**Лабораторна робота №9**

**з дисципліни Прикладна криптологія**

**Тема лабораторної роботи**

**«Методи криптоаналізу асиметричних криптоперетворень в групі точок еліптичних кривих»**

**Мета роботи**: Розглянути методи криптоаналізу та дослідити криптостійкість асиметричних криптоперетворень в групі точок еліптичних кривих

**9.1 Криптоаналіз. Загальні положення.**

Криптоаналіз – наука про методи розшифрування зашифрованої інформації без призначеного для такого розшифрування ключа.

Термін був введений американським криптографом Вільямом Ф. Фрідманом в 1920 році. Неформально криптоаналіз називають також зломом шифру.

У більшості випадків під криптоаналізу розуміється з’ясування ключа; Криптоаналіз включає також методи виявлення уразливості криптографічних алгоритмів або протоколів.

Спочатку методи криптоаналізу ґрунтувалися на лінгвістичних закономірності природного тексту і реалізовувалися з використанням тільки олівця та паперу. З часом в криптоаналізі зростає роль чисто математичних методів, для реалізації яких використовуються спеціалізовані криптоаналітичних комп’ютери.

Спробу розкриття конкретного шифру із застосуванням методів криптоаналізу називають криптографічного атакою на цей шифр. Криптографічну атаку, в ході якої розкрити шифр вдалося, називають зломом або розкриттям.

Криптоаналіз еволюціонував разом з розвитком криптографії: нові, більш досконалі шифри приходили на зміну вже зламаним системам кодування тільки для того, щоб криптоаналітики винайшли більш витончені методи злому систем шифрування. Поняття криптографії та криптоаналізу нерозривно пов’язані один з одним: для того, щоб створити стійку до злому систему, необхідно врахувати всі можливі способи атак на неї.

**9.2 Методи криптоаналізу**

Брюс Шнайер виділяє 4 основних і 3 додаткових методів криптоаналізу, припускаючи знання криптоаналітика алгоритму шифру:

Основні методи криптоаналізу:

* Атака на основі шифротексту
* Атака на основі відкритих текстів та відповідних шифротекстів
* Атака на основі підібраного відкритого тексту (можливість вибрати текст для шифрування)
* Атака на основі адаптивно-підібраного відкритого тексту

Додаткові методи криптоаналізу:

* Атака на основі підібраного шифротексту
* Атака на основі підібраного ключа
* Бандитський криптоаналіз

**Атаки на основі шифротексту**

Припустимо, криптоаналітик має деяке число шифротекстів, отриманих в результаті використання одного і того ж алгоритму шифрування. В цьому випадку криптоаналітик може зробити тільки атаку на основі шифротексту. Метою криптографічного атаки в цьому випадку є знаходження як можна більшого числа відкритих текстів, які відповідають наявному шифротексту, або, що ще краще, знаходження використовуваного при шифруванні ключа.

Вхідні дані для подібного типу атак криптоаналітик може отримати в результаті простого перехоплення зашифрованих повідомлень. Якщо передача здійснюється за відкритим каналом, то реалізація завдання зі збору даних порівняно легка і тривіальна. Атаки на основі шифротексту є найбільш слабкими і незручними.

**Атака на основі відкритих текстів та відповідних шифротекстів**

Нехай в розпорядженні криптоаналітика є не тільки шифротексти, а й відповідні їм відкриті тексти. Тоді існують два варіанти постановки задачі:

1. знайти ключ, використаний для перетворення відкритого тексту в шифротекст;
2. створити алгоритм, здатний дешифрувати будь-яке повідомлення, закодоване за допомогою цього ключа.

Отримання відкритих текстів відіграє вирішальну роль у здійсненні цієї атаки. Відкриті тексти витягують з самих різних джерел. Так, наприклад, можна здогадатися про вміст файлу по його розширенню.

У разі злому листування можна зробити припущення, що лист має структуру типу:

«Привітання»

«Основний текст»

«Заключна форма ввічливості»

«Підпис»

Отже, атака може бути організована шляхом підбору різних видів «Привітання» (наприклад, «Здрастуйте!», «Добрий день» і т. д.) та/або «Заключною форми ввічливості» (таких як «З повагою», «Щиро Ваш »і т. п.). Легко помітити, що дана атака сильніше атаки на основі одного лише шифротексту.

