AIM: To implement AES Algorithm

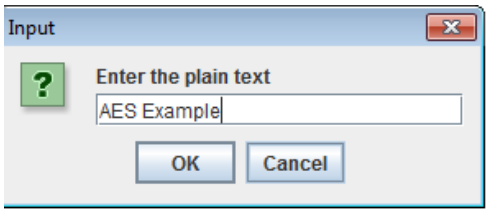
AES(Advance Encryption Standard) is a symmetric block cipher to protect information.The need for AES algorithm was the weekness of DES algorithm. The 56 bits key used in DES algorithm were no longer considered safe therefore we use AES algorithm which uses 128 bits key.

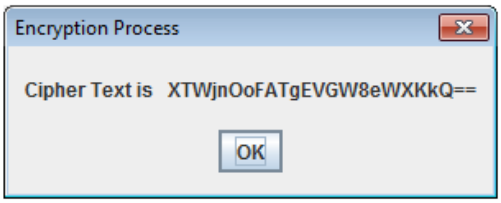
Program

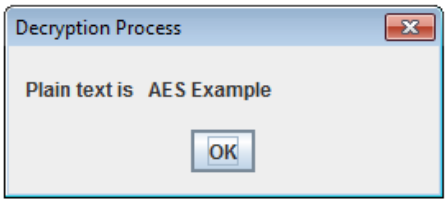
```
packageaesalgorithm;
importjava.io.BufferedReader;
importjava.io.InputStreamReader;
importjava.security.Key;
importjavax.crypto.Cipher;
importjavax.crypto.spec.SecretKeySpec;
importjavax.swing.JOptionPane;
import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder;
public class AESAlgorithm
{
      byte key[]={'T','h','i','s','i','s','S','e','c','r','e','t','K','e','y','!'};
   String encrypt(String plain) throws Exception
   {
      Key keysp=new SecretKeySpec(key, "AES");
      Cipher c=Cipher.getInstance("AES");
c.init(Cipher.ENCRYPT_MODE, keysp);
byte[] envalue=c.doFinal(plain.getBytes());
      String enstring=new BASE64Encoder().encode(envalue);
returnenstring;
   }

   String decrypt(String ciphertext) throws Exception
   {
      Key keysp=new SecretKeySpec(key, "AES");
      Cipher c=Cipher.getInstance("AES");
c.init(Cipher.DECRYPT_MODE, keysp);
byte[] deval=new BASE64Decoder().decodeBuffer(ciphertext);
byte[] decode=c.doFinal(deval);
System.out.println("Decrypted values in bytes____");
       String plain=new String(decode);
return plain;
   }
public static void main(String[] args) throws Exception
   {
      // TODO code application logic here
      String plain="",ciphertext="",dec="";
AESAlgorithm as=new AESAlgorithm();
plain = JOptionPane.showInputDialog("Enter the plain text");
System.out.println("Plain Text : "+plain);
ciphertext=as.encrypt(plain);
JOptionPane.showMessageDialog(null,ciphertext);
System.out.println("Encrypted Text : "+ciphertext);
dec=as.decrypt(ciphertext);
JOptionPane.showMessageDialog(null,plain);
System.out.println("Decrypted Text : "+dec);
   }
```

Output:


Input
Enter the plain text
AES Example
OK
Cancel


Encryption Process
Cipher Text is XTWjnOoFATgEVGW8eWXKkQ==
OK


Decryption Process
Plain text is AES Example
OK