Група ІПС-42, Гончарук Ангеліна Віталіївна

Тема: Алгебра **Варіант 25**

Текст для шифрування:

the conference will be chaired by mister nnn

Ключове слово:

interrupt

Завдання:

Зашифрувати і розшифрувати заданий текст, використавши властивості таких алгебр:

1. Групи підстановок;
2. Скінченні кільця;
3. Скінченні поля.

Описати хід виконання завдання.

Розв'язання

1. Групи підстановок

Текст для шифрування:

the conference will be chaired by mister nnn

Для шифрування та дешифрації в даному завданні було використано блоковий спосіб підстановки з використанням техніки підстановок:

шифрування слова $p = y_1y_2...y_m$ у алфавіті зі звичним порядком літер виконується таким чином:

- слово p розбивається на блоки по t символів кожний
- кожний символ у блоці перетворюється за допомогою підстановок $\alpha_1\alpha_2\ldots\alpha_t$, кожна з яких має вигляд:

$$\alpha_i(k) = k + j_i \ (mod\ 26),$$

де k – номер літери у алфавіті X, а $k + j_i\ (mod\ 26)$– її відповідник у алфавіті X при підстановці α_i, $i = 1, 2, 3, \ldots t$.

В заданому умовою слові використані маленькі букви латинського алфавіту, тому візьмемо латинський алфавіт та пронумеруємо від 0 до 25:

a	b	c	d	e	f
0	1	2	3	4	5
g	h	i	j	k	l
6	7	8	9	10	11
m	n	o	p	q	r
12	13	14	15	16	17
s	t	u	v	w	x
18	19	20	21	22	23
y	z				
24	25				

Оскільки в даному повідомленні ми маємо 3 однакові літери підряд, то три *ji*, наприклад: 7, 13, 3. Зашифруємо *p = the conference will be chaired by mister nnn:*

p	*k*	*ji*	*αi*	*q*
t	19	7	0	a
h	7	13	20	u
e	4	3	7	h
c	2	7	9	j
o	14	13	1	b
n	13	3	16	q
f	5	7	12	m
e	4	13	17	r
r	5	3	8	i
e	4	7	11	l
n	13	13	0	a
c	2	3	5	f
e	4	7	11	l
w	22	13	9	j
i	8	3	11	l
l	11	7	18	s
l	11	13	24	y
b	1	3	4	e
e	4	7	11	l
c	2	13	15	p
h	7	3	10	k
a	0	7	7	h
i	8	13	21	v
r	17	3	20	u
e	4	7	11	l
d	3	13	16	q
b	1	3	4	e
y	24	7	5	f
m	12	13	25	z
i	8	3	11	l
s	18	7	25	z
t	19	13	6	g
e	4	3	7	h
r	17	7	24	y

n	13	13	0	a
n	13	3	16	q
n	13	7	20	u

Отримаємо: the conference will be chaired by mister nnn

Дешифрація відбувається за формулою:

$$\alpha^{-1}(k) = \begin{cases} k - j_i, & \text{якщо } k - j_i \geq 0, \\ k - j_i + 26, & \text{якщо } k - j_i < 0. \end{cases}$$

q	*k*	j_i	$\alpha^{-1}{}_i$	*p*
a	0	7	19	t
u	20	13	7	h
h	7	3	4	e
j	9	7	2	c
b	1	13	14	o
q	16	3	13	n
m	12	7	5	f
r	17	13	4	e
i	8	3	5	r
l	11	7	4	e
a	0	13	13	n
f	5	3	2	c
l	11	7	4	e
j	9	13	22	w
l	11	3	8	i
s	18	7	11	l
y	24	13	11	l
e	4	3	1	b
l	11	7	4	e
p	15	13	2	c
k	10	3	7	h
h	7	7	0	a
v	21	13	8	i
u	20	3	17	r
l	11	7	4	e
q	16	13	3	d
e	4	3	1	b
f	5	7	24	y
z	25	13	12	m

l	11	3	8	i
z	25	7	18	s
g	6	13	19	t
h	7	3	4	e
y	24	7	17	r
a	0	13	13	n
q	16	3	13	n
u	20	7	13	n

Ми отримали початкове повідомлення.

2. Скінченні кільця

Текст для шифрування:

the conference will be chaired by mister nnn

2.9.4 Кільця

Ця алгебра будується шляхом розширення сигнатури операцій та множини тотожних співвідношень для цих операцій.

Означення 62. *Універсальна алгебра* $G(A, \Omega)$ *називається* **кільцем**, *якщо вона*

а) *абелева група відносно додавання;*

б) *групоїд відносно множення;*

в) *задовольняє закон дистрибутивності, тобто для довільних її елементів* x, x', x''

$$x(x' + x'') = (xx') + (xx''), \qquad (x + x')x'' = (xx'') + (x'x'').$$

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.

