Підвищення обчислювальної ефективності криптосистеми Рабіна у кільці гауссових цілих чисел

УДК 519.7

Андрій Алілуйко[1]

Західноукраїнський національний університет, [1]aliluyko82@gmail.com

Криптосистема Рабіна є високоефективною завдяки швидкості шифрування та стійкості, що базується на складності факторизації та пошуку квадратного кореня за модулем. Проте її реалізація як у кільці цілих, так і гауссових чисел ($A = a + bi,\ a,b \in Z$) має недоліки: високу часову складність дешифрування через використання КТЗ (зокрема, пошук оберненого елемента) та обмеження у виборі параметрів (зокрема, вибір цілих чисел Блюма). Тому актуальним завданням є розробка нових підходів до реалізації системи в кільці гауссових чисел для оптимізації обчислювальних витрат.

Аналогічно до цілочисельної асиметричної криптографії, можна розглядати криптосистему Рабіна, коли повідомлення M та два прості числа p та q є цілими комплексними числами. Число $N = pq$ виступає відкритим ключем, а p та q – закритим. Шифрування відкритого повідомлення M відбувається за формулою $C = M^2 \bmod N$. При дешифруванні шифр тексту C вводяться додаткові допоміжні величини μ та ν: $\mu = C \bmod p,\ \nu = C \bmod q$. Для знаходження M необхідно знайти квадратні корені x та y за модулями p та q: $x^2 \bmod p = \mu,\ y^2 \bmod q = \nu.$

У результаті утворюються чотири системи рівнянь ($i = \overline{1,4}$):

$$\begin{cases} M_i \bmod p = \pm x, \\ M_i \bmod q = \pm y. \end{cases} \quad (1)$$

Один з розв'язків (1), пошук якого здійснюється на основі КТЗ, і буде шуканим відкритим повідомленням M.

Для уникнення ресурсномістких операцій пошуку оберненого елемента за комплексним модулем при застосуванні КТЗ запропоновано вибирати ключі p та q, які утворюють досконалу або модифіковану досконалу форму [1].

Для спрощення знаходження комплексних коренів за комплексним модулем при дешифруванні розроблено алгоритм розв'язування конгруенції $x^2 \equiv c \bmod \pi$, в якій комплексний модуль має норму виду $N(\pi) = 8k + 5, k \in Z$.

1. Aliluiko A., Kasianchuk M., Dziubanovska N., Netrebiak M. Construction of Perfect Form of Residue Number System for Gaussian Integers to Asymmetric Cryptosystems, *15th International Conference on Advanced Computer Information Technologies (ACIT)*, Sibenik, Croatia, 2025, pp. 471-475.