Київський національний університет імені Тараса Шевченка

Факультет комп’ютерних наук та кібернетики

Кафедра інтелектуальних програмних систем

Математичні основи захисту інформації

Лабораторна робота №12

“Побудова кільця порядку 30 і шифрування повідомлень за допомогою нього повідомлень”

Виконали студенти 3-го курсу

Групи ІПС-32

Роботу виконали:

Ольховатий Ігор

Ковальов Володимир

Тряско Софія

Цілинко Олександр

Бондар Юлія

Волик Артем

Київ 2023

Тема: побудувати скінченне поля порядку 30. І використавши наведений алгоритм зашифрувати повідомлення

***Побудова кільця**:*
Маємо наступний алгоритм

GEN-$G(a, c, k)$
Вхід: Порядок k і коефіцієнти виразу $f(i) = a \cdot i + c$, де НСД(a, k)=1.
Вихід: Рядок таблиці додавання – одновимірний масив $b = (b_1, b_2, \ldots, b_k)$.
Метод:
1) for $i = 0$ to $k - 1$ do $b_{i+1} := a \cdot i + c \ (mod\ k)$ od
2) for $i = 1$ to k do
   if $(b_i = 0 \wedge i \neq k)$ then change b_i and b_k;
   if $(b_i = 1 \wedge i \neq 0)$ then change b_i and b_1;
   od (* визначили ізоморфізм $g(i) = b_i$, де $i = 1, 2, \ldots, k$ *)
3) за масивом $b = (b_1, b_2, \ldots, b_k)$ будуємо масив $P[1 \times k]$
   (* де зберігається визначальний рядок *)
   $P[0] := b_1$;
   for $i = 1$ to $k - 2$ do $P[b_i] := b_{i+1}$ od
   $P[b_{k-1}] := 0$. (* побудували визначальний рядок P *)

Правильність алгоритму випливає з того, що коли i пробігає повну систему лишків, то $a \cdot i + c$ теж пробігає повну систему лишків за умови, що НСД(a, k)=1 [2].

Візьмемо $f(i) = 7 * i + 3\ (7, 30) = 1$
Виконаємо перший пункт і отримаємо наступний рядок

```
3 10 17 24 1 8 15 22 29 6 13 20 27 4 11 18 25 2 9 16 23 0 7 14 21 28 5 12 19 26
```

Поставимо все на свої місця і отримаємо наступний рядок

```
1 10 17 24 3 8 15 22 29 6 13 20 27 4 11 18 25 2 9 16 23 26 7 14 21 28 5 12 19 0
```

Отже маємо наступний ізоморфізм $g : Z_{30} -> G_{30}$

```
g(0)=0
g(1)=1
g(2)=10
g(3)=17
g(4)=24
g(5)=3
g(6)=8
g(7)=15
g(8)=22
g(9)=29
g(10)=6
g(11)=13
g(12)=20
g(13)=27
g(14)=4
g(15)=11
g(16)=18
g(17)=25
g(18)=2
g(19)=9
g(20)=16
g(21)=23
g(22)=26
g(23)=7
g(24)=14
g(25)=21
g(26)=28
g(27)=5
g(28)=12
g(29)=19
```

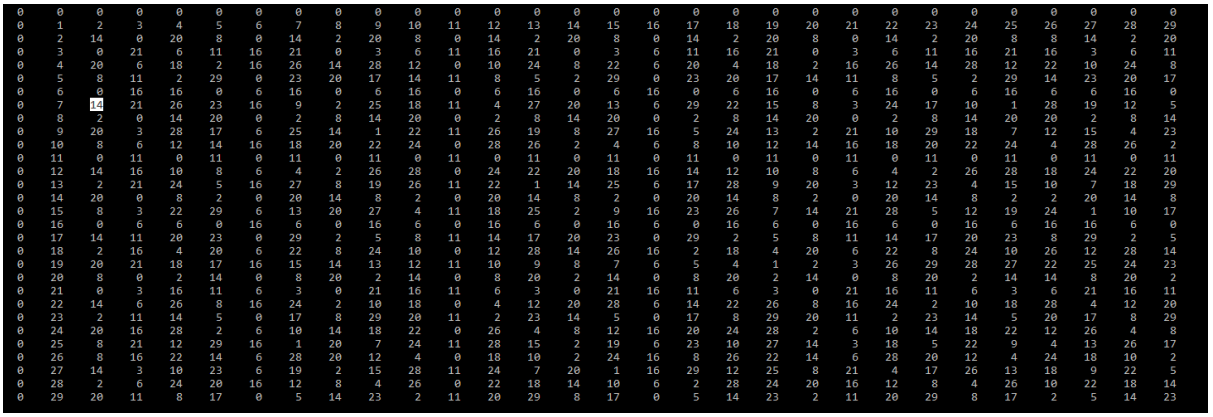
За допомогою 3 пункту згеренуємо визначальний рядок $P[1 * k]$
Отримали наступний визначальний рядок

```
1 10 9 8 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 0 27 28 29 26 3 2 7 4 5 6
```

