Міністерство освіти і науки України Львівський
національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра програмування

Звіт до лабораторної роботи №5 з теми

# “RSA шифр”

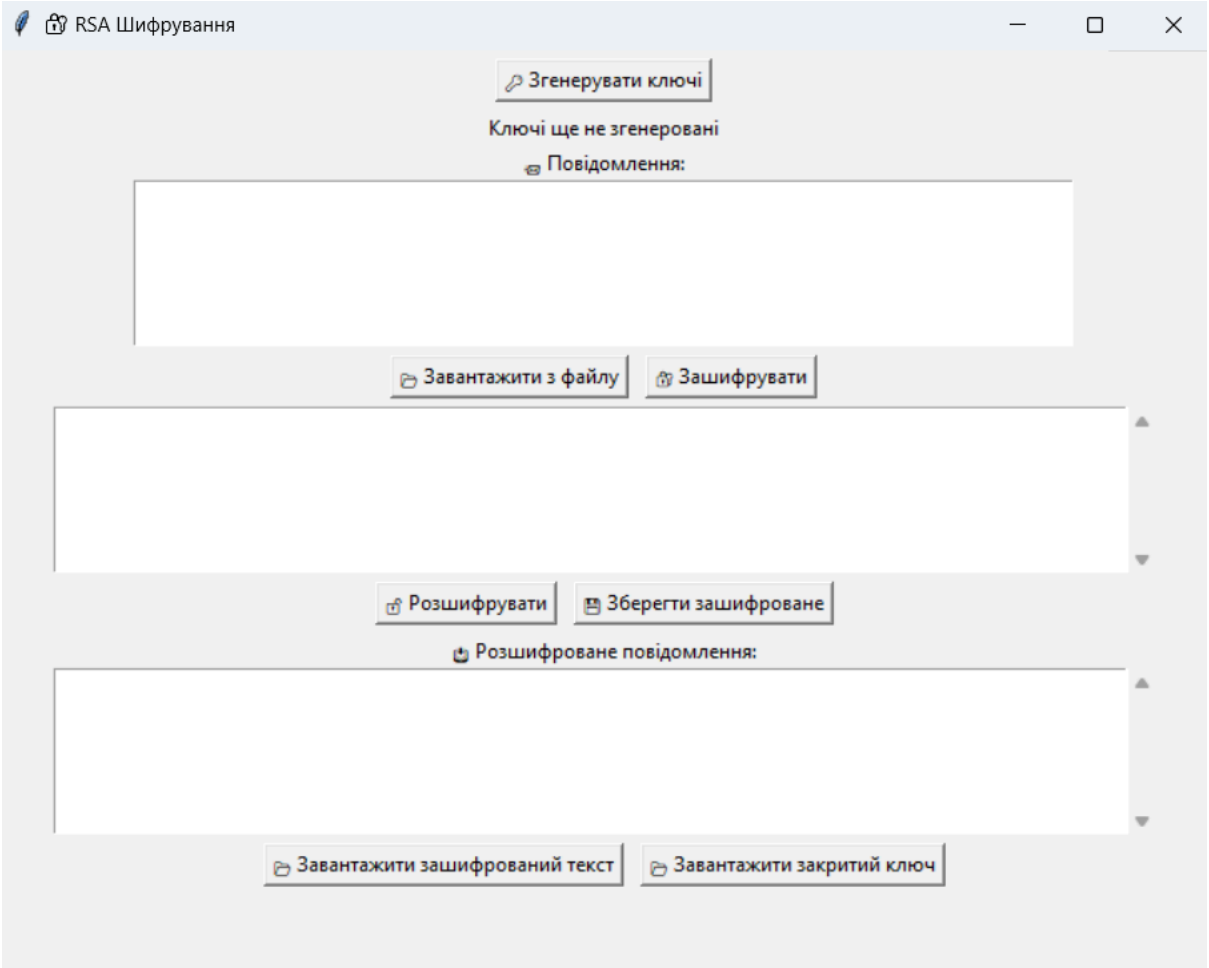
Підготував:
студент групи ПМІ-31
Урбанський Максим

Львів-2025

**Мета:** реалізувати шифр RSA.

## Хід роботи

1. Реалізував інтерфейс за допомогою Python, tkinter.



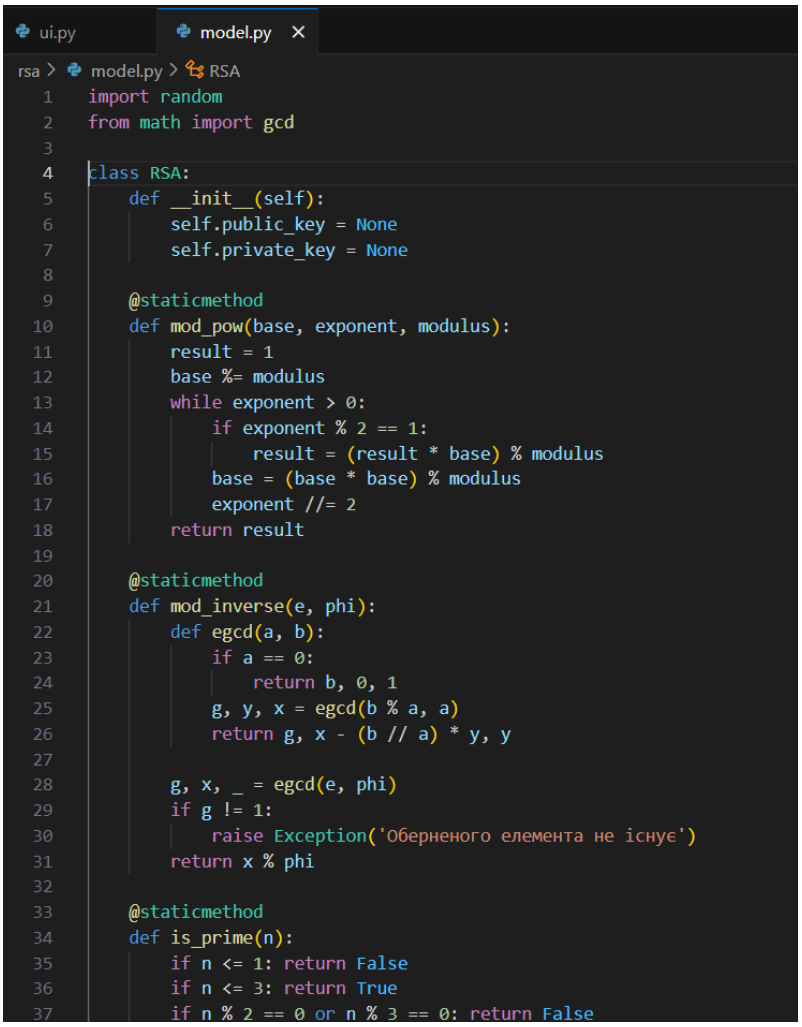

Ми можемо згенерувати публічний і приватний ключі як і зберегти приватний ключ.

Можемо завантажити текст з файлу так і ввести вручну.

Можемо завантажити і зберегти зашифрований текст.

Підтримується і англійська і українська мови.

2. Розробив клас, де реалізував методи потрібні для роботи програми.



3. Написав тести перевірити функціонал.

```python
class TestRSA(unittest.TestCase):
    def setUp(self):
        self.rsa = RSA()
        self.public_key, self.private_key, self.p, self.q = self.rsa.generate_keys()

    def test_keys_are_not_none(self):
        self.assertIsNotNone(self.public_key)
        self.assertIsNotNone(self.private_key)

    def test_keys_are_distinct(self):
        self.assertNotEqual(self.p, self.q)

    def test_mod_pow(self):
        base, exp, mod = 4, 13, 497
        expected = pow(base, exp, mod)
        result = self.rsa.mod_pow(base, exp, mod)
        self.assertEqual(result, expected)

    def test_mod_inverse(self):
        e = 17
        phi = 3120
        d = self.rsa.mod_inverse(e, phi)
        self.assertEqual((e * d) % phi, 1)

    def test_is_prime_true(self):
        self.assertTrue(self.rsa.is_prime(101))

    def test_is_prime_false(self):
        self.assertFalse(self.rsa.is_prime(100))

    def test_encrypt_decrypt(self):
        message = "Привіт, RSA!"
        encrypted = self.rsa.encrypt(message, self.public_key)
        self.assertIsInstance(encrypted, list)
        decrypted = self.rsa.decrypt(encrypted, self.private_key)
        self.assertEqual(decrypted, message)
```

**Висновок:** на цій практичній роботі я навчився реалізовувати шифрування за допомогою RSA.