SRM VALLIAMMAI ENGINEERING COLLEGE
(An Autonomous Institution)

SRM Nagar, Kattankulathur–603203

DEPARTMENT OF CYBERSECURITY

QUESTION BANK

VIII SEMESTER

1923805 – MOBILE AND WIRELESS SECURITY

Regulation– 2019

Academic Year 2024–2025 (Even Semester)

Prepared by

Ms. K. R. Nandhashree, A.P / CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

S.R.M. Nagar, Kattankulathur - 603 203.

DEPARTMENT OF CYBER SECURITY

(Even Semester 2023-2024)

SUBJECT : MOBILE AND WIRELESS SECURITY

SEM / YEAR : VIII SEMESTER/ FINAL YEAR

UNIT – I : BASIC ANALYSIS

Basic Static Techniques, Antivirus Scanning – Static Analysis in practice – Malware Analysis in Virtual, Machines, Basic Dynamic Analysis

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Define Mobile cellular networks	Remember	BTL1
2	Define Cellular network basic concepts	Remember	BTL1
3	What is Cell design?	Remember	BTL1
4	Define Traffic engineering.	Remember	BTL1
5	Define the generation of mobiles	Remember	BTL1
6	List out the general rule IEEE wireless networks	Remember	BTL1
7	Explain WLAN: IEEE 802.11	Remember	BTL1
8	What is DSSS (Direct Sequence Spectrum)?	Understand	BTL2
9	Define FHSS (Frequency Hopping Spread Spectrum)	Understand	BTL2
10	Explain the Infrared with an example	Understand	BTL2
11	Describe MAC layer	Understand	BTL2
12	What is WPAN: IEEE 802.15?	Understand	BTL2
13	Show the purpose of Bluetooth	Apply	BTL3
14	How to use Zigbee?	Apply	BTL3
15	How to use WMAN: IEEE 802.16	Apply	BTL3
16	How to use WMAN mobile: IEEE 802.20	Apply	BTL3
17	Evaluate and analyze MIH: IEEE 802.21 and its examples.	Analyze	BTL4
18	How to analyze WRAN: IEEE 802.22	Analyze	BTL4

19	Analyze the Mobile Internet networks	Analyze	BTL4
20	How to analyze the All-IP, IMS and FMC	Analyze	BTL4
21	Compare the Micro mobility and Macro mobility.	Evaluate	BTL5
22	Compare NEMO and MANET networks	Evaluate	BTL5
23	Explain about the Security in the digital age	Evaluate	BTL5
24	How to create Security awareness.	Create	BTL6
25	How to Trust and subjectivity in security?	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	Explain about Security in the digital age (13)	Remember	BTL1
2	In detail, explain the Threats and risks to telecommunications systems (13)	Remember	BTL1
3	Explain about wireline vulnerabilities to vulnerabilities in wireless communications	Remember	BTL1
4	Explain about MANET networks (13)	Remember	BTL1
5	Explain Mobile cellular networks (13)	Remember	BTL1
6	How to examine the real time IEEE wireless networks (13)	Understand	BTL2
7	Explain the bluetooth with an examples(13)	Understand	BTL2
8	Explain about the mobility. (13)	Understand	BTL2
9	Explain about the structure of WPAN: IEEE 802.15 (13)	Understand	BTL2
10	How to use WLAN: IEEE 802.11 with an example.	Apply	BTL3
11	How to apply the WMAN: IEEE 802.16 with an example. (13)	Apply	BTL3
12	Are there any indications that WMAN mobile: IEEE 802.20? (13)	Apply	BTL3
13	How to use MIH: IEEE 802.21? (13)	Analyze	BTL4
14	How to analyze the structure Mobile Internet networks.	Analyze	BTL4
15	How to analyze the Personal mobility and SIP. (13)	Analyze	BTL4
16	Evaluate the Current trends in mobile networks. (13)	Evaluate	BTL5
17	Explain about the All-IP, IMS and FMC. (13)	Evaluate	BTL5
18	Explain about the B3G and 4G (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Illustrate Security in the digital age. (15)	Evaluate	BTL5
2	Explain in detail Threats and risks to telecommunications systems. (15)	Evaluate	BTL5
3	Summarize the wireline vulnerabilities to vulnerabilities in wireless communications. (15)	Evaluate	BTL5
4	Describe in detail about Mobile Internet networks. (15)	Create	BTL6

5	With some examples explain IEEE wireless networks (15)	Create	BTL6

UNIT – II : SECURITY SERVICES

Security services - Symmetric and asymmetric cryptography - Hash functions - Electronic signatures and MAC- Public Key Infrastructure (PKI) and electronic certificates - Management of cryptographic keys - Cryptographic protocols - IPsec protocol suite - Authentication mechanisms - Access control-Firewalls.

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Define Mobile Security Services.	Remember	BTL1
2	Enumerate various types of security services.	Remember	BTL1
3	Elaborate on the role of replay detection mechanisms in averting the processing of duplicated data.	Remember	BTL1
4	Provide a definition of Cryptography and delineate the classifications.	Remember	BTL1
5	Define RSA and outline its significance.	Remember	BTL1
6	Outline the essential properties characterizing a hash function.	Remember	BTL1
7	Give a comparative analysis between SHA-256 and MD5.	Remember	BTL1
8	Define MAC (Message Authentication Code).	Understand	BTL2
9	Define Electronic Signatures.	Understand	BTL2
10	What is Public Key Infrastructure (PKI)?	Understand	BTL2
11	Examine the challenges associated with the utilization of electronic certificates in digital security.	Understand	BTL2
12	Explain the differences between SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols.	Understand	BTL2
13	Present a visual representation of the SSL handshake protocol exchanges.	Apply	BTL3
14	Define the IPsec protocol suite	Apply	BTL3
15	Explain the concept of Encapsulating Security Payload (ESP).	Apply	BTL3
16	Differentiate between ESP (Encapsulating Security Payload) and AH (Authentication Header) in the IPsec framework.	Apply	BTL3
17	What is SSL VPN.	Analyze	BTL4
18	Define authentication.	Analyze	BTL4
19	Explore the functionalities of Kerberos ticket-based authentication.	Analyze	BTL4
20	Enumerate various types of wireless authentication methods.	Analyze	BTL4
21	Articulate the methods employed in controlling access to a network through AAA.	Evaluate	BTL5
22	Provide an overview of firewalls.	Evaluate	BTL5
23	Highlight the essential characteristics that define an effective firewall.	Evaluate	BTL5
24	Investigate the concept of the vulnerabilities market and its implications in the cybersecurity landscape.	Create	BTL6
25	Give the different types of cryptographic algorithms.	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	Define security services and explain the different types of security services. (13)	Remember	BTL1

2	Define Cryptography and explain the types of cryptography. (13)	Remember	BTL1
3	What is public key cryptography & implementation of RSA algorithm. (13)	Remember	BTL1
4	Discuss on hash functions, emphasizing their role and significance. (13)	Remember	BTL1
5	Examine the implementation aspects of Electronic Signatures and MAC (Message Authentication Code), give illustrative examples. (13)	Remember	BTL1
6	Explain about Public Key Infrastructure (PKI). (7) Explain about electronic certificates. (6)	Understand	BTL2
7	Discuss about Secure Socket Layer (SSL) (13)	Understand	BTL2
8	Define IPsec protocol suite (13)	Understand	BTL2
9	Explain the concepts of IPsec VPN and SSL VPN. (13)	Understand	BTL2
10	Define authentication and categorize the various types of authentications, providing insights into their mechanisms. (13)	Apply	BTL3
11	Elaborate on the methodologies for controlling access to a private network using AAA protocols. (13)	Apply	BTL3
12	What is access control. Give the implementation of access control.(13)	Apply	BTL3
13	Explain about Intrusion detection. (6) Explain about firewalls. (7)	Analyze	BTL4
14	Discuss about MD-5 and SHA-256 (13)	Analyze	BTL4
15	How to analyze the firewall and give the uses of firewall(13)	Analyze	BTL4
16	Evaluate VPN. How it is implemented (13)	Evaluate	BTL5
17	Explain the different types of mobile security attacks(13)	Evaluate	BTL5
18	What is antivirus. Give the uses & application of antivirus (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Evaluate authentication and classify the different types of authentication methods, offering insights into their respective mechanisms. (15)	Evaluate	BTL5
2	Explain the strategies for managing access to a private network through the implementation of AAA protocols. (15)	Evaluate	BTL5
3	Define security services and elucidate the diverse categories of security services, providing detailed explanations. (15)	Evaluate	BTL5
4	Discuss the Secure Socket Layer (SSL) protocol, covering its functionalities and importance in securing communications. (15) (15)	Create	BTL6
5	Explore the principles and functionalities of intrusion detection systems (IDS), and firewalls, including their architecture, functionalities, and significance in network security. (15)	Create	BTL6

