

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

Звіт з виконання кваліфікаційного дослідження

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

З КУРСУ

МЕТОДИ КРИПТОАНАЛІЗУ 1

Виконала студентка
групи ФІ-32мн
Міснік Аліна Олексіївна

Викладач:
Ядуха Д.В.

Київ — 2024

ВСТУП

Метою роботи є 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.

Задача полягає у реалізації атаки з малою експонентою на основі китайської теореми про лишки, а також атаки «зустріч посередині».

Будемо використовувати дані для варіанта №10.

1 ХІД РОБОТИ

Наведемо результати проведених атак.

1.1 Атака з малою експонентою на основі китайської теореми про лишки

За допомогою китайської теореми про лишки було вирішено систему з трьох конгруенцій, після чого з отриманого результату шляхом взяття кореня третього степеня було отримано вихідне повідомлення. Для даних довжини 256 бітів атака зайняла 0.5181310007174034 мілісекунд.

Отримане повідомлення: $M = 3.5336941295567357e + 72$

1.2 Атака «зустріч посередині»

За алгоритмом, наведеним у теоритичних відомостях до практикуму, було реалізовано атаку «зустріч посередині» для даних довжини 2048 бітів.

Час виконання атаки склав 0.5601907769996615 секунд.

Отримали відкритий текст: $M = baf93$.

1.3 Опис труднощів

При першій спробі проведення атак було неправильно ініціалізовано масив для множини X в атаці «зустріч посередині». Через це в масив неможливо було передати великі значення чисел і атака не працювала. Було декілька спроб використання бібліотек для обчислення довгої арифметики поки стало зрозуміло, що проблема не в обчисленнях, а в ініціалізації. Після виправлення масива все запрацювало і труднощів більше не виникало.

ВИСНОВКИ

У роботі було програмно реалізовано 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.

Порівнюючи час виконання атак бачимо, що атака з малою експонентою на основі китайської теореми про лишки відбувається в 1000 разів швидше атаки «зустріч посередині», але обидві атаки знаходять правильний відкритий текст.