Name:Mohan Ramchandra Patil
Reg. No : 19141267

IS Exp4: Implement Advanced Encryption Standard Algorithm (AES).

Code:

```
import java.io.UnsupportedEncodingException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Arrays;
import java.util.Base64;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
public class AES {
   private static SecretKeySpec secretKey;
   private static byte[] key;
   public static void setKey(String myKey) {
      MessageDigest sha = null;
      try {
         key = myKey.getBytes("UTF-8");
         sha = MessageDigest.getInstance("SHA-1");
         key = sha.digest(key);
         key = Arrays.copyOf(key, 16);
         secretKey = new SecretKeySpec(key, "AES");
      } catch (NoSuchAlgorithmException e) {
         e.printStackTrace();
      } catch (UnsupportedEncodingException e) {
         e.printStackTrace();
      }
   }
   public static String encrypt(String strToEncrypt, String secret) {
      try {
         setKey(secret);
         Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
         cipher.init(Cipher.ENCRYPT_MODE, secretKey);
         return Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));
      } catch (Exception e) {

         return null;
      }
   }
      public static String decrypt(String strToDecrypt, String secret) {
         try {
            setKey(secret);
            Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
            cipher.init(Cipher.DECRYPT_MODE, secretKey);
            return new String(cipher.doFinal(Base64.getDecoder().decode(strToDecrypt)));
         } catch (Exception e) {
            System.out.println("Error while decrypting: " + e.toString());
         }
```

```
        return null;
    }
    public static void main(String[] args) {
        final String secretKey = "Mohan Patil";
        System.out.println("Mohan Patil (19141267)");
        System.out.println();
        String originalString = " https://auth.geeksforgeeks.org/user/raufashaikh5/";
        String encryptedString = AES.encrypt(originalString, secretKey);
        String decryptedString = AES.decrypt(encryptedString, secretKey);
        System.out.println("URL Encryption Using AES Algorithm\n------------");
        System.out.println("Original URL : " + originalString);
        System.out.println("Encrypted URL : " + encryptedString);
        System.out.println("Decrypted URL : " + decryptedString);
    }
}
```

Output:

```
PS C:\Users\mohan\Desktop\sub codes\is codes\4> javac AES.java
PS C:\Users\mohan\Desktop\sub codes\is codes\4> java AES
Mohan Patil (19141267)

URL Encryption Using AES Algorithm
------------
Original URL :  https://auth.geeksforgeeks.org/user/raufashaikh5/
Encrypted URL : qFWvcAJOFEgfTZqiQRGC+icj01vE4YDwZ7JYCkZWzqD6EYxxsfQGRW+EIstyPdx
FEgQOvyrW8UAqB58Q4V/Qag==
Decrypted URL :  https://auth.geeksforgeeks.org/user/raufashaikh5/
PS C:\Users\mohan\Desktop\sub codes\is codes\4>
```