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:

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

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

Таблиця 1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	**1**	**3**	**0**	**5**	**2**	**4**
2	2	0				
3	3	5				
4	4	2				
5	5	4				

Таблиця 2

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	**1**	**3**	**0**	**5**	**2**	**4**
2	2	0	4	1	5	3
3	3	5	1	4	0	2
4	4	2	5	0	3	1
5	5	4	3	2	1	0

Таблиця 3

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	**0**	**1**	**2**	**3**	**4**	**5**
2	0	2	1	4	3	5
3	0	3	4	4	3	0
4	0	4	3	3	4	0
5	0	5	5	0	0	5

Знаходимо значення $4 = 5 + 1$ і обчислюємо результат операції додавання з елементом 4, потім знаходимо значення $4 + 1 = 2$ і обчислюємо значення операції додавання з елементом 2, запишемо ці значення у табл. 2. Оскільки $2 + 1 = 0$, а для 0 результати вже відомі, то на цьому закінчуємо побудову таблиці операції додавання групи GN_6 (див. табл. 2).

Для побудови Абелевої групи GN_k, як зазначалося, недостатньо вимагати тільки однозначності операції додавання. Якщо визначити додавання в групі так, що $0 + 1 = 1, 1 + 1 = 0, 1 + 2 = 3, 1 + 3 = 4, 1 + 4 = 5, 1 + 5 = 2$, то, обчислюючи $1 + 3$, отримаємо $1 + 3 = 1 + (1 + 2) = (1 + 1) + 2 = 0 + 2 = 2$, що не узгоджується з визначеним раніше. Задана у такий спосіб операція додавання не охоплює всіх елементів групи, оскільки існує елемент скінченного порядку $2 < 6$ $(1 + 1 = 0)$. Поставимо у відповідність операції додавання з елементом групи a_1 підстановку

$$f = \begin{pmatrix} 0 & a_1 & a_2 & \dots & a_{k-1} \\ a_1 & a_{i1} & a_{i2} & \dots & a_{ik} \end{pmatrix}.$$

За цією підстановкою $f(0) = 0 + a_1 = a_1$, $f(a_1) = a_1 + a_1 = a_{i1}$, $f(a_{ij}) = a_{ij} + a_1$, $j = 2, \dots, k - 1$. Назвемо групу GN_k повноциклічною, якщо підстановка f є повним циклом довжини k. Наприклад, група, представлена табл. 2, повноциклічна і її підстановка

$$f = \begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 0\ 5\ 2\ 4 \end{pmatrix}$$

є повним циклом.

Справедливе твердження.

Теорема 1. Скінченні повноциклічні Абелеві групи однакових порядків ізоморфні.

Доведення випливає з того, що повноциклічні групи є циклічними групами, а скінченні циклічні групи однакових порядків ізоморфні.

Асоціативно-комутативним кільцем з одиницею називається алгебра, яка є Абелевою групою стосовно операції додавання і Абелевим моноїдом стосовно операції множення, а для операції додавання і множення виконується закон дистрибутивності, тобто $(\forall x, x', x'')\ x(x' + x'') = xx' + xx''$.

КРИПТОГРАФІЧНА СИСТЕМА НА ОСНОВІ ГРУП І КІЛЕЦЬ

Розглянемо спосіб побудови за групою GN_6, яка задана табл. 2, асоціативно-комутативного кільця з одиницею $AKK1_6$. Із аксіом кільця з одиницею випливає, що $\forall a \in GN_6$ $(a \cdot 0 = 0 \cdot a = 0,\ a \cdot 1 = 1 \cdot a = a)$. Отже, два рядки і два стовпчики таблиці множення визначені. Далі, за таблицею додавання, застосовуючи закон дистрибутивності, будуємо таблицю операції множення. Дійсно, оскільки $3 = 1 + 1$, отримуємо

$$3 \cdot 2 = (1 + 1) \cdot 2 = 2 + 2 = 4;\ 3 \cdot 3 = (1 + 1) \cdot 3 = 3 + 3 = 4;$$

$$3 \cdot 4 = (1 + 1) \cdot 4 = 4 + 4 = 3;\ 3 \cdot 5 = (1 + 1) \cdot 5 = 5 + 5 = 0.$$

Оскільки $5 = 1 + 3$, маємо

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

Аналогічно знаходимо результати множення з елементом $4 = 5 + 1$ і потім з елементом $2 = 1 + 4$. Оскільки $1 + 2 = 0$, на підставі повноциклічності вся таблиця операції множення побудована (табл. 3). Із симетричності цієї таблиці випливає комутативність операції множення в кільці $AKK1_6$. Можна перевірити, що ця операція задовольняє закон асоціативності, тобто $AKK1_6$ — асоціативно-комутативне кільце з одиницею.

Нехай операція додавання визначена для елемента 1. Тоді в загальному випадку для побудови асоціативно-комутативного кільця k-го порядку з одиницею $AKK1_k$, потрібно виконати такі алгоритми.

ADD-TAB-AKK1$(1, k)$

0. Задекларувати масив $\mathrm{T}_+[k \times k]$.

1. Записати в T_+ в перший рядок і перший стовпчик результати додавання з нулем кільця.

2. Записати в T_+ в рядок і стовпчик з номером 2 значення операції додавання з елементом 1.

3. $c := 1$.

4. Взяти з T_+ елемент $c' = c + 1$.

5. Для всіх x записати в рядок і стовпчик з номером c' масиву T_+ значення $c' + x = (c+1) + x = c + (1 + x)$.

6. $c := c'$, $c' := c + 1$; якщо $c' = 0$, то СТОП, інакше перейти на крок 5.

MUL-TAB-AKK1$(1, k)$

0. Задекларувати масив $\mathrm{T}.[k \times k]$.

1. Записати в $\mathrm{T}.$ в рядок і стовпчик з номерами 0 і 1 відповідно результати операції множення на 0 і на 1.

2. $c := 1$.

3. Взяти з T_+ елемент $c' = c + 1$.

4. Для всіх x записати в рядок і стовпчик з номером c' масиву $\mathrm{T}.$ значення $c' \cdot x = (c+1) \cdot x = c \cdot x + x$.

5. $c := c'$; $c' := c + 1$; якщо $c' = 0$, то СТОП, інакше перейти на крок 4.

Часова складність першого алгоритму $O(k^2 \log k)$, а другого — $O((k \log k)^2)$, де k — порядок кільця.

Правильність цих алгоритмів випливає з того, що елементи $c_1 = 1 + 1$, $c_2 = c_1 + 1, \ldots, c_k = c_{k-1} + 1$ пробігають всі елементи Абелевої групи, а також із того, що в групі рівняння $a + x = b$ має єдиний розв'язок.

