УДК 51.681.3

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

СИСТЕМА ОБМІНУ ІНФОРМАЦІЄЮ НА ОСНОВІ ВІДОБРАЖЕНЬ КІЛЕЦЬ

Анотація. Запропоновано криптосистему обміну інформацією між абонентами на основі сюр'єктивних відображень скінченних асоціативно-комутативних кілець з одиницею та систем лінійних конгруенцій над такими кільцями. Наведено алгоритми побудови сюр'єктивних відображень кілець, а також протокол обміну та обчислювальні особливості засобів реалізації протоколу. Система не потребує громіздких обчислень та побудови таблиць операцій кілець. Її стійкість ґрунтується на комбінаторній складності множини сюр'єктивних відображень та ізоморфізмів між скінченними кільцями порівняно невеликих порядків. Алгоритми розв'язання систем лінійних конгруенцій, які фігурують у протоколі обміну, слугують для шифрування повідомлень і мають поліноміальну складність. Роботу криптосистеми продемонстровано на прикладах.

Ключові слова: криптографія, симетрична криптосистема, скінченні кільця, ізоморфізм, система лінійних конгруенцій.

У криптографічних застосуваннях часто використовують скінченні поля і Діофантові рівняння та системи таких рівнянь [1, 2]. Це пояснюється тим, що скінченне поле має циклічну мультиплікативну групу, і в такій групі ефективним є використання функції дискретного логарифму, а алгоритми розв'язання Діофантових рівнянь у множині натуральних чисел та систем таких рівнянь мають велику часову складність [3]. Криптосистеми, які ґрунтуються на цих структурах, потребують побудови великих простих чисел, полів великих порядків, або великих обсягів пам'яті та часових затрат на підготовчі дії [4].

Основна мотивація цієї роботи полягає у створенні достатньо надійної криптосистеми, в якій фігурують об'єкти відносно невеликих розмірів, але яка має необхідний запас стійкості до зламу. Систему такого типу запропоновано в роботі [5], і ця робота є подальшим її розвитком. Основою криптосистеми є сюр'єктивні відображення скінченних кілець та їхні ізоморфізми з використанням систем лінійних конгруенцій над кільцями лишків. Надійність такої системи ґрунтується на комбінаторній складності множини відображень між кільцями, порядки яких порівняно невеликі.

Системи лінійних конгруенцій використовують для формування і шифрування повідомлення, що практично повністю унеможливлює застосування методів частотного аналізу та гамування.

НЕОБХІДНІ ОЗНАЧЕННЯ ТА ПОНЯТТЯ

Алгебру $G(A,\Omega)$ називають кільцем, якщо вона — Абелева група відносно додавання, групоїд відносно операції множення і для довільних її елементів $a,\ b,\ c \in A$

$$a(b+c) = (ab) + (ac),\ \ (a+b)c = (ac) + (bc).$$

Нульовий елемент адитивної групи кільця називають нулем кільця.

Кільце називають асоціативно-комутативним, якщо його операція множення асоціативна і комутативна, та кільцем з одиницею, коли воно має одиничний елемент відносно операції множення. Кількість елементів кільця називають по-