Paper / Subject Code: 37481 / Cryptography and Network Security

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 the three security objectives for information and information system? **5**

[B] How C-Ciphertext and P-Plaintext expressed in Caesar Cipher? Explain with example. **5**

[C] Differentiate between block and stream Cipher. **5**

[D] What are Elements of Network Access Control (NAC)? **5**

[E] What is Intrusion Detection System (IDS)? Give its type. **5**

[F] List applications of IPsec. **5**

Q2 [A] What are traditional ciphers? Discuss Hill Cipher substitution method with example. **10**

[B] Explain various transformations of AES encryption in detail. **10**

Q3 [A] Elaborate the steps of key generation using RSA algorithm. In RSA system, what is the public key (E, n) and private key (D, n) and Ø (n) of this user if n=187. is defined. If the Ciphertext C =11, What is plaintext? Explain various kind of attacks on RSA algorithm. **10**

[B] How security is achieved in the transport and tunnel modes of IPsec? What are security associations? **10**

Q4 [A] Explain steps involved for message digest generation using SHA 512. **10**

[B] Explain Kerberos protocol with simplified overview. **10**

Q5 [A] What are various types of Malicious software? Explain phishing attack. **10**

[B] Explain operation of TLS Record Protocol. **10**

Q6 [A] Explain EAP protocol exchanges with components involved. **10**

[B] Explain Transport mode and Tunnel mode of IPsec? **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.

1 **Attempt any FOUR.** **[20]**

a Explain the following terms: (any five)s
a. Bit-stream image b. Chain of custody c. Evidence custody form d. Evidence bags e. Repeatable findings f. forensic workstations

b Give classification of hackers.

c Briefly explain what an expert witness and scientific witness is?

d How can email be used as evidence?

e Write a note on enumeration techniques and tools.

2 a Define digital forensics. Explain the need of digital forensics along with the lifecycle of digital forensics. **[10]**

b Explain the goal of incident response. Mention incidence response methodology with suitable diagram. **[10]**

3 a Explain the importance of evidence handling in digital forensics. **[10]**

b Explain forensics analysis of the data acquired from any one of the operating system. **[10]**

4 a Explain the data acquisition in network forensics in detail. **[10]**

b Define data carving. List and discuss differ tools for forensic analysis. **[10]**

5 a Explain the goal of forensic report writing. Give the outline of the report. **[10]**

b Point out the features of Forensic Duplication and Investigation & also outline the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider. **[10]**

6 a Explain various stages in penetration testing. **[10]**

b Write short note on the following **[10]**

i) Footprinting
ii) Ethical hacking

****

Time :(3 hrs.) **Maximum Marks = 80**

NB:

1. Question No. 1 is compulsory and solve any THREE questions from remaining questions
2. Assume suitable data if necessary
3. Draw clean and neat diagrams

Q1.			**Marks**
	a.	Differentiate RDBMS v/s MongoDB	**5**
	b.	Explain Multilevel inheritance in TypeScript with example	**5**
	c.	Explain Asynchronous programming	**5**
	d.	What is expressions in AngularJS	**5**
Q2.	a.	Explain components of Semantic Web stack.	**10**
	b.	Illustrate Streams in Nodejs	**10**
Q3.	a.	Explain AngularJS ng-app, ng-init, ng-model directive with examples	**10**
	b	Explain CRUD operations in MongoDB with example	**10**
Q4	a.	Construct a Simple application for AngularJs form Validation. it will check if an email is valid or not. Draw a mock UI of the Output.	**10**
	b.	Explain different methods available in the networking module of Node.js.	**10**
Q5	a.	Explain REST API in detail.	**10**
	b.	State the significance of the Request Object in Express.js. Also, explain the different properties of Express.js Request Object.	**10**
Q6	a.	Explain functions in TypeScript with suitable example	**10**
	b.	Explain Express.js Cookies management with example	**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 structure of block in blockchain

b What are different types of blockchain?

c Explain the concept of block headers and how they are used to link blocks in a blockchain.

d Explain architecture of ethereum.

e Describe the role of Metamask in the Ethereum ecosystem.

2 a Discuss the concept of a Bitcoin wallet. What are the different types of wallets, and how do they manage private keys and facilitate transactions? [10]

b Describe the role and responsibilities of peer nodes in the Hyperledger Fabric architecture. Also discuss the concept of channels in Hyperledger Fabric. [10]

3 a Describe the step-by-step process of a typical Bitcoin transaction. Include the roles of the sender, recipient, miners, and the blockchain network. [10]

b What are the essential tools and frameworks for setting up a development environment for Solidity programming? Discuss the role of tools like Remix and Truffle in the development process. [10]

4 a Discuss the purpose and significance of Bitcoin relay networks. How do they improve the propagation of transactions and blocks within the network? [10]

b Define ERC721 tokens and explain their primary purpose. How do ERC721 tokens differ from ERC20 tokens in terms of ownership and uniqueness? [10]

5 a Provide an overview of the Truffle framework. What is its primary purpose in the context of blockchain development, and how does it simplify the development process? [10]

b Contrast the security aspects of ICOs and STOs. How does the classification of tokens (security vs. utility) influence the security of the fundraising process? [10]

6 a Describe the roles played by different entities in the RAFT consensus algorithm. What are the specific responsibilities of leaders, followers, and candidates? [10]

b Discuss the key security challenges in traditional IoT architectures. How can blockchain address these challenges and provide a more secure foundation for IoT deployments? [10]

****

[TIME:3 hrs] **[Marks:80]**

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) Illustrate IoT Application Transport Methods 5

b) Discuss how low power consumption is essential for prolonging the life of battery-operated devices in IoT. 5

c) Short note on Communication models & API. 5

d) Explain Data Versus Network Analytics 5

e) Briefly elaborate the DICE. 5

Q2

a) Explain Mesh-Under Versus Mesh-Over Routing in 6LoWPAN 10

b) Explore the Purdue Model for Control Hierarchy and its implications for security practices in OT. 10

Q3

a) Explain working of AMQP with an example 10

b) Compare and contrast OCTAVE and FAIR 10

Q4

a) Examine the considerations for adopting or adapting the Internet Protocol in IoT applications. 10

b) Explain the importance of the physical layer and MAC (Medium Access Control) layer in IoT access technologies. 10

Q5

a) Explain the concepts of objective function rank, RPL headers, and metrics in the context of RPL. 10

b) List and explain LTE Variations with the applications where we can use them 10

Q6

a) Examine the impact of legacy systems on OT security. Discuss how the continued use of outdated technologies poses challenges in terms of vulnerabilities, patching, and overall security management. 10

b) Write short note on 1. IPV6 Ready Logo 2. Functional blocks of IoT 10

****