НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

МЕТОДИ КРИПТОАНАЛІЗУ 1

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз асиметричних криптосистем на прикладі атак на криптосистему RSA

Варіант 18

Виконав:
Бєш Радомир ФІ-42мн
Перевірив:
Ядуха Д.В.

Київ — 2025

Зміст

1 Мета

Ознайомлення з підходами побудови атак на асиметричні критпосистеми 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 по середині», яка можлива у випадку, якщо шифротекст є невеликим числом, що є добутком двох чисел.

2 Постановка задачі та варіант завдання

Номер варіанту завдань: 18

-1. Ознайомитись з порядком виконання комп'ютерного практикуму та відповідними вимогами до виконання роботи.
0. Уважно прочитати необхідні теоретичні відомості до комп'ютерного практикуму.
1. Створити новий репозиторій в системі контролю версій Git (бажано використовувати вебсервіс GitHub).
2. Реалізувати атаку з малою експонентою на основі китайської теореми про лишки.
3. Реалізувати атаку «зустріч по середині» та порівняти її швидкодію з повним перебором можливих текстів.
4. Оформити звіт комп'ютерного практикуму.

3 Хід роботи

3.1 Атака з малою експонентою на основі китайської теореми про лишки

Результати:

Шифротекст:
0x1fffffffffffffb032c587867387d6f049acfca39808f1f92e5e561a8dd7f54f8cab4d9d54464869b31b73e671dbfa
c6d278d8cb5900ab7accb6386d8f092e9b78872fd1445363546e4e5848339679c14e2dd1a6f48ffcc903a44bf9a6f936d
e404acf3b75ff27591e88e6b34ff5e067541e767a34b3bf0954d3e271f81d4000cb0be43bb8e7c693add2df5e8ec5bd1
a4d92545500eab0f3b6b798ab43c6438cac30124a73692a00e431bf0d6425bce9b28f80d665be96450838bd83548036
cd45ae2b81b83af81e33a5a8df1af34825a3d31abfce809feeca5f76690b147a745969a0061522ecde457f67aad63df
e29dfe567c2f2ad21f014031d267ecdb4f827d6bbfe5f43e09ae8b1931037060a882b6e462e5890a8fd0112f7e85c43
1ed39a1459c9db36694021c33951fa98d738a4899220d0e7449f779719364e38569c40c7c742d045dc7a85a63bb7aa8
7f18ebc0eeea3ea2e0392f2f9b4ab139c1a03f92382054bfa39289791affa44d7f09db9e1a7dacdf898985d056fa70b
512f48dea319b7ecff4e3d96f7f2faba74dfaca578443530493da08bf37b84655e0a8c8315286acb4b496877580d1de
31db7001d6b83c0461325afc16c2f99e3f7bda98a495ab52a42cd778e4ec0389aa3acf625adf0872b0de9c212d9d6a1
8312ed21f021ef6b9300b97704cee922f5f8c74e015ff3608a0b3f86f739b7c7082dcb41dfa3c880402e25387ffa520
792565252aef2bd309a1fcaa4aecc822a5424afde8d9bfc5f5b26ad03bc7adafd30d5a912ea41e85fbcca98c95fb6a5
80ff79ca90b574c3db0058f11645fc151522b5a37729be8aadb750df64f9d854fc00ecf06f37bfa82751421a8151a06
810cfaeac11607d7d17f81f

Повідомлення:
E= 5:
0x1ffffffffffffff00a2781814a4e5e202304c3c645f987969ddf040f6c1fc401f1bdeeebfea3972aebed4f8ec63
85b6be90b26019c32471a888b87be25b7209c2fe5cc1f82897aa7cfdebb419ecf6128d00f3321f5a50715c6d5bf7b38
b11cb0264e2bc64d8d13865593f18a5f166d1acdb5b994d9ef6164cf321b7799f
Перевірка: True

3.2 Атака «зустріч по середині»

Результати:
M_1: 703, M_2: 937
M: 658711
Перевірка: True

3.3 Порівняння результатів

Результати:
Атака зустріч по середині: 0.0007166862487792969 секунд
Атака повного перебору: 0.06906390190124512 секунд
Атака зустріч по середині швидше у 96 разів

3.4 Опис труднощів

Робота була не складна, труднощів не виникло.

3.5 Висновки

В ході виконання роботи було програмно реалізовано атаки на асиметричні критпосистеми 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 по середині», яка можлива у випадку, якщо шифротекст є невеликим числом, що є добутком двох чисел. Реалізовано атаку на основі китайської теореми про лишки, яка успішно виконана для випадку використання однакових малих значень відкритої експоненти E для кількох користувачів. Повідомлення було відновлено, а правильність результату підтверджена. Також реалізовано атаку «зустріч посередині», яка виконана для сценарію, де шифротекст є добутком двох малих чисел M_1 та M_2. Було обчислено їх добуток M, а також підтверджено правильність результату. Атака «зустріч посередині» продемонструвала значно вищу ефективність порівняно з методом повного перебору. Атака виявилась швидшою приблизно у 96 разів. Це демонструє, що застосування спеціалізованих алгоритмів значно підвищує ефективність порівняно з базовими підходами. Для підвищення стійкості криптосистеми RSA рекомендується використовувати великі значення відкритої експоненти E, використовувати паддинг, забезпечувати унікальність параметрів для різних користувачів та уникати малих значень шифротекстів, які можуть бути вразливими до атак. Результати роботи підкреслюють важливість дотримання криптографічних стандартів при реалізації асиметричних криптосистем.