/\*

Name: Furkhan Mujibodden Shaikh

Class: BECSEII;

Aim: WAP to implement RSA ENCRYPTION ALGORITHM

\*/

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.PrivateKey;

import java.security.PublicKey;

import java.util.Base64;

import java.util.HashMap;

import java.util.Map;

import java.util.Scanner;

import javax.crypto.Cipher;

public class RSAEncryptionFurkhan {

public static void main(String[] args) throws Exception {

Scanner sc = new Scanner(System.in);

System.out.println("Enter the Input String");

String plainText = sc.nextLine();

Map<String, Object> keys = getRSAKeys();

PrivateKey privateKey = (PrivateKey) keys.get("private");

PublicKey publicKey = (PublicKey) keys.get("public");

String encryptedText = encryptMessage(plainText, privateKey);

String decryptedText = decryptMessage(encryptedText, publicKey);

System.out.println();

System.out.println(plainText +" is Encrypted to [ " +encryptedText +" ]\n");

System.out.println("[ " +encryptedText + " ] is Decrypted to " + decryptedText);

sc.close();

}

// Get RSA keys. Uses key size of 2048.

private static Map<String,Object> getRSAKeys() throws Exception {

KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("RSA");

keyPairGenerator.initialize(2048);

KeyPair keyPair = keyPairGenerator.generateKeyPair();

PrivateKey privateKey = keyPair.getPrivate();

PublicKey publicKey = keyPair.getPublic();

Map<String, Object> keys = new HashMap<String,Object>();

keys.put("private", privateKey);

keys.put("public", publicKey);

return keys;

}

private static String decryptMessage(String encryptedText, PublicKey publicKey) throws Exception {

Cipher cipher = Cipher.getInstance("RSA");

cipher.init(Cipher.DECRYPT\_MODE, publicKey);

return new String(cipher.doFinal(Base64.getDecoder().decode(encryptedText)));

}

private static String encryptMessage(String plainText, PrivateKey privateKey) throws Exception {

Cipher cipher = Cipher.getInstance("RSA");

cipher.init(Cipher.ENCRYPT\_MODE, privateKey);

return Base64.getEncoder().encodeToString(cipher.doFinal(plainText.getBytes()));

}}

// OUTPUT

/\*

Enter the Input String

Furkhan Mujibodden Shaikh

**Furkhan Mujibodden Shaikh** is Encrypted to **[ GRwaRAkxJimNEvtAV8DDPkENPGomVAPQLZ1qGtnoEUE/3iUjqmb05NT8rqx5d/mFGLRzK2p5IMLk3DcknTHIYo0eRQjdeSx8n0CKGOVCEEamvLle92ueDWg7MCBTwtpeTKuulv1EKKRmaUaYc150SDFui6jDCSUO/AuHBqj7MGvMUAzNJUNNXJu84YZekQCu0HP7nHmoXpogwNSSoSMMsinfNWt/3i17LzwODnHhRu2dZE0fy/SqA6zQ6X3MrncVuKdgmMMdqzeklt41JGzYEntFsExGmImrzmH4E6MEz8MMxpdQwHSTggSEKVdgahYUoW26OWvfyJXpWWZ5eoT6sQ== ]**

**[ GRwaRAkxJimNEvtAV8DDPkENPGomVAPQLZ1qGtnoEUE/3iUjqmb05NT8rqx5d/mFGLRzK2p5IMLk3DcknTHIYo0eRQjdeSx8n0CKGOVCEEamvLle92ueDWg7MCBTwtpeTKuulv1EKKRmaUaYc150SDFui6jDCSUO/AuHBqj7MGvMUAzNJUNNXJu84YZekQCu0HP7nHmoXpogwNSSoSMMsinfNWt/3i17LzwODnHhRu2dZE0fy/SqA6zQ6X3MrncVuKdgmMMdqzeklt41JGzYEntFsExGmImrzmH4E6MEz8MMxpdQwHSTggSEKVdgahYUoW26OWvfyJXpWWZ5eoT6sQ== ]** is Decrypted to **Furkhan Mujibodden Shaikh**\*/