



[Home](#)
[C/C++](#)
[Java](#)
[SQL](#)
[SPM](#)
[Network](#)
[OpenGL](#)
[Android](#)
[Automata](#)
[Data Structure](#)
[Operating System](#)
[Interview Question](#)
[Dov](#)

Donate to Improve



Become Author

Now publish your code or article related to given label on coders hub. To become author on coders hub, mail me : info@coders-hub.com

Popular Posts

Download Android Applications Source Codes and Projects

Finally came with lots of projects to help all android developers. Hope you all will like my below given android projects. If you are new i...

Extract source code (Java and XML) from Android APK File

Not getting any idea how to make good layout in Android activity or not getting how any application doing that things which you want in your...

C code to implement RSA Algorithm(Encryption and Decryption)

C program to implement RSA algorithm. The given program will Encrypt and Decrypt a message using RSA Algorithm. #include<stdio.h>...

Android Location, Address and Distance Tutorial with Example

In this application, first we will learn how to find the best location of the user. To know about location of any user, we have to find lat...

Android SQLite Database Tutorial and Project

In this application, we will learn how to use SQLite database in android to save values and retrieve back from it. SQLite database does not...

C code to implement Lexical Analyzer

C program to implement Lexical Analyzer #include<stdio.h> #include<string.h> #include<stdlib.h> void removeduplic...

Latest Posts

Red Black Tree (RB-Tree) Using C++

A red-black tree is a special type of binary tree, used in computer science to organize...

Android Linphone source code tutorial - Part 2

I have published first part of Android Linphone SDK integration

Search Tutorials

Wednesday, 17 April 2013

Implementation of RSA Algorithm(Encryption and Decryption) in Java

Here, we have given 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.

```
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);

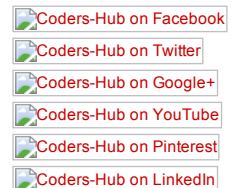
        while (phi.gcd(e).compareTo(BigInteger.ONE) > 0 && e.compareTo(phi) < 0 ) {
            e.add(BigInteger.ONE);
        }
        d = e.modInverse(phi);
    }

    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));
    }
}
```

Follow us on



Join Facebook Group: [Coders](#)

My Best Android Apps

1. [Helper Plus](#)
2. [Namaz Guide](#)

Follow by Email

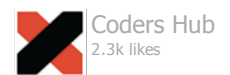
Google+ Followers

Md Mohsin

Add to circles



694 have me in circles [View](#)



Be the first of your friends to like this



Google+ Page

already. In this...

**Android Twitter Fabric SDK
Integration with user details in
Android Studio**

Recently, I updated Facebook SDK
integration with user details post.
Now, I am going to...

**Longest Common Sub-sequence
(LCS) Using C++**

The longest common sub-
sequence (LCS) problem is the
problem of finding the longest...

Randomized Quick Sort Using C++

Quicksort is a divide and conquer
algorithm. Quicksort first divides a
large array into...

Hits since Jan, 2014

7 1 4 7 9 2 0 6

Like

Tweet

- Contributors
- Naim Hashmi
 - MD Naseem Ashraf
 - Md Mohsin
 - Avi Dhall

281

```
// 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();
}
}
```


For more programs related to Network, Check Network Label. Share and comment to improve this blog.


Posted by Md Mohsin at 11:23 p.m.


 +5 Recommend this on Google

Labels: [java](#), [Network](#)

3 comments:

 **krishan dev** 10:28 a.m.
increase my knowledge thanks a lot.
[Reply](#)

 **dhona** 12:41 p.m.
tnkq
[Reply](#)

 **Max Wicked** 11:24 p.m.
How do i print out the public key?
[Reply](#)

Comment as: VISHWARUP ▼ Sign out

Publish Preview ☐ Notify me



Coders Hub

google.com/+InnosBlogs
otco...

Find Code, project and news
related to computer science

 **Follow** 

+ 452

