Java Security- Cryptography

Encrypting Data

```java
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.Signature;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;

public class Test
{
        public static void main(String args[]) throws Exception{
        //Creating a Signature object
        Signature sign = Signature.getInstance("SHA256withRSA");

        //Creating KeyPair generator object
        KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("RSA");

        //Initializing the key pair generator
        keyPairGen.initialize(2048);

         //Generating the pair of keys
        KeyPair pair = keyPairGen.generateKeyPair();

        //Creating a Cipher object
        Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");

        //Initializing a Cipher object
        cipher.init(Cipher.ENCRYPT_MODE, pair.getPublic());

        //Adding data to the cipher
        byte[] input = "I am a Certified Java Developer.".getBytes();
        cipher.update(input);

        //encrypting the data
        byte[] cipherText = cipher.doFinal();
        System.out.println(new String(cipherText, "UTF8"));
  }
}
```

Encrypting and Decrypting Data

```java
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.Signature;
import java.security.PublicKey;

import javax.crypto.Cipher;

public class Test
{
        public static void main(String args[]) throws Exception
        {
                //Creating a Signature object
                Signature sign = Signature.getInstance("SHA256withRSA");

                //Creating KeyPair generator object
                 KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("RSA");

                //Initializing the key pair generator
                keyPairGen.initialize(2048);

                //Generate the pair of keys
                KeyPair pair = keyPairGen.generateKeyPair();

                //Getting the public key from the key pair
                PublicKey publicKey = pair.getPublic();

                //Creating a Cipher object
                Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");

                //Initializing a Cipher object
                cipher.init(Cipher.ENCRYPT_MODE, publicKey);

                //Add data to the cipher
                byte[] input = "I love Java Programming.".getBytes();
                cipher.update(input);

                //encrypting the data
                byte[] cipherText = cipher.doFinal();
                System.out.println( new String(cipherText, "UTF8"));

                //Initializing the same cipher for decryption
                cipher.init(Cipher.DECRYPT_MODE, pair.getPrivate());

                //Decrypting the text
                byte[] decipheredText = cipher.doFinal(cipherText);
                System.out.println(new String(decipheredText));
        }
}
```

```
C:\Program Files\Java\jdk-11.0.12\bin\Manish>javac Test.java

C:\Program Files\Java\jdk-11.0.12\bin\Manish>java Test
8Nd?à?<????K??=[?(?{?>Z?p??^0[U??=↑1?►|\???4??~→?34?????▲WQ???????|@??u???!!Q,???G?j?1@O_.o♠!!?UV#§?♦←?c????0??P??=?
?????SRK►?v0↓b←p?X^?6S\?zJ?ᴧ?HD???↑?????Tu?p?+=E↑?S¶N?~???P?.F??l?k?r.?z?(?6?>,;nU??]f?▼??35?????<??J?I??_"9]ᴧ♠?O?
I love Java Programming.
```