Cyber Security

J-Component REVIEW-III

TITLE: Cryptosystem using Displacement equation

SUBMITTED TO:

PROF. Chandrasegar T

SLOT: C1

PROJECT MEMBERS –

17BCE0422 - SAHITH D
17BCI 0147 - KARUMANCHI RAJESH

REVIEW -1

Cyber Security - CSE4003

Digital assignment - 1

Name	Reg No
Sahith D	17BCE0422
Kamandhi Rajesh	17BCE0147

1. Taking displacement equation $v^2 - u^2 = 2as$

$$\Rightarrow \frac{v^2}{2as} - \frac{u^2}{2as} = 1 \quad \text{— (1)}$$

2. Append RSA terminology

$$\frac{(v+e)^2}{2as} - \frac{(u+\phi(n))^2}{2as} = 1$$

$$\frac{v^2+e^2+2ve}{2as} - \frac{(u^2+\phi(n)^2+2u\phi(n))}{2as} = 1$$

Apply mod $\phi(n)$ on both sides

$$\frac{v^2}{2as} + \frac{e^2+2ve}{2as} - \frac{u^2}{2as} = 1 \bmod \phi(n)$$

$$1 + \frac{e(e+2v) \bmod \phi(n)}{2as} = 1 \bmod \phi(n)$$

↓ equate to α

$$1 + \frac{e(e+2v)}{2as} = \alpha$$

$$\therefore 1 \cdot \alpha - \frac{e}{2as}(e+2v) \bmod \phi(n) = 1$$

Now, encryption

$M^{\alpha} \longrightarrow C \cdot T_1$

$M^{(e+2v) \bmod \phi(N)} \longrightarrow C \cdot T_2$

Decryption

$CT_1 \cdot CT_2^{-s} \pmod{\phi(N)}$

Key Generation

Input (V, P, q)

output Public key $(\alpha, e+2V, N)$

Private key (e, as, N)

Let, the Randomly given input be $P=3, q=5, V=3$

The R.S.A Components are:

(a) Euler totient Function, $\phi(N) = (P-1).(q-1) = 2 \times 4 = 8$

(b) The Common modulus, $N = Pq = 3 \times 5 = 15$

(c) Select R.S.A Public key e, Satisfying $\frac{\phi(N)}{2} < e < \phi(N)$ and

$\gcd(e, \phi(N)) = 1$

Let, e be $5 \Rightarrow e + 2V = 5 + 6 = 11$

$\therefore$ public key $= (\alpha, 11, 15)$

Now, For as Consider the equation

$V^2 - u^2 = 2as$

we Can Select it Randomly, Let $u = 2$

$\therefore 9 - 4 = 2as$

$2as = 5$

Encryption:-

Let M be 5

$C.T_1 \Rightarrow M^x = (5)^x$

Now, $C.T_2 \Rightarrow 5^{(11 \bmod 8)} \Rightarrow 5^3 \Rightarrow 125 \bmod 15$

$\Rightarrow 5$

$5^3 = 8.3$

23×625

$10 \cdot 10$

Decryption:-

$D = CT_1 \cdot CT_2^{-e/203} \bmod 8 \cdot \bmod 15$

$D = (5)^x \cdot 5^{(-\frac{x'}{8} \bmod 8)} \bmod 15$

$\Rightarrow 5^a \cdot \bmod 15 \Rightarrow 5$

Review-2 (Code and Snapshot)