Множення у кільці зводиться, на підставі законів дистрибутивності, до множення елементів із X, яке виконується за правилом множення слів у групоїді.

Із законів 1) – 3) випливають співвідношення, які дає

Для виконання завдання було використано гомофонічний шифр.

a	b	c	d	e	f

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

Таблиця додавання кільця KGN_{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	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	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

Шифрування

Виконаємо підрахунок літер та задамо новий числовий показник:

p	*Кількість повторів*	*Новий числовий відповідник*
t	2	20
h	2	7
e	7	4
c	3	0
o	1	13
n	5	14
f	1	3
e		
r	3	16
e		
n		
c		
e		
w	1	23
i	3	6
l	2	10
l		
b	2	1
e		
c		
h		
a	1	2
i		
r		
e		
d	1	5
b		
y	1	21
m	1	9
i		
s	1	15
t		
e		
r		
n		

n		
n		

Приклад знаходження гомофонів:

	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	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	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

Заповнимо таблицю гомофонфів:

Символ	Гомофони						
t	1505	1801					
h	1520	1817					
e	1514	1811	0201	2407	1316	1316	0808
c	1513	1802	0218				
o	1523						
n	1502	1822	0215	2420	1304		
f	1516						
r	1504	1823	0217				
w	1511						
i	1517	1803	0224				
l	1521	1807					

b	1515	1804					
a	1512						
d	1518						
y	1508						
m	1524						
s	2012						

Підставимо дані:

p	*шифр*
t	1505
h	1520
e	1514
c	1513
o	1523
n	1502
f	1516
e	1504
r	1504
e	1811
n	1822
c	1802
e	0808
w	1511
i	1517
l	1521
l	1807
b	1515
e	0201
c	0218
h	1817
a	1512
i	1803
r	1823
e	2407
d	1518
b	1804
y	1508
m	1524
i	0224

s	2012
t	1801
e	1316
r	0217
n	0215
n	2420
n	1304

Зашифрований текст:

150515201514 151315231502151615041504181118221802080815111517152118071515020 102181817151218031823240715181804150815240224201218011316021702152420130 4

Дешифрація

Дешифрація винонується за допомогою таблиці гомофонів, виконавши дії вище наоборот:

шифр	*p*
1505	t
1520	h
1514	e
1513	c
1523	o
1502	n
1516	f
1504	e
1504	r
1811	e
1822	n
1802	c
0808	e
1511	w
1517	i
1521	l
1807	l
1515	b
0201	e
0218	c
1817	h
1512	a

1803	i
1823	r
2407	e
1518	d
1804	b
1508	y
1524	m
0224	i
2012	s
1801	t
1316	e
0217	r
0215	n
2420	n
1304	n

Розшифрований текст: the conference will be chaired by mister nnn

3. Скінченні поля

Текст для шифрування:

the conference will be chaired by mister nnn

Ключове слово:

interrupt

Додамо до таблиці з алфавітом із завдання 1 ще один символ – *« »(пробіл)*

a	b	c	d	e	f
0	1	2	3	4	5
g	h	i	j	k	l
6	7	8	9	10	11
m	n	o	p	q	r
12	13	14	15	16	17
s	t	u	v	w	x
18	19	20	21	22	23
y	z				
24	25	26			

Щоб зашифрувати текст «the conference will be chaired by mister nnn» використаємо ключ «interrupt» та «Адитивна група поля $F_3{}^3$»

Адитивна група поля $F_3{}^3$

	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
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	25	26
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	23
3	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
4	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	19	22	23	21	25	26	24	19	20	18
5	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19
6	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
7	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
8	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
10	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
11	11	9	10	14’	12	13	17	15	16	20	18	19	23	21	22	26	24	25	22	0	1	5	3	4	8	6	7
12	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
13	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
14	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
15	15	16	171	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
16	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
17	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
18	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
20	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
21	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
22	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
23	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
24	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
25	25	26	24	19	20	18	22	23	21	7	8	6	1	0	2	4	5	3	16	17	15	10	11	9	13	14	12
26	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13

Шифрування

Для того, щоб зашифрувати текст, ми маємо повтрювати ключ навпроти тексту (символ до сивола) до закінчення тексту. Наступним етапом є виписання числових відповідників до літер тексту та літер ключа. Далі використовуємо «Адитивну групу поля $F_3{}^3$». Наприклад, якщо числовий відповідник (ЧВ) до літири ключа «і» дорівнює «8», а якщо числовий відповідник до літири тексту «t» дорівнює «19», то використовуюючи таблицю отримуємо в результаті їх перетин ЧВ «24», а саме результат шифрування – «у»:

	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
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	25	26
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	23
3	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
4	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	19	22	23	21	25	26	24	19	20	18
5	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19

6	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
7	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
8	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
10	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
11	11	9	10	14’	12	13	17	15	16	20	18	19	23	21	22	26	24	25	22	0	1	5	3	4	8	6	7
12	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
13	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
14	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
15	15	16	171	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
16	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
17	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
18	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
20	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
21	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
22	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
23	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
24	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
25	25	26	24	19	20	18	22	23	21	7	8	6	1	0	2	4	5	3	16	17	15	10	11	9	13	14	12
26	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13

Отже, заповнюємо таблицю описаним вище методом:

i	n	t	e	r	r	u	p	t	i	n	t	e	r	r	u	p	t	i	n	t	e	r	r
t	h	e		c	o	n	f	e	r	e	n	c	e		w	i	l	l		b	e		c
8	13	19	4	17	17	20	15	19	8	13	19	4	17	17	20	15	19	8	13	19	4	17	17
19	7	4	26	2	14	13	5	4	17	4	13	2	4	26	22	8	11	11	26	1	4	26	2
24	11	23	18	16	19	3	11	23	13	17	5	3	9	4	12	14	0	16	0	20	8	4	16
y	l	x	s	q	t	d	l	x	n	r	f	d	j	e	m	o	a	q	a	u	i	e	q

u	p	t	i	n	t	e	r	r	u	p	t	i	n	t	e	r	r	u	p
h	a	i	r	e	d		b	y		m	i	s	t	e	r		n	n	n
20	15	19	8	13	19	4	17	17	20	15	19	8	13	19	4	17	17	20	15
7	0	8	17	4	3	26	1	24	26	12	8	18	19	4	17	26	13	13	13
24	15	24	13	17	22	18	15	5	16	18	24	26	5	23	19	4	18	3	19
y	p	y	n	r	w	s	p	f	q	s	y		f	x	t	e	s	d	t

Зашифрований текст: ylxsqtdlxnrfdjemoaqauieqypynrwspfqsy fxtesdt

Дешифрування

Для того, щоб розшифрувати текст, ми маємо аналогічно повтрювати ключ навпроти тексту (символ до сивола) до закінчення тексту. Наступним етапом є виписання числових відповідників до літер тексту та літер ключа. Далі використовуємо «Адитивну групу поля F_3^3». Наприклад, якщо числовий

відповідник (ЧВ) до літири ключа «і» дорівнює «8», а якщо числовий відповідник до літири зашифрованого тексту «у» дорівнює «24», то використовуючи таблицюшукаємо «24» в колонці «8» і обираємо ЧВ з першої колонки того ж рядка що й «24», а далі отримуємо як «t»:

	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
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	25	26
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	23
3	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
4	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	19	22	23	21	25	26	24	19	20	18
5	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19
6	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
7	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
8	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
10	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
11	11	9	10	14’	12	13	17	15	16	20	18	19	23	21	22	26	24	25	22	0	1	5	3	4	8	6	7
12	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
13	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
14	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
15	15	16	171	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
16	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
17	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
18	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
20	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
21	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
22	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
23	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
24	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
25	25	26	24	19	20	18	22	23	21	7	8	6	1	0	2	4	5	3	16	17	15	10	11	9	13	14	12
26	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13

Отже, заповнюємо таблицю описаним вище методом:

i	n	t	e	r	r	u	p	t	i	n	t	e	r	r	u	p	t	i	n	t	e	r	r	u	p
y	l	x	s	q	t	d	l	x	n	r	f	d	j	e	m	o	a	q	a	u	i	e	q	y	p
8	13	19	4	17	17	20	15	19	8	13	19	4	17	17	20	15	19	8	13	19	4	17	17	20	15
24	11	23	18	16	19	3	11	23	13	17	5	3	9	4	12	14	0	16	0	20	8	4	16	24	15
19	7	4	26	2	14	13	5	4	17	4	13	2	4	26	22	8	11	11	26	1	4	26	2	7	0
t	h	e		c	o	n	f	e	r	e	n	c	e		w	i	l	l		b	e		c	h	a

t	i	n	t	e	r	r	u	p	t	i	n	t	e	r	r	u	p

y	n	r	w	s	p	f	q	s	y		f	x	t	e	s	d	t
19	8	13	19	4	17	17	20	15	19	8	13	19	4	17	17	20	15
24	13	17	22	18	15	5	16	18	24	26	5	23	19	4	18	3	19
8	17	4	3	26	1	24	26	12	8	18	19	4	17	26	13	13	13
i	r	e	d		b	y		m	i	s	t	e	r		n	n	n

Розшифрований текст: the conference will be chaired by mister nnn