**Міністерство освіти і науки України**

**Національний технічний університет України**

**“Київський політехнічний інститут імені Ігоря Сікорського”**

**Фізико-технічний інститут**

**Методи реалізації криптографічних механізмів**

Лабораторна робота №3

**Виконала:**

студентка ФІ-31мн

Двоєглазова (Панкєєва) С.Д.

**Перевірила:**

Селюх П. В.

Київ – 2024

**Лабораторна робота №3. Реалізація основних асиметричних криптосистем.**

***Мета:***

Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

***Завдання:***

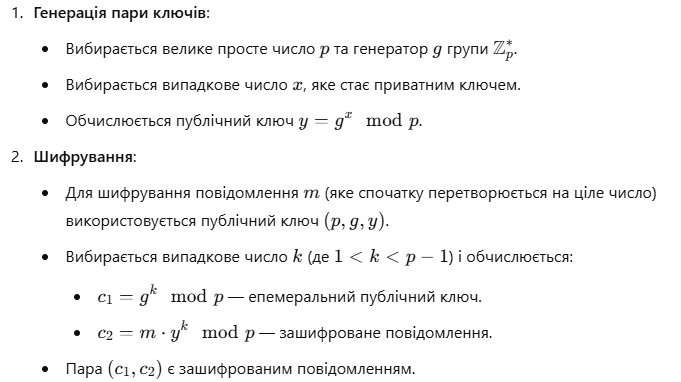
Для другого типу лабораторних робіт ― розробити реалізацію асиметричної криптосистеми.

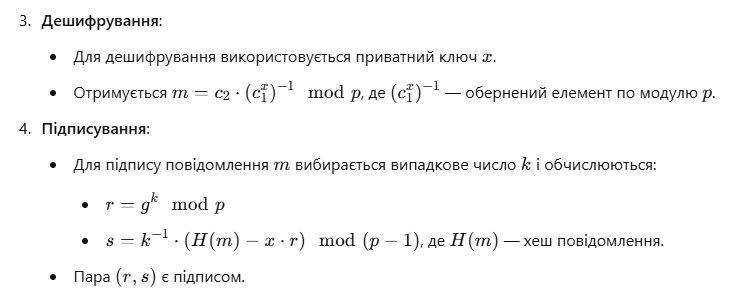
Бібліотека OpenSSL під Windows платформу. Кр\с Ель Гамаля.

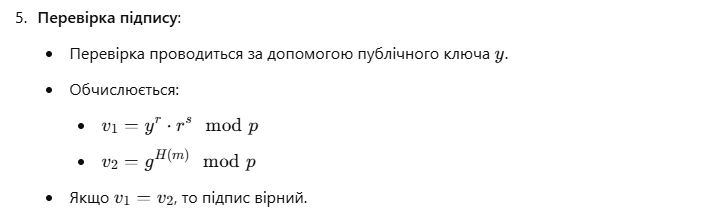
Оформлення результатів. Контрольний приклад роботи з асиметричною криптосистемою.

**Хід роботи:**

Схема Ель Гамаля ― це криптографічна система, яка забезпечує шифрування, дешифрування, підпис та перевірку цифрового підпису на основі задачі дискретного логарифмування.







**1. Клас ElGamalCrypto**

Основний клас, що реалізує всі криптографічні операції системи Ель Гамаля.

**Допоміжні функції:**

* text\_to\_number(text: str) -> int:

Вхід: текстовий рядок

Вихід: числове представлення тексту

Призначення: конвертація тексту в числовий формат для криптографічних операцій

* number\_to\_text(number: int) -> str:

Вхід: число

Вихід: декодований текст

Призначення: конвертація числа назад у текст

**Основні криптографічні функції:**

1. create\_key\_pair():

Вхід: немає

Вихід: кортеж (приватний ключ, публічний ключ)

Призначення: генерація пари ключів для шифрування

1. encode\_message(pub\_key, plaintext):

Вхід:

* + - pub\_key: публічний ключ отримувача
    - plaintext: текст для шифрування

Вихід: кортеж (тимчасовий ключ, зашифроване повідомлення)

Призначення: шифрування повідомлення

1. decode\_message(priv\_key, temp\_key, encrypted):

Вхід:

* + - priv\_key: приватний ключ
    - temp\_key: тимчасовий ключ
    - encrypted: зашифроване повідомлення

Вихід: розшифрований текст

Призначення: дешифрування повідомлення

1. create\_signature(priv\_key, message):

Вхід:

* + - priv\_key: приватний ключ
    - message: повідомлення для підпису

Вихід: цифровий підпис (r, s)

