УДК 004.9

ПІДВИЩЕННЯ ШВИДКОДІЇ АЛГОРИТМІВ ШИФРУВАННЯ

Б.Л. Шрамченко, кандидат технічних наук, с.н.с.
Київський національний університет технологій та дизайну

Ключові слова: шифрування інформації, скінчене кільце, скінчене поле, операція за модулем, розширений алгоритм Евкліда, обернений елемент до поданого.

Сучасні мехатронні системи пов'язані з автоматизованою обробкою та захистом інформації [1]. Методи захисту інформації значною мірою побудовані на використанні алгоритмів шифрування, які дозволяють захиститись від несанкціонованого доступу до інформації. Велика кількість сучасних алгоритмів шифрування використовує операцію знаходження оберненого елементу до поданого у скінченому кільці або полі. До них відносяться такі відомі алгоритми як AES, RSA, алгоритм Ель-Гамаля, алгоритм шифрування з використанням еліптичних кривих [2]. Тому представляється доцільним дослідження шляхів підвищення швидкодії операції знаходження оберненого числа.

Традиційно ця задача розв'язується за допомогою розширеного алгоритму Евкліда, що у свою чергу ґрунтується на відомому з давніх часів алгоритмі Евкліда обчислення найбільшого спільного дільника *(НСД)*.

Будемо говорити, що a є дільником b (або a ділить b, це позначають $a \mid b$), якщо існує таке c, що $a \cdot c = b$. Якщо a ділить b, і a ділить c, кажуть, що a є спільним дільником a та b. В алгоритмі Евкліда використовується операція $a \bmod b$ (a за модулем b), яка визначає таке c, що $a = p \cdot b + c$, і $0 \le c < b$. Будемо позначати найбільший спільний дільник чисел a та b як $НСД(a, b)$.

Алгоритм Евкліда складається з двох кроків.

1. Якщо $a = 0$, $НСД(a, b) = b$, кінець алгоритму.
2. Обчислити $НСД(b \bmod a, a)$.

Скористатися розглянутим алгоритмом для обчислення оберненого числа до поданого a можна, якщо знайти таке число b, що $НСД(a, b) = 1$, і представити $НСД(a, b)$ у вигляді $НСД(a, b) = u \cdot a + v \cdot b$. У випадку, коли $v \cdot b = 0$, отримуємо $u \cdot a = 1$, що означає – u є оберненим до a.

Позначимо поточні значення чисел, *НСД* для яких у алгоритмі Евкліда збігається з $НСД(a, b)$, як c і d ($НСД(c, d) = НСД(a, b)$). Числа c і d завжди можна представити у вигляді $c = u_c \cdot a + v_c \cdot b$, $d = u_d \cdot a + v_d \cdot b$. Спочатку $c = a$, $d = b$, відповідно $u_c = 1$, $v_c = 0$, $u_d = 0$, $v_d = 1$. На кожному кроці алгоритму Евкліда, якщо $c \neq 0$, c замінюється на $d \bmod c$, а d - на c. Тому $c' = d - q \cdot c$, $d' = c$, де $q = \lfloor d / c \rfloor$. (Позначення $\lfloor d / c \rfloor$ означає цілу частину числа (d / c)). Або $c' = u_d \cdot a + v_d \cdot b - q \cdot (u_c \cdot a + v_c \cdot b)$. Звідки маємо

$c' = (u_d - q \cdot u_c) \cdot a + (v_d - q \cdot v_c) \cdot b$, або $u_c' = u_d - q \cdot u_c$, і $v_c' = v_d - q \cdot v_c$.

Алгоритм, що обчислює значення *НСД*(*a, b*) та представлення *НСД*(*a, b*) = *u a* + *v b*, називається розширеним алгоритмом Евкліда. Він складається з наступних кроків.

1. Покласти $c = a, d = b, u_c = 1, v_c = 0, u_d = 0, v_d = 1$.
2. Якщо $c = 0$, $НСД(a, b) = d$, $u = u_d$, $v = v_d$, кінець алгоритму.
3. Обчислити $q = \lfloor d / c \rfloor$, $c' = d \bmod c$, $u_c' = u_d - q\, u_c$, $v_c' = v_d - q\, v_c$.
4. Покласти $d = c$, $c = c'$, $u_d = u_c$, $v_d = v_c$, $u_c = u_c'$, $v_c = v_c'$, і перейти до 2.

Наведений алгоритм при обчисленні оберненого числа до числа *a* може бути удосконалений шляхом вилучення обчислень значень v_c та v_d , оскільки останні не потрібні для обчислення u_d та u_c [3]. Крім того, оскільки для взаємно простих *a, b* на передостанній ітерації завжди *c* = 1, то цією умовою можна скористатися для закінчення алгоритму і таким чином вилучити виконання останньої ітерації. Виконання умови *c* = 1 на передостанній ітерації розширеного алгоритму Евкліда випливає з наступних міркувань. На останній ітерації, коли *a* і *b* взаємно прості, отримуємо *c* = 0, *d* = 1. Оскільки на кожній ітерації *d* отримує значення, якому дорівнювало *c* у попередній ітерації, то у передостанній ітерації у поданому випадку *c* = 1.

У загальному випадку, коли *a* належить кільцю Z_n для визначення числа *x*, оберненого до *a*, застосовують розширений алгоритм Евкліда до пари *(a, n)*, тобто *b* = *n*. При цьому обчислення зупиняють на кроці, коли *c* = *1*, і шуканий елемент дорівнює u_c.

Остаточно пропонований алгоритм обчислення для поданого числа *a*, яке більше одиниці, оберненого числа *x* відносно операції множення за модулем *b* має наступний вигляд.

1. Покласти $c = a, d = b, u_c = 1, u_d = 0$.
2. Обчислити $q = \lfloor d / c \rfloor$, $c' = d \bmod c$, $d = c$, $u_c' = u_d - q\, u_c$.
3. Покласти $c = c'$, $u_d = u_c$, $u_c = u_c'$, якщо $c > 1$, перейти до кроку 2.
4. Якщо $c = 0$, обернене число *x* не існує, кінець алгоритму.
5. $x = u_c$, кінець алгоритму.

Таким чином пропонована модифікація алгоритму обчислення оберненого числа для поданого у скінченому кільці дає змогу скоротити кількість елементарних операцій і тим самим підвищити швидкодію алгоритмів шифрування. Цей алгоритм дозволяє також обчислювати частку від ділення чисел a_1 на a_2 шляхом множення a_1 на число обернене до a_2.

Список використаних джерел

1. Егоров О.Д. Конструирование мехатронных модулей: Учебник. / О.Д. Егоров, Ю.В. Подураев. - М.: ИЦ МГТУ "СТАНКИН", 2004.- 360 с.

2. Бобало Ю.Я. Інформаційна безпека. / Ю.Я. Бобало, І.В. Горбатий, М.А. Кіселичник. – Л.: Видавництво Львівської політехніки, - 2019. – 580 с.

3. Фергюсон Н. Практическая криптография. : Пер. с англ. / Н. Фергюсон, Б. Шнайер . – М. : Издательский дом «Вильямс», - 2005. – 424 с.