УДК 004.056.55:519.21

***Шоломинський Ю.Р.,* здобувач,**
Маслова Н.О., к.т.н., доцент,
Балацька В.С., д-р філ.
Львівський державний університет безпеки життєдіяльності

КРИПТОГРАФІЧНІ АСПЕКТИ ГЕНЕРАЦІЇ БЕЗПЕЧНИХ ПРОСТИХ ЧИСЕЛ

Безпечні прості числа (safe primes) – це спеціальний клас простих чисел, що забезпечує максимальну криптографічну стійкість групових протоколів. Їх використання зменшує ризики атак на малі підгрупи й гарантує, що порядок групи має великий простий дільник, що є критично важливим для безпечного обміну ключами та цифрових підписів. Тож безпечне просте число – це просте число p, для якого виконується умова: $p = 2q+1$, де q також є простим числом [1,2].

Наприклад: $q = 11$ – просте; тоді $p = 2\times11 + 1 = 23$ – також просте, отже, $p=23$ – безпечне просте.

У криптографічних протоколах, таких як Diffie–Hellman або DSA, ми працюємо у мультиплікативній групі за модулем простого числа p:

$\mathbb{Z}^*_p = \{1,2,3,\ldots,p-1\}$.

Порядок цієї групи дорівнює $p-1$. Якщо $p=2q+1$, то:

$|\mathbb{Z}^*_p|=2q$. Тобто група має великий простий підгруповий порядок q.

Це дуже важливо, бо:

- робить дискретний логарифм складнішим (менше вразливостей через малі підгрупи);
- забезпечує відсутність коротких циклів;
- дозволяє будувати надійний генератор (primitive root) для створення криптографічних ключів.

Безпечні прості числа затосовуються у сучасних крипографічних протоколах. Так, у протоколі Diffie–Hellman затосовується алгорим:

1. обирається велике безпечне просте p=2q+1.
2. вибирається генератор g, який має порядок q у групі $\mathbb{Z}^*_p$. Ключі користувачів обчислюються за формулами:

$A=g^a \bmod p$, $B=g^b \bmod p$, і спільний ключ: $K = g^{ab} \bmod p$.

Якщо p не є безпечним простим, можливі атаки через підгрупи малого порядку (small subgroup attacks).

В той же час алгорим DSA (Digital Signature Algorithm) використовує ті самі параметри p,q,g, де $p=2q+1$. Але безпечність підпису гарантується складністю обчислення дискретного логарифма в підгрупі порядку q. Прикладами безпечних простих чисел є, наприклад, для q= 5,11,23,29,83; p = 2q+1 = 11,23,47,59,167 відповідно.

У реальних криптографічних системах q і p мають сотні або тисячі біт (наприклад, $q \approx 256$ біт, $p \approx 2048$ біт), тож приклади безпечних простих чисел є демонстраційними.

Наведемо алгоритм пошуку Safe prime:

1) генеруємо випадкове непарне просте q;

2) обчислюємо p=2q+1;

3) перевіряємо, чи p також просте (наприклад, тестом Міллера–Рабіна). Якщо обидва прості – p є безпечним простим. Результати роботи алгоритму й частотний розподіл безпечних простих чисел в інтервалі [1-2000] наведено на рисунку 1.

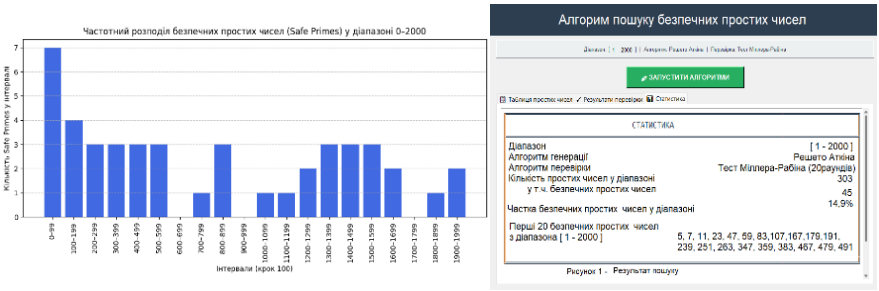

Рисунок 1 – Результати роботи алгоритму

Кількість простих чисел, наприклад, на інтервалі від 1 до 2000 дорівнює 303, тоді як Safe primes – усього сорок п’ять.

Реалізація дозволяє поєднати генерацію простих чисел та пошук безпечних простих чисел в одному проході, й цим знизити обчислювальні витрати.

Новий аспект полягає в тому, що решето Аткіна застосовано не лише для пошуку простих чисел в діапазоні, а й для фільтрації їх підмножини вигляду p=2q+1, релевантної криптографічним протоколам (Diffie–Hellman, DSA).

Список використаних джерел:

1. Gathen J., Shparlinski I. E. Generating safe primes // Journal of Mathematical Cryptology. – 2013. – Vol. 7, № 4. – P. 333–365. – DOI 10.1515/jmc-2013-5011.

2. Sieve of Atkin Revisited: Algorithmic Enhancements” // Scientific Bulletin of the „Politehnica” University of Bucharest, Series A. Applied Mathematics and Physics. – 2021. – Vol. 83, Issue 3. – P. 15-26.