Призначення: створення цифрового підпису

1. verify\_signature(pub\_key, message, signature):

Вхід:

* + - pub\_key: публічний ключ
    - message: повідомлення
    - signature: підпис для перевірки

Вихід: булеве значення (true/false)

Призначення: перевірка цифрового підпису

**Використані бібліотеки**

1. cryptography.hazmat.primitives:

hashes: для хешування

dh: реалізація протоколу Діффі-Хеллмана

HKDF: для генерації ключів

**Висновки**

1. Реалізована криптосистема забезпечує:

* Безпечне шифрування/дешифрування повідомлень
* Створення та перевірку цифрових підписів
* Надійну генерацію ключів

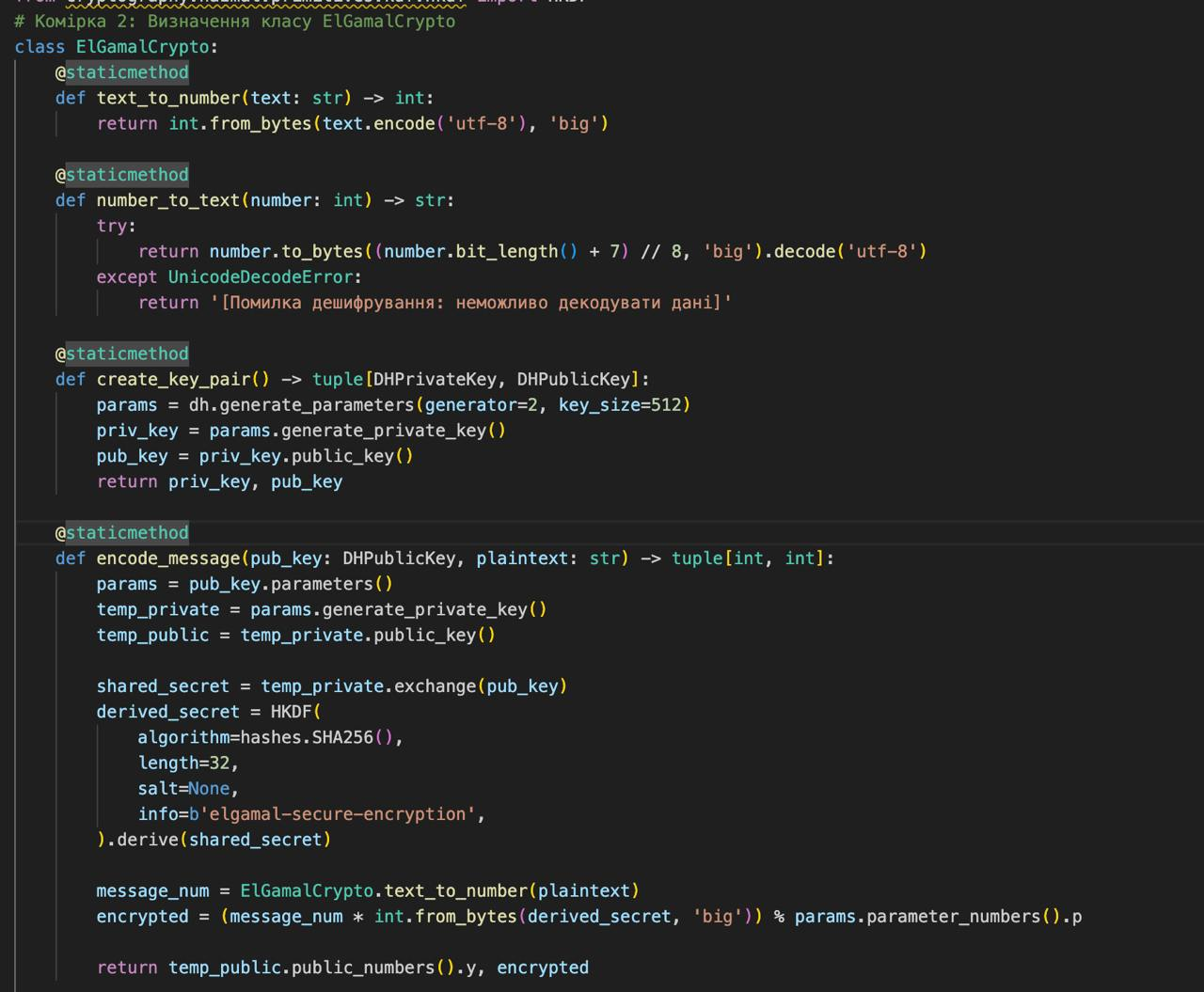
1. Основні переваги реалізації:

