НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК: 025.042

Рассоха І.В., к.ф.-м. н.,доцент,
О.С. Величко, студент гр.101-ТН,
А.Р. Золотайко, студентка гр. 101-ТН.
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ВИКОРИСТАННЯ ТЕОРІЇ ЧИСЕЛ В СУЧАСНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Питання захисту інформації було важливим для людства ще з давніх часів. У Давньому Римі для шифрування повідомлень використовували шифр Цезаря. У XX столітті з розвитком обчислювальних машин з'являється Енігма.

Одночасно розвивається й теорія чисел. Її основи та нові здобутки широко використовуються в криптографії, зокрема в хешуванні, для перевірки цілісності файлів, створення цифрових підписів, збереження паролів, індексації вмісту в базах даних, створення унікальних кодів для інших алгоритмів (наприклад для HMAC) тощо. [1]

Суть хешування у тому, що воно одностороннє, що унеможливлює отримання початкових даних з хеш-суми (рядка символів фіксованої довжини, отриманого з хеш-функції).

В криптографічних алгоритмах хешування найчастіше використовують побітові операції, але елементи теорії чисел відіграють не менш важливу роль в отриманні хеш-функції, яка буде стійкою до колізій (тобто одна хеш-сума повинна відповідати лише одному повідомленню). Саме через це в деяких відомих та широко вживаних хеш-функціях, таких як MD5 або SHA1, були знайдені вразливості, якими можуть скористатися зловмисники. [2]

Для обчислення хеш-суми крім бітових операцій також можуть застосовувати ділення по модулю, кратність чисел, округлення, переведення з однієї системи числення в іншу. Для створення констант, що беруть участь у хешуванні, зазвичай проводять операції над ірраціональними числами: в алгоритмі Blake-256 беруть перші цифри числа пі, в SHA-256 – квадратні та кубічні корені перших 8 та 64 простих чисел відповідно.

Теорія чисел відіграє вирішальну роль й у сучасних методах шифрування, таких як RSA (Rivest-Shamir-Adleman). З ним пов'язано кілька ключових понять.

Одним із головних аспектів RSA є використання складності розкладання великих простих чисел. Шифрування та дешифрування використовують ключі, що складаються з великих простих чисел. Теорія чисел надає методи та алгоритми для ефективного знаходження великих простих чисел, які необхідні для ефективного застосування RSA.

RSA використовує властивість мультиплікативності та властивість зворотного модуля для шифрування та дешифрування повідомлень. Теорія чисел забезпечує основу для розв'язання задачі обчислення оберненого залишку за модулем, що важливо для ефективної реалізації RSA [3].

Багато інших криптографічних алгоритмів також покладаються на теорію чисел, наприклад алгоритми Діффі-Хеллмана та Ель-Гамала. Ці алгоритми використовуються для обміну ключами та створення цифрових підписів. Теорія чисел забезпечує математичну основу для створення та аналізу цих алгоритмів.

Методи криптографії та шифрування необхідні для захисту конфіденційної інформації та забезпечення безпеки зв'язку в різних сферах сучасного життя. Важливі сфери застосування включають державну та оборонну інформаційну безпеку, фінансову безпеку для банків і фінансових установ, безпеку корпоративної інформації, безпеку мережі, безпеку мобільних пристроїв, безпеку Інтернету речей (IoT) і безпеку електронної пошти. Ці сфери демонструють важливість криптографії для збереження конфіденційності та інформаційної безпеки в сучасному світі при цьому теоретичним підґрунтям, при цьому широко залучаються математичні методи, зокрема, теорія подільності та модульна алгебра. Очевидно, що використання математичних методів і надалі буде надавати нові перспективи для розвитку та вдосконалення методів шифрування.

Література

1. *Wade Trappe .Introduction to Cryptography with Coding Theory Lawrence C. Washington, Prentice Hall, 2002 - 490 p.*

2. Марк Дж. Несбітт. The Mathematics of Public-Key Cryptography. Cambridge University Press, 2012, 615 p.

3. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 с.