Diffie-Hellman b) RSA c) DES d) AES

iv. DES is a _____ cipher.
a) block cipher b) stream cipher c) bit cipher d) byte cipher

v. Cipher based on substitution, using multiple substitution alphabets is called_____.
a) Monoalphabetic cipher b) Monocipher
c) Polyalphabetic cipher d) two-cipher

vi. _____ is an authentication algorithm.
a) MAC b) AES c) DAS d) DES

vii. For a client-server authentication, the client requests from the KDC a _____ for access to a specific asset.
a) ticket b) local c) token d) user

viii. In a ____ the keys involved are identical for both encrypting and decrypting a message.
a) Asymmetric b) Symmetric c) HMAC d) Hash

ix. S/MIME stands for_____.
a) Simple multipurpose internet mail extension
b) Secure multipurpose internet mail extension
c) Simple multimedia internet mail extension
d) Standard multipurpose internet mail extension

x. A stateful firewall maintains a _____ which is a list of active connections.
a) Routing table b) Bridging table c) State table d) Connection table

9BF3D1FF996635D692980B2145454493

(b) **Fill in the blanks** (5M)

(Intruder, Tester, CIR, Intranet, RSA, Message Authentication)

i) _____ is a mode of operation technique

ii) _____ is a process to make sure that messages arrived from the alleged source are not altered while transmitting

iii) An _____ is a private network that uses the Internet model

iv) PGP makes use of _____ cryptographic algorithm.

v) _____ is a person who attempts to gain unauthorized access to a network

Q. 2 Attempt the following (Any THREE) (15M)

(a) Explain the terms: i) Threat, ii) Attack.

(b) Write a short note on Active Attack.

(c) Describe Steganography.

(d) Explain Feistel Encryption and Decryption.

(e) Explain ECB (Electronic Codebook).

(f) Encrypt the following plain text to cipher text using Caeser Cipher Technique. (Key=3)
"LAST ATTACK TOMORROW EARLY MORNING AT FOUR".

Q. 3 Attempt the following (Any THREE) (15M)

(a) Write a short note on Digital Signature Algorithm (DSA).

(b) Explain RSA.

(c) Give X.509 Certificate Format.

(d) What are the PKIX management functions?

(e) Give overview of Kerberos.

(f) How is Message Digest Generation done Using SHA-512?

Q. 4 Attempt the following (Any THREE) (15M)

(a) What are the Benefits of IPSec.

(b) Explain SSL architecture.

(c) Explain different approaches of intrusion detection.

(d) Explain the following terms: i) Logic bomb; ii) Mobile Code

(e) State different types of Firewalls.

(f) What is MIME? What are the five header fields defined in MIME?

Q. 5 Attempt the following (Any FIVE) (15M)

(a) Write are the four main steps of AES.

(b) State the difference between a block cipher and a stream cipher.

(c) Elaborate Diffie-Hellman key exchange algorithm.

(d) Explain Trojan Horse.

(e) What are honeypots?

(f) Explain different types of Intruders.

(g) What is OSI? Explain the following terms in OSI security architecture:
i)Security Attack ii) Security Mechanism iii) Security Service

(h) What is Realm?

****

9BF3D1FF996635D692980B2145454493