CODE:

```
import java.math.*;
import java.util.*;
import java.io.*;
import java.lang.Exception;

public class displacement {
    public static void main(String[] args)
    {
        int ieph,inte,alpha;
        BigInteger p, q, sub1, phin, n, v, e, a, two, m, e_phi,e2v,u,two_as,de
c,en1;
        p=new BigInteger("53");
        q=new BigInteger("59");
        sub1=new BigInteger("1");
        phin= ((p.subtract(sub1)).multiply(q.subtract(sub1)));
        n=p.multiply(q);
        v=new BigInteger("13650076834972190782364291762870185962");
        two_as= new BigInteger("186054328713671");
        two_as= two_as.modInverse(phin);
        System.out.println("Enter the value for e such that GCD of e "+phin+"
is 1");
        Scanner sc=new Scanner(System.in);
        e = sc.nextBigInteger();
        // key generatiom
        two = new BigInteger("2");
        e2v = e.add(v.multiply(two));
        a=((sub1.add(e.multiply(e2v))).multiply(two_as)).mod(phin);

        // encryption
        System.out.println("enter the message");
        m=sc.nextBigInteger();


        e_phi= phin.subtract(e2v);
        ieph = e_phi.intValue();
        alpha=a.intValue();
        en1=m.pow(alpha).mod(n);
        m=m.pow(ieph);
        m=m.mod(n);
        m=m.multiply(en1);
        System.out.println("encrypted value is "+m);
        // decryption
        System.out.println("enter your private u square value");
```

```
        u=sc.nextBigInteger();
        two_as=(v.pow(2)).subtract(u);
        two_as=two_as.modInverse(phin);
        e=e.mod(phin);
        e=(e.multiply(two_as)).mod(phin);
        inte=e.intValue();
        dec=(m.pow(inte)).mod(n);
        System.out.println("decrypted_value is "+2);

    }
}
```

Output:

```
PS C:\Users\Rajesh\desktop> javac GFG.java
PS C:\Users\Rajesh\desktop> java GFG
Enter the value for e such that GCD of e 3016 is 1
7
enter the message
2
encrypted value is 3324741
enter your private u square value
1863245976006444213101034643996567872101109664142594723674866997507905791 15
decrypted_value is 2
```

Review 3

Analysis of Cryptographic System using different Files

Code:

Encryption Code:

```
import java.math.*;
import java.util.*;
import java.io.*;
import java.lang.Exception;

public class GFG {

    public static void main(String[] args)
    {
        long t1 = System.currentTimeMillis();
        int ieph,inte,alpha, k;
        BigInteger p, q, sub1, phin, n, v, e_, a, two, m, e_phi,e2v,u,two_as,d
ec,en1;
        p=new BigInteger("3");
        q=new BigInteger("5");
        sub1=new BigInteger("1");
        phin= ((p.subtract(sub1)).multiply(q.subtract(sub1)));
        n=p.multiply(q);
        v=new BigInteger("3");
        two_as= new BigInteger("7");
        two_as= two_as.modInverse(phin);
        System.out.println("Enter the value for e such that GCD of e "+phin+"
is 1");
        Scanner sc=new Scanner(System.in);
        e_ = sc.nextBigInteger();
        // key generatiom
        two = new BigInteger("2");
        e2v = e_.add(v.multiply(two));
        a=((sub1.add(e_.multiply(e2v))).multiply(two_as)).mod(phin);
        String strFilePath = "C://Users////Rajesh//Desktop//encrypt.txt";
        // encryption
        try
        {
            File file=new File("1mb.txt");
            FileReader fr=new FileReader(file);
            BufferedReader br=new BufferedReader(fr);
            StringBuffer sb=new StringBuffer();
            String line;
            while((line=br.readLine())!=null)
            {
                String[] arrOfStr = line.split(" ");

                    for (String z : arrOfStr){ // reads numbers space by space
```

```
                        m=new BigInteger(z);


                        e_phi= e2v.mod(phin);
                        ieph = e_phi.intValue();
                        alpha=a.intValue();
                        en1=m.pow(alpha).mod(n);
                        m=m.pow(ieph);
                        m=m.mod(n);
                        m=m.multiply(en1);
                        //System.out.println("encrypted value is "+m);
                        k=m.intValue();
                        FileOutputStream fos = new FileOutputStream(strFilePat
h);
                        DataOutputStream dos = new DataOutputStream(fos);
                        dos.writeInt(k);

                    }

            }
            fr.close();    //closes the stream and release the resources

            //System.out.println(sb.toString());   //returns a string that tex
tually represents the object
        }
        catch(IOException e)
        {
        e.printStackTrace();
        }
        long t2 = System.currentTimeMillis();
        double res = (double)(t2 - t1) / (double)1000;
        System.out.println("Total Time for encryption is: " + res + " s");




    }
}
```

