# **PRACTICAL -9**

**Aim:** Implement Diffie-Hellman Key exchange Method.

**Solution :**

public class DiffieHellmanAlgorithm {

public static int PrivateKay(int publicKey, int alpha, int q) {

return ((int) Math.pow(alpha, publicKey) % q);

}

public static String checkExchange(int ya, int yb, int xa, int xb, int q) {

int k1 = ((int) Math.pow(yb, xa) % q);

int k2 = ((int) Math.pow(ya, xb) % q);

boolean scusses = (k1 == k2);

if (scusses) {

return "SUCCESSFULL KEY CHANGE";

}

return "Failed KEY CHANGE";

}

public static void main(String[] args) {

int xa = 2;

int xb = 3;

int alpha = 327;

int q = 919;

int ya = PrivateKay(xa, alpha, q);

int yb = PrivateKay(xb, alpha, q);

String ans = checkExchange(ya, yb, xa, xb, q);

System.out.println("Public Key A : " + xa + " Private Key A : " + ya);

System.out.println("Public Key B : " + xb + " Private Key B : " + yb);

System.out.println(ans);

}

}

**Output** (Screenshot):

Signature of Faculty:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: