**Name – Snehal Trigune**

**Roll No – B1821024**

**Batch - A2**

**Assignment No 3**

**Title – Implementation of Diffie-Hellman key exchange**

**Program –**

package Diffie\_Hellman;

// using the Diffie-Hellman Key exchange algorithm

class Diffie\_Hellman {

// Power function to return value of a ^ b mod P

private static long power(long a, long b, long p)

{

if (b == 1)

return a;

else

return (((long)Math.pow(a, b)) % p);

}

// Driver code

public static void main(String[] args)

{

long P, G, x, a, y, b, ka, kb;

// Both the persons will be agreed upon the

// public keys G and P

// A prime number P is taken

P = 23;

System.out.println("The value of P:" + P);

// A primitive root for P, G is taken

G = 9;

System.out.println("The value of G:" + G);

// Alice will choose the private key a

// a is the chosen private key

a = 4;

System.out.println("The private key a for Alice:" + a);

// Gets the generated key

x = power(G, a, P);

// Bob will choose the private key b

// b is the chosen private key

b = 3;

System.out.println("The private key b for Bob:" + b);

// Gets the generated key

y = power(G, b, P);

// Generating the secret key after the exchange

// of keys

ka = power(y, a, P); // Secret key for Alice

kb = power(x, b, P); // Secret key for Bob

System.out.println("Secret key for the Alice is:" + ka);

System.out.println("Secret key for the Bob is:" + kb);

}

}

**Output –**

The value of P:23

The value of G:9

The private key a for Alice:4

The private key b for Bob:3

Secret key for the Alice is:9

Secret key for the Bob is:9