UNIT – III : WIRELESS SENSOR NETWORK SECURITY

Introduction–Attacks on wireless sensor networks and counter–measures–Prevention mechanisms: authentication and traffic production–centralized and passive intruder detection intrusion tolerance with multiple routes

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	What is a Denial-of-Service (DoS) attack in wireless sensor networks?	Remember	BTL1

2	How can eavesdropping attacks compromise the security of wireless sensor networks?	Remember	BTL1
3	What are the potential consequences of a wormhole attack?	Remember	BTL1
4	What are the vulnerabilities associated with physical attacks on wireless sensor networks?	Remember	BTL1
5	What are the risks associated with time synchronization attacks?	Remember	BTL1
6	What is a traffic analysis attack and how does it threaten the privacy of wireless sensor networks?	Remember	BTL1
7	What countermeasures can be implemented to prevent attacks on wireless sensor networks?	Remember	BTL1
8	What is authentication and why is it important in network security?	Understand	BTL2
9	What are the common authentication factors used in multi-factor authentication?	Understand	BTL2
10	How does two-factor authentication enhance the security of user accounts?	Understand	BTL2
11	What are the advantages of using biometric authentication methods?	Understand	BTL2
12	Why is password security crucial for authentication?	Understand	BTL2
13	What is the role ofencryption in securing network traffic?	Apply	BTL3
14	How does digital certificates contribute to authentication in network communication?	Apply	BTL3
15	What is the purpose of secure socket layers (SSL) in securing network traffic?	Apply	BTL3
16	What is the role of intrusion detection systems (IDS) in preventing unauthorized access and detecting suspicious network traffic?	Apply	BTL3
17	What are access controls and how do they contribute to preventing unauthorized access to network resources?	Analyze	BTL4
18	Why is strong password management important for authentication?	Analyze	BTL4
19	What is centralized intrusion detection, and how does it differ from decentralized intrusion detection?	Analyze	BTL4
20	Explain the concept of passive intrusion detection and its benefits in network security.	Analyze	BTL4
21	What are the key challenges associated with implementing centralized intrusion detection systems?	Evaluate	BTL5
22	What are the key considerations when designing an intrusion tolerance system with multiple routes?	Evaluate	BTL5
23	Discuss the potential limitations or drawbacks of relying solely on centralized intrusion detection for network security.	Evaluate	BTL5
24	Can you compare and contrast active and passive intrusion detection techniques in the context of intrusion tolerance with multiple routes?	Create	BTL6
25	What are the advantages of using multiple routes in intrusion tolerance mechanisms?	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	What are the major types of attacks that can target wireless sensor networks (WSNs), and what are their potential impacts on network security and functionality? (13)	Remember	BTL1
2	Explain the concept of a Denial-of-Service (DoS) attack in the context of WSNs, and discuss countermeasures that can be employed to mitigate such attacks. (13)	Remember	BTL1

