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 п'яти конгруенцій, після чого з отриманого результата шляхом взяття кореня п'ятого степеня було отримано вихідне повідомлення. Для даних довжини 1024 бітів атака зайняла 3.0921249999664724 мілісекунд.

Отримане повідомлення:
$M = 0x1ffffffffffffffffff006c319af38cdd6cb17f2213133f9fd0bbefdd78f7bb1fda81221668e6be27d8130fafd41238587f4e5201fd18534847a0480450f4107b98dd67a9103265649dde3752d6de9c0fc9d879a32c7cc4b80a7ba770499032b1d6487906b9b27d9da5b262922d36023d9266c1a028cf655fa91e6df4b5204e$

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 вико- ристанні 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.