Ministerul Educaţiei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**Raport**

Disciplina: Securitatea informațională.

Lucrarea de laborator nr. 2

**Tema:** Securitatea informațională.

A efectuat: st.gr. TI-194, Zavorot Daniel

A verificat: asist. univ. Răducanu Octavian

Chișinău - 2022

Codul:

import javax.crypto.BadPaddingException;  
import javax.crypto.Cipher;  
import javax.crypto.IllegalBlockSizeException;  
import javax.crypto.NoSuchPaddingException;  
import java.security.\*;  
import java.util.Base64;  
  
public class Main {  
 public static void main(String[] args) throws NoSuchAlgorithmException, InvalidKeyException, NoSuchPaddingException, IllegalBlockSizeException, BadPaddingException {  
 KeyPairGenerator keyPairGenerator =  
 KeyPairGenerator.*getInstance*("RSA");  
 SecureRandom secureRandom = new SecureRandom();  
  
 keyPairGenerator.initialize(2048, secureRandom);  
  
 KeyPair pair = keyPairGenerator.generateKeyPair();  
  
 PublicKey publicKey = pair.getPublic();  
  
 String publicKeyString =  
 Base64.*getEncoder*().encodeToString(publicKey.getEncoded());  
  
 System.*out*.println("public key = " + publicKeyString);  
  
 PrivateKey privateKey = pair.getPrivate();  
  
 String privateKeyString =  
 Base64.*getEncoder*().encodeToString(privateKey.getEncoded());  
  
 System.*out*.println("private key = " + privateKeyString);  
  
 //Encrypt message  
 Cipher encryptionCipher = Cipher.*getInstance*("RSA");  
 encryptionCipher.init(Cipher.*ENCRYPT\_MODE*, privateKey);  
 String message = "Mesajul meu!!!!";  
 byte[] encryptedMessage =  
 encryptionCipher.doFinal(message.getBytes());  
 String encryption =  
 Base64.*getEncoder*().encodeToString(encryptedMessage);  
 System.*out*.println("encrypted message = " + encryption);  
  
 //Decrypt message  
 Cipher decryptionCipher = Cipher.*getInstance*("RSA");  
 decryptionCipher.init(Cipher.*DECRYPT\_MODE*, publicKey);  
 byte[] decryptedMessage =  
 decryptionCipher.doFinal(encryptedMessage);  
 String decryption = new String(decryptedMessage);  
 System.*out*.println("decrypted message = " + decryption);  
 }  
}

Rezultatul:

