# Experiment – 4

Name: Ruturaj Kadam Roll Number: 20141272

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 = "Mahesh Thorat"; System.out.println("20141272 Ruturaj kadam)"); System.out.println();

String originalString = " https://github.com/mahesh249"; 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:

