# CMPE-552 Database and File Security

# Problem Session 11.01.2022

1. What is digital signature? What is hash (digest) function? What is one-way function? What are requirements to hash function?
2. How digital signature can be used to provide non-repudiation?
3. What is the use of S in message M1 in Kerberos?
4. Why message M2 has two items?
5. What is the use of authenticator in Kerberos?
6. What is the use of Ticket Granting Server in Single Sign-On Kerberos?
7. How nonces can be implemented in Kerberos?
8. How session key is established in Secure Sockets Layer protocol?
9. What is the use of cookies in Passport protocol?
10. How money can be sent with PayPal?
11. How messages to a merchant and payment gateway are bound in Secure Electronic Transaction (SET) protocol?
12. How goods atomicity can be provided by SET extension?
13. What escrow service is?
14. What is notational money? Token money? What is redundancy predicate? How redundancy predicate is used to verify validness of token money? How denomination of token money is verified?
15. Electronic money: Why Simple Digital Cash protocol does not provide anonymity to customer?
16. Electronic money: What does it mean – “blinded token”? Why is it called so? How blinding-un-blinding is made? Examples?
17. XML: What is XML encryption?
18. XML: What is XML signature?
19. Authentication procedures: What is simple unprotected authentication procedure?
20. Authentication procedures: How in simple unprotected authentication client is authenticated to the server?
21. Authentication procedures: How in simple protected authentication client is authenticated to the server?
22. Authentication procedures: Who is authenticated in X.509 one-way authentication works? In two-way authentication? In three-way authentication?
23. Authentication procedures: How client is authenticated to server in Lamport’s One-Time password? Why re-initialization is necessary after N authentications?
24. Authentication procedures: How small number attack is conducted on OTP?
25. Discretionary access control in database management systems. Granting and revoking of privileges. Granting privileges with grant option.
26. Mandatory access control in database management systems. Attribute and tuple classification labels. Filtering of records. Poly-instantiation
27. Role-based access control, hierarchical organization of roles
28. Statistical databases, statistical queries, population, securing personal data by restrictions on statistical queries and introducing noise
29. Covert channels: timing and spatial. Hiding data in IPv4 packets, disk arm covert channel, inter quantum time covert channel