



## End Term (Even) Semester Examination May-June 2025

Roll no.....

Name of the Program and semester: Bachelor of Computer Applications (6<sup>th</sup> Semester)

Name of the Course: *Network Security and Cyber Law*

Course Code: TBC602

Time: 3 hour

Maximum Marks: 100

### Note:

- (i) All the questions are compulsory.
- (ii) Answer any two sub questions from a, b and c in each main question.
- (iii) Total marks for each question is 20 (twenty).
- (iv) Each sub-question carries 10 marks.

Q1. //

(2X10=20 Marks)

- a. What are the primary goals of network security? Explain how ISO Security Architecture maps attacks to services and mechanisms. (CO1)
- b. Differentiate between active and passive attacks with examples. How do these attacks challenge the security goals? (CO1)
- c. Describe the working of X.509 Directory Authentication Service. How does it ensure secure identity validation? (CO1)

Q2. //

(2X10=20 Marks)

- a. Analyze the SET protocol in securing online credit card transactions. How does it differ from SSL/TLS? (CO2)
- b. Explain how Pretty Good Privacy (PGP) and S/MIME provide email security. Compare their encryption techniques and key management. (CO2)
- c. Evaluate the role of Wireless Transport Layer Security (WTLS) in mobile applications. What are its key limitations? (CO3)

Q3. //

(2X10=20 Marks)

- a. Explain the structure and role of Authentication Header (AH) and Encapsulating Security Payload (ESP) in IP Security. (CO3)
- b. Analyze the different types of intruders and their methods of gaining unauthorized access. How do intrusion detection systems (IDS) mitigate their impact? (CO4)
- c. Evaluate firewall design principles. What makes a firewall effective against both internal and external threats? (CO4)

Q4. //

(2X10=20 Marks)

- a. What is the genesis and scope of the IT Act 2000? How has it facilitated e-governance in India? (CO4)
- b. Analyze how digital signatures and electronic records are legally recognized under the IT Act. How does this influence e-commerce? (CO5)
- c. Explain how IP addresses, port numbers, and sockets work together in network communication. How can IPs be traced or hidden? (CO5)

Q5. /

(2X10=20 Marks)

- a. Describe the working of ping sweeping, ICMP scanning, and port scanning. How are they used in ethical hacking? (CO5)
- b. Evaluate internal attack vectors like dumpster diving, FTP uploads, shoulder surfing, and instant messengers. Which is the most dangerous and why? (CO6)
- c. Design a security policy that addresses the prevention of DoS and DDoS attacks such as SYN flood, Ping of Death, and Smurf attacks. Include both proactive and reactive measures. (CO6)