Université de Batna 2 Mostepha Benboulaid

Département d'informatique

Formation : Master 1 CS

Module: Programmation Orientée Objet 2

TP 02

Exemple d'utilisation de l'algorithme de cryptographie asymétrique RSA

```java
import java.security.*;
import javax.crypto.*;
import java.io.*;
public class rsa{

private PrivateKey rsaPrivate;
private PublicKey rsaPublic;
private Cipher cipher=null;
private  final String ALGORITHM = "RSA";


public void init()
  throws NoSuchAlgorithmException,
         NoSuchPaddingException, NoSuchProviderException
{

    KeyPairGenerator keyGen = KeyPairGenerator.getInstance
(ALGORITHM);
    keyGen.initialize(1024);
    KeyPair keyPair = keyGen.generateKeyPair();
    this.setRsaPrivate(keyPair.getPrivate())  ;
    this.setRsaPublic(keyPair.getPublic());
}


public void setRsaPrivate(PrivateKey p){rsaPrivate=p;}
public void setRsaPublic(PublicKey p){rsaPublic=p;}
public PrivateKey getRsaPrivate(){return rsaPrivate;}
public PublicKey getRsaPublic(){return rsaPublic;}

```

```java
public byte[] encryption(String Message)
    throws InvalidKeyException,IllegalBlockSizeException,
                BadPaddingException, NoSuchAlgorithmException,
                NoSuchProviderException, NoSuchPaddingException,
                UnsupportedEncodingException
{
    cipher=Cipher.getInstance(ALGORITHM );
    cipher.init(Cipher.ENCRYPT_MODE,this.getRsaPublic());
    byte[] encryptedMsg = cipher.doFinal(Message.getBytes());
    return encryptedMsg;

}


public String decryption(byte[] encryptedMsg)
    throws InvalidKeyException, IllegalBlockSizeException,
                BadPaddingException, UnsupportedEncodingException,
                NoSuchAlgorithmException, NoSuchProviderException,
                NoSuchPaddingException
{

    Cipher cipher = Cipher.getInstance(ALGORITHM );
    cipher.init(Cipher.DECRYPT_MODE,this.getRsaPrivate());
    byte[] decryptedText = cipher.doFinal(encryptedMsg);
    return new String(decryptedText);
}

public static void main(String args[]) throws Exception
{
    String message="Comment ça va?";
    byte[] messagecrypte;
    rsa r=new rsa();

    r.init();

    messagecrypte=r.encryption(message);

    System.out.println("Test cryptage: "+new String(messagecrypte) );

    System.out.println("Test décryptage: "+r.decryption(messagecrypte));
}
}
```