3	Describe the vulnerabilities associated with eavesdropping attacks on WSNs, and discuss encryption and authentication techniques that can be used to protect the confidentiality and integrity of sensor data. (13)	Remember	BTL1
4	What are the potential risks and consequences of node replication attacks in WSNs, and how can techniques such as node authentication and secure localization be utilized to detect and prevent such attacks? (13)	Remember	BTL1
5	Elaborate on the potential risks and consequences of a Sybil attack in a WSN, and discuss techniques such as distributed key management and neighbor verification that can be employed to detect and prevent Sybil attacks. (13)	Remember	BTL1
6	Describe the vulnerabilities associated with data injection attacks in WSNs, and discuss techniques such as data validation and anomaly detection that can be utilized to detect and mitigate such attacks. (13)	Understand	BTL2
7	What are the potential security risks posed by wormhole attacks in WSNs, and how can techniques such as packet leashes and cryptographic mechanisms be employed to detect and prevent these attacks? (13)	Understand	BTL2
8	Describe the vulnerabilities associated with a replay attack in WSNs, and discuss techniques such as sequence number-based detection and time-stamping that can be utilized to detect and prevent replay attacks. (13)	Understand	BTL2
9	What is authentication in the context of network security, and how does it contribute to preventing unauthorized access and attacks? Discuss different authentication mechanisms and their strengths and weaknesses. (13)	Understand	BTL2
10	a) Describe the concept of two-factor authentication (2FA) and its effectiveness in preventing unauthorized access. (6) b) Discuss the different types of factors that can be used in 2FA and their relative strengths. (7)	Apply	BTL3
11	a) Elaborate on the concept of biometric authentication and its role in enhancing network security. (6) b) Discuss the advantages and challenges associated with the implementation of biometric authentication mechanisms.(7)	Apply	BTL3
12	What are the potential risks and vulnerabilities associated with password-based authentication? Discuss best practices for password management and password security to prevent unauthorized access. (13)	Apply	BTL3
13	Explain the role of digital certificates in authentication and their significance in establishing trust between entities in a network. Discuss the process of certificate issuance, validation, and revocation. (13)	Analyze	BTL4
14	How can multi-factor authentication (MFA) enhance network security? Discuss the concept of MFA and the different factors that can be used for authentication, such as passwords, biometrics, tokens, and smart cards. (13)	Analyze	BTL4
15	How can virtual private networks (VPNs) contribute to preventing unauthorized access and protecting network traffic? Discuss the concept of VPNs, their components, and how they establish secure tunnels for data transmission. (13)	Analyze	BTL4
16	a) Discuss the role of firewall systems in preventing unauthorized access and protecting network traffic. (6) b) Explain different types of firewalls, such as packet-filtering, stateful inspection, and application-layer firewalls, and their functionalities. (7)	Evaluate	BTL5
17	Discuss the concept of intrusion prevention systems (IPS) and their role in preventing unauthorized access and detecting and blocking malicious network traffic. (7)	Evaluate	BTL5

	Explain the differences between IDS and IPS and their complementary functions. (6)		
18	What is the role of strong passwords in preventing unauthorized access? Discuss best practices for creating and managing strong passwords, as well as the risks associated with using weak or easily guessable passwords. (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Elaborate on the concept of biometric authentication and its role in enhancing network security. Discuss the advantages and challenges associated with the implementation of biometric authentication mechanisms.(15)	Evaluate	BTL5
2	Describe the vulnerabilities associated with a replay attack in WSNs, and discuss techniques such as sequence number-based detection and time-stamping that can be utilized to detect and prevent replay attacks. (15)	Evaluate	BTL5
3	What is authentication in the context of network security, and how does it contribute to preventing unauthorized access and attacks? Discuss different authentication mechanisms and their strengths and weaknesses. (15)	Evaluate	BTL5
4	Discuss the role of firewall systems in preventing unauthorized access and protecting network traffic. Explain different types of firewalls, such as packet-filtering, stateful inspection, and application-layer firewalls, and their functionalities. (15)	Create	BTL6
5	What are the potential security risks associated with insider threats? Discuss prevention mechanisms, such as user access controls, monitoring, and employee education, to mitigate the risks posed by insider threats. (15)	Create	BTL6

UNIT – IV : KEY MANAGEMENT IN WIRELESS SENSOR NETWORKS

IP Multimedia Subsystem (IMS) - IMS architecture and security - 4G security - Confidentiality - Security of IP-Based Mobile Networks - Vulnerabilities of Mobile IP networks Discovery mechanisms and Authenticity of the mobile location - Data protection (IP tunnels) - IPv6 mobility mechanisms - Mobile IPv6 bootstrapping - Mobility with Mobile IPv4 - Protocol and security - Mobility with MOBIKE - IP mobility with HIP

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Explain the role of Session Initiation Protocol (SIP).	Remember	BTL1
2	How does the Home Subscriber Server (HSS) contribute to the security of IMS networks?	Remember	BTL1
3	Outline the key security features implemented in 4G networks to ensure data confidentiality.	Remember	BTL1
4	Define EPS.	Remember	BTL1
5	Define IP Multimedia Subsystem (IMS).	Remember	BTL1
6	Explain about IMS architecture.	Remember	BTL1
7	What is 4G security.	Remember	BTL1
8	State the term Confidentiality and Data protection.	Understand	BTL2
9	Define Mobile IPv6 bootstrapping.	Understand	BTL2
10	Explain Vulnerabilities of Mobile IP networks.	Understand	BTL2
11	Discuss the role of the Authentication, Authorization, and Accounting	Understand	BTL2

