**/\***

**NAME: FURKHAN MUJIBODDEN SHAIKH**

**CLASS: BECSEII**

**AIM: Write a program to implement ElGamal encryption algorithm.**

**ROLL: 63**

**--------------------------------------------------------------------**

**\*/**

**import java.math.\*;**

**import java.util.\*;**

**import java.security.\*;**

**import java.io.\*;**

**public class EXP9**

**{**

**public static void main(String[] args) throws IOException**

**{**

**Scanner in = new Scanner(System.in);**

**BigInteger p, b, c, secretKey;**

**Random sc = new SecureRandom();**

**secretKey = new BigInteger("12345678901234567890");**

**System.out.println("Secret Key = " + secretKey);**

**p = BigInteger.probablePrime(64, sc);**

**b = new BigInteger("3");**

**c = b.modPow(secretKey, p);**

**System.out.println("p = " + p);**

**System.out.println("b = " + b);**

**System.out.println("c = " + c);**

**System.out.println("Enter your Big Number message ");**

**String s = in.nextLine();**

**BigInteger X = new BigInteger(s);**

**BigInteger r = new BigInteger(64, sc);**

**BigInteger EC = X.multiply(c.modPow(r, p)).mod(p);**

**BigInteger brmodp = b.modPow(r, p);**

**System.out.println("Plaintext = " + X);**

**System.out.println("r = " + r);**

**System.out.println("EC = " + EC);**

**System.out.println("b^r mod p = " + brmodp);**

**BigInteger crmodp = brmodp.modPow(secretKey, p);**

**BigInteger d = crmodp.modInverse(p);**

**BigInteger ad = d.multiply(EC).mod(p);**

**System.out.println("\n\nc^r mod p = " + crmodp);**

**System.out.println("d = " + d);**

**System.out.println("Decrypted Code is: " + ad);**

**in.close();**

**}**

**}**

**/\***

**OUTPUT:**

**Secret Key = 12345678901234567890**

**p = 11011430496307263017**

**b = 3**

**c = 762684688640510407**

**Enter your Big Number message**

**123456778**

**Plaintext = 123456778**

**r = 1466427748554375912**

**EC = 11001532579463450987**

**b^r mod p = 7637210775905307426**

**c^r mod p = 3743922534478032680**

**d = 4009754735560853414**

**Decrypted Code is: 123456778**

**\*/**