Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech S6 (Hons.) Degree Examination May 2025 (2022 Admn)

Course Code: CST394

Course Name: NETWORK SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1		Differentiate between spyware and adware	(3)
2		Outline on the network security model with neat sketch	(3)
3		How to protect the privacy and integrity of a message in Kerberos V4	(3)
4		Differentiate between the monopoly model and delegated CA in Public key Infrastructure.	(3)
5		How public and private keys are established for the messages between Alice and Bob?	(3)
6		Show how to protect the integrity of the messages in PEM	(3)
7		What is the difference between an SSL connection and an SSL session?	(3)
8		What is the purpose of HTTPS?	(3)
9		List four general techniques that firewalls use to control access and enforce the site's security policy	(3)
10		List out the benefits of Transport layer security (TLS)	(3)

PART B

Answer one full question from each module, each carries 14 marks.

Module I

11	a)	Differentiate between host-based and network-based intrusion detection system	(6)
	b)	Explain about Schnorr's scheme for digital signature	(8)

OR

12	a)	Illustrate the requirements and challenges in computer security	(5)
	b)	Given a prime filed q=19 with its primitive root α=10 from various primitive roots {2,3,10,13.14,15}. A user generates it private key Xa=16 for sending a message. A random number is chosen to compute the signature as K=5 , to authenticate the message and send to the other side and the hash value of the message is taken as m=14. Using the Elgamal signature scheme, verify the signatures generated by the sender and receiver.	(9)

Module II

13 a) Why certificate revocation is necessary. Describe the various revocation mechanisms available in public key Infrastructure (8)

b) Differentiate between Kerberos v4 and version5 (6)

OR

14 a) What are the roles of the Oakley key determination protocol and ISAKMP in IPsec? (8)

b) How can you prevent an eavesdropper to decrypt a conversation between Alice and Bob even if the eavesdropper records the entire encrypted session? Describe the method in detail (6)

Module III

15 a) Define non-repudiation. Describe the different ways by which it is implemented in email communication. (8)

b) Illustrate the anomalies that is present in the object formats of PGP (6)

OR

16 a) Describe the differences in S/MIME over PEM (5)

b) Explain how authentication, confidentiality, compression are ensured on messages in PGP (9)

Module IV

17 a) Describe about the web security threats, their consequences and countermeasures (8)

b) Compare SSL and TLS (6)

OR

18 a) How a server and client to authenticate each other and to negotiate an encryption in SSL?.Detail the idea with neat figure. (8)

b) Explain about the SSH connection protocol (6)

Module V

19 a) Describe the services that IEEE802.11 defines for wirelsss LAN (7)

b) How are encryption and decryption done in wired equivalent privacy? Detail with neat figures (7)

OR

20 a) Compare wireless session protocol and Wireless transaction protocol of WAP architecture (6)

b) Explain briefly about packet filtering firewall and circuit level gateway firewall. List the limitations of firewalls. (8)

****