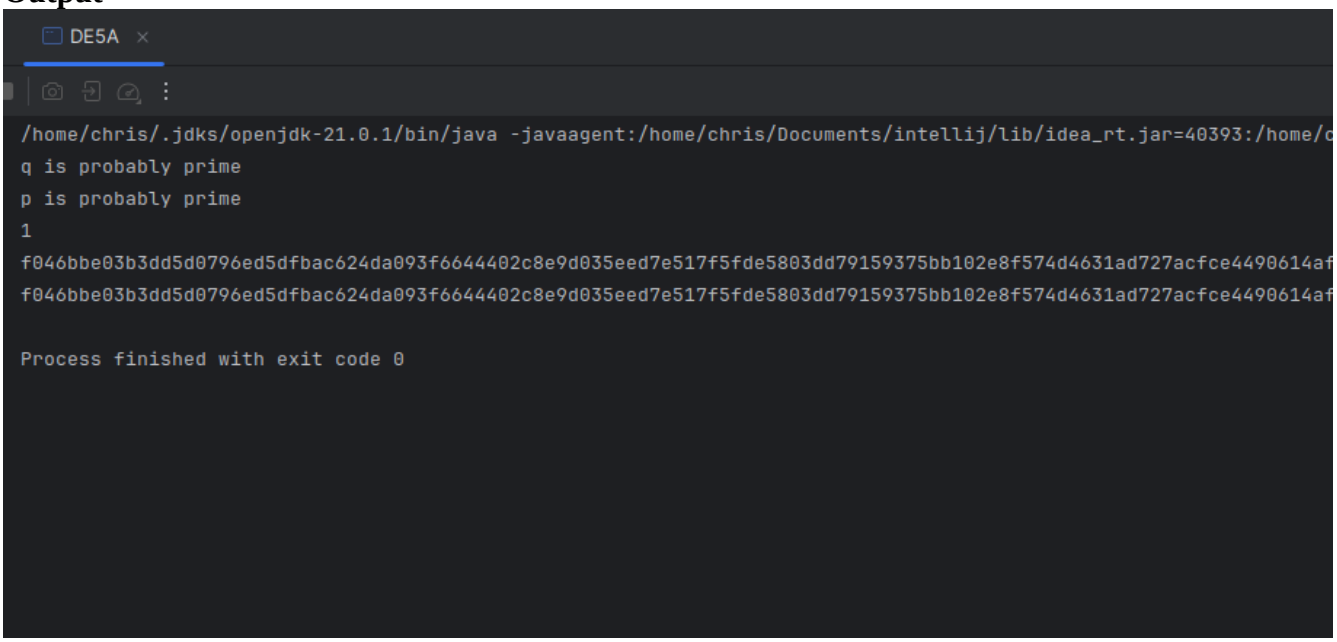
CS5125 Assignment 2
Chris Lee

Code

```
// DE5A.java CS5125/6025 cheng 2024
// This work was done by Chris Lee (chruffins).
// checking primality of Group 5 q and (q-1)/2
// checking that 2 is a primitive root of q
// generating private and public keys for Alice and Bob
// finding the secret they can share using the other's public key
// needs file DHgroup5.txt
// Usage: java DE5A
import java.math.*;
import java.io.*;
import java.util.*;
public class DE5A{
   String hexQ = null;
   BigInteger q = null;
   BigInteger p = null; // p = (q-1)/ 2
   static BigInteger two = new BigInteger("2");
   void readQ(String filename){
      Scanner in = null;
      try {
         in = new Scanner(new File(filename));
      } catch (FileNotFoundException e){
         System.err.println(filename + " not found");
         System.exit(1);
      }
      hexQ = in.nextLine();
      in.close();
      q = new BigInteger(hexQ, 16);
   }
   void testPrimality(){
      if (q.isProbablePrime(200))
         System.out.println("q is probably prime");
      p = q.subtract(BigInteger.ONE).divide(two); // your code for (q-1)/2
      if (p.isProbablePrime(200))
         System.out.println("p is probably prime");
   }
   void testPrimitiveness(){
      BigInteger pq2 = two.modPow(p, q); // compute pow(2, p) mod q
      System.out.println(pq2.toString(16));
   }
   void diffieHellman(){
      Random random = new Random();
      BigInteger Xa = new BigInteger(1235, random); // Alice's private key
      BigInteger Xb = new BigInteger(1235, random); // Bob's private key
      // p is alpha here so use that
      BigInteger Ya = p.modPow(Xa, q); // Alice's public key
      BigInteger Yb = p.modPow(Xb, q); // Bob's public key
      BigInteger K1 = Yb.modPow(Xa, q); // how Alice computes the shared secret using Xa and Yb
      BigInteger K2 = Ya.modPow(Xb, q); // how Bob computes the shared secret using Xb and Ya
      System.out.println(K1.toString(16));
      System.out.println(K2.toString(16)); // make sure K1 == K2.
   }
   public static void main(String[] args){
      DE5A de5 = new DE5A();
      de5.readQ("DHgroup5.txt");
```

```
        de5.testPrimality();
        de5.testPrimitiveness();
        de5.diffieHellman();
    }
}
```

Output



The output key is cut off. Here's the full key:

f046bbe03b3dd5d0796ed5dfbac624da093f6644402c8e9d035eed7e517f5fde5803dd79159375bb102e8f574d4631ad727acfce4490614af0ef190f35ebf4aeb39781fac7ebe717d0269909ad511a45f9eeab9f32a7d86a9e5d664a80c055895173464bf141d89dce6381b331c34ee2c17c4c0874f72cd19efcf4c9b7a77595dd3acc41a8cdcc0c24820b52ade75532dfb1da77deab6a7ff5f78a171dc7de982af988dd7b631d53634bbcddc31de0761a26449274ad57c978316a6de8be3b36