**Problem Session CMPE-455 “Security of Computer Systems and Networks” 05.04.2019**

**RSA, Digital signature, Certificates, SSL/TLS, Diffie-Hellman key exchange, DSA**

1. RSA settings, modulo value, Euler totient function, keys generation
2. RSA encryption/decryption
3. Use of RSA public key encryption
4. Use of RSA private key encryption
5. What is RSA digital signature? How calculated? How verified? Why hash function is used? Give example of hash function with 8-bit output
6. 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?
7. What for SSL is used? How certificate is used in SSL? How session key is defined in SSL? How client authenticates a server in SSL? How server authenticates a client in SSL?
8. How TLS extends SSL? What is Diffie-Hellman key exchange? How it works? Give example
9. What is DSA? What for it is used in TLS? How it works? Give example