**IT8761 – Security Laboratory**

**Reshma Ramesh Babu**

**312217104129**

**Exercise 5**

**Aim:** To implement the Advanced Encryption Standard (AES) algorithm.

**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)

{

System.out.println("Error while encrypting: " + e.toString());

}

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 = "aessecretkey!!!!";

String originalString;

System.out.println("Enter plain text:");

originalString = System.console().readLine();

int ch;

String encryptedString = AES.encrypt(originalString, secretKey) ;

do{

System.out.println("MENU\n1.Encrypt\n2.Decrypt\n3.Exit");

System.out.println("Enter Choice:");

String c = System.console().readLine();

ch=Integer.parseInt(c);

if(ch==1)

{

System.out.println(encryptedString);

}

else if(ch==2)

{

String decryptedString = AES.decrypt(encryptedString, secretKey) ;

System.out.println(decryptedString);

}

}while(ch!=3);

}

}

**Output:**