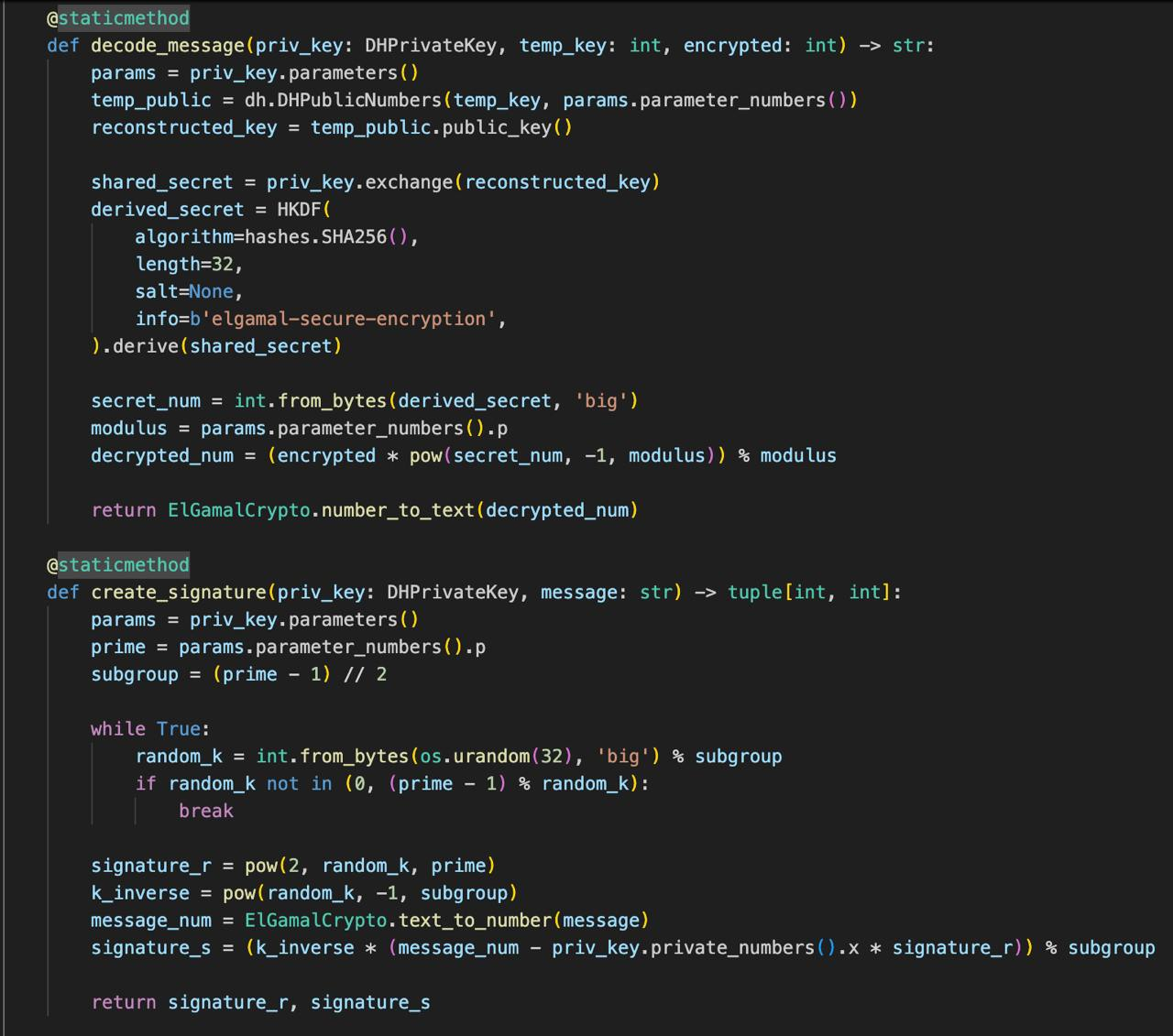
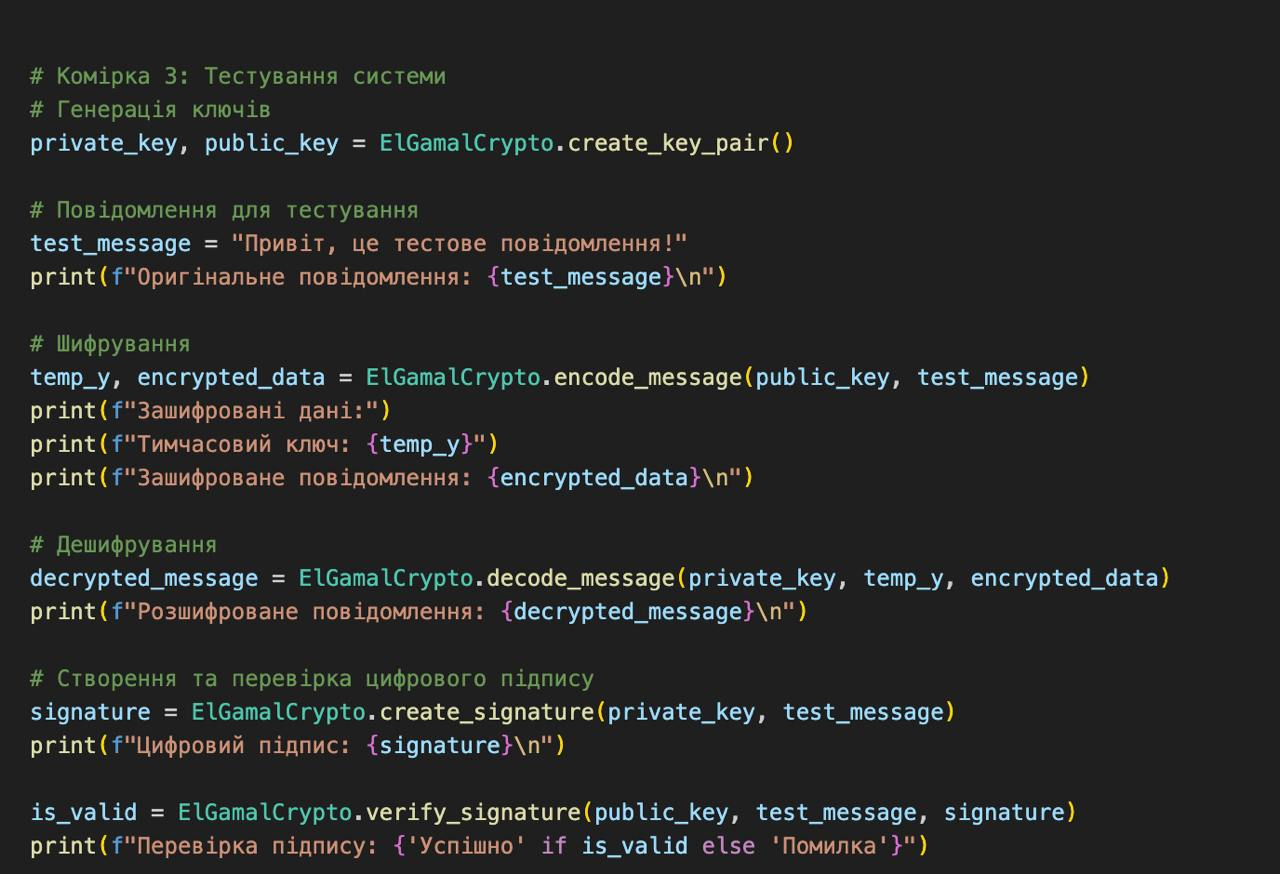
* Використання сучасних криптографічних примітивів
* Структурований об'єктно-орієнтований підхід
* Захист від базових криптографічних атак

1. Покращення порівняно з оригінальним кодом:

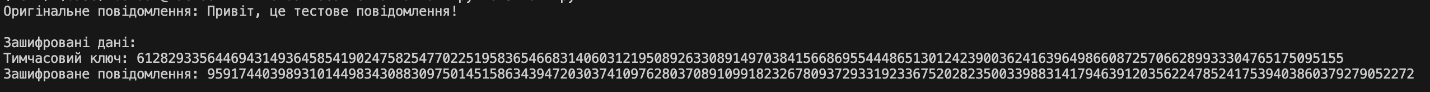
* Кращій організація коду через використання класу
* Більш інформативні назви функцій
* Покращена обробка помилок
* Додаткові перевірки безпеки

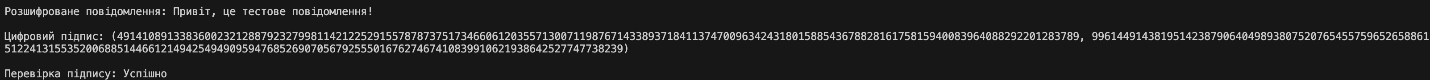
**Код програми:**



**Скріни виконання програми:**

****

****

**Використана література :**

1. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.:Изд-во ТРИУМФ, 2002. -816 с