**CSS UT2 Question Bank**

**April 2023**

**Modules from Syllabus**

**MAC, HMAC, Digital signatures, RSA as digital signature, Kerberos,** Needham-Schroeder protocol, Network security basics: OSI layer attacks (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing, Internet Security Protocols: SSL, IPSEC. Network security: IDS, Firewalls

1. How do you use RSA for both authentication and secrecy?

2. Assume a client C wants to communicate with a server S using Kerberos protocol. Infer how can it be achieved?

3. Discuss the objectives of HMAC algorithm and its working.

4. How SSL handshake protocol is used for authentication?

5. Why replay attack is not possible in Kerberos?

6. What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end.

7. What is the difference between MAC and message digest? What are the approaches are used for user authentication in standalone & distributed environment? (Consider algorithm, protocol, methods)

8. Compare and contrast SSL and IPSEC with respect to authenticity, confidentiality, integrity and the level of security provided.

9. What is the difference between proxy, firewall, IDS and IPS (Intrusion Prevention System)?

10. Explain different attacks on OSI layers.

11. What are the different types of viruses and worms? How do they propagate? 12. Explain SQL injection attack.

13. Explain symmetric Needham-Schroeder protocol.

14. What is Firewall? Explain types of Firewall.