**Міністерство Освіти І НАУКИ України**

**Національний університет "Львівська політехніка"**

Інститут **ІКНІ**

Кафедра **СШІ**

**ЗВІТ**

До лабораторної роботи №5

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

**На тему:** «Дослідження програми асиметричного алгоритму RSA»

**Виконав:**

ст. гр. КН-307

Шиманський П.С.

**Прийняв:**

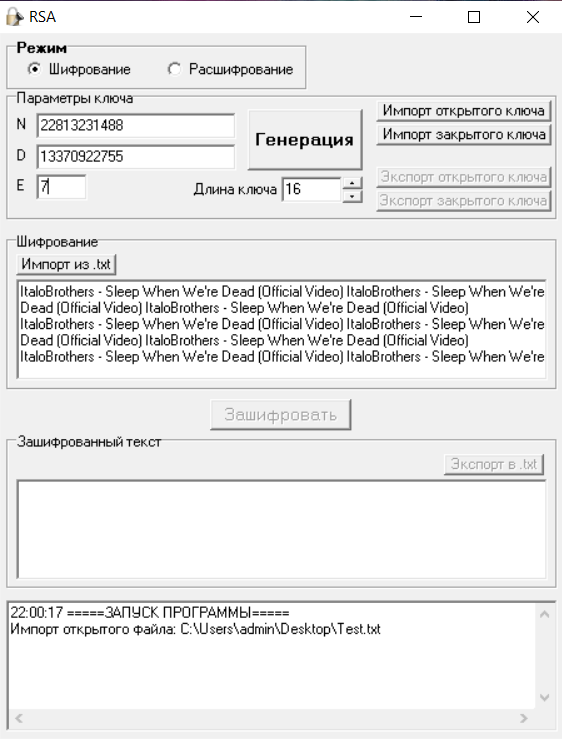
Матвійчук Я.М.

Львів – 2019

**Мета:** дослідити програму асиметричного алгоритму RSA.

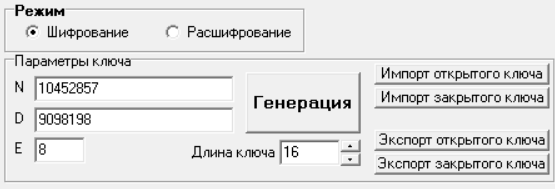
**Хід роботи:**

1. Запустити програму і переконатись у її працездатності.



**Рис.1.** Програма працює

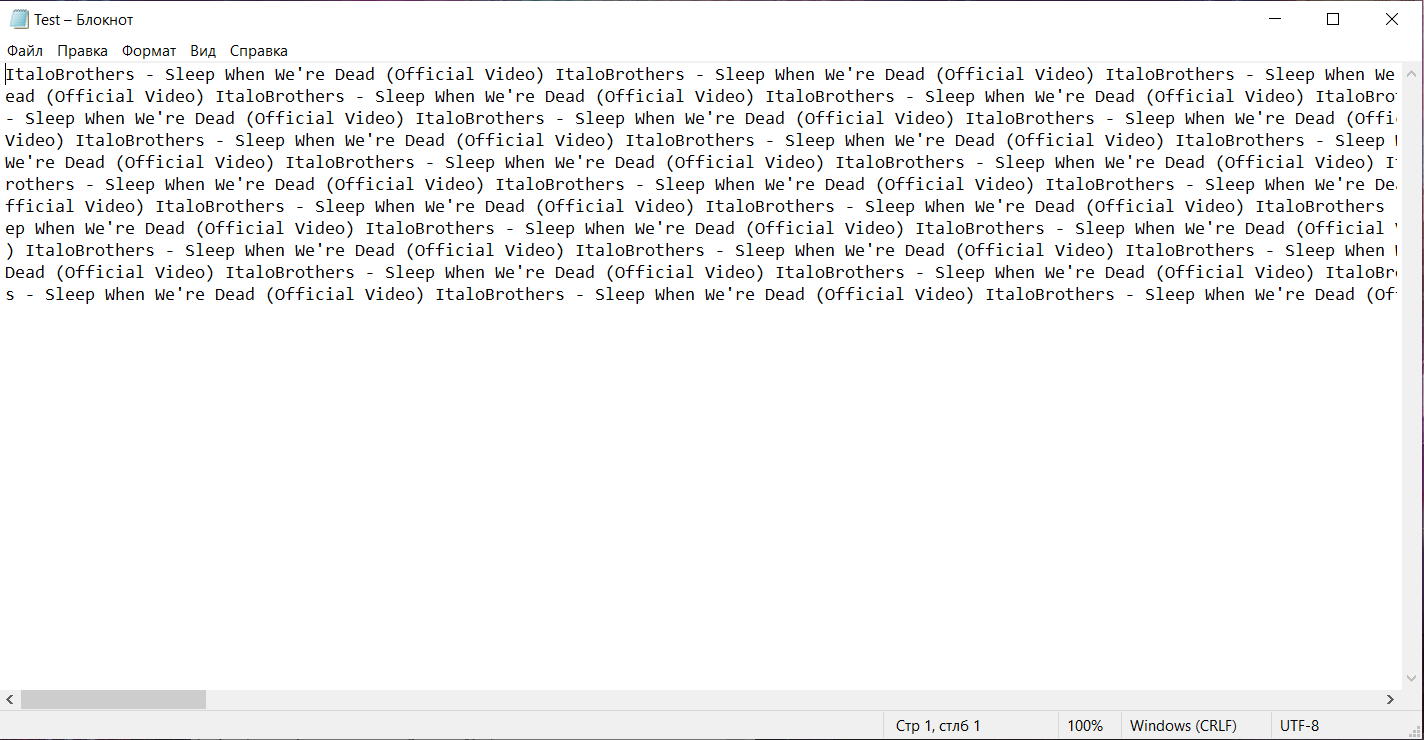
1. Створити публічну та секретну пари ключів. Уважно вивчити і зрозуміти протокол.



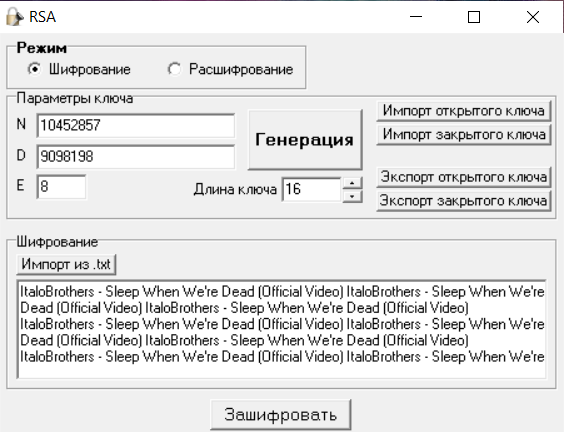


**Рис.2.** Створив пару ключів

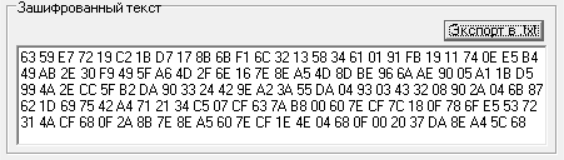
1. Зашифрувати і розшифрувати текстове повідомлення (до 20 Кб).



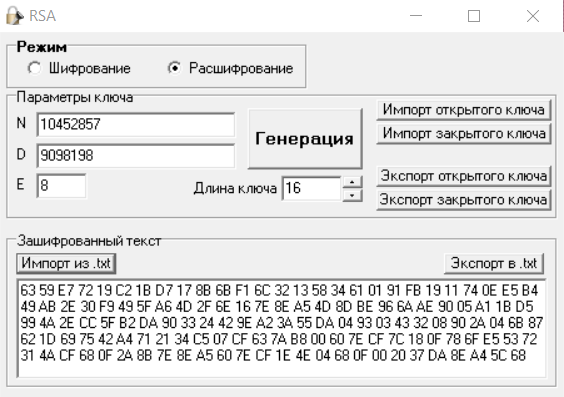
**Рис.3.** Текстове повідомлення, яке буде зашифроване (розмір файлу – 10 Кб)



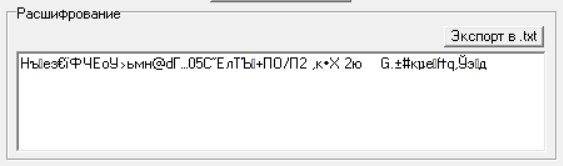
**Рис.4.** Шифрування тектсового повідомлення



**Рис.5.** Результат шифрування



**Рис.6.** Розшифрування текстового повідомлення



**Рис.7.** Результат розшифрування повідомлення

1. Зафіксувати час генерації ключів і швидкості шифрування і дешифрування для трьох значень довжини ключа: 16, 32, 64 біт. Порівняти їх з відповідними швидкостями симетричного алгоритму з лаб. роб. 2.

Час генерації публічного та приватного ключа довжиною 16 біт:





**Рис.8.** Час генерації ключів(довжина ключів – 16 біт)

Час, за який програма зашифрувала текстове повідомлення розміром 10 Кб становить – 56 секунд:



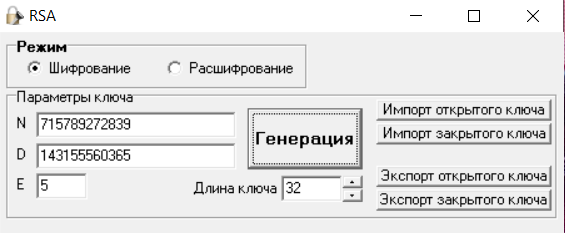
**Рис.9.** Час шифрування(довжина ключів – 16 біт)

Час, за який програма розшифрувала текстове повідомлення розміром 46,8 Кб становить – 82 секунди:



**Рис.10.** Час розшифрування(довжина ключів – 16 біт)

Генерація ключів довжиною 32 біт становить 1 секунду:



**Рис.11.** Час генерації ключів(довжина ключів – 32 біт)

Час шифрування текстового повідомлення, розміри ключів якого дорівнюють 32 біт становить 38 секунд:



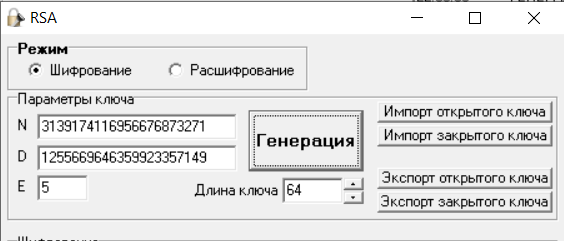
**Рис.12.** Час шифрування(довжина ключів – 32 біт)

Час розшифровування текстового повідомлення ключами розміри яких становить 32 біт, дорівнює 88 секунд:



**Рис.13.** Час розшифровування(довжина ключів – 32 біт)

Час генерації ключів, довжина яких становитиме 64 біт, становить – 1 секунду







**Рис.14.** Час генерації(довжина ключів – 64 біт)

Час шифрування текстового повідомлення ключами, розмір яких становить 64 біт, дорівнює – 45 секунд



**Рис.15.** Час шифрування(довжина ключа – 64 біт)

Час розшифровування текстового повідомлення, ключами розмір яких становить 64 біт, дорівнює – 174 секунди



**Рис.16.** Час розшифрування(довжина ключа – 64 біт)

Якщо порівнювати час шифрування із лабораторної роботи №2, то там відповідний файл шифрувався 2 секунди, що набагато швидше ніж за допомогою алгоритму RSA у випадку RSA залежно від довжини ключів це число різне, у моєму випадку 56, 38, 45 секунд, але у той час у RSA алгоритму час розифрування відбувався також залежно від довжини ключів, у моєму випадку це 82, 88, 174 секунд, а розшифровування у №2 лабораторній роботі виконувалося за 1,5 секунд.

Швидкості:

1. 10.4 / 2 = 5.2 (Кб/с) – швидкість програми Kryptel (№2 лабораторна)
2. 10.4 / 1.5 = 6.93 (Кб/с) – швидкість дешифрування Kryptel.
3. 10.4 / 56 = 0.18 (Кб/с) – швидкість шифрування для ключа довжиною 16 біт
4. 10.4 / 82 = 0.12 (Кб/с) – швидкість розшифрування для ключа довжиною 16 біт
5. 10.4 / 38 = 0.27 (Кб/с) – швидкість шифрування для ключа довжиною 32 біт
6. 10.4 / 88 = 0.11 (Кб/с) – швидкість розшифровування для ключа довжиною 32 біт
7. 10.4 / 45 = 0.23 (Кб/с) – швидкість шифрування для ключа довжиною 64 біт
8. 10.4 / 174 = 0.05 (Кб/с) – швидкість розшифровування для ключа довжиною 64 біт

Отже, симетричний алгоритм шифрування швичший, ніж алгоритм RSA.

**Висновок:**

На лабораторній роботі я дослідив програму асиметричного алгоритму RSA, навчився в ній працювати, а саме: створювати приватні та публічні ключі для подальшого їх використання у шифруванні та розшифруванні текстового повідомлення. Зрозумів, що при збільшуванні довжини ключів процес генерації, шифрування та розшифрування буде збільшуватися у часі.