Маємо наступну таблицю операцій
Додавання

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	10	9	8	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
2	9	8	7	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3	8	7	6	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
4	11	10	9	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	27
5	12	11	10	13	14	15	16	17	18	19	20	21	22	23	24	25	0	27	28
6	13	12	11	14	15	16	17	18	19	20	21	22	23	24	25	0	27	28	29
7	14	13	12	15	16	17	18	19	20	21	22	23	24	25	0	27	28	29	26
8	15	14	13	16	17	18	19	20	21	22	23	24	25	0	27	28	29	26	3
9	16	15	14	17	18	19	20	21	22	23	24	25	0	27	28	29	26	3	2
10	17	16	15	18	19	20	21	22	23	24	25	0	27	28	29	26	3	2	1
11	18	17	16	19	20	21	22	23	24	25	0	27	28	29	26	3	2	1	4
12	19	18	17	20	21	22	23	24	25	0	27	28	29	26	3	2	1	4	5
13	20	19	18	21	22	23	24	25	0	27	28	29	26	3	2	1	4	5	6
14	21	20	19	22	23	24	25	0	27	28	29	26	3	2	1	4	5	6	7
15	22	21	20	23	24	25	0	27	28	29	26	3	2	1	4	5	6	7	8
16	23	22	21	24	25	0	27	28	29	26	3	2	1	4	5	6	7	8	9
17	24	23	22	25	0	27	28	29	26	3	2	1	4	5	6	7	8	9	10
18	25	24	23	0	27	28	29	26	3	2	1	4	5	6	7	8	9	10	11
19	0	25	24	27	28	29	26	3	2	1	4	5	6	7	8	9	10	11	12

Множення



Отже ми отримали кільце за заданим визначальним рядком

Робота 1 абонента

Маємо наступну систему, яку ми згенерували випадковим чином

$2x_1 + 13x_2 + 28x_3 + 4x_4$

$25x_1 + 3x_2 + 8x_3 + 5x_4$

Це дорівнює $l(x)$

$L(x) = B_1(l(x) + (2,3)^T)$

Де $B_1 = \begin{bmatrix} 7 & 13 \\ 23 & 29 \end{bmatrix}$

Тоді маємо,що $L(x) = B_1(l(x) + (2,3)^T) =$

$$\begin{bmatrix} x_1 + 22x_2 + 24x_3 + 9x_4 + 9 \\ 23x_1 + 8x_2 + 0x_3 + 5x_4 + 17 \end{bmatrix}$$

Передаємо це 2 абоненту

Розв'язуємо систему $l(x) = 2x_1 + 13x_2 + 28x_3 + 4x_4 = 5$

$25x_1 + 3x_2 + 8x_3 + 5x_4 = 11$

Вибираємо довільний розв'язок $x = (0,4,0,0)$

Беремо довільне $a = (1,0,6,2)$

$x + a = (1,4,6,2)$

$l(a) = (16,20)$

$L(x + a) = (20,0)$

Він відправляє абоненту 1 ці значення

Абонент 1

Знаходимо обернену матрицю B_1^{-1} в G_{30}

$$B_1^{-1} = \begin{bmatrix} 2 & 29 \\ 9 & 15 \end{bmatrix}$$

б) $B_1^{-1} * (20,0)^T = (15,7)^T = l(x + a) + (2,3)^T$

в)$(15,7) - ((16,20) + (2,3)) = (5,11) = v$

Література

- Лекції з предмету “Математичні основи захисту інформації”
- https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D1%91%D1%85%D1%8D%D1%82%D0%B0%D0%BF%D0%BD%D1%8B%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%A8%D0%B0%D0%BC%D0%B8%D1%80%D0%B0
- https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0