

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ
Кафедра математичних методів захисту інформації

Комп'ютерний практикум №3
з курсу
Методи криптоаналізу 1

Підготували:
студенти 5 курсу
групи ФІ-22мн
Ковальчук О.М.
Коломієць А.Ю.

КРИПТОАНАЛІЗ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ НА ПРИКЛАДІ АТАК НА КРИПТОСИСТЕМУ RSA

Мета лабораторної роботи

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.

Постановка задачі

Здійснити криптоаналіз криптосистеми RSA. Потрібно здійснити комп'ютерну реалізацію атак поданих нижче:

- 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.

Додаткове завдання №1: Самостійно реалізувати алгоритм обчислення кореня m — степеня для дійсних (цілих) чисел, що використовується в атаці з використанням китайської теореми про лишки.

Додаткове завдання №2: Реалізувати атаку типу «зустріч посередині» для значення $l = 56$ (потребує значної оптимізації та, можливо, застосування додаткових обчислювальних ресурсів).

Варіанти завдання

Вхідні дані для виконання комп'ютерного практикуму представлені у вигляді *.txt* файлів:

1) з каталогу *SE_RSA_size_e*, де визначаються значення C_i , n_i при відкритій експоненті e для атаки на основі китайської теореми про лишки:

/vars_2022/SE_vars/test_SE_RSA_256_3_for_dummy_dummies/11.txt

/vars_2022/SE_vars/SE_RSA_1024_5_hard/11.txt

2) з каталогу *MitM_RSA_size_l.txt*, де задані значення C та n для атаки «зустріч посередині» при параметрі l :

/vars_2022/MitM_vars/test_MitM_RSA_512_20_for_dummy_dummies/11.txt

/vars_2022/MitM_vars/MitM_RSA_2048_20_regular/11.txt

При реалізації криптосистеми RSA для випадку малих експонент (для подальшої побудови атаки з використанням китайської теореми про лишки) використовувався паддинг для цифрового підпису RSA, що описаний у специфікації RFC 8017. При реалізації криптосистеми RSA для подальшої побудови атаки «зустріч посередині» використовувався параметр $e = 65537$.

Хід роботи

Атака з малою експонентою на основі китайської теореми про лишки

Результат атаки на `./vars_2022/SE_vars/test_SE_RSA_256_3_for_dummy_dummies/11.txt` виявився відкритий текст:

'0x1fffffffffffffffff00633b0b2351cfcaa22b6539734270284c1d497c7891'

Час виконання атаки: 10.2s

Результатом атаки на `./vars_2022/SE_vars/SE_RSA_1024_5_hard/11.txt` виявився відкритий текст:

'0x1fffffffffffffffff0061d1f637a844983fe9225ee597bc228c4f52a9eb482c86cc
fc59e1d00b16d177320f95ba69e780760e4a91bfc57b807e18e2469c225e975e04a932
ebb504137923aae00a7e36d81d54370e9aeb1edafe4b89d1f48d6d02572429a65df972
b8754452b2319d0939bec01c11311d5c785a4951d5abc'

Час виконання атаки: 2m 33.1s

Атака «зустріч посередині»

Результатом атаки на `./vars_2022/MitM_vars/test_MitM_RSA_512_20_for_dummy_dummies/11.txt` виявився відкритий текст:

620535

Час роботи атаки: 1.1s

У випадку застосування грубої сили час складає: 19.5s

Результатом атаки на `./vars_2022/MitM_vars/MitM_RSA_2048_20_regular/11.txt` виявився відкритий текст:

967415

Час роботи атаки: 6.5s

У випадку застосування грубої сили час складає: 3m 1.3s

Опис труднощів, що виникали при виконанні комп'ютерного практикуму, та шляхи їх розв'язання

У лабораторній роботі були труднощі в розумінні алгоритму знаходження відкритих текстів у атаці «зустріч посередині», а саме значень T та S . Значення T шукається по першій координаті кожної пари в множині всіх пар виду:

$$X = \left\{ (1,1), (2, 2^e \bmod n), (3, 3^e \bmod n), \dots, \left(2^{l/2}, (2^{l/2})^e \bmod n \right) \right\},$$

тобто кожна з пар множини має вигляд $(T, T^e \bmod n)$, $T = \overline{1, 2^{l/2}}$. Якщо пару за якої виконується рівність $C_S = (T^e \bmod n)$ знайдена, то лишається виписати першу координату даного кортежу $(T, T^e \bmod n)$, $T = \overline{1, 2^{l/2}}$. Для повідомлення S необхідно розглядати значення C_S за якого виконується:

$$C_S = C \cdot S^{-e} \bmod n, S = \overline{1, 2^{l/2}},$$

і при цьому ми звертаємо знову ж таки свою увагу на множину X , та вибираємо необхідну першу координату певної пари.

Додатково можна зауважити, що в методичних рекомендаціях знайдено помилку $M_S = (T^e \bmod n)$, котра викликала плутанину в розумінні матеріалу, але насправді там має бути запис виду $C_S = (T^e \bmod n)$.

Висновок

Ознайомилися 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.