СИМЕТРИЧНА КРИПТОСИСТЕМА НА ОСНОВІ ВІДОБРАЖЕНЬ КІЛЕЦЬ

Кривий С.Л., Рябов К.

Анотація. Пропонуються алгоритми обміну інформацією між абонентами на основі сюр'єктивних відображень скінченних асоціативно-комутативних кілець з одиницею та систем лінійних рівнянь над такими кільцями. Наводяться алгоритми побудови скінченних кілець, побудова сюр'єктивних відображень кілець, а також протокол обміну інформацією та обчислювальні особливості засобів реалізації протоколу. Основною мотивацією розробки такої криптосистеми є те, що практично всі існуючі криптосистеми потребують обчислення або великих простих чисел, або побудови скінченних полів великих порядків. А такі обчислення та побудови потребують застосування досить складних алгоритмів. Пропонована система не потребує громіздких обчислень, не потребує побудови таблиць операцій кілець і її стійкість ґрунтується на комбінаторній складності множини сюр'єктивних відображень та ізоморфізмів між скінченними кільцями відносно невеликих порядків. Алгоритми розв'язання систем лінійних рівнянь, які фігурують в протоколі обміну інфоомацією, над такими кільцями мають поліноміальну складність. Робота криптосистеми демонструється на прикладах.

SYMMETRIC CRYPTOSYSTEM BASED ON RING IMAGES

Abstract. Algorithms for the exchange of information between subscribers on the basis of surjective mappings of finite associative-commutative rings with unit and systems of linear equations over such rings. Are given algorithms for constructing finite rings, construction surjective mappings of rings, as well as the exchange protocol information and computing features of realization of this protocol. The main motivation for the development of such a cryptosystem is the fact that almost all established cryptosystems require calculations or large prime numbers, or the construction of finite fields of large orders. These constructions also require application quite complex algorithms. The proposed system does not require complex calculations, no need to build tables of rings operations and its stability depends on the combinatorial complexity of the set surjective mappings and isomorphisms between finite rings relatively small orders. Algorithms for solving systems of linear equations, which are included in the information exchange protocols, over such rings have polinomial complexity. The operation of the cryptosystem is demonstrated by examples.

1 Вступ

В криптографічних застосуваннях часто використовуються 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 ефективне використання функції дискретного логарифму, а алгоритми розв'язання Діофантових рівнянь та систем таких рівнянь у множині натуральних чисел мають велику часову складність [3]. Криптосистеми, побудовані на таких структурах потребують побудови великих простих чисел, або полів великих порядків, або великих об'ємів пам'яті та часових затрат на підготовчі дії [4].

Мотивацією даної роботи є створення криптосистеми, яка побудована на об'єктах відносно невеликих розмірів і яка має необхідний запас стійкості до злому. Такого типу система була запропонована в роботі [5] і ця робота є подальшим її розвитком. Основою криптосистеми є сюр'єктивні відображення скінченних кілець та їх ізоморфізми з використанням систем лінійних рівнянь над кільцями лишків. Надійність такої системи ґрунтується на комбінаторній складності множини відображень між кільцями, порядки яких невеликі.

Системи лінійних рівнянь над кільцем лишків використовується для формування і шифрування повідомлення, що дає можливість практично повністю унеможливити застосування методів частотного аналізу та гамування.

2 Необхідні означення та поняття

Нехай Z_k означає скінченне кільце лишків за модулем k, тобто Z_k – це асоціативно-комутативне кільце (АК-кільце) з одиницею. Елементи $a, b \in Z_k \setminus \{0\}$ називаються протилежними, якщо $a+b \equiv 0 \pmod{k}$, і називають *дільниками нуля*, якщо $a \cdot b \equiv 0 \pmod{k}$. Оскільки кільце Z_k з одиницею, то елементи $c, d \in Z_k$ такі, що $c \cdot d \equiv 1 \pmod{k}$, називають *дільниками одиниці*. Дільники одиниці в кільці Z_k утворюють абелеву групу [6].

Нехай G_k означає скінченне АК-кільце з одиницею, ізоморфне кільцю Z_k, побудова якого виконується за заданим рядком додавання з одиницею. Цей рядок називатимемо *визначальним* і за ним на підставі законів, яким задовольняють операції додавання і множення кільця, будуються таблиці цих операцій (алгоритми побудови таблиць кільця G_k можна знайти в [5]). Цей рядок задає також ізоморфізм між кільцем Z_k і кільцем G_k, який дає можливість уникнути побудови таблиць операцій кільця G_k, тому що операції можна виконувати в кільці Z_k і за ізоморфізмом знаходити результати операцій в кільці G_k, а в кільці Z_k операції виконуються ефективніше.

В загальному випадку визначальний рядок кільця G_k $a = (1, a_1, a_2, \ldots, a_{k-2}, 0)$ задається таким відображенням $f(0) = 0+1 = 1, f(1) = 1+1 = a_1, f(a_i) = a_i+1 = = a_{i+1}, f(a_{k-2}) = a_{k-2}+1 = a_{k-1} = 0$, де $i = 0, 1, \ldots, k-1$.

Визначальний рядок кільця G_k генерується таким алгоритмом.

GEN-G(a, c, l, k)

Вхід: Порядок k і коефіцієнти виразу $f(i) = a \cdot i + c$, де $k = lm$, НСД(a, m)=НСД(a, k)=1.

Вихід: Рядок таблиці додавання з одиницею у вигляді одномірного масиву $b = (b_1, b_2, \ldots, b_k)$ довжини k.

Метод:

1) for $i = 0$ to $k-1$ do $b[i+1] := a \cdot i + c \pmod{k}$ od

2) За спільними правилами перетворити масив b і зафіксувати його значення (створення спільного визначального рядка).

3) for $i = 1$ to k do

if $(b_i = 0 \wedge i \neq k)$ then change b_i and b_k;

if $(b_i = 1 \wedge i \neq 1)$ then change b_i and b_1;

od

(* задання ізоморфізму $g(i) = b_i$, де $i = 1, 2, \ldots, k$ *)

4) за масивом $b = (b_1, b_2, \ldots, b_k)$ будуємо масив $P[1 \times k]$ (за яким в разі потреби будуються таблиці операцій кільця)

$P[0] := b_1$;

for $i = 1$ to $k - 2$ do $P[b_i] := b_{i+1}$ od

$P[b_{k-1}] := 0$.

Правильність алгоритма випливає з того, що коли НСД(a, k)=1 і i пробігає повну систему лишків, то $a \cdot i + c$ теж пробігає повну систему лишків [6].

Часова складність алгоритму GEN-G – $O(k \log^2 k)$, оскільки множення цілих чисел має складність $O(\log^2 k)$, а всіх таких множень не більше ніж k.

Зазначимо, що оператор 1) алгоритму GEN-G може згенерувати не більше ніж $(k-2)\varphi(k)$ початкових рядків, де φ – функція Ойлера. Для криптографічних застосувань такої кількості не достатньо. Тому за домовленістю між абонентами згенерований алгоритмом початковий рядок оператором 2) перетворюється однаковим чином, що визначає криптосистему як симетричну.

Приклад 1. Згенерувати визначальний рядок для $k = 6$ і $f(i) = i + 4$.

Перший цикл алгоритму (оператор 1) генерує такий початковий рядок:

1) $b_1 = 4$; $b_2 = 5$; $b_3 = 0$; $b_4 = 1$; $b_5 = 2$; $b_6 = 3$.

2) Другий оператор виконує перетворення: міняє пари сусідніх елементів місцями і виконує одну циклічну перестановку всіх елементів. Дістаємо рядок $2, 5, 4, 1, 0, 3$.

3) Другий цикл (оператор 3) розставляє на свої місця 0 і 1 та видає визначальний рядок і ізоморфізм: $g(i) = b_i, i = 1, 2, \ldots, 6$, де

$b_1 = 1$; $b_2 = 5$; $b_3 = 4$; $b_4 = 2$; $b_5 = 3$; $b_6 = 0$.

4) Третій цикл (оператор 4) генерує за масивом $b_1 = 1, b_2 = 5, b_3 = 3, b_4 = 0, b_5 = 2, b_6 = 4$ рядок $P = (1, 5, 3, 0, 2, 4)$, за яким будуються таблиці операцій кільця G_6. ♠[1]

Отже, ізоморфзм кілець G_k і Z_k знаходиться за визначальним рядком, який згенерований алгоритмом GEN-G. Дійсно, маємо таку відповідність:

1	2	3	4	...	$k-1$	k
b_1	b_2	b_3	b_4	...	b_{k-1}	0

,

де ізоморфне відображення g буде таким: $g(k) = 0, g(1) = b_1 = 1, g(i) = b_i, i = = 2, \ldots, k-1$.

3 Протокол обміну повідомленнями

Ідея побудови криптосистеми ґрунтується на такій схемі:

[1] Символи ♠ і ■ означають кінець приклада і кінець доведення відповідно.

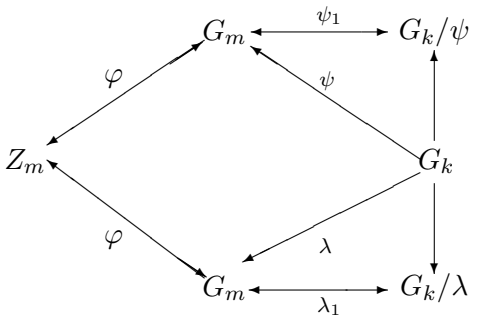

Рис. 1. Схема системи

В цій схемі відображення

– φ – ізоморфізм між кільцями Z_m і G_m,

– ψ – сюр'єкція кільця G_k на кільце G_m,

– λ – сюр'єкція кільця G_k на кільце G_m,

– ψ_1 – бієкція між фактор множиною G_k/ψ і кільцем G_m,

– λ_1 – бієкція між фактор множиною G_k/λ і кільцем G_m.

Обмін повідомленнями між Алісою і Бобом виконується за таким протоколом.

Попередньо Аліса і Боб секретним каналом обмінюються четвіркою (a, c, l, m), елементи якої є параметрами алгоритму GEN-G(a, c, l, m). За допомогою виразу $f(i) = a \cdot i + c$, де НСД(a, k)= НСД(a, m)=1, згенерували початкові рядки кілець G_k і G_m і за домовленістю однаковим способом побудували визначальні рядоки $b = (b_1 = 1,\ b_2, \ldots, b_{m-1}, b_m = 0)$ і $c = (c_1 = 1, c_2, \ldots, c_k = 0)$ кілець G_m і G_k відповідно.

Після цього Аліса і Боб виконують такі кроки.

Крок 1. а) Аліса будує систему виразів в кільці G_m:

$$l(x) = Ax = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + a_{p2}x_q + \ldots + a_{pq}x_q. \end{cases}$$

б) Перетворює $l(x)$ в кільці G_m таким чином:

$$L(x) = Bx + a = B_r(B_{r-1}(\ldots B_2(B_1(l(x) + a) + a_1) \ldots + a_{r-1}) + a_r) + a_{r+1},$$

де B_i – невироджені матриці розмірності $p \times p$, a, a_j – вектори розмірності $1 \times p$, $i = 1, 2, \ldots, r, x\ j = 1, 2, \ldots, r + 1$. Результатом такого перетворення є система

$$L(x) = Bx + a = \begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1q}x_q + a_1, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2q}x_q + a_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{p1}x_1 + b_{p2}x_q + \ldots + b_{pq}x_q + a_q. \end{cases}$$

в) Виконує зміну коефіцієнтів у $l(x)$ і $L(x)$ їхніми відповідниками з фактор-множини G_k/λ_1:

$$\bar{l}(x) = \bar{A}x = \begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1q}x_q, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2q}x_q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{p1}x_1 + b_{p2}x_q + \ldots + b_{pq}x_q. \end{cases}$$

і

$$\bar{L}(x) = \bar{B}x + b = \begin{cases} c_{11}x_1 + c_{12}x_2 + \ldots + c_{1q}x_q + b_1, \\ c_{21}x_1 + c_{22}x_2 + \ldots + c_{2q}x_q + b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{p1}x_1 + c_{p2}x_q + \ldots + c_{pq}x_q + b_q. \end{cases}$$

Аліса висилає відкритим каналом або виставляє на сайті вирази $\bar{l}(x)$ і $\bar{L}(x)$.

Крок 2. а) Боб за виразами $\bar{l}(x)$ і $\bar{L}(x)$ та відображеннями λ_1^{-1} і φ^{-1} знаходить вирази $\hat{l}(x)$ і $\hat{L}(x)$ в кільці Z_m, вибирає довільний вектор $\bar{a}$ розмірності $1 \times q$.

б) Боб хоче передати Алісі повідомлення v. Для цього він розв'язує систему $\hat{l}(x) = v$, знаходить розв'язок $\bar{x}$ і обчислює вектори $\hat{l}(\bar{a}) = d$ та $\hat{L}(\bar{x} + \bar{a}) = d_1$ у кільці Z_m.

в) Вектор v Боб зберігає в таємниці, а значення d і d_1 замінює відповідниками однієї із фактор-множини G_k/ψ або G_k/λ і висилає Алісі відкритим каналом пару векторів $(\bar{d}, \bar{d_1})$.

Крок 3. а) Аліса обчислює обернені матриці до матриць B_i в кільці G_m (а це обчислення виконується в кільці Z_m за ізоморфізмом φ).

б) Знаходить значення v, оскільки всі дані для цього в неї є.

Твердження 1. *Обмін повідомленнями за протоколом виконується коректно.*

Доведення очевидним чином випливає з властивостей лінійних операторів, бієкції λ_1 та ізоморфізму φ. Дійсно, позначимо добуток матриць $B_r B_{r-1} \ldots B_1 = D$, тоді

$$d_1 = L((\bar{x} + \bar{a}) + a_1) = D(l(\bar{x} + \bar{a}) + a_1) + b + a_{r+1} = D(l(\bar{x} + \bar{a}) + a_1) + c,$$

де $c = b + a_{r+1}$, а b – вектор значень, отриманий в результаті множення матриць $B_1, B_2, \ldots, B_r$ на вектори $a_1, a_2, \ldots, a_r$. Тоді

$$D^{-1}(D(d_1 - a_{r+1})) - D^{-1}b = D^{-1}(D(l(\bar{x} + \bar{a}) + a_1) + b) - D^{-1}b = l(\bar{x} + \bar{a}) + a_1.$$

Отже, $l(\bar{x} + \bar{a}) + a_1 - [a_1 + d] = l(\bar{x})$. ■

З рисунка 1 випливає, що в схемі системи існує принаймні три шляхи створення шифрограми:

1) $G_k/\psi \to G_m \to Z_m \to G_m$ означає, що явно фігурують вирази $l(x)$ і $L(x)$, записані у фактор-множині G_k/ψ, які за бієкціями φ і ψ_1 відтворюються у кільці Z_m, де виконуються обчислення і будується шифрограма в кільці G_m.

2) $G_k/\lambda \to G_m \to Z_m \to G_k/\psi$ означає, що явно фігурують вирази $l(x)$ і $L(x)$ записані у фактор-множині G_k/λ, за бієкціями λ_1 і φ ці вирази відтворюються у кільці Z_m, де виконуються обчислення і будується шифрограма за бієкціями φ і ψ_1 у фактор-множині G_k/ψ.

Цьому шляху відповідає вищенаведений протокол.

3) $G_m/\psi \to G_m \to Z_m \to G_k/\lambda$ означає,що явно фігурують вирази $l(x)$ і $L(x)$ записані у фактор-множині G_k/ψ, за бієкціями ψ_1 і φ ці вирази відтворюються у кільці Z_m, де виконуються обчислення і будується шифрограма у фактор-множині G_k/λ.

Приклад 2. Розглянемо підготовчі дії протоколу.

Нехай Аліса і Боб вибрали перший шлях створення шифрограми, обмінялися трійкою $(7, 5, 2, 25)$ і зафіксували такий визначальний рядок кільця G_{25} (виконали оператори 1) і 2)):

$$b = (1, 6, 8, 10, 2, 4, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 12, 14, 16, 18, 20, 24, 22, 23, 0).$$

Оператор 3) алгоритму GEN-$G(7, 5, 2, 25)$ визначає ізоморфне відображення $\varphi : Z_{25} \to G_{25}$, яке в даному випадку набуває вигляду:

$$\begin{array}{lllll}
\varphi(0) = 0, & \varphi(5) = 2, & \varphi(10) = 9, & \varphi(15) = 19, & \varphi(20) = 18, \\
\varphi(1) = 1, & \varphi(6) = 4, & \varphi(11) = 11, & \varphi(16) = 21, & \varphi(21) = 20, \\
\varphi(2) = 6, & \varphi(7) = 3, & \varphi(12) = 13, & \varphi(17) = 12, & \varphi(22) = 24, \\
\varphi(3) = 8, & \varphi(8) = 5, & \varphi(13) = 15, & \varphi(18) = 14, & \varphi(23) = 22, \\
\varphi(4) = 10, & \varphi(9) = 7, & \varphi(14) = 17, & \varphi(19) = 16, & \varphi(24) = 23,
\end{array}$$

де $\varphi(25) = \varphi(0) = 0, \varphi(1) = 1, \varphi(2) = \varphi(1 + 1) = 6, \varphi(3) = 6 + 1 = 8, \varphi(4) = 8 + 1 = 10, \ldots, \varphi(24) = 23$.

За цим ізоморфізмом оператор 4) алгоритму GEN-G будує масив $P[1 \times 25]$ (для зручності читання він поданий нижнім рядком підстановки).

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 \\ 1 & 6 & 4 & 5 & 3 & 7 & 8 & 9 & 10 & 11 & 2 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 24 & 12 & 23 & 0 & 22 \end{pmatrix}.$$

Нехай літери алфавіту англійської мови перенумеровані природним чином:

Таблиця 1 (цифрових відповідників символів алфавіту)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
a	b	c	d	e	f	g	h	i/j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

і визначальний рядок кільця G_{50}, згенеруваний алгоритмом GEN-G, має вигляд

1,5,49,7,10,17,2,34,11,20,39,33,48,3,45,4,37,6,41,13,43,15,36,8,38,9,
35,12,40,14,44,19,46,16,47,21,31,24,27,42,29,22,32,23,30,25,28,18,26,0.

Задаючи бієкцію ψ_1 кільця G_{50}[2], на кільце G_{25} вигляду

$$\psi_1 = \begin{cases} \psi(0) = 7 = m_0, & i = 0 \\ \psi(i \ (mod\ 25)) & = \quad m_{i-1} + 1, \ i \geq 1, \end{cases}$$

де $i = 1, 2, \ldots, 50$, дістаємо порядковий номер j класу елемента m_i:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
7	10	17	2	34	11	20	39	33	48	3	45	4	37	6	41	13	43	15	36	8	38	9	35	12
40	14	44	19	46	16	47	21	31	24	27	42	29	22	32	23	30	25	28	18	26	0	1	5	49
a	b	c	d	e	f	g	h	i/j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

На цьому підготовчі дії закінчуються. ♠

3.1 Криптоаналіз протоколу

Розглянемо варіанти криптоаналізу розглянутого протоколу. Криптоаналітику доступні такі дані:

а) система $\bar{L}(x)$, з якої за кількістю конгруенцій у системі знаходиться довжина блоків повідомлення;

б) довжина шифрограми, яка знаходиться за кількістю невідомих у конгруенціях;

в) можливо порядки кілець G_m і G_k.

Невідомими є ізоморфізм φ, бієкції ψ_1, λ_1 та сюр'єкції ψ і λ.

і) Припустимо, що у варіанті а) криптоаналітику більше нічого не відомо. Тоді можливим способом отримати відкритий текст є метод повного перебору. Складність такого перебору визначається кількістю способів зашифрувати повідомлення, а ця кількість складється із

1) кількості можливих ізоморфізмів (бієкцій) φ – $O((m-2)!)$, де m – порядок кільця G_m,

2) кількості бієкцій ψ_1і λ_1 – відповідно $O(m!)$,

3) кількості сюр'єкцій ψ і λ – відповідно $O(\frac{k!}{m!(l!)^m})$, де $k = lm$.

Загальна складність, навіть для такої простої криптосистеми, як у наведеному вище прикладі складає

$$23! \cdot 25! \cdot \tfrac{50!}{25!2^{25}} > \tfrac{23!50!}{2^{25}} > 2^{94} > 10^{31}\text{сек.}$$

Якщо припустити, що одна комбінація генерується в часі 10^{-14} сек., то для того щоб знайти всі комбінації потрібно буде

$$10^{31} \cdot 10^{-14} = 10^{17}$$

секунд, а це більше ніж 10^7 років.

[2]В якості G_{50} можна взяти довільну множину потужності $25 \cdot l$, а Аліса і Боб повинні однаковим чином упорядкувати елементи цієї множини і побудувати бієкцію λ_1.

Зрозуміло, що коли взяти порядки k і m більшими, то перебірний метод стає незастосовним.

б) Припустимо, що у варіанті б) криптоаналітику відомі декілька зашифрованих повідомлень, тобто йому доступні тексти

$$\bar{m}_1 = \varphi(\hat{d}_{11}, \hat{d}_{12}), \quad \bar{m}_2 = \varphi(\hat{d}_{21}, \hat{d}_{22}), \quad \bar{m}_3 = \varphi(\hat{d}_{31}, \hat{d}_{32}),$$

Оскільки бієкцій типу φ існує $(m-2)!$ і вектори $m_1, m_2, \ldots$ належать різним множинам, то ця інформація потребує знання бієкції φ, тобто визначального рядкая G_m. Але ці об'єкти йому не доступні і пошук цих об'єктів перебірним методом потребує генерації $m!(m-2)!$ комбінацій. А за цими комбінаціями потрібно ще знайти символьні відповідники (а це теж $m!$ комбінацій), то ця інформація теж не дає можливості в розумному проміжку часу знайти текст явний.

в) Припустимо, що у варіанті в) криптоаналітику відомі зашифровані повідомленняі і розшифровані повідомлення, тобто доступні

$$m_1, m_2, m_3, \ldots \text{ і } m_1 = \xi^{-1}(\varphi^{-1}(\bar{m}_1)), \quad m_2 = \xi^{-1}(\varphi^{-1}(\bar{m}_2)), \quad m_3 = \xi^{-1}(\varphi^{-1}(\bar{m}_3)), \ldots.$$

де ξ^{-1} відображає цифровий текст у символьний текст.

Оскільки відображення ξ, φ та система $\hat{l}(x)$ криптоаналітикові невідомі, то знайти відповідники і за цими даними визначальний рядок у нього немає можливості.

З вищенаведеного прикладу видно, що в обчислювальному сенсі найскладнішим етапом є побудова обернених матриць в кільці G_m. Для того, щоб спростити ці обчислення, краще скористатися ізоморфізмом між кільцями $\varphi : G_m \to Z_m$ і вести обчислення в кільці лишків Z_m. Коли обернені матриці будуть знайдені, то виконати зворотні підстановки і отримати відповідні матриці в кільці G_m.

Як відомо, мультиплікативна група дільників одиниці кільця G_k є абелевою групою [6]. Для того, щоб в цій групі можна було застосовувати функцію дискретного логарифма, вона повинна бути циклічною. Тобто мати твірний елемент, який її породжує. Отже, виникає питання: за яких умов група дільників одиниці кільця G_k буде циклічною? Відповідь на це питання дає

Теорема 1. *Мультиплікативна група кільця Z_k буде циклічною тоді і тільки тоді, коли k дорівнює 2, 4, p^m або $2p^m$, де $m \geq 1$, p – непарне просте число [6].*

4 Формування повідомлення

Зі сказаного випливає, що Аліса і Боб повинні обмінятися закритим каналом числами (a, c, l, k), де a, c, l, k – параметри алгоритма GEN-G(a, c, l, k). Якщо вибрати порядок кільця k кратним порядку кільця Z_m, тобто $k = l \cdot m$, то на підставі

взаємної простоти чисел k, m і a, способи побудова кілець будуть відомі, а перетворення з метою побудови визначальних рядків кілець взяти однаковими для G_k і G_m.

Далі з наведеного протоколу і прикладу випливає, що для передачі потрібного повідомлення $b = (b_1, b_2, \ldots, b_p)$ необхідно щоб система рівнянь

$$l(x) = Ax = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q \equiv b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q \equiv b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + a_{p2}x_q + \ldots + a_{pq}x_q \equiv b_p \end{cases} \pmod m \qquad (1)$$

мала розв'язок для довільних значень $b_1, b_2, \ldots, b_p$. Ізоморфізм кілець G_m і Z_m дозволяє розглядати лише кільце лишків Z_m. Критерій сумісності СЛНДР $Ax \equiv b\ (mod\ m)$ розмірності $p \times q, (p < q)$ над кільцем Z_m вимагає існування розв'язку порівняння

$$d_1y_1 + d_2y_2 + \ldots + d_sy_s \equiv 1\ (mod\ m),$$

де $d_1, d_2, \ldots, d_s$ – значення останніх координат у розв'язках СЛОДР $Ax - bx_0 = 0$ [7]. Ця умова виконується для довільного b, якщо рівняння системи лінійно незалежні і детермінант матриці підсистеми $A_1u \equiv b \pmod m$) розмірності $p \times p$, яка утворена лінійно незалежними стовпчиками $b_{i_1}, b_{i_2}, \ldots, b_{i_p}$ СЛНДР $Ax \equiv b \pmod m$, взаємно простий з модулем m. Тоді для матриці підсистеми існує обернена матриця, тобто із $A_1u = b \pmod m$ випливає $A_1^{-1}A_1u = u \equiv A_1^{-1}b \pmod m$ для довільного b. А вектор $a = (a_1, a_2, \ldots, a_q)$, у якого номери координат $i_1, i_2, \ldots, i_p$ такі як у вектора $u \equiv A_1^{-1}b \pmod m$ а решта координат мають нульові значення, буде розв'язком СЛНДР.

Отже, Алісі потрібно будувати СЛР, у якої рівняння лінійно незалежні і мають підсистему з детермінантом її матриці, який взаємно простий з модулем m. Для перевірки лінійної незалежності виразів Алісі потрібно розв'язати систему $A^Ty \equiv 0 \pmod m$ і переконатися, що ця система має лише нцльовий розв'язок. Потім побудувати підсистему з описаними властивостями детермінанта її матриці.

Приклад 3. Нехай літери алфавіту англійської мови перенумеровані природним чином (див. табл. 1).

Крок 1. а) Нехай Аліса побудувала в кільці G_{25} такі вирази (в дужках показані вирази, де від'ємні коефіцієнти замінені своїми протилежними):

$$l(x) = \begin{cases} 2x_1 - 16x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 - 17x_3 - 11x_4 \end{cases} \left(\begin{cases} 2x_1 + 4x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4 \end{cases} \right)$$

і перетворила їх до вигляду

$$L(x) = B_1(l(x)+(1,2)^t) = \begin{cases} 9x_1 - 13x_2 + 10x_3 - 16x_4 + 3, \\ 18x_1 + 14x_2 - 18x_3 + 19x_4 + 16, \end{cases} \left(\begin{cases} 9x_1 + 15x_2 + 10x_3 + 4x_4 + 3, \\ 18x_1 + 14x_2 + 2x_3 + 19x_4 + 16, \end{cases} \right)$$

де матриця $B_1 = \begin{pmatrix} 6 & 1 \\ 23 & 23 \end{pmatrix}$ і її відповідник у кільці Z_{25} $\bar{B}_1 = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$.

в) Аліса виконує заміну коефіцієнтів у побудованих виразах $l(x)$, $L(x)$ і матриці B_1 відповідниками з фактор множини G_{50}/ψ і дістає вирази

$$\bar{l}(x) = \begin{cases} 17x_1 + 34x_2 + 21x_3 + 26x_4, \\ 7x_1 + 14x_2 + 42x_3 + 43x_4, \end{cases}$$

$$\bar{L}(x) = B_1(l(x) + (1,2)^t) = \begin{cases} 48x_1 + 41x_2 + 3x_3 + 46x_4 + 19, \\ 15x_1 + 32x_2 + 44x_3 + 36x_4 + 30, \end{cases}$$

які висилає Бобу відкритим каналом або виставляє на своєму сайті.

Крок 2. а) Боб за бієкціями φ і ψ_1 знаходить відповідники виразів $\hat{l}(x)$ і $\hat{L}(x)$ у кільці Z_{25}:

$$\hat{l}(x) = \begin{cases} 5x_1 + 6x_2 + 9x_3 + 21x_4, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4. \end{cases}$$

$$\hat{L}(x) = \begin{cases} 10x_1 + 13x_2 + 4x_3 + 6x_4 + 7, \\ 20x_1 + 18x_2 + 5x_3 + 15x_4 + 19. \end{cases}$$

Неважко переконатися, що в системі виразів $\hat{l}(x)$ другий і третій стовпчики утворюють підсистему, детермінант якої дорівнює 7, а 7 – взаємно простий з модулем 25 в кільці Z_{25} (умови сумісності системи $\hat{l}(x)$ виконуються).

Боб хоче передати Алісі повідомлення

tara tara tarara.

б) Боб розбиває повідомлення на блоки по два символи в блоці (відступи між символами повідомлення, яким відповідає елемент 49, не враховані з метою спрощення обчислень у прикладі), замінює їх цифровими відповідниками, які взяті з табл. 1:

ta	ra	ta	ra	ta	ra	ra
18,0	16,0	18,0	16,0	18,0	16,0	16,0

.

б) Розв'язує систему рівнянь в кільці Z_{25}

$$\hat{l}(x) = \begin{cases} 5x_1 + 6x_2 + 9x_3 + 21x_4 = 18, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4 = 0. \end{cases} \pmod{25}$$

і знаходить розв'язок $\bar{x} = (0, 14, 1, 0)$.

в) Значення $v_1 = (18, 0)$ він тримає в секреті. Обирає вектор $\bar{a} = (0, 1, 0, 1)$ і обчислює значення $d = l(\bar{a}) = (2, 15)$ і до розв'язку даної системи $\bar{x} = (0, 14, 1, 0)$ додає вектор $\bar{a} = (0, 1, 0, 1)$ і цю суму векторів $\bar{x} + \bar{a} = (0, 15, 1, 1)$ підставляє в $L(x)$, знаходячи тим самим значення $d_1 = (12, 9)$. Відповідники значень d і d_1 у кільці G_m Боб висилає Алісі.

Аліса, за отриманими відповідниками знаходить значення d, d_1, і виконує такі обчислення.

а) Обчислює обернену матрицю до матриці $\bar{B}_1^{-1}$ у кільці Z_{25}:

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix}.$$

б) Обчислює $\bar{B}_1^{-1}(d_1^t - (7,19)^t = \bar{B}_1^{-1}(12,9) - (7,19))^t = \bar{B}_1^{-1}(5,15)^t$ і знаходить

$$\bar{B}_1^{-1}(5,15)^t - (2,15)^t = (20,15) - (2,15) = (18,0) = v_1.$$

а) Боб розв'язує систему рівнянь

$$\hat{l}(x) = \begin{cases} 5x_1 + 6x_2 + 9x_3 + 21x_4 = 16, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4 = 0. \end{cases} \pmod{25}$$

і знаходить розв'язок $\bar{x} = (0, 18, 12, 0)$.

б) Значення $v_2 = (16, 0)$ він тримає в секреті. Обирає вектор $\bar{a} = (1, 0, 1, 0)$ і обчислює значення $d = l(\bar{a}) = (14, 11)$ і до розв'язку даної системи $\bar{x} = (0, 18, 12, 0)$ додає вектор $\bar{a} = (1, 0, 1, 0)$ і цю суму векторів $\bar{x} + \bar{a} = (1, 18, 13, 0)$ підставляє в $L(x)$, знаходячи тим самим значення $d_1 = (3, 3)$.

в) Відповідники значень d і d_1 у кільці G_m Боб висилає Алісі.

Крок 3. Аліса, за отриманими відповідниками знаходить значення d, d_1 і виконує такі обчислення.

а) Знаходить обернену матрицю до $\bar{B}_1^{-1}$ в кільці Z_{25}:

б) Обчислює $B_1^{-1}(d_1^t - (7, 19)^t) = B_1^{-1}(21, 9)^t$ і знаходить

$$\bar{B}_1^{-1}(21, 9)^t) - (14, 11)^t = (5, 11) + (11, 14) = (16, 0) = v_2.$$

б) Боб розв'язує систему рівнянь в кільці Z_{25}

$$l(x) = \begin{cases} 5x_1 + 6x_2 + 9x_3 + 21x_4 = 18, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4 = 0. \end{cases} \pmod{25}$$

і знаходить розв'язок $\bar{x} = (0, 14, 1, 0)$. Оскільки наступний блок такий самий як і перший, тобто $v_3 = (18, 0)$. Це змушує Боба вибрати новий вектор $\bar{a} = (0, 0, 1, 1)$, за яким він обчислює значення

$$d = l(\bar{a}) = (5, 0),\ \bar{x} + \bar{a} = (0, 14, 2, 1),\ d_1 = L(\bar{x} + \bar{a}) = (3, 21).$$

і висилає Алісі відповідники $d = (5, 0),\ d_1 = (3, 21)$ у кільці G_{25}.

Аліса обчислює

$$B_1^{-1}(d_1^t - (7, 19)^t) = B_1^{-1}(21, 2)^t = (23, 0) = l(\bar{x} + \bar{a}).$$

Звідки знаходить

$$(23, 0) - (5, 0) = (18, 0) = v_3.$$

Оскільки наступний блок такий самий як і другий, тобто $v_4 = (16, 0)$, то це змушує Боба вибрати новий вектор $\bar{a} = (0, 0, 0, 1)$, за яким він обчислює значення

$$d = l(\bar{a}) = (21, 14),\ \bar{x} + \bar{a} = (0, 18, 12, 1),\ d_1 = L(\bar{x} + \bar{a}) = (20, 18).$$

і висилає Алісі відповідники $d = (21, 14),\ d_1 = (20, 18)$ у кільці G_{25}.

Аліса обчислює

$$B_1^{-1}(d_1^t - (7, 19)^t) = B_1^{-1}(13, 24)^t = (12, 14) = l(\bar{x} + \bar{a}).$$

Звідки знаходить

$$(12, 14) - (21, 14) = (12, 14) + (4, 11) = (16, 0) = v_4.$$

Цю процедуру Боб і Аліса повторюють стільки разів, скільки блоків у повідомленні (в даному випадку ще три рази). Таким чином Аліса отримує шифрограму

(2,15,12,9) (14,11,3,3) (5,0,3,21) (21,14,20,18) ⋯ ⋯ ⋯

Після дешифраці Аліса відкриває повідомлення

18,0	16,0	18,0	16,0	18,0	16,0	16,0	♠
ta	ra	ta	ra	ta	ra	ra	

В наведеному прикладі використовувалося одне і те саме кільце, але можна при кожному сеансі передачі або з певним періодом між передачами змінювати кільце. Можна змінювати вектори a і $\bar{a}$, які змінюють значення $l(\bar{a})$ і $L(\bar{x}+\bar{a})$.

Наведений протокол можна зробити складнішим, якщо використовувати при шифруванні кожного блоку різні кільця або різні значення параметрів – матриць і векторів. Крім того, якщо шифрований текст представити відповідниками в кільці G_{50}

(44,23,4,48) (6,45,2,19) (11,40,19,0) (38,22,8,15) ⋯ ⋯ ⋯,

то криптоаналітику зовсім недоступні системи виразів, кільця G_{25}, Z_{25} та відображення $\lambda, \lambda_1, \psi, \psi_1$ і φ.

5 Обчислювальні особливості

Виходячи з того, що обчислення в кільці G_m не є звичним при обчисленнях, то покращити ефективність шифрування і розшифрування можна, якщо знову скористатися ізоморфізмом між кільцями G_m і Z_m. Дійсно, пошук протилежного елемента до елемента a в кільці Z_m зводиться до обчислення різниці $m-a$, а обчислення оберненого елемента до a виконується шляхом застосування розширеного алгоритму Евкліда для розв'язання рівняння $ax+my=1$ (розширений алгоритм Евкліда обчислює розклад $ax+by=d$, де d =НСД(a,b)). Результатом виконання цього алгоритму є значення $x=a^{-1}$.

Очевидним недоліком описаного протоколу є те, що довжина шифрограми у двічі довша тексту повідомлення.

Література

[1] *Wenbo Mao.* Modern Cryptography. – Pearson Education. – Prentice Hall Professional Technical Reference Upper Saddle River. – New Jersey. – 2004. – 768 p.

[2] *Kameswari P.A., Sriniasarao S.S., Belay A.* An application of Linear Diophantine equations to Cryptography. – Advanced in Mathematics: Scientific Journal. –2021. – v. 10. – P. 2799 – 2806.

[3] *Hermann M., Juban L., Kolaitis P. G.* On the Complexity of Counting the Hilbert Basis of a Linear Diophantine System. – Springer Verlag. – LNCS. – 1999. – № 1705. – P. 13–32.

[4] *Berczes A., Lajos H., Hirete-Kohno N., Kovacs T.* A key exchange propocol based on Diophantine equations and S-integers. – JSIAM Letters. – 2014. – p. 85–88.

[5] *Kryvyi S., Opanasenko V., Grinenko O., Nortman Yu.* Symmetric system for Exchange Information on the Base of Surjective Isomorphism of Rings. *12th Int. IEEE Conf. on Dependable Systems, Services and Technologies (DESSERT 2022). – 2022.– December 9-11. – pp. 1-7.*

[6] *Shoup V.* An Computational Introduction to Number Theory and Algebra. – Cambridge University Press. – 2008. – 580 p.

[7] *Кривий С.Л.* Лінійні Діофантові обмеження та їх застосування. – Київ: Інтерсервіс. – 2021. – 257 с.