МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Чернігівська політехніка»

Навчально-науковий інститут електроних та інформаційних технологій

Кафедра кібербезпеки та математичного моделювання

**ЗВІТ**

про виконання лабораторної роботи

з дисципліни «Основи криптографічного захисту інформації»

Виконав: здобувач 3 курсу, групи КБ-221 Регент Анастасія

Перевірив: Шелест Михайло Євгенович

НУ «Чернігівська політехніка» 2025

Лабораторна робота № 8

**Криптографія на еліптичних кривих**

**Мета роботи:**

Набути навичок роботи з точками на еліптичних кривих.

Зрозуміти основні операції: додавання, подвоєння, множення на скаляр та інверсія точки.

Застосувати ці операції в криптографічних алгоритмах.

**Завдання № 1 Основні операції з точками на еліптичній кривій Веєштраса**

**Теоретична частина**

Еліптична крива Веєштраса має рівняння: = + ax + b (mod p), де:

a, b - коефіцієнти кривої,

p - просте число (характеристика поля),

O - нейтральний елемент (нескінченність).

**Можливі такі основні операції:**

**Додавання двох точок P і Q:**

**якщо P ≠ Q:**

λ = ( - ) / ( - ) (mod p)

= - - (mod p)

= λ( -) - (mod p)

**якщо P = Q (подвоєння):**

λ = (3 + a) / (2) (mod p)

x3 = - 2 (mod p)

y3 = λ(- ) - (mod p)

**Множення точки на скаляр kP:**

Реалізується методом подвоєння і додавання.

**Інверсія точки:**

Якщо P = (x, y), то -P = (x, -y mod p)

**Завдання:**

Для заданих параметрів кривої та двох точок P і Q (у відповідності до варіанту з таблиці 1):

Обчислити суму точок P + Q.

Обчислити подвоєння точки 2P.

Знайти множення на скаляр 3P.

Обчислити інверсію точки -P.

Зауваження: обчислення можна зробити вручну або скласти програму.

Оформити результати у вигляді звіту із поясненням кожного обчислення.

Таблиця 1 – Дані

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Варіант | p |  | b | P | Q |
| 2 | 16 | 19 | 16 | (6,9) | (20,9) |

**Вирішення вручну**

**Обчислення суми точок P + Q**

Модуль 16 не є простим, тому не всі елементи мають обернені – це потрібно враховувати під час обчислень.

|  |  |
| --- | --- |
| Крок 1: Перевірка умови | |
|  | (1.1) |
|  | (1.2) |
| , , | (1.3) |
| , – можна використати формулу для додавання різних точок | (1.4) |
| Крок 2: Формула | |
|  | (1.5) |
|  | (1.6) |
|  | (1.7) |
| Крок 3: Перевірка оберненого | |
|  | (1.8) |
| Отже, оберненого не існує, тому | (1.9) |

**Обчислення подвоєння точки 2P**

|  |  |
| --- | --- |
| Крок 1: Формула | |
|  | (2.1) |
| , , | (2.2) |
| Крок 2: Знаходження чисельника та знаменника | |
| Чисельник: | (2.3) |
|  | (2.4) |
| Знаменник: | (2.5) |
|  | (2.6) |
| Крок 3: Знаходження обернене до 2 | |
|  | (2.7) |
| Отже, оберненого не існує, тому | (2.8) |

**Знаходження множення на скаляр 3P**

|  |  |
| --- | --- |
|  | (3.1) |
|  | (3.2) |
|  | (3.3) |
| Отже, 3 | (3.4) |

**Обчислення інверсії точки -P (інверсія точки)**

|  |  |
| --- | --- |
|  | (4.1) |
|  | (4.2) |
|  | (4.3) |
| Отже, - | (4.4) |

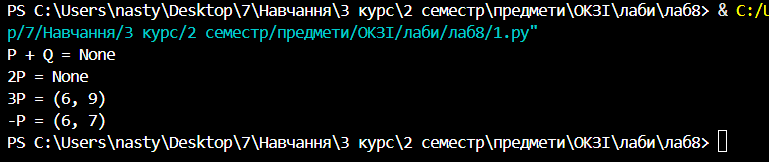


Рисунок 1 – Результат в терміналі

**Завдання № 2** **Криптографічні алгоритми на еліптичних кривих**

У цьому завдані знайомимся з основами роботи криптографічних алгоритмів на еліптичних кривих.

