УДК 003.26+511.17

ГЕНЕРУВАННЯ ПАР ВЗАЄМНО ПРОСТИХ ЧИСЕЛ

О. В. Дмитришин, магістр з інформаційної безпеки, аспірант
Вінницький національний технічний університет
olexanderdm@gmail.com

Для побудови сучасних симетричних блокових шифрів, які використовують операції множення за секретним змінним модулем, потрібні пари взаємно простих чисел. Відомі такі методи перевірки чисел на взаємну простоту, як алгоритм Евкліда і алгоритм ділення, які за своєю архітектурою не є швидкими. Все це зумовлює актуальність пошуку нових методів генерування пар взаємно простих чисел.

Відомим є таке твердження, що для будь-якого $a \in N$, число $(2a + 1)$ буде взаємно простим з a, тобто

$$\text{НСД}(a, 2a+1) = 1.$$

Вище згадане твердження використано для розроблення метода генерування пар взаємно простих чисел, основна ідея якого полягає в том, що генерують n-бітне псевдовипадкове число $p = \{x_0, x_1, \ldots, x_{n-1}\}$, де x_0 – найбільш значущий біт, а x_{n-1} – найменш значущий біт і $a = \{x_1, \ldots, x_{n-1}\}$. Тоді, генерування пар взаємно простих чисел a і b виконується за таким правилом:

$$a = \begin{cases} a = a + 1, \textit{якщо } x_0 = 0 \\ a = a - 1, \textit{якщо } x_0 = 1 \end{cases}, \quad b = \begin{cases} b = 2a - 2, \textit{якщо } x_0 = 0 \\ b = 2a - 1, \textit{якщо } x_0 = 1 \end{cases}.$$

Отже, для n-розрядного генератора псевдовипад-кових чисел використовуючи запропонований метод генерування пар взаємно простих чисел можна отримати 2^{n-1} таких пар.