Ex No : 3

RSA ALGORITHM

**Program :**

import java.io.BufferedReader;

import java.io.InputStreamReader;

import java.math.\*;

import java.util.Random;

import java.util.Scanner;

public class RSA {

static Scanner sc = new Scanner(System.in);

public static void main(String[] args) {

// TODO code application logic here

System.out.print("Enter a Prime number: ");

BigInteger p = sc.nextBigInteger(); // Here's one prime number..

System.out.print("Enter another prime number: ");

BigInteger q = sc.nextBigInteger(); // ..and another.

BigInteger n = p.multiply(q);

BigInteger n2 = p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE));

BigInteger e = generateE(n2);

BigInteger d = e.modInverse(n2); // Here's the multiplicative inverse

System.out.println("Encryption keys are: " + e + ", " + n);

System.out.println("Decryption keys are: " + d + ", " + n);

}

public static BigInteger generateE(BigInteger fiofn) {

int y, intGCD;

BigInteger e;

BigInteger gcd;

Random x = new Random();

do {

y = x.nextInt(fiofn.intValue()-1);

String z = Integer.toString(y);

e = new BigInteger(z);

gcd = fiofn.gcd(e);

intGCD = gcd.intValue();

}

while(y <= 2 || intGCD != 1);

return e;

}

}

**Output :**

