**Міністерство Освіти І НАУКИ України**

**Національний університет "Львівська політехніка"**

Інститут **ІКНІ**

Кафедра **СШІ**

**ЗВІТ**

До лабораторної роботи №4

**З дисципліни:** «Технології захисту інформації»

**На тему:** «Дослідження програми гібридного алгоритму PGP»

**Виконав:**

ст. гр. КН-307

Шиманський П.С.

**Прийняв:**

Матвійчук Я.М.

Львів – 2019

**Мета:** Дослідження програми гібридного алгоритму PGP.

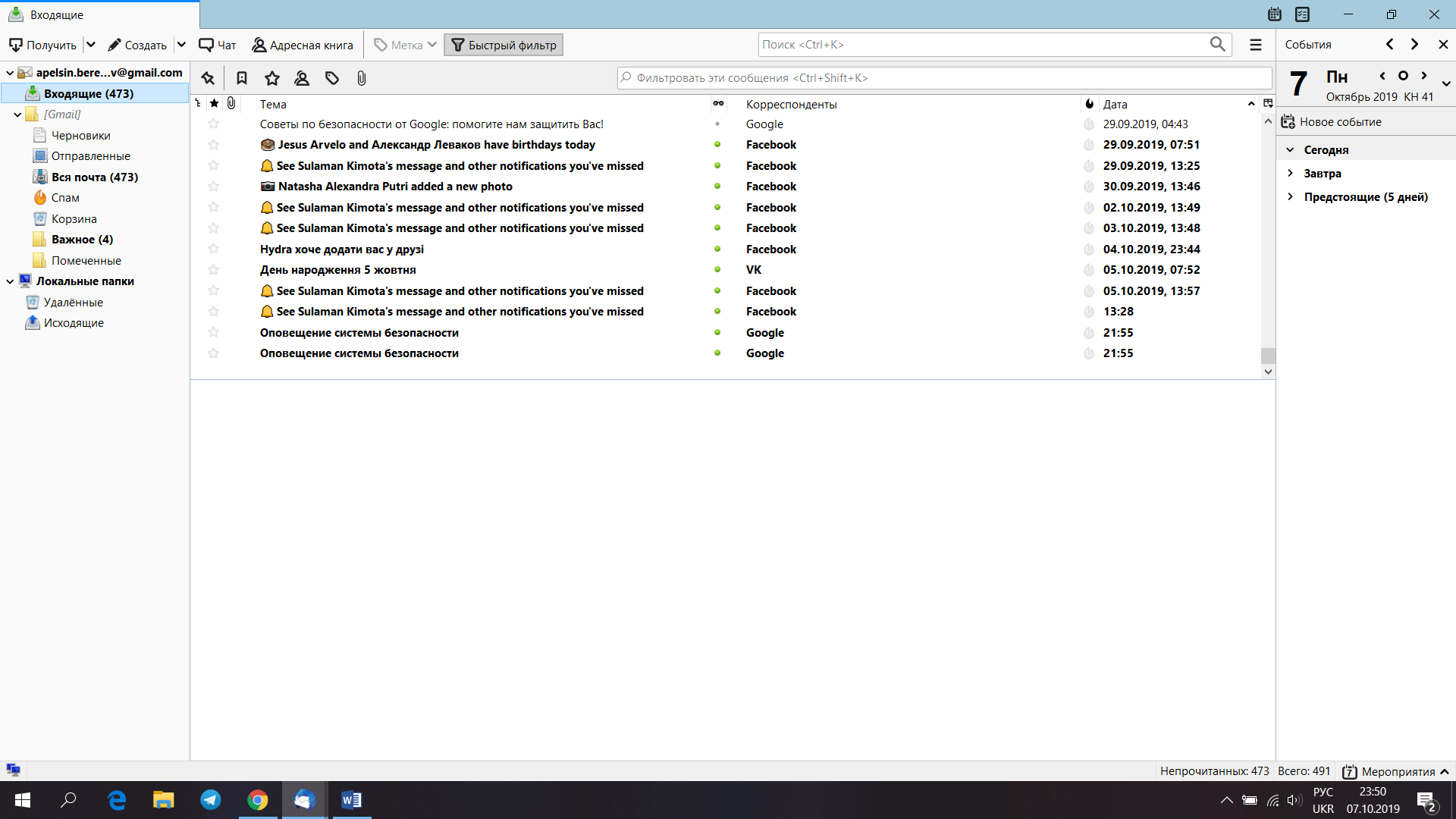
**Хід роботи:**

1. Вивчити україномовну відеоінструкцію з встановлення і використання програми PGP, що міститься за адресою:



**Рис.1.** Ознайомився із інструкцією встановлення і використання

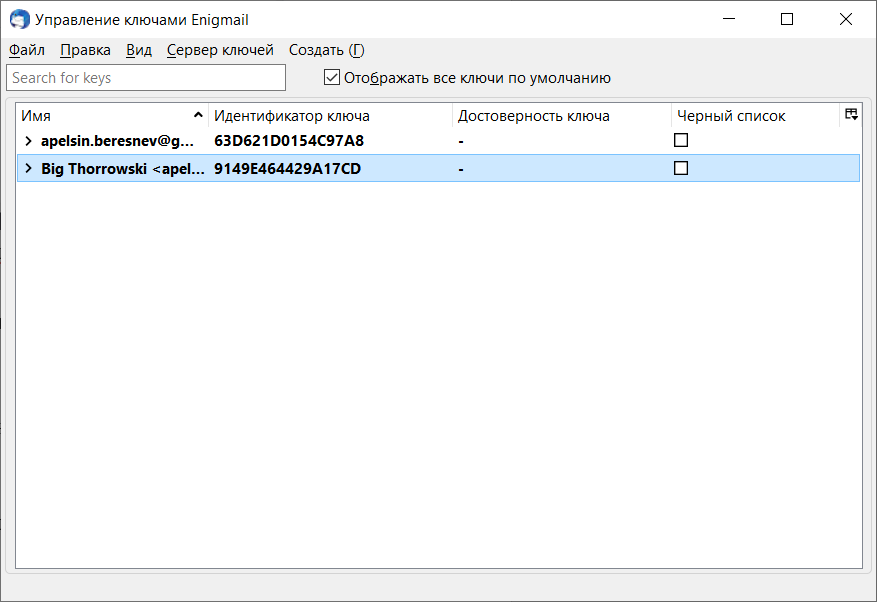
1. Встановити програму на комп’ютер, що буде тримачем секретного ключа (адреса 1).



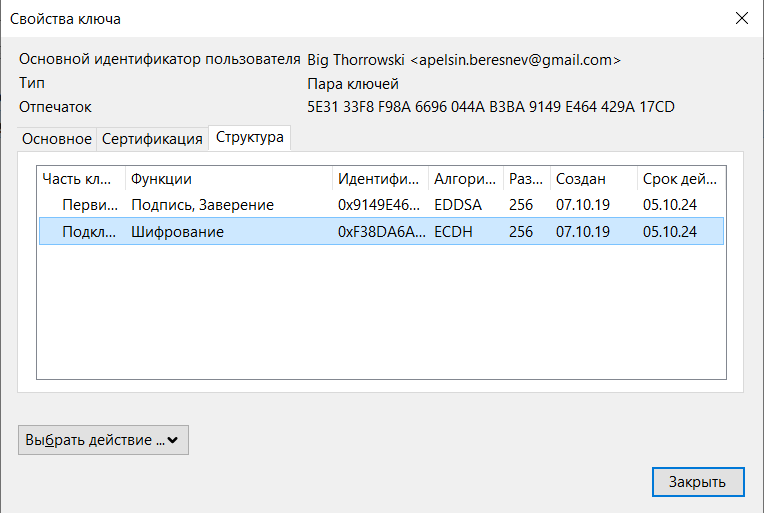
**Рис.2.** Встановив програму, що буде тримачем секретного ключа

* Не забути подякувати автору інструкції Артему Бабаку.
* Подякував.

