КІБЕРНЕТИКА

УДК 51.681.3

С.Л. КРИВИЙ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *sl.krivoi@gmail.com*.

ЗАСТОСУВАННЯ КОМУТАТИВНИХ КІЛЕЦЬ З ОДИНИЦЕЮ ДЛЯ ПОБУДОВИ СИСТЕМИ СИМЕТРИЧНОГО ШИФРУВАННЯ

Анотація. Запропоновано метод побудови симетричної криптосистеми, що базується на властивостях скінченних асоціативно-комутативних кілець з одиницею. Наведено поліноміальні алгоритми побудови таблиць додавання та множення для цих кілець. Розглянуто приклади використання системи, а також її розширення моделлю математичного сейфа для автентифікації абонентів. Наведено умови використання функції дискретного логарифма в кільцях. Показано переваги математичного сейфа, заданого графом, в порівнянні з його заданням матрицею.

Ключові слова: асоціативно-комутативне кільце, криптосистема, математичний сейф, алгоритм.

НЕОБХІДНІ ОЗНАЧЕННЯ І ПОНЯТТЯ

У цій статті розглядається спосіб побудови симетричної системи шифрування на основі властивостей скінченних асоціативно-комутативних кілець з одиницею [1, 2]. Стаття є продовженням роботи [3].

Нехай задано деяку скінченну множину цілих чисел, наприклад $N_6 = \{0, 1, 2, 3, 4, 5\}$. Побудуємо адитивну Абелеву групу GN_6 над N_6, яка має містити 0 і 1 (як кільце з одиницею), і для її побудови достатньо коректно задати значення операції додавання з одним із ненульових елементів групи, наприклад з елементом 1 (ненульовий елемент може бути довільним) [2]. Дійсно, оскільки $a + 0 = a$ для довільного $a \in GN_6$, перший рядок таблиці додавання елементів групи повною мірою визначений (див. табл. 1), а на підставі комутативності операції додавання визначений і перший стовпчик цієї таблиці.

Нехай задано $0 + 1 = 1, 1 + 1 = 3, 1 + 3 = 5, 1 + 5 = 4, 1 + 4 = 2, 1 + 2 = 0$. Таке визначення операції додавання коректне, оскільки має місце однозначність результату (яка не гарантує коректності). Далі отримаємо результати додавання з елементом 3, оскільки $3 = 1 + 1$ і це дає змогу знайти результати операції додавання з цим елементом:

$$3 + 2 = (1 + 1) + 2 = 1 + (1 + 2) = 1 + 0 = 1,\ 3 + 3 = (1 + 1) + 3 = 1 + (1 + 3) = 1 + 5 = 4,$$

$$3 + 4 = (1 + 1) + 4 = 1 + (1 + 4) = 1 + 2 = 0,\ 3 + 5 = (1 + 1) + 5 = 1 + (1 + 5) = 1 + 4 = 2.$$

Знаходимо значення $3 + 1 = 5$ і обчислюємо результат операції додавання з елементом 5:

$$5 + 2 = (1 + 3) + 2 = 1 + (3 + 2) = 1 + 1 = 3,\ 5 + 3 = (1 + 3) + 3 = 1 + (3 + 3) = 1 + 4 = 2,$$

$$5 + 4 = (1 + 3) + 4 = 1 + (3 + 4) = 1 + 0 = 1,\ 5 + 5 = (1 + 3) + 5 = 1 + (3 + 5) = 1 + 2 = 0.$$