# Problem Session CMSE-456/CMPE-455 Security of Computer Systems and Networks, 30.05.2025

1) [SHA-512](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/SHA512%2018032025.pdf) (generation of words Wi on p. 361), 2) [Digital signatures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Digital%20Signatures%2019032023.docx) 3) [Ch. 5 AES](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Ch5.AES.docx) (p. 5-11, S-box construction is not included), 4) [Ch. 5 AES part 2](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/AES%20CIPHER.Part2.docx) (p. 2-4, 6-7, inverse S-box construction is not included), 5) [Ch. 5 Network Security](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Ch%205%20Network%20Security%2023042019.docx) , 6) [Authentication procedures](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Authentication%20Procedures.docx) (p. 1-6, MD5 is not included), 7) [Elliptic cryptography](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/ECC%2009052019.docx), and 8) [Physical security](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Physical%20Security%2020052019.docx))

1. How words Wi are generated in SHA-512?
2. What a certificate is? What for is it 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?
3. How TLS extends SSL? What is Diffie-Hellman key exchange? How it works? Give an example
4. What is DSA? What for is it used in TLS? How it works? Give an example
5. 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.
6. AES: Expanded key generation.
7. Network security: five layer Internet structure, IP addresses, IPv4, IPv6, hosts, routers, hops, packets, headers, footers, payload
8. Network security: Ethernet, common bus, star topology, hubs, switches, MAC addresses, MAC address structure, local MAC addresses administering
9. 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.
10. Simple protected authentications procedures, one-, two-, and three-way authentication procedures using certificates, one-time password, small number attack
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. Physical security. Mechanical locks. Attacks on mechanical locks. Electronic locks. Authentication by bar-code, QR-code, SIM cards, RFID, biometric authentication. Physical attacks on computers. Social engineering