**NIRMA UNIVERSITY**

**Institute of Technology**

**B.Tech. Computer Science and Engineering**

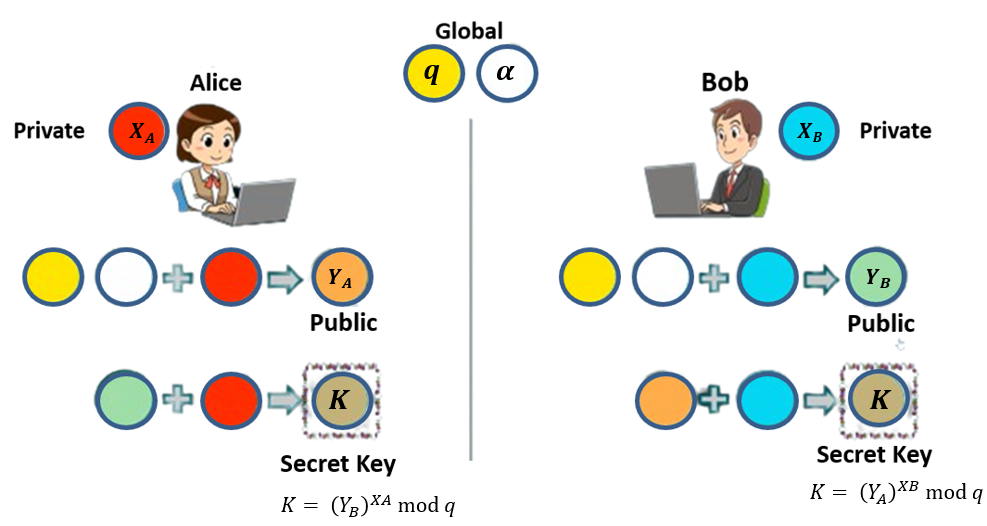
**2CSDE54 Information and Network Security**

**Implement the Diffie-Hellman Key Exchange algorithm for a given problem..**

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime **q** and **α** (a primitive root of q) and two private values **Xa** and **Xb.**

q and α are both publicly available numbers. Users (say Alice and Bob) pick private values **Xa** and **Xb** and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

****

**Step-by-Step explanation is as follows:**

1. Global Public Elements

prime number

< and is primitive root of

1. User A Key Generation

Select private

Calculate public

1. User B Key Generation

Select private

Calculate public

1. User A Key Generation

Select private

Calculate public

1. User B Key Generation

Select private

Calculate public

1. Calculation of Secret Key by User A
2. Calculation of Secret Key by User b

Solved Example:

* Alice and bob agrees on a prime number
* as primitive root of
* Alice selects a private integer
* Alice computes =>
* Bob selects a private integer
* Bob computes =>
* Alice sends to Bob and Bob sends to Alice
* Alice computes key =>
* Bob computes key =>

**Instructions:**

1. You need to read the value of **Xa**, **Xb** and from the file and compute the value of **K.**
2. Create separate function to compute **primitive root()** using the following formula.

**Example:** p = 7 then primitive root is 3 because powers of 3 mod 7 generates all the integers from 1 to 6 **i.e. 1 to (p-1)**