**Атака на основі підібраного відкритого тексту**

Для здійснення такого типу атаки криптоаналітику необхідно мати не тільки якусь кількість відкритих текстів та отриманих на їх основі шифротекстів. Крім іншого в даному випадку криптоаналітик повинен мати можливість підібрати кілька відкритих текстів і отримати результат їх шифрування.

Завдання криптоаналітика повторюють завдання для атаки на основі відкритого тексту, тобто отримати ключ шифрування, або створити дешифрувальний алгоритм для даного ключа.

Отримати вхідні дані для такого виду атаки можна, наприклад, наступним чином: створити і відправити підроблене НЕ зашифроване повідомлення нібито від одного з користувачів, які зазвичай користуються шифруванням.

При здійсненні атаки подібного типу, криптоаналітик має можливість підбирати блоки відкритого тексту, що при певних умовах може дозволити отримати більше інформації про ключ шифрування.

**Атака на основі адаптивно-підібраного відкритого тексту**

Атака такого типу є більш зручним частковим випадком атаки на основі підібраного відкритого тексту. Зручність атаки на основі адаптивно-підібраного відкритого тексту полягає в тому, що крім можливості вибирати шифруємий текст, криптоаналітик може прийняти рішення про шифрування того чи іншого відкритого тексту на основі вже отриманих результатів операцій шифрування. Іншими словами, при здійсненні атаки на основі підібраного відкритого тексту криптоаналітик вибирає всього один великий блок відкритого тексту для подальшого шифрування, а потім на основі цих даних починає зламувати систему.

У разі організації адаптивної атаки криптоаналітик може отримувати результати шифрування будь-яких блоків відкритого тексту. Наявність зворотного зв’язку дає атаці на основі адаптивно-підібраного шифротексту перевагу перед усіма перерахованими вище типами атак.

**9.3 Стійкість асиметричних криптосистем, що базуються на криптоперетвореннях в групі точок еліптичних кривих**

**Методи Полларда**

Розглядаючи метод Полларда для вирішення проблеми дискретного логарифмування розв’яжемо наступну задачу.

*Задача* 1*.* Нехай точка  належить ЕК

,

причому  і , тобто

.

Відкритий ключ . Порядок точки , порядок *ЕК*, де -кофактор. Необхідно знайти відкритий ключ  із порівняння



У нашому випадку

.

*Розв'язання задачі.* Використовуючи співвідношення, отримаємо



Результати розв'язку задачі наведено в таблиці 1.

Таблиця 1 – Результати розв’язку задачі 1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | 1 | 0 |  |
|  | 2 | 0 |  |
|  | 3 | 0 |  |
|  | 4 | 1 |  |



Виберемо як  тоді  належить , тому





.

Розв'язуємо це рівняння, використовуючи алгоритм Евкліда



Отже, . Таким чином, .



У результаті маємо, що



Таким чином .

Другий крок: . Знаходимо .



Мультиплікативно зворотний елемент числу 2 у полі  знаходимо з рівняння ; дійсно



Таким чином,



Далі знаходимо .







Таким чином, у таблиці ми знайшли, що



Знаходимо



Перевіряємо



Таким чином



Цей алгоритм при великих значеннях  стає менш ефективним. Як показали дослідження, алгоритм можна поліпшити. Для цього точки еліптичної кривої розбивають на три множини та обчислюють функцію  рекурентно за правилом

,

де  – випадкові цілі числа з інтервалу .

Під час використання формул даного виду можна зменшити складність криптоаналізу. Крім того це дозволяє ефективно розпаралелити процес знаходження коефіцієнтів  та , для яких виконується вимога ,  як мінімум на  процесів.