Нехай алфавіт $X = \{x_1, x_2, \ldots, x_m\}$ містить m елементів, які певним чином упорядковані числами із множини $M = \{0, 1, \ldots, m-1\}$, а кільце $G = \{a_1, a_2, \ldots, a_k\}$ має k елементів, де $k \geq m$. Визначимо сюр'єкцію $g : G \to M$, наприклад у вигляді

$$g(a_i) = \begin{cases} m_1, & \text{якщо } i = 0, \\ g(a_{i-1}) + 1, & \text{якщо } i > 0, \end{cases} \qquad (1)$$

де $m_1 \in M$ вибирають довільно, а індекс i обчислюється за модулем m. Це означає, що m_1 потрапляє в клас з індексом 0, а $m_1 + 1$ потрапляє в клас з індексом 1 і т.д.

Нехай потрібно зашифрувати повідомлення $b = x_1 x_2 \ldots x_s$, де $x_i \in X$. Повідомленню b відповідає цифрове зображення $\overline{b} = n_1 n_2 \ldots n_s$, де $n_i = g(a_i)$, а n_i — порядковий номер символа $x_i \in X$. Сюр'єкція g визначає відношення еквівалентності

~ на елементах кільця G. Якщо $k = m$, то сюр'єкція g буде бієкцією, оскільки класи еквівалентності за відношенням, яке індукується цією сюр'єкцією, будуть одноелементними. Для того, щоб приховати частоту появи символів у повідомленні, потрібно вибирати $k > m$, причому k має бути досить великим для збільшення кількості елементів у класах еквівалентності (ці елементи в класах відіграють роль гомофонів під час шифрування). Вибираємо ключове слово p, яке може бути довільним словом в алфавіті X і яке має цифрове зображення (відповідно до відображення g): $\overline{p} = k_1 k_2 \dots k_r$.

Із цих побудов випливає алгоритм шифрування з використанням властивостей кільця.

RG-EN($\mathrm{T}_+ [1, k], g, p$)

1. Задати рядок додавання з одиницею $\mathrm{T}_+ [1, k]$ (вибирають довільно, але так, щоб адитивна група кільця була повноциклічною), сюр'єкцію $g : G \to M$ і ключове слово p.

2. Побудувати кільце G, порядок якого $k \geq m$ за рядком $\mathrm{T}_+ [1, k]$.

3. Побудувати шифрограму $d = d_1 d_2 \dots d_s$ (посимвольно) для $\overline{b} = n_1 n_2 \dots n_s$ за правилом $d_i = k_i + g(a_i)$, де k_i — номер символа ключового слова, n_i — образ номера символа $x_i \in X$ повідомлення b, а + є операцією додавання кільця G (шифрування може використовувати і операцію множення кільця);

4. Надіслати відкритим каналом абоненту шифрограму d, а закритим каналом — трійку ($\mathrm{T}_+ [1, k], g, p$).

Розшифрування виконується відповідно до такого алгоритму.

RG-DE(t)

1. Абонент за рядком $\mathrm{T}_+ [1, k]$ будує кільце G_k.

2. За отриманою шифрограмою d і ключовим словом p (в їхньому цифровому зображенні) для кожної пари відповідних символів розв'язує рівняння $a_i + x_i = d_i$ ($a_i \cdot x_i = d_i$) за допомогою таблиці додавання (множення) кільця, де a_i — номер символа ключового слова, d_i — символ шифрограми.

3. Знаходить номер m_i класу, який відповідає символу відкритого тексту x_i, і в такий спосіб відкриває оригінальний текст (див. далі приклад 1).

У разі $k = m$ кількість таких сюр'єкцій (які будуть бієкціями) складає $m!$. Ключове слово може бути довільним словом в алфавіті X, який розширений, наприклад, знаками пунктуації або іншими символами, що мають номери. Потужність такого розширеного алфавіту не повинна перевищувати кількості елементів кільця. Таку сюр'єкцію і спосіб її використання в кільці $AKK1_{25}$ наведено в прикладі.

Приклад 1. Зашифрувати текст «UKRPROGTWENTY» в кільці $AKK1_{25}$, заданому наведеною далі підстановкою f, яка відповідає рядку $\mathrm{T}_+ [1, 25]$. Символи алфавіту англійської мови мають стандартне упорядкування:

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

Задаючи сюр'єкцію (у цьому випадку бієкцію) відображенням вигляду (1) з початковим значенням $m_1 = 7$, знаходимо такі відповідності символів алфавіту:

7	9	11	13	15	17	19	21	12	14	16	18	20	24	22	23	0	1	6	8	10	2	4	3	5
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

Застосовуючи алгоритми **ADD-TAB-AKK1**(1, 25) і **MUL-TAB-AKK1**(1, 25), знаходимо таблиці операцій кільця $AKK1_{25}$, що задані підстановкою $\mathrm{T}_+ [1, 25]$):

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

Таблиця операції додавання кільця $AKK1_{25}$

+	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
0	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
$1(T_+[1, 25])$	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**
2	2	4	9	13	11	15	3	17	5	19	7	21	24	12	22	14	23	16	0	18	1	20	8	10	6
3	3	5	13	17	15	19	7	21	9	12	11	14	23	16	0	18	1	20	6	24	8	22	2	4	10
4	4	3	11	15	13	17	5	19	7	21	9	12	22	14	23	16	0	18	1	20	6	24	10	2	8
5	5	7	15	19	17	21	9	12	11	14	13	16	0	18	1	20	6	24	8	22	10	23	4	3	2
6	6	8	3	7	5	9	10	11	2	13	4	15	16	17	18	19	20	21	24	12	22	14	0	1	23
7	7	9	17	21	19	12	11	14	13	16	15	18	1	20	6	24	8	22	10	23	2	0	3	5	4
8	8	10	5	9	7	11	2	13	4	15	3	17	18	19	20	21	24	12	22	14	23	16	1	6	0
9	9	11	19	12	21	14	13	16	15	18	17	20	6	24	8	22	10	23	2	0	4	1	5	7	3
10	10	2	7	11	9	13	4	15	3	17	5	19	20	21	24	12	22	14	23	16	0	18	6	8	1
11	11	13	21	14	12	16	15	18	17	20	19	24	8	22	10	23	2	0	4	1	3	6	7	9	5
12	12	14	24	23	22	0	16	1	18	6	20	8	7	10	9	2	11	4	13	3	15	5	19	21	17
13	13	15	12	16	14	18	17	20	19	24	21	22	10	23	2	0	4	1	3	6	5	8	9	11	7
14	14	16	22	0	23	1	18	6	20	8	24	10	9	2	11	4	13	3	15	5	17	7	21	12	19
15	15	17	14	18	16	20	19	24	21	22	12	23	2	0	4	1	3	6	5	8	7	10	11	13	9
16	16	18	23	1	0	6	20	8	24	10	22	2	11	4	13	3	15	5	17	7	19	9	12	14	21
17	17	19	16	20	18	24	21	22	12	23	14	0	4	1	3	6	5	8	7	10	9	2	13	15	11
18	18	20	0	6	1	8	24	10	22	2	23	4	13	3	15	5	17	7	19	9	21	11	14	16	12
19	19	21	18	24	20	22	12	23	14	0	16	1	3	6	5	8	7	10	9	2	11	4	15	17	13
20	20	24	1	8	6	10	22	2	23	4	0	3	15	5	17	7	19	9	21	11	12	13	16	18	14
21	21	12	20	22	24	23	14	0	16	1	18	6	5	8	7	10	9	2	11	4	13	3	17	19	15
22	22	23	8	2	10	4	0	3	1	5	6	7	19	9	21	11	12	13	14	15	16	17	20	24	18
23	23	0	10	4	2	3	1	5	6	7	8	9	21	11	12	13	14	15	16	17	18	19	24	22	20
24	24	22	6	10	8	2	23	4	0	3	1	5	17	7	19	9	21	11	12	13	14	15	18	20	16

Таблиця операції множення кільця $AKK1_{25}$

·	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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	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
2	0	2	0	9	2	19	9	18	19	0	18	2	9	9	19	19	18	18	0	0	2	2	19	18	9
3	0	3	9	23	12	4	17	15	20	18	8	6	16	7	1	21	5	22	19	2	24	13	11	14	10
4	0	4	2	12	11	22	13	10	14	9	23	21	6	24	5	8	17	7	18	19	1	20	15	16	3
5	0	5	19	4	22	17	21	24	23	2	3	15	11	20	16	10	6	13	9	18	14	8	7	12	1
6	0	6	9	17	13	21	10	14	4	18	5	24	7	23	11	1	15	8	19	2	12	3	20	22	16
7	0	7	18	15	10	24	14	4	6	19	11	23	8	5	13	12	20	1	2	9	17	16	3	21	22
8	0	8	19	20	14	23	4	6	7	2	13	5	1	11	10	17	3	12	9	18	15	22	16	24	21
9	0	9	0	18	9	2	18	19	2	0	19	9	18	18	2	2	19	19	0	0	9	9	2	19	18
10	0	10	18	8	23	3	5	11	13	19	21	16	14	22	24	6	1	4	2	9	7	17	12	20	15
11	0	11	2	6	21	15	24	23	5	9	16	20	13	3	22	14	7	10	18	19	4	1	8	17	12
12	0	12	9	16	6	11	7	8	1	18	14	13	17	10	4	20	22	15	19	2	3	24	21	5	23
13	0	13	9	7	24	20	23	5	11	18	22	3	10	16	21	4	8	14	19	2	6	12	1	15	17
14	0	14	19	1	5	16	11	13	10	2	24	22	4	21	23	7	12	6	9	18	8	15	17	3	20
15	0	15	19	21	8	10	1	12	17	2	6	14	20	4	7	16	24	3	9	18	22	5	23	13	11
16	0	16	18	5	17	6	15	20	3	19	1	7	22	8	12	24	11	21	2	9	23	10	13	4	14
17	0	17	18	22	7	13	8	1	12	19	4	10	15	14	6	3	21	20	2	9	16	23	24	11	5
18	0	18	0	19	18	9	19	2	9	0	2	18	19	19	9	9	2	2	0	0	18	18	9	2	19
19	0	19	0	2	19	18	2	9	18	0	9	19	2	2	18	18	9	9	0	0	19	19	18	9	2
20	0	20	2	24	1	14	12	17	15	9	7	4	3	6	8	22	23	16	18	19	21	11	5	10	13
21	0	21	2	13	20	8	3	16	22	9	17	1	24	12	15	5	10	23	18	19	11	4	14	7	6
22	0	22	19	11	15	7	20	3	16	2	12	8	21	1	17	23	13	24	9	18	5	14	10	6	4
23	0	23	18	14	16	12	22	21	24	19	20	17	5	15	3	13	4	11	2	9	10	7	6	1	8
24	0	24	9	10	3	1	16	22	21	18	15	12	23	17	20	11	14	5	19	2	13	6	4	8	7

Зауважимо, що коли таблиці операцій, наприклад, кільця $AKK1_{25}$ збігаються з таблицями кільця лишків Z_{25}, то таблиця додавання цього кільця відповідає відомому шифру Віженера. Оскільки адитивна група кільця Z_{25} повноциклічна, між кільцями Z_{25} і $AKK1_{25}$ існує ізоморфізм, який є продовженням ізоморфізму повноциклічних груп таких кілець. Це інколи дає змогу уникнути побудови таблиць операцій кільця $AKK1_k$ і користуватися ізоморфними відображеннями та виконувати операції в кільці лишків Z_{25}, а потім знаходити образи значень виконаних операцій в кільці $AKK1_{25}$.

Потрібно зашифрувати в цьому кільці текст «UKRPROGTWENTY». Для цього за рядком з номером 1 таблиці додавання будуємо кільце $AKK1_{25}$, задаємо сюр'єкцію g і вибираємо ключове слово $p = \text{IPRSP}$. Знаходимо суми числових пар, які відповідають символам алфавіту із таблиці додавання, і отримуємо шифрограму:

I	P	R	S	P	U	K	R	P	R	O	G	T		
U	K	R	P	R	O	G	T	W	E	N	T	Y		
12	**22**	**0**	**1**	**22**	**8**	**14**	**0**	**22**	**0**	**24**	**19**	**6**	— $\overline{p}\overline{b}$	цифрові відповідності ключового слова і тексту
+	+	+	+	+	+	+	+	+	+	+	+	+		
8	**14**	**0**	**22**	**0**	**24**	**19**	**6**	**2**	**15**	**20**	**6**	**3**	— $\overline{b}$	цифрові відповідності символів тексту
=	=	=	=	=	=	=	=	=	=	=	=	=		
18	**21**	**0**	**23**	**22**	**0**	**5**	**6**	**8**	**15**	**14**	**12**	**7**	— d	шифрограма цифрова (сума відповідностей)

Розшифрування: абоненту, якому адресована ця шифрограма, відомий ключ таблиці додавання $\mathrm{T}_+[1, k]$, ключове слово $p = \text{IPRSP}$ і сюр'єкція g. Абонент будує кільце за рядком $\mathrm{T}_+[1, k]$; записує цифрову шифрограму d і цифрові значення ключового слова $\overline{p}$; за першим символом k_1 ключового слова знаходить символ, який є першим символом n_1 шифрограми d в таблиці додавання (в прикладі: в рядку з номером $k_1 = 12$ знаходить значення $n_1 = 18$, тобто розв'язує рівняння $k_1 + x = n_1$); за знайденим значенням в стовпчику, який відповідає значенню n_1, знаходить відповідник (у прикладі це число $x_1 = 8$, йому відповідає символ *и*) і т.д.:

	18	**21**	**0**	**23**	**22**	**0**	**5**	**6**	**8**	**15**	**14**	**12**	**7**	$= d$
	12	**22**	**0**	**1**	**22**	**8**	**14**	**0**	**22**	**0**	**24**	**19**	**6**	$= \overline{p}\overline{b}$
$\overline{b} =$	**8**	**14**	**0**	**22**	**0**	**24**	**19**	**6**	**2**	**15**	**20**	**6**	**3**	
$b =$	U	K	R	P	R	O	G	T	W	E	N	T	Y	

Наведений у прикладі текст можна зашифрувати, використовуючи таблицю множення. Це дає змогу користуватися обома таблицями одночасно: одній парі номерів ставимо у відповідність елемент таблиці додавання, а наступній парі, що повторюється, — відповідне значення із таблиці множення (відповідником буде елемент $m = i \cdot j$). Але ця відповідність можлива лише, коли аргументи в добутку (елементи i, j) є дільниками одиниці в кільці $AKK1_k$. Відомо, що множина дільників одиниці в кільці є Абелевою групою [1] і її порядок легко знайти.

Теорема 2. Скінченне асоціативно-комутативне кільце з одиницею k-го порядку має $\varphi(k)$ дільників одиниці, де φ — функція Ойлера.

Доведення. Розглянемо Z_k — кільце лишків за модулем k. Вочевидь, що адитивна група цього кільця повноциклічна. Дільниками одиниці в цьому кільці є елементи, які взаємно прості з модулем кільця k, а кількість таких елементів дорівнює значенню функції Ойлера $\varphi(k)$. Згідно з теоремою 1 існує ізоморфізм між кільцем лишків Z_k і кільцем $AKK1_k$, який є продовженням ізоморфізму між адитивними групами цих кілець. Ізоморфний образ дільника одиниці є дільником одиниці [1]. Звідси випливає справедливість теореми.

На підставі теореми 1 таблиці операцій кільця $AKK1_{25}$, як зазначалося, можна не будувати, а використовувати ізоморфізм $f : Z_{25} \to AKK1_{25}$. Дійсно, таблиця відповідностей має вигляд

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

Дільниками нуля в кільці лищків Z_{25} є елементи $0, 5, 10, 15, 20$, яким в кільці $AKK1_{25}$ відповідають елементи $0, 2, 9, 19, 18$. Решта елементів цього кільця — дільники одиниці, які утворюють Абелеву мультиплікативну групу кільця. Отже, для обчислення, наприклад, добутку елементів 6 і 7 знаходимо добуток їхніх образів 2 і 9 в кільці лишків $Z_{25}: 18 = 18 \pmod{25}$. Тоді в кільці $AKK1_{25}$ елементу 18 відповідає елемент $f(18) = 14$. Звідси отримуємо, що $6 \cdot 7 = 14$ в кільці $AKK1_{25}$. Отже, твірними елементами мультиплікативної групи кільця $AKK1_{25}$ є елементи 5, 6, 8, 12, 13, 15, 22, 24. Це випливає із такої теореми.

Теорема 3. Якщо мультиплікативна група дільників одиниці асоціативно-комутативного кільця з одиницею має твірний елемент z, то твірними елементами цієї групи будуть елементи z^j такі, що НСД $(j, \varphi(k)) = 1$ [4].

Дійсно, в прикладі мультиплікативної групи кільця $AKK1_{25}$ маємо $\varphi(25) = 20$. Тоді кількість твірних у цій групі дорівнює $\varphi(20) = 8$ (твірні виокремлено жирним шрифтом):

$$\mathbf{6^1} = 6,\ 6^2 = 10,\ \mathbf{6^3} = 5,\ 6^4 = 21,\ 6^5 = 3,\ 6^6 = 17,\ \mathbf{6^7} = 8,\ 6^8 = 4,\ \mathbf{6^9} = 13,\ 6^{10} = 23,$$

$$\mathbf{6^{11}} = 22,\ 6^{12} = 20,\ \mathbf{6^{13}} = 12,\ 6^{14} = 7,\ 6^{15} = 14,\ 6^{16} = 11,$$

$$\mathbf{6^{17}} = 24,\ 6^{18} = 16,\ \mathbf{6^{19}} = 15,\ 6^{20} = 1,$$

а також

$$\mathbf{5^1} = 5,\ 5^2 = 17,\ \mathbf{5^3} = 13,\ 5^4 = 20,\ 5^5 = 14,\ 5^6 = 16,\ \mathbf{5^7} = 6,\ 5^8 = 21,\ \mathbf{5^9} = 8,\ 5^{10} = 23,$$

$$\mathbf{5^{11}} = 12,\ 5^{12} = 11,\ \mathbf{5^{13}} = 15,\ 5^{14} = 10,\ 6^{15} = 3,\ 5^{16} = 4,\ \mathbf{5^{17}} = 22,\ 5^{18} = 7,\ \mathbf{5^{19}} = 24,\ 5^{20} = 1.$$

Отже, в групі дільників одиниці можна використовувати функцію дискретного логарифма для шифрування повідомлень і передавання ключів. Наприклад, рівняння $6^x = 20 \pmod{25}$ має розв'язок $x = 12$, а $5^x = 24 \pmod{25}$ має розв'язок $x = 19$, тобто $\log_5 24 = 19$.

Основною перешкодою використання дискретного логарифма в кільцях є те, що не завжди його мультиплікативна група буде циклічною. Наприклад, у кільці лишків за модулем $k = 16$ маємо $\varphi(k) = 8$ і дільниками одиниці є елементи 1, 3, 5, 7, 9, 11, 13, 15. Кожен з цих елементів має порядок 2 або 4 і тому група дільників одиниці не буде циклічною. Це одна з причин того, що в криптографії частіше використовуються скінченні поля, а не кільця, оскільки в скінченному полі його мультиплікативна група завжди циклічна і це дає змогу використовувати в скінченних полях функцію дискретного логарифма.

Оскільки порядок мультиплікативної групи кільця дорівнює $\varphi(k)$, то порядок кільця k буде максимальним тоді, коли $\varphi(k)$ — просте число. У цьому разі мультиплікативна група дільників кільця проста і за теоремою Лагранжа циклічна, тобто буде породжуватися довільним своїм елементом. Задовольняють цю умову числа 3, 4, 6 ($\varphi(3) = \varphi(4) = \varphi(6) = 2$). Інших таких чисел не існує. Дійсно, якщо

$k = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ — канонічний розклад числа $k > 6$ на прості множники, то $\varphi(k) = p_1^{s_1-1}(p_1 - 1) p_2^{s_2-1}(p_2 - 1) \dots p_r^{s_r-1}(p_r - 1)$ і тому $\varphi(k)$ не є простим числом.

Якщо такого числа не існує, то виникає запитання: яким умовам повинен задовольняти порядок кільця, щоб його мультиплікативна група була циклічною групою великого порядку? Відповідь на це запитання дає таке твердження.

Теорема 4 (Гауса). Мультиплікативна група кільця лишків Z_k буде циклічною тоді і тільки тоді, коли k дорівнюватиме 2, 4, p^s або $2p^s$, $s \geq 1$, p — непарне просте число [5].

Звідси випливає, що мультиплікативна група кільця $AKK1_{25}$, яке ізоморфне примарному кільцю Z_{25}, буде циклічною, оскільки $k = 25 = 5^2$ задовольняє умови теореми 4 і порядок цієї групи дорівнює $\varphi(25) = 20$. До того ж, відповідно до теореми 3 кількість твірних елементів у цій групі складатиме 8, оскільки $\varphi(20) = 8$.

Отже, потрібно вибрати порядок кільця $k = p^m$, де $m \geq 1$, p — непарне просте число, тобто в криптографічних застосунках слід використовувати примарні кільця. Наприклад, якщо $k = 5^{19}$, то його мультиплікативна циклічна група матиме порядок $\varphi(k) = 4 \cdot 5^{18} = 4 \cdot 1953125 > 2^{41}$. Для простої криптосистеми з одноразовим ключем такого порядку достатньо для обміну одноразовими повідомленнями. Отже, в примарних кільцях можна використовувати функцію дискретного логарифма, якщо вибирати порядок кільця на підставі теореми 4. Для порівняння, якщо поле має порядок $k = 5^{19}$, то його мультиплікативна група матиме порядок $k = 5^{19} - 1$, але побудова такого поля потребує значно більших затрат часу і пам'яті, ніж побудова кільця.

Можливість використання обох таблиць операцій кільця дає змогу краще приховати частоту появи символів у шифрограмі, використовуючи гомофони, які розглядалися в [3].

Розглянемо питання надійності такого алгоритму. Надійність розглянутого алгоритму найбільше залежить від кількості сюр'єкцій $g : G \to M$.

Якщо $k = m$, то кількість таких сюр'єкцій складатиме $m!$ і тоді наведений алгоритм — це деяка модифікація шифру Віженера, для якого відомі ефективні методи криптоаналізу [10, 11].

У випадку $k > m$ кожна сюр'єкція $g : G \to M$ породжує $m = |X|$ класів еквівалентності з $t = \lfloor k / m \rfloor$ (t — ціла частина дробу k / m) елементами в класі і $m!$ способами зіставлювання цих класів символам алфавіту. Тоді кількість методів шифрування повідомлення складає $S = D(k, m)(t(t+1)/2)$, де $D(k, m)$ — кількість сюр'єкцій k-ементної множини на m-елементну множину. Відомо, що значення $D(k, m)$ обчислюється за формулою $D(k, m) = \sum_{j=0}^{m} (-1)^j C_m^j (m - j)^k$ [9]. Навіть для невеликих k і m значення S зростає досить швидко. Наприклад, для $k = 9$, $m = 4$ маємо $S = 186480 \cdot 3 > 2^{19}$. Це число потрібно помножити на кількість способів вибору ключового слова p, яка дорівнює m^r де $m = |X|$, r — довжина слова p. У результаті отримаємо таку кількість способів шифрування повідомлення: $m^r \cdot S = m^r \cdot D(k, m) \cdot (t \cdot (t+1)/2)$, де r — довжина ключового слова p, $m = |X|$, $k = |G|$, а $(t(t+1)/2)$ — кількість різних пар, які можна побудувати із t елементів класу еквівалентності. Вибираючи порядок кільця досить великим,

отримуємо можливість суттєво приховати частоту входження символів у повідомленні. Для такого способу шифрування методи частотного криптоаналізу і гамування [10, 11] значно ускладнюються.

Приклад 2. Нехай символи алфавіту англійської мови упорядковані так само, як в прикладі 1, а кільце має порядок $k = 49 = 7^2$. Значення рядка T_+ [1, 49]) задано такою підстановкою:

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

Задаючи сюр'єкцію відображенням вигляду (1) з початковим значенням $m_1 = 7$ і модулем $m = 25$, знаходимо такі класи еквівалентності за правилом: порядковий номер класу елемента m_i дорівнює i за модулем 25:

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	
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

Скористаємося ізоморфізмами $\varphi : Z_{49} \to AKK1_{49}$ і $\varphi^{-1}: AKK1_{49} \to Z_{49}$ (таблиці відповідностей яких наведено в таблицях φ і φ^{-1}) для обчислення значень операцій у кільці Z_{49}:

Таблиця ізоморфізму φ

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

Таблиця ізоморфізму φ^{-1}

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

Тепер символам алфавіту можна ставити у відповідність різні значення з класів еквівалентності, які відповідають цим символам, і виконувати шифрування за допомогою наведених вище алгоритмів. Наприклад, для ключового слова **KUKU** і тексту **KUKURIKU**, який потрібно зашифрувати, отримаємо таку шифрограму:

K U K U K U K U
K U K U R I K U
48 36 24 18 24 36 48 36 — $\bar{p}\,\bar{b}$ цифрові відповідності ключового слова і тексту
\+ + + + + + + +
24 18 24 18 13 31 48 36 — $\bar{b}$ цифрові відповідності символів тексту
= = = = = = = =
0 43 9 25 34 20 38 30 — d (зашифрований текст), де символи тексту, що повторюються, приховані.

З наведених алгоритмів **RG-EN** і **RG-DE** випливає, що зміна початкового значення m_1 сюр'єкції g (наприклад, у відображенні (1)), ключового слова p і визначального рядка T[l, k], за яким будується кільце, досить проста. Порядок k кільця завжди можна вибрати таким, щоб він був кратним $m = |X|$ (це не завжди можна зробити для поля).

Залишається описати спосіб передавання трійки $(\mathrm{T}_+[1,k], g, p)$. Рядок $\mathrm{T}_+[1,k]$ задається вектором $(1, a_1, a_2, \ldots, a_{k-1})$, де $a_i = a_{i-1} + 1$, $a_0 = 1$, $i = 1, \ldots, k-1$. Сюр'єкція задається парою $(m_1, m_{i-1} + 1)$ (модуль k отримується з рядка $\mathrm{T}_+[1,k]$). Ключове слово p передається вектором $(\overline{p}) = (k_1, k_2, \ldots, k_r)$.

Хоча наведена оцінка способів побудови шифрованого тексту має високий порядок зростання і може використовуватися в системі з одноразовим ключем, але досліджений спосіб шифрування має недолік (автентифікація абонентів відсутня).

ВИКОРИСТАННЯ МОДЕЛІ МАТЕМАТИЧНОГО СЕЙФА

Для автентифікації абонентів у запропонованій криптосистемі скористаємося моделлю математичного сейфа [6]. Неформально під математичним сейфом (МС) розуміють таку систему $Z = (z_1, z_2, \ldots, z_n)$ взаємозв'язаних засувів, що коли виконується поворот ключа в одному із засувів, то такий же поворот виконується і у всіх засувах, зв'язаних з ним. МС може задаватися або за допомогою прямокутної матриці або за допомогою графу. Якщо МС задається матрицею, то її елементи відповідають засувам, а значення цих елементів — позиціям засувів, тобто у вигляді матриці $Z = ||z_{ij}||$, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Цей спосіб називають матричним сейфом. А коли МС задається графом, то його вершини відповідають засувам. Цей спосіб називають графовим сейфом. У матричному сейфі кожний засув z_{ij} зв'язаний з тими засувами, які розміщені в i-му рядку і в j-му стовпчику, а в графовому сейфі з засувом у вершині v_i зв'язаними вважаються засуви, які знаходяться у вершинах, суміжних з вершиною v_i. Кожен засув може знаходитись в одній із позицій, а кількість всіх таких позицій — скінченне число: $0, 1, \ldots, k-1$. Засув відімкнений, якщо він є в позиції 0. У довільній іншій позиції засув вважається замкненим. Початковий стан сейфа Z визначає матриця $A = ||a_{ij}||$ або граф $G(V, E)$ (орієнтований або неорієнтований). Якщо в якому-небудь засуві виконується поворот ключа, то всі засуви, зв'язані з цим засувом, збільшують значення своїх позицій на одиницю за модулем k.

Потрібно розв'язати таку задачу. Виходячи з початкового стану МС, знайти таку послідовність засувів і кількість поворотів ключа в них, щоб сейф перейшов у позицію відімкненого, тобто коли всі засуви знаходяться в позиції 0.

Розглянемо матричний сейф. Нехай матриця $X = ||x_{ij}||$ — шуканий розв'язок задачі, де x_{ij} — кількість поворотів ключа в засуві z_{ij}. Позначимо $x = (x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{m1}, \ldots, x_{mn})$ вектор-стовпчик, отриманий з матриці X послідовним записом її рядків. Аналогічно з матриці A початкових станів засувів отримуємо вектор-стовпчик a. Тоді розв'язання задачі про математичний сейф зводиться до розв'язання системи лінійних однорідних рівнянь (СЛОР) за модулем k, що має вигляд $Bx + a \equiv 0 \pmod{k}$, де матриця B має розмір $mn \times mn$ і коефіцієнти 0 і 1 (див. матрицю B' з прикладу 3). Ускладнимо задачу: будемо шукати розв'язок задачі про МС, розв'язуючи СЛОР вигляду $Bx + a - c \equiv 0 \pmod{k}$, в скінченному кільці типу $AKK1_k$. Це означає, що числовою областю, над якою задано МС, є кільце $AKK1_k$, побудоване наведеним вище способом, а сейф відімкнутий, коли позиції засувів дорівнюють значенням вектора c. Деталі про МС можна знайти в роботі [7].

Використання моделі МС дає змогу організувати процес автентифікації абонентів (причому обох), які обмінюються повідомленнями. Дійсно, автентифікацію можна організувати у такий спосіб: надіслати абоненту пару $(\mathrm{T}_+[1,k], c)$; отримати від нього розв'язок, який повинен відмикати сейф. При

цьому кільце, в якому розв'язується задача про МС, не обов'язково повинно бути кільцем G_k, воно може бути довільним скінченним кільцем або полем. Якщо цей розв'язок відмикає сейф, то абонент легальний, інакше абонент хибний. Отримання підтвердження легальності абонента за одержаним розв'язком уможливлює доступ абонентам до параметрів алгоритма RG-EN для виконання шифрування.

Отже, алгоритми **RG-EN** і **RG-DE** перетворюються в такі алгоритми.

RGM-EN($\mathrm{T}_+ [1, k_1]$, c)

1. Надіслати закритим каналом рядок $\mathrm{T}_+ [1, k_1]$ і вектор c, які визначають кільце $AKK1_k$ (або параметри поля, де розв'язується задача про МС) і комбінацію, що відмикає сейф.

2. Надіслати відкритим каналом вектор a.

3. Отримати розв'язок d задачі про МС в кільці $AKK1_{k1}$. Якщо d відмикає сейф, то виконати крок 4, інакше СТОП («нелегал у мережі»).

4. Виконати алгорим **RG-EN**($\mathrm{T}_+ [1, k]$, g, p) і надіслати абоненту дозвіл на роботу.

RGM-DE($\mathrm{T}_+ [1, k_1]$, c)

1. За отриманим рядком $\mathrm{T}_+ [1, k_1]$ побудувати кільце $AKK1_k$.

2. За отриманими векторами a і c розв'язати систему $Bx + a - c \equiv 0 \pmod{k}$ в кільці $AKK1_k$ і знайти розв'язок d.

3. Надіслати отриманий розв'язок d абонету, від якого отримано параметри ($\mathrm{T}_+ [1, k_1]$, c).

4. Якщо дозвіл на роботу від абонента отриманий, то (йому відкривається доступ до шифрограми) виконати алгоритм **RG-DE**($\mathrm{T}_+ [1, k]$, g, p).

Приклад 3. Розглянемо роботу алгоритмів шифрування і розшифрування з використанням моделі МС. Нехай МС заданий матрицею A, за якою будується СЛОР $Bx + a = c \pmod{25}$, де

$$A = \begin{pmatrix} 9 & 7 & 12 & 4 & 5 & 21 \\ 5 & 4 & 2 & 17 & 20 & 20 \end{pmatrix}.$$

Матриця системи B, розширена останнім стовпчиком $a - c$, набуває вигляду:

$$B' = \left| \begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \mathbf{21} \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \mathbf{12} \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & \mathbf{11} \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & \mathbf{6} \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & \mathbf{12} \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \mathbf{18} \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \mathbf{23} \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \mathbf{22} \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \mathbf{0} \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \mathbf{14} \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & \mathbf{21} \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \mathbf{13} \end{array} \right|.$$

Розв'язуємо систему $Bx + a = c \pmod{25}$ з параметрами $a = (9, 7, 12, 4, 5, 21, 5, 4, 2, 17, 20, 20)$, $c = (16, 12, 4, 10, 21, 20, 7, 5, 2, 20, 2, 7)$ в кільці $AKK1_{25}$ з прикладу 1. Переносимо стовпчик вільних членів у ліву частину і, виконуючи операції віднімання в кільці $AKK1_{25}$, отримаємо систему неоднорідних лінійних рівнянь

$B'x = d' \pmod{25}$. Розв'язком цієї системи є вектор $d = (21, 12, 19, 24, 23, 8, 13, 11, 12, 1, 11, 5)$, який надсилається абоненту, від якого отримано рядок $T_+[1, 25]$ і вектор c. Якщо надісланий вектор d відмикає сейф (що означає легальність отримувача), то потім відправник виконує крок 4 алгоритму **RGM-EN**$(T_+[1, k], g, p)$ і надсилає абоненту дозвіл на подальшу роботу. Одержаний розв'язок для отримувача означає легальність відправника. Отримувач має доступ до шифрограми.

Зауважимо, що для сумісності системи лінійних рівнянь потрібним є виконання умови, щоб сума коефіцієнтів рядків матриці B' за модулем k не дорівнювала нулю, а сума координат вектора d' дорівнювала нулю і навпаки. Ця умова є достатньою для сумісності системи.

У цьому випадку слабким місцем автентифікації є те, що матриця B' системи $Bx + a = c$ має стандартний вигляд, що спрощує роботу криптоаналітику. Для того щоб уникнути цього недоліка, краще задавати математичний сейф на графах, оскільки в такому разі структура матриці залежитиме від топології графу і тому може бути довільною. Топологія графу передається вектором списків суміжності вершин графу, довжина якого не перевищує $2|E|$, де $|E|$ — кількість ребер графу.

Приклад 4. Розглянемо МС, заданий наведеним на рис. 1 неорієнтованим графом, вектор списку суміжних вершин якого має вигляд (**1**:2, 4, 11; **2**:8; **3**:5, 9; **4**:7, 10; **5**:12; **6**:7, 9; **7**:8; **9**:12; 1**0**:11), і параметрами a, c із прикладу 3.

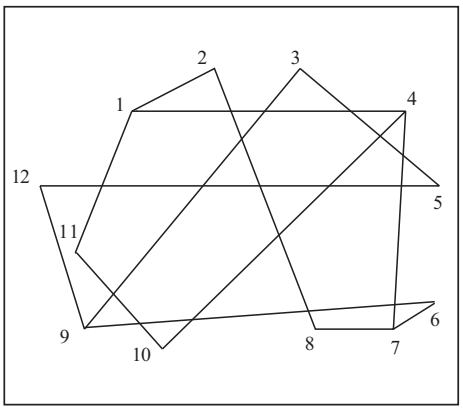

Рис. 1. Граф, який задає сейф

Матриця системи $Bx + a - c = 0$, для заданого таким графом сейфа, має вигляд:

$$B' = \begin{pmatrix} 1&1&0&1&0&0&0&0&0&0&1&0&21 \\ 1&1&0&0&0&0&0&1&0&0&0&0&12 \\ 0&0&1&0&1&0&0&0&1&0&0&0&11 \\ 1&0&0&1&0&0&1&0&0&1&0&0&6 \\ 0&0&1&0&1&0&0&0&0&0&0&1&12 \\ 0&0&0&0&0&1&1&0&1&0&0&0&18 \\ 0&0&0&1&0&1&1&1&0&0&0&0&23 \\ 0&1&0&0&0&0&1&1&0&0&0&0&22 \\ 0&0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&0&0&1&0&0&0&0&0&1&1&0&14 \\ 1&0&0&0&0&0&0&0&0&1&1&0&21 \\ 0&0&0&0&1&0&0&0&1&0&0&1&13 \end{pmatrix}.$$

Розв'язком цієї системи в кільці $AKK1_{25}$ є вектор (2, 1, 15, 14, 11, 19, 24, 15, 16, 8, 15, 18, 14), який після нормалізації (множення на коефіцієнт 3, оскільки $3 \cdot 14 = 1$) дає розв'язок $d = (9, 3, 21, 1, 6, 2, 10, 21, 5, 20, 21, 19)$, який відмикає сейф. Подальша робота виконується відповідно до наведених алгоритмів **RGM-EN**$(T_+[1, k_1], c)$ і **RGM-DE**$(T_+[1, k_1], c)$.

Отже, в цьому варіанті криптоаналітику серед іншого невідома також структура матриці B, що ускладнює його роботу. Можливі також варіації і з матрицею сейфа [7], одну з яких наведено далі в прикладі.

Приклад 5. Нехай задача про МС розв'язується в кільці за модулем 27 з матрицею початкових позицій засувів $A = \begin{pmatrix} 1&2&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$ і комбінацією, яка відкриває сейф, $c = \begin{pmatrix} 1&2&3 \\ 4&5&6 \\ 7&8&9 \end{pmatrix}$. А матриця B системи має вигляд

$$\begin{vmatrix} 1&1&1&3&0&0&2&0&0 \\ 1&1&1&0&3&0&0&2&0 \\ 1&1&1&0&0&3&0&0&2 \\ 1&0&0&3&3&3&2&0&0 \\ 0&1&0&3&3&3&0&2&0 \\ 0&0&1&3&3&3&0&0&2 \\ 1&0&0&3&0&0&2&2&2 \\ 0&1&0&0&3&0&2&2&2 \\ 0&0&1&0&0&3&2&2&2 \end{vmatrix}.$$

Це означає, що поворот ключа в засувах першого рядка змінить значення позиції засувів на одиницю, поворот у засувах другого рядка змінить позиції засувів на три одиниці, а третього рядка — змінить позиції засувів на дві одиниці. Тоді система лінійних неоднорідних Діофантових рівнянь (СЛНДР) $Bx + a \equiv c \pmod{27}$ набуває вигляду

$$Bx + a = c \pmod{27} \to \begin{cases} 1\ 1\ 1\ 3\ 0\ 0\ 2\ 0\ 0\ 1 = 1 \\ 1\ 1\ 1\ 0\ 3\ 0\ 0\ 2\ 0\ 2 = 2 \\ 1\ 1\ 1\ 0\ 0\ 3\ 0\ 0\ 2\ 0 = 3 \\ 1\ 0\ 0\ 3\ 3\ 3\ 2\ 0\ 0\ 0 = 4 \\ 0\ 1\ 0\ 3\ 3\ 3\ 0\ 2\ 0\ 0 = 5 \\ 0\ 0\ 1\ 3\ 3\ 3\ 0\ 0\ 2\ 0 = 6 \\ 1\ 0\ 0\ 3\ 0\ 0\ 2\ 2\ 2\ 0 = 7 \\ 0\ 1\ 0\ 0\ 3\ 0\ 2\ 2\ 2\ 0 = 8 \\ 0\ 0\ 1\ 0\ 0\ 3\ 2\ 2\ 2\ 0 = 9 \end{cases} (\text{mod } 27).$$

Розв'язком цієї системи є вектор $x = (4, 5, 18, 20, 20, 7, 24, 24, 18)$, який не відмикає сейфа. Для того щоб цей розв'язок відкривав сейф, потрібно його перетворити таким чином:

- перші три координати, які відповідають коефіцієнтам 1, залишаються незмінними;
- другі три координати, які відповідають коефіцієнтам 3, помножити на три за модулем 27;
- треті три координати, які відповідають коефіцієнтам 2, помножити на два за модулем 27.

У результаті отримаємо розв'язок $d = (4, 5, 18, 6, 6, 21, 21, 21, 9)$, який відмикає сейф. Дійсно,

$$\begin{pmatrix} 1&2&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix} \to (x_{11} = 4) \begin{pmatrix} 5&6&4 \\ 4&0&0 \\ 4&0&0 \end{pmatrix} \to (x_{12} = 5) \begin{pmatrix} 10&11&9 \\ 4&5&0 \\ 4&5&0 \end{pmatrix} \to (x_{13} = 18) \begin{pmatrix} 1&2&0 \\ 4&5&18 \\ 4&5&18 \end{pmatrix} \to$$

$$\to (x_{21} = 6) \begin{pmatrix} 7&2&0 \\ 10&11&24 \\ 10&5&18 \end{pmatrix} \to (x_{22} = 6) \begin{pmatrix} 7&8&0 \\ 16&17&3 \\ 10&11&18 \end{pmatrix} \to (x_{23} = 21) \begin{pmatrix} 7&8&21 \\ 10&11&24 \\ 10&11&12 \end{pmatrix} \to$$

$$\to (x_{31} = 21) \begin{pmatrix} 1&8&21 \\ 4&11&24 \\ 4&5&6 \end{pmatrix} \to (x_{32} = 21) \begin{pmatrix} 1&2&21 \\ 4&5&24 \\ 25&26&0 \end{pmatrix} \to (x_{33} = 9) \begin{pmatrix} 1&2&3 \\ 4&5&6 \\ 7&8&9 \end{pmatrix}.$$

Наведений метод побудови криптосистеми можна покращити, якщо використовувати прямі добутки примарних кілець. Це уможливлює автентифікацію в одному кільці, шифрування в другому кільці, а обмін секретних даних в третьому кільці (яке, зокрема, може бути полем).

Отже, запропоновано спосіб побудови простої криптосистеми з урахуванням властивостей асоціативно-комутативних кілець з одиницею і моделлю математичного сейфа, заданого матрицею або графом.

Ця система має великий простір ключів, потрібний для її стійкості. Для побудови такої системи можна реалізувати (у разі потреби) алгоритми конструювання таблиць операцій кільця і пошуку розв'язків систем лінійних рівнянь $Bx + a = c$ в кільці $AKK1_k$. Знайдені розв'язки такої системи мають відмикати сейф, а це означає ідентифікацію абонентів, які обмінюються повідомленнями. З цією метою запропоновано алгоритми побудови таблиць операцій кільця з поліноміальною оцінкою складності, поліноміальні алгоритми розв'язання систем лінійних рівнянь в примарних кільцях і полях. Шифрування і розшифрування теж виконуються за поліноміальний час від величини порядку кільця (відповідні оцінки складності наведено в [7, 8]). Показано, що графовий сейф у криптографічному сенсі має певні переваги над матричним сейфом.

СПИСОК ЛІТЕРАТУРИ

1. Калужнин Л.А. Введение в общую алгебру. Москва: Наука, 1973. 447 с.
2. Кук Д., Бейз Г. Компьютерная математика. Москва: Наука, 1990. 384 с.
3. Кривий С.Л. Криптосистема на основі абелевих груп і кілець. *Проблемы программирования.* 2020. № 2-3. С. 270–277.
4. Коблиц Н. Курс теории чисел и криптографии. Москва: ТВП, 2001. 260 с.
5. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии, Москва: МЦНМО, 2002. 103 с.
6. Донец Г.А. Решение задачи о сейфе на (0, 1)-матрицах. *Кибернетика и системный анализ.* 2002. № 1. С. 98–105.
7. Крывый С.Л. Численные методы решения задачи о математическом сейфе. *Кибернетика и системный анализ*. 2019. Т. 55, № 5. С. 18–34.
8. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов. *Кибернетика и системный анализ*. 2007. № 6. С. 27–40.
9. Rosen K., Michaels J., Gross J., Grossman J., Shier D. (Eds.). Handbook of discrete and combinatorial mathematics. CRC Press, 2000. Ch. 2.4. P. 219.
10. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Санкт-Петербург: ИТМО, 2004. 109 с.
11. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Москва: Гелиос АРВ, 2001. 480 с.

S. Kryvyi

APPLICATION OF COMMUTATIVE RINGS WITH UNITY FOR CONSTRUCTION OF SYMMETRIC ENCRYPTION SYSTEM

Abstract. A method is proposed for constructing a symmetric cryptosystem based on the properties of finite associative-commutative rings with unity. Algorithms with polynomial time and memory complexity for constructing addition and multiplication tables for these rings are presented. Examples of using this system, as well as its extension by the model of a mathematical safe for subscriber identification are considered. Conditions for using the discrete logarithm function in rings are given. The advantages of the graph task of the safe in comparison with the matrix task are shown.

Keywords: associative-commutative ring, cryptosystem, mathematical safe, algorithm.

Надійшла до редакції 04.11.2021