

Duration: 3 Hours

Maximum Marks: 80

N.B.: -

1. Question No 1 is Compulsory
2. Solve any three questions out of remaining questions
3. Assume suitable data if required and mention it clearly
4. Figures to right indicate full marks

- Q1 Solve any four of following: -
- [A] What are CIA triads? **5**
 - [B] How are C-Ciphertext and P-Plaintext expressed in Caesar Cipher? Encrypt the plaintext message “**Meet me after the toga party**” using it. **5**
 - [C] Compare block and stream Cipher. **5**
 - [D] What are Elements of Network Access Control (NAC)? **5**
 - [E] What is an Intrusion Detection System (IDS)? Give its type. **5**
 - [F] List various services provided by IPsec. **5**
- Q2 [A] What are traditional ciphers? Discuss Hill Cipher substitution method with example. **10**
[B] Explain AES encryption algorithm with detailing of four different stages. **10**
- Q3 [A] Elaborate the steps of key generation using the RSA algorithm. In the RSA system, What is the public key (E, n) and private key (D, n) and $\phi(n)$ of this user if $n=187$. is defined. If the plaintext input $M=88$, What is Ciphertext? Explain various kinds of attacks on the RSA algorithm. **10**
[B] How is security achieved in the transport and tunnel modes of IPsec? What are security associations? **10**
- Q4 [A] Summarize the behaviour of SHA512 with round functions. **10**
[B] Explain Kerberos protocol with a simplified overview. **10**
- Q5 [A] What is meant by Malicious software? What are its various types? Explain DOS attack. **10**
[B] What protocols comprise SSL? Explain all phases of SSL Handshake protocol in detail. **10**
- Q6 [A] What is Network Access Control (NAC)? Explain NAC enforcement methods. **10**
[B] Define Firewall. What are various types of it? **10**

[3 hrs]

[80 Marks]

- Note:** 1. Question 1 is compulsory
 2. Answer any three out of remaining questions
 3. Assume suitable data where required

Q1 Solve any 4

- a) Write your observations regarding Device Insecurity in IoT 5
- b) Explain how data rate and throughput are related 5
- c) Data Analytics vs Business Benefits 5
- d) Define a smart object. 5
- e) Explain convergence of IT and OT. 5

Q2

- a) State use the use of Purdue Model for Control Hierarchy in IoT. 10
- b) Explain Authentication and Encryption on Constrained Nodes in 6LoWPAN protocol 10

Q3

- a) Explain IoT Access Technologies LTE Cat 0 , LTE-M and NB-IoT 10
- b) Explain in detail CIA for IoT 10

Q4

- a) Elaborate how OT Network Characteristics Impacting on security aspect of IoT. 10
- b) In IoT ecosystem, describe the use of Edge computing, Fog computing, and Cloud computing. Give advantages and disadvantages of each. 10

Q5

- a) Explain any two IoT Application Layer Protocols with respect to its packet format , working and security. 10
- b) List and Explain Common Challenge in Securing IoT 10

Q6

- a) In brief explain how formal risk analysis is done using any one framework. 10
- b) Justify IT and OT Responsibilities in the IoT Reference Model. 10

Duration: 3hrs

[Max Marks:80]

- N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

- Q1.** Attempt any four
- a. Discuss the different opportunities associated with smart contracts. **5**
 - b. List different Node Types and explain their Roles. **5**
 - c. What is IPFS? How is IPFS helpful in blockchains? **5**
 - d. Differentiate between Kafka and RAFT **5**
 - e. Draw the structure of the block. What is genesis block? **5**
- Q2.**
- a. Explain the challenges and benefits of Cyber Security in blockchain based application. **10**
 - b. Define crypto assets. Compare between ERC20 & ERC721. **10**
- Q3.**
- a. Discuss the different challenges addressed by blockchain in healthcare industry. **10**
 - b. Explain different components of Hyperledger Fabric in detail. **10**
- Q4**
- a. List different consensus algorithms. Explain Proof-of-Work consensus in detail. **10**
 - b. Explain Architecture of Ethereum. **10**
- Q5**
- a. What is an ERC21 token? Explain the steps to create ERC21 tokens. **10**
 - b. With the help of a suitable example explain the different types of accounts in Ethereum. **10**
- Q6** Write short note on (any 4) **20**
- a. Different types of blockchain
 - b. SPV Node
 - c. Metamask
 - d. Merkle tree
 - e. Framework in Hyperledger Fabric

(3 Hours)

[Total Marks: 80]

N.B.: (1) Question No.1 is **Compulsory**.

- (2) Attempt **any three** questions from the **remaining** questions.
 (3) Assume **suitable** data wherever required but **justify** the same.
 (4) **Figures** to the **right** indicate **full marks**.
 (5) Answer each new question to be started on a **fresh page**.

1. (a) Explain the strategy to choose a web analytics tool. (5)
 (b) Write a Typescript program to find a factorial of the given number using the “while” loop. (5)
 (c) Discuss ng-click built-in directive in AngularJS with a suitable example. (5)
 (d) Explain the features of MongoDB. (5)
2. (a) Explain how events are handled in Node.js with EventEmitter class. Write a suitable program for the same. (10)
 (b) Explain Routing using ng-Route, ng-Repeat, ng-Style, and ng-View in AngularJS with suitable examples. (10)
3. (a) Define Semantic Web. Explain in detail the components of the Semantic Web Stack. (10)
 (b) State the significance of the Request Object in Express.js. Also, explain the different properties of Express.js Request Object. (10)
4. (a) Write a Typescript program to explain the concept of inheritance. (10)
 (b) Illustrate the use of Expressions in AngularJS with a suitable example, (10)
5. (a) Explain different methods available in the networking module of Node.js. (10)
 (b) Explain Accessing and Manipulating Databases commands in MongoDB. (10)
6. (a) Create a simple “Hello World” application in Express.js. Add three middleware functions to the application: one called **myLogger** which prints a simple log message, one called **requestTime** which displays the timestamp of the HTTP request, and one called **validateCookies** that validates incoming cookies. (10)
 (b) Explain REST API in detail. (10)

Duration: 3hrs

[Max Marks:80]

- N.B.:** (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

- 1 Attempt any FOUR. [20]
- a Explain foot printing in detail. Also mention a few tools used for foot printing.
 - b Define digital forensics? Explain types of digital forensics.
 - c Classify hackers based on their knowledge and activities performed on computers.
 - d List and discuss various system hacking tools.
 - e Explain investigation triad in detail.
- 2 a Explain penetration testing with its various phases? Also explain how social engineering can be used for penetration testing. [10]
- b What is ethical hacking? Describe the steps of the ethical hacking process. [10]
- 3 a Explain incident response methodology in detail. [10]
- b Explain the guidelines for digital forensics report writing along with its goals. [10]
- 4 a Explain the importance of forensics duplication and its methods. [10]
- b Define the following terms: a. Bit-stream image b. Chain of custody c. Evidence custody form d. Evidence bags e. Repeatable findings f. forensic workstations g. qualified forensic duplicate h. restored image i. mirror image j. Volatile data [10]
- 5 a Explain the roles of an expert witness and scientific witness with suitable examples? [10]
- b Briefly explain the types of digital evidence with examples. [10]
- 6 Write short note on the following: (any two) [20]
- a) Volatile data collection for Windows system.
 - b) Analysis of forensics data in Linux system
 - c) Data carving and various tools of forensic analysis

30041