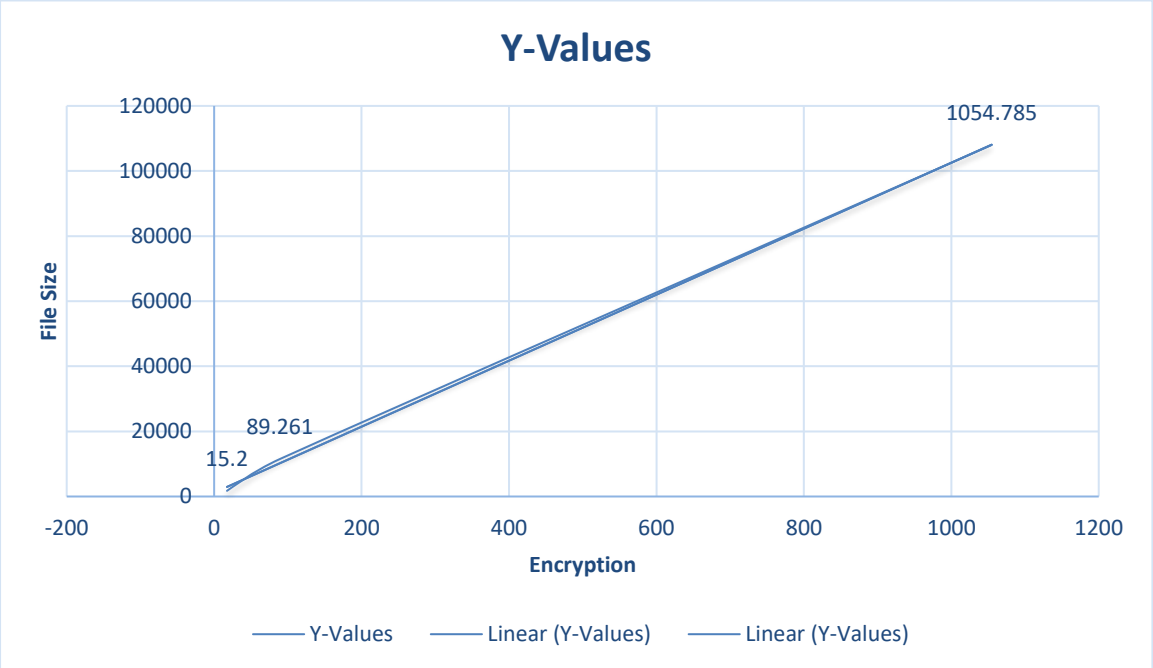
Outputs:

```
PS C:\Users\Rajesh\desktop> javac GFG.java
PS C:\Users\Rajesh\desktop> java GFG
Enter the value for e such that GCD of e 8 is 1
7
Total Time for encryption is: 15.2 s
PS C:\Users\Rajesh\desktop>
```

```
PS C:\Users\Rajesh\desktop> javac GFG.java
PS C:\Users\Rajesh\desktop> java GFG
Enter the value for e such that GCD of e 8 is 1
7
Total Time for encryption is: 89.261 s
```

```
PS C:\Users\Rajesh\desktop> javac GFG.java
PS C:\Users\Rajesh\desktop> java GFG
Enter the value for e such that GCD of e 8 is 1
7
Total Time for encryption is: 1054.785 s
PS C:\Users\Rajesh\desktop>
```

Graph:



Decryption Code:

```
import java.math.*;
import java.util.*;
import java.io.*;
import java.lang.Exception;
public class decrypt {
```

```
    public static void main(String[] args)
    {
        long t1 = System.currentTimeMillis();
        int ieph,inte,alpha,k;
        BigInteger p, q, sub1, phin, n, v, e_, a, two, m, e_phi,e2v,u,two_as,d
ec,en1;
        p=new BigInteger("3");
        q=new BigInteger("5");
        sub1=new BigInteger("1");
        phin= ((p.subtract(sub1)).multiply(q.subtract(sub1)));
        n=p.multiply(q);
        Scanner sc=new Scanner(System.in);
        v=new BigInteger("3");
        System.out.println("Enter the value for e such that GCD of e "+phin+"
is 1");

        e_ = sc.nextBigInteger();
        try
        {
            File file=new File("encrypt.txt");    //creates a new file instanc
e
            FileReader fr=new FileReader(file);   //reads the file
            BufferedReader br=new BufferedReader(fr);  //creates a buffering c
haracter input stream
            StringBuffer sb=new StringBuffer();    //constructs a string buffe
r with no characters
            String line;
            System.out.println("please enter our private u^2 value");
            u=sc.nextBigInteger();
            String strFilePath = "C://Users////Rajesh//Desktop//decrypt.txt";
            while((line=br.readLine())!=null)
            {
                String[] arrOfStr = line.split(" ");

                    for (String z : arrOfStr){

                        m=new BigInteger(z);

                        two_as=(v.pow(2)).subtract(u);
                        two_as=two_as.modInverse(phin);
                        e_=phin.subtract(e_);
                        e_=(e_.multiply(two_as)).mod(phin);
                        inte=e_.intValue();
                        dec=(m.pow(inte)).mod(n);
                        //System.out.println("Decrypted value is "+dec);
                        k=dec.intValue();
                        FileOutputStream fos = new FileOutputStream(strFilePat
h);
```

```
                    DataOutputStream dos = new DataOutputStream(fos);
                    dos.writeInt(k);
                }

            }
            fr.close();
        }
        catch(IOException e)
        {
        e.printStackTrace();
        }
        long t2 = System.currentTimeMillis();
        double res = (double)(t2 - t1) / (double)1000;
        System.out.println("Total Time for decryption is: "+res+" s");

    }
}
```

