Лабораторна робота №2
З курсу: Теоретико-числові алгоритми в криптології
Тема: Застосування алгоритму дискретного логарифмування

Анучіна Максима ФБ-11

2024

1 Мета роботи

Ознайомлення з алгоритмом дискретного логарифмування Сільвера-Поля-Хеллмана. Практична реалізація цього алгоритму. Пошук переваг, недоліків та особливостей застосування даного алгоритму дискретного логарифмування. Практична оцінка складності роботи алгоритму.

2 Постановка задачі

Реалізувати два алгоритми для розв'язання задачі дискретного логарифмування:

1. Алгоритм повного перебору.
2. Алгоритм Сільвера-Поля-Хеллмана.

Для кожного алгоритму провести вимірювання часу роботи та порівняти результати.

3 Хід роботи

Для програмної реалізації обрано мову Python. Основною проблемою, з якою я зіткнувся, було обмеження часу виконання для великих значень параметра p. Для уникнення цих обмежень було використано обробку сигналів, що дозволяє завершити програму при перевищенні часу виконання. Також при тестуванні алгоритму Сільвера-Поля-Хеллмана виникали проблеми з таблицею значень β_{q_i}, одну з проблем вдалось вирішити завдяки заміні звичайних таблиць на хеш-таблиці, це прибрало багато помилок, але все ж таки залишась невідома мені помилка, що може бути пов'язано з обмеженнями пам'яті або ресурсів. Бо при дебазі просто не вистачало розрахункових потужностей.

4 Результати дослідження

Задачі мають вигляд $x = \log_\alpha \beta$. У випадку перевищення часу виконання у 5 хвилин програма завершується з повідомленням "Time limit exceeded". Задачі першого типу мають порядки, канонічний розклад яких не містить великих простих чисел. Натомість задачі другого типу мають у канонічному розкладі порядку великі прості.

Приклад запуску програми для розв'язання задачі пошуку дискретного логарифма за випадковими значеннями параметрів і до number = кількість цифр у числі:

```
docker run -it --rm discrete_log_solver --test [number] [number]
```

При виконанні алгоритму Сільвера-Поля-Хеллмана виникали проблеми з таблицею значень β_{q_i}. При деяких значеннях β_{q_i} програма не знаходила відповідних значень у таблиці, що викликало помилку. Це може бути пов'язано з недостатньою пам'яттю або іншими обмеженнями ресурсів. Також виникали проблеми з обчислювальною складністю при великих значеннях параметра p, що призводило до перевищення часу виконання.

5 Оцінка максимального порядку

Максимальний порядок параметра p, при якому процес побудови задачі і її розв'язання відбувався за відведений час, склав $p = 100000037$ для

α	β	p	Час (повний перебір) [с]	Час (С-П-Х) [с]	Результат
2	2	3	0.00002	0.00006	1
5	4	11	0.00002	0.00008	3
3	7	13	0.00002	-	None
74	39	101	0.00007	0.00006	55
44	32	103	0.00007	0.00007	98
327	885	1009	0.00088	0.00011	None
521	261	1013	0.00087	0.00006	None
8636	5322	10007	0.00535	0.00449	5968
4669	1470	10009	0.00168	0.00020	1946
21531	95502	100003	0.00826	0.00287	7874
9280	15399	100019	0.02747	0.00153	26159
688979	830890	1000003	0.23991	0.21984	182560
200489	366465	1000033	1.43864	0.00014	None
4229237	6325732	10000019	2.62054	0.00212	1788724
3512346	3514593	10000079	0.90222	0.02313	647801
66112151	65563534	100000007	0.03023	0.00287	24175
51033572	45973358	100000037	1.73027	0.00014	1088180

Таблица 1: Результати вимірювання часу роботи алгоритмів

алгоритму повного перебору та значно менші значення для алгоритму Сільвера-Поля-Хеллмана.

6 Висновки

Метою лабораторної роботи було ознайомлення з алгоритмом дискретного логарифмування Сільвера-Поля-Хеллмана. Було реалізовано два алгоритми для розв'язання задачі дискретного логарифмування та проведено порівняльний аналіз їх продуктивності. Алгоритм повного перебору показав стабільну роботу для всіх значень параметра p, тоді як алгоритм Сільвера-Поля-Хеллмана зіткнувся з проблемами при великих значеннях p, що може бути пов'язано з обмеженнями пам'яті або ресурсів.

Вихідний код реалізованої програми розміщено на платформі GitHub за посиланням (https://github.com/deathmaks/NTA2). Docker-контейнер з реалізованою програмою доступний за посиланням

(https://hub.docker.com/r/anmatos/discrete-log-solver).(P.S. потрібно замінити - на нижній дефіс)

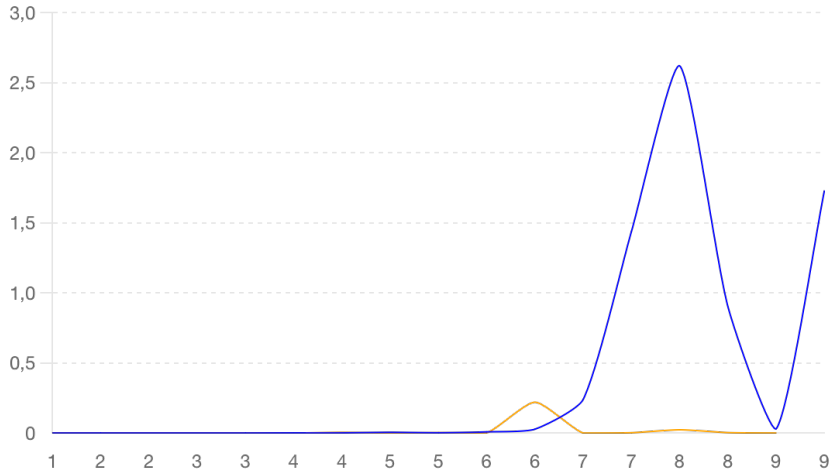

Рис. 1: Залежність часу роботи алгоритмів від параметра p

7 Оцінка максимального порядку

Максимальний порядок параметра p, при якому процес побудови задачі і її розв'язання відбувався за відведений час, склав $p = 1000000007$.