

ЛАБОРАТОРНА РОБОТА №3

з курсу

ТЕОРЕТИКО-ЧИСЛОВІ АЛГОРИТМИ В КРИПТОЛОГІЇ

Реалізація та застосування алгоритму дискретного логарифмування
index-calculus

Мета роботи

Ознайомлення з алгоритмом дискретного логарифмування index-calculus. Програмна реалізація цього алгоритму та визначення його переваг, недоліків та особливостей застосування. Практична оцінка складності роботи та порівняння різних реалізацій цього алгоритму.

Хід роботи

Написали програмні реалізації алгоритму index-calculus з і без розпаралелювання, продемонструємо працездатність для $p = 3$

```

$ python3 Lab3Index_calculus_threaded.py
Please enter alpha: 193
Please enter beta: 254
Please enter p: 373
[0, 0, 0, 0, 210]
[266, 0, 0, 0, 210]
[266, 353, 0, 0, 210]
[266, 353, 90, 0, 210]
[266, 353, 90, 241, 210]
Answer to equation  $193^x = 254 \bmod 373$  is 198
Time taken 0.031

(kali@kali)-[~/Desktop/lab3crypto]
$ python3 Lab3Index_calculus_threaded.py
Please enter alpha: 5
Please enter beta: 9
Please enter p: 307
[81, 0, 0, 0, 0]
[81, 1, 0, 0, 0]
[81, 1, 116, 0, 0]
[81, 1, 116, 4, 0]
[81, 1, 116, 4, 253]
Answer to equation  $5^x = 9 \bmod 307$  is 162
Time taken 0.035

$ python3 Lab3Index_calculus1.py
Please enter alpha: 193
Please enter beta: 254
Please enter p: 373
[266, 0, 0, 0, 0]
[266, 353, 0, 0, 0]
[266, 353, 90, 0, 0]
[266, 353, 90, 241, 0]
[266, 353, 90, 241, 210]
Answer to equation  $193^x = 254 \bmod 373$  is 198
Time taken 0.008

(kali@kali)-[~/Desktop/lab3crypto]
$ python3 Lab3Index_calculus1.py
Please enter alpha: 5
Please enter beta: 9
Please enter p: 307
[0, 1, 0, 0, 0]
[0, 1, 116, 0, 0]
[0, 1, 116, 4, 0]
[81, 1, 116, 4, 0]
[81, 1, 116, 4, 253]
Answer to equation  $5^x = 9 \bmod 307$  is 162
Time taken 0.047

Enter prime number decimal digit length: 3

Task Type 1:
a = 193;
b = 254;
p = 373.
2024-05-23 09:22:44 Please, found the discrete logarithm:  $a^x = b \bmod p$ . You have 5 minutes, starting now.
Enter x value: x = 198

2024-05-23 09:23:19 BINGO!!! You solve the discrete logarithm correct.
Next, please, solve the type 2 task.

Task Type 2:
a = 5;
b = 9;
p = 307.
2024-05-23 09:23:19 Please, found the discrete logarithm:  $a^x = b \bmod p$ . You have 5 minutes, starting now.
Enter x value: x = 162

2024-05-23 09:23:43 BINGO!!! You solve both tasks correct. You can be proud of yourself!
You can try again with bigger prime number decimal digit length. If you know what I mean ;)

2024-05-23 09:23:43 Tool closed.
```

Для генерування задач дискретного логарифмування використовували салюїда з другої лаби*

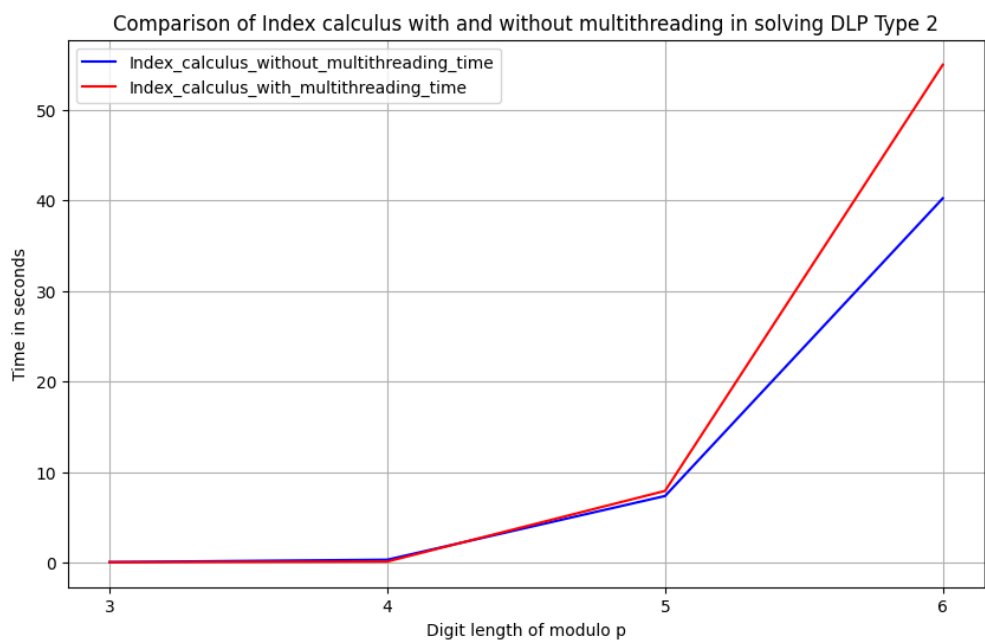
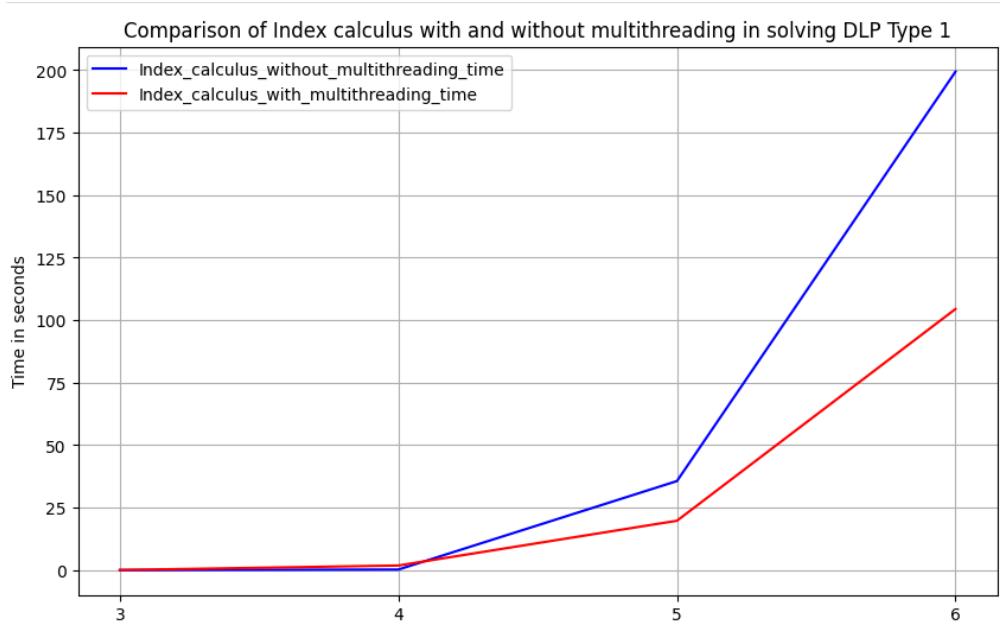
Результати для нашого граничного значення, з яким час роботи перевищує 5 хвилин (p = 7)

```
l-$ python3 Lab3Index_calculus_threaded.py
Please enter alpha: 601522
Please enter beta: 508792
Please enter p: 2244163
[0, 0, 0, 0, 0, 0, 1205189, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1978243, 0, 0, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 768796, 1978243, 0, 0, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 768796, 1978243, 0, 0, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 0, 0, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 0, 1670011, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 0, 0, 0, 47845, 0, 0, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 0, 681200, 0, 47845, 0, 0, 0, 792418, 0, 0, 0, 0]
]
[0, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 0, 681200, 0, 47845, 0, 480053, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 0, 47845, 0, 480053, 0, 792418, 0, 0, 0, 0]
[0, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 0, 47845, 0, 480053, 145250, 792418, 0, 0, 0, 0]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 0, 47845, 0, 480053, 145250, 792418, 0, 0, 0, 0]
8, 0, 0, 0, 0]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 647277, 47845, 0, 480053, 145250, 792418, 0, 0, 0, 0]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 647277, 47845, 0, 480053, 145250, 792418, 0, 0, 0, 186522]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 647277, 47845, 0, 480053, 145250, 792418, 0, 289409, 0, 186522]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 0, 1308725, 681200, 647277, 47845, 0, 480053, 145250, 792418, 0, 289409, 2036750, 186522]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 429640, 1308725, 681200, 647277, 47845, 0, 480053, 145250, 792418, 0, 289409, 2036750, 186522]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 429640, 1308725, 681200, 647277, 47845, 1497257, 480053, 145250, 792418, 0, 289409, 2036750, 186522]
]
[1818357, 277465, 768796, 1978243, 478818, 1670011, 1205189, 429640, 1308725, 681200, 647277, 47845, 1497257, 480053, 145250, 792418, 536624, 289409, 2036750, 186522]
Answer to equation 601522^x = 508792 mod 2244163 is 704834
Time taken 1672.923
```

Внесемо результати тестів в таблицю

Порядок	З розпаралелюванням		Без розпаралелювання	
	1 тип	2 тип	1 тип	2 тип
p = 3	0,031	0,035	0,008	0,047
p = 4	1,835	0,105	0,222	0,307
p = 5	19,742	7,915	35,611	7,349
p = 6	104,438	55,008	199,375	40,247

Візуалізація



Опис реалізації алгоритму з розпаралелюванням

Для розпаралелювання використовувалася python бібліотека threads

```
def generate_equations():
    total_length = len(factor_base) + const
    half_length = total_length // 2

    results1 = []
    results2 = []










    thread1 = threading.Thread(target=generate_half_equations, args=(half_length, results1))
    thread2 = threading.Thread(target=generate_half_equations, args=(total_length - half_length, results2))

    thread1.start()
    thread2.start()

    thread1.join()
    thread2.join()

    return results1 + results2
```

Виконання тестів відбувалося на віртуальній машині Kali Linux

Device	Summary
 Memory	8 GB
 Processors	4
 Hard Disk (SCSI)	80.1 GB
 Network Adapter	NAT
 Network Adapter 2	Custom (VMnet0)
 Network Adapter 3	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

Формування СЛР відбувалося двома потоками, кожен генерував половину з $t + c$ рівнянь

Висновок

У ході виконання лабораторної роботи, було релізовано алгоритм `index-calculus` з розпаралеленням і без. Під час реалізації зіштовхнулися з наступною проблемою: сформована СЛР з $t + c$ рівнянь не є квадратною, тому її потрібно було звести до квадратного виду, ми використовували зведення до ступінчатої форми, але не змогли реалізувати врахування модуля. Через це вирішення СЛР не завжди коректні, проте зустрічаються правильно пораховані маленькі дискретні логарифми, тому ми генеруємо СЛР, вирішуємо її та зберігаємо лише правильні відповіді поки всі маленькі дискретні логарифми не будуть пораховані. Це є найслабшим і найбільш часозатратним місцем нашої реалізації. Також слід зауважити, що різниця у часі між задачами типу 1 і типу 2 може бути зумовлена тим, що під час наших тестів у задач першого типу p було більше ніж у другого, відповідно більший розмір факторної бази і більший час знаходження маленьких дискретних логарифмів

<pre>Task Type 1: a = 8798; b = 4953; p = 8893. 2024-05-23 09:26:50 Please, found the disc arting now. Enter x value: x = 4795 2024-05-23 09:27:11 BINGO!!! You solve the Next, please, solve the type 2 task. Task Type 2: a = 165; b = 854; p = 2063. 2024-05-23 09:27:11 Please, found the disc arting now. Enter x value: x = 783</pre>	<pre>Task Type 1: a = 52620; b = 74121; p = 89209. 2024-05-23 09:30:59 Please, found the disc arting now. Enter x value: x = 20430 2024-05-23 09:31:39 BINGO!!! You solve the Next, please, solve the type 2 task. Task Type 2: a = 680; b = 22505; p = 41771. 2024-05-23 09:31:39 Please, found the disc arting now. Enter x value: x = 19579</pre>	<pre>Task Type 1: a = 83722; b = 310563; p = 561809. 2024-05-23 09:35:15 Please, found the disc arting now. Enter x value: x = 110514 2024-05-23 09:37:21 BINGO!!! You solve the Next, please, solve the type 2 task. Task Type 2: a = 83739; b = 100745; p = 113497. 2024-05-23 09:37:21 Please, found the disc arting now. Enter x value: x = 86871</pre>
---	--	---