# Bansilal Ramnath Agarwal Charitable Trust’s

Vishwakarma Institute of Technology, Pune-37

*(An autonomous Institute of Savitribai Phule Pune University)*

**

# Department of Computer Engineering

|  |  |
| --- | --- |
| **Name** | Thakare Prathamesh Prabhakar |
| **Batch** | Batch - 2 |
| **PRN** | 12220016 |
| **Roll No** | 58 |
| **Division** | CS-D |
| **Subject** | Cyber Security |

**Problem Statement:** Implement Simplified AES Algorithm.

**Code:**

import java.util.\*;

import java.math.\*;

public class RSA

{

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

public static void main(String args[])

{

int nSender = 0, eSender = 0, phiSender = 0;

System.out.print("This program is the implementation of RSA Algorithm.");

System.out.print("\n\nEnter the first prime number: ");

int no1Prime = sc.nextInt();

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

int no2Prime = sc.nextInt();

nSender = calculateN(no1Prime, no2Prime);

System.out.print("\nValue of n: "+ nSender);

phiSender = calculatePhi(no1Prime, no2Prime);

System.out.print("\nValue of phi: "+ phiSender);

eSender = calculateE(phiSender);

System.out.print("\nValue of e: "+ eSender);

int inverse = calculateD(eSender, phiSender);

//System.out.print("\nValue of d: "+ inverse);

int decryptionKey = inverse % phiSender;

System.out.print("\nValue of decryption key: "+ decryptionKey);

sc.nextLine();

String msg = "";

System.out.print("\n\nEnter your meaasge: ");

msg = sc.nextLine();

long plainText = convertMsgToDecimal(msg);

System.out.print("\nPlain text in decimal format: "+ plainText);

long ptPowE = (long)Math.pow(plainText, eSender);

System.out.print("\nPlain text power to e: "+ ptPowE);

long decryptedText = ptPowE % nSender;

System.out.print("\nCipher Text: "+ decryptedText);

long dtPowD = (long)Math.pow(decryptedText, decryptionKey);

//long encryptedText = dtPowD % nSender;

//System.out.print("\nEncrypted Text: "+ encryptedText);

//encryption

long encryptedText = (long)Math.pow(decryptedText, decryptionKey) % nSender;

System.out.print("\nAt receiver's side: "+ encryptedText);

}

public static int calculateN(int p, int q)

{

return p \* q;

}

public static int calculatePhi(int p, int q)

{

return (p-1) \* (q-1);

}

public static int calculateE(int phi)

{

boolean flag = false;

Random rand = new Random();

do

{

int random = rand.nextInt(phi);

if(random == 1)

continue;

BigInteger bigPhi = BigInteger.valueOf(phi);

BigInteger bigInt = BigInteger.valueOf(random);

BigInteger temp = bigPhi.gcd(bigInt);

if(temp.intValue() == 1)

{

flag = true;

return random;

}

}while(flag == false);

return 0;

}

public static int calculateD(int e, int phi)

{

int i = 1, j = 1;

while(((e\*i) - (phi\*j)) != 1)

{

if((i\*e) > (j \* phi))

j++;

i++;

//System.out.println("i: "+i+ "j: "+j);

}

return i;

}

public static long convertMsgToDecimal(String msg)

{

String str = "";

for(int i = 0; i < msg.length(); i++)

{

str = str + (int)msg.charAt(i);

}

return Long.parseLong(str);

}

}

**Output:**