1. Створити публічний та секретний ключі. Публічний ключ передати обраному адресату (адреса 2).

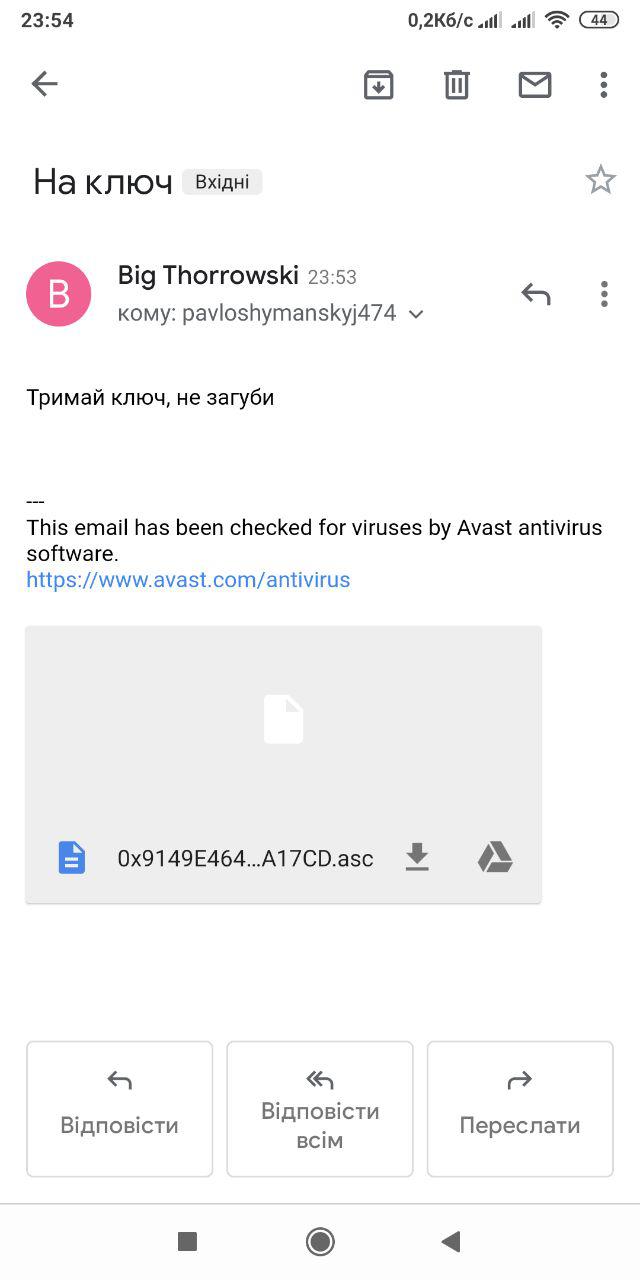


**Рис.3.** Створив публічний та секретний ключі



**Рис.4.** Шифрування

1. Відправити зашифроване і підписане повідомлення з адреси 2 до адреси 1 та розшифрувати його.



**Рис.5.** Результат відправки та отримання повідомлення з адреси 2 до адреси 1

1. Виміряти швидкості шифрування і розшифрування. Порівняти їх з відповідними швидкостями симетричного алгоритму з лаб. роб. 2.

Під час проведення лабораторної роботи №2, я використовував програму KRYPTEL, під час проведення лабораторної я шифрував відносно невеликий файл, тому в результаті швидкість шифрування була приблизно ~0,81 с.

Під час проведення лабораторної роботи №3, використовувалася зовсі інакша програма для шифрування, але я також шифрував відносно невеликий файл, тому в результаті час шифрування був ~0,76 c.

**Висновок:**

На цій лабораторній роботі, я навчився користуватися програмою Mozilla Thunderbird, Kleopatra та додатком Enigmail, порівняв швидкості шифрування з минулими роботами.