Name – Krishnaprasad Awala

Enrollment no – MITU21BTITD006

Roll no – D2215004

Q. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value p= 7. Find out the prinitive root 'q' using 'p'. If Alice’s private key is 3 and Bob’s private key is 4, what is the secret key they exchanged?

To find the primitive root 'q' using 'p', we need to check the values of q for which the equation q^x mod p takes on all values from 1 to p-1 at least once, where x is an integer. One way to do this is to check each value of q from 2 to p-1 and see if it satisfies the condition. However, since p=7 is a small prime, we can simply calculate the powers of 2, 3, and 4 modulo 7 and see which one generates all possible values:

q^1 mod p = q (where q is any value from 2 to 6) q^2 mod p = (q^1 mod p) \* (q^1 mod p) mod p q^3 mod p = (q^2 mod p) \* (q^1 mod p) mod p q^4 mod p = (q^2 mod p) \* (q^2 mod p) mod p q^5 mod p = (q^4 mod p) \* (q^1 mod p) mod p q^6 mod p = (q^3 mod p) \* (q^3 mod p) mod p

If we check each of these values for q=2,3,4,5,6, we find that only q=3 is a primitive root modulo 7, since it generates all values from 1 to 6.

Now, to calculate the secret key that Alice and Bob exchange, they each generate a public key by calculating q raised to their private key mod p:

Alice: A = q^a mod p = 3^3 mod 7 = 27 mod 7 = 6 Bob: B = q^b mod p = 3^4 mod 7 = 81 mod 7 = 4

Alice and Bob exchange their public keys A and B. To calculate the secret key, Alice raises Bob's public key to her private key, and Bob raises Alice's public key to his private key:

Alice: K = B^a mod p = 4^3 mod 7 = 64 mod 7 = 1 Bob: K = A^b mod p = 6^4 mod 7 = 1296 mod 7 = 1

Both Alice and Bob now have the secret key K=1, which they can use for secure communication.

