RSA - Implementation

Code

```java
import java.math.BigInteger;
import java.util.*;
public class RSA {
    static int gcd(int x, int y) {
        if(x == 0) {
            return y;
        }
        else {
            return gcd(y % x, x);
        }
    }
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);
        int prime1, prime2, product, phi, publicKey, privateKey = 0,
plainTextInt, cipherTextInt, decryptedTextInt;
        System.out.println("Implementing RSA algorithm: ");
        System.out.println("Let us generate the keys...");
        System.out.print("Choose 2 prime numbers: ");
        prime1 = sc.nextInt();
        prime2 = sc.nextInt();
        product = prime1 * prime2;
        phi = (prime1 - 1) * (prime2 - 1);
        System.out.println("Phi was calculated to be: " + phi);

        for(publicKey = 2; publicKey < phi; publicKey++) {
            if(gcd(publicKey, phi) == 1) {
                break;
            }
        }

        System.out.println("Public key was calculated to be: (" +
publicKey + ", " + product + ")");

        for(int i = 0; i <= 9; i++) {
```

Dheeraj Lalwani
1902085

```java
        int x = 1 + (i * phi);

        if(x % publicKey == 0) {
            privateKey = x / publicKey;
            break;
        }
    }

    System.out.println("Private key was calculated to be: (" +
privateKey + ", " + product + ")");
    System.out.print("Enter number to be encrypted: ");
    plainTextInt = sc.nextInt();
    cipherTextInt = (int)Math.pow(plainTextInt, publicKey);
    System.out.println("Encrypted message is: " + cipherTextInt);
    BigInteger PRODUCT = BigInteger.valueOf(product);
    BigInteger CIPHERTEXTINT = BigInteger.valueOf(cipherTextInt);
    BigInteger DECRYPTEDTEXTINT;
    DECRYPTEDTEXTINT = (CIPHERTEXTINT.pow(privateKey)).mod(PRODUCT);
    decryptedTextInt = DECRYPTEDTEXTINT.intValue();

    if(plainTextInt == decryptedTextInt) {
        System.out.println("Decrypted text is: " + decryptedTextInt);
    }
    else {
        System.out.println("Kuch to gadbad hai bhai...");
    }
  }
}
```

Output

```
C:\Users\USER\OneDrive\Desktop\practicals\CSS\RSA>java RSA
Implementing RSA algorithm:
Let us generate the keys...
Choose 2 prime numbers: 3 11
Phi was calculated to be: 20
Public key was calculated to be: (3, 33)
Private key was calculated to be: (7, 33)
Enter number to be encrypted: 12
Encrypted message is: 1728
Decrypted text is: 12
```

Dheeraj Lalwani
1902085