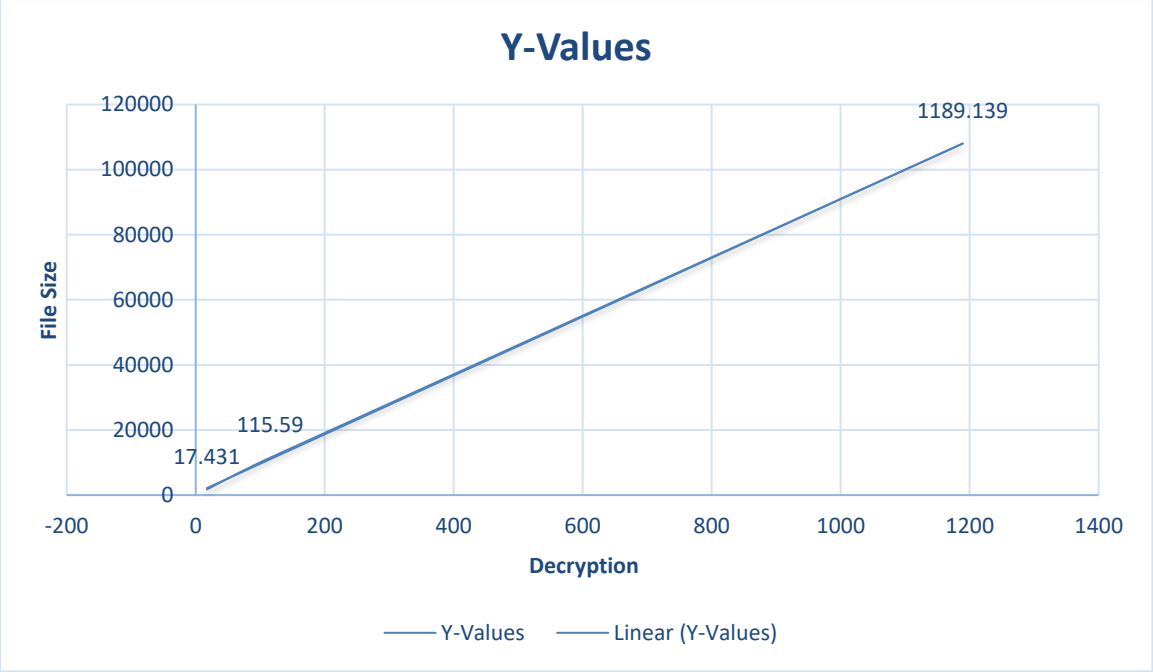
Output:

```
Enter the value for e such that GCD of e 8 is 1
7
please enter our private u^2 value
2
Total Time for decryption is: 17.431 s
PS C:\Users\Rajesh\desktop>
```

```
PS C:\Users\Rajesh\desktop> javac decrypt.java
PS C:\Users\Rajesh\desktop> java decrypt
Enter the value for e such that GCD of e 8 is 1
7
please enter our private u^2 value
2
Total Time for decryption is: 115.59 s
```

```
PS C:\Users\Rajesh\desktop> javac decrypt.java
PS C:\Users\Rajesh\desktop> java decrypt
Enter the value for e such that GCD of e 8 is 1
7
please enter our private u^2 value
2
Total Time for decryption is: 1189.139 s
PS C:\Users\Rajesh\desktop>
```

Graph



Decryption vs Encryption Times: