НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАКУОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт за темою:
«Криптоаналіз асиметричних криптосистем на прикладі атак на криптосистему RSA»

Виконав студент
групи ФІ-32мн
Кріпака Ілля

Київ — 2024

1 Мета практикуму

Ознайомлення з підходами побудови атак на асиметричні криптосистеми на прикладі атак на криптосистему RSA, а саме атаки на основі китайської теореми про лишки, що є успішною при використанні однакового малого значення відкритої експоненти для багатьох користувачів, та атаки «зустріч посередині», яка можлива у випадку, якщо шифротекст є невеликим числом, що є добутком двох чисел.

Практично ознайомитися із принципами статистичних методів розрізнення змістовного тексту від випадкової послідовності, порівняти їх.

1.1 Постановка задачі та варіант

У даній роботі виконував варіант №4 як і звичайний так і простий длля атаки малої експоненти, а для атаки посередині використовую простий варіант та простіший так як у бібліотеці погано працює піднесення до степеня. Усі файли, що були використані для обчислень наведені на гіт репозиторії.

Треба виконати	**Зроблено**
Провести атаки та навести результати включно із часом їх виконання	✓

2 Хід роботи/Опис труднощів

У ході роботи над даною лабораторною роботою було дуже просто реалізовано атаку малої експоненти, так як код для вирішення ситеми рівнянь уже був готовий і реалізований у попередніх лабах із асиметричної криптографії. Якщо говорити щодо атаки «зустріч посередині», то чомусь думав, що код не працює, а це лише довго обчислювалося піднесення до степеня. Якщо не враховувати свої власні непопрозуміння, то проблем особливих не було.

3 Результати дослідження

У ході роботи було успішно на практиці проведено атаку на основі Китайської теореми про лишки та атаку «зустріч посередині».

4 Результат проведення атаки на основі Китайської теореми про лишки

Атака була проведено успішно, адже значення ШТ та m^e співпали.

Рис. 1: Атака на легкий варіант.

В результаті проведеднння атаки отримав такі часові результати:

- для легкого варіанту **time.spent** = 0.001804 секунди;
- для звичайного варіанту **time.spent** = 0.0514 секунди.

is_hard: 1, [Hastard broadcast attack] m: 01FFFFFFFFFFFFFFFF001E2FDC8651E810351428DB3E3EFAFFAA9CD03CDA7E6058F69615196E459DE05A102B634CBC92223FBB8FD0EE35029CBCCAFFA61AE9772345322D9B3513F7625F4193DC1711063E24F66739AA1A65FC34929813289996328040002DE91F7B4454A8A0F7449C35BC5B6EB8594F0D4BB211934370790F5, time_spent: 12 milliseconds, check: Ok(true)

Рис. 2: Атака на звичайний варіант.

5 Результат проведення атаки «зустріч посередині»

Атака була проведено успішно, адже значення ШТ та m^e співпали.

```
T: "37d", S: "321"
is hard: 0, [Meet in the middle] m: "0AEA1D", time_spent: 1445 milliseconds, check: Ok(true)
```

Рис. 3: Атака на легкий варіант разом із повідомленням m та перевіркою на правильність.

```
T: "2bb", S: "24f"
is hard: 1, [Meet in the middle] m: "064DB5", time_spent: 510 milliseconds, check: Ok(true)
```

Рис. 4: Атака на найлегший варіант разом із повідомленням m та перевіркою на правильність.

В результаті проведеднння атаки отримав такі часові результати:

- для найлегшого варіанту **time.spent** = 0.51 секунд;
- для легкого варіанту **time.spent** = 1.445 секунд;
- для звичайного варіанту **time.spent** =? не зміг дочекатися.

5.1 Маленьке порівняння швидкодії із повним перебором

На жаль, не проводилося, так як бачу скільки програма виконувала звичайний варіант по часу, не думаю, що саме моя програма виконає перебір швидше, буде тільки довше.

6 Висновки

В даному практикумі за допомогою програмної реалізації на практиці ознайомилися із підходами побудови атак на асиметричні криптосистеми на прикладі атак на криптосистему RSA, а саме атаки на основі китайської теореми про лишки та атаки «зустріч посередині». Перша атака вийшла добре, але друга за допомоги неоптимізованої реалізації працює дуже довго. Щоб покащити алгортими досить будде використати інший крейт із ефективнішою операцією піднесення до степеня.