# Problem Session CMPE-455 Security of Computer Systems and Networks, 24.05.2024

1. What certificate is? What for it is used? What three conditions are used to verify a certificate? Who issues a certificate? What is CA? How public key of CA is delivered to a verifier?
2. How TLS extends SSL? What is Diffie-Hellman key exchange? How it works? Give an example
3. What is DSA? What for it is used in TLS? How it works? Give an example
4. SHA-512 general schema, message padding, message block size, hash size, initial value and its calculation, elementary function structure, use of constants Kt, derived words Wt, constants Kt calculation, round structure, functions Ch, Maj, Sum0, Sum1, calculation of Wt
5. Simple protected authentications procedures, one-, two-, and three-way authentication procedures using certificates, one-time password
6. AES structure, encryption, decryption, add round key, substitute byte, shift rows, mix columns, polynomials arithmetic, monic polynomial, find (x2+3x+1)(x4-2x3+2) mod (x5+2x+1) over Z6.
7. AES: Expanded key generation.
8. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
9. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
10. Network security: Ethernet frame structure, CRC32, ARP Protocol, ARP request, ARP reply, ARP cache, ARP Spoofing, ARP cache poisoning, ARP Spoofing counter-measures, IP protocol, IP spoofing.
11. ECC. Elliptic curve definition. Elliptic curve group over real numbers. Elliptic curve group over GF(p) and GF(2^m). ECC Diffie-Hellman key exchange, ECC encryption/decryption
12. 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?