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. 3

**Tema:** Algoritmul DSA

A efectuat: st.gr. TI-194 Ceban Vitalie

A verificat: asis. univ. Răducanu Octavian

Chişinău 2022

**Scopul lucrării:**

- Studierea noţiunii de semnătură digitală

- Domeniul de aplicare

- Metode de calcul  
**Obiectivele lucrării:**

- Dezvoltarea unei aplicaţi ce utilizează semnătura digital

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.PrivateKey;

import java.security.Signature;

import java.util.Scanner;

public class CreatingDigitalSignature {

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

Scanner sc = new Scanner(System.in);

System.out.println("Enter some text");

String msg = sc.nextLine();

KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

keyPairGen.initialize(2048);

KeyPair pair = keyPairGen.generateKeyPair();

PrivateKey privKey = pair.getPrivate();

Signature sign = Signature.getInstance("SHA256withDSA");

sign.initSign(privKey);

byte[] bytes = "msg".getBytes();

sign.update(bytes);

byte[] signature = sign.sign();

System.out.println("Digital signature for given text: "+new String(signature, "UTF8"));

}

}