УДК 519.1:004.056.55
Пожуєва І.С.[1], Левченко А.М.[2]
[1] канд. техн. наук, доц. ЗНТУ
[2] студ. гр. КНТ-528 ЗНТУ

АНАЛІЗ МАТЕМАТИЧНИХ МЕТОДІВ У КРИПТОГРАФІЇ

Задача дискретного логарифмування є однією з основних задач, на яких базуються асиметричні алгоритми шифрування. Головним досягненням

асиметричного шифрування є те, що воно дозволяє людям, що не мають наперед наявної домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналу цілком відпала. Також на асиметричних алгоритмах шифрування базується електронний цифровий підпис, що дозволяє підтвердити авторство електронного документа та має високу надійність через велику складність підробки.

В даній роботі нами розглядається задача дискретного логарифмування в кільці класів рівності за модулем простого числа. Нехай маємо рівняння:

$$3^x \equiv 13(\mathrm{mod}17). \qquad (1)$$

Будемо вирішувати задачу методом перебору. Випишемо таблицу всіх степенів числа 3. Кожен раз ми обчислюємо залишок від ділення на 17.

$$3^1 \equiv 3 \quad 3^2 \equiv 9 \quad 3^3 \equiv 10 \quad 3^4 \equiv 13 \quad 3^5 \equiv 5 \quad 3^6 \equiv 15 \quad 3^7 \equiv 11 \quad 3^8 \equiv 16$$

$$3^9 \equiv 14 \quad 3^{10} \equiv 8 \quad 3^{11} \equiv 7 \quad 3^{12} \equiv 4 \quad 3^{13} \equiv 12 \quad 3^{14} \equiv 2 \quad 3^{15} \equiv 6 \quad 3^{16} \equiv 1. \qquad (2)$$

Тепер легко побачити, що розв'язком розглянутого рівняння є x=4, оскільки $3^4 \equiv 13$. На практиці модуль як правило є досить великим числом, і метод перебору є занадто повільним, тому виникає потреба в більш швидких алгоритмах. Розглянемо алгоритми розв'язання у кільці лишків за простим модулем, як приклад, візьмемо рівняння:

$$a^x \equiv b(\mathrm{mod}\, p), \qquad (3)$$

де p — просте, b не ділиться на p.

Якщо a є твірним елементом групи Z/pZ, то рівняння (3) має розв'язок за будь-яких b. Такі числа a ще відомі як первісні корені, і їх кількість дорівнює φ(p)=p-1, де φ — функція Ейлера.

Розв'язок рівняння (3) можливо знайти за формулою

$$x \equiv \sum_{i=1}^{p-2}\left(1 - a^i\right)^{-1} b^i \ \ (mod\ p) \quad . \qquad (4)$$

Проте, складність обчислення за цією формулою гірше за складність перебору.

Також існує безліч інших алгоритмів для вирішення задачі дискретного логарифмування у полі лишків, але поліноміального алгоритму для розв'язання цієї задачі поки не існує. Інші алгоритми розв'язання заведено розділяти на експоненціальні й субекспоненціальні. Наприклад, алгоритми Шенкса, Поліга-Геллмана та ρ-метод Поларда мають експоненціальну

складність, а алгоритми Адлемана і COS мають субекспоненціальну складність.

Як висновок, необхідно зазначити, що криптостійкість криптосистем, що базуються на дискретному логарифмуванні, ґрунтується на імовірно високій обчислювальній складності звернення показникової функції. Хоча сама показникова функція обчислюється досить ефективно, навіть найсучасніші алгоритми обчислення дискретного логарифма мають дуже високу складність, яка порівнянна зі складністю найшвидших алгоритмів розкладання чисел на множники.

Інша можливість ефективного вирішення задачі обчислення дискретного логарифма пов'язана з квантовими обчисленнями. Теоретично доведено, що за допомогою алгоритму Шора дискретний логарифм можна обчислити за поліноміальний час. У будь-якому випадку, якщо поліноміальний алгоритм обчислення дискретного логарифма буде реалізований, це буде означати практичну непридатність криптосистем на його основі для довготривалого захисту даних.