# Problem Session CMPE-455 Security of Computer Systems and Networks, 02.06.2023

1. AES: Mix column transformation. Add round key transformation. Expanded key generation.
2. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
3. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
4. 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.
5. 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?
6. Password attacking. Social engineering. Internal attackers. Malicious software types
7. 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.
8. ECC. Elliptic curve definition. Elliptic curve group over real numbers. Elliptic curve group over GF(p), ECC encryption