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

Лабораторна робота 3

Виконали студенти
групи ФІ-32мн
Панасюк Єгор Сергійович
Костюк Кирило Миколайович

Перевірила:
Ядуха Д.В.

Київ — 2024

1 КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

Мета роботи: Ознайомлення з підходами побудови атак на асиметричні криптосистеми на прикладі атак накриптосистему 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 «зу- стріч посередині», яка можлива у випадку, якщо шифротекст є невеликим числом, що є добутком двох чисел.

Постановка задачі: для заданого варіантом моделі шифру, реалізувати атаку з малою експонентою на основі китайської теореми про лишки та Атаку «зустріч посередині».

Варіант: 5.

Хід роботи:

1 Реалізувати атаку з малою експонентою на основі китайської теореми про лишки.

2 Реалізувати атаку «зустріч посередині» та порівняти її швидкодію з повним перебором можливих відкритих текстів.

3 Оформити звіт до комп'ютерного практикуму.

1.1 Атака з малою експонентою

Для проведення цієї атаки було вибрано варіант на 3 системи рівнянь для наших значень(256 біт)

Отриманий результат:

M=1fffffffffffff003eeb08d037a852d10f4367210ada8553ed6275bf14

Час роботи 0.001sec

1.2 Атака «зустріч посередині»

Для проведення цієї атаки було вибрано варіант на 2048 біт.

Отриманий результат:

M=b1d53

Час роботи 1.54sec

Якщо провести перевірку і піднести $M^e mod N = b1d53^{65537} mod N$ і справді отримаємо C.

Будемо вважати за одиницю виміру складності в нашому випадку - обрахування функції RSA.

При повному переборі за наших умов буде 2^20 таких операцій.

У випадку атаки ж всього $2 * 2^{10}$, що у 9 разів швидше.

ВИСНОВКИ

У роботі було розглянуто атаку з малою експонентою на основі китайської теореми про лишки та Атаку «зустріч посередині». Вони були реалізовані. Також було проведено порівняльний аналіз повного перебору та атаки «зустріч посередині», як висновок атака виявилась приблизно в 9 разів швидша.