CMPE553 Problem Session 13.01.2021

1. Key exchange methods. Diffie-Hellman key exchange
2. RSA method, encryption, digital signatures. Key generation, relative primality, GCD, Extended Euclid algorithm, exponentiation by squaring
3. AES method, definition of transformations add round key, substitute byte, shift row, mix column, round key generation procedure; GF(2^8), elements, addition/subtraction, multiplication/division, irreducible polynomial, finding remainder after division by irreducible polynomial
4. DES cipher encryption/decryption, round transformation, round function, initial permutation and its inverse, Expansion/permutation, S-boxes, Permutation of S-boxes outputs, round key generation