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 № 7

**Протоколи узгодження ключів**

**Мета лабораторної роботи:** ознайомлення з основами протоколів узгодження ключів та придбання практичних навичок їх реалізації та використання у криптографії.

**Мета завдань:** Освоїти основні кроки функціонування протоколу Діффі-Геллмана та системи шифрування Ель-Гамаля.

**Завдання № 1 Обчислення загального секрету за протоком Діффі-Геллмана**

Дві сторони, Аліса і Боб, хочуть узгодити спільний секрет за допомогою протоколу Діффі-Геллмана.

**Задано (згідно з порядковим номером у таблиці 1):**

просте число p,

генератор ,

закритий ключ Аліси a,

закритий ключ Боба b.

**Потрібно знайти:**

Відкритий ключі A = (mod  p) і B = mod  p).

Спільний секрет S = (mod  p) з боку Аліси.

Спільний секрет S = (mod  p) з боку Боба.

Пояснити, чому отримані значення S збігаються.

Напишіть програм**у** (якщо неохота рахувати руками :), яка реалізує протокол Діффі-Геллмана. Програма повинна:

Обчислювати відкриті ключі A і B.

Обчислювати спільний секрет S для обох сторін.

Перевіряти, що отриманий спільний секрет однаковий.

Підказка: Використовуйте Python-функцію pow(base, exp, mod) для обчислення модульного піднесення до степеня.

Таблиця 1 – Дані

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Варіант | p |  | a | b |
| 7 | 29 | 2 | 23 | 13 |

**Ручний розрахунок**

**Обчислення відкритого ключа Аліси**

|  |  |
| --- | --- |
|  | (1.1) |
| Покрокове піднесення до степення : | (1.2) |
|  | (1.3) |
|  | (1.4) |
|  | (1.5) |
|  | (1.6) |
|  | (1.7) |
| Розкладемо: | (1.8) |
|  | (1.9) |
|  | (1.10) |
|  | (1.11) |

**Обчислення відкритого ключа Боба**

|  |  |
| --- | --- |
|  | (2.1) |
| Покрокове піднесення до степення : | (2.2) |
|  | (2.3) |
|  | (2.4) |
|  | (2.5) |
|  | (2.6) |
|  | (2.7) |
|  | (2.8) |

**Обчислення спільного секрету**

|  |  |
| --- | --- |
| З боку Аліси | |
|  | (3.1) |
| Поетапне обчислення: | (3.2) |
|  | (3.3) |
|  | (3.4) |
|  | (3.5) |
|  | (3.6) |
|  | (3.7) |
|  | (3.8) |
|  | (3.9) |
|  | (3.10) |

**Обчислення спільного секрету**

|  |  |
| --- | --- |
| З боку Боба | |
|  | (4.1) |
| Поетапне обчислення: 1 | (4.2) |
|  | (4.3) |
|  | (4.4) |
|  | (4.5) |
|  | (4.6) |
|  | (4.7) |
|  | (4.8) |
|  | (4.9) |

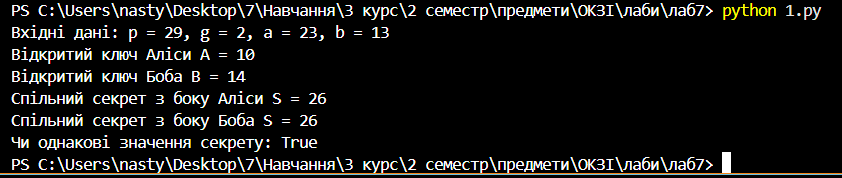


Рисунок 1 – Результат в терміналі

**Завдання № 2** **Атака "людина посередині"**

Продемонструйте вразливість класичного протоколу Діффі-Геллмана до атаки "людина посередині" (Man-in-the-Middle).

**Сценарій:**

Аліса хоче узгодити ключ із Бобом через відкритий канал.

Зловмисник Малін підміняє повідомлення:

Відправляє Бобу свій ключ замість Аліси.

Відправляє Алісі свій ключ замість Боба.

Аліса й Боб обчислюють ключі (значення параметрів **p, a** та **b** згідно з варіантом у таблиці 1), думаючи, що спілкуються між собою, але насправді Малін отримує всі дані.

**Завдання:**

Покажіть, як Малін, який використовує m=10 як свій закритий ключ, може обчислити спільний секрет із кожною стороною.

Обчисліть підроблені ключі ​ і .

**Ручний розрахунок**

|  |  |
| --- | --- |
| Сценарій атаки | |
|  | (5.1) |
|  | (5.2) |
| Відправляє , але Малвін перехоплює. | |
| Малвін підміняє і надсилає Бобу свій відкритий ключ: | |
|  | (5.3) |
|  | (5.4) |
|  | (5.5) |
|  | (5.6) |
| З боку Боба | |
|  | (5.7) |
| Надсилає , але Малвін перехоплює, надсилає Алісі свій | |

**Обчислення підроблених секретів**

|  |  |
| --- | --- |
| Спільний секрет між Алісою та Маліним | |
|  | (6.1) |
| Поетапне обчислення: | (6.2) |
|  | (6.3) |
|  | (6.4) |
|  | (6.5) |
|  | (6.6) |
|  | (6.7) |
|  | (6.8) |
|  | (6.9) |
|  | (6.10) |
|  | (6.11) |
| Спільний секрет між Бобом та Маліним | |
|  | (6.12) |
| Поетапне обчислення: 1 | (6.13) |
|  | (6.14) |
|  | (6.15) |
|  | (6.16) |
|  | (6.17) |
|  | (6.18) |
|  | (6.19) |
|  | (6.20) |
|  | (6.21) |

Отже, спільний секрет між Бобом та Маліним є , а спільний секрет між Бобом та Маліним є .

**Завдання № 3 Автентифікований протокол Діффі-Хеллмана.**

До лабораторної роботи №7 додано файл з прикладом реалізації анонімного протоколу Діффі-Хеллмана з використанням бібліотеки cryptography. Як нам відомо з лекції – анонімний протокол Діффі-Хеллмана вразливий до атак посередника.

**Ваше завдання:** Аналогічним чином реалізувати автентифікований протокол Діффі-Хеллмана, використовуючи схему RSA-PSS для підпису.

**Додаткова інформація:**

Для довідки користуйтесь слайдами лекції, що описують автентифікований протокол Діффі-Хеллмана.

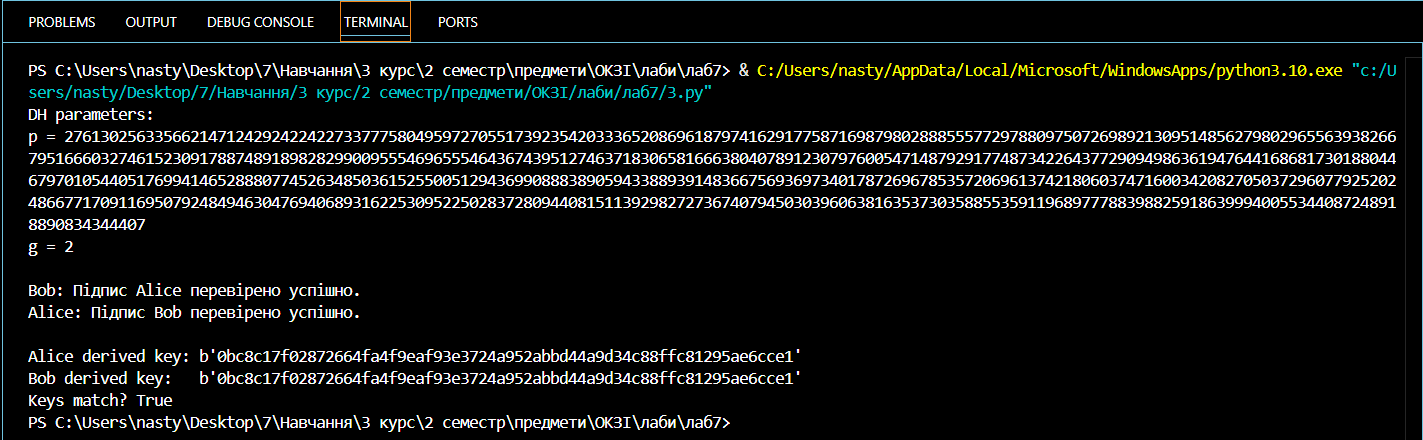
****

Рисунок 2 – Результат в терміналі

**Завдання № 4 Шифрування та розшифрування в системі Ель-Гамаля**

**Дано (**згідно з варіантом у таблиці 2**):**

повідомлення M.

просте число p.

генератор g.

закритий ключ Аліси x.

випадкове число для шифрування k.

**Потрібно:**

Обчислити відкритий ключ Аліси y = mod p.

Виконати шифрування повідомлення M

= mod p

= M \* mod p

Виконати розшифрування шифротексту (, )

s = mod p

M' = \* mod p ( — обернене до s за модулем p).

Перевірити, що M' = M.

Очікуваний результат: при правильних обчисленнях вихідне M має відновитися.

Таблиця 2 – Дані

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Варіант | M |  | g | b | k |
| 7 | 21 | 29 | 2 | 9 | 4 |

**Написати код (якщо неохота рахувати руками :), який:**

Обчислює відкритий ключ y.

Виконує шифрування повідомлення M випадковим k.

Виконує розшифрування отриманого шифртексту.

Підказка.

**Важливо правильно використовувати функцію для знаходження оберненого елемента** (**modinv**):

використовується pow(a, -1, p) (Python 3.8+) або extended Euclidean algorithm у старих версіях.

pow(base, exp, mod) — функція Python для швидких обчислень модульної експоненти.

**Ручний розрахунок**

|  |  |
| --- | --- |
| Обчислення відкритого ключа Аліси | |
|  | (7.1) |
|  | (7.2) |
|  | (7.3) |
|  | (7.4) |
| Шифрування | |
|  | (7.5) |
|  | (7.6) |
|  | (7.7) |
|  | (7.8) |
|  | (7.9) |
|  | (7.10) |
|  | (7.11) |
|  | (7.12) |
| Розшифрування | |
|  | (7.13) |
|  | (7.14) |
|  | (7.15) |
|  | (7.16) |
|  | (7.17) |
|  | (7.18) |
|  | (7.19) |
|  | (7.20) |
| Отже, розшифрування успішне | (7.21) |

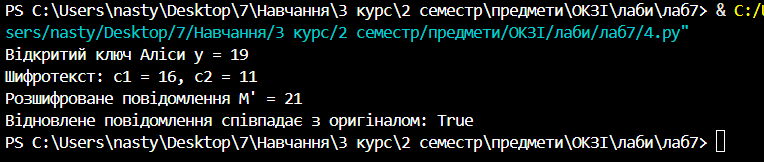


Рисунок 3 – Результат в терміналі

**Контрольні запитання**

1. Що таке проблема узгодження ключів у криптографії?

Проблема узгодження ключів — це задача, коли дві (або більше) сторони, які хочуть спілкуватися конфіденційно, повинні домовитися про спільний секретний ключ для шифрування, але не мають безпечного каналу для його передачі. Необхідно знайти спосіб узгодити ключ так, щоб він залишався недоступним для зловмисників.

2. Які переваги та недоліки криптографії на відкритих ключах у порівнянні з симетричною криптографією?

**Переваги:**

Не потрібно безпечного каналу для передачі ключа.

Легше керувати ключами у великих мережах (кожен має відкритий і закритий ключ).

Підтримка цифрових підписів і автентифікації.

**Недоліки:**

Повільніше за симетричну криптографію через складніші математичні операції.

Великі ключі і більше обчислювальних ресурсів.

Зазвичай використовується для обміну симетричними ключами, а не для прямого шифрування великих обсягів даних.

3. Яка основна ідея протоколу Діффі-Геллмана?

Основна ідея — дві сторони за допомогою відкритих параметрів (просте число ppp і генератор ggg) і своїх секретних чисел створюють спільний секретний ключ, який обчислюється незалежно і безпечно, навіть якщо зловмисник перехопить всю інформацію, що передається.

4. Як саме дві сторони можуть узгодити спільний секретний ключ без його відкритої передачі?

Кожна сторона вибирає секретне число (закритий ключ), обчислює відповідний відкритий ключ, передає його іншій стороні. Потім кожна сторона підносить отриманий відкритий ключ іншої сторони до своєї секретної степені по модулю ppp. Обидва отримують однаковий спільний секрет завдяки властивостям степеневих обчислень в модульній арифметиці.

5. Які атаки можливі на класичний DH-протокол? Як від них захиститися?

Атака "людина посередині" (MITM): зловмисник перехоплює та підмінює відкриті ключі сторін.

Захист – це використання автентифікації (сертифікати, цифрові підписи) та автентифікованих протоколів DH.

6. Чим автентифікований DH відрізняється від класичного? Які методи автентифікації можуть використовуватися?

В автентифікованому DH обмін ключами супроводжується перевіркою ідентичності сторін, що запобігає MITM-атакам.

**Методи автентифікації:**

1. Цифрові підписи.

2. Сертифікати від довірених центрів сертифікації.

3. Використання паролів чи додаткових секретів.

7. Яку криптографічну задачу використовує алгоритм Ель-Гамаля для забезпечення безпеки?

Задачу дискретного логарифму — знаходження xxx з y=gxmod  py = g^x \mod py=gxmodp вважають складною. Без розв’язку цієї задачі неможливо відновити секретний ключ із відкритого ключа.

8. У чому відмінність між шифруванням та цифровим підписом у схемі Ель-Гамаля?

Шифрування – захищає конфіденційність повідомлення, дозволяючи лише власнику секретного ключа розшифрувати.

Цифровий підпис – забезпечує автентичність і цілісність повідомлення, підтверджує, що повідомлення створене саме власником секретного ключа.

9. Чому в алгоритмі використовується випадкове число kkk при шифруванні та що станеться, якщо використовувати однакове випадкове число kkk для різних повідомлень?

Випадкове число kkk забезпечує унікальність шифротексту, навіть якщо повідомлення однакові, і підвищує стійкість до криптоаналізу.

Якщо використовувати однакове kkk для різних повідомлень:

Зловмисник може вирахувати співвідношення між повідомленнями або навіть відновити секретний ключ, що призведе до компрометації безпеки.