.

Printed Page:-3 **Subject Code:- BCSCY0611**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: VI - THEORY EXAMINATION (2025 - 2026)
Subject: IoT Security and Forensic

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*

2. *Maximum marks for each question are indicated on right -hand side of each question.*

3. *Illustrate your answers with neat sketches wherever necessary.*

4. *Assume suitable data if necessary.*

5. *Preferably, write the answers in sequential order.*

6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

(1.1) Internet of Things (IoT) refers to(CO1, K1) 1

(a) Network of computers
(b) Network of interconnected physical devices with sensors
(c) Cloud computing systems
(d) Social media platforms

(1.2) Smart meters are an example of(CO1,K1) 1

(a) Industrial IoT
(b) Smart Home
(c) Smart Cities
(d) Healthcare IoT

(1.3) OWASP IoT Top 10 focuses on(CO2,K2) 1

(a) Common IoT vulnerabilities
(b) Encryption standards
(c) Network topology
(d) Cloud pricing

(1.4) Weak passwords fall under(CO2,K1) 1

(a) OWASP IoT vulnerabilities
(b) Physical attacks
(c) Network faults
(d) Cloud risks

(1.5) Certificate-based authentication relies on which technology?(CO3,K2) 1

(a) Symmetric keys
(b) Digital certificates
(c) Passwords
(d) Biometric data

(1.6) NIST SP 800-183 provides guidance related to(CO3,K3) 1

(a) IoT security model
(b) Mobile apps
(c) Database security
(d) Social networks

(1.7) _____ is required when collecting digital evidence from IoT systems.(CO4,K2) 1

(a) Follow legal procedures
(b) Disable encryption
(c) Change passwords
(d) Reset devices

(1.8) Digital forensic investigation concludes with _____(CO4,K1) 1

(a) Reporting findings
(b) Formatting disks
(c) Resetting devices
(d) Updating firmware

(1.9) Wearable device forensic analysis often requires:_____(CO5,K1) 1

(a) Network routers
(b) Cloud servers
(c) Industrial controllers
(d) Specialized tools

(1.10) Edge forensics reduces dependency on:_____(CO5,K2) 1

(a) Mobile devices
(b) Centralized cloud analysis
(c) Sensors
(d) Firmware

2. Attempt all parts:-

(2.1) Mention two resource constraints in IoT devices.(CO1,K2) 2

(2.2) Explain replay attack (CO2,K2) 2

(2.3) Define ISO/IEC 30141 architecture(CO3,K1) 2

(2.4) Define Digital Forensics(CO4,K1) 2

(2.5) Define Autopsy tool in digital forensics?(CO5,K1) 2

SECTION-B 30

Answer any one of the following:-

(3.1) Explain IoT architecture layers(CO1,K2) 6

(3.2) Explain Zigbee and its applications(CO1,K2) 6

Answer any one of the following:-

(3.3)	Describe DREAD risk assessment model(CO2,K2)	6
(3.4)	Explain side-channel attacks with examples(CO2,K2)	6

Answer any one of the following:-

(3.5)	Explain AES-CCM encryption algorithm in IoT communication(CO3,K2)	6
(3.6)	Explain end-to-end security architecture for IoT systems.(CO3,K2)	6

Answer any one of the following:-

(3.7)	Explain device-based evidence collection in IoT investigations.(CO4,K2)	6
(3.8)	Describe network-based evidence in IoT forensic analysis(CO4,K2)	6

Answer any one of the following:-

(3.9)	Discuss the concept of edge forensics(CO5,K2)	6
(3.10)	Discuss firmware vulnerabilities and their impact on security(CO5,K2)	6

SECTION-C 50

4. Answer any one of the following:-

(4.1)	Explain IoT architecture in detail with a neat diagram.(CO1,K2)	10
(4.2)	Discuss smart home architecture using IoT.(CO1,K2)	10

5. Answer any one of the following:-

(5.1)	Give explanation of maintenance and update challenges in IoT Devices(CO2,K2)	10
(5.2)	Give explanation of threat modeling in IoT systems(CO2,K2)	10

6. Answer any one of the following:-

(6.1)	Explain Trusted Platform Module architecture and functions(CO3,K2)	10
(6.2)	Analyze secure firmware update mechanism.(CO3,K3)	10

7. Answer any one of the following:-

(7.1)	Discuss major challenges faced in IoT forensic investigations.(CO4,K2)	10
(7.2)	Propose a secure method for remote acquisition of IoT forensic data.(CO4,K4)	10

8. Answer any one of the following:-

(8.1)	Explain wearable device forensic investigation methods(CO5,K2)	10
(8.2)	Explain the role of digital forensic tools in IoT environments(CO5,K2)	10