# Problem Session CMPE-455 Security of Computer Systems and Networks, 24.05.2019

1. Digital signature: How in SSL protocol a client authenticates a server? How a server authenticates a client?
2. Digital signature: How a server authenticates a client in Microsoft Passport protocol?
3. Certificates: What for certificates are used? Who issues them? How certificates are protected from forge? How certificate is validated? What three checks are necessary to validate a certificate?
4. Diffie-Hellman key exchange. Man-in-the-middle attack
5. DSA
6. Authentication procedures: What is simple unprotected authentication procedure?
7. Authentication procedures: How in simple unprotected authentication client is authenticated to the server?
8. Authentication procedures: Who is authenticated in X.509 one-way authentication works? In two-way authentication? In three-way authentication?
9. Authentication procedures: How client is authenticated to server in Lamport’s One-Time password? Why re-initialization is necessary after N authentications?
10. Authentication procedures: How small number attack is conducted on OTP?
11. MD5: Messages of what sizes can be used as input to MD5? How original message length is saved in MD5 padding process? What is the length of a message after appending? How appending is conducted? Why in the result 0’s and 1’s padding, the message length shall be congruent to 448 mod 512 bits? What happens if the original message length is divisible by 512?
12. How message is processed in MD5? What two inputs are used by each block in the processing chain? What is the resulting hash? What is the number of bits used in each input of MD5 block? How 128-bit input is represented? How 512-bit is represented? How IV is initialized?
13. How many rounds has MD5 block? What are the inputs/outputs of the rounds? What is the difference between the rounds? What is the similarity of the rounds? How MD5 output is obtained? What arrays, permutations, and logical functions are used in the rounds? How arrays X and T are initialized? What is the use of the permutations? How many steps each round has? What transformations are made in one step of a round?
14. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
15. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
16. Network security: Ethernet frame structure, CRC32, ARP Protocol, ARP request, ARP reply, ARP cache, ARP Spoofing, ARP cache poisoning, ARP Spoofing counter-measures.
17. Kerberos: What is the role of the Key Distribution Sever (KDS)? What shall be shared between KDS, Client, and Server? What is the content of message M1 from Client to KDS? How many items are returned by KDS to Client? What is content of the items of M2? How they are represented? What is a ticket? How Client uses a ticket to get service of Server? What is an authenticator? How Server authenticates Client? How Client can authenticate Server? How Kerberos counters replay attacks? How single sign-on is implanted using Authentication Server and Ticket Granting Server?
18. ECC. Elliptic curve definition. Elliptic curve group over real numbers. Elliptic curve group over GF(p) and GF(2n).
19. ECC. Diffie-Hellman key exchange. Encryption. ECDSA
20. Password attacking. Social engineering. Internal attackers. Malicious software types
21. Physical security. Locks tubular mechanism. Locks attacking. Combination locks. Bar codes. RFIDs. SIM card authentication. Biometric authentication. Wire tapping. Key logging. Emanation blockage. Computer forensics.