S Shankar Narayanan
312217104146
3-9-2020

SSN College of Engineering

Ex 5 : Advanced Encryption Standard

Aim : To implement Advanced Encryption Standard (AES) Algorithm

Code :

```
import java.io.*;
import java.util.*;
import javax.crypto.*;
import java.security.*;
import javax.crypto.spec.SecretKeySpec;

class AES{

    public SecretKeySpec secretKey;
    public byte[] key;

    public 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(Exception e){

        }
}

public String encrypt(String ptext, String secret){
try{
        setKey(secret);
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);
        return Base64.getEncoder().encodeToString(cipher.doFinal(ptext.getBytes("UTF-8")));
        } catch (Exception e){
                System.out.println("Error while encrypting");
        }
        return null;
}

public String decrypt(String ctext ,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(ctext)));
            } catch (Exception e){
                    System.out.println("Error while decrypting");
            }

            return null;
    }
}

public class AESDriver{

    public static void main(String[] args){
            String sKey;
            String ptext;

            Scanner in = new Scanner(System.in);
            System.out.println("Enter a secret key : ");
            sKey = in.nextLine();

            System.out.println("Enter a plaintext : ");
```

```
        ptext = in.nextLine();


        AES aes = new AES();
        String encr = aes.encrypt(ptext, sKey);
        String decr = aes.decrypt(encr, sKey);


        System.out.println("plaintext : "+ptext);
        System.out.println("Encrypted String : "+encr);
        System.out.println("Decrypted String : "+decr);
    }
}
```

OUTPUT :

base) Shankars-MacBook-Pro:Ex14 shankar99$ javac AESDriver.java

(base) Shankars-MacBook-Pro:Ex14 shankar99$ java AESDriver

Enter a secret key :

iamkira

Enter a plaintext :

iwriteinanotebook

plaintext : iwriteinanotebook

Encrypted String : Ku5TRQcvQSPi7htEnFluVZntLX1dDP7PbO84rZvegL0=

Decrypted String : iwriteinanotebook

(base) Shankars-MacBook-Pro:Ex14 shankar99$