

[Toggle navigation](#) [Scanfree.com](#)

- [Data Structure](#)
- [OS](#)
- [C](#)
- [Graph Theory](#)
- [Microprocessor](#)
- [DBMS](#)
 - [Database Concept](#)
 - [SQL](#)
 - [SQLite](#)
- [Programs](#)
 - [C](#)
 - [JAVA](#)
 - [C++](#)
- [Extra](#)
 - [Css/Html Maker](#)
 - [Cheat Sheets](#)
 - [SEO](#)
 - [IFSC Codes](#)

Search

- [1-D Array Programs](#)
- [Algorithm Implementation](#)
- [Array](#)
- [Data structure](#)
- [Date and Time](#)
- [Decision and Loops](#)
- [File Handling](#)
- [Free Books](#)
- [Mathematical Programs](#)
- [Matrix](#)
- [Miscellaneous](#)
- [Networking](#)
- [Number Programs](#)
- [Patterns](#)
- [Searching](#)
- [Sorting](#)
- [String](#)
- [Swapping](#)

Implementation of RSA Algorithm(Encryption and Decryption) in Java

Levels of difficulty: [Hard](#) / perform operation: [Algorithm Implementation](#), [Networking](#)

Java program to encrypt and decrypt a given message using RSA algorithm. Open Command Prompt and compile & Run. RSA algorithm is used to changing message that no one can understand the communication between sender and receiver. Sender and Receiver have public and private key and they can only understand message.

JAVA Program

```
import java.math.BigInteger;

import java.util.Random;

import java.io.*;

public class RSA {

    private BigInteger p;

    private BigInteger q;
```

```
private BigInteger N;
private BigInteger phi;
private BigInteger e;
private BigInteger d;
private int bitlength = 1024;
private int blocksize = 256;
//blocksize in byte
private Random r;
public RSA() {
    r = new Random();
    p = BigInteger.probablePrime(bitlength, r);
    q = BigInteger.probablePrime(bitlength, r);
    N = p.multiply(q);
    phi = p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE));
    e = BigInteger.probablePrime(bitlength/2, r);
    while (phi.gcd(e).compareTo(BigInteger.ONE) > 0 && e.compareTo(phi) < 0 ) {
        e.add(BigInteger.ONE);
    }
    d = e.modInverse(phi);
}
public RSA(BigInteger e, BigInteger d, BigInteger N) {
    this.e = e;
    this.d = d;
    this.N = N;
}
public static void main (String[] args) throws IOException {
    RSA rsa = new RSA();
    DataInputStream in=new DataInputStream(System.in);
    String teststring ;
    System.out.println("Enter the plain text:");
    teststring=in.readLine();
    System.out.println("Encrypting String: " + teststring);
    System.out.println("String in Bytes: " + bytesToString(teststring.getBytes()));
    // encrypt
    byte[] encrypted = rsa.encrypt(teststring.getBytes());
}
```

```

        System.out.println("Encrypted String in Bytes: " + bytesToString(encrypted));

        // decrypt

        byte[] decrypted = rsa.decrypt(encrypted);

        System.out.println("Decrypted String in Bytes: " + bytesToString(decrypted));

        System.out.println("Decrypted String: " + new String(decrypted));

    }

    private static String bytesToString(byte[] encrypted) {

        String test = "";

        for (byte b : encrypted) {

            test += Byte.toString(b);

        }

        return test;

    }

    //Encrypt message

    public byte[] encrypt(byte[] message) {

        return (new BigInteger(message)).modPow(e, N).toByteArray();

    }

    // Decrypt message

    public byte[] decrypt(byte[] message) {

        return (new BigInteger(message)).modPow(d, N).toByteArray();

    }

}

```

Other Related Programs in java

1. [Implementation of MD5 Algorithm in Java](#)
2. [Implementation of RSA Algorithm\(Encryption and Decryption\) in Java](#)
3. [java program to get the date of URL connection](#)
4. [java program to read and download a webpage](#)
5. [java program to find hostname from IP Address](#)
6. [java program to determine IP Address & hostname of Local Computer?](#)
7. [java program to check whether a port is being used or not](#)
8. [java program to find proxy settings of a System](#)
9. [java program to create a socket at a specific port](#)
10. [java program to get the parts of an URL](#)

Scanfree is optimized for learning, testing, and training. Examples might be simplified to improve reading and basic understanding. Tutorials, references, and examples are constantly reviewed to avoid errors, but we cannot warrant full correctness of all content. While using this site, you agree to have read and accepted our terms of use and privacy policy.

Ankit kumar singh

 Follow

1,019 followers