Assignment 5

Title: Advanced Encryption Standard (AES)

Code:

```
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.StandardCharsets;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.KeySpec;
import java.util.Base64;
import javax.crypto.BadPaddingException;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
public class AES
{
    private static final String SECRET_KEY = "123456789";
    private static final String SALTVALUE = "abcdefg";

    public static String encrypt(String strToEncrypt)
    {
    try
    {
      byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
      IvParameterSpec ivspec = new IvParameterSpec(iv);
      SecretKeyFactory factory =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
      KeySpec spec = new PBEKeySpec(SECRET_KEY.toCharArray(), SALTVALUE.getBytes(),
65536, 256);
      SecretKey tmp = factory.generateSecret(spec);
      SecretKeySpec secretKey = new SecretKeySpec(tmp.getEncoded(), "AES");
      Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
      cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);
      return Base64.getEncoder()
.encodeToString(cipher.doFinal(strToEncrypt.getBytes(StandardCharsets.UTF_8)));
    }
    catch (InvalidAlgorithmParameterException | InvalidKeyException |
NoSuchAlgorithmException | InvalidKeySpecException | BadPaddingException |
IllegalBlockSizeException | NoSuchPaddingException e)
    {
      System.out.println("Error occured during encryption: " + e.toString());
    }
    return null;
    }

    public static String decrypt(String strToDecrypt)
    {
    try
    {
      byte[] iv = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
      IvParameterSpec ivspec = new IvParameterSpec(iv);
```

```
      SecretKeyFactory factory =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
      KeySpec spec = new PBEKeySpec(SECRET_KEY.toCharArray(), SALTVALUE.getBytes(),
65536, 256);
      SecretKey tmp = factory.generateSecret(spec);
      SecretKeySpec secretKey = new SecretKeySpec(tmp.getEncoded(), "AES");
      Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
      cipher.init(Cipher.DECRYPT_MODE, secretKey, ivspec);
      return new String(cipher.doFinal(Base64.getDecoder().decode(strToDecrypt)));
    }
    catch (InvalidAlgorithmParameterException | InvalidKeyException |
NoSuchAlgorithmException | InvalidKeySpecException | BadPaddingException |
IllegalBlockSizeException | NoSuchPaddingException e)
    {
      System.out.println("Error occured during decryption: " + e.toString());
    }
    return null;
    }
    /* Driver Code */
    public static void main(String[] args)
    {
        String originalval = "AES Encryption";
        String encryptedval = encrypt(originalval);
        String decryptedval = decrypt(encryptedval);
        System.out.println("Original value: " + originalval);
        System.out.println("Encrypted value: " + encryptedval);
        System.out.println("Decrypted value: " + decryptedval);
    }
}
```

OUTPUT: