**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”**

**Кафедра систем штучного інтелекту**



# **Лабораторна робота**

з дисципліни

«Технології захисту інформації»

**Виконав:**

студент групи КН-314

Ляшеник Остап

**Викладач:**

Яковина В. С.

2023 р.

**Лабораторна робота №5**

**СТВОРЕННЯ ПРОГРАМНОГО ЗАСОБУ ДЛЯ ЦИФРОВОГО ПІДПИСУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ CRYPTOAPI**

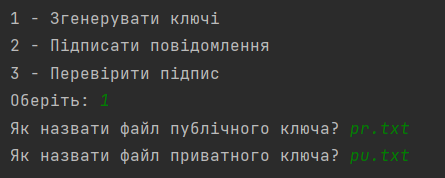
**Мета роботи:** ознайомитись з методами криптографічного забезпечення цифрового підпису, навчитись створювати програмні засоби для цифрового підпису з використанням криптографічних інтерфейсів.

**Завдання:** З використання функцій CryptoAPI створити прикладну програму для створення і перевірки цифрового підпису за стандартом DSS. Програмна реалізація повинна виводити значення підпису як для рядка, заданого в полі вводу, так і для файлу. Результат роботи програми повинен відображатись на екрані з можливістю наступного запису в файл. Крім того програма повинна мати можливість перевірити цифровий підпис будь-якого файлу за наявним файлом підпису, записаним у шістнадцятковому форматі. У звіті навести протокол роботи програми та зробити висновки.

**Код програми:** from Crypto.Hash import SHA256  
from Crypto.PublicKey import DSA  
from Crypto.Signature import DSS  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 print("1 - Згенерувати ключі")  
 print("2 - Підписати повідомлення")  
 print("3 - Перевірити підпис")  
  
 k = int(input("Оберіть: "))  
  
 #Випадок генеруввання ключів  
 if k == 1:  
 public = input("Як назвати файл публічного ключа? ")  
 privat = input("Як назвати файл приватного ключа? ")  
 key = DSA.generate(bits=1024)  
 with open(privat, "wb") as input\_file\_pr:  
 input\_file\_pr.write(key.exportKey())  
 with open(public, "wb") as input\_file\_pb:  
 input\_file\_pb.write(key.publickey().exportKey())  
  
 #Випадок запису підпису  
 elif k == 2:  
 privateFile = input("Файл приватного ключа: ")  
 with open(privateFile, "rb") as file:  
 privateKey = DSA.import\_key(file.read())  
 print("Звідки тягнути повідомлення для шифрування?")  
 print("1 - З файлу")  
 print("2 - З консолі")  
 m = int(input("Оберіть: "))  
 message = ""  
 if m == 1:  
 filename = input("Ім'я файлу: ")  
 with open(filename, "rb") as file:  
 message = file.read()  
 elif m == 2:  
 message = bytes(input("Повідомлення: "), encoding="utf-8")  
 mess\_enc = SHA256.new(message)  
 sign = DSS.new(privateKey, "fips-186-3")  
 signature = sign.sign(mess\_enc)  
 print("Підписане повідомлення: " + signature.hex())  
 write\_to\_file = input("Записати у файл? (y/n)")  
 if write\_to\_file.lower() == "y" or write\_to\_file.lower() == "":  
 filename = input("Ім'я файлу: ")  
 with open(filename, "w") as output:  
 output.write(signature.hex())  
  
 #Випадок перевірки підпису  
 elif k == 3:  
 publicFile = input("Файл публічного ключа: ")  
 with open(publicFile, "rb") as file:  
 publicKey = DSA.import\_key(file.read())  
 message = str.encode(input("Підпис: "))  
 print("Звідки тягнути зашифрований підпис?")  
 print("1 - З файлу")  
 print("2 - З консолі")  
 m = int(input("Оберіть: "))  
 signature = ""  
 if m == 1:  
 filename = input("Ім'я файлу: ")  
 with open(filename, "r") as file:  
 signature = file.read()  
 elif m == 2:  
 signature = input("Підпис: ")  
 message = SHA256.new(message)  
 signature = bytes.fromhex(signature)  
 verifier = DSS.new(publicKey, "fips-186-3")  
 try:  
 verifier.verify(message, signature)  
 print("Дійсний підпис")  
 except ValueError:  
 print("Недійсний підпис")  
 pass

**Результати виконання:**

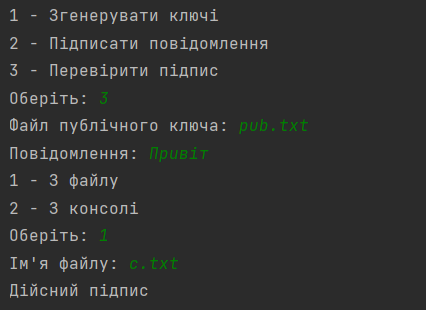
Отримання ключів:



Підписання:



Перевірка підпису:



**Висновок:** виконуючи цю лабораторну роботу я навчився використовувати алгоритм DSS з CryptoApi. Розробив програму для генерації ключів, підписання та перевірки підпису.