	(AAA) server in ensuring network security.		
12	Explain the challenges associated with securing IP-based mobile networks.	Understand	BTL2
13	Identify and elaborate on two common vulnerabilities in Mobile IP networks.	Apply	BTL3
14	Discuss the importance of authenticating the mobile location information.	Apply	BTL3
15	Describe the purpose of IP tunnels in Mobile IP networks.	Apply	BTL3
16	Discuss the advantages of implementing IPv6 mobility in mobile networks.	Apply	BTL3
17	Explain the process of bootstrapping in Mobile IPv6.	Analyze	BTL4
18	How does bootstrapping contribute to the establishment of secure connections in mobile networks?	Analyze	BTL4
19	Explain the purpose of MOBIKE in IP mobility.	Analyze	BTL4
20	Describe the Host Identity Protocol (HIP).	Analyze	BTL4
21	Discuss the challenges of implementing IPv6 mobility in mobile networks.	Evaluate	BTL5
22	Discuss the security advantages of employing HIP in mobile communication.	Evaluate	BTL5
23	How does MOBIKE contribute to seamless mobility in IP networks	Evaluate	BTL5
24	How to mitigate the risk of Denial of Service (DoS) attacks in Mobile IP environments?	Create	BTL6
25	Explain the role of IP tunnel in data protection.	Create	BTL6
	PART-B (13 Marks)		
Q.No	**Question**	**Competence**	**Level**
1	Provide a detailed overview of the IMS architecture, highlighting the key components. (13)	Remember	BTL1
2	a. Explain SIP Security flaws.(7) b. Analyze the IMS Architecture in detail.(6)	Remember	BTL1
3	Explain in detail about two categories of IMS Security.(13)	Remember	BTL1
4	Describe in detail about IMS Security flaws. (13)	Remember	BTL1
5	Discuss in detail about 4G Security. (13)	Remember	BTL1
6	a. Write short notes on Confidentiality.(6) b. Explain about Visited IMS network security. (7)	Understand	BTL2
7	Discuss the Mobile IPv4 protocol in detail, focusing on its key features and security considerations in the context of mobile communication.	Understand	BTL2
8	Provide a detailed explanation of the Mobile IPv6 bootstrapping process.(13)	Understand	BTL2
9	List in detail about Vulnerabilities of Mobile IP networks.(13)	Understand	BTL2
10	a) Explain Authenticity of the mobile location.(7) b) Describe Data protection (IP tunnels). (6)	Apply	BTL3
11	Explain about IPv6 mobility mechanisms. (13)	Apply	BTL3
12	Explain Mobile IPv6 bootstrapping. (13)	Apply	BTL3
13	Explain IMS Architecture and its Security flaws. (13)	Analyze	BTL4
14	Describe Mobility with MOBIKE in detail. (13)	Analyze	BTL4
15	Write a short note on,	Analyze	BTL4

	a) IPv6 mobility mechanisms (7) b) Mobile IPv4 protocol (6)		
16	Discuss IP mobility with HIP in detail. (13)	Evaluate	BTL5
17	a. Explain about Visited IMS network security. (8) b. IMS core network security. (5)	Evaluate	BTL5
18	Describe the different entities involved in the bootstrapping process. (13)	Create	BTL6

PART-C (15 Marks)

Q.No	Question	Competence	Level
1	Explain in detail about two categories of IMS Security.(15)	Evaluate	BTL5
2	Explain IMS Architecture and its Security flaws. (15)	Evaluate	BTL5
3	a. Explain SIP Security flaws.(7) b. Analyze the IMS A c. Architecture in detail.(8)	Evaluate	BTL5
4	a. Write short notes on Confidentiality? (5) b. Explain Authenticity of the mobile location. (5) c. Describe Data protection (IP tunnels). (5)	Understand	BTL6
5	List in detail about Vulnerabilities of Mobile IP networks. (15)	Understand	BTL6

UNIT – V : BLUETOOTH SECURITY

Overview of Bluetooth Scanning and Reconnaissance - Bluetooth Eavesdropping - Commercial Bluetooth Sniffing - Open-Source Bluetooth Sniffing - ZigBee Security – ZigBee Attacks.

PART-A (2 Marks)

Q.No	Question	Competence	Level
1	Define Bluetooth Security.	Remember	BTL1
2	Define Bluetooth Scanning.	Remember	BTL1
3	Define Reconnaissance.	Remember	BTL1
4	What are the types of Bluetooth Scanning.	Remember	BTL1
5	Explain Bluetooth Security.	Remember	BTL1
6	Define Bluetooth eavesdropping.	Remember	BTL1
7	How to mitigate the risk of eavesdropping in Bluetooth communications?	Remember	BTL1
8	Discuss the role of commercial Bluetooth sniffing tools.	Understand	BTL2
9	Define open-source Bluetooth sniffing tools.	Understand	BTL2
10	Highlight two advantages of using open-source tools for Bluetooth security.	Understand	BTL2
11	Briefly explain the importance of securing ZigBee networks.	Understand	BTL2
12	Outline two common vulnerabilities in the Bluetooth protocol.	Understand	BTL2
13	Define a Bluetooth Man-in-the-Middle (MitM) attack.	Apply	BTL3
14	Explain the role of authentication in Bluetooth security.	Apply	BTL3
15	Define open-source Bluetooth sniffing.	Apply	BTL3
16	Explain the role of Bluetooth security in Bluetooth communication.	Apply	BTL3
17	Describe two authentication mechanisms used in Bluetooth communication.	Analyze	BTL4
18	What is Bluetooth Sniffing.	Analyze	BTL4

19	Define Zigbee Security.	Analyze	BTL4
20	Define two potential risks associated with Bluetooth eavesdropping.	Analyze	BTL4
21	Important of Bluetooth security in security world.	Evaluate	BTL5
22	Briefly explain the importance of securing ZigBee networks.	Evaluate	BTL5
23	Analyze the Commercial Bluetooth Sniffing.	Evaluate	BTL5
24	Define Bluetooth eavesdropping.	Create	BTL6
25	What are the Security mode in Bluetooth.	Create	BTL6

PART-B (13 Marks)

Q.No	Question	Competence	Level
1	Define Bluetooth scanning and briefly explain why reconnaissance is important in Bluetooth security. (13)	Remember	BTL1
2	What is Bluetooth eavesdropping, and why is it a security concern in wireless communication? (13)	Remember	BTL1
3	How do commercial Bluetooth sniffing tools contribute to security assessments, and what challenges may arise when using them? (13)	Remember	BTL1
4	Explain briefly how Bluetooth nodes are organized within a network. (13)	Remember	BTL1
5	Explain briefly about layers in the protocol architecture of a Bluetooth node. (13)		
6	Write a short note of a) Bluetooth Security and its Security mode.(5) b) Authentication and pairing (8)	Understand	BTL2
7	Describe briefly what the security mode in Bluetooth entails.	Understand	BTL2
8	What is the role of authentication and pairing in Bluetooth security?	Understand	BTL2
9	Describe briefly various attacks in Bluetooth.	Understand	BTL2
10	Write a short note of a) Bluetooth scanning.(7) b) Bluetooth eavesdropping. (6)	Apply	BTL3
11	a) Define Bluetooth snarfing and Bluejacking. (5) b) Explain the effect of Bluetooth wardriving attack in Bluetooth security.(5) c) Define Bluebugging. (3)	Apply	BTL3
12	a) Write a note on Attacks on the pairing. (7) b) Describe Cryptanalytics attack in Bluetooth. (6)	Apply	BTL3
13	Define Zigbee Security and explain about the attack on Zigbee security. (13)	Analyze	BTL4
14	a) Explain the Attacks on the Bluetooth stack?(7) b) Write about Cryptanalytic attacks?(6)	Analyze	BTL4
15	Explain about Radio Physical layer and Baseband in protocol architecture in a Bluetooth node. (13)	Analyze	BTL4
16	a) Explain link controller. (6) b) Describe Authentication in bluetooth security.(7)	Evaluate	BTL5
17	Explain about Bluetooth encoding and attack on pairing with bluetooth.(13)	Evaluate	BTL5
18	Discuss the role of securing bluetooth in mobile security. (13)	Create	BTL6

PART-C (`15 Marks)			
Q.No	**Question**	**Competence**	**Level**
1	a) What are the various attacks in Bluetooth and explain Attacks on the pairing & Cryptanalytics attack. (15)	Evaluate	BTL5
2	Define Zigbee Security and explain about the attack on Zigbee security. (15)	Evaluate	BTL5
3	Analyze and explain about a) Bluetooth Scanning.(5) b) Bluetooth Reconnaissance.(5) Bluetooth Sniffing.(5)	Evaluate	BTL5
4	a) Define Bluetooth snarfing and Bluejacking. (5) b) Explain the effect of Bluetooth wardriving attack in Bluetooth security.(5) c) Define Bluebugging. (5)	Create	BTL6
5	Explain briefly about layers in the protocol architecture of a Bluetooth node. (15)	Create	BTL6