Використовуйте бібліотеку cryptography або ecdsa для генерації ключової пари на основі еліптичної кривої.

**Крок 1: Генерація ключової пари ECDSA**

**Вхідні дані**: крива: secp256k1.

**Завдання**:

Згенеруйте приватний ключ на основі кривої secp256k1.

Згенеруйте відповідний публічний ключ.

Збережіть ключі у форматі PEM.

Перевірте, що публічний ключ відповідає приватному.

**Крок 2: Підпис повідомлення за допомогою ECDSA**

Реалізуйте підпис повідомлення за допомогою приватного ключа та перевірку підпису публічним ключем.

**Вхідні дані**: текст повідомлення "Hello, ECDSA!".

**Завдання**:

Згенеруйте підпис повідомлення приватним ключем.

Збережіть підпис у файлі.

Реалізуйте функцію для перевірки підпису з використанням публічного ключа.

Перевірте коректність підпису.

**Крок 3: Реалізація протоколу Діффі-Геллмана на еліптичних кривих (ECDH)**

Реалізуйте обмін ключами на основі еліптичних кривих.

**Вхідні дані**:

Крива: = + 2x + 3 (mod  97)

Генератор: G = (3, 6)

Закриті ключі: a = 5, b = 7

**Завдання**:

Обчисліть відкриті ключі A = aG і B = bG.

Знайдіть спільний секрет S = aB = bA.

Перевірте, що S однаковий для обох сторін.

Збережіть спільний секрет у захищеному форматі.

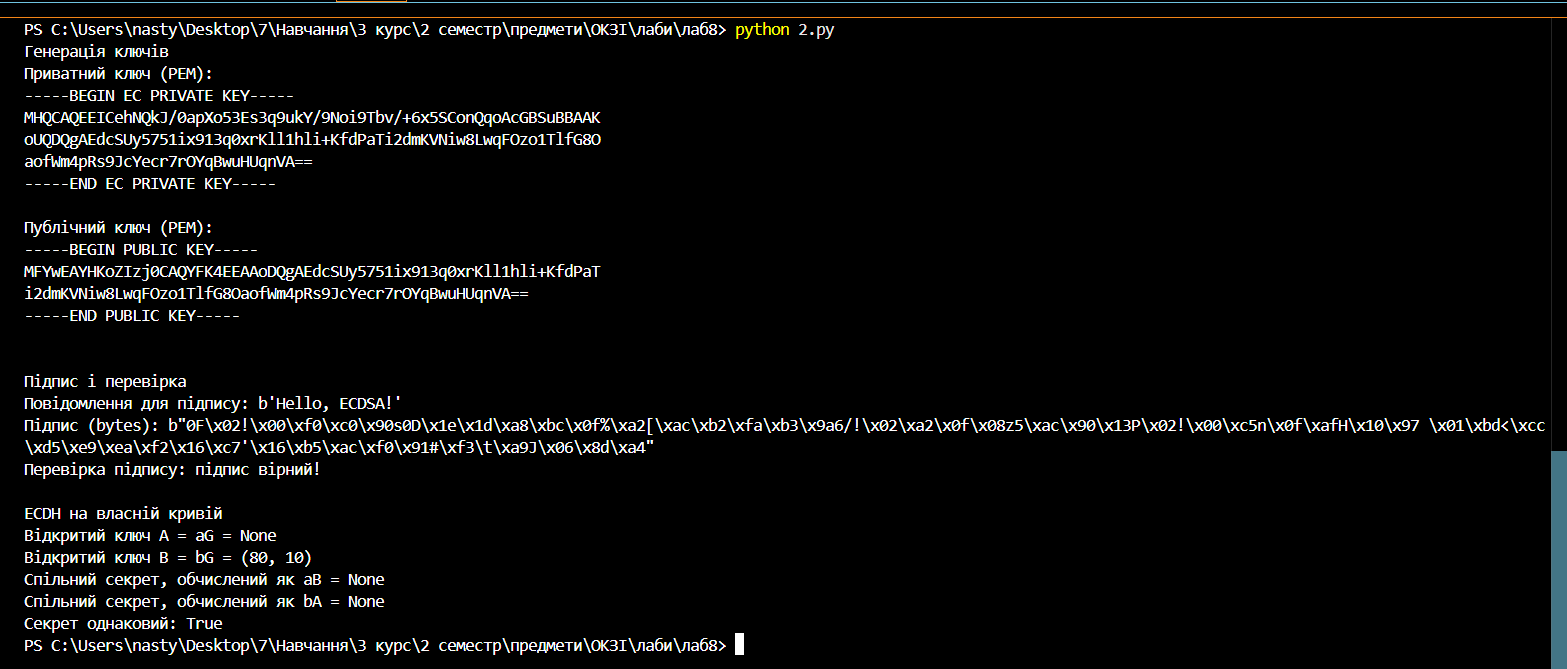


Рисунок 2 – Результат в терміналі

**Посилання на репозиторій:** [**https://github.com/Anasteishha/FCIP**](https://github.com/Anasteishha/FCIP)

**Контрольні питання**

1. Які основні операції можна виконувати з точками на еліптичних кривих?

Основні операції з точками на еліптичних кривих включають додавання двох точок, подвоєння точки та знаходження оберненої точки. Ці операції формують алгебраїчну групу, що використовується в криптографії для побудови ключів та обчислення спільних секретів.

2. Яка різниця між ECDH та ECDSA?

Різниця між ECDH та ECDSA полягає в їхніх призначеннях: ECDH (Elliptic Curve Diffie-Hellman) — це протокол обміну ключами, який дозволяє двом сторонам безпечно створити спільний секрет, тоді як ECDSA (Elliptic Curve Digital Signature Algorithm) — це алгоритм цифрового підпису, який забезпечує автентифікацію та цілісність повідомлень.

3. Чому криптографія на еліптичних кривих вважається безпечною?

Криптографія на еліптичних кривих вважається безпечною через складність задачі дискретного логарифмування на еліптичних кривих, яку поки що не вдається ефективно розв’язати класичними методами, що робить ключі набагато менш вразливими при меншій довжині у порівнянні з традиційними алгоритмами.

4. Які переваги використання еліптичних кривих у порівнянні з RSA?

Переваги використання еліптичних кривих порівняно з RSA полягають у меншій довжині ключів при аналогічному рівні безпеки, що забезпечує швидші обчислення, зменшену пам’ять для зберігання ключів і менші вимоги до пропускної здатності мережі.

5. Які атаки можливі на еліптичні криві і як їх уникнути?

Атаки на еліптичні криві можуть включати атаки стороннього каналу (side-channel attacks), атаки на слабкі або неправильно вибрані параметри кривої, а також атаки за допомогою квантових комп’ютерів. Для уникнення цих атак необхідно використовувати стандартні перевірені криві, захищені реалізації, стійкі до сторонніх каналів, та слідкувати за розвитком квантової криптографії.

6. Як можна зберегти отриманий у ECDH спільний секрет у захищеному форматі?

Отриманий у ECDH спільний секрет можна зберегти у захищеному форматі шляхом застосування симетричного шифрування (наприклад, AES) з ключем, похідним від спільного секрету, або використанням функцій виводу ключів (KDF) для генерації криптографічно стійкого ключа перед зберіганням.