# Bài Lab 8: RSA

- Viết chương trình mã hóa và giãi mã sử dụng thuật toán RSA:
  - Viết hàm tạo khóa Private key và Public key.
  - Viết hàm mã hóa sử dụng Publickey để mã hóa văn bản.
  - Viết hàm giải mã sử dụng private key để giải mã văn bản.
- Hướng dẫn:
  - Hàm tạo khóa

```
public class Skey_RSA{
   public static void main(String args[]) throws Exception{
       // KeyPairGenerator: giúp tạo ra các cặp key
        KeyPairGenerator kpg=KeyPairGenerator.getInstance("RSA");
        kpg.initialize(1024);
       //  public/private keypairs được dùng để khởi tạo phase của
        // quá trình đăng ký key
        KeyPair kp=kpg.genKeyPair();
        PublicKey pbkey=kp.getPublic();
        PrivateKey prkey=kp.getPrivate();
        //Ghi file publickey
        FileOutputStream  f1=new FileOutputStream("D:\\Skey_RSA_pub.dat");
        ObjectOutputStream b1=new  ObjectOutputStream(f1);
        b1.writeObject(pbkey);
        // ghi file private key
        FileOutputStream  f2=new FileOutputStream("D:\\Skey_RSA_priv.dat");
        ObjectOutputStream b2=new  ObjectOutputStream(f2);
        b2.writeObject(prkey);


   }
}
```

  - Hàm mã hóa

```
public class Enc_RSA{
   public static void main(String args[]) throws Exception{
        // chuoi can ma hoa
        String s="Hello World!";
        //doc file public key
        FileInputStream f=new FileInputStream("D:\\Skey_RSA_pub.dat");
        ObjectInputStream b=new ObjectInputStream(f);
        //Sử dụng hàm readObject của ObjectInputStream
        //để đọc dữ liệu từ tập tin nhị phân lên.
         //Thứ tự đọc cần đảm bảo đúng với thứ tự ghi
        RSAPublicKey  pbk=(RSAPublicKey)b.readObject( );
        BigInteger e=pbk.getPublicExponent();
        BigInteger n=pbk.getModulus();
        System.out.println("e= "+e);
        System.out.println("n= "+n);
        byte ptext[]=s.getBytes("UTF8");
        BigInteger m=new BigInteger(ptext);
        BigInteger c=m.modPow(e,n);
        System.out.println("c= "+c);
        String cs=c.toString( );
        BufferedWriter out=
          new BufferedWriter(new OutputStreamWriter(
            new FileOutputStream("D:\\Enc_RSA.dat")));
        out.write(cs,0,cs.length( ));
        out.close( );

   }
}
```

- Hàm giải mã

```
public class Dec_RSA{
   public static void main(String args[]) throws Exception{
       //doc van ban da ma hoa
        BufferedReader in=
          new BufferedReader(new InputStreamReader
          (new FileInputStream("D:\\Enc_RSA.dat")));
        String ctext=in.readLine();
        // chuyển sang kiểu biginteger
        BigInteger c=new BigInteger(ctext);
        //doc khóa private key
         FileInputStream f=new FileInputStream("D:\\Skey_RSA_priv.dat");
         //Sử dụng hàm readObject của ObjectInputStream
        //để đọc dữ liệu từ tập tin nhị phân lên.
         //Thứ tự đọc cần đảm bảo đúng với thứ tự ghi
        ObjectInputStream b=new ObjectInputStream(f);
        RSAPrivateKey prk=(RSAPrivateKey)b.readObject( );
        BigInteger d=prk.getPrivateExponent();
        BigInteger n=prk.getModulus();
        System.out.println("d= "+d);
        System.out.println("n= "+n);
        BigInteger m=c.modPow(d,n);
        System.out.println("m= "+m);
        byte[] mt=m.toByteArray();
        System.out.println("PlainText is ");
        for(int i=0;i<mt.length;i++){
             System.out.print((char) mt[i]);
       }
```

- Bài tập mở rộng: Viết chương trình như trên nhưng thiết kế trên Jfame Form và viết hàm xử lý.