**9.4 Порядок виконання лабораторної роботи**

1. Ознайомитись з теоретичним матеріалом щодо дискретного логарифмування в групі точок еліптичних кривих.
2. Відкрити програму Pollard.ехе.
3. Відповідно до таблиці 2 вибрати точку на еліптичній кривій згідно з номером робочої групи та занести обрані дані у програму.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Модулі | | | | | | | |
| 15 біт | | 20 біт | | 25 біт | | 27 біт | |
| p = 26497  n = 13163  G=(17644,6553) | | p = 959941  n = 480349  G=(676058,399379) | | p = 29024113  n = 14514667  G=(17177079,17338199) | | p = 106920299  n = 106913789  G=(12952536,38456565) | |
| 1 | (8051,4583) | (2406, 24469) | (431185,637141) | (880626,157069) | (1103732,62350) | (2504318,22818733) | (23039292, 8524847) | (106855147,21455383) |
| 2 | (4685,10476) | (14429, 7741) | (584672,229521) | (499502,319672) | (1715970,4155183) | (2687281,24279490) | (3682232, 49392124) | (78593, 75502996) |
| 3 | (21003,21393) | (15591, 13864) | (490391,583796) | (315266,741016) | (1644990,1334471) | (2265573,20757244) | (32322185, 26509861) | (18314723, 65964620) |
| 4 | (15171, 402) | (4244, 17244) | (444566,323956) | (850827,609336) | (2555549,23888867) | (1748610,13778552) | (85833659, 63198117) | (60511798, 45341126) |
| 5 | (2406, 24469) | (8064, 21847) | (499502,319672) | (584672,229521) | (1346518,12151101) | (1715970,4155183) | (106855147,21455383) | (79010240, 57009114) |
| 6 | (23568, 313) | (15171, 402) | (850827, 609336) | (431185,637141) | (1748610,13778552) | (1103732,62350) | (78593, 75502996) | (32322185, 26509861) |
| 7 | (8064, 21847) | (8051,4583) | (802154, 216358) | (444566,323956) | (2265573,20757244) | (1644990,1334471) | (76692622, 93840895) | (3682232, 49392124) |
| 8 | (15591, 13864) | (21003,21393) | (356441, 849847) | (490391,583796) | (2687281,24279490) | (1346518,12151101) | (18314723, 65964620) | (23039292, 8524847) |
| 9 | (14429, 7741) | (23568, 313) | (315266, 741016) | (802154,216358) | (5668030, 20322722) | (2555549,23888867) | (79010240, 57009114) | (85833659, 63198117) |
| 10 | (4244, 17244) | (4685,10476) | (880626, 157069) | (356441,849847) | (2504318,22818733) | (5668030, 20322722) | (60511798, 45341126) | (76692622, 93840895) |

Таблиця 2 – Точки еліптичної кривої для різних модулів

1. Програмно отримати d та час дискретного логарифмування для заданих даних. Отриманий час занести до таблиці.

Таблиця 3 – Результати роботи програми

|  |  |  |
| --- | --- | --- |
| Розмір модуля | Отриманий час, мс | |
| 15 біт |  |  |
| 20 біт |  |  |
| 25 біт |  |  |
| 27 біт |  |  |

1. Повторити для різних модулів, дані занести до таблиці та побудувати графіки. Зробити висновки.

**9.5 Контрольні запитання та завдання**

1. Що називається криптографічною атакою на шифр?
2. На чому ґрунтується метод частотного аналізу?
3. Як застосовується метод Казіскі?
4. Виділіть 4 основних методів криптоаналізу?
5. На чому базується атака на основі відкритого шифротексту?
6. На чому базується атака на основі відкритих текстів та відповідних шифротекстів?
7. На чому базується атака на основі підібраного відкритого тексту?
8. Що вивчає диференційний криптоаналіз?
9. За який рахунок може бути підвищена стійкість до диференційного криптоаналізу?
10. Принцип роботи лінійного криптоаналізу?
11. Як захистити блоковий шифр від лінійного криптоаналізу?
12. Сутність методу квадратичного решета?
13. Як розраховується база квадратичного решета?
14. Як рекомендується обирати значення числа Z?
15. Викладіть сутність двійкового решета? В чому сутність алгоритму Евкліда та які умови його застосування?
16. Скільки розкладів таблиці квадратичного решета мають бути позитивними?
17. Яким чином стійкість криптоперетворень залежить від методу криптоаналізу?
18. Які вимоги ставляться до простих чисел, щоб складність криптоаналізу була найбільшою?
19. Порівняйте складність основних методів факторизації складених чисел.
20. Сутність ρ-метода Поларда?
21. Чому метод Поларда називають ρ-методом?
22. Що таке "факторизація модуля"?
23. Які вимоги до модуля N?
24. В чому полягає криптоаналіз дискретних логарифмів методом ρ-Полларда?
25. Як обирають коефіцієнти с при розв’язку дискретного логарифмічного порівняння?
26. Які обмеження притаманні методу ρ-Поларда при факторизації та розв’язку дискретних логарифмічних рівнянь?
27. Поясніть суть алгоритму ρ-Полларда.
28. Оцініть складність розв’язку задачі дискретного логарифмічного рівняння з використанням алгоритму ρ-Полларда.