УДК: 51.681.3

КРИПТОСИСТЕМА НА ОСНОВІ АБЕЛЕВИХ ГРУП І КІЛЕЦЬ

С.Л. Кривий[0000-0065-0736-4579]

Київський національний університет імені Т.Г. Шевченка м. Київ, просп. Глушкова, 4Д.

В роботі пропонується проста криптосистема на основі властивостей абелевих груп та асоціативно-комутативних кілець з одиницею. Приводяться алгоритми побудови таблиць додавання та множення для цих алгебр. Розглянуті приклади використання цієї системи, а також її розширення на випадок роботи з гомофонами. Показано яким чином природним способом знаходяться гомофони з ілюстрацією їх використання на простому прикладі повіломлення. Табл. 5. Бібліогр.: 3 назв.

Ключові слова: :абелева група, кільце, криптосистема, гомофон, алгоритм.

В работе предлагается простая криптосистема на основе свойств абелевых групп и ассоциативно-коммутативных колец с единицей. Приведены алгоритмы с квадратичной временной и квадратичной сложностью по памяти для построения таблиц сложения и умножения для этих алгебр. Рассмотрены примеры использования этой системы, а также ее расширение на случай работы с гомофонами. Показано каким образом естественным путем находятся гомофоны с иллюстрацией их использования на простом примере сообщения. Табл. 5. Библиогр.: 3 назв.

Ключевые слова: абелева группа, кольцо, криптосистема, гомофон, алгоритм.

In the paper simple symmetric encryption system is proposed. This system is build on properties of abelian groups an associative-commutative rings with unit. To work in system is necessary to declare key row corresponding to addition with one element of group. Using this row full table of addition of group and full table of multiplication of ring are build. To build groups and rings of larger orders are used operations of direct sum for abelian groups or direct multiply for rings. After definition a correspondence between elements of group or ring and symbols of alphabet. In the paper used a group with complete cycle. Group is called with complete cycle if the key row includeof their elements. All finite groups with complete cycle are isomorphic. The set of all groups of the same orders are equal (/k-2/)!.Having taken key word and using the correspondence between elements of ring and symbols of alphabet is build security message. If we used ring for encryption then we can used two tables of ring and do coding in interleaving manner (one code take from table of addition and next code from table of multiplication). Such approach makes practical impossible using of frequency method. Showed that In such systems space of keys is (/k-2/)!/k/!, where /k/ is power of alphabet (it is order of group or ring).The complexity of algorithms for building group and ring are O(/k^2 /) and the same complexity of encryption and decoding. The guarantee of unambiguous decoding is a well-known property: the mapping of the set A to the set B determines the equivalence relation on the set A. The elements of the partition classes according to this equivalence relation are the homophones of the letters of the alphabet.The work of algorithms isdemonstrated on example group's order25. The equivalents can be different homophones and can then be used in a rotational random manner. In the general case, the homophones of the alphabet symbol, which corresponds to the element of the table m, will be such pairs i, j of the elements of the table of addition (multiplication), which satisfy the condition i + j = m (i · j = m). In this case, if the pair i, j is already selected as a homophone, then the pair j, i should not be taken as a homophone (symmetry of the occurrence of numbers - a hint to the cryptanalyst). All homophones in the addition table will be k, and in the multiplication table □□ (k), where φ is the Euler function. Another possibility to encryption is using the tables of ring for building of gomophones for symbols of alphabet.

Key words: abelian group, ring, encryption system, gomofon, algorithm.

1. Необхідні означення та поняття

В роботі пропонується проста криптосистема, яка побудована на властивостях скінченних абелевих груп та асоціативно-комутативних кілець з одиницею [1, 2].

Нехай задана деяка скінченна множина цілих чисел, наприклад, $N_5 = \{0,1,2,3,4\}$. Оскільки потрібно побудувати адитивну абелеву групу, то ця група обов'язково повинна включати 0. Для того, щоб N_5 перетворити в групу GN_5, необхідно коректно задати значення для операції додавання з одним із елементів групи, скажімо з 1 [3]. Дійсно, оскільки $a + 0 = a$ для довільного $a \square GN_5$, то перший рядок таблиці додавання елементів групи визначений (табл. 1), а на підставі комутативності (оскільки група абелева) і перший стовпчик цієї таблиці. Нехай, наприклад, задано $0 + 1 = 1$, $1 + 1 = 4$, 1+4=2, 1+2=3, 1+3 = 0. Таке означення коректне, оскільки має місце однозначність результату (але однозначність результату не достатня умова гарантії коректності). Тепер послідовно знаходимо результати додавання з елементом 1+1=4, що дає змогу знайти результати додавання елементів групи з елементом 4:

4+2=(1+1)+2=1+(1+2)=1+3=0, 4+3=(1+1)+3=1+(1+3)=1, 4+4=(1+1)+4=1+(1+4)=1+2=3.

Далі знаходимо значення 4+1=2 і обчислюємо операцію додавання з елементом 2:

2+2=(1+4)+2=1+(4+2)=1+0=1, 2+3=(1+4)+3=1+(4+3)=1+1=4, 2+4=(1+4)+4=1+(4+4)=1+3=0.

Далі знаходимо значення 2+1=3 і обчислюємо операцію додавання з елементом 3:

3+2=(1+2)+2=1+(2+2)=1+1=4, 3+3=(1+2)+3=1+(2+3)=1+4=2, 3+4=(1+2)+4=1+(2+4)=1+0=1.

Заносимо ці значення в таблицю 2 і на цьому закінчуємо побудову групи GN_5.

Варто зауважити, що для визначення групи можна взяти довільний її елемент, а не обов'язково одиницю. Наприклад, якщо задано такий рядок додавання з елементом 3: $3+0=3$, $3+1=4$, $3+2=1$, $3+3=2$, $3+4=0$, то за цим рядком дістаємо таблицю 3.

Для побудови абелевої групи GN_k, мало вимагати тільки однозначності операції додавання. Якщо визначити додавання в групі так $0+1=1$, 1+1=0, 1+2=3, 1+3=4, 1+4=2, то, обчислюючи 1+3, отримаємо 1+3 =1+(1+2)=(1+1)+2=0 + 2 = 2, що не збігається з визначеним вище. Справа в тім, що так визначена операція додавання не охоплює весь цикл елементів групи, тому що має елемент скінченного порядку $2<5$ (1+1=0). Обидві групи, побудовані вище, циклічні на підставі теореми Лагранжа (вони мають простий порядок 5). Неважко переконатися, що ці групи ізоморфні. Дійсно, бієктивне відображення для перших двох груп має вигляд: $f(0)=0$, $f(1)=1$, $f(4)=3$, $f(2)=4$, $f(3)=2$.

Таблиця 1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	3			
3	3	0			
4	4	2			

Таблиця 2

+	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	3	1	4	0
3	3	0	4	2	1
4	4	2	0	1	3

Таблиця 3

+	0	1	2	3	4
0	0	1	2	3	4
1	1	3	0	4	2
2	2	0	4	1	3
3	3	4	1	2	0
4	4	2	3	0	1

Поставимо у відповідність операції додавання з елементом групи a_1, за допомогою якого визначається група, підстановку

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

Ця підстановка означає, що $f_{a_1}(0)=0+a_1=a_1$, $f_{a_1}(a_1)=a_1+a_1=a_{i1}$, $f_{a1}(a_{i1})=a_{i1}+a_1=a_{i2}$,…, $f_{a1}(a_{k-1})=a_{ik-1}+a_1=a_{ik}$, $f(a_{ik})=a_{ik}+a_1=0$. Назвемо групу GN_k *повноциклічною*, якщо підстановка f_{a1} є повним циклом довжини k. Наприклад, групи, представлені таблицями 2 і 3, повноциклічні. Справедлива

Теорема 1. Всі скінченні повноциклічні абелеві групи одного і того порядку ізоморфні між собою.

Доведення очевидним чином випливає з того, що коли дві підстановки f_{a1} і f_{b1} двох k-повноциклічних груп визначають ці групи, то ізоморфізмом буде відображення

$$f(0)=0,\ f(a_1)=b_1,\ f(a_{i1})=b_{b1}(b_1)=b_{i1},$$

$$f(a_{i2})=f(a_{i1}+a_1)\ =\ b_{i1}+\ b_1, f(a_{ij})=f(a_{ij-1})+b_1,\ f(a_{ij})=f(a_{ij-1})+b_1,$$

де $j=2,\dots,k$.

Асоціативно-комутативні кільця з одиницею. Ця алгебра будується шляхом розширення сигнатури операцій та множини тотожних співвідношень для цих операцій.

Універсальна алгебра G(A, Ω) називається *асоціативно-комутативним кільцем з одиницею,* якщо вона є

а) абелевою групою відносно додавання;

б) абелевою напівгрупою з одиницею відносно операції множення;

Операції додавання і множення задовольняють закон дистрибутивності, тобто для довільних елементів x, x', x' справедлива тотожність $x(x'+x'')=(xx')+(xx'')$. Це означає, що Ω включає чотири операції: бінарні

операції додавання і множення, унарну операцію взяття оберненого відносно операції додавання і нульарну операцію, яка фіксує нульовий елемент абелевої групи кільця. Цей нульовий елемент називається нулем кільця.

2. Криптографічна система на основі груп і кілець

При побудові абелевої групи була знайдена таблиця Келі для операції додавання. Ця таблиця дозволяє розширити таку побудову і на операцію множення.

Розглянемо як можна побудувати за групою GN_6, яка задана нижченаведеною табл. 4, асоціативно-комутативне кільце з одиницею KGN_6. Роль одиниці буде відігравати 1. На підставі аксіом кільця з одиницею дістаємо: для довільного елемента a із GN_5 $a \cdot 0 = 0 \cdot a = 0$, $a \cdot 1 = 1 \cdot a = a$. Таким чином, два рядки і два стовпчики таблиці множення визначені. Далі, за таблицею додавання і законом дистрибутивності знаходимо таблицю для операції множення. Дійсно, оскільки 1+1=3, то

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

Далі, оскільки 1+3=5, то дістаємо:

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

За таблицею додавання 5+1 = 4 і це дає змогу знайти значення операції множення з елементом 4, з елементом 2=1+4 решту елементів табл. 4. Оскільки 1+2=0, то це означає, що вся таблиця множення побудована. Із симетричності таблиці випливає, що операція множення елементів KGN_6 задовольняє закон комутативності. Легко перевірити, що ця операція задовольняє також закон асоціативності, тобто KGN_6 – асоціативно-комутативне кільце з одиницею (табл. 5).

Таблиця 4

+	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 5

*	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

Нехай операція додавання визначена для елемента групи a. Тоді в загальному випадку для побудови комутативного кільця KGN_k з одиницею, порядок якого k, необхідно задекларувати два двомірні масиви T_+ і Т. розмірності $k \times k$ і виконати такі алгоритми:

ADD-TAB-KG (a,k)

0) Занести в T_+ перший рядок і стовпчик результати додавання з нулем кільця;

1) Занести в T_+ рядок, де визначаються результати додавання з елементом a (задати ключ);

2) Покласти $c = a$;

3) Взяти в T_+ елемент $c' = c + a$;

4) Для всіх x занести в T_+ суми $c' + x = (c + a) + x = c + (a + x)$;

5) Покласти $c = c'$, $c' = c + a$; Якщо $c' = 0$, то СТОП, інакше на крок 4).

MUL-TAB-KG (l,k)

0) Занести в Т. рядки і стовпчики з результатами множення на 0 і на 1;

1) Покласти $c = 1$;

2) Взяти в T_+ елемент $c' = c + 1$;

3) Для всіх x занести в Т. добутки $c' \cdot x = (c+1) \cdot x = c \cdot x + x$;

4) Покласти $c = c'$; $c' = c + 1$; Якщо $c' = 0$, то СТОП, інакше на крок 3).

Складність першого алгоритму $O(k^2)$, а другого $O(k^3)$, де k – порядок кільця (групи).

Правильність цього алгоритму випливає з того, що всі елементи $c_1 = a + a$, $c_2 = c_1 + a$, …, $c_k = c_{k-1} + a$ пробігають всі елементи абелевої групи на підставі того, що рівняння $a + x = b$ в групі має єдиний розв'язок. З цих побудов випливає такий спосіб шифрування з використанням властивостей кільця:

RG-EN(k)

1) Будуємо кільце (або тільки групу) порядку $k > 26$;
2) Задаючи бієкцію f між елементами кільця (або групи) і символами алфавіту, виконуємо шифрування тексту T . Шифрування можна виконувати з використанням однієї з таблиць, або з використанням обох таблиць.

RG-DE(T)

1) Розшифрування виконується в зворотному порядку: знаходимо значення f^{-1} на символах шифрограми; потім на основі таблиць кільця повністю дешифруємо отриманий текст (див. нижченаведений приклад).

Розглянемо питання стійкості даного алгоритму та надійності. Оскільки при визначенні групи GN_k повинні породжуватися всі елементи, то простір ключів, як випливає з теореми 1, складатиме $(k-2)!$ варіантів. Дійсно, кількість способів, якими можна задати ключ, дорівнює кількості ізоморфізмі групи k -го порядку а це кількість способів упорядкування $(k-2)$ -елементної множини (два елементи 0 і 1 мають фіксовані позиції). Далі, приписування номерів символам алфавіту може виконуватися $n!$ способами , де n – кількість символів алфавіту. Отже, простір ключів має розмір $(k-2)!n!$.

Наприклад, якщо розглядається група з 25 елементів, то такого простору $(23!\cdot 25!)$ вибору ключів достатньо для забезпечення хорошої стійкості шифру.

Побудову групи або кільця, наприклад, KGN_{25} , маючи в розпорядженні групу порядку GN_5 , можна виконати шляхом застосування операції прямого добутку кілець або прямої суми груп $GN_{25} = GN_5 \oplus GN_5$, операції додавання і множення в яких виконуються покомпонентно, тобто

$$(a,b)+(c,d) = (a+c,\ b+d), \qquad (a,b)*(c,d) = (a\cdot c,\ b\cdot d).$$

Приклад 1. Розглянемо на прикладі групи (яка є прямою сумою абелевих груп $GN_{25} = GN_5 \oplus GN_5$) кільця KGN_{25} застосування алгоритму шифрування і дешифрування.

Нехай літери алфавіту англійської мови перенумеровані таким чином:

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
c	b	a	f	e	d	i/j	h	g	m	l	k	p	O	n	s	r	q	v	u	t	y	x	w	z

Група AGN_{25} має вигляд:

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

Мультиплікативна група MGN_{25} кільця KGN_{25}:

Необхідно зашифрувати в цій групі текст «UKRPROGtwenty». Для цього вибираємо ключове слово

	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

«IPRSP» і знаходимо пари літер та їх числові відповідники в таблиці додавання, які знаходяться на перетині відповідного рядка і стовпчика. Дістаємо 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	
6	**12**	**16**	**15**	**12**	**19**	**11**	**16**	**12**	**12**	**13**	**8**	**20**	– цифровий відповідник ключового слова і тексту;
+	+	+	+	+	+	+	+	+	+	+	+	+	
19	**11**	**16**	**12**	**16**	**13**	**8**	**20**	**23**	**4**	**14**	**20**	**21**	– цифровий відповідник тексту;
=	=	=	=	=	=	=	=	=	=	=	=	=	
12	**8**	**15**	**2**	**11**	**6**	**17**	**19**	**21**	**22**	**2**	**23**	**13**	– **T (**шифрограма цифрова) (сума відповідників);
p	**g**	**s**	**a**	**e**	**i**	**q**	**u**	**y**	**x**	**b**	**w**	**o**	– **T (**шифрограма літерова).

Розшифрування відбувається в зворотному напрямку. Абоненту, якому адресована ця шифрограма, відомий ключ таблиці додавання і ключове слово «IPRSP». Виписуємо цифрову шифрограму і цифрові значення ключового слова; за першим символом *a* ключового слова знаходимо символ, який є першим символом шифрограми в таблиці додавання групи (в прикладі за символом $a = 6$ знаходимо значення $b = 12$, тобто розв'язуємо рівняння $a + x = b$); за знайденим значенням в стовпчику, що відповідає цьому значенню *b*, знаходимо відповідник (у прикладі це число $x = 19$, якому відповідає символ ***u***); цей цикл повторюється доти, доки не буде знайдено весь текст повідомлення.

12	**8**	**15**	**2**	**11**	**6**	**17**	**19**	**21**	**22**	**2**	**23**	**13**
6	**12**	**16**	**15**	**12**	**19**	**11**	**16**	**12**	**12**	**13**	**8**	**20**
U	K	R	P	R	O	G	t	w	e	n	t	y

Наведений в прикладі текст можна зашифрувати, використовуючи таблицю множення. Ця обставина дозволяє використовувати одночасно дві таблиці для шифрування, тобто одній парі літер ставимо у відповідність елемент таблиці додавання, а наступній парі літер, яка повторюється, – відповідник з таблиці множення (тобто відповідником буде елемент $m = i \cdot j$). Але це можливо лише у випадку, коли один з елементів добутку є дільником одиниці в кільці KGN_k . Відомо, що множина дільників одиниці є абелевою групою в такому кільці [1]. У випадку скінченного асоціативно-комутативного кільця з одиницею, адитивна група якого є повноциклічною, легко знайти дільники нуля і їх кількість. Це випливає з такої теореми.

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

Доведення. Розглянемо Z_k – кільце лишків за модулем *k*. Неважко переконатися в тому, що адитивна група цього кільця є повноциклічною групою. Дільниками одиниці в цьому кільці будуть елементи, які взаємно прості з модулем кільця k , а кількість таких елементів, як відомо, дорівнює значенню функції Ойлера $\varphi(k)$. На підставі теореми 1 існує ізоморфізм між кільцем лишків Z_k і кільцем KGN_k , який є продовженням ізоморфізму між адитивними групами цих кілець. Звідси випливає справедливість твердження теореми.

Ілюстрацією теореми 2 є кільце KGN_6 , задане вищенаведеними табл. 4 і 5. Оскільки кільце лишків за модулем 6 має єдиний елемент 5, який взаємно простий з модулем 6, а цьому елементу при ізоморфізмі відповідає елемент 2, то з таблиці 5 легко побачити, що 2 – дільник одиниці. На підставі теореми 1 побудову таблиці множення можна не приводити, а використати ізоморфізм $f\colon Z_{25} \to KGN_{25}$. Дійсно, таблиця відповідностей має вигляд:

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

Дільниками нуля в цьому кільці лишків є елементи 5,10,15, 20. Цим елементам в кільці KGN_{25} відповідають елементи 2,9,18,19. Решта елементів цього кільця – дільники одиниці, які утворюють абелеву мультиплікативну групу цього кільця. Отже, для знаходження добутку, наприклад, елементів 6 і 7, знаходимо добуток їх відповідників 2 і 9 в кільці лишків 18 = 18 (mod 25). Тоді в кільці KGN_{25} відповідником є елемент $f(18) = 14$. Отже, 6·7=14 в кільці KGN_{25} .

Неважко переконатися, що породжуючими елементами цієї мультиплікативної групи є елементи 5, 6, 8,12,13,15, 22, 24. Це випливає з такої теореми.

Теорема 3. Якщо мультиплікативна група дільників одиниці асоціативно-комутативного кільця з одиницею має твірний елемент g, то твірними елементами цієї групи будуть елементи g^j такі, що $\text{НСД}(j,\varphi(k))=1$ [5].

Дійсно, в нашому прикладі мультиплікативної групи кільця KGN_{25} маємо:

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

а також

5^1=6^3, 5^2 = 17, 5^3=13, 5^4=20, 5^5=14, 5^6=16, 5^7=6, 5^8=21, 5^9=8, 5^{10}=23,
5^{11}=12, 5^{12}=11, 5^{13}=15, 5^{14}=10, 6^{15}=3, 5^{16}=4, 5^{17}=22, 5^{18}=7, 5^{19}=24, 5^{20}=1.

Отже, в цій групі можна застосувати функцію дискретного логарифму для шифрування повідомлень та передачі ключів. Наприклад, порівняння $6^x = 20 \pmod{25}$ має розв'язок $x=12$, а $5^x = 24 \pmod{25}$ має розв'язок $x=19$.

Основною перешкодою використання дискретного логарифму в кільцях є те, що не завжди його мультиплікативна група буде циклічною. Наприклад, в кільці лишків за модулем k=16, маємо $\varphi(k)=8$ і дільниками одиниці будуть елементи 1,3,5,7,9,11,13,15. Ці елементи мають порядок 2 або 4 і тому група дільників одиниці не буде циклічною. Це одна з причин того, що в криптографії застосовуються скінченні поля а не кільця, оскільки в скінченному полі його мультиплікативна група завжди циклічна. Ця обставина дозволяє використовувати в скінченних полях функцію дискретного логарифму.

Виходячи з того, що порядок мультиплікативної групи кільця дорівнює $\varphi(k)$, то звідси випливає, що найкращий порядок кільця k буде тоді, коли $\varphi(k)$ просте число. В цьому випадку мультиплікативна група дільників кільця проста і тому на підставі теореми Лагранжа буде циклічною, тобто породжуватиметься довільним своїм елементом. Але **автору невідомо існування такого числа** k!.

Якщо такого числа не існує, то потрібно вибрати число k таким, щоб у розкладі числа $\varphi(k)$ на прості множники був великий простий дільник. Така ситуація буде мати місце тоді, коли $\varphi(k)=2r$, де r – просте число. Наприклад, якщо $k=9$, то $\varphi(9)=6=3\cdot 2$ і тоді мультиплікативна група цього кільця матиме циклічну підгрупу 3-го порядку. Зрештою при шифруванні в разі потреби можна використовувати довільну циклічну підгрупу мультиплікативної групи дільників кільця KGN_k.

Можливість використання обох таблиць операцій кільця дозволяє краще «розчинити» частоту появи двознаків у шифрограмі.

Шифри гомофонічні. Відомо, що моноалфавітні шифри ламаються методом частотного аналізу, тоді запобігти такому криптоаналізу можна відображенням однієї літери в декілька її образів, які називаються *гомофонами* [4]. Кількість гомофонів для кожної літери повинна бути пропорціональна частоті появи цієї літери в явному тексті. Якщо гомофони використати ротаційно, то можна сподіватися, що частота появи літер не буде ідентична і це призведе до неможливості використання частотного криптоаналізу. Ідею застосування гомофонів приписують Карлу Гаусу (гомофонічний шифр ілюструє приклад 2). В гомофонічних шифрах частотний аналіз стає неможливим, але частота появи комбінацій сусідніх літер дає можливість застосувати цей тип аналізу. Сусідня пара літер називається двознаком. В англійській мові маємо 676 різних двознаків, з них 18 становить більше 25 % тексту. Таким чином, гомофони теж проявляють частоту появи літер і атака методом частотного аналізу стає можливою, але використання гомофонів значно ускладнює роботу криптоаналітика.

Приклад 2. Застосуємо гомофонічний шифр до шифрування тексту «kukuriku» з ключовим словом «kuku». Шифрування відбувається на основі таблиці гомофонів, взятих з таблиці додавання вищенаведеної групи :

Символ	**Гомофони адитивні**	**Гомофони мультиплікативні**
K –	0402, 0310, 1216, 1522, 2417;	1101, 1205, 2415, 1723;
U –	0209, 0117, 0902, 1224;	0802, 0709, 0502, 0207;
R –	1511, 0709, 1206;	0312, 0423, 1921, 2418;
I –	0318, 0420, 1121, 1317.	0311, 0807, 0514, 2322.

Ключове слово:	**K**	U	K	U	K	U	K	U
	0402	0209	1216	0117	0310	1424	1522	1424
Текст відкритий:	K	U	K	U	R	I	K	U
	1522	1424	0310	0209	1206	0209	0310	0117
Шифрограма:	1608	2203	2322	0423	2304	2203	1806	1611

Гарантією однозначного розшифрування є добра відома властивість: *відображення множини A на множину B визначає на множині A відношення еквівалентності.* Елементами класів розбиття за цим відношенням еквівалентності є гомофони літер алфавіту.

Відповідниками можуть бути різні гомофони і їх можна далі застосовувати ротаційно випадковим чином. В загальному випадку гомофонами символу алфавіту, якому відповідає елемент таблиці m, будуть такі пари i, j елементів таблиці додавання (множення), які задовольняють умову $i + j = m$ $(i \cdot j = m)$. При цьому, якщо пара i, j вже вибрана гомофоном, то пару j, i не варто брати гомофоном (симетрія входження цифр – підказка криптоаналітику). Всіх гомофонів в таблиці додавання буде k, а в таблиці множення $\varphi(k)$.

Висновки

Запропонована проста криптосистема на основі властивостей абелевих груп і асоціативно-комутативних кілець з одиницею. Зауважимо, що при традиційно прийнятому порядку літер англійського алфавіту таблиця додавання кільця лишків Z_{25} буде відповідає таблиці шифру Віженера. Пропонована система має широкий простір ключів, що є достатнім для стійкості системи. Для побудови такої системи потрібно побудувати таблиці додавання і множення групи і кільця. З цією метою пропонуються алгоритми побудови цих таблиць з квадратичною оцінкою складності. Шифрування і розшифрування теж виконуються в квадратичному часі.

Література

1. Калужнин Л.А. Введение в общую алгебру. М.: Наука. 1973. 447 с.
2. Сергієнко І.В., Кривий С.Л., Провотар О.І. Алгебраїчні аспекти інформаційних технологій. К.: Інтерсервіс. 2018. 411 с.
3. Кук Д., Бейз Г. Компьютерная математика. М.: Наука. 1990. 384 с.
4. Menezes A., van Oorschot P., Vanstons S. Handbook of Applied Cryptography. CRC Press. 1996. 661 p.
5. Коблиц Н. Курс теории чисел и криптографии. М.: Изд-во ТВП. 2001. 260 с.

References

1. Kaluznin L.A. Introduction to general algebra. M.: Nauka. 1973. 447 p.
2. Sergienko I.V., Kryvyi S.L., Provotar O.I. Algebraic aspects of informational technologies. K.:Interservice. 2018. 411 p.
3. Cooke D.J., Bez H.E. Computer mathematics. Cambridge University Press. Cambridge. 1984. 384 p.
4. Menezes A., van Oorschot P., Vanstons S. Handbook of Applied Cryptography. CRC Press. 1996. 661 p.
5. Coblitz N. A course of number theory and cryptography. M.: ТВП. 2001. 260 p.

Одержано 17.02.2020

Про автора:

Кривий Сергій Лук'янович,
доктор фізико-математичних наук, професор,
професор Київського національного університету імені Т.Г. Шевченка.
Кількість наукових публікацій в українських виданнях – 201.
Кількість наукових публікацій в зарубіжних виданнях – 52.

h-index: Google Scholar – 14;
Scopus – 7.
http://orcid.org/0000-0065-0736-4579.

Місце роботи автора:

Київський національний університет імені Т.Г. Шевченка
м. Київ, просп. Глушкова, 4Д.
Телефон службовий: (044) 259-05-11.
E-mail: sl.krivoi@gmail.com.