CMPE553 Problem Session 13.01.2021

1. Key exchange methods. Diffie-Hellman key exchange

Q=11

$$α?$$

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | ~~0~~ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $α=2^{n}$ mod q | ~~1~~ | 2 | 4 | 8 | 5 | 10 | 10\*2=20 mod 11= 9 | 18 mod 11 =7 | 14 mod 11 =3 | 6 | 12 mod 11 =1 |
| Q=7 |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  | 2 | 4 | 1 | 2 | 4 | 1 |  |  |  |  |

Xa=2, Xb=3

Ya=2^2 mod 11 = 4

Yb=2^3 mod 11 = 8

A: K=(Yb)^Xa mod q = 8^2 mod 11 = 64 mod 11 = 9

B: K’=(Ya)^Xb mod q = 4^3 mod 11 = 64 mod 11 = 9 => K=K’

1. RSA method, encryption, digital signatures. Key generation, relative primality, GCD, Extended Euclid algorithm, exponentiation by squaring

12^(-1) mod 345